ไมโครคอมพิวเตอร์

MICRO COMPUTER

วารสารเพื่อการพัฒนาเทคโนโลยีในองค์กรธุรกิจทุกระดับ

MAGAZINE
Vol. 35 No. 384
JULY 2017

Top Story

- WannaCrypt : มหันตภัยในโลกไซเบอร์
- การรับมือ "Ransomware" ของประเทศไทย
- ล้อมคอกก่อนวัวหาย จากภัยของ Ransomware
- Ransomware โจรเรียกค่าไถ่ยุคไซเบอร์ ที่ต้องรู้เท่าทันเพื่อป้องกันตัว
- Ransomware มัลแวร์เรียกค่าไถ่จับเป็นตัวประกัน

Attack & Defend

- วิเคราะห์เครือข่ายและระบบรักษาความปลอดภัย ด้วย Wireshark

ISSN 0857-0140

ซีเอ็ด

70 บาท

www.microvsmart.com

ยืน ภู่วรวรรณ

เมื่อเรากำลังก้าวสู่ยุคเอไอ

เมื่อประมาณ 30 ปีก่อนเมื่อครั้งที่ผมทำวิจัยเรื่องการประมวลผลภาษาธรรมชาติที่เน้นภาษาไทย มีโจทย์วิจัยจำนวนมาก เช่น การแบ่งแยกคำไทย ได้ทำการตัดแบ่งคำไทยเพื่อประโยชน์ในงานเวิร์ดโปรเซสซิ่ง ในสมัยนั้นเริ่มการวิจัยจากการหากฎเกณฑ์ ใช้กฎจำนวนมากเพื่อทำการแบ่งแยกพยางค์ไทย การประมวลผลกฎมีปัญหามาก ยิ่งเพิ่มกฎยิ่งต้องการการประมวลผลมากในเรื่องความเร็วในการทำงานของคอมพิวเตอร์ในสมัยนั้นที่จะคำนวณได้ทัน ทำให้ไม่สามารถประมวลผลได้เร็วตามที่ต้องการ ต่อมาจึงคิดหาวิธีการทางด้านสถิติ และการสร้างพจนานุกรมคำไทยจำนวนมากเข้ามาช่วย เพื่อทำการประมวลผลแบบเปรียบเทียบคำในพจนานุกรมกับข้อความในภาษาไทยเพื่อแบ่งแยกพยางค์ไทย ทำให้การประมวลผลทันต่อการใช้งาน อย่างไรก็ตามถ้าต้องการให้การประมวลผลได้ผลดี เสมือนใกล้เคียงกับการแบ่งแยกด้วยมนุษย์ จะต้องใช้ผสมระหว่างการใช้กฎกับการประมวลผลด้วยการใช้พจนานุกรมและเพิ่มเทคนิคทางอัลกอริทึมใหม่ๆ เข้าไป การทำให้ได้ดีจึงเสมือนการสร้างปัญญาประดิษฐ์หรือ “เอไอ” นั่นเอง

แต่ในปัจจุบันนี้การประมวลผลของคอมพิวเตอร์ดีกว่าครั้งเมื่อ 30 ปีก่อนหลายพันหลายล้านเท่า ทำให้การประมวลผลต่างๆ ทำได้ง่ายขึ้น การประยุกต์ทางด้านเอไอต่างๆ เริ่มสดใสขึ้น ดังจะเห็นได้จากการพัฒนาระบบประมวลผลภาษาธรรมชาติในปัจจุบันที่มีการใช้งานอย่างกว้างขวาง อย่างไรก็ตามการประมวลผลส่วนใหญ่ต้องใช้ซีพียูประสิทธิภาพสูงมากๆ และฐานข้อมูลประกอบขนาดใหญ่ การทำงานประมวลผลดังกล่าวจึงทำที่คลาวด์ซึ่งเป็นศูนย์ประมวลผลที่ใหญ่มาก

การที่คอมพิวเตอร์ใช้งานได้ดีจึงต้องทำให้คอมพิวเตอร์มีความสามารถในการทำงานสูง มีลักษณะของการเรียนรู้เหมือนมนุษย์ที่เรียกว่าปัญญาประดิษฐ์นั่นเอง ปัญญาประดิษฐ์จึงขึ้นอยู่กับกระบวนการของการสร้างกฎเกณฑ์และอัลกอริทึมต่างๆ ใช้ข้อมูลประกอบจำนวนมากในการคิดคำนวณ จึงขึ้นกับความเร็วของการประมวลผลของคอมพิวเตอร์โดยตรง

เมื่อขีดความสามารถของคอมพิวเตอร์ดีขึ้นกว่าเดิมเป็นจำนวนมาก ตามหลักการกฎของมัวร์ การประมวลผลในเชิงปัญญาประดิษฐ์จึงทำได้ดีกว่าเดิมอย่างมากมาย ดังจะเห็นได้จากการประมวลผลภาษาธรรมชาติ การแปลภาษาด้วยคอมพิวเตอร์สามารถทำได้ในเชิงพาณิชย์ในปัจจุบัน และมีแนวโน้มที่ดีขึ้นมาก

ในปี ค.ศ. 2017 กูเกิ้ลได้จัดงาน “กูเกิ้ลไอโอ” นำเสนอให้เห็นว่าขีดความสามารถของการประมวลผลแบบเอไอที่กำลังจะมีความสามารถเหนือกว่ามนุษย์ มีแนวโน้มที่จะประมวลผลเชิงความรอบรู้ต่างๆ ได้ดีกว่ามนุษย์ นับเป็นการปฏิรูปครั้งยิ่งใหญ่ต่อการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งการประมวลผลบนคลาวด์ กูเกิ้ลสร้างหน่วยประมวลผลเชิงสถาปัตยกรรมใหม่ที่เรียกว่า TPU ให้มีขีดความสามารถเพื่อรองรับเอไอในยุคต่อไป ทั้งนี้เนื่องจากว่าสามารถสร้างขีดความสามารถของการคำนวณบนคลาวด์ได้ดีกว่าการคำนวณด้วยเครื่องคอมพิวเตอร์แบบตั้งโต๊ะอย่างมาก

“อัลฟาโกะ” เป็นตัวอย่างการใช้ปัญญาประดิษฐ์ซึ่งเป็นการคำนวณบนคลาวด์ พัฒนาโดยบริษัท อัลฟ่า กูเกิ้ลเอาชนะเซียนโกะหรือหมากล้อมมือวางอันดับหนึ่งของโลกอย่าง “Ke Jie” หนุ่มชาวจีนวัย 19 ปีลงได้ นับเป็นการตอกย้ำความอัจฉริยะของปัญญาประดิษฐ์หรือเอไอ ซึ่งเท่ากับว่าอัลฟาโกะเป็นเอไอที่มีความเหนือกว่ามนุษย์

ในงานกูเกิ้ลไอโอ ซันดาร์ พิชัย ซีอีโอของกูเกิ้ลประกาศเปิดเวทีงานประชุมด้วยการโชว์ตัวเลขว่าระบบปฏิบัติการแอนดรอยด์ของกูเกิ้ลมีการใช้งานบนอุปกรณ์มากกว่า 2 พันล้านเครื่อง โดยในปีนี้กูเกิ้ลยังเปิดตัวเอไอใหม่ชื่อกูเกิลเลนส์ (Google Lens) ซึ่งจะเป็นส่วนหนึ่งของบริการผู้ช่วยส่วนตัว (Google Assistant) สำหรับผู้ใช้สมาร์ทโฟนแอนดรอยด์ โดย Lens สามารถวิเคราะห์วัตถุรอบตัวผู้ใช้งาน โดยผู้ใช้สามารถสแกนหรือถ่ายภาพสิ่งที่ต้องการรู้ นอกจากนี้กูเกิ้ลได้พัฒนากูเกิ้ลโฮม (Google Home) เครื่องโต้ตอบกับมนุษย์ด้วยเสียงพูดให้ดีขึ้นกว่าเดิม และเสนอ “เอพีไอ” ให้บริษัทผลิตเครื่องไฟฟ้าในบ้านได้พัฒนาเครื่องใช้ไฟฟ้าอัจฉริยะหลากหลายรูปแบบที่สามารถทำงานร่วมกับระบบผู้ช่วยของกูเกิ้ลบนกูเกิ้ลโฮมได้อย่างเต็มประสิทธิภาพเพื่อทำให้เทคโนโลยีการเชื่อมต่อที่ล้ำสมัยโดยร่วมกับ IoT เพื่อความสะดวกสบายต่อการใช้ชีวิตแบบสมาร์ทในปัจจุบัน โดยเริ่มทยอยเปิดใช้งานร่วมกับกูเกิ้ล โฮมแล้วสำหรับเครื่องใช้ไฟฟ้าที่เป็นแบบ IoT สามารถเชื่อมต่ออินเทอร์เน็ตได้สั่งงานผ่านกูเกิ้ลโฮม เช่น เครื่องซักผ้าและเครื่องอบผ้า ตู้เย็น เตาอบ เครื่องฟอกอากาศ เครื่องปรับอากาศ และหุ่นยนต์เครื่องดูดฝุ่น

เตรียมพบกับ “เอไอ” ในยุคที่เอไอกำลังมีขีดความสามารถและการใช้งานได้ใกล้เคียงกับมนุษย์มากขึ้นที่จะพบเห็นได้ในชีวิตประจำวัน

วางแผงแล้ววันนี้

ผลงานล่าสุดของทีมงานนิตยสารไมโครคอมพิวเตอร์

MICRO COMPUTER

เมื่อสุดยอดอุปกรณ์ได้สุดยอดปรมาจารย์
วิเคราะห์เจาะเบื้องลึกตกผลึกถึงแก่นเครือข่าย
ด้วยคำอธิบายง่ายๆ ครบเครื่องสมบูรณ์แบบสุดๆ

คัมภีร์ออกแบบติดตั้งอุปกรณ์เครือข่าย Cisco เล่ม 1
New Edition

- ปรับปรุงเนื้อหาเพิ่มเติมจาก “คัมภีร์ออกแบบติดตั้งอุปกรณ์เครือข่าย Cisco เล่ม 1” โดยสิ้นเชิงเพื่อให้สอดคล้องกับเทคโนโลยีที่มีการเปลี่ยนแปลง
- เรียนรู้แนวทางออกแบบติดตั้งและแก้ไขปัญหาจากการวิเคราะห์เจาะเบื้องลึกถึงแก่นของระบบเครือข่าย Cisco อย่างครบเครื่องสมบูรณ์แบบที่สุด
- เน้นทั้งภาคทฤษฎีและภาคปฏิบัติที่นำไปใช้งานได้จริง
- สามารถนำไปใช้เป็นหนังสืออ้างอิง ตำราประกอบการเรียนตำราที่ใช้สอนในสถาบันการศึกษาหลายแห่ง
- ตลอดจนผู้ที่กำลังศึกษาเกี่ยวกับการดูแลติดตั้งอุปกรณ์เครือข่าย Cisco รวมทั้งเพื่อเตรียมสอบ CCNA, CCNP และ CCIE
- เหมาะสำหรับท่านที่สนใจและหลงใหลในวิชาการระบบเครือข่ายอย่างแท้จริง

หาซื้อได้ที่ซีเอ็ดบุ๊คเซ็นเตอร์ทุกสาขา หรือที่ร้านหนังสือชั้นนำทุกแห่งทั่วประเทศ
สั่งซื้อจำนวนมาก กรุณาติดต่อ ฝ่ายขาย บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน) โทรศัพท์ 0-2739-8222

จัดพิมพ์และจัดจำหน่ายโดย

บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน)
SE-EDUCATION PUBLIC COMPANY LIMITED
อินเตอร์ลิ้งค์ทาวเวอร์ ชั้น 19 เลขที่ 1858/87-90 ถนนบางนา-ตราด กม. 4.5 แขวงบางนา เขตบางนา กรุงเทพฯ 10260

From Editor

ณิญาพัณณ์ ฤทธิพีระศักดิ์
niyaphan@se-ed.com

AI และ Internet of Things จะมีผลกระทบกับชีวิตในอนาคตมากที่สุด

เมื่อเร็วๆ นี้ ไมโครซอฟท์ได้เปิดเผยผลการสำรวจหัวข้อ **อนาคตด้านดิจิทัลในเอเชีย (Microsoft Asia Digital Future Survey)** ในกลุ่มคนอายุ 18-24 ปี จำนวน 1,400 คน ทั่วเอเชียแปซิฟิก อาทิ ออสเตรเลีย จีน ฮ่องกง อินเดีย อินโดนีเซีย ญี่ปุ่น เกาหลี มาเลเซีย นิวซีแลนด์ ฟิลิปปินส์ สิงคโปร์ ไต้หวันและเวียดนาม โดยมีตัวแทน 100 คนจากประเทศไทย

ผู้ตอบแบบสำรวจชาวไทยจัดให้ปัญญาประดิษฐ์ (AI) และอินเทอร์เน็ตออฟธิงส์ (IoT) เป็นเทคโนโลยีอันดับต้นๆ ที่จะเข้ามามีอิทธิพลเปลี่ยนแปลงวิถีชีวิตผู้คน เพราะไม่กี่ปีที่ผ่านมานี้ได้เกิดอุปกรณ์ล้ำสมัยใหม่ๆ รวมทั้งคลาวด์และโลกข้อมูลที่ประสานพลังกันทำให้วิสัยทัศน์ที่มองอนาคตว่า *AI และ IoT จะก้าวเข้ามาเป็นส่วนหนึ่งในชีวิตแบบดิจิทัลของมนุษย์อย่างแยกไม่ออกและมีความชัดเจนมากขึ้น*

AI ยังเกี่ยวข้องกับการสร้างจักรกลอัจฉริยะ หรืองานบริการที่ตอบโต้เหมือนมนุษย์ ฟีเจอร์ที่เริ่มพบได้ในแทบทุกอย่างตั้งแต่การแปลภาษา ไปจนถึงผู้ช่วยเสมือนหรือวิดีโอเกมส์ การนำเอาศักยภาพของ AI เข้ามาทำงานซ้ำๆ เช่น การวิเคราะห์ข้อมูลจำนวนมาก การจดจำคำพูด การแก้ปัญหาจะช่วยให้ผู้คนบรรลุเป้าหมายได้มากขึ้นในขณะที่ทำงานน้อยลง หรือการเพิ่มประสิทธิภาพให้แก่งานนั่นเอง

IoT หมายถึง เครือข่ายของวัตถุที่เชื่อมต่อเข้ากับอินเทอร์เน็ต ที่สามารถสื่อสารระหว่างกัน ระหว่างอุปกรณ์และข้ามระบบได้ ซึ่งกำลังเติบโตขยายวงกว้างขึ้นเรื่อยๆ อินเทอร์เน็ตออฟธิงส์ รวมถึงทุกสิ่งทุกอย่างตั้งแต่เซนเซอร์บนท้องถนน เครื่องใช้ไฟฟ้าในบ้าน อุปกรณ์สวมใส่ และยานพาหนะ

เทคโนโลยีอันดับสองที่คนรุ่นใหม่กล่าวถึงกันมากรองลงมา คือ **VR/MR/AR** เทคโนโลยีความจริงเสริมคือการนำเอาโลกเสมือนไปวางอยู่ในโลกแห่งความจริง ขณะที่ความจริงเสมือนคือการสร้างความรู้สึกแบบโลกแห่งความจริงมาไว้ข้างในโลกเสมือน ส่วนความจริงผสมรวบรวมเอาทั้งสองส่วนประกอบเข้าด้วยกัน โดยขณะที่ผู้ใช้กำลังท่องไปในโลกความจริงก็จะสามารถมีปฏิสัมพันธ์กับวัตถุเสมือนได้ เห็นและสัมผัสมันได้ โดยจำลองความรู้สึกในมิติต่างๆ อาทิเช่นการสัมผัสได้ถึงความลึกของวัตถุเสมือน เป็นต้น

เมื่อถามถึงชีวิตในวันข้างหน้า เยาวชนไทยเชื่อว่าการที่จะประสบความสำเร็จในอนาคตได้นั้น จะต้องอาศัยสถาบันการศึกษาที่สามารถสร้างความพร้อมให้นักเรียนมีทักษะที่ทันยุคสมัย เพื่อนำเอานวัตกรรมในอนาคตมาใช้ได้อย่างมีประสิทธิภาพ (57%) ตามด้วยการทำให้เทคโนโลยีในอนาคตมีราคาไม่แพงและสามารถเข้าถึงได้ (17%) และการสร้างสภาวะแวดล้อมทางธุรกิจที่เอื้อต่อสตาร์ทอัพ (13%)

นอกจากนั้นแล้วกลุ่มคนรุ่นใหม่เหล่านี้ยังแสดงความเชื่อมั่นว่าความร่วมมือระหว่างภาครัฐและภาคเอกชน (49%) จะมีความจำเป็นอย่างยิ่งในการพลักดันนวัตกรรมใหม่ๆ มากกว่าการที่รัฐบาลเดินหน้าอยู่เพียงฝ่ายเดียว (20%) หรือภาคเอกชนทำเพียงลำพัง (16%)

สนับสนุน
โดย บริษัทพลิตภัณฑ์กระดาษไทย จำกัด
WWW.THAIPAPER.COM
SCG

- เจ้าของ บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน)
- ที่ปรึกษา ศ.ดร.ศรีศักดิ์ จามรมาน, ดร.ควรชิต มาลัยวงศ์, น.พ.ณรงค์ บุณยะรัตเวช, รศ.กฤษดา วิศวธีรานนท์, วิชิต ปุณวัตร์
- คณะบรรณาธิการที่ปรึกษา รศ.ยืน ภู่วรวรรณ, รศ.ดร.พิชิต สุขเจริญพงษ์, รศ.ดร.ชัยยงค์ วงศ์ชัยสุวัฒน์, อัญชลี จำรัสฤทธิรงค์, น.อ.ไพศาล สงวนหมู่, จเร เลิศสุดวิชัย, ดร.สมนึก คีรีโต, สุรศักดิ์ สงวนพงษ์, อดิศักดิ์ ตันตาปกุล
- หัวหน้ากองบรรณาธิการ ณิญาพัณณ์ ฤทธิพีระศักดิ์
- กองบรรณาธิการ ปฐมาภรณ์ กันตาคม
- หัวหน้าแผนกศิลป์ รังสฤษฏ์ ผมประทุม
- ฝ่ายโฆษณา ณัฐวีร์ วงศ์สิริกุล โทรศัพท์ 0-2739-8226
- พนักงานรับ-ส่งเอกสาร สุรเชษฐ พู่ระหง, กสิวัฒน์ มฤคสนธิ
- หน่วยบริการสมาชิก มานิต เข็มเงิน โทรศัพท์ 0-2739-8111 กด 1 อัตราค่าสมาชิก 840 บาท (12) ฉบับ ส่งเงินค่าสมาชิกในนามบริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน) ชั้นที่ 20 อาคารอินเตอร์ลิงค์ทาวเวอร์ (อาคารเนชั่นทาวเวอร์เดิม) เลขที่ 1858/87-90 ถ.บางนาตราด แขวงบางนา เขตบางนา กรุงเทพฯ 10260 โทรศัพท์ 0-2739-8111 โทรสาร 0-2739-8294, 0-2739-8117
- ทำเพลตสี/ขาว-ดำ โมเดอร์น ฟิล์ม เซ็นเตอร์ จำกัด โทรศัพท์ 0-2938-0403-4, 0-2513-4723
- ฝ่ายจัดจำหน่ายเขตกรุงเทพฯ บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน) โทรศัพท์ 0-2739-8222
- ฝ่ายจัดจำหน่ายต่างจังหวัด บริษัท นานาสาส์น จำกัด โทรศัพท์ 0-2433-6855, 0-2880-7345-6
- บรรณาธิการผู้พิมพ์ผู้โฆษณา วิบูลย์ศักดิ์ อุดมวนิช จดหมายถึงกองบรรณาธิการบทความและข้อคิดเห็นต่าง ๆ กรุณาส่งไปที่ หัวหน้ากองบรรณาธิการ นิตยสารไมโครคอมพิวเตอร์ niyaphan@se-ed.com (กองบรรณาธิการขอสงวนสิทธิ์ในการตัดต่อ ย่อสรุปต้นฉบับได้โดยไม่ต้องขอความเห็นจากผู้ส่ง)
- สำนักงานติดต่อ บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน) ชั้น 20 อาคารอินเตอร์ลิงค์ทาวเวอร์ (อาคารเนชั่นทาวเวอร์เดิม) เลขที่ 1858/87-90 ถ.บางนา-ตราด แขวงบางนา เขตบางนา กรุงเทพฯ 10260 โทรศัพท์ 0-2739-8111 โทรสาร 0-2739-8228 ฝ่ายข่าว micropress@se-ed.com

วางแผงแล้ว

ผลงานล่าสุดของทีมงานนิตยสารไมโครคอมพิวเตอร์

MICRO COMPUTER

เปิดมุมมองของแนวความคิดด้านบริการไอทีภายใต้มาตรฐานระดับสากลสำหรับทุกองค์กร

- เนื้อหาเจาะลึกมาตรฐานบริการไอทีระดับโลกเล่มแรกและเล่มเดียวในเมืองไทย
- เพื่อการเริ่มต้นแผนยุทธศาสตร์แห่งการบริหารจัดการวงจรชีวิตของกระบวนการบริการที่แผนกไอทีสามารถให้กับหน่วยธุรกิจ โดยเน้นคำว่า “Best Practice” หรือวิธีการทำงานเชิงปฏิบัติที่ดีที่สุด
- จากวิสัยทัศน์ไปสู่การจัดสร้างกลยุทธ์และแปรเปลี่ยนเป็นภารกิจของงานบริการไอทีที่จะต้องกำหนดขึ้นเพื่อจัดสร้างยุทธศาสตร์ในการพัฒนาจัดสร้างปรับปรุงระบบบริการไอทีให้มีประสิทธิภาพ
- เมื่อเทคโนโลยีและสภาพแวดล้อมเปลี่ยนไป วิธีให้บริการในระบบไอทีต้องได้รับการออกแบบและพัฒนาบริการใหม่ๆ ขึ้นมารองรับ
- ช่วยให้องค์กรรับมือกับการเปลี่ยนแปลงที่จะนำมาซึ่งประโยชน์หลายสถานด้วยการปรับปรุงกระบวนการเซอร์วิสทั้งที่มีอยู่แล้วและจัดทำขึ้นมาใหม่
- เน้นการดำเนินการบริการไอทีให้กับผู้ใช้งานโดยเฉพาะพร้อมกับมองหาจุดบกพร่องและจัดการแก้ไขให้ลุล่วง
- ปรับปรุงประสิทธิภาพของ IT Service อย่างต่อเนื่องเพื่อช่วยให้สามารถคงไว้ซึ่งประสิทธิภาพและความต้องการในการใช้บริการต่อไป
- เหมาะสำหรับเป็นคู่มือเตรียมสอบรับรองมาตรฐานและคู่มือประกอบแนวทางปฏิบัติด้านงานบริการไอทีภายในองค์กร

หาซื้อได้ที่ ซีเอ็ดบุ๊คเซ็นเตอร์ ทุกสาขา หรือที่ร้านหนังสือชั้นนำทุกแห่งทั่วประเทศ

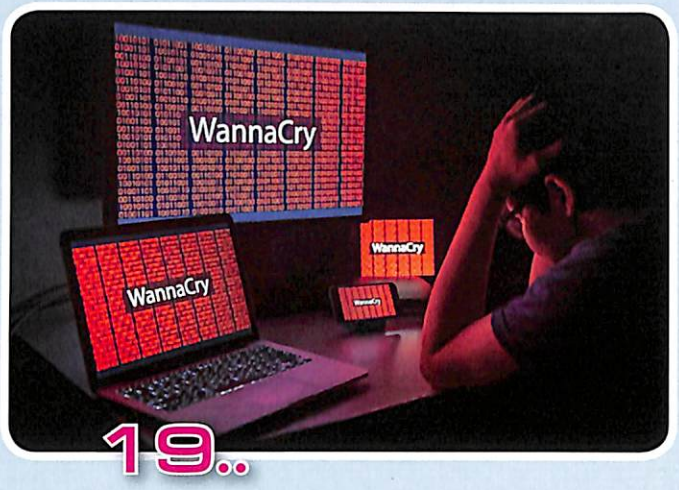
สั่งซื้อจำนวนมาก กรุณาติดต่อ **ฝ่ายขาย** บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน) โทรศัพท์ 0-2739-8222

จัดพิมพ์และจำหน่ายโดย **บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน)**

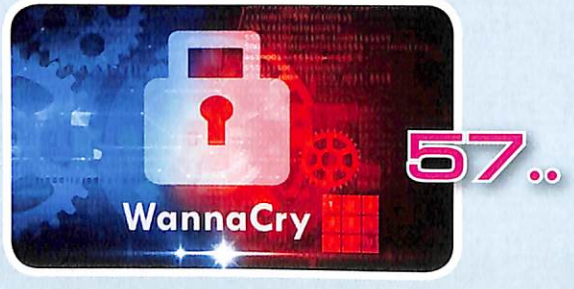
อาคารอินเตอร์ลิ้งค์ ชั้น 19 เลขที่ 1858/87-90 ถนนบางนา-ตราด กิโลเมตรที่ 4.5
แขวงบางนา เขตบางนา กรุงเทพฯ 10260
โทรศัพท์ 0-2739-8000 โทรสาร 0-2751-5058-59, 0-2751-5460-31 http://www.se-ed.com

CONTENTS

• Vol. 35 No. 384
• JULY 2017



Top Story



45..

ผลงานล่าสุดของทีมงานนิตยสารไมโครคอมพิวเตอร์

MICRO COMPUTER

วางแผงแล้ววันนี้

ออกแบบชีวิต
ให้เท่าทันความผันแปรบนโลกดิจิทัล
ที่จะช่วยให้คุณรวยได้

เวทีธุรกิจบนโลกดิจิทัล ที่ช่วยให้คุณรวยได้

- ประตูที่เปิดกว้างขึ้นของผู้ประกอบการรายใหม่ ที่สามารถกำหนดจุดขายของสินค้าและบริการของตน
- เป็นกระจกสะท้อนครรลองของการเริ่มต้นจากศูนย์ เพื่อสร้างสินค้าด้านฮาร์ดแวร์ที่สามารถขยายขนาดการเติบโตทางธุรกิจตนเองได้
- ยกระดับฐานะของการทำธุรกิจจาก Startups ไปเป็นกิจการขนาดใหญ่
- ฉายภาพของผลิตภัณฑ์สินค้าในอุตสาหกรรมต่างๆ ที่มีในปัจจุบันเพื่อให้เกิดทั้งแรงบันดาลใจ และความเข้าใจต่อการเติบโตของตลาด

หาซื้อได้ที่ซีเอ็ดบุ๊คเซ็นเตอร์ทุกสาขา หรือที่ร้านหนังสือชั้นนำทุกแห่งทั่วประเทศ
สั่งซื้อจำนวนมาก กรุณาติดต่อ ฝ่ายขาย *บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน) โทรศัพท์ 0-2739-8222*

จัดพิมพ์และจัดจำหน่ายโดย

บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน)
SE-EDUCATION PUBLIC COMPANY LIMITED
อินเตอร์ลิ้งค์ทาวเวอร์ ชั้น 19 เลขที่ 1858/87-90 ถนนบางนา-ตราด กม. 4.5 แขวงบางนา เขตบางนา กรุงเทพฯ 10260

CONTENTS

• Vol. 35 No. 384
• JULY 2017

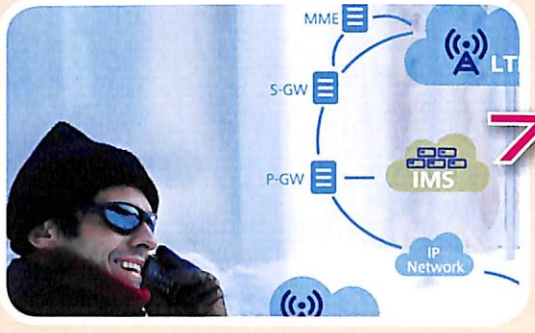
Attack & Defend

Intrend

Technology Update

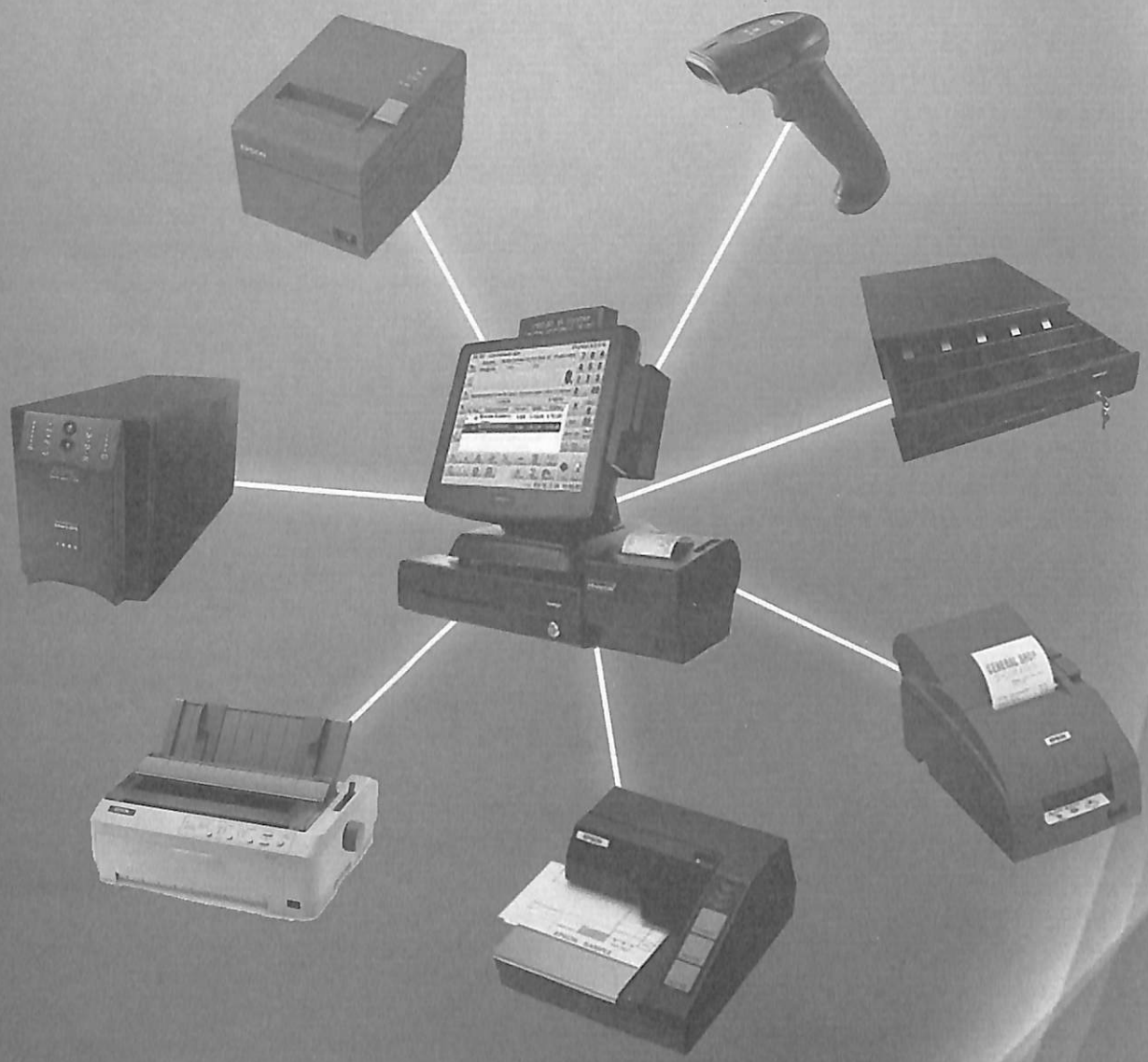
Professional Office

VB's Corner



Column

GREATERTECH CO.,LTD.



อะไหล่แท้
บริการ รับ-ส่ง นอกสถานที่
เครื่องสำรองสำหรับ Maintenance

★ เครื่อง Slip Printer ตระกูล TM-Series ของ EPSON ที่ยังอยู่ในประกันสามารถส่งเคลมได้ที่ Greatertech ★

EPSON EXCEED YOUR VISION | CIPHERLAB | Honeywell | POSIFLEX | VPOS | MAKEN Make It Happen

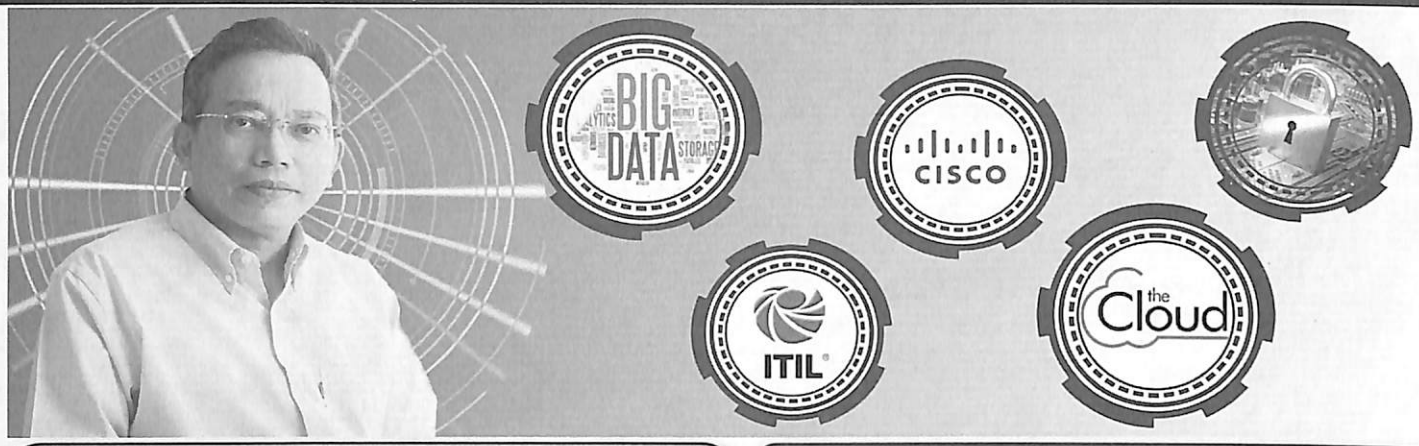
EPSON SERVICE

สำนักงานใหญ่ : 999/43 หมู่ 4 แขวงคลองถนน
เขตสายไหม กรุงเทพฯ 10220
โทร.0-2153-0581-2 แฟกซ์. 0-21530581-2 ต่อ 18

สาขา 1 (ศูนย์บริการ) : 44/156 หมู่ 8 แขวงท่าแร้ง เขตบางเขน
กรุงเทพฯ 10230 โทร. 0-2945-9295-6, 081-256-6638, 081-616-3453
แฟกซ์. 0-2945-9295-6 ต่อ 18

★ ปรัชญามุ่งมั่นของเรา : เรียนจบแล้วต้องทำได้ ★

เราสามารถให้หลักประกันความสำเร็จด้านไอทีแก่ท่าน ด้วยหลักสูตรที่เน้นภาคปฏิบัติ และวิธีคิดและแก้ปัญหาด้านไอที ที่สามารถนำไปใช้ได้ในชีวิตจริง ตอบโจทย์ทุกปัญหาที่ท่านจะเผชิญจากอาจารย์ผู้ถ่ายทอดในระดับแนวหน้า



เรียนจบแล้วต้องทำได้

วลีนี้เป็นปรัชญาของเรา ที่เราใช้กำหนดเป็นเป้าหมาย ในการสรรหาวิธีการพัฒนาบุคลากรด้านไอที ที่มีประสิทธิภาพสูง เราเน้นวิธีการที่จะนำไปสู่ความสำเร็จ 2 วิธีคือ

1. วิธีคิด และวิธีการเรียนรู้

วิธีคิดคือแนวทางเชิงตรรกะ การนำเสนอ การสื่อสาร การถ่ายทอดความรู้ วิธีการเรียนรู้ วิธีการแก้ปัญหาต่างๆในวิชาด้านไอที เป้าหมายคือให้ผู้ผ่านการอบรม สามารถนำไปประยุกต์ใช้งาน โดยไม่ขึ้นอยู่กับเทคโนโลยีของผลิตภัณฑ์รุ่นใด ตัวอย่างเช่น วิธีการติดตั้ง VPN เราจะให้แนวทางที่ท่านสามารถนำไปใช้กับอุปกรณ์ Firewall /Router /Server ทุกรุ่น ทุกแบรนด์เนม ทุกระบบปฏิบัติการได้ ดังนั้นผู้เข้าอบรมจะสามารถนำเอาเครื่องมือความรู้นี้ไปใช้ประโยชน์ได้อย่างกว้างขวาง สามารถรับมือกับเทคโนโลยีเดียวกันจากทุกผลิตภัณฑ์

การนำเสนอและการถ่ายทอดความรู้ ในรูปแบบจังหวะย่างก้าว เป็นขั้นเป็นตอน ซึ่งเป็นจุดเด่นของเรามากกว่า 20 ปี ผู้เรียนสามารถได้ประเด็นหลักมีความชัดเจน สามารถมองเห็นภาพและสามารถต่อยอด ไปใช้ประโยชน์ได้

20 ปีที่ผ่านมา เราสร้าง บุคลากรที่ประสบผลสำเร็จมามากมาย เราอยู่ได้ทุกวันนี้ จากการตลาดที่บอกต่อๆกัน และท่านที่ผ่านการอบรมกลับมา อัพเดทความรู้ใหม่ๆ อย่างต่อเนื่อง

การทำ Group Discussion ก็เป็นอีกรูปแบบหนึ่งที่ผู้เข้าอบรมช่วยกันแก้ปัญหาและจัดทำ Solution ที่อาจารย์ผู้สอนกำหนดขึ้นจากชีวิตจริง วิธีนี้จะช่วยให้ผู้เข้ารับการอบรม มีแนวคิดสร้างสรรค์ และสามารถทำงานเป็นทีมได้เป็นอย่างดี

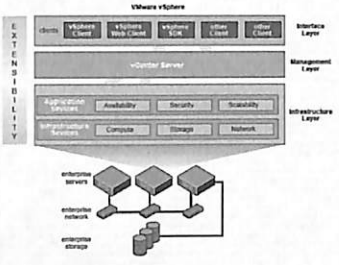
2. ภาคปฏิบัติ และภาคทดลองที่นำไปใช้งานได้จริง

การทดลอง และภาคปฏิบัติต่างๆ ที่ใช้กับเครื่องมือจริง และสภาพห้องเรียนที่จำลองระบบไอทีในองค์กรขนาดกลางและขนาดใหญ่ รวมทั้งวิธีการพิสูจน์ ความสำเร็จของ ภาคทดลอง จะช่วยให้ท่านมีทักษะ และความชำนาญ สูงสุด สามารถนำไปใช้งานในชีวิตจริงได้

นอกจากนี้ ในบางหลักสูตร ยังเปิดโอกาสให้ท่านที่ผ่านการอบรม ได้ฝึกงานเพื่อเพิ่มทักษะและความรู้อย่างต่อเนื่อง เพื่อให้มั่นใจว่าจะสามารถนำไปใช้งานได้เต็มที่

แนะนำเรียนหลักสูตร

VMware vSphere: Install, Configure, Manage and Deployment



หลักสูตรนี้ เน้นหนักไปในแนวทางปฏิบัติ เชิงติดตั้ง การจัดคอนฟิก การบริหารจัดการ และการนำมาใช้งาน สำหรับองค์กรทั่วไป ทุกขนาด รวมทั้ง Data Center ด้วยการใช้ VMware vSphere 6 ซึ่งรวมทั้ง VMware ESXi 6 ตลอดจน VMware vCenter Server 6 โดยกว่าครึ่งหนึ่งของเวลาในห้องเรียน เน้นหนักไปที่ Hand On หรือภาคปฏิบัติล้วนๆ หลักสูตรนี้จะช่วยให้ท่านมีความเข้าใจ และสามารถติดตั้ง และบริหารจัดการ vSphere ได้อย่างมีประสิทธิภาพ สามารถนำไปใช้งานได้จริง

ท่านจะได้เรียนอะไรจากหลักสูตรนี้

- สามารถติดตั้งและใช้งาน รวมทั้งคอนฟิก Virtual Infrastructure ด้วย VMware vSphere
- จัดสรร เครือข่าย และแหล่งจัดเก็บข้อมูลอย่างมีประสิทธิภาพ
- จัดสร้าง Direct Attached Storage และ Storage Area Network
- ยกระดับ vCenter Server สำหรับการรักษาความปลอดภัยและมีประสิทธิภาพภายในที่ทำงาน
- สามารถจัดสรร ทรัพยากรในรูปแบบของ Cluster แบบพลวัตร
- สามารถปรับปรุงความพร้อมใช้งาน ของระบบโดยใช้ vMotion และ High Availability (HA)
- ใช้ VMware vSphere Update Manager เพื่อจัดการกับ patches
- ดำเนินการ Troubleshooting ESXi hosts, Virtual Machines, และการทำงานของ vCenter Server
- ใช้ VMware vSphere Storage vMotion เพื่อที่จะ Migrate Virtual Machine Storage
- เฝ้าดู การใช้งานของทรัพยากร และบริหารจัดการกับ Resource Pools
- ใช้ VMware vRealize Operations Manager เพื่อระบุและแก้ไขปัญหา โดยใช้วิธีการ Analytics และ Alerts

หลักสูตรเตรียมสอบ CISSP (CISSP Certification Prep Course)

หลักสูตรนี้เน้นเกี่ยวกับแนวความคิดในการบริหารจัดการกับระบบรักษาความปลอดภัย ที่ได้มาตรฐานเป็นที่ยอมรับ ในวงการธุรกิจและอุตสาหกรรม ครอบคลุมโดเมนทั้ง 8 ที่เป็นมาตรฐานของ CISSP CBK (Common Body of Knowledge) จากความรู้ที่ท่านจะได้รับในหลักสูตรนี้ จะช่วยเพิ่มขีดความสามารถในการดูแลเกี่ยวกับระบบรักษาความปลอดภัย ซึ่งนับวันทวีความต้องการมากยิ่งขึ้น หลักสูตรนี้ท่านจะสามารถกำหนดหรือระบุความเสี่ยง ที่มีผลกระทบต่อความปลอดภัยแก่ข้อมูลข่าวสาร อย่างรอบด้าน ที่สำคัญคือหลักสูตรนี้ จะช่วยให้ท่านเตรียมความพร้อม ด้วยข้อมูลทุกอย่างที่จำเป็น เพื่อให้ท่านมีความพร้อมมากที่สุด เพื่อรับใบประกาศ CCISP จาก International Information system security Consortium เนื้อหาสาระครอบคลุม CCISP อย่างครบถ้วน

สอบถามรายละเอียดเพิ่มเติมได้ ที่ www.cyberthai.com

American Information System

บริษัท อเมริกัน อินฟอร์เมชั่น ซิสเต็ม จำกัด

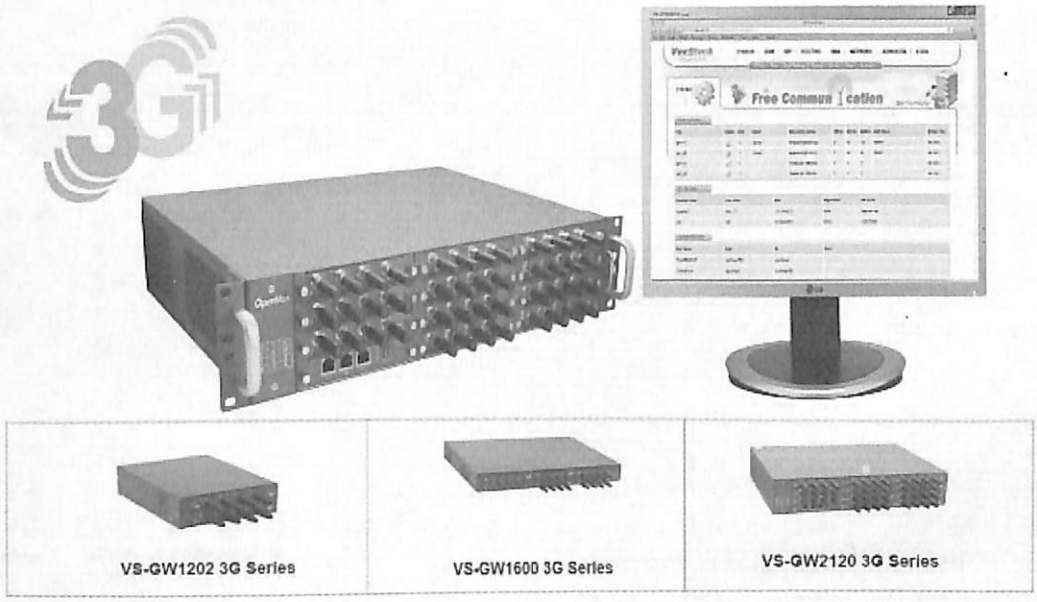
230 CS Tower ชั้น 10 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพฯ 10310

Tel. 0-2274-0864, 0-2274-0867, 0-2692-5203 Mobile. 089-776-7190, 081-667-6981

สอบถามรายละเอียดเพิ่มเติมได้ ที่ www.cyberthai.com หรือ infodesk@cyberthai.com, cyberthaiais@gmail.com, www.facebook.com/cyberthai

■ Poise Technology Co., Ltd.

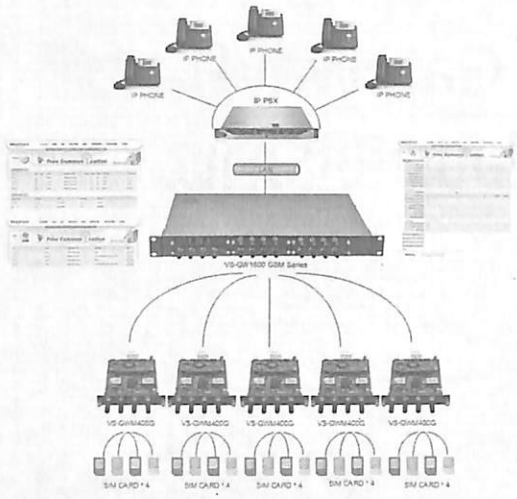
OpenVox VoxStack 3G Gateway!! วางใจได้เหมือนเดิมที่เพิ่มเติมคือประสิทธิภาพ



อุปกรณ์ GSM Gateway ที่เพียบพร้อมด้วยฟังก์ชั่นการทำงานหลากหลาย ออกแบบให้ครอบคลุมทุกการใช้งานเพื่อรองรับการเพิ่มโมดูลเป็นสล้อต

หากวันนี้คุณกำลังมองหา GSM Gateway ที่รองรับคลื่นความถี่ 3G 850/900/1900/2100 เมกะเฮิรตซ์ เพื่อใช้งานร่วมกับระบบ VoIP ของคุณ เราขอเสนอ VoxStack 3G Gateway เป็นอุปกรณ์ GSM Gateway ที่เพียบพร้อมไปด้วยฟังก์ชั่นการทำงานที่หลากหลาย ครอบคลุมทุกๆ การใช้งานที่คุณต้องการ ด้วยการออกแบบอุปกรณ์มาเพื่อรองรับการใส่เพิ่มโมดูลเป็นสล้อต โดยอุปกรณ์ VoxStack 3G Gateway สามารถรองรับเครือข่าย 3G/UMTS ได้ตั้งแต่ 4-44 คู่สาย หรือรองรับการใช้งานซิม 4-44 ซิมการ์ดนั้นเอง โดย 1 โมดูลจะรองรับซิมการ์ด 4 ซิม ผู้ใช้สามารถเลือกเพิ่มโมดูลได้ตามความต้องการของผู้ใช้งาน เริ่มต้นที่ 1 โมดูลรองรับการใช้งานซิมการ์ด 4 ซิม 2 โมดูลรองรับรับการใช้งานซิมการ์ด 8 ซิม หรือรองรับการใช้งานซิมการ์ดมากสุดต่ออุปกรณ์ถึง 44 ซิม โดยแต่ละโมดูลจะทำงานเป็นอิสระแยกออกจากกัน เนื่องจากแต่ละโมดูลมีซีพียูในตัวเอง เพื่อการทำงานที่มีประสิทธิภาพสูงสุด หากโมดูลใดโมดูลหนึ่งเกิดการขัดข้องจะไม่มีผลกระทบกับโมดูลอื่น นั่นหมายความว่าตัวอุปกรณ์ยังคงสามารถใช้งานได้ปกติ โดยระบบจะทำการสลับการทำงานไปใช้อีกโมดูลหนึ่งทันที ในกรณีเดียวกันใน 1 โมดูลรองรับการใช้งานซิมการ์ด 4 ซิม ถ้าซิมใดซิมหนึ่งเกิดการขัดข้อง ระบบจะสลับให้อีกซิมทำงานโดยอัตโนมัติเช่นเดียวกัน ซึ่งรูปแบบการทำงานที่เป็นอิสระต่อกันเป็นการลดอัตราการดาวน์ของระบบให้เป็นศูนย์ ซึ่งเป็นจุดเด่นของแบรนด์ OpenVox ที่สามารถเอาชนะใจผู้ใช้งานได้ทั่วโลก

เนื่องจากการพัฒนาระบบของ OpenVox เล็งเห็นถึงความสำคัญของการใช้งานที่ต่อเนื่องและให้เกิดอัตราการผิดพลาดในการทำงานที่น้อยที่สุด จึงเกิดเป็นอุปกรณ์ VoxStack 3G Gateway ซึ่งปัจจุบันได้รับความนิยมโดยเฉพาะองค์กรธุรกิจขนาดเล็กถึงขนาดกลาง เนื่องจากเป็นอุปกรณ์ที่สามารถติดตั้งใช้งานได้ง่าย และง่ายต่อการดูแลรักษา การปรับเปลี่ยนค่าการใช้งานในอนาคต เนื่องจากรองรับการตั้งค่าผ่านหน้าเว็บอินเตอร์เฟซ สามารถปรับแต่งฟังก์ชั่นใช้งานได้ตามความต้องการได้ตลอดเวลา โดยคุณสมบัติหลักของอุปกรณ์รองรับการบีบอัดเสียงตามมาตรฐานโปรโตคอล G.711A, G.711U, G.729, G.722, G.726 อีกทั้งยังรองรับการทำ Hot-swap ทั้งในตัวซิมการ์ดและโมดูล รวมไปถึงรองรับการรับส่งข้อความ SMS (SMS Message) รองรับการส่งในรูปแบบกลุ่มและส่งข้อความไปยังอีเมล อีกทั้งยังรองรับการทำงานร่วมกับ Asterisk, Elastix, Trixbox และ 3cx ได้ 100%

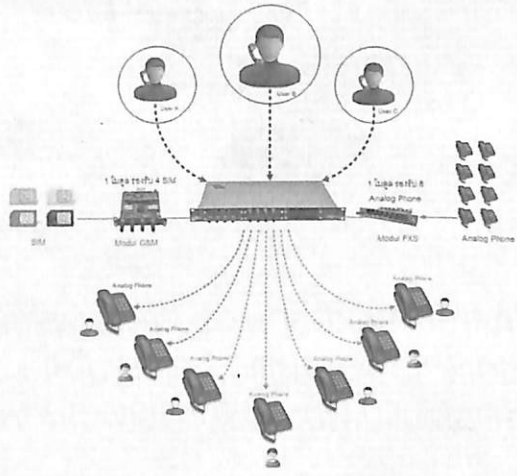


รูปแบบการเชื่อมต่อใช้งานอุปกรณ์ VoxStack 3G Gateway เชื่อมต่อกับตู้สาขาแบบ IP PBX

การใช้งานร่วมกับระบบโทรศัพท์แบบอะนาล็อกเป็นช่องทางหนึ่งให้ผู้ใช้ระบบโทรศัพท์แบบอะนาล็อกมีตัวเลือกในการใช้งานอุปกรณ์ VoxStack 3G Gateway ในขณะที่ยังไม่พร้อมจะเปลี่ยนแปลงระบบโทรศัพท์ทั้งหมดเป็นแบบ IP ซึ่งการนำเอาระบบโทรศัพท์แบบเดิมหรือระบบโทรศัพท์แบบอะนาล็อกมาทำงานควบคู่กับอุปกรณ์ GSM Gateway ทำให้เกิดประโยชน์ด้านการใช้จ่าย โดยช่วยลดค่าใช้จ่ายในแง่การใช้งานในแต่ละครั้งได้ เนื่องจากอุปกรณ์ GSM Gateway ภายใต้แบรนด์ OpenVox ตัวนี้สามารถกำหนดจากการใช้งานเพื่อสร้างเส้นทางโทรเข้าและโทรออกได้หลากหลาย ควบคุมการทำงานโดยที่ผู้ใช้งานสามารถเรียนรู้ระบบได้เร็ว จึงเกิดความสะดวกสบายในการใช้งาน เปิดช่องทางการเจรจาทางธุรกิจให้ทันต่อสถานการณ์มากยิ่งขึ้น

การทำงานของ VoxStack 3G Gateway ภายใต้แบรนด์ OpenVox ใน 1 ตัวจะประกอบไปด้วย 5 Plug-in สำหรับการเลือกโมดูลเข้าไป โดย 1 ตัวจะประกอบไปด้วยโมดูล FXS เพื่อรองรับการใช้งานโทรศัพท์แบบอะนาล็อก 1 โมดูล FXS จะรองรับโทรศัพท์แบบอะนาล็อกได้ 8 เครื่อง กับโมดูล GSM โดยที่ 1 โมดูล GSM จะรองรับการใช้งานซิมการ์ดได้ 4 ซิม จากการออกแบบดังกล่าวทำให้ผู้ใช้งานสามารถเลือกใช้งานให้เหมาะสมสำหรับความต้องการของผู้ใช้งานเองอย่างลงตัว ข้อดีที่เป็นจุดเด่นของอุปกรณ์ VoxStack 3G Gateway ที่สำคัญก็คือผู้ใช้งานสามารถกำหนดการใช้งานของแต่ละซิมการ์ดได้ นั่นคือสามารถกำหนดได้ว่า SIM A ใช้เฉพาะ User A เท่านั้น หรือ SIM A ใช้ทั้ง User A,B,C,.....n ก็สามารถทำได้

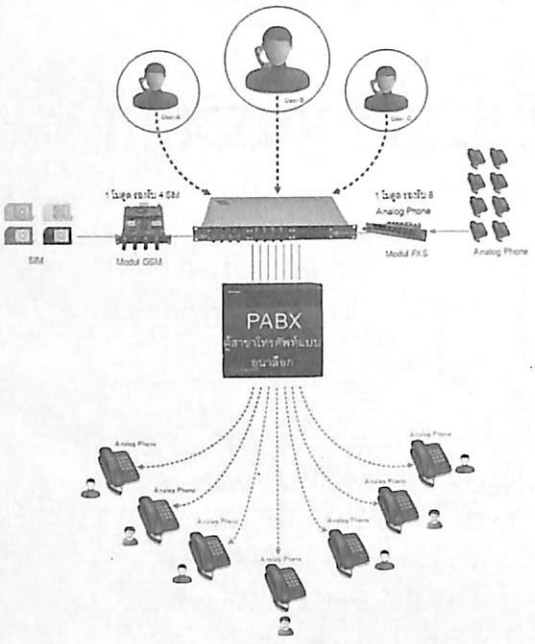
ด้วยลักษณะในการทำงานทางด้านการสื่อสารขององค์กรที่หลากหลาย การพัฒนาตัวอุปกรณ์ VoxStack 3G Gateway ให้ครอบคลุมการใช้งานในทุกรูปแบบจึงมีความจำเป็น เนื่องจากปัจจุบันมีผู้ใช้จำนวนไม่น้อยที่ต้องการพัฒนาระบบโทรศัพท์ภายในองค์กร แต่ต้องการคงระบบโทรศัพท์แบบเดิมเอาไว้ ความต้องการการใช้งานอุปกรณ์ VoxStack 3G Gateway ที่รองรับการทำงานกับระบบโทรศัพท์แบบอะนาล็อกจึงมีแนวโน้มเพิ่มมากขึ้น เนื่องจากปัจจุบันเป็นช่วงที่หลายองค์กรเข้าสู่ช่วงพัฒนาเปลี่ยนผ่านระบบโทรศัพท์ จึงทำให้เกิดความต้องการใช้งานร่วมกันระหว่างอุปกรณ์อะนาล็อกกับอุปกรณ์ VoxStack 3G Gateway แต่เนื่องจาก VoxStack 3G Gateway ภายใต้แบรนด์ OpenVox ผู้พัฒนาไม่ได้คิดแค่รองรับการทำงานร่วมกับระบบโทรศัพท์แบบอะนาล็อกเพียงอย่างเดียว แต่ยังรองรับการทำงานร่วมกับระบบโทรศัพท์แบบ IP ดังรายละเอียดที่กล่าวมาแล้วข้างต้นเพื่อรองรับการพัฒนาในอนาคตและตอบโจทย์ทุกความต้องการของลูกค้าด้วยอุปกรณ์ VoxStack 3G Gateway ภายใต้แบรนด์ OpenVox



รูปแบบการเชื่อมต่อใช้งานอุปกรณ์ VoxStack 3G Gateway กับหัวเครื่องโทรศัพท์แบบอะนาล็อก

การทำงานร่วมกับระบบโทรศัพท์แบบอะนาล็อก

การทำงานร่วมกับตู้สาขาแบบอะนาล็อกเป็นอีกโซลูชั่นหนึ่งที่ได้รับความนิยม เนื่องจากการนำเอา VoxStack 3G Gateway มาใช้งานร่วมกับตู้สาขาแบบอะนาล็อกจะเพิ่มช่องทางการสื่อสารให้กับผู้ใช้ให้มีช่องทางการสื่อสารที่เหมาะสมมากยิ่งขึ้นกับการใช้งานจริงในปัจจุบัน จากเดิมที่ต้องเสียค่าใช้จ่ายกับการโทรออกสายนอกที่เป็นหมายเลขมือถือโดยใช้หมายเลขพื้นที่ (02 เป็นต้น) ในการโทรออกที่มีค่าใช้จ่ายในส่วนนี้ค่อนข้างสูง เมื่อนำเอาอุปกรณ์ VoxStack 3G Gateway มาใช้งานร่วมก็จะช่วยลดค่าใช้จ่ายในส่วนนี้ได้อย่างมีประสิทธิผลควบคู่กับการใช้งานที่มีประสิทธิภาพ



รูปแบบการเชื่อมต่อใช้งานอุปกรณ์ VoxStack 3G Gateway กับระบบโทรศัพท์แบบอะนาล็อก (PABX)

ข้อดีของการใช้ GSM Gateway ร่วมกับระบบ VoIP

- ลดค่าใช้จ่ายในด้านต่างๆ ไม่ว่าจะเป็นค่าใช้จ่ายทางด้านค่าบริการโทรศัพท์ทางไกล รวมถึงสามารถลดค่าใช้จ่ายด้านบุคลากรที่จะมาดูแลในเรื่องของการให้บริการทางโทรศัพท์ได้อีกด้วย เพราะพนักงานเพียงคนเดียวสามารถให้บริการลูกค้าผ่านระบบโทรศัพท์กลางขององค์กร และเชื่อมต่อไปยังสาขาต่างๆ ด้วยเทคโนโลยี VoIP
- เพื่อเป็นการติดต่อสื่อสารระหว่างสาขาที่อยู่ในระยะทางไกล จะทำให้องค์กรได้ประโยชน์ในแง่ของข้อมูลข่าวสารต่างๆ ระหว่างองค์กรมากยิ่งขึ้น เนื่องจากมีการสื่อสารแลกเปลี่ยนข่าวสารกันระหว่างสาขาขององค์กรมากยิ่งขึ้น โดยที่ไม่ต้องกังวลในเรื่องของค่าใช้จ่ายของการสื่อสารทางไกล ทำให้แต่ละสาขาได้รับข่าวสารข้อมูลล่าสุดขององค์กรอย่างทันท่วงที
- ลดค่าใช้จ่ายในการดูแลระบบ เนื่องจาก GSM Gateway เป็นอุปกรณ์ที่สามารถเฝ้าดูหรือควบคุมผ่านทางหน้าเว็บ มีความยืดหยุ่นสูง จึงสามารถช่วยลดค่าใช้จ่ายด้านการจัดการและการดูแลรักษา

คุณสมบัติหลักของอุปกรณ์ (Main Features)

- ออกแบบมาเป็นรูปแบบของ Modular และ VoxStack
- พื้นฐานระบบแบบ Asterisk
- สามารถแก้ไข Asterisk ตั้งค่าไฟล์ได้
- สามารถเลือกตัวแปลงสัญญาณและโปรโตคอลการส่งสัญญาณได้ครอบคลุม
- รองรับการรับส่งข้อความ SMS การส่งข้อความแบบกลุ่ม
- รองรับส่งข้อความ SMS ไปยังอีเมล
- รองรับการส่งข้อความแบบอัตโนมัติ
- รองรับการบริการ USSD
- รองรับการเปลี่ยนแปลง IMEI
- รองรับการกำหนดรหัสผ่าน (PIN Identification)
- รองรับการกำหนดเส้นทางการใช้งานได้ไม่จำกัด (Unlimited Routing)
- รองรับการทำ Hot-swap ทั้ง SIM และ Modules
- มีประสิทธิภาพ มีความยืดหยุ่นในการใช้งาน การโทร การตั้งค่าผ่าน GUI

สนใจสินค้าติดต่อสอบถามข้อมูลเพิ่มเติมได้ที่

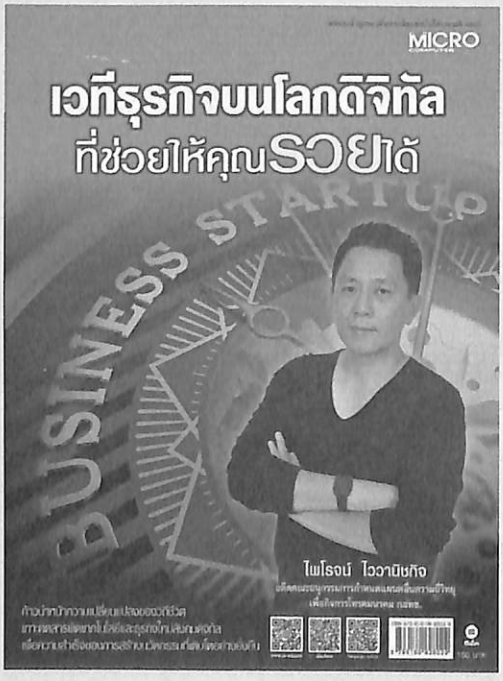
บริษัท พอยซ เทคโนโลยี จำกัด
76 สุขุมวิท ซ. 2 แขวงคลองเตย เขตคลองเตย กรุงเทพ 10110
โทรศัพท์ 0 2656 8598 โทรสาร 0 2250 9769
http://www.poisetechnology.com/

เวทีธุรกิจบนโลกดิจิทัลที่ช่วยให้คุณรวยได้

ออกแบบชีวิตให้เท่าทันการไหลเข้ามารวมกันของโลกเสมือนกับโลกที่แท้จริง จึงต้องวิ่งตามความผันแปรของเทคโนโลยีเพื่อใช้ประโยชน์จากโลกดิจิทัลที่จะช่วยให้คุณรวยได้

เทคโนโลยีสื่อสารโทรคมนาคม โลกของสมาร์ทโฟนและแอพพลิเคชั่น สังคมที่ไร้พรมแดนอย่าง Social Network และการต่อยอดทางธุรกิจอย่างไม่สิ้นสุดของเทคโนโลยี Data Analytics เสริมด้วยยุคทองของนวัตกรรม Internet of Things ก่อให้เกิดความเปลี่ยนแปลงต่อรูปแบบการใช้ชีวิตและการดำเนินธุรกิจ ทำให้วิถีการทำธุรกิจหลายประเภทต้องปิดตัวลงชั่วข้ามคืน เกิดธุรกิจรูปแบบใหม่ขึ้นอย่างไม่เคยปรากฏมาก่อน การแข่งขันอย่างรุนแรงของการสร้างแอพพลิเคชั่น นวัตกรรมผลิตภัณฑ์ สินค้าและโซลูชั่นทางฮาร์ดแวร์กลายเป็นประตูที่เปิดกว้างขึ้นของผู้ประกอบการรายใหม่ที่สามารถกำหนดจุดขายของสินค้าและบริการของตน

หนังสือ **"เวทีธุรกิจบนโลกดิจิทัลที่ช่วยให้คุณรวยได้"** เล่มนี้จึงขอทำหน้าที่เป็นกระจกสะท้อนครรลองของการเริ่มต้นจากศูนย์เพื่อสร้างสินค้าด้านฮาร์ดแวร์ที่สามารถขยายขนาดการเติบโตทางธุรกิจตนเองได้ เพื่อยกระดับฐานะของการทำธุรกิจจาก Startups ไปเป็นกิจการขนาดใหญ่ พร้อมกับฉายภาพของผลิตภัณฑ์สินค้าในอุตสาหกรรมต่างๆ ที่มีในปัจจุบันเพื่อให้เกิดทั้งแรงบันดาลใจและความเข้าใจต่อการเติบโตของตลาด อีกทั้งยังสามารถนำไปศึกษาและต่อยอดความรู้ในขั้นสูงต่อไป



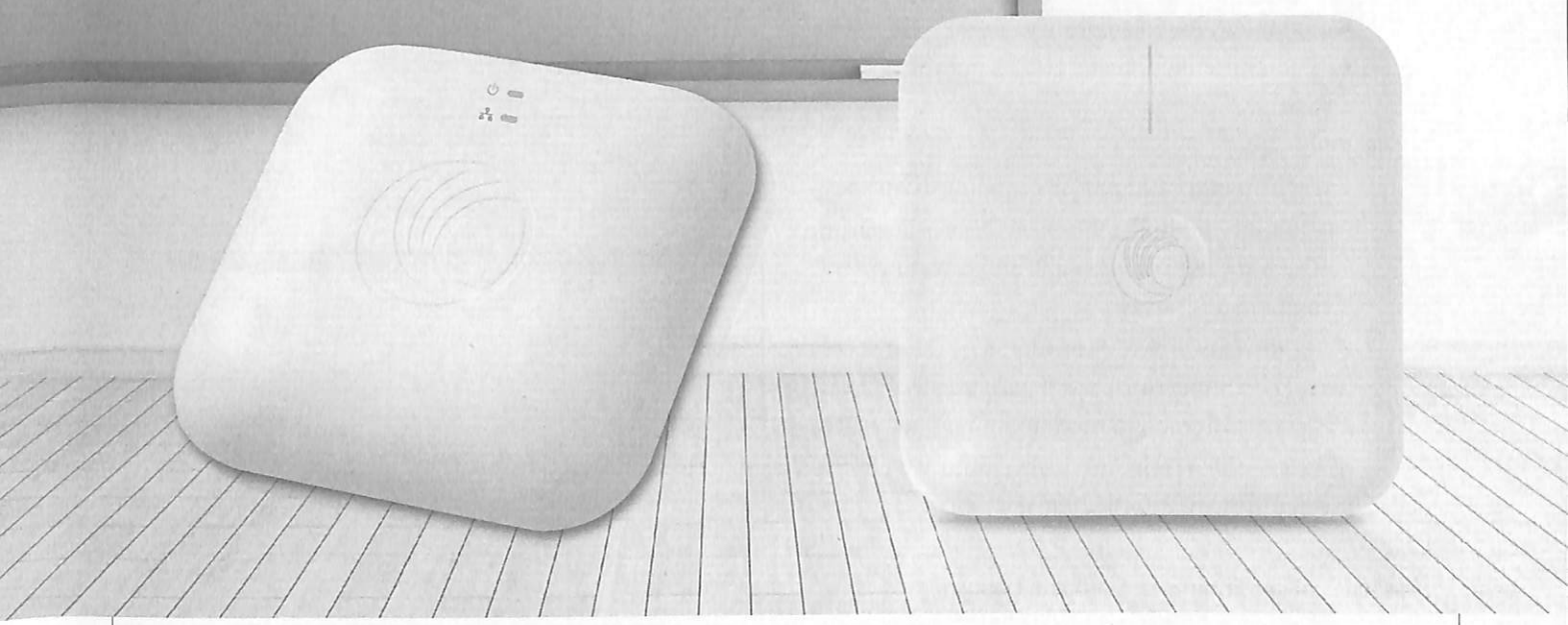
ผู้เขียน : ไพโรจน์ ไววานิชกิจ
รหัสสินค้า : 978-616-08-2802-9
ราคาปกติ : 150 บาท

■ King Intelligent Technology Co., Ltd.

King I.T. Network

รับประกัน 3 ปี

cnPilot Wi-Fi AP ในอาคาร ประสิทธิภาพสูงด้วยมาตรฐาน 802.11ac Wave 2



cnPilot Enterprise E400 โซลูชั่นที่มีประสิทธิภาพสูง มุ่งเน้นสำหรับธุรกิจขนาดเล็กและขนาดกลาง

cnPilot Enterprise E400 802.11ac Dual Access Point Wi-Fi สำหรับใช้งานภายในอาคาร พร้อมหัวต่อสาย PoE และ CAT5 Ethernet Cable, RoW เป็นแอกเซสพอยต์ภายในอาคารที่เหมาะสำหรับการขยายสัญญาณในกลุ่ม Enterprise โดย cnPilot E400 ได้รับการออกแบบมาสำหรับผู้ให้บริการอุปกรณ์ไร้สายของทั้งองค์กรและเครือข่ายองค์กรแบบกระจาย (Distributed Enterprise Networks) มี WLAN ที่สามารถปรับขนาดได้ มีความปลอดภัยและสร้างความน่าเชื่อถือได้ เป็นแอกเซสพอยต์มาตรฐาน 802.11ac ระดับองค์กร สนับสนุนการจัดการภายในองค์กรได้เป็นอย่างดีหรือการเชื่อมต่อกับระบบคลาวด์ได้อย่างรวดเร็ว และการติดตั้งที่แสนง่าย

คุณลักษณะ AP Wi-Fi ในอาคาร cnPilot

1. **มาตรฐาน 802.11ac**
2. **cnMaestro Management การแก้ไขปัญหาแบบ End-to-End** : ระบบมีแดชบอร์ด (Dashboard) เพียงหน้าเดียวที่แสดงสถิติที่สมบูรณ์ ช่วยให้มั่นใจได้ว่าการตรวจหาปัญหาและการแก้ไขปัญหาเป็นไปอย่างรวดเร็ว
   - ฟังก์ชั่นการทำงานที่เพียงเชื่อมต่ออุปกรณ์กับอินเทอร์เน็ต อุปกรณ์ก็จะแสดงเครือข่ายทั้งหมดที่เกี่ยวข้อง และสามารถระบุพื้นที่ที่มีปัญหาของสัญญาณได้ชัดเจน โดยเป็นฟังก์ชั่นที่ติดมากับอุปกรณ์ ทำให้การแก้ไขเรื่องสัญญาณรวดเร็วขึ้น

- แก้ไขการเชื่อมต่อไคลเอนต์ของผู้ใช้ปลายทางบน WLAN ใดๆ จากหน้าคอนโซลเดียวได้เลย
- การแก้ปัญหา การกำหนดค่าการเชื่อมต่อแบบมีสายหรือแบบไร้สายสามารถทำได้จุดเดียว

3. ความเรียบง่ายที่มีประสิทธิภาพ License-Free High Performance : โซลูชั่น cnPilot 802.11ac มาพร้อมกับตัวควบคุม (Controller) ฟรี ผ่าน Cloud Manage โดยไม่มีค่าใช้จ่ายและค่าธรรมเนียมในการจัดการ AP สำหรับลูกค้าได้ถึง 1,000 ราย

4. การเชื่อมต่อเครือข่ายอื่นๆ

- สามารถเชื่อมต่อกับโซลูชั่น Guest Access จากยี่ห้ออื่นๆ ได้
- พอร์ทัล (Portal) การเข้าถึงสำหรับการใช้งานแบบ Guest On-board ใช้งานง่าย

5. ความปลอดภัย

- สนับสนุน WPA2 Enterprise และ WPA2 PSK
- เชื่อมต่ออย่างปลอดภัยผ่าน HTTPS กลับไปเพื่อจัดการยังระบบคลาวด์

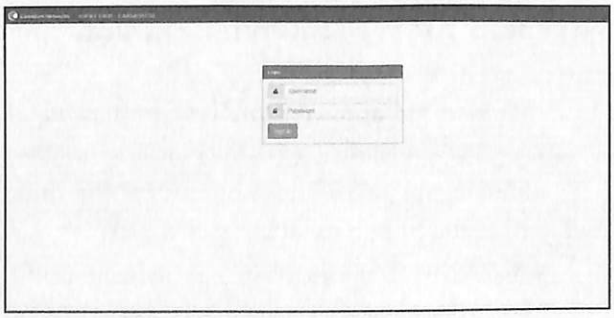
6. SSID

- รองรับ 16 SSID สนับสนุนผู้ใช้พร้อมกัน 256 คน รองรับการสแกนช่องอัตโนมัติ (Automatic Channel Scanning : ACS) และคุณสมบัติขั้นสูงเน้นความเที่ยงตรงในการรับส่งข้อมูล Band Steering

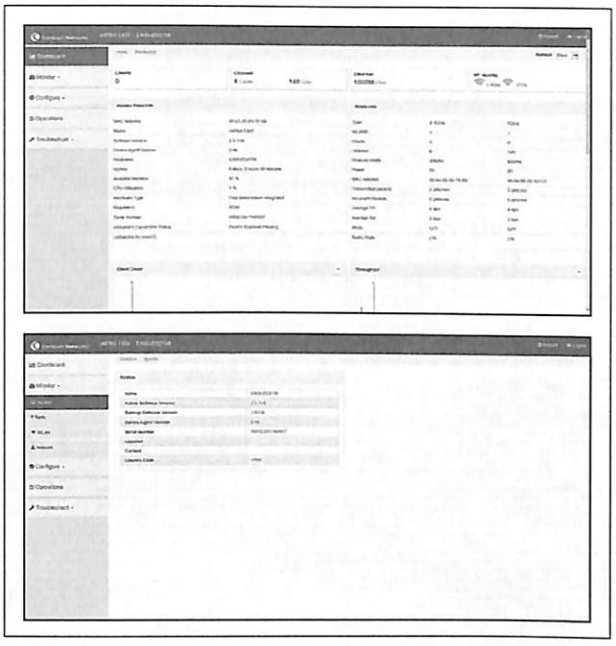
7. สร้างรายได้จากบริการ Wi-Fi ของคุณ : สร้าง Guest Access ได้รวดเร็ว กำหนดการเข้าถึง จำกัดเวลาและอัตราความเร็ว ตัวเลือกการเข้าใช้งาน เช่น การเข้าสู่ระบบโซเชี่ยลและคูปอง พร้อมกับการซื้อ จึงเหมาะอย่างยิ่งที่จะใช้เป็น WiFi สำหรับผู้เข้าพักในโรงแรม ร้านกาแฟ และสำนักงาน

การติดตั้ง cnPilot Enterprise E400 ผ่านตัวอุปกรณ์

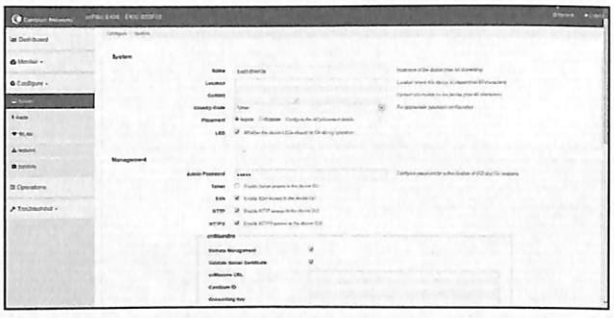
1. เริ่มต้นด้วยการเข้าไปตั้งค่าผ่านทางไอพีที่ได้รับมาจาก DHCP ซึ่งแอกเซสพอยต์ตัวนี้จะไม่มี IP Address Default ให้ใช้ Username : admin Password : admin (รูปที่ 1)
2. หน้าจอแสดงสถานะการทำงานของแอกเซสพอยต์ (รูปที่ 2)
3. หน้าจอสำหรับการคอนฟิกระบบ ซึ่งสามารถตั้งชื่อ รหัสผ่าน และอื่นๆ (รูปที่ 3)



รูปที่ 1



รูปที่ 2

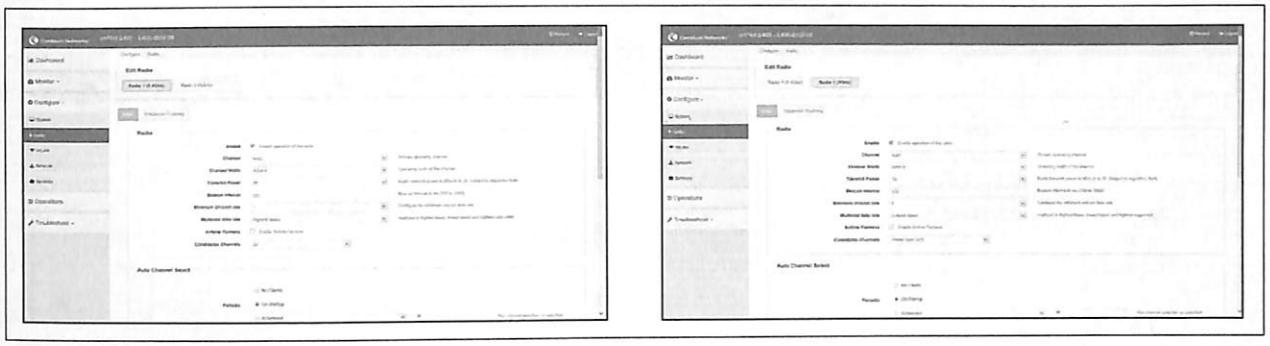


รูปที่ 3

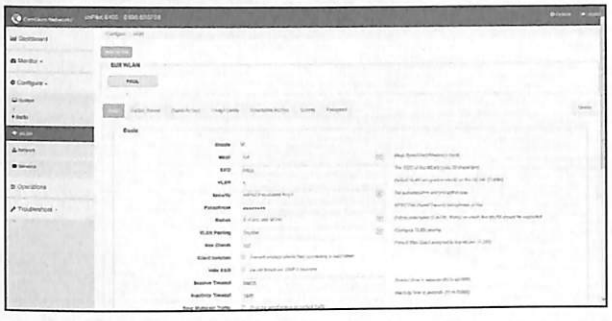
4. หน้าจอสำหรับการคอนฟิกสัญญาณ Radio ซึ่งจะมี Radio 1 ความถี่ 2.4 GHz และ Radio 2 ความถี่ 5 GHz (รูปที่ 4)
5. หน้าจอสำหรับการคอนฟิก WLAN สามารถตั้งชื่อ SSIDs และรหัสผ่าน รวมถึงการตั้งค่า Guess Access, การจำกัดความเร็ว และอื่นๆ ซึ่งเราสามารถตั้งได้ถึง 16 SSIDs (รูปที่ 5)
6. หน้าจอสำหรับการคอนฟิก VLAN และเซอร์วิสต่างๆ ก็มีให้สามารถคอนฟิกได้เช่นเดียวกับแอกเซสพอยต์ตัวอื่นๆ (รูปที่ 6)
7. ในตัวแอกเซสพอยต์ยังมีบริการในการวิเคราะห์ WiFi, Capture Packet ได้อีกด้วย (รูปที่ 7)

การติดตั้ง cnPilot Enterprise E400 ผ่านคลาวด์ให้ใช้งานฟรี

เราสามารถใช้บริการผ่านคลาวด์ได้โดยการสมัครสมาชิกผ่านเว็บไซต์ https://cloud.cambiumnetworks.com ซึ่งสะดวกอย่างยิ่ง ไม่จำเป็นต้องติดตั้งบนเซิร์ฟเวอร์ขององค์กรแต่อย่างใด (รูปที่ 8 และ 9)



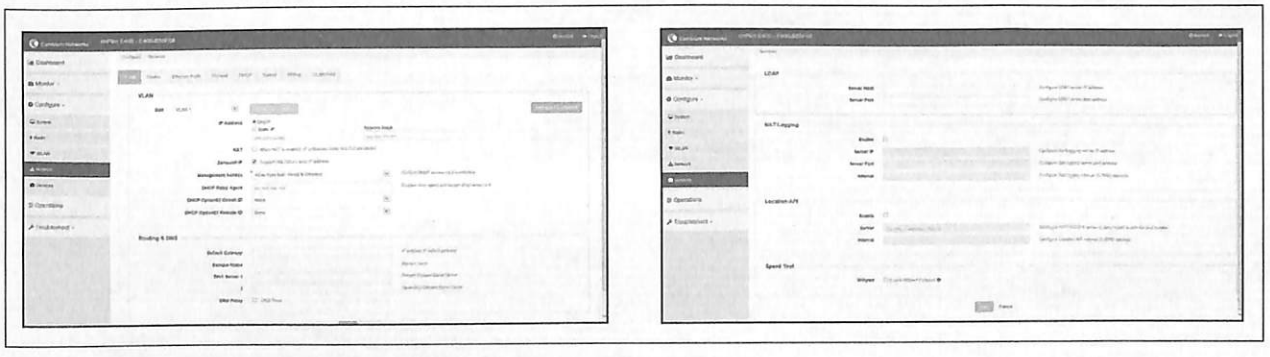
รูปที่ 4



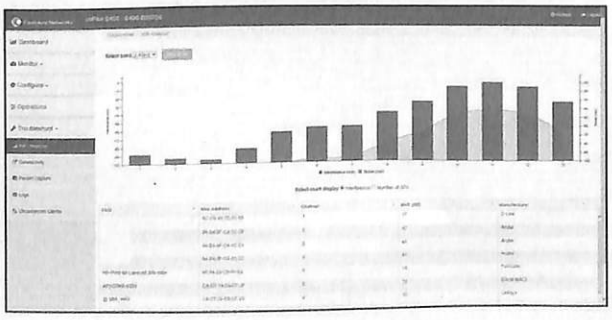
รูปที่ 5

การทดสอบ

1. เริ่มต้นการทดสอบด้วยการดาวน์โหลด โดยทดสอบการโยนไฟล์ไปยัง NAS Server การก๊อบปี้ทำงานค่อนข้างเร็วและเสถียร
2. ลอง Ping ไปยังแอกเซสพอยต์ ถือว่าความเสถียรอยู่ในระดับดี (รูปที่ 10)
3. ทดสอบกับเว็บเพื่อทดสอบการอัปโหลดและดาวน์โหลดบนเครื่องโน้ตบุ๊ก โดยการทดสอบกับอินเทอร์เน็ตความเร็ว 100/100 Mbps โดยมีไฟร์วอลล์กั้นอยู่ ซึ่งอาจไม่ได้ความเร็วที่สูงสุด แต่กับความเร็วระดับนี้ถือว่าผ่านสามารถใช้ภายในองค์กร หรือ SME ได้อย่างสบายๆ (รูปที่ 11)

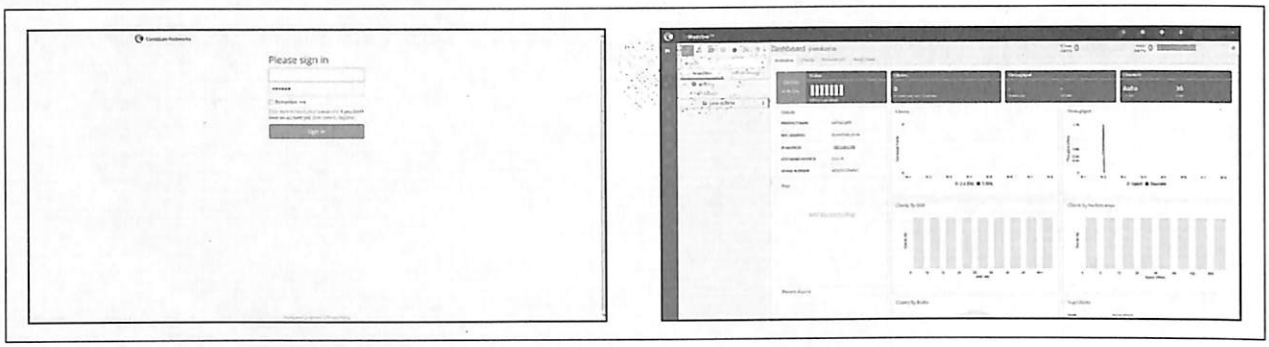


รูปที่ 6

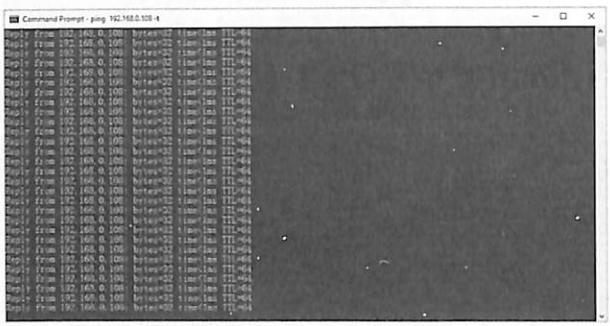


รูปที่ 7

รูปที่ 8 หน้าจอ Dashboard และหน้าจอสำหรับเพิ่มอุปกรณ์แอกเซสพอยต์เข้าไป

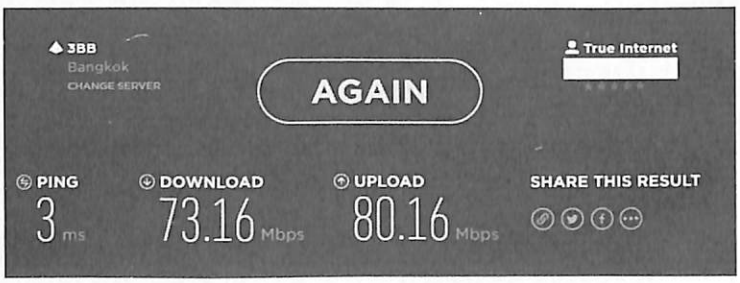


รูปที่ 9



รูปที่ 10

รูปที่ 12



รูปที่ 11

- สเปกของเครื่องโน้ตบุ๊กที่ใช้ทดสอบเป็น HP 348 G3 เป็น Wireless LanRealtek 802.11b/g/n (1x1) ซึ่งสามารถรองรับการใช้งานบนความถี่ 5 Ghz

4. การทดสอบการใช้งานผ่านอุปกรณ์ cnPilot E400 (รูปที่ 12)

บทสรุป

จากการทดสอบจะเห็นได้ว่าทางด้านความเสถียรถือว่าใช้งานได้ดี สามารถใช้ได้โดยไม่หลุดหรือติดขัดปัญหาแต่อย่างใด cnPilot Enterprise E400 ตอบโจทย์การใช้งานที่มีประสิทธิภาพสูง มุ่งเน้นสำหรับธุรกิจขนาดเล็กและขนาดกลาง ใช้งานง่าย ติดตั้งง่าย บริหารจัดการได้ง่าย ที่สำคัญในราคาที่เป็นเจ้าของได้ง่าย

อีกทั้ง King i.t. ยังมีบริการ HOTLINE 24 ชั่วโมง และศูนย์บริการลูกค้าถึง 31 ศูนย์บริการทั่วประเทศ บริการทั่วถึงอย่างนี้ คิดจะเลือกอุปกรณ์เน็ตเวิร์กเมื่อไร อย่าลืมเลือกอุปกรณ์ของ King i.t. นะครับ เพราะบริการเขาดีจริงๆ

ดร.วิรินทร์ เมฆประดิษฐสิน

WannaCrypt : มหันตภัยในโลกไซเบอร์

โลกไซเบอร์ได้เรียนรู้ภัยอันตรายจาก Ransomware ตัวใหม่ ที่แพร่กระจายดุจโรคระบาดไปยังคอมพิวเตอร์ที่มีช่องโหว่ทั่วโลก ชื่อของมันคือ WannaCrypt แต่ถึงจะร้ายแค่ไหนก็จัดการได้ไม่ยาก

วันที่ 12 พฤษภาคม ค.ศ. 2017 โลกของไซเบอร์ได้เรียนรู้ภัยอันตรายจาก Ransomware ตัวใหม่ที่แพร่กระจายดุจโรคระบาดไปทั่วโลกไปยังเครื่องคอมพิวเตอร์ต่างๆ ที่มีช่องโหว่ แต่ยังไม่ได้รับการปรับปรุงหรืออัปเดตระบบปฏิบัติการ ขณะที่มีเครื่องคอมพิวเตอร์อยู่มากมายที่ได้รับการอัปเดตระบบเพื่อลดปัญหาช่องโหว่เป็นที่เรียบร้อยแล้ว ในขณะเดียวกันก็ยังมีคอมพิวเตอร์ส่วนใหญ่ภายในองค์กรบางแห่งอาจชะลอการติดตั้งแพตช์ (Patch) แต่น่าเสียดายที่ Ransomware หรือที่เรียกว่า WannaCrypt ดูเหมือนจะส่งผลกระทบต่อเครื่องคอมพิวเตอร์ที่ไม่ได้ใช้แพตช์สำหรับอุดช่องโหว่เหล่านี้ ขณะการโจมตีกำลังเกิดขึ้นเว็บไซต์หลายแห่ง รวมทั้งไมโครซอฟท์ได้เตือนให้ผู้ใช้ติดตั้ง MS17-010 หากยังไม่ได้ดำเนินการ

ทิศทางการโจมตีของ WannaCrypt

ภยันตรายจากการแพร่ขยายของ Ransomware ไม่ได้เกิดขึ้นอย่างรวดเร็ว ภยันตราย ตัวอย่างเช่น WannaCrypt (หรือที่เรียกว่า WannaCry, WanaCrypt0r, WCrypt หรือ WCRY) ปกติจะใช้วิธีการทางวิศวกรรมสังคม (Social Engineering) หรืออีเมลเป็นสื่อหรือวิธีการในการโจมตีหลัก ขึ้นอยู่กับการดาวน์โหลดของผู้ใช้งาน รวมทั้งเรียกใช้งานโปรแกรมหรือข้อมูลที่มี Malicious Code แฝงตัวอยู่ อย่างไรก็ตามในกรณีพิเศษนี้ผู้โจมตีด้วย Ransomware จะใช้ Exploit Code ซึ่งมีอยู่แล้วทั่วไปเพื่อเจาะช่องโหว่ของ SMB “EternalBlue” CVE-2017-0145 (เซิร์ฟเวอร์ SMBv1 ใน Microsoft Windows Vista SP2, Windows Server 2008 SP2 และ R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold และ R2, Windows RT 8.1 และ Windows 10 Gold, 1511 และ 1607 และ Windows Server 2016 ช่วยให้ผู้โจมตีจากระยะไกลสามารถรันโค้ดจากแพ็กเกจที่สร้างขึ้นมาได้โดยใช้แพ็กเกจที่สร้างขึ้น ซึ่งมีชื่อว่า “Windows Labs Remote SMTP Execution Vulnerability” ช่องโหว่นี้แตกต่างจากช่องโหว่ที่อธิบายไว้ใน CVE-2017-0143, CVE-2017-0144, CVE-2017-0146 และ CVE-2017-0148) ซึ่งสามารถถูกกระตุ้นเตือนโดยการจัดส่งแพ็กเก็ตที่ผ่านการปรับแต่งโดยมีเป้าหมายอยู่ที่ SMBv1 Server ช่องโหว่นี้ได้รับการแก้ไขโดย Security Bulletin MS17-010 ซึ่งเผยแพร่ในวันที่ 14 พฤษภาคม ค.ศ. 2017

กลไกการแพร่กระจายของ WannaCrypt ถูกยืมมาจากการทำ Exploit SMB ที่รู้จักกันดี ซึ่งติดอาวุธให้กับ Ransomware ปกติ โดยมีฟังก์ชั่นการทำงานคล้ายหนอน ทำให้เกิดการชี้นำให้คอมพิวเตอร์เพื่อค้นหาเครื่องคอมพิวเตอร์อื่นๆ ที่ไม่ได้ติดตั้งหรืออัปเดตแพตช์ หรือแม้แต่อัปเดตหลังปนเปื้อนแล้วก็ตาม

รหัสที่ใช้สำหรับ Exploit โดย WannaCrypt ถูกออกแบบมาเพื่อใช้งานเฉพาะกับ Windows 7 และ Windows Server 2008 (หรือระบบปฏิบัติการก่อนหน้า) ที่ยังไม่ได้รับการติดตั้ง ดังนั้นคอมพิวเตอร์ Windows 10 จะไม่ได้รับผลกระทบจากการโจมตีนี้ (หากมีการป้องกันล่วงหน้าก่อนหน้านี้)

ผู้เชี่ยวชาญไม่พบหลักฐานของการจัดทำกระบวนการชี้ทาง (Vector) ที่ใช้โดยภัยคุกคามนี้ แต่มี 2 สถานการณ์ที่ผู้เชี่ยวชาญเชื่อว่าเป็นคำอธิบายที่เป็นไปได้สูงสำหรับการแพร่กระจายของ Ransomware ตัวนี้

- การใช้อีเมลเพื่อดำเนินการทางวิศวกรรมสังคมที่ออกแบบมาเพื่อหลอกลวงผู้ใช้งานให้เรียกใช้มัลแวร์ (Malware) โดยไม่ตั้งใจ และเปิดใช้งานฟังก์ชั่นการแพร่กระจายหนอนไวรัสด้วยการใช้ประโยชน์จาก SMB
- การติดเชื้อผ่านการ Exploit SMB เมื่อคอมพิวเตอร์ที่ไม่ได้รับการติดตั้งแพตช์ และได้รับการติดต่อสื่อสารกับคอมพิวเตอร์เครื่องอื่นๆ

Dropper

ภัยคุกคามมาในรูปแบบ Trojan Dropper ที่ประกอบด้วยองค์ประกอบ 2 อย่างดังนี้

1. ส่วนประกอบที่พยายามใช้ช่องโหว่หรือบั๊ก (Bug) ของ SMB CVE-2017-0145 ในทางที่ไม่เหมาะสมกับเครื่องคอมพิวเตอร์เครื่องอื่นๆ
2. Ransomware ที่เรียกว่า WannaCrypt Dropper พยายามเชื่อมต่อโดเมนต่อไปนี้โดยใช้ API InternetOpenUrlA ():
   - www [.] iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea [. com]
   - www [.] ifferfsodp9ifjaposdfjhgosurijfaewrwergwea [. com]

หากการเชื่อมต่อกับโดเมนสำเร็จ ตัว Dropper จะไม่ส่งผลต่อระบบที่ปนเปื้อนอีกต่อไปด้วย Ransomware หรือพยายามที่จะใช้ประโยชน์จากระบบ เช่น คอมพิวเตอร์อื่นๆ เพื่อแพร่กระจาย มันจะหยุดดำเนินการ อย่างไรก็ตามหากการเชื่อมต่อล้มเหลว ภัยคุกคามจะดำเนินการ Drop Ransomware และสร้างเซอร์วิสใหม่ขึ้นมาในระบบ กล่าวอีกนัยหนึ่งคือแตกต่างจากการติดมัลแวร์ส่วนใหญ่ ผู้ดูแลระบบไอทีไม่ควรบล็อกโดเมนเหล่านี้ โปรดทราบว่ามัลแวร์ไม่ได้เป็นระบบ Proxy-Aware (ไม่สนใจความมีอยู่ของ Proxy) ดังนั้นอาจจำเป็นต้องมีระเบียน DNS (DNS Record) ในระบบ ซึ่งไม่จำเป็นต้องชี้ไปยังอินเทอร์เน็ต แต่สามารถ Resolve คำร้องขอทราบข้อมูล DNS สำหรับเซิร์ฟเวอร์ใดๆ ที่สามารถเข้าถึงได้ ซึ่งติดต่อเข้ามาภายใต้พอร์ต 80 (รูปที่ 1)

รูปที่ 1 แสดง Dropper

รูปที่ 2 แสดงชื่อเซอร์วิสที่สร้างขึ้น

ภยันตรายที่เกิดจากมัลแวร์ตัวนี้อีกอย่างคือการสร้างเซอร์วิสตัวหนึ่งชื่อว่า mssecsvc2.0 โดยมีหน้าที่การทำงานคือเจาะเข้าไปในช่องโหว่ของ SMB ในคอมพิวเตอร์เครื่องอื่นๆ ที่ได้เชื่อมต่อหรือสามารถเข้าถึงคอมพิวเตอร์เครื่องที่ปนเปื้อนนี้ได้ (รูปที่ 2)

- Service Name: mssecsvc2.0
- Service Description: (Microsoft Security Center (2.0) Service)
- Service Parameters: "-m security"
- Service Parameters: "-m security"

WannaCrypt Ransomware

Ransomware คือ Dropper (Dropper เป็นโปรแกรมหรือส่วนประกอบของมัลแวร์) ที่ประกอบด้วยไฟล์ .zip ที่มีการป้องกันด้วยรหัสผ่านในส่วนของทรัพยากร โดยมีรูทีน (Routine) การเข้ารหัสเอกสารและไฟล์ ในไฟล์ .zip ยังประกอบด้วยเครื่องมือสนับสนุนและเครื่องมือถอดรหัส รวมทั้งข้อความค่าไถ่ ในตัวอย่างที่วิเคราะห์รหัสผ่านสำหรับไฟล์ .zip นั่นคือ "WNcry @ 2ol7" เมื่อมีการรัน WannaCrypt แล้ว จะมีการสร้าง Registry Key ดังต่อไปนี้

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\\<random string> = "<malware working directory>\tasksche.exe"
- HKLM\SOFTWARE\WanaCrypt0r\\wd = "<malware working directory>"

มีการเปลี่ยนวอลล์เปเปอร์ (Wallpaper) ไปเป็นข่าวสารแสดงการเรียกค่าไถ่โดยการปรับแก้ Registry Key ดังต่อไปนี้

- HKCU\Control Panel\Desktop\Wallpaper: "<malware working directory>\@WanaDecryptor@.bmp"

นอกจากนี้ยังมีการจัดสร้างไฟล์ต่อไปนี้ในไดเรกทอรี (Directory) ของมัลแวร์

- 00000000.eky
- 00000000.pky
- 00000000.res
- 274901494632976.bat
- @Please_Read_Me@.txt
- @WanaDecryptor@.bmp
- @WanaDecryptor@.exe
- b.wnry
- c.wnry
- f.wnry
- m.vbs
- msg\m_bulgarian.wnry
- msg\m_chinese (simplified).wnry
- msg\m_chinese (traditional).wnry
- msg\m_croatian.wnry
- msg\m_czech.wnry
- msg\m_danish.wnry
- msg\m_dutch.wnry
- msg\m_english.wnry
- msg\m_filipino.wnry
- msg\m_finnish.wnry
- msg\m_french.wnry
- msg\m_german.wnry
- msg\m_greek.wnry
- msg\m_indonesian.wnry
- msg\m_italian.wnry
- msg\m_japanese.wnry
- msg\m_korean.wnry
- msg\m_latvian.wnry
- msg\m_norwegian.wnry
- msg\m_polish.wnry
- msg\m_portuguese.wnry
- msg\m_romanian.wnry
- msg\m_russian.wnry
- msg\m_slovak.wnry
- msg\m_spanish.wnry
- msg\m_swedish.wnry
- msg\m_turkish.wnry
- msg\m_vietnamese.wnry
- r.wnry
- s.wnry
- t.wnry
- TaskData\Tor\libeay32.dll
- TaskData\Tor\libevent-2-0-5.dll
- TaskData\Tor\libevent_core-2-0-5.dll
- TaskData\Tor\libevent_extra-2-0-5.dll
- TaskData\Tor\libgcc_s_sjlj-1.dll
- TaskData\Tor\libssp-0.dll
- TaskData\Tor\ssleay32.dll
- TaskData\Tor\taskhsvc.exe
- TaskData\Tor\tor.exe
- TaskData\Tor\zlib1.dll
- taskdl.exe
- taskse.exe
- u.wnry

WannaCrypt อาจสร้างไฟล์ต่างๆ ต่อไปนี้

- %SystemRoot%\tasksche.exe
- %SystemDrive%\intel\<random directory name>\tasksche.exe
- %ProgramData%\<random directory name>\tasksche.exe

แล้วยังอาจสร้าง Named Service แบบสุ่มที่มีข้อมูลเกี่ยวข้องกับ ImagePath ต่อไปนี้

"cmd.exe /c "<malware working directory>\tasksche.exe""

จากนั้นมีการค้นหาไฟล์ทั้งหมดในคอมพิวเตอร์ที่มีนามสกุล (Extension) ต่อไปนี้

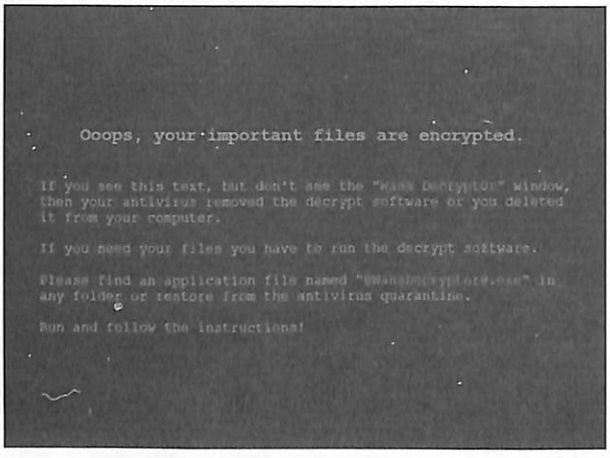
.123, .jpeg , .rb , .602 , .jpg , .rtf , .doc , .js , .sch , .3dm , .jsp , .sh , .3ds , .key , .sldm , .3g2 , .lay , .sldm , .3gp , .lay6 , .sldx , .7z , .ldf , .slk , .accdb , .m3u , .sln , .aes , .m4u , .snt , .ai , .max , .sql , .ARC , .mdb , .sqlite3 , .asc , .mdf , .sqlitedb , .asf , .mid , .stc , .asm , .mkv , .std , .asp , .mml , .sti , .avi , .mov , .stw , .backup , .mp3 , .suo , .bak , .mp4 , .svg , .bat , .mpeg , .swf , .bmp , .mpg , .sxc , .brd , .msg , .sxd , .bz2 , .myd , .sxi , .c , .myi , .sxm , .cgm , .nef , .sxw , .class , .odb , .tar , .cmd , .odg , .tbk , .cpp , .odp , .tgz , .crt , .ods , .tif , .cs , .odt , .tiff , .csr , .onetoc2 , .txt , .csv , .ost , .uop , .db , .otg , .uot , .dbf , .otp , .vb , .dch , .ots , .vbs , .der" , .ott , .vcd , .dif , .p12 , .vdi , .dip , .PAQ , .vmdk , .djvu , .pas , .vmx , .docb , .pdf , .vob , .docm , .pem , .vsd , .docx , .pfx , .vsdx , .dot , .php , .wav , .dotm , .pl , .wb2 , .dotx , .png , .wk1 , .dwg , .pot , .wks , .edb , .potm , .wma , .eml , .potx , .wmv , .fla , .ppam , .xlc , .flv , .pps , .xlm , .frm , .ppsm , .xls , .gif , .ppsx , .xlsb , .gpg , .ppt , .xlsm , .gz , .pptm , .xlsx , .h , .pptx , .xlt , .hwp , .ps1 , .xltm , .ibd , .psd , .xltx , .iso , .pst , .xlw , .jar , .rar , .zip , .java , .raw.

WannaCrypt จะดำเนินการเข้ารหัสไฟล์ทั้งหมดที่มันพบ จากนั้นดำเนินการเปลี่ยนชื่อโดยเติม .WNCRY ไปที่ชื่อของไฟล์ ตัวอย่างเช่น หากไฟล์นั้นมีชื่อว่า picture.jpg เจ้าตัว Ransomware จะเข้ารหัสแล้วเปลี่ยนชื่อไฟล์ไปเป็น picture.jpg.WNCRY

Ransomware ตัวนี้ยังสร้างไฟล์ @ Please_Read_Me @ .txt ในโฟลเดอร์ที่มีการเข้ารหัสไฟล์ทุกไฟล์ โดยภายในไฟล์นี้จะมีข้อมูลเรียกค่าไถ่เหมือนกัน ดังแสดงในภาพวอลล์เปเปอร์ที่ได้รับการแทนที่ หลังจากเสร็จสิ้นกระบวนการเข้ารหัส มัลแวร์จะทำการลบสำเนาเงา (Shadow Copy) ของไดรฟ์ข้อมูลโดยเรียกใช้คำสั่งต่อไปนี้

cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog –quiet

จากนั้นจะแทนที่ภาพพื้นหลังเดสก์ท็อปที่มีข้อความต่อไปนี้ (รูปที่ 3)



รูปที่ 3 หน้าจอที่แสดงว่าแฟ้มข้อมูลถูกเข้ารหัสแล้ว

นอกจากนี้ยังเรียกใช้โปรแกรมที่แสดงค่าไถ่ซึ่งระบุค่าไถ่ที่ 300 เหรียญใน Bitcoins รวมถึงตัวจับเวลาและข้อความเป็นภาษาต่างๆ โดยข้อความดังกล่าวจะเป็นภาษาท้องถิ่น อาทิ บัลแกเรีย จีน (ตัวย่อ) จีน (ดั้งเดิม) โครเอเชีย เช็ก เดนมาร์ก ดัตช์ อังกฤษ ฟิลิปปินส์ ฟินแลนด์ ฝรั่งเศส เยอรมัน กรีก อินโดนีเซีย อิตาลี ญี่ปุ่น เกาหลี ลัตเวีย นอร์เวย์ โปแลนด์ โปรตุเกส โรมาเนีย รัสเซีย สโลวัก สเปน สวีเดน ตุรกี และเวียตนาม

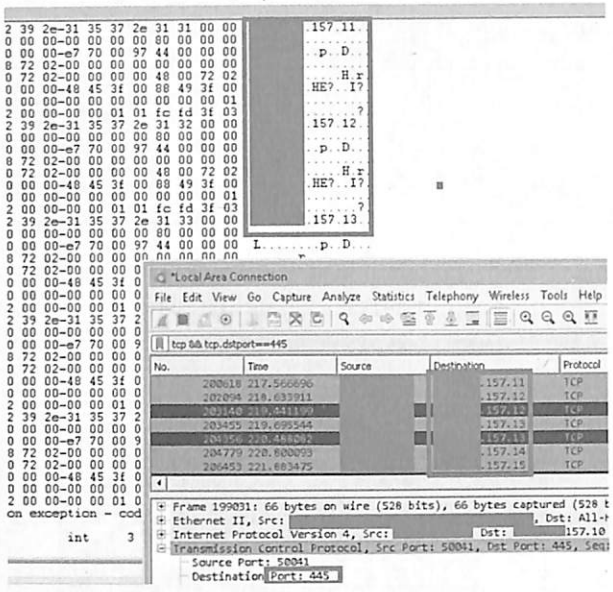
Ransomware ยังแสดงให้เห็นถึงความสามารถในการถอดรหัสโดยให้ผู้ใช้งานสามารถถอดรหัสไฟล์สุ่มได้สองสามแบบโดยไม่เสียค่าใช้จ่าย จากนั้นจะแจ้งเตือนผู้ใช้งานให้ชำระค่าไถ่เพื่อถอดรหัสไฟล์ที่เหลือทั้งหมด (รูปที่ 4 และ 5)

รูปที่ 4 แสดงว่าเครื่องติด Ransomware เรียบร้อย

รูปที่ 5 ข้อความขู่กรรโชกจากเครื่องที่ติด Ransomware

ความสามารถในการแพร่กระจาย

Worm ตัวนี้มีหน้าที่ที่จะพยายามปนเปื้อนเข้าไปในเครื่อง Windows ที่ไม่ได้ติดตั้งแพตช์ในเครือข่าย ในเวลาเดียวกันระบบยังทำการสแกนข้อมูลอินเทอร์เน็ต ไอพีแอดเดรสเพื่อค้นหาคอมพิวเตอร์ที่อยู่ในเครือข่ายเพื่อหาช่องโหว่ของแต่ละเครื่องอย่างขนานใหญ่ กิจกรรมนี้ทำให้มีการรับส่งข้อมูลขนาดใหญ่จากเครื่องคอมพิวเตอร์ที่ติดไวรัส ซึ่งเจ้าหน้าที่ฝ่ายดูแลเกี่ยวกับความปลอดภัยหรือ Security สามารถสังเกตได้ดังรูปที่ 6

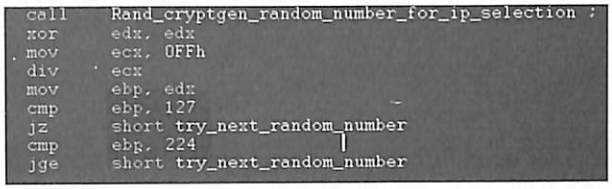


รูปที่ 6 การใช้ Wireshark ตรวจสอบการทำงานของ Ransomware

ขั้นตอนการสแกนอินเทอร์เน็ตของ Worm ตัวนี้จะสุ่มสร้าง Octets เพื่อสร้าง IPv4 Address จากนั้นมัลแวร์จะกำหนดเป้าหมายไอพีดังกล่าวเพื่อพยายามใช้ CVE-2017-0145 ภัยคุกคามนี้จะหลีกเลี่ยงการติดไวรัสที่อยู่ IPv4 ถ้าค่าที่สร้างขึ้นโดยสุ่มสำหรับ Octet แรกคือ 127 หรือหากค่าเท่ากับหรือมากกว่า 224 และเพื่อที่จะข้าม Loopback Interface ภายในเครื่อง และเมื่อเครื่องที่มีช่องโหว่ถูกตรวจพบว่าติดเชื้อ จะกลายเป็นการก้าวกระโดดต่อไปเพื่อทำให้เครื่องอื่นๆ ติดเชื้อตามไปด้วย วัฏจักรการติดเชื้อยังคงดำเนินต่อไป เนื่องจากการสแกนเส้นทางพบคอมพิวเตอร์ที่ยังไม่ได้รับการติดตั้งแพตช์ที่ผ่านการอัปเดต

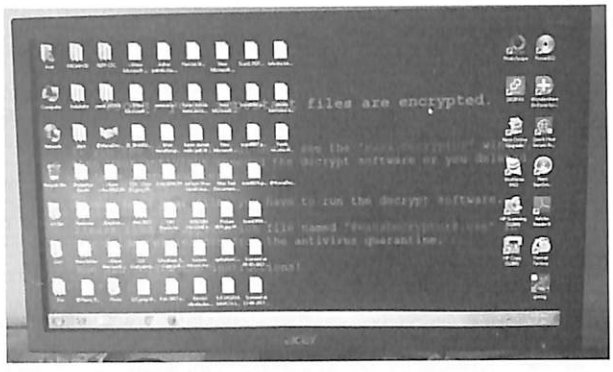
หลังจากที่ประสบความสำเร็จในการทำให้เครื่องที่มีช่องโหว่ติดเชื้อแล้ว มัลแวร์จะรันเชลล์โค้ด (Shell Code) ในระดับเคอร์เนล (Kernel) ซึ่งดูเหมือนว่าวิธีนี้จะถูกคัดลอกมาจาก Public Backdoor ที่รู้จักกันในนาม DOUBLEPULSAR แต่มีการปรับเปลี่ยนบางอย่างเพื่อลดและเรียกใช้งาน Dropper ของ Ransomware ทั้งที่ออกแบบมาสำหรับระบบ x86 และ x64 (รูปที่ 7 และ 8)

รูปที่ 7 แสดงการปนเปื้อนจาก WannaCrypt0r 2.0



```
call    Rand_cryptgen_random_number_for_ip_selection ; Crypt CrSec
xor     edx, edx
mov     ecx, OFFh
div     ecx
mov     ebp, edx
cmp     ebp, 127
jz      short try_next_random_number
cmp     ebp, 224
jge     short try_next_random_number
```

รูปที่ 8 แสดงการปนเปื้อนจาก WannaCrypt0r 2.0



รูปที่ 9 แสดงหน้าจอที่ถูกเข้ารหัสโดย WannaCrypt

วิธีลบ WannaCrypt0r 2.0 ออกจากพีซีให้สิ้นซาก

จากคำถามที่ว่า WannaCrypt0r 2.0 Ransomware คืออะไร เรามารู้จักกับ Ransomware กันก่อน Ransomware ถูกตรวจพบโดยผู้เชี่ยวชาญด้านความปลอดภัยเมื่อวันศุกร์ที่ 12 พฤษภาคม ค.ศ. 2017 เวลาบ่ายประมาณ 14.00 น. ในประเทศอังกฤษน้อยกว่า 4 ชั่วโมง หลังจากนั้น Ransomware ได้ถูกติดตั้งบนคอมพิวเตอร์ของ NHS และระบบคอมพิวเตอร์หลายแห่งทั่วโลก ปัจจุบันนี้ Ransomware ตัวนี้ถูกเรียกว่า WannaCrypt0r 2.0 Ransomware, WCry 2, WannaCry 2 และ Wanna Decrypt0r 2.0 Ransomware เห็นได้ชัดว่า WannaCrypt0r 2.0 Ransomware ขอค่าไถ่ $300 สำหรับ Bitcoin เพื่อปลดล็อคไฟล์ของเครื่องคอมพิวเตอร์ (รูปที่ 9)

ใครอยู่เบื้องหลังการโจมตีไซเบอร์ทั่วโลกครั้งแรก

ช่วงแรกๆ ผู้ผลิตโปรแกรมเรียกค่าไถ่ชนิดนี้ยังไม่เป็นที่รู้จัก แต่ WannaCrypt0r 2.0 Ransomware เป็นความพยายามครั้งที่ 2 ในการแบล็กเมล โดยได้มีการค้นพบเวอร์ชั่นก่อนหน้านี้ชื่อว่า '.wryriver File Extension' Ransomware ในเดือนกุมภาพันธ์ ค.ศ. 2017 โดยรุ่นเก่าขอให้จ่ายค่าไถ่ Bitcoin 0.1 หรือมีมูลค่าประมาณ 177 เหรียญสหรัฐเพื่อเปิดไฟล์และโปรแกรม

ผู้เสียหายควรจ่ายค่าไถ่เพื่อถอดรหัสข้อมูลหรือไม่

บางครั้งการจ่ายเงินค่าไถ่ได้ช่วยในการถอดรหัส แต่บางครั้งก็ไม่สำหรับ Cryptolocker Ransomware เมื่อไม่กี่ปีที่ผ่านมาผู้ใช้บางรายรายงานว่าพวกเขาได้รับข้อมูลหลังจากชำระค่าไถ่โดยปกติประมาณ 300 ปอนด์ แต่ไม่มีการรับประกันว่าการจ่ายเงินไปแล้วจะช่วยให้ผู้ตกเป็นเหยื่อ WannaCrypt0r 2.0 Ransomware ได้รับข้อมูล

กลับคืน เนื่องจากอาชญากรออนไลน์ไม่ใช่คนที่น่าเชื่อถือ นอกจากนี้ยังมีประเด็นทางจริยธรรมด้วย เช่น การจ่ายค่าไถ่จะช่วยส่งเสริมอาชญากรกระทำความผิดมากยิ่งขึ้น

เคล็ดลับเพื่อที่จะหลีกเลี่ยง WannaCrypt0r 2.0 Ransomware

อ่านข้อกำหนดการให้สิทธิ์ผู้ใช้งานปลายทางทั้งหมดในระหว่างการติดตั้งของขวัญส่งเสริมการขายบางอย่าง

- ตรวจสอบให้แน่ใจว่าอีเมลสแปมได้รับจากผู้เขียนที่เชื่อถือได้ก่อนที่จะเปิดหรือดาวน์โหลด
- ติดตั้งโปรแกรมปรับปรุงความปลอดภัยสำหรับโปรแกรมหรือไดรเวอร์เฉพาะบนเว็บไซต์อย่างเป็นทางการเท่านั้น
- ตรวจสอบเว็บไซต์ที่น่าสงสัยก่อนคลิกที่รายการ
- ต้องมีประสิทธิภาพมากขึ้นในการติดตั้งด้านความปลอดภัยเพื่อให้เครื่องพีซีได้รับการปกป้องเลย
- เลือกการติดตั้งแบบกำหนดเองและปิดการติดตั้งไฟล์ที่ไม่รู้จัก

วิธีถอนการติดตั้ง WannaCrypt0r 2.0 Ransomware

สำหรับวิธีแก้ปัญหาอย่างรวดเร็วและมีประสิทธิภาพในการกำจัด WannaCrypt0r 2.0 Ransomware จากคอมพิวเตอร์ของท่าน โดยท่านสามารถเรียกใช้การสแกนด้วยเครื่องมือกำจัดมัลแวร์ขั้นสูงและลบ WannaCrypt0r 2.0 Ransomware ได้ภายในไม่กี่คลิกเท่านั้น

ขั้นตอนที่ 1 : เริ่มต้นคอมพิวเตอร์ของคุณใน Safe Mode พร้อมด้วยเครือข่าย การบูตเข้าสู่ Safe Mode ใน Windows 8 หรือ 10

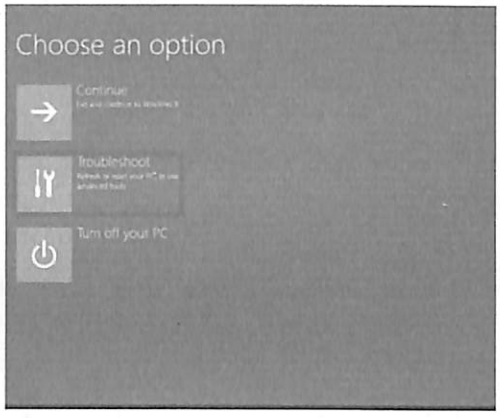
รูปที่ 10 หน้าจอสำหรับ Windows 8

รูปที่ 11 หน้าจอ Windows 10

มีหลายวิธีในการเข้าสู่โหมดปลอดภัยด้วยตัวเลือกเครือข่ายบนระบบคอมพิวเตอร์ Windows ของท่าน แต่ใช้ Windows 8 & 10 OS มีฟังก์ชั่นบางอย่างจำเป็นต้องเข้าถึงด้วยขั้นตอนเพียงเล็กน้อย เรามาเข้าสู่ Safe Mode ใน Windows 8 หรือ Windows 10 (รูปที่ 10 และ 11)

ต่อไปนี้เป็นวิธีการที่ง่ายที่สุด เรียกได้ว่าเป็น Safe Mode ในระบบเครือข่าย

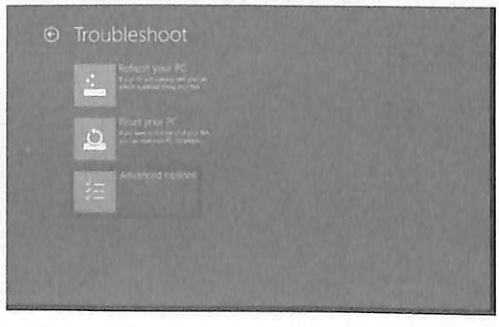
1. บูตเครื่องคอมพิวเตอร์ของคุณไปยังหน้าจอเพื่อเข้าสู่ระบบแล้วกดปุ่ม SHIFT ขณะที่กดปุ่ม RESTART ค้างไว้
2. ขั้นตอนนี้จะพาท่านเข้าสู่หน้าจอ Troubleshooting Option ซึ่งทำให้มีการ Enable Safe Mode (รูปที่ 12)



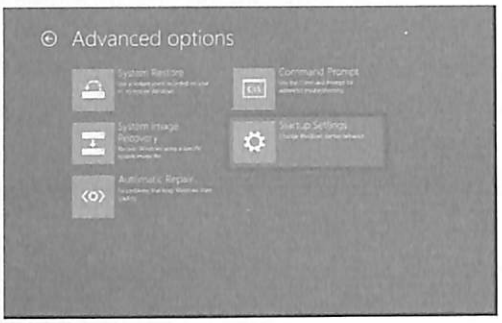
รูปที่ 12 หน้าจอ Troubleshooting Option

ในสถานการณ์อื่นๆ มีตัวเลือกที่คุณไม่สามารถบูตหน้าจอการเข้าสู่ระบบได้ ตรงนี้ท่านสามารถดูหน้าจออื่นที่เรียกว่าหน้าจอการกู้คืน เมื่อต้องการเข้าถึงหน้าต่างนี้ท่านสามารถกดปุ่ม SHIFT ค้างไว้และแตะที่ปุ่ม F8 ขั้นตอนนี้จะทำให้ท่านสามารถเข้าสู่ “โหมดการกู้คืน” ขั้นสูง ตรงจุดนี้ท่านสามารถเลือกตัวเลือกขั้นสูงได้

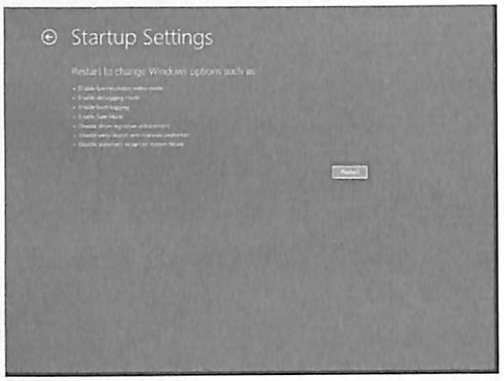
- คลิกเลือก Advanced options (รูปที่ 13)
- มาที่ Startup Settings (รูปที่ 14)
- ตรงนี้ให้คลิกที่ปุ่ม Restart (รูปที่ 15)
- เมื่อคอมพิวเตอร์ได้ดำเนินรีสตาร์ท รอบสุดท้ายเลือกหัวข้อหมายเลข 5 เพื่อ Enable Safe Mode with Networking จากหน้าจอเมนู (รูปที่ 16) ใส่รายละเอียดของ Admin Login และเข้าสู่ Windows ด้วย Safe Mode พร้อมด้วย Networking



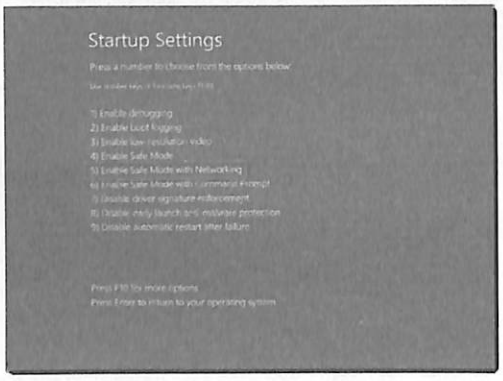
รูปที่ 13 หน้าจอเลือก Advanced Options



รูปที่ 14 หน้าจอ Startup Settings

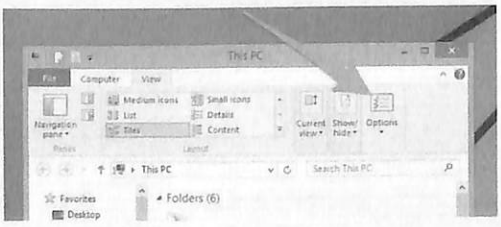


รูปที่ 15 หน้าจอเมนูใน Startup Settings

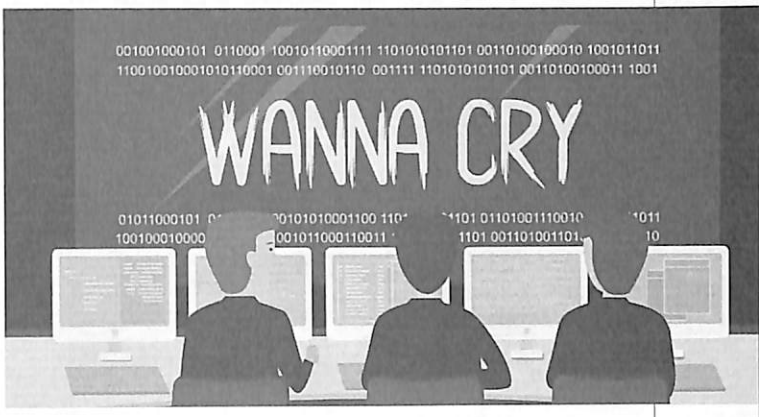


รูปที่ 16 หน้าจอเมนูสำหรับ Startup Settings

ขั้นตอนที่ 2 : วิธีแสดงแฟ้มข้อมูลหรือโฟลเดอร์ที่แอบซ่อนอยู่ ให้กดปุ่ม Windows Key+E จากหน้าต่างที่แสดง ให้ไปที่ View Tab บนเมนู Options จากตำแหน่งไอคอน Options ให้คลิกตรงไอคอน Options (รูปที่ 17)



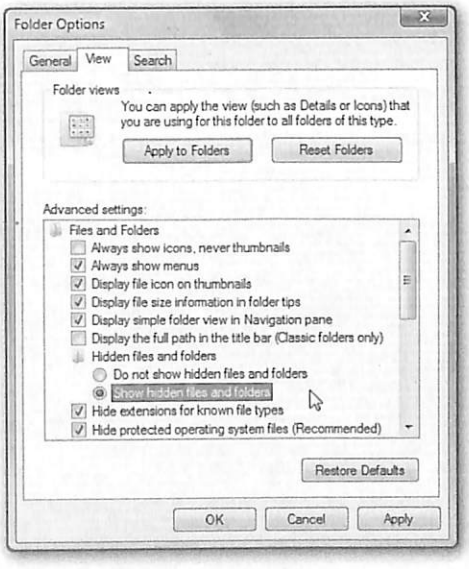
รูปที่ 17 หน้าจอสำหรับเลือก Options



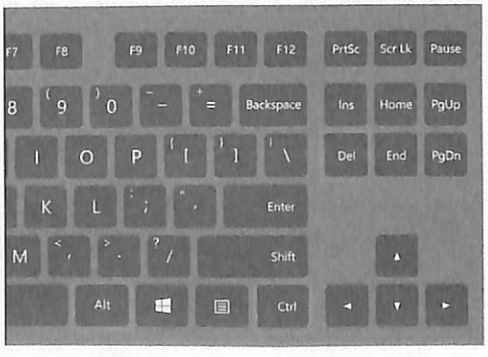
จะทำให้เกิด Dialog Box ขึ้นบนหน้าจอ จากนั้นให้คลิกที่ "Show Hidden Files and Folders" จากนั้นคลิกตรง Apply แล้วตามด้วยปุ่ม OK (รูปที่ 18)

ขั้นตอนที่ 3 : หยุดการทำงานของโปรเซสต่างๆ ที่เกี่ยวข้องกับ WannaCrypt0r 2.0 Ransomware จาก Task Manager

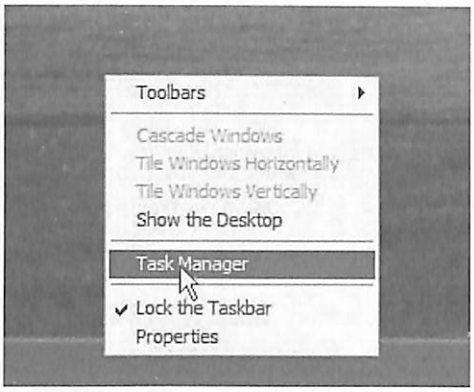
- เพื่อที่จะเปิด Task Manager ให้กดปุ่ม CTRL+ALT+DEL พร้อมกัน (รูปที่ 19)



รูปที่ 18 แสดงหน้าจอ Folder Options



รูปที่ 19 ปุ่มที่ใช้เรียก Task Manager



รูปที่ 20 หน้าจอเรียกใช้ Task Manager

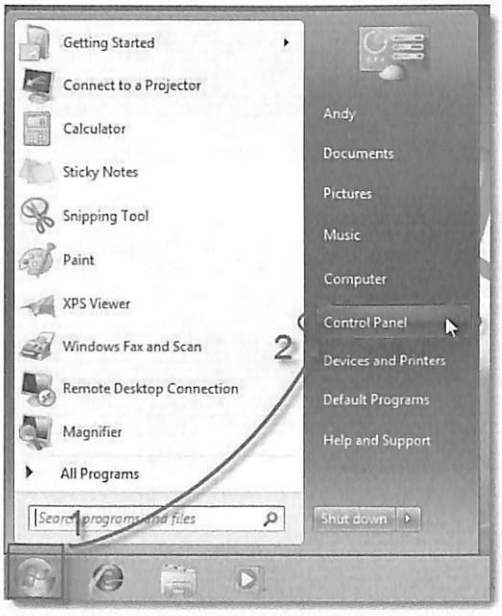
รูปที่ 21 แสดงหน้าจอรายการของโปรเซสต่างๆ

รูปที่ 22 หน้าจอ Windows Task Manager

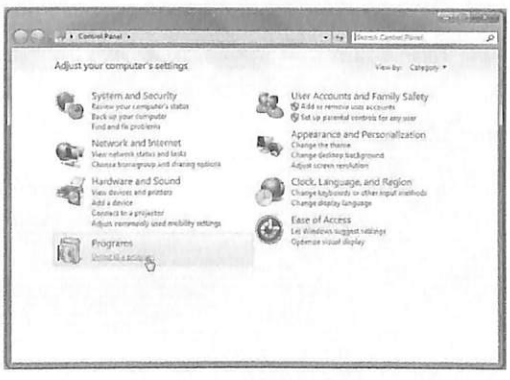
- ท่านสามารถคลิกขวาบน Task Bar และเลือก Task Manager เพื่อเปิด Task Manager บนหน้าจอ (รูปที่ 20)
- ไปที่ Processes Tab และคลิกบนแท็บ ซึ่งจะแสดงรายการของโปรเซสที่กำลังทำงานอยู่ (รูปที่ 21)
- เลือกโปรเซสที่เกี่ยวกับ WannaCrypt0r 2.0 Ransomware และดำเนินการหยุดมันทันทีด้วยปุ่ม End Process
- ตอนนี้ไปที่ Service Tab และหยุดการทำงานของเซอร์วิสที่ไม่รู้จักทั้งหมด (รูปที่ 22)

ขั้นตอนที่ 4 : วิธีเคลื่อนย้าย WannaCrypt0r 2.0 Ransomware จาก Windows Control Panel

- ไปที่เมนู Start จากนั้นคลิกที่ Control Panel ดังตัวอย่างในรูปที่ 23
- หน้าต่างถัดไปจะปรากฏขึ้นพร้อมกับตัวเลือกที่พร้อมใช้งานภายใน Control Panel ซึ่งท่านต้องเลือกถอนการติดตั้งตัวเลือกของโปรแกรม (รูปที่ 24)
- หน้าต่างถัดไปจะแสดงรายการโปรแกรมที่ติดตั้งไว้ในเครื่องคอมพิวเตอร์ของท่าน จากตรงนี้ท่านต้องถอนการติดตั้งโปรแกรมเหล่านั้นทั้งหมดที่ไม่รู้จักแหล่งที่มา หรือไม่ปรากฏชื่อหรือมีความเกี่ยวข้องกับ WannaCrypt0r 2.0 Ransomware

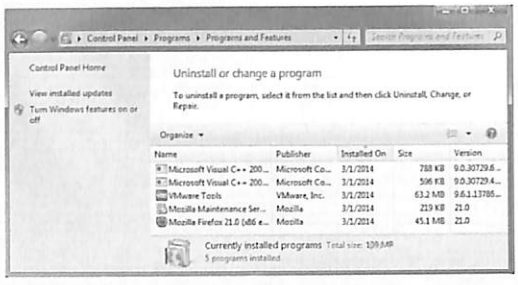


รูปที่ 23 หน้าจอเพื่อเรียกใช้ Control Panel



รูปที่ 24 แสดงหน้าจอ Control Panel

- หน้าต่างถัดไปจะแสดงรายการโปรแกรมที่ติดตั้งไว้ในเครื่องคอมพิวเตอร์ของท่าน จากตรงนี้ท่านต้องถอนการติดตั้งโปรแกรมเหล่านั้นทั้งหมดซึ่งไม่ทราบแหล่งที่มา หรือไม่รู้จักหรือไม่ปรากฏชื่อ หรือเกี่ยวข้องกับ WannaCrypt0r 2.0 Ransomware (รูปที่ 25)



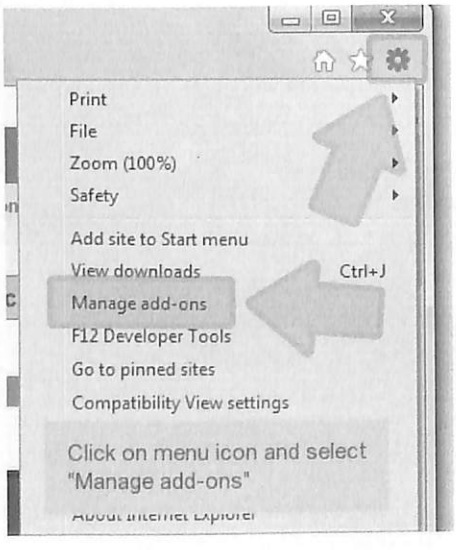
รูปที่ 25 หน้าจอสำหรับถอนโปรแกรมออกจากระบบ

หมายเหตุ

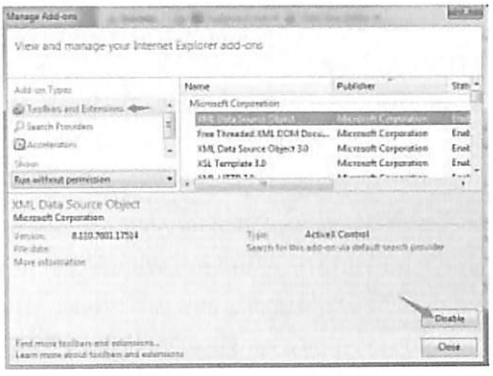
แม้ว่าจะมีการแสดงภาพของหน้าจอ Windows 7 ไว้แล้วก็ตาม แต่ตัวเลือกและการนำทางไปยังหน้าจอต่างๆ สำหรับ Windows XP และ Vista ก็เหมือนกัน

ขั้นตอนที่ 5 : วิธีลบ WannaCrypt0r 2.0 Ransomware ออกจากบราวเซอร์ หาก WannaCrypt0r 2.0 Ransomware ติดค้างอยู่ในเว็บบราวเซอร์ และมักปรากฏตัวให้เห็นอยู่เสมอด้วยเว็บบราวเซอร์จำเป็นต้องตรวจสอบและนำออกจากบราวเซอร์ของท่าน ต่อไปนี้เป็นวิธีนำ Ransomware Wannacrypt 2.0 ออกจากเว็บบราวเซอร์ต่างๆ

- เปิด IE Browser ของท่านแล้ว คลิกที่ปุ่ม Tools ที่มีสัญลักษณ์ ⚙ (รูปที่ 26)
- หลังจากนั้นให้คลิกบน Manage add-ons



รูปที่ 26 หน้าจอ IE Browser ใน Tools



รูปที่ 27 หน้าจอ Manage Add-ons

- จากด้านซ้ายของหน้าต่างถัดไปที่ปรากฏให้คลิกแถบเครื่องมือและส่วนขยายแล้วเลือก WannaCrypt0r 2.0 Ransomware หากมีปรากฏอยู่ในนั้น นอกจากนั้นให้ลบ BHO ทั้งหมดที่ท่านรู้จักและไม่รู้จัก คลิกเพื่อลบส่วนขยายเหล่านั้น หรือคลิก Disable เมื่อใดก็ตามที่เป็นไปได้ (รูปที่ 27) จากนั้นให้รีสตาร์ทบราวเซอร์ของท่าน

การกำจัด WannaCrypt0r 2.0 Ransomware ด้วยตนเองต้องใช้ทักษะทางด้านเทคนิคที่ดีและความรู้ด้านเสียงของไฟล์ระบบและการลงทะเบียนเช่นกัน หากข้อมูลสำคัญใดๆ ถูกลบโดยบังเอิญความเสียหายของระบบถาวรสามารถประสบได้ เพื่อป้องกันไม่ให้เกิดปัญหานี้ควรลบ WannaCrypt0r 2.0 Ransomware ด้วยเครื่องมือลบมัลแวร์ที่เชื่อถือได้

ขั้นตอนที่ 6 : การลบ Wanscrypt0r 2.0 Ransomware จากคอมพิวเตอร์โดยอัตโนมัติ ปัจจุบันมีสแกนเนอร์ฟรีหลายตัวในท้องตลาดที่ท่านสามารถดาวน์โหลดมาเพื่อขจัด Wannacrypt02.0 ให้ใช้เครื่องมือดังกล่าวดำเนินการสแกนและลบออกไปจากระบบ

วิธีป้องกันการโจมตีจาก WannaCrypt

ดังที่เราทราบกันดีว่า Wannacrypt เป็น Ransomware ที่มุ่งเน้นการโจมตีไปที่คอมพิวเตอร์ทั่วโลกที่มีการใช้ Windows ที่ต่ำกว่า Windows 10 ซึ่งได้แก่ Windows XP, Windows 8 และ Windows Server 2003 ที่ไม่ได้รับการป้องกันด้วยการอัปเดตแพตช์จากไมโครซอฟท์ ดังนั้นหากท่านต้องการป้องกัน Ransomware ชนิดนี้ท่านต้องดำเนินการอัปเดตแพตช์ของไมโครซอฟท์ทันที หรือไม่ก็เปลี่ยนแปลงไปใช้ Windows 10 แทน แต่อย่างไรก็ตามคอมพิวเตอร์ที่ใช้ Windows 10 ก็ยังต้องมีการอัปเดตแพตช์เช่นกันเพื่อป้องกันมิให้มีโอกาสติด Ransomware ขึ้นในอนาคต สังเกตว่าบรรดามัลแวร์หรือ Ransomware ทั้งหลายมักจะเกิดขึ้นกับผลิตภัณฑ์ซอฟต์แวร์หรือระบบปฏิบัติการที่ทางผู้ผลิตยกเลิกหรือหมดอายุ License ซึ่งจะทำให้เกิดช่องโหว่ที่ทางผู้ไม่หวังดีพัฒนาขึ้นมา

เพื่อที่จะดำเนินการป้องกัน Ransomware ล่าสุดไมโครซอฟท์ได้ตอบสนองด้วยการเปิดให้อัปเดตแพตช์ล่าสุดเพื่อป้องกันเครื่องที่ยังไม่ติด Ransomware โดยติดตั้ง Security Update MS17-010 ให้เร็วที่สุดเท่าที่จะทำได้จนกว่าจะมีการใช้แพตช์ อย่างไรก็ดีแนะนำให้ดำเนินการดังนี้โดยด่วน

- Disable SMBv1 ด้วยขั้นตอนวิธีการที่ระบุไว้ใน Microsoft Knowledge Base Article 2696547
- พิจารณาเพิ่มกฎกติกาบนเราเตอร์หรือไฟร์วอลล์เพื่อบล็อก (Block) กระแสการจราจรของ SMB ที่วิ่งเข้ามาด้วยพอร์ตหมายเลข 445
- หากท่านใช้ Windows Defender Antivirus มันจะตรวจพบอันตรายนี้ภายใต้ชื่อ **Ransom:Win32/WannaCrypt** เป็นของ 1.243.297.0 Update อย่างไรก็ดี Windows Defender Antivirus ใช้ระบบ Cloud-based Protection ซึ่งเป็นระบบป้องกันที่ซับซ้อนในปัจจุบันเพื่อช่วยท่านในการป้องกันจากภยันตรายล่าสุด
- สำหรับองค์กรขนาดใหญ่ให้ใช้ Device Guard เพื่อดำเนินการ Lock Down อุปกรณ์ และเพื่อทำให้มีการป้องกันในระดับเคอร์เนลโดยอนุญาตให้เฉพาะแอพพลิเคชั่นที่น่าเชื่อถือได้เท่านั้นสามารถทำงานบนระบบ วิธีนี้เป็นการป้องกันมัลแวร์ได้อย่างมีประสิทธิภาพ
- ใช้ Office 365 Advanced Threat Protection ซึ่งภายในมีระบบที่มีขีดความสามารถในระดับเครื่องจักรเรียนรู้ (Machine Learning) ที่สามารถบล็อกอันตรายจากอีเมล เช่น อีเมลที่เป็นพาหะของ Ransomware
- มอนิเตอร์ (Monitor) ระบบเครือข่ายด้วย Windows Defender Advanced Threat Protection ซึ่งจะช่วยแจ้งเตือนทีมงานที่ดูแลระบบรักษาความปลอดภัยเกี่ยวกับกิจกรรมที่น่าสงสัย ให้ดาวน์โหลด Playbook นี้เพื่อดูว่าท่านสามารถยกระดับการทำงานของ Windows Defender ATP เพื่อการตรวจหาสืบค้น และหากต้องการบรรเทา Ransomware ภายในเครือข่าย ให้ดาวน์โหลด Windows Defender Advanced Threat Protection – Ransomware Response Playbook จากเว็บไซต์ของไมโครซอฟท์ หรือ https://www.microsoft.com/en-us/download/details.aspx?id=55090

แหล่งสำหรับดาวน์โหลด Security Update เพื่อป้องกันระบบ

- ให้ดาวน์โหลด Security Updates ฉบับภาษาอังกฤษ ได้แก่ Windows Server 2003 SP2 x64, Windows Server 2003 SP2 x86, Windows XP SP2 x64, Windows XP SP3 x86, Windows XP Embedded SP3 x86, Windows 8 x86, Windows 8 x64
- ให้ดาวน์โหลด Security Updates ที่เป็นภาษาท้องถิ่น ได้แก่ Windows Server 2003 SP2 x64, Windows Server 2003 SP2 x86, Windows XP SP2 x64, Windows XP SP3 x86, Windows XP Embedded SP3 x86, Windows 8 x86, Windows 8 x64
- MS17-010 Security Update : https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- หากต้องการคำแนะนำเกี่ยวกับการโจมตีของ WannaCrypt ของไมโครซอฟท์ให้ไปที่เว็บไซต์ https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
- ข้อมูลข่าวสารทั่วไปเกี่ยวกับ Ransomware : https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

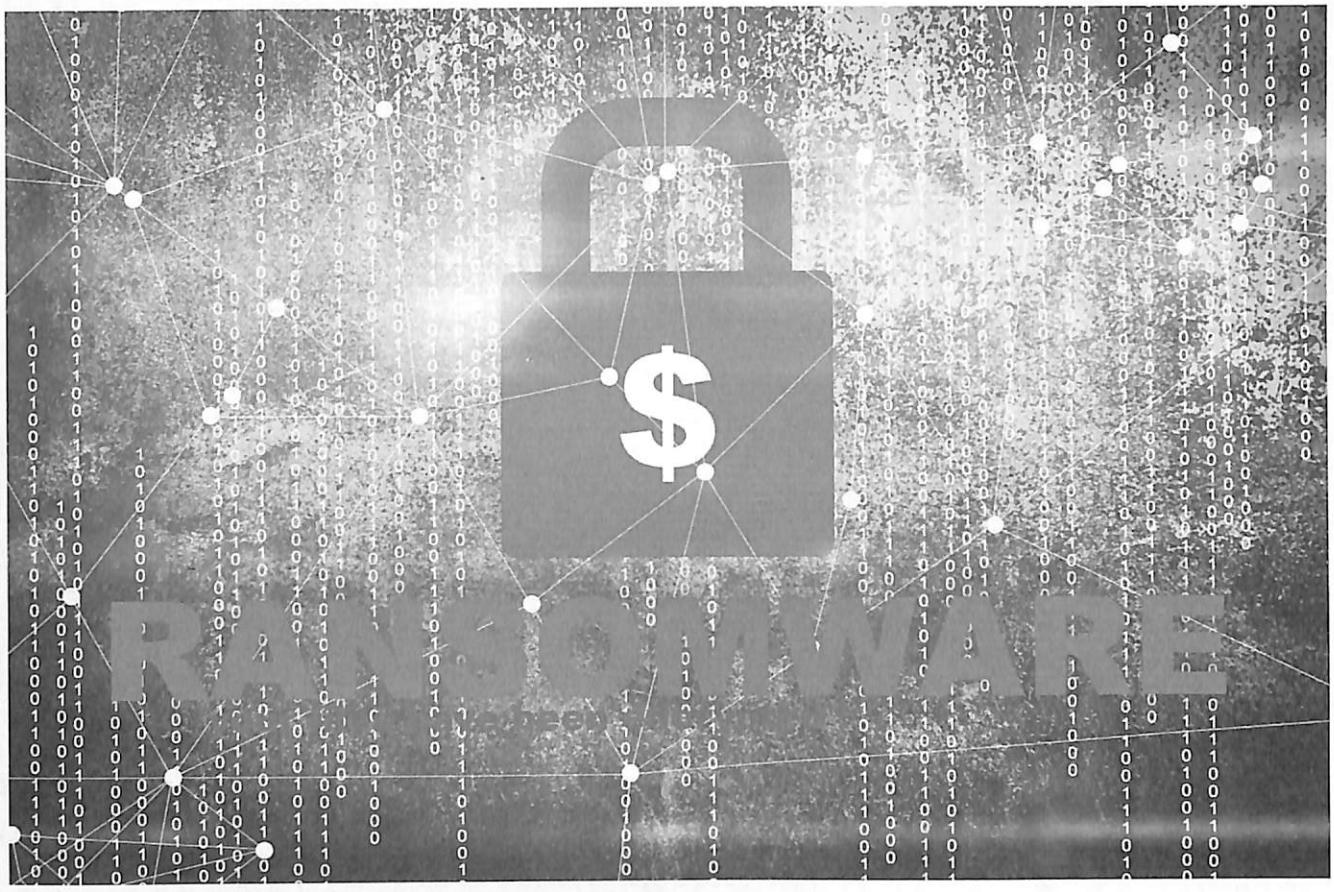
สิ่งที่บ่งบอกว่าเครื่องมีช่องโหว่และกำลังติด Ransomware

ตัวอย่างที่วิเคราะห์บน SHA1

51e4307093f8ca8854359c0ac882ddca427a813c
e889544aff85ffaf8b0d0da705105dee7c97fe26
Files created:
%SystemRoot%\mssecsvc.exe
%SystemRoot%\tasksche.exe
%SystemRoot%\qeriuwjhrf
b.wnry
c.wnry
f.wnry
r.wnry
s.wnry
t.wnry
u.wnry
taskdl.exe
taskse.exe
00000000.eky
00000000.res
00000000.pky
@WanaDecryptor@.exe
@Please_Read_Me@.txt
m.vbs
@WanaDecryptor@.exe.lnk
@WanaDecryptor@.bmp
274901494632976.bat
taskdl.exe
Taskse.exe
Files with ".wnry" extension
Files with ".WNCRY" extension
Registry keys created:
HKLM\SOFTWARE\WanaCrypt0r\wd

ข้อมูลส่วนใหญ่ในบทความนี้มาจากแหล่งต่างๆ ในอินเทอร์เน็ต รวมทั้งเว็บไซต์จากไมโครซอฟท์ หากท่านต้องการข้อมูลเพิ่มเติมสามารถติดตามดูจากเว็บไซต์ต่างๆ ได้ครับ

■ ทศพนธ์ นรทัศน์
hs4hnl@gmail.com



การรับมือ “Ransomware” ของประเทศไทย

บทบาทการดำเนินงานของหน่วยงาน นโยบาย แผน ยุทธศาสตร์ กฎหมาย และมาตรการรับมือแรนซัมแวร์ของประเทศไทย ที่มีอยู่ในปัจจุบัน และที่จะมีในอนาคต

บทนำ

การโจมตีทางไซเบอร์ถือเป็นภัยคุกคามรูปแบบใหม่ที่ส่งผลกระทบต่อความมั่นคงของชาติ รัฐบาลของหลายประเทศ จึงได้มีการออกกฎหมาย การจัดตั้งหน่วยงาน การออกนโยบาย แผน และยุทธศาสตร์มารับมือกับภัยคุกคามดังกล่าว สำหรับประเทศไทย แม้ภาครัฐจะให้ความสำคัญต่อการรับมือภัยคุกคามรูปแบบใหม่นี้มาอย่างต่อเนื่อง แต่สถานการณ์ในห้วงเวลาที่ผ่านมาหลายปี ก็ยังไม่การโจมตีที่ก่อให้เกิดความเสียหายและผลกระทบในวงกว้าง เช่นเดียวกับกรณีของแรนซัมแวร์ (Ransomware) หรือมัลแวร์เรียกค่าไถ่ ที่ชื่อ “WannaCry” ซึ่งระบาดผ่านช่องโหว่ของระบบปฏิบัติการวินโดว์ไปทั่วโลก เมื่อเดือนพฤษภาคม 2560 ที่ผ่านมา

กองบรรณาธิการนิตยสารไมโครคอมพิวเตอร์ (2560) ได้ระบุว่า *“เพียงไม่กี่วันที่ผ่านมาแรนซัมแวร์ WannaCry ได้โจมตีองค์กรนับพันและยูสเซอร์ทั่วโลก กระทบต่อองค์กรจำนวนมหาศาลในหลายกลุ่มธุรกิจทั่วโลก WannaCry ได้สะท้อนให้เห็นถึงผลกระทบที่เกิดขึ้นได้ในชีวิตจริงของแรนซัมแวร์ ไม่ว่าจะเป็นการทำลายระบบ ทำให้การปฏิบัติงานหยุดชะงัก ทำให้ชื่อเสียงเสื่อมเสีย และสร้างความเสียหายทางการเงิน อันเป็นผลมาจากการที่ไม่สามารถดำเนินธุรกิจ*

ได้ตามปกติ ทั้งนี้ยังไม่รวมถึงค่าใช้จ่ายที่เกิดขึ้นจากการจัดการกับเหตุการณ์ด้านความปลอดภัยที่เกิดขึ้นและการกู้คืนระบบ"

บทความนี้ จะนำเสนอถึงบทบาทการดำเนินงานของหน่วยงานนโยบาย แผน ยุทธศาสตร์ กฎหมาย และมาตราการรับมือแรนซัมแวร์ของประเทศไทยที่มีอยู่ในปัจจุบัน และที่จะมีในอนาคต เพื่อเป็นหลักประกันความมั่นคงปลอดภัยของระบบเศรษฐกิจและสังคมดิจิทัลของประเทศไทย ตามนโยบาย Thailand 4.0

การรับมือของภาครัฐในปัจจุบัน

1. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้ออกประกาศ "ระวังภัยมัลแวร์เรียกค่าไถ่ WannaCry แพร่กระจายผ่านช่องโหว่ของวินโดวส์ รีบอัปเดตทันที" เมื่อวันที่ 13 พฤษภาคม 2560 ผ่านทางเว็บไซต์ www.thaicert.or.th/alerts/user/2017/al2017us001.html โดยไทยเซิร์ตระบุว่ามัลแวร์ดังกล่าวเป็นภัยคุกคามประเภท : Intrusion (การบุกรุก)

สถานการณ์การโจมตี เมื่อวันที่ 12 พฤษภาคม 2560 บริษัท Avast ได้รายงานการแพร่ระบาดของมัลแวร์เรียกค่าไถ่ชื่อ WannaCry โดยมัลแวร์ดังกล่าวมีจุดประสงค์หลักเพื่อเข้ารหัสลับข้อมูลในคอมพิวเตอร์เพื่อเรียกค่าไถ่ หากไม่จ่ายเงินตามที่เรียกจะไม่สามารถเปิดไฟล์ได้

สิ่งที่น่ากังวลเป็นพิเศษสำหรับมัลแวร์นี้ คือ ความสามารถในการกระจายตัวเองจากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่นๆ ในเครือข่ายได้โดยอัตโนมัติผ่านช่องโหว่ระบบ SMB (Server Message Block) ของวินโดวส์ ผู้ใช้งานที่ไม่อัปเดตระบบปฏิบัติการวินโดวส์มีความเสี่ยงที่จะติดมัลแวร์นี้

ช่องโหว่ที่ถูกใช้ในการแพร่กระจายมัลแวร์เป็นช่องโหว่ที่ถูกเปิดเผยสู่สาธารณะตั้งแต่ช่วงเดือนเมษายน 2560 และถึงแม้ทาง Microsoft จะเผยแพร่อัปเดตแก้ไขช่องโหว่ดังกล่าวไปตั้งแต่วันที่ 14 มีนาคม 2560 แล้ว แต่ก็ยังพบว่าปัจจุบันมีเครื่องคอมพิวเตอร์ที่ยังไม่ได้อัปเดตแพตช์ดังกล่าวและถูกโจมตีจากมัลแวร์นี้มากกว่า 200,000 เครื่อง จาก 112 ประเทศ โดยเกิดผลกระทบสูงต่อหน่วยงานสาธารณสุขของประเทศอังกฤษ **ในประเทศไทยพบผู้ติดมัลแวร์ตัวนี้อยู่บ้าง แต่ยังไม่พบการแพร่กระจายในวงกว้าง**

จากข้อมูลของ Microsoft ระบบปฏิบัติการที่มีช่องโหว่ในระบบ SMB เวอร์ชัน 1 ที่ถูกใช้ในการโจมตีโดยมัลแวร์นี้ มีตั้งแต่ Windows XP, Windows Server 2003 ไปจนถึง Windows 10 และ Windows Server 2016 แต่เมื่อเดือนมีนาคม 2560 ทาง Microsoft ไม่ได้ออกอัปเดตแก้ไขช่องโหว่นี้ให้กับ Windows XP และ Windows Server 2003 เนื่องจากสิ้นสุดระยะเวลาสนับสนุนไปแล้ว อย่างไรก็ตาม เนื่องจากปัจจุบันยังมีเครื่องคอมพิวเตอร์ที่ใช้งานสองระบบปฏิบัติการดังกล่าวและยังเชื่อมต่อกับอินเทอร์เน็ตอยู่ จึงทำให้ถูกโจมตีได้ Microsoft จึงออกอัปเดตฉุกเฉินมาเพื่อแก้ไขปัญหานี้ โดยผู้ใช้สามารถดาวน์โหลดอัปเดตดังกล่าวได้จากเว็บไซต์ของ Microsoft

ที่มา : www.facebook.com/thaicert/photos/rpp.178292355652239/901033540044780/?type=3&theater

พฤติกรรมของมัลแวร์ WannaCry พบข้อมูลรายงานการตรวจสอบมัลแวร์จากเว็บไซต์ Hybrid Analysis ซึ่งให้บริการวิเคราะห์มัลแวร์ มีผลลัพธ์ของการวิเคราะห์ไฟล์ต้องสงสัย ซึ่งผู้ใช้งานตั้งชื่อว่า wannacry.exe โดยผลลัพธ์แสดงให้เห็นว่าเป็นมัลแวร์ประเภท Ransomware และมีสายพันธุ์สอดคล้องกับมัลแวร์ WannaCry ที่แพร่ระบาดอยู่ในปัจจุบัน ซึ่งมีฟังก์ชันที่พบเรื่องการเข้ารหัสลับข้อมูลไฟล์เอกสารบนเครื่องคอมพิวเตอร์ การแสดงผลข้อความเรียกค่าไถ่ เป็นต้น โดยในรายงานกล่าวถึงการเชื่อมโยงข้อมูลกับไอพีแอดเดรสจากต่างประเทศ ซึ่งคาดว่าเป็นไอพีแอดเดรสของผู้ไม่ประสงค์ดีที่ใช้ในการควบคุมและสั่งการ

นอกจากนี้ ยังพบว่ามีผู้รวบรวมข้อมูลเกี่ยวกับพฤติกรรมของมัลแวร์ WannaCry ไว้บนเว็บไซต์ Github รวมถึงไฟล์มัลแวร์ตัวอย่าง ซึ่งทางไทยเซิร์ตกำลังอยู่ในระหว่างการนำไฟล์ดังกล่าวมาเข้ากระบวนการตรวจวิเคราะห์ต่อไป

ทั้งนี้ ไทยเซิร์ตยังได้ออก **"ข้อแนะนำวิธีสำรองข้อมูลเพื่อป้องกันมัลแวร์เรียกค่าไถ่หรือข้อมูลสูญหาย"** จัดทำโดย เสฏฐวุฒิ แสนนาม และ ณัฐโชติ ดุสิตานนท์ เผยแพร่เมื่อวันที่ 1 มิถุนายน 2560 (www.thaicert.or.th/papers/general/2017/pa2017ge002.html) และบริการดาวน์โหลดโปรแกรมป้องกันมัลแวร์ WannaCry (thcert.co/T5G9Dn) **รวมทั้งได้แจ้งเตือนและเผยแพร่คำแนะนำดังกล่าวทางเฟซบุ๊ก ThaiCERT (@thaicert) www.facebook.com/thaicert** ตลอดจนทางทวิตเตอร์ @ThaiCERT

2. รัฐบาลเตือน!! ระวังมัลแวร์เรียกค่าไถ่ WannaCry สั่งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศ.) ติดตามสถานการณ์และให้คำแนะนำแก่ประชาชน โดยเมื่อวันที่ 13 พฤษภาคม 2560 **พลเอก ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี** ได้รับรายงานจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศ.) ว่ามีมัลแวร์เรียกค่าไถ่ ชื่อ "WannaCry" ระบาดไปยังคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Microsoft ทั่วโลก จึงฝากเตือนประชาชนให้ระมัดระวังการดาวน์โหลดไฟล์เอกสารจากโลกออนไลน์

"ผู้ใช้งานคอมพิวเตอร์อาจดาวน์โหลดมัลแวร์ หรือโปรแกรมที่ถูกสร้างขึ้นมาเพื่อสร้างความเสียหายแก่ข้อมูลในคอมพิวเตอร์โดยไม่รู้ตัวจากการเปิดไฟล์เอกสารที่แนบมากับอีเมล เมื่อมัลแวร์เรียกค่าไถ่ WannaCry เข้ามาอยู่ในระบบคอมพิวเตอร์แล้ว ก็จะเข้าไปบล็อกไฟล์เอกสารต่างๆ ทำให้ไม่สามารถเปิดใช้งานได้ และขู่ให้ผู้ใช้งานจ่ายเงินค่าไถ่เพื่อปลดล็อกไฟล์เอกสาร"

นายกรัฐมนตรี ได้กำชับให้ ดศ. เร่งตรวจสอบสถานการณ์การแพร่ระบาดของมัลแวร์เรียกค่าไถ่ในไทย พร้อมเผยแพร่คำแนะนำในการป้องกันและแก้ไขให้ประชาชนทราบโดยเร็ว พร้อมฝากเตือนประชาชนที่ใช้งานคอมพิวเตอร์ระบบ Microsoft หลีกเลี่ยงการเปิดเอกสารแนบอีเมล โดยไม่จำเป็น ซึ่งหากเอกสารใดจำเป็นต้องเปิดควรตรวจสอบกับผู้ส่งก่อนทุกครั้งว่ามีการส่งเอกสารนั้นมาจริงหรือไม่ พร้อมทั้งปรับปรุงระบบปฏิบัติการให้เป็นปัจจุบันและ **หากมีข้อสงสัยสอบถามเพิ่มเติมได้ที่ศูนย์ประสานงานความมั่นคงปลอดภัยไซเบอร์ (ThaiCERT) 1212 (www.thaigov.go.th/news/contents/details/3700)**

3. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศ.) มอบไทยเซิร์ตรับมือและช่วยแก้ไขปัญหามัลแวร์เรียกค่าไถ่

เมื่อวันที่ 15 พฤษภาคม 2560 เอกสารข่าวของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศ.) (www.thaigov.go.th/news/contents/details/3737) ระบุว่า**นาวาอากาศเอก สมศักดิ์ ขาวสุวรรณ์** รองปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เปิดเผยว่า จากกรณีที่มีมัลแวร์เรียกค่าไถ่ ชื่อ "WannaCry" ระบาดไปยังคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการไมโครซอฟต์ทั่วโลก เมื่อวันที่ 12 พฤษภาคมที่ผ่านมา ... ปัจจุบันมีคอมพิวเตอร์ที่ถูกระบบ WannaCry นี้เข้าบล็อกข้อมูลแล้วกว่า 1 แสนเครื่องทั่วโลก โดยเฉพาะในประเทศอังกฤษ โรงพยาบาลกว่า 10 แห่ง ไม่สามารถเปิดบริการได้ เนื่องจากคอมพิวเตอร์ถูกมัลแวร์ดังกล่าวเล่นงาน

เมื่อคอมพิวเตอร์ของผู้ใช้คนใดกลายเป็นเหยื่อ หากต้องการที่จะปลดล็อกจะต้องจ่ายเงินประมาณ 300 ดอลลาร์ หรือประมาณ 10,500 บาท และจะเพิ่มมูลค่าขึ้นไปเรื่อยๆ เพื่อเป็นการไถ่ข้อมูลคืน ในรูปแบบของ Bit Coin ไม่เช่นนั้นก็ไม่สามารถเปิดไฟล์เอกสารต่างๆ ได้

รัฐบาลมีความเป็นห่วงกรณีดังกล่าวโดยพลเอกประยุทธ์ จันทร์โอชา นายกรัฐมนตรี ได้สั่งการให้กระทรวงดิจิทัลฯ เร่งติดตามเฝ้าระวังปัญหาที่อาจจะเกิดขึ้นอย่างใกล้ชิด ซึ่ง **ดร.พิเชฐ ดุรงคเวโรจน์** รัฐมนตรีว่าการกระทรวงดิจิทัลฯ ได้มอบหมายให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (ThaiCERT) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ ETDA ดำเนินการแจ้งเตือนและให้คำแนะนำแก่ผู้ใช้คอมพิวเตอร์และผู้ดูแลระบบคอมพิวเตอร์ของหน่วยงานในทันที รวมทั้งติดตามเฝ้าระวังและเตรียมพร้อมให้ความช่วยเหลือผู้ใช้คอมพิวเตอร์หรือผู้ดูแลระบบคอมพิวเตอร์ของหน่วยงานต่างๆ อย่างทันการณ์ตลอดเวลา **ซึ่งในส่วนของประเทศไทยขณะนี้ยังไม่พบความเสียหายที่ร้ายแรงจากการติดมัลแวร์ดังกล่าวแต่อย่างใด**

อย่างไรก็ตาม สิ่งที่ผู้ใช้คอมพิวเตอร์หรือผู้ดูแลระบบของหน่วยงานต้องดำเนินการในเบื้องต้น คือ การป้องกันไม่ให้มัลแวร์ดังกล่าวเข้ามาอยู่ในคอมพิวเตอร์ของเราด้วยการไม่เปิดไฟล์เอกสารแนบของอีเมลโดยไม่จำเป็น และควรตรวจสอบแหล่งที่มาของไฟล์ที่ถูกส่งเข้ามาในอีเมล หรือช่องทางต่างๆ ให้แน่ใจก่อนเปิดอ่าน ที่สำคัญควรปรับปรุงระบบปฏิบัติการคอมพิวเตอร์ หรือ OS ของระบบวินโดว์ (Windows) ให้เป็นเวอร์ชั่นล่าสุด รวมทั้งควรสำเนาข้อมูลสำคัญต่างๆ ไว้ในฮาร์ดดิสก์อื่น (External Hardisk) อยู่เสมอ เพื่อเป็นการสำรองข้อมูล

สำหรับแนวทางการป้องกันการแพร่ระบาดนั้น กรณีผู้ใช้งานทั่วไปเมื่อผู้ใช้พบว่าคอมพิวเตอร์ติดมัลแวร์ดังกล่าวแล้ว ให้ปิดเครื่องและแจ้งผู้ดูแลระบบของหน่วยงาน หรือแจ้งศูนย์ OCC (Online Complaint Center) โทร. 1212 สำหรับผู้ดูแลระบบคอมพิวเตอร์ให้ปิดบริการ SMBv1 ที่ Windows servers และปิดการเข้าถึงพอร์ต TCP/UDP 135-139 และ TCP 445 ที่อุปกรณ์ Firewall โดยสามารถติดต่อ ThaiCERT ETDA โทร. 02-123-1212 ได้ตลอด 24 ชม.

4. คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) จัดทำแนวทางปฏิบัติและกติการับมือมัลแวร์เรียกค่าไถ่ พร้อมแจ้งเตือนบริษัทประกันภัยให้เฝ้าระวังและเตรียมการอย่างเป็นระบบ รวมทั้งเสนอแนะว่าถึงเวลาแล้วที่ต้องใช้การประกันภัยไซเบอร์ ในการบริหารความเสี่ยง

เมื่อวันที่ 18 พฤษภาคม 2560 เอกสารข่าวของกลุ่มสารนิเทศการคลัง สำนักงานปลัดกระทรวงการคลัง (www.thaigov.go.th/news/contents/details/3817) ระบุว่า **ดร.สุทธิพล ทวีชัยการ** เลขาธิการคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) เปิดเผยว่า...สำนักงาน คปภ. มีความตระหนักถึงผลกระทบจากภัยคุกคามดังกล่าวต่อระบบประกันภัย โดยได้กำหนดมาตรการรับมือภัยคุกคามในสองระดับ คือ ในระดับขององค์กรเบื้องต้นได้จัดทำแนวทางปฏิบัติในการป้องกันมัลแวร์ภายในองค์กร และสั่งการให้ สำนักงาน คปภ. ทั่วประเทศ ดำเนินการตามแนวปฏิบัติดังกล่าวอย่างเคร่งครัด เพื่อเป็นการเฝ้าระวังและป้องกันภัยคุกคามทางคอมพิวเตอร์ที่อาจเจาะเข้ามาในระบบของสำนักงานคปภ. ระดับที่สองเป็นมาตรการในส่วนของภาคอุตสาหกรรมประกันภัย

สำนักงาน คปภ. ในฐานะหน่วยงานกำกับได้เฝ้าติดตามสถานการณ์อย่างใกล้ชิดแม้ในขณะนี้ยังไม่ได้รับรายงานผลกระทบจากเหตุการณ์ดังกล่าวในธุรกิจประกันภัย แต่เพื่อเป็นการป้องกันภัยคุกคามทางคอมพิวเตอร์ของภาคธุรกิจประกันภัย จึงได้ประสานไปยังสมาคมประกันชีวิตไทย และสมาคมประกันวินาศภัยไทย แจ้งเวียนบริษัทสมาชิกให้เฝ้าระวัง และเตรียมการอย่างเป็นระบบ ตั้งแต่การป้องกัน การรับมือกับภัยคุกคามทางคอมพิวเตอร์ รวมทั้งสื่อสารให้พนักงานและประชาชนทราบแนวทางป้องกันการแพร่ระบาดอย่างเหมาะสม และขอให้รายงานสถานการณ์เฝ้าระวังภัยคุกคามทางคอมพิวเตอร์ต่อสำนักงาน คปภ. เป็นระยะๆ โดยหากได้รับผลกระทบจากภัยดังกล่าว ขอให้แจ้งมายังสำนักงาน คปภ. เพื่อประสานให้ความช่วยเหลือ โดยจะมีการบูรณาการทำงานร่วมกันอย่างเป็นระบบเพื่อเตรียมการรับมือในเรื่องนี้

นอกจากนี้ **สำนักงาน คปภ.มีนโยบายส่งเสริมให้บริษัทประกันภัยพัฒนาผลิตภัณฑ์ประกันภัยที่จะช่วยรองรับความเสี่ยงจากการจู่โจมหรือคุกคามทางไซเบอร์ นั่นคือการประกันภัยไซเบอร์ (Cyber Insurance)** ซึ่งถูกออกแบบมาเพื่อป้องกันความเสี่ยงต่อความเสียหายทางคอมพิวเตอร์ที่เกิดขึ้นกับธุรกิจในเชิงพาณิชย์ได้ทุกประเภท ไม่ว่าจะเป็นผู้ผลิตสินค้า ผู้ให้บริการประเภทต่างๆ และโดยเฉพาะอย่างยิ่งสถาบันการเงินซึ่งมีความเสี่ยงภัยในระดับสูงโดยจะคุ้มครอง

ทั้งในส่วนความรับผิดต่อผู้เอาประกันภัย (First Party) หรือความรับผิดต่อบุคคลภายนอก (Third Party) ซึ่งเกิดขึ้นกับข้อมูลของลูกค้าสูญหาย หรือถูกโจรกรรมไป

สำหรับการระบาดของ "มัลแวร์เรียกค่าไถ่" กรมธรรม์ประกันภัยไซเบอร์ (Cyber Insurance Policy) จะคุ้มครองครอบคลุมความเสียหายทั้งหมดหรือไม่ ต้องพิจารณาว่าไวรัสดังกล่าวได้ทำให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ และการสื่อสารหรือถ่ายโอนข้อมูลทางอิเล็กทรอนิกส์มากน้อยเพียงใด อย่างไรก็ตามการทำประกันภัยไว้ย่อมเป็นการป้องกันความเสี่ยงภัยและได้รับความคุ้มครองในกรณีเกิดความเสียหายที่อาจเกิดขึ้นต่อระบบคอมพิวเตอร์ รวมถึงข้อมูลทางธุรกิจ และข้อมูลส่วนบุคคลต่างๆ ที่อยู่ในความครอบครองของตนได้

"ขอเรียนว่า สำนักงาน คปภ. คำนึงถึงความปลอดภัยของประชาชนในการทำธุรกรรมประกันภัยออนไลน์ เพื่อป้องกันมิให้ประชาชนได้รับผลกระทบต่อการจู่โจมทางไซเบอร์ ในกรณีมีการเสนอขายกรมธรรม์ประกันภัย และการชดใช้เงินตามสัญญาประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์ สำนักงาน คปภ.จึงได้กำหนดหลักเกณฑ์และวิธีการให้บริษัทหรือตัวแทน หรือนายหน้าประกันภัยหรือธนาคาร ที่ใช้วิธีการเสนอขายผ่านช่องทางดังกล่าวนี้ต้องปฏิบัติซึ่งนอกจากผู้ขายจะต้องมีนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเป็นส่วนตัวและข้อมูลส่วนบุคคลแล้ว ยังต้องจัดให้มีการตรวจรับรองระบบสารสนเทศจากผู้ตรวจสอบอิสระที่ได้รับใบอนุญาต หรือโดยหน่วยงานรับรองระบบสารสนเทศ (Certified Body) รวมถึงต้องขึ้นทะเบียนกับสำนักงาน คปภ. ก่อนดำเนินธุรกรรมด้วย เพื่อให้มั่นใจว่าวิธีการเสนอขายผ่านช่องทางอิเล็กทรอนิกส์จะมีมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอันจะเป็นการส่งเสริมการประกอบธุรกิจประกันภัยให้มีความน่าเชื่อถือ มีมาตรฐานเพียงพอในการคุ้มครองประชาชน และเป็นไปตาม พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม"

5. กสทช. กำชับผู้ให้บริการโทรศัพท์เคลื่อนที่ ผู้ให้บริการอินเทอร์เน็ต (ISP) และผู้ให้บริการวงจรสื่อสารระหว่างประเทศ (IIG) ทุกรายในประเทศ เข้มข้นการตรวจสอบระบบเครือข่ายและเตรียมการป้องกันมัลแวร์ WannaCry โจมตี

เมื่อวันที่ 15 พฤษภาคม 2560 **นายฐากร ตัณฑสิทธิ์** เลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) กล่าวว่า ...จากการตรวจสอบของสำนักงาน กสทช. ขณะนี้ยังไม่มีผู้ให้บริการโทรศัพท์เคลื่อนที่ ผู้ให้บริการอินเทอร์เน็ต (ISP) และผู้ให้บริการวงจรสื่อสารระหว่างประเทศ (IIG) ในประเทศไทยได้รับผลกระทบจากการโจมตีของมัลแวร์เหมือนในบางประเทศที่มัลแวร์นี้เข้าไปในระบบ ทำให้ผู้ให้บริการโทรคมนาคมไม่สามารถคิดค่าบริการและให้บริการได้ เพื่อเป็นการป้องกัน กสทช. ได้กำชับไปยังผู้ให้บริการทุกรายเข้มข้นการตรวจสอบระบบเครือข่ายสารสนเทศ และเตรียมการป้องกันการคุกคามจากมัลแวร์ WannaCry ไม่ให้เกิดความกระทบกระเทือนต่อระบบคอมพิวเตอร์ที่เกี่ยวกับการให้บริการ ทั้งการให้บริการ การคิดค่าโทรศัพท์ ค่าบริการ บริการคลาวด์เซอร์วิสต่างๆ ที่ให้บริการกับผู้ใช้งาน พร้อมทั้งให้ผู้ให้บริการทุกรายเตรียม Call Center เพื่อให้ข้อมูลการป้องกันการโจมตีจากมัลแวร์ WannaCry ให้กับผู้ใช้บริการด้วย *(ข้อมูลข่าวและที่มา: ปิยาพรรณ ยังเทียน และ ธนพิชฌน์ แก้วกา, สถานีวิทยุกระจายเสียงแห่งประเทศไทย/สำนักข่าว กรมประชาสัมพันธ์; goo.gl/KLX4s5)*

6. มหาวิทยาลัยเทคโนโลยีเทคโนโลยีสุรนารี (มทส.) พัฒนาโปรแกรมป้องกันการทำงานของ WannaCry เปิดให้ดาวน์โหลดใช้งานฟรี โดย ผู้ช่วยศาสตราจารย์ ดร.ชาญวิทย์ แก้วกสิ อาจารย์ประจำสาขาวิชาวิศวกรรมคอมพิวเตอร์ สำนักวิชาวิศวกรรมศาสตร์ มทส. และนักวิจัยประจำห้องปฏิบัติการ "ไอยราคลัสเตอร์" ได้พัฒนาซอฟต์แวร์ป้องกัน WannaCry ขึ้น เรียกว่า 'block_wannacry' เพื่อใช้งานในห้องปฏิบัติการฯ และเปิดให้บุคคลทั่วไปโหลดไปใช้งานได้ฟรีทางเฟซบุ๊กของห้องปฏิบัติการไอยราคลัสเตอร์ *(SUT Aiyara Cluster--www.facebook.com/SUTAiyaraCluster) ดูเพิ่มเติม web.sut.ac.th/2012/news/detail/1/news20170516*

การจัดการภัยคุกคามไซเบอร์ของประเทศไทยในอนาคต

นโยบาย แผน ยุทธศาสตร์ กฎหมาย และมาตราการจัดการภัยคุกคามไซเบอร์ของประเทศไทยในอนาคต ที่สำคัญมีดังนี้

1. ร่าง กรอบยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2560-2579) ได้กำหนดวิสัยทัศน์ *"ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจพอเพียง"* หรือเป็นคติพจน์ประจำชาติว่า *"มั่นคง มั่งคั่ง ยั่งยืน"* ทั้งนี้ วิสัยทัศน์ดังกล่าวจะต้องสนองตอบต่อผลประโยชน์แห่งชาติ อันได้แก่ การมีเอกราช อธิปไตย และบูรณภาพแห่งเขตอำนาจรัฐ การดำรงอยู่อย่างมั่นคง ยั่งยืนของสถาบันหลักของชาติ **การดำรงอยู่อย่างมั่นคงของชาติและประชาชนจากภัยคุกคามทุกรูปแบบ** ฯลฯ โดย**ยุทธศาสตร์ที่ 1 ด้านความมั่นคง** มีเป้าหมายทั้งในการสร้างเสถียรภาพภายในประเทศ และช่วยลดและป้องกันภัยคุกคามจากภายนอก ฯลฯ โดยมีกรอบแนวทางที่ต้องให้ความสำคัญ อาทิ การพัฒนาระบบ กลไก มาตรการและความร่วมมือระหว่างประเทศทุกระดับ และรักษาดุลยภาพความสัมพันธ์กับประเทศมหาอำนาจ เพื่อป้องกันและแก้ไขปัญหาความมั่นคงรูปแบบใหม่

2. แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่สิบสอง (พ.ศ. 2560-2564) ได้ระบุว่า "ประเทศไทยมีความเสี่ยงสูงจากปัญหาอาชญากรรมคอมพิวเตอร์ โดยเฉพาะการคุกคามที่ส่งผลกระทบทางเศรษฐกิจ ...และมีแนวโน้มในการสร้างความเสียหายต่อโครงสร้างพื้นฐานที่มีความสำคัญยิ่งยวด (Critical Information Infrastructure Breakdown) ซึ่งอาชญากรรมทางไซเบอร์ได้ปรับเปลี่ยนรูปแบบไปสู่การโจมตีระบบขององค์กรขนาดใหญ่ที่ส่งผลกระทบในวงกว้างและมีมูลค่าความเสียหายสูง และยังเกี่ยวพันกับอาชญากรรมทางเศรษฐกิจอื่น เช่น การคุกคามในระบบฐานข้อมูลของสถาบันการเงิน ประกอบกับการเพิ่มขึ้นของการใช้งานอุปกรณ์อิเล็กทรอนิกส์ต่างๆ ที่กำลังเข้าสู่ยุค Internet of Things (IoT) ซึ่งอุปกรณ์ต่างๆ ถูกเชื่อมโยงเข้าสู่โลกอินเทอร์เน็ต ทำให้สามารถสั่งการควบคุมใช้งานอุปกรณ์ต่างๆ ผ่านทางเครือข่ายอินเทอร์เน็ต ซึ่งสร้างความสะดวกรวดเร็วในการดำเนินธุรกรรมต่างๆ แต่ยังมีความเสี่ยงต่อการรักษาความปลอดภัยข้อมูลทั้งระดับองค์กร และบุคคล ประกอบกับการโจมตีทางไซเบอร์ทั่วโลกมีจำนวนเพิ่มขึ้นอย่างรวดเร็ว และมีความเสี่ยงต่อการโจมตีระบบการให้บริการสาธารณะในเมืองใหญ่ ซึ่งประเทศไทยเริ่มตกเป้าหมายในการโจมตีทางไซเบอร์บ่อยครั้งขึ้น ...การถูกโจมตีของโปรแกรมที่ไม่พึงประสงค์ (Threat Exposure Rate: TER) ทำให้การบริหารจัดการภาครัฐ ภาคธุรกิจ และภาคประชาชนของไทยที่จะก้าวไปสู่การบริหารจัดการในรูปแบบดิจิทัล มีความเสี่ยงสูงในด้านความมั่นคงของระบบและอาชญากรรมที่มาพร้อมกับความก้าวหน้าของเทคโนโลยีดิจิทัล"

ยุทธศาสตร์ที่ 5 การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน ของแผนพัฒนาฯ ฉบับที่ 12 ได้กำหนดเป้าหมายที่ 5 ประเทศไทยมีความพร้อมต่อการรับมือภัยคุกคามทั้งภัยคุกคามทางทหารและภัยคุกคามอื่นๆ ตัวชี้วัด 5.3 อันดับความเสี่ยงจากการโจมตีด้านไซเบอร์ต่ำกว่าอันดับที่ 10 ของโลก (ดัชนีความปลอดภัยไซเบอร์ของโลกของ International Telecommunication Union: ITU) โดยมีแนวทางการพัฒนาที่สำคัญดังนี้

(1) ดำเนินบทบาทเชิงรุก และใช้กรอบความร่วมมือระหว่างประเทศทั้งระดับภูมิภาคและพหุภาคี ...ตลอดจนเสริมสร้างขีดความสามารถแลกเปลี่ยนและเรียนรู้แนวปฏิบัติที่เป็นเลิศและร่วมมือในการรับมือกับภัยคุกคามด้านความมั่นคงระหว่างประเทศ อาทิ ปัญหายาเสพติด การก่อการร้าย ... **ความมั่นคงด้านไซเบอร์** ฯลฯ

(2) พัฒนาระบบการเก็บรักษาข้อมูลส่วนบุคคลด้านไซเบอร์ให้มีความมั่นคงปลอดภัยและกำกับดูแลระบบการส่งข้อมูลส่วนบุคคลข้ามแดนไปต่างประเทศให้เป็นไปตามมาตรฐานสากล

แผนงานรองรับ ด้านความมั่นคงปลอดภัยไซเบอร์ ได้แก่ (1) กรอบนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2555–2559 (2) แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงกลาโหม ฉบับที่ 3 พ.ศ. 2557–2561 (3) ยุทธศาสตร์การวิจัยและแผนพัฒนาเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ฉบับที่ 1 พ.ศ. 2556-2560

แผนงานและโครงการสำคัญ ด้านการป้องกันภัยและแก้ไขปัญหาภัยคุกคามทางเทคโนโลยีสารสนเทศและไซเบอร์ ได้ระบุสาระสำคัญว่า ภัยคุกคามทางไซเบอร์ได้เพิ่มระดับความรุนแรงและมีความซับซ้อนใน การโจมตีมากขึ้น ความเสียหายที่เกิดจากการอาชญากรรมและการโจมตีทางไซเบอร์จะมีผลอย่างร้ายแรง ซึ่งต้องให้ความสำคัญและมีมาตรการป้องกันภัยคุกคามทางไซเบอร์ให้สอดรับกับการเปลี่ยนแปลงทางสภาพแวดล้อม โดยเฉพาะการกำหนดกฎหมายและมาตรการที่เกี่ยวกับความปลอดภัยบนโลกไซเบอร์ให้รัดกุมมากยิ่งขึ้น ตั้งแต่ระดับชาติถึงระดับบุคคล โดยมีหน่วยงานดำเนินการหลัก คือ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงกลาโหม และสำนักงานตำรวจแห่งชาติ กรอบระยะเวลาดำเนินการ 5 ปี (พ.ศ. 2560-2564) (ดูเพิ่มเติม goo.gl/rjE9Dn ,หน้า 121-128)

3. นโยบายความมั่นคงแห่งชาติ พ.ศ. 2558–2564 นโยบายที่ 10 เสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ ได้ระบุถึงแนวนโยบายไว้ดังนี้

(1) ปกป้อง ป้องกัน ภัยคุกคามด้านไซเบอร์ สงครามไซเบอร์ และเสริมสร้างความ ปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยการบูรณาการการจัดการความมั่นคงทางไซเบอร์ระหว่างหน่วยงานภาครัฐ การประสานความร่วมมือและเสริมสร้างเครือข่ายกับภาคเอกชน ภาควิชาการ บุคลากร องค์กร และผู้เชี่ยวชาญทางด้านการรักษาความมั่นคงทางไซเบอร์ การเสริมสร้างความร่วมมือระหว่างประเทศ การเฝ้าระวังและการพัฒนาระบบป้องกัน การโจมตีระบบสารสนเทศ การพัฒนาความพร้อมต่อสงครามไซเบอร์ การปกป้องโครงสร้างพื้นฐานสำคัญด้านสารสนเทศของประเทศ การกู้คืนข้อมูล ระบบ/เครือข่าย และการพัฒนามาตรฐานด้านความปลอดภัยในทุกด้าน

(2) พัฒนาการบังคับใช้กฎหมาย โดยการพัฒนาระเบียบและกฎหมายเพื่อความมั่นคง ปลอดภัยไซเบอร์และการพัฒนาเทคโนโลยีสำหรับงานสืบสวนและป้องกันอาชญากรรมไซเบอร์ให้สามารถลดภัยคุกคามหรืออันตรายที่ส่งผลกระทบกับบุคคล ข้อมูลและระบบเทคโนโลยีสารสนเทศ โดยเฉพาะที่อยู่ในรูปของการทำธุรกรรมทางอิเล็กทรอนิกส์ การละเมิดทรัพย์สินทางปัญญา การโจรกรรมข้อมูลสารสนเทศ การละเมิดสิทธิเสรีภาพของบุคคล การกรรโชกข้อมูลสารสนเทศ การกระทำผิดตลอดจนการก่อวินาศกรรมหรือทำลายระบบสารสนเทศ รวมถึงการสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์

(3) พัฒนาศักยภาพทางด้านเทคโนโลยีสารสนเทศ โดยส่งเสริมการวิจัย พัฒนา และจดสิทธิบัตรเทคโนโลยีสารสนเทศที่ผลิตโดยคนไทย การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์ การบูรณาการเชื่อมโยงระบบฐานข้อมูลภาครัฐ การพัฒนาระบบรัฐบาลอิเล็กทรอนิกส์แบบบูรณาการ รวมถึงการใช้ระบบรัฐบาลอิเล็กทรอนิกส์ เครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) ระบบคลาวด์ภาครัฐ (G-Cloud) ตลอดจนการพัฒนาบุคลากรภาครัฐ องค์กรทุกภาคส่วนที่เกี่ยวข้องให้มีความรู้ ความชำนาญทางด้านระบบเทคโนโลยีสารสนเทศและการรักษาความปลอดภัยทางไซเบอร์ เพื่อให้บุคลากรภาครัฐและองค์กรทุกภาคส่วนที่เกี่ยวข้องมีข้อมูลข่าวสารและความรู้ทางด้านเทคโนโลยีที่ทันสมัย และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงการพัฒนาบุคลากรทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในเชิงปริมาณและคุณภาพอย่างต่อเนื่อง *(ดูเพิ่มเติม goo.gl/15FMDw , หน้า 17)*

4. กรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร ระยะ พ.ศ. 2554-2563 (ICT2020) ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐาน ICT ที่เป็นอินเทอร์เน็ตความเร็วสูง หรือการสื่อสารรูปแบบอื่นที่เป็น Broadband ให้มีความทันสมัย มีการกระจาย อย่างทั่วถึง และมีความมั่นคงปลอดภัย สามารถรองรับความต้องการของภาคส่วนต่างๆ ได้ *(ดูเพิ่มเติม goo.gl/yLTbOS,หน้า 13-19)* โดยมีเป้าหมายภายในปี พ.ศ. 2563 บริการด้านโครงสร้างพื้นฐานสารสนเทศและการสื่อสารของประเทศไทยจะเป็นสาธารณูปโภคขั้นพื้นฐาน ที่ประชาชนทั่วไปสามารถเข้าถึงได้ มีคุณภาพ และความมั่นคงปลอดภัยเทียบเท่ามาตรฐานสากล

มีกลยุทธ์และมาตรการที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ คือ **"ประกันความมั่นคงปลอดภัยของโครงข่าย เพื่อสร้างความเชื่อมั่นให้กับทั้งภาคธุรกิจและประชาชนในการสื่อสาร และการทำธุรกรรมออนไลน์"** ดังนี้

(1) สร้างความตระหนักและให้ความรู้แก่ผู้บริหารเทคโนโลยีสารสนเทศ (CIO) ของหน่วยงานทั้งภาครัฐและภาคเอกชน โดยเฉพาะหน่วยงานที่รับผิดชอบโครงสร้างพื้นฐานที่สำคัญของประเทศ (Critical Infrastructure) ถึงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงความสำคัญในการดำเนินการตามมาตรฐานความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้จัดทำขึ้น รวมถึงให้ความรู้แก่ประชาชนเกี่ยวกับผลกระทบที่อาจพึงมี หากระบบสารสนเทศหรือโครงข่ายมีความเสี่ยงต่อความมั่นคงปลอดภัย โดยสำหรับหน่วยงานของรัฐ ควรกำหนดให้การดำเนินการตามมาตรฐานดังกล่าวเป็นหนึ่งในตัวชี้วัดผลการดำเนินงานของ CIO เพื่อให้เกิดการปฏิบัติตามมาตรฐานโดยเคร่งครัด ทั้งนี้ เพื่อประกันความมั่นคงปลอดภัยของการสื่อสารและการทำธุรกรรมออนไลน์

(2) จัดตั้ง National Cyber Security Agency เพื่อทำงานประสานกับสภาความมั่นคงแห่งชาติ โดยมีหน้าที่รับผิดชอบดำเนินการในส่วนที่เกี่ยวข้องกับความมั่นคงปลอดภัยในโลกไซเบอร์ (Cyber Security) การให้ความรู้ความเข้าใจ คำปรึกษา และประสานงานกับผู้ที่รับผิดชอบงานด้านความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงานอื่นๆ การดำเนินการเรื่องการตรวจสอบและประเมิน (Compliance and Monitoring) การประเมินความเสี่ยงของระบบสารสนเทศ (ICT Risk Assessment) ในระดับประเทศ โดยมีกลไกประสานเชื่อมโยงกับคณะกรรมการนโยบายระดับชาติที่เกี่ยวข้อง ฯลฯ

(3) สนับสนุนการวิจัยพัฒนา และเพิ่มจำนวนผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยของระบบสารสนเทศและโครงข่าย (Network Security) ของประเทศ รวมถึงการจัดทำ ทบทวน และปรับปรุง แผนแม่บทด้านความมั่นคงปลอดภัยของระบบสารสนเทศและโครงข่าย (National Information Security Roadmap) อย่างต่อเนื่อง

5. แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ซึ่งได้รับความเห็นชอบจากคณะรัฐมนตรี เมื่อวันที่ 5 เมษายน 2559 กล่าวถึงการจัดการภัยคุกคามทางไซเบอร์ไว้ใน **"ยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล"** ซึ่งมุ่งเน้นการสร้างความมั่นคงปลอดภัย และความเชื่อมั่นในการทำธุรกรรมด้วยเทคโนโลยีดิจิทัลให้กับผู้ประกอบการ ผู้ทำงาน และผู้ใช้บริการ ซึ่งถือได้ว่าเป็นปัจจัยพื้นฐานที่ช่วยขับเคลื่อนประเทศสู่ยุคเศรษฐกิจดิจิทัล และเป็นบทบาทหน้าที่หลักของภาครัฐในการอำนวยความสะดวกให้กับทุกภาคส่วน โดยภารกิจสำคัญยิ่งยวดของยุทธศาสตร์นี้จะครอบคลุมเรื่องมาตรฐาน (Standard) การคุ้มครองความเป็นส่วนตัวและข้อมูลส่วนบุคคล (Privacy) **การรักษาความมั่นคงปลอดภัย (Cyber Security)**

แผนงานที่สำคัญในส่วนที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ คือ การกำหนดมาตรการการเฝ้าระวังและรับมือภัยคุกคามไซเบอร์ที่เหมาะสมและสอดคล้องตามมาตรฐานสากล โดยเฉพาะการปกป้องโครงสร้างพื้นฐานที่มีความจำเป็นอย่างยิ่งยวด (Critical Infrastructure) เช่น โครงสร้างพื้นฐานทางไฟฟ้า โครงสร้างพื้นฐานทางการเงิน เพื่อให้มีความมั่นคงปลอดภัยเพียงพอต่อการค้าและการลงทุน การสร้างเครือข่ายแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ พร้อมกำหนดหน่วยงานรับแจ้งเหตุ และสร้างกลไกการบังคับใช้กฎหมายที่มีประสิทธิภาพในการป้องกันปราบปรามการกระทำความผิดที่มีผลต่อระบบความมั่นคงปลอดภัยดิจิทัล ทั้งนี้ การส่งเสริมให้เกิดความตระหนักและรู้เท่าทันภัยคุกคามทางไซเบอร์เป็นสิ่งสำคัญที่ต้องดำเนินการอย่างต่อเนื่อง *(ดูเพิ่มเติม goo.gl/uVsi6e ,หน้า 53-56)*

6. กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

คณะรัฐมนตรีได้อนุมัติหลักการของร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. .... เมื่อวันที่ 6 มกราคม 2558 และส่งให้สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณา โดยมีสาระสำคัญเพื่อให้ประเทศไทยสามารถปกป้อง ป้องกันหรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม ซึ่งกระทบต่อความมั่นคงของชาติในมิติต่างๆ อันครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจได้อย่างเหมาะสม มีการดำเนินการที่รวดเร็ว และมีความเป็นเอกภาพ สมควรกำหนดให้มี**คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ** (กปช.) และให้ใช้ชื่อภาษาอังกฤษว่า National Cybersecurity Committee (NCSC) ขึ้นเพื่อกำหนดมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ให้เป็นไปอย่างมีประสิทธิภาพ และเกิดผลสัมฤทธิ์

ร่างกฎหมายดังกล่าว กำหนดให้มีการจัดตั้ง **"สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ"** ขึ้นเป็นหน่วยงานของรัฐที่มีฐานะเป็นนิติบุคคล ไม่เป็นส่วนราชการและรัฐวิสาหกิจ มีสำนักงานใหญ่ในกรุงเทพมหานครหรือจังหวัดใกล้เคียง

สำนักงานฯ มีอำนาจและหน้าที่ อาทิ

(1) ตอบสนองและรับมือกับภัยคุกคามไซเบอร์ เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัย หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ที่ส่งผลกระทบ หรืออาจก่อให้เกิดผลกระทบ ความสูญเสีย หรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรง โดยวางมาตรการ เกี่ยวกับการดำเนินการที่คำนึงถึงชั้นความลับและการเข้าถึงข้อมูลที่มีชั้นความลับ

(2) ประสานความร่วมมือทางปฏิบัติในการดำเนินการกับหน่วยงานของรัฐ หรือหน่วยงาน ภาคเอกชน เพื่อให้การยับยั้งปัญหาภัยคุกคามไซเบอร์ ได้รับการแก้ไขอย่างมีประสิทธิภาพและรวดเร็ว

(3) ประสานงานกับหน่วยงานของรัฐและเอกชน เพื่อรวบรวมข้อมูลเกี่ยวกับภัยคุกคาม การป้องกัน การรับมือความเสี่ยงจากสถานการณ์ด้านภัยคุกคามทางไซเบอร์และข้อมูลอื่นใดอันเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อวิเคราะห์เสนอต่อ กปช.

(4) บริหารแผนงานรวม ประสานการบริหารและการปฏิบัติการตามแผนปฏิบัติการหรือตาม คำสั่งการของ กปช.

(5) ติดตามและเร่งรัดการปฏิบัติงานของหน่วยงานของรัฐที่เกี่ยวข้องกับการรักษาความ มั่นคงปลอดภัยไซเบอร์ และรายงานต่อ กปช.

(6) เป็นศูนย์กลางเครือข่ายข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ทั้งภายใน และภายนอกประเทศ

(7) ติดตาม เฝ้าระวัง รวมทั้งสร้างความตระหนักเกี่ยวกับภัยคุกคามทางระบบสารสนเทศ รวมทั้งจัดตั้งและบริหารจัดการศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT)

(8) ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำ ข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(9) ส่งเสริม สนับสนุน และดำเนินการเผยแพร่ความรู้และการให้บริการเกี่ยวกับการรักษา ความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะเกี่ยวกับมาตรฐานความมั่นคงปลอดภัย หรือกรณีอื่นใดเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(10) รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามระเบียบนี้ รวมทั้งปัญหา และอุปสรรคต่อ กปช.

ขณะนี้ (มิถุนายน 2560) ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... อยู่ระหว่างการตรวจพิจารณาของสำนักงานคณะกรรมการกฤษฎีกา ซึ่งเมื่อผ่านการตรวจพิจารณาจากสำนักงานคณะกรรมการกฤษฎีกาแล้ว จะได้เสนอต่อคณะรัฐมนตรี เพื่อพิจารณาอนุมัติร่างฯ และส่งไปยังสภานิติบัญญัติแห่งชาติพิจารณาต่อไป (ดูเพิ่มเติม ictlawcenter.etda.or.th/de_laws)

7. รายงานของคณะกรรมาธิการขับเคลื่อนการปฏิรูปประเทศด้านการสื่อสารมวลชน สภาขับเคลื่อนการปฏิรูปประเทศ (สปท.) เรื่อง "การปกป้องคุ้มครองและรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญ ด้านสารสนเทศของประเทศ"

ที่ประชุมสภาขับเคลื่อนการปฏิรูปประเทศ (สปท.) ครั้งที่ 17/2560 เมื่อวันที่ 23 พฤษภาคม 2560 ได้เห็นชอบรายงานของคณะกรรมาธิการขับเคลื่อนการปฏิรูปประเทศด้านการสื่อสารมวลชน เรื่อง "การปกป้องคุ้มครองและรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญ ด้านสารสนเทศของประเทศ" เพื่อส่งรายงานไปยังคณะรัฐมนตรี เพื่อพิจารณาดำเนินการต่อไป *(ดูเพิ่มเติม goo.gl/iLUu7P)*

รายงานดังกล่าวมีข้อเสนอแนะที่สำคัญเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยระบุว่า "...ในกรณีของประเทศไทยกล่าวได้ว่าถึงเวลาที่ต้องดำเนินการทั้งในด้านนโยบายและมาตรการที่เป็นรูปธรรมและกรอบแนวปฏิบัติที่ดีในระดับสากล เพื่อป้องกันความเสียหายและผลกระทบที่อาจเกิดขึ้นดังต่อไปนี้

1) ให้ดำเนินการกระตุ้นเตือนองค์กรทั้งภาครัฐและภาคเอกชนให้คำนึงถึงการรักษาความมั่นคงปลอดภัยของเครือข่ายไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญ (ภายใต้ความรับผิดชอบของคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เมื่อพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ มีผลบังคับใช้ ในห้วงเวลานี้ให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) ดำเนินการไปพลางก่อน)

2) สร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และมีเป้าหมายสูงสุดที่ต้องการทำให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นวัฒนธรรม การหลอมรวมให้อยู่ในแก่นของเทคโนโลยีสารสนเทศและการสื่อสาร โดยพิจารณานำแนวปฏิบัติที่เป็นมาตรฐานในระดับสากลทั้งของ ISO 27001 และ ITU มาเป็นแนวทางในการดำเนินการที่สำคัญ ได้แก่ การพัฒนาด้านกฎหมาย ด้านเทคนิค ด้านองค์กร ด้านความสามารถ และด้านการดำเนินความพร้อม

3) เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญดำเนินการได้อย่างมีประสิทธิภาพทั่วประเทศ จึงสมควรให้มีการดำเนินการที่ครอบคลุมหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทั้งของภาครัฐและเอกชน รวมถึงมีการรวมกลุ่มร่วมกันดำเนินงานในระดับภาคส่วน (Sectors) เช่น ภาคการสื่อสารโทรคมนาคม ภาคการขนส่ง ภาคพลังงาน เป็นต้น

โดยมีกระบวนการดำเนินงานที่เป็นสาระสำคัญดังต่อไปนี้

(1) สนับสนุนให้มีการจัดตั้งหน่วยงานประกันด้านความมั่นคงปลอดภัย (Security Assurance) ในหน่วยงานแต่ละกลุ่ม

(2) เร่งรัดให้มีการศึกษาและจัดทำรายงานวิเคราะห์ความเสี่ยงเรื่องความมั่นคงปลอดภัยของทั้งระบบฮาร์ดแวร์และซอฟต์แวร์ที่ใช้งานและผลกระทบที่อาจเกิดขึ้นจากการโจมตีในหน่วยงานแต่ละกลุ่ม โดยกำหนดมาตรการป้องกัน การบรรเทาเมื่อเกิดปัญหา แผนรับมือฉุกเฉินและการกู้คืนระบบ

(3) เร่งรัดให้มีการวางมาตรการที่เป็นรูปธรรมในการป้องกันปัญหาและผลกระทบที่เกิดขึ้นจากการโจมตีทางเครือข่าย

(4) ส่งเสริมและจัดหาแหล่งทุนเพื่อสนับสนุนการทดสอบและประเมินความเสียหายโดยการจำลองสถานการณ์เมื่อเกิดปัญหาความมั่นคงปลอดภัย

(5) จัดให้มีและสนับสนุนแผนการฝึกอบรมการประกันความมั่นคงปลอดภัยโครงสร้างพื้นฐาน

(6) จัดให้มีและสนับสนุนการสร้างเครือข่ายความร่วมมือเพื่อแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัย

(7) ส่งเสริมให้ทั้งภาครัฐและภาคเอกชนพัฒนาและจัดทำกระบวนการเกี่ยวกับการรายงานปัญหาความปลอดภัยและการนำไปใช้อย่างเป็นรูปธรรมส่งเสริมงานวิจัยและพัฒนาเรื่องการประกันคุณภาพความมั่นคงปลอดภัยของเครือข่าย

(ให้อยู่ในความรับผิดชอบของสำนักงานคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เมื่อพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ มีผลบังคับใช้ ในห้วงเวลานี้ให้ สพธอ. ดำเนินการไปพลางก่อน)

4) รัฐบาลผลักดันร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ..... รวมทั้งการผ่านกฎหมายอื่นๆ ที่เกี่ยวข้อง เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล เป็นต้น ให้มีผลบังคับใช้โดยเร็ว

บทส่งท้าย

การโจมตีของแรนซัมแวร์หรือมัลแวร์เรียกค่าไถ่ "WannaCry" เมื่อเดือนพฤษภาคม 2560 ได้ส่งผลให้ภาครัฐไทยเกิดความตระหนักในเรื่องความปลอดภัยไซเบอร์อย่างจริงจังขึ้นมาอีกครั้งหนึ่ง รวมทั้งทำให้เกิดความใส่ใจต่อความมั่นคงปลอดภัยสารสนเทศในภาคธุรกิจเอกชน และภาคประชาชนในวงกว้างอย่างที่ไม่เคยปรากฏมาก่อน ซึ่งก็ถือเป็นโอกาสที่เกิดขึ้นท่ามกลางวิกฤติ นั่นคือ ทำให้ทุกภาคส่วนเกิดความตระหนักและให้ความสำคัญต่อการรักษาความปลอดภัยไซเบอร์อย่างจริงจังมากยิ่งขึ้น โดยเฉพาะในกลุ่มโครงสร้างพื้นฐานสำคัญของประเทศ *(กลุ่มสารสนเทศและโทรคมนาคม, กลุ่มธนาคารและสถาบันการเงิน, กลุ่มพลังงาน, กลุ่มการขนส่งทางกายภาพ, กลุ่มบริการที่จำเป็นต่อชีวิตประจำวัน)* รวมทั้งการที่ คปภ. มีนโยบายส่งเสริมให้บริษัทประกันภัยพัฒนาผลิตภัณฑ์ประกันภัยที่จะช่วยรองรับความเสี่ยงจากภัยคุกคามทางไซเบอร์ในรูปแบบ "การประกันภัยไซเบอร์ (Cyber Insurance)"

เมื่อพิจารณาการรับมือการโจมตีของแรนซัมแวร์ "WannaCry" ของภาครัฐไทย พบว่า สามารถดำเนินการได้ในระดับดีมาก ทำให้ไม่เกิดความเสียหายในวงกว้าง ซึ่งความสำเร็จส่วนหนึ่งก็มาจากการที่สื่อมวลชนและเครือข่ายสังคมออนไลน์ได้ช่วยกันกระจายข่าวแนวทางการป้องกันแรนซัมแวร์ ในขณะที่มหาวิทยาลัยเทคโนโลยีเทคโนโลยีสุรนารี (มทส.) โดย ผู้ช่วยศาสตราจารย์ ดร.ชาญวิทย์ แก้วกสิ อาจารย์ประจำสาขาวิชาวิศวกรรมคอมพิวเตอร์ สำนักวิชาวิศวกรรมศาสตร์ ได้พัฒนาโปรแกรมป้องกันการทำงานของ WannaCry ภายใต้ชื่อ 'block_wannacry' เปิดให้ดาวน์โหลดไปใช้งานฟรี

สำหรับนโยบาย แผน ยุทธศาสตร์ กฎหมาย และมาตราการรับมือแรนซัมแวร์ของประเทศไทย เพื่อเป็นหลักประกันความมั่นคงปลอดภัยของระบบเศรษฐกิจและสังคมดิจิทัลของประเทศไทยในอนาคตตามนโยบาย Thailand 4.0 นั้น พบว่า มีการกำหนดไว้อย่างชัดเจนในแผนระดับต่างๆ โดยเฉพาะอย่างยิ่งการที่ภาครัฐพยายามผลักดันให้มีพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งหากกฎหมายฉบับนี้ประกาศใช้ ก็จะทำให้มี "คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSC)" และ "สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ" ขึ้นมาทำหน้าที่ตอบสนองและรับมือกับภัยคุกคามไซเบอร์ในระดับชาติ อย่างเป็นทางการและเป็นระบบต่อไป

■ ไพโรจน์ ไววานิชกิจ

ล้อมคอกก่อนวัวหาย จากภัยของ Ransomware

พัฒนาการของ Ransomware รูปแบบการจู่โจมและ Ransomware จำนวนหนึ่งที่แพลงฤทธิ์อยู่บนโลกอินเทอร์เน็ต และปิดท้ายด้วยคำแนะนำในการใช้งานเครื่องคอมพิวเตอร์ที่จะช่วยลดความเสี่ยงในการถูกจู่โจมของ Ransomware

เรื่องของ Ransomware เป็นหนึ่งในภัยคุกคามทางคอมพิวเตอร์ที่ผู้คนจำนวนมากรับรู้ มีหน่วยงานทั้งภาครัฐและภาคธุรกิจที่ให้ความสำคัญกับการพัฒนาทั้งซอฟต์แวร์และกลไกการทำงานเพื่อป้องกันภัยคุกคามประเภทนี้ เฉกเช่นเดียวกับภัยคุกคามประเภทอื่นๆ แต่เหตุการณ์การจู่โจมของ Ransomware ชื่อดังอย่าง WannaCry ซึ่งแผลงฤทธิ์ถล่มโลกอินเทอร์เน็ตไปทั่วโลกอย่างร้ายแรงที่สุดในประวัติศาสตร์ นับตั้งแต่วันที่ 12 พฤษภาคม พ.ศ. 2560 ที่ผ่านมา โดยโจมตีผู้ใช้งานคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Windows ผ่านทางช่องโหว่ของระบบปฏิบัติการที่ผู้ใช้งานจำนวนมากทั่วโลกดังกล่าว จนกลายเป็นความโกลาหลและมีผู้เสียหายกับข้อมูลบนเครื่องคอมพิวเตอร์ของตนทุกมุมเมือง มีผลทำให้สังคมออนไลน์ให้ความสำคัญกับการรักษาปลอดภัยจากภัยอย่าง Ransomware และภัยอื่นๆ รวมถึงการตั้งคำถามกับระบบรักษาความปลอดภัยของหน่วยงานที่ตนทำงาน รวมถึงการปัดฝุ่นถึงระบบซอฟต์แวร์ป้องกันความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนตนครั้งใหญ่ อันที่จริงแล้ว Ransomware เป็นภัยคุกคามบนโลกอินเทอร์เน็ตที่ทวีความรุนแรงและมีรูปแบบการโจมตีที่หลากหลายมากขึ้นนับตั้งแต่ พ.ศ. 2558 รูปแบบการสร้างความเดือดร้อนของ Ransomware อันเป็นที่รับทราบกันก็คือการลักลอกเข้ารหัสไฟล์ข้อมูลของผู้คน ซึ่งต้องแลกกับการโอนเงินไปให้กับอาชญากรเพื่อขอรหัสปลดล็อค สิ่งที่น่าเป็นห่วงก็คือผู้ใช้งานคอมพิวเตอร์จำนวนมากทั่วโลก ก็ไม่ได้มีนิสัยที่จะทำสำรอง (Backup) ของตนเองสักเท่าไร จึงเท่ากับว่ามีเหยื่อทางธุรกิจของอาชญากรผู้สร้าง Ransomware อยู่ทั่วโลก

บทความเรื่องนี้จะกล่าวถึงเรื่องของและพัฒนาการของ Ransomware รูปแบบการจู่โจมและ Ransomware จำนวนหนึ่งที่แพลงฤทธิ์อยู่บนโลกอินเทอร์เน็ต และปิดท้ายด้วยคำแนะนำในการใช้งานเครื่องคอมพิวเตอร์ที่จะช่วยลดความเสี่ยงในการถูกจู่โจมของ Ransomware

โลกมืดของ Ransomware

อันที่จริงแล้ว Ransomware ก็คือ Malware ประเภทหนึ่งที่ได้รับการออกแบบจากบรรดาอาชญากรโปรแกรมเมอร์ ให้ทำหน้าที่ล็อคการเข้าถึงไฟล์ของผู้ใช้คอมพิวเตอร์ที่โชคร้ายถูก Ransomware บุกรุกผ่านระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ของตน ซึ่งจุดประสงค์ของอาชญากรเหล่านี้ก็คือการเรียกเงินค่าไถ่จากเหยื่อของตนแลกกับการปลดล็อคการเข้าถึงไฟล์ข้อมูลเหล่านั้น ทั้งนี้สามารถจำแนกประเภทการโจมตีของ Ransomware ออกได้เป็น 2 ประเภท ดังนี้

1. การเข้ารหัสข้อมูล (Encryptors) เป็นการออกแบบ Ransomware ให้ทำการเข้ารหัสไฟล์บนเครื่องคอมพิวเตอร์ที่บริหารจัดการระบบทั้งหมด โดยการฝังอัลกอริธึมในการเข้ารหัสชั้นสูงไว้ใน Ransomware โดยมีเงื่อนไขให้ผู้เสียหายต้องทำการโอนเงิน เพื่อแลกกับกุญแจอิเล็กทรอนิกส์ที่สามารถใช้ปลดรหัสไฟล์ทั้งหมดได้ ตัวอย่างของ Ransomware ที่มีรูปแบบการโจมตีในลักษณะนี้ก็เช่น CryptoLocker, Locky, CrytpoWall ฯลฯ

2. การล็อคไฟล์ (Lokcers) เป็นการล็อคไม่ให้ผู้เสียหายเข้าถึงระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ได้ ผลก็คือผู้ใช้งานดังกล่าวจะไม่สามารถเข้าถึงระบบ Desktop ตลอดจนถึงไฟล์ และแอปพลิเคชั่นต่างๆ บนเครื่องคอมพิวเตอร์ได้ ซึ่งในกรณีนี้อาชญากรไม่ได้ทำการเข้ารหัสไฟล์แต่อย่างไร ทั้งนี้ก็ยังเป็นการกรรโชคทรัพย์ของผู้เสียหายโดยให้โอนเงินตามที่เรียนร้อง เพื่อแลกกับการปลดล็อคการเข้าถึงเครื่องคอมพิวเตอร์ ตัวอย่างของ Ransomware ที่มีพฤติกรรมในลักษณะนี้ ก็เช่น police-themed ransomware หรือ WinLocker นอกจากนั้น Ransomware บางตัวในกลุ่มนี้ยังได้รับการออกแบบให้ไปขัดขวางการทำงานของ Master Boot Record (MBR) ซึ่งเป็นพื้นที่บนฮาร์ดดิสค์ของเครื่องคอมพิวเตอร์ ที่ได้รับการกำหนดให้เก็บข้อมูลที่จำเป็นสำหรับใช้ในการบูตเครื่อง เครื่องคอมพิวเตอร์ที่ถูกโจมตีจาก Ransomware ประเภทนี้จะแสดงข้อความเตือนที่อาชญากรกำหนดไว้บนหน้าจอ หลังจากที่มีการบูตเครื่องไปถึงขั้นหนึ่ง ตัวอย่างเช่นบรรดา Ransomware ในตระกูล Satana และ Petya

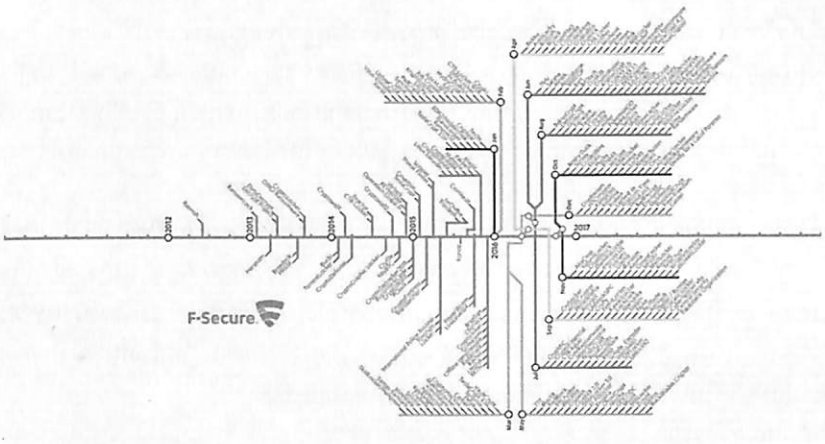
Ransomware ประเภทเข้ารหัสข้อมูล นับเป็นประเภทของภัยคุกคามที่มีการระบาดแพร่หลาย และได้รับการจัดประเภทให้เป็นภัยคุกคามบนโลกอินเทอร์เน็ตที่มีความอันตรายที่สุดในโลกปัจจุบัน สิ่งที่สำคัญที่จะช่วยให้เราแยกแยะได้ว่าภัยคุกคามที่เกิดขึ้นบนเครื่องคอมพิวเตอร์เป็น Ransomware มิใช่ Malware มีแสดงดังนี้

- ผู้ใช้งานคอมพิวเตอร์ไม่สามารถถอดรหัสไฟล์ต่างๆ บนเครื่องคอมพิวเตอร์ได้เลย
- Ransomware สามารถเข้ารหัสไฟล์ทุกประเภทบนเครื่องคอมพิวเตอร์ ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ไฟล์เสียง หรือไฟล์อื่นใดก็ตาม
- Ransomware อาจมีการแก้ไขชื่อไฟล์ สำเนาไฟล์ขึ้นใหม่โดยใช้นามสกุลอื่น ทำให้ยากต่อการตรวจสอบและพยายามแก้ปัญหาด้วยตนเอง
- เมื่อสามารถเจาะช่วงโหว่ของระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ได้แล้ว Ransomware จะทำการแสดงทั้งรูปภาพหรือข้อความต่างๆ เพื่อแจ้งให้ผู้ใช้งานทราบว่าบัดนี้ข้อมูลบนเครื่องคอมพิวเตอร์ถูกเข้ารหัสแล้ว พร้อมกับเรียกร้องให้จ่ายเงินค่าไถ่ ซึ่งรูปแบบการจ่ายเงินที่อาชญากรเรียนร้องจะเป็น Bitcoins เพื่อให้ยากต่อการตรวจสอบและติดตามเส้นทางการลำเลียงเงินของนักสืบไซเบอร์หรือองค์กรทางการกฎหมาย
- รูปแบบการจู่โจมของ Ransomware โดยทั่วไปมักมีการตั้งเงื่อนไขเวลาไว้ด้วย เช่น หากไม่จ่ายเงินค่าไถ่ภายในเวลาที่กำหนดก็จะมีการยกระดับการเข้ารหัส หรือมิฉะนั้นก็จะทำลายข้อมูลบนเครื่องคอมพิวเตอร์ของเหยื่อไปตลอดกาล
- สิ่งที่น่ากลัวก็คือ ในกรณีของเครือข่ายคอมพิวเตอร์ที่เชื่อมต่อถึงกันในองค์กร หรือชุมชนใดๆ หากมีคอมพิวเตอร์เครื่องใดติด Ransomware แล้วก็จะมีผลให้เกิดการแพร่ระบาดไปยังคอมพิวเตอร์เครื่องอื่นๆ อย่างรวดเร็ว เป็นการขยายผล

ตัวอย่างของพฤติกรรมการโจมตีจาก Ransomware ข้างต้นเป็นเพียงส่วนหนึ่งของเหตุการณ์ที่เกิดขึ้นจริงเท่านั้น นับวันอาชญากรคอมพิวเตอร์ที่พัฒนาซอฟต์แวร์ Ransomware ก็จะยิ่งเพิ่มรูปแบบและพฤติกรรมการโจมตีมากขึ้นเรื่อยๆ

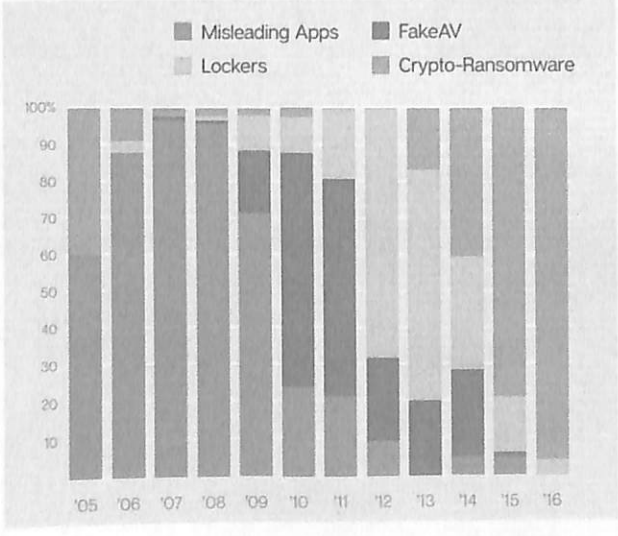
ประวัติศาสตร์ของ Ransomwar

ประวัติที่สามารถสืบค้นได้บนโลกอินเทอร์เน็ต พบว่ามี Ransomware ตัวแรกของโลกซึ่งมีชื่อว่า AIDS Trojan ปรากฏขึ้นในปี พ.ศ. 2532 หรือเมื่อ 28 ปีที่แล้ว โดย Ransomware นี้มีการแพร่ระบาดแผ่นดิสค์ประเภท Floppy Disk ซึ่งเป็นเทคโนโลยีการบันทึกข้อมูลที่มีการใช้งานแพร่หลายในขณะนั้น โปรแกรมดังกล่าวจะทำการเข้ารหัสข้อมูลบนเครื่องคอมพิวเตอร์ โดยเรียกค่าไถ่ให้ผู้เสียหายโอนเงินจำนวน 189 เหรียญสหรัฐไปยังเลขที่ตู้ไปรษณีย์ในประเทศปานามา กลไกการทำงานของ AIDS Trojan นั้นได้กลายเป็นรากฐานและแม่แบบให้กับบรรดา Ransomware จำนวนมากในปัจจุบัน และเมื่อมาถึงวันนี้ ที่สกุลเงินอิเล็กทรอนิกส์อย่าง Bitcoin กำลังมีบทบาทสำคัญบนโลกอินเทอร์เน็ต พร้อมๆ กับความก้าวหน้าของอัลกอริธึมเข้ารหัสไฟล์ ก็ยิ่งทำให้อาชญากรที่หากินกับ Ransomware ยกระดับความรุนแรงของการโจมตี และเรียกเงินค่าไถ่ในราคาที่สูงมากขึ้น กลายเป็นแรงจูงใจให้อาชญากรรายอื่นๆ หันมาพัฒนา Ransomware เพิ่มมากขึ้นเพื่อหารายได้จากผู้รับเคราะห์ทั่วโลก รูปที่ 1 เป็นรายชื่อของ Ransomware แยกตามสายพันธุ์ ซึ่งบันทึกมาตั้งแต่ปี พ.ศ. 2545 โดยบริษัท F-Secure อันจะเห็นได้ว่าจำนวนของภัยคุกคามอย่าง Ransomware มีความหลากหลาย และยากต่อการพัฒนาเทคโนโลยีและกระบวนการเพื่อป้องกันได้อย่างทันท่วงที นอกจากนั้นยังเป็นการเพิ่มความเสี่ยงของการถูกโจมตีกับผู้ใช้งานคอมพิวเตอร์ทั่วโลก โดยเฉพาะรายที่ไม่ตระหนักถึงภัยคุกคาม และยังไม่มีการสร้างนิสัยในการทำสำรองข้อมูล



รูปที่ 1 รายชื่อของ Malware ที่มีพฤติกรรมเข้ารหัสไฟล์ข้อมูลบนเครื่องคอมพิวเตอร์ของเหยื่อ ตลอดระยะเวลา 10 ปีที่ผ่าน (ข้อมูลจากบริษัท F-Secure)

รูปแบบการแพร่ระบาดของ Ransomware สามารถจำแนกได้ดังแสดงในรูปที่ 2 ไม่ว่าจะเป็นการแสร้งว่าเป็นแอปพลิเคชั่นการใช้งานประเภทใดประเภทหนึ่ง เพื่อล่อหลอกให้ผู้ใช้งานคอมพิวเตอร์ดาวน์โหลดมาใช้งาน (Misleading Apps) ซึ่งเป็นกลยุทธ์การแพร่กระจายที่อาชญากรนิยมในช่วง พ.ศ. 2548 – 2552 การแฝงมากับ Link ของภาพยนตร์ผู้ใหญ่ (AV) ซึ่งมีการใช้วิธีอย่างมากในช่วง พ.ศ. 2553-2554 จนมาถึงการแพร่ระบาดของ Ransomware ประเภทล็อคไฟล์ในช่วง พ.ศ. 2555 – 2556 มาจนถึงปัจจุบัน รูปแบบการแพร่ระบาดของ Ransomware ก็ได้ปรับเปลี่ยนมาเป็นแบบเข้ารหัสไฟล์ สิ่งที่ผู้อ่านพึงตระหนักก็คือข้อมูลต่างๆ ที่ได้กล่าวถึงทั้งในรูปที่ 1 และรูปที่ 2 นี้เป็นเพียงสิ่งที่ตรวจพบเท่านั้น ยังมี Ransomware อีกเป็นจำนวนมากที่ยังไม่สามารถตรวจพบ นอกจากนั้นในแต่ละวันก็น่าจะมี Ransomware ตัวใหม่ๆ ที่มีรูปแบบและระดับการโจมตีที่มีความซับซ้อนและรุนแรงเกิดขึ้นในโลกอีกเป็นจำนวนมาก ข้อมูลเหล่านี้จึงเป็นการย้ำเตือนให้ระมัดระวังถึงการใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์กับโลกอินเทอร์เน็ต เพื่อมิให้ตกเป็นเหยื่อของอาชญากรเหล่านี้



รูปที่ 2 รูปแบบการแพร่ระบาดของ Ransomware ในอดีตจนถึงปัจจุบัน (ข้อมูลจากบริษัท Symantec)

เป้าหมายของผู้ผลิตและผู้แพร่กระจาย Ransomware

แน่นอนอยู่แล้วว่าจุดประสงค์ของบรรดาโปรแกรม Ransomware ในปัจจุบัน เน้นที่การเข้ารหัสไฟล์บนเครื่องคอมพิวเตอร์ของเหยื่อ โดยอาชญากรจะเรียกร้องเงินค่าไถ่ เมื่อพิจารณาถึงเป้าหมายของการก่อการร้าย อาชญากรเหล่านี้ย่อมทราบดีว่าผลกระทบของ Ransomware จะกับองค์กรต่างๆ มากกว่าผู้ใช้งานตามบ้าน และมูลค่าของเงินค่าไถ่ที่เรียกจากองค์กรเหล่านี้ย่อมมีมากกว่าการมุ่งเป้าโจมตีผู้ใช้งานทั่วไป ดังนั้นเป้าหมายหลักของ Ransomware โดยส่วนใหญ่จึงมุ่งไปที่หน่วยงานอย่าง กรมตำรวจ หน่วยราชการทั้งในระดับท้องถิ่นและระดับประเทศ โรงเรียน และที่เลวร้ายไปกว่านั้นก็คือโรงพยาบาล หน่วยงานธุรกิจต่างๆ ก็เป็นเป้าหมายสำคัญของอาชญากรผู้ผลิต Ransomware สิ่งที่เกิดขึ้นแล้วก็คือปฏิกิริยาขององค์กรธุรกิจที่ประสบกับภัยการจู่โจมจาก Ransomware พบว่ามากกว่าร้อยละ 70 ของบริษัทเหล่านี้ยินดีจ่ายเงินเรียกค่าไถ่เพื่อแลกกับการปลดรหัสไฟล์ทางธุรกิจของตน ครั้งหนึ่งของบริษัทเหล่านี้ยอมจ่ายเงินค่าไถ่ที่มีมูลค่าในช่วง 10,000 – 40,000 เหรียญสหรัฐ

แต่ทั้งนี้ก็มิได้หมายความว่าการใช้งานเครื่องคอมพิวเตอร์ตามบ้านจะปลอดภัยจาก Ransomware สิ่งที่ควรพิจารณาก็คือมุมมองของอาชญากรที่มีต่อกลุ่มเป้าหมายของการโจมตี และความคาดหวังต่อผลประโยชน์ตนจะได้รับ เพื่อที่จะได้เข้าใจถึงความเสี่ยงและระดับความรุนแรงที่เราอาจได้รับในฐานะของผู้บริโภคทั่วไป พนักงานบริษัทหรือองค์กร หรือแม้ในฐานะเจ้าของธุรกิจต่างๆ

1. เหตุผลของการเลือกโจมตีผู้ใช้งานรายย่อย (ผู้ใช้คอมพิวเตอร์ตามบ้าน)

- ผู้บริโภคส่วนใหญ่ไม่มีนิสัยในการทำสำรองข้อมูล
- ผู้บริโภคส่วนใหญ่มีความรู้ความเข้าใจ และความระแวดระวังต่อภัยคุกคามทางอินเทอร์เน็ตต่ำ ซึ่งหมายความว่าในการใช้งานอินเทอร์เน็ต ผู้ใช้งานเหล่านี้จะคลิก link ต่างๆ ไปทั่วโดยไม่ระมัดระวัง
- เมื่อเป็นดังนี้ หากอาชญากร มีการข่มขู่ไม่ว่าจะเป็นเรื่องจริงหรือไม่ก็ตาม เหยื่อก็จะหลงเชื่อได้ง่าย
- ผู้บริโภคส่วนใหญ่มักไม่มีการติดตั้งระบบป้องกันการโจมตีทางไซเบอร์

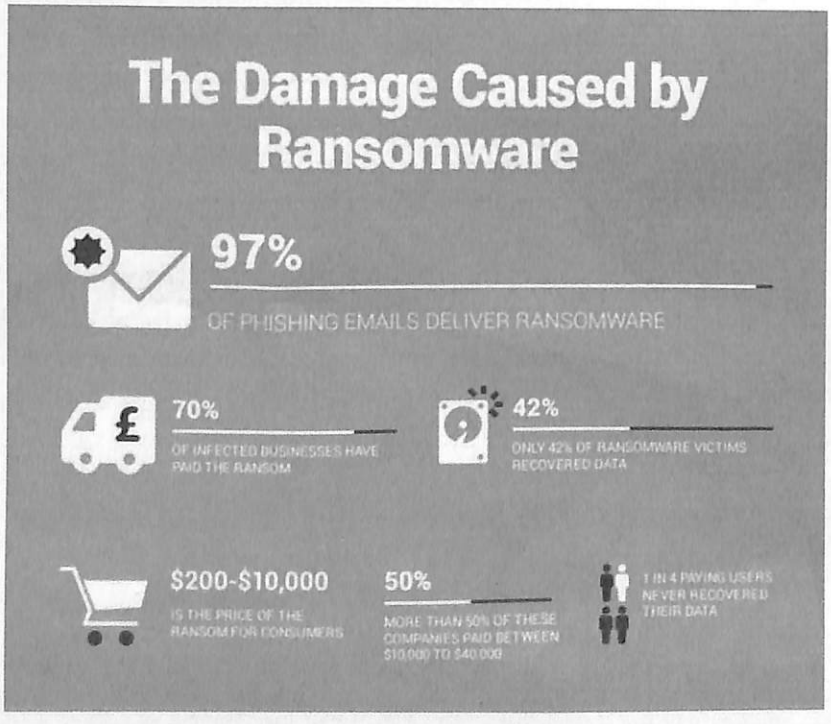
- ที่สำคัญผู้ใช้คอมพิวเตอร์ตามบ้านมักไม่สนใจที่จะ update ซอฟต์แวร์ของตน และไม่ลงทุนจ่ายเงินเพื่อติดตั้งโปรแกรมป้องกันภัยคุกคาม
- ผู้ใช้งานส่วนมากได้แต่ฝันลมแล้งๆ ว่าตนเองคงไม่โชคร้ายถูกโจมตีทางไซเบอร์
- ความเข้าใจของผู้บริโภคว่าโปรแกรมป้องกันไวรัสที่มีอยู่จะสามารถป้องกันภัยต่างๆ ได้ครบถ้วน ซึ่งในความเป็นจริงแล้วโปรแกรมจำนวนมากที่มีในท้องตลาดก็ไม่ได้ครอบคลุมและป้องกันภัยจาก Ransomware ครบทั้งหมด
- แม้เงินค่าไถ่ที่เรียกจากผู้บริโภคแต่ละคนจะไม่มาก แต่ในเมื่อจำนวนผู้บริโภคทั่วโลกมีอยู่มหาศาล และล้วนมีความเสี่ยงที่จะถูกโจมตีได้ง่ายๆ มูลค่ารายได้จากค่าไถ่โดยรวมก็มิใช่น้อย

2. เหตุผลของการเลือกโจมตีหน่วยงานธุรกิจ

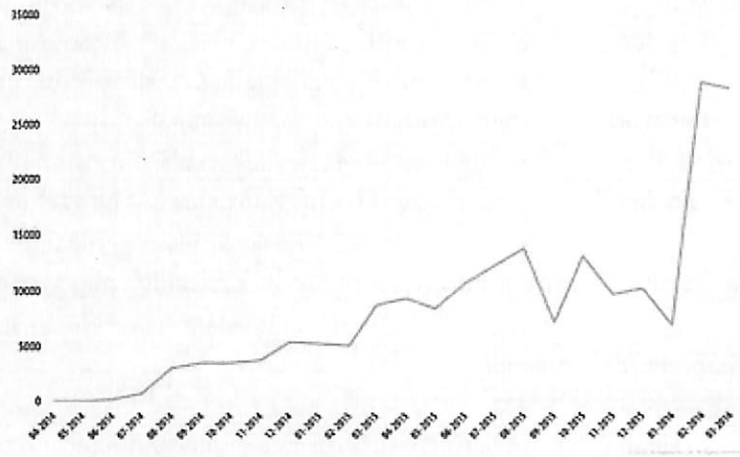
- องค์กรธุรกิจเป็นแหล่งทำเงินของอาชญากร เพราะการโจมตีมีผลต่อการทำธุรกิจโดยตรง บรรดาอาชญากรทราบดีว่าหาก Ransomware ของยิ่งสร้างผลกระทบต่อธุรกิจมากเท่าไร ปริมาณเงินค่าไถ่ที่จะได้รับก็มากขึ้นเท่านั้น
- เนื่องจากระบบคอมพิวเตอร์ในองค์ธุรกิจมีความหลากหลายซับซ้อน และเปิดช่องให้เกิดช่วงโหว่ด้านความปลอดภัยได้ง่าย โดยผู้ดูแลระบบภายในองค์กรก็ไม่อาจตามตรวจสอบหรือสกัดกั้นได้ทัน
- Ransomware มิได้สร้างผลกระทบเฉพาะกับเครื่องคอมพิวเตอร์เท่านั้น แต่ยังมีผลไปถึงเครื่องคอมพิวเตอร์เซิร์ฟเวอร์และเครือข่าย Cloud ที่องค์กรใช้งาน ยิ่งไปกว่านั้นหากสามารถเจาะช่องโหว่ด้านความปลอดภัยเข้าไปถึงเครือข่าย Cloud ที่เป็นแบบ Public ได้ ก็จะทำให้สามารถแพร่ผลกระทบไปยังบริษัทอื่นๆ ที่ร่วมใช้งานได้อีกด้วย
- ที่สำคัญก็คือบรรดาอาชญากรไซเบอร์ทราบดีว่า บริษัทส่วนใหญ่จะรักษาความลับ ซึ่งหมายถึงการรักษาชื่อเสียงและความน่าเชื่อถือทางธุรกิจ ไม่ให้บุคคลภายนอกหรือคู่ค้าทราบว่าถูกโจมตีทางไซเบอร์ ซึ่งก็คือการที่ยอดจ่ายเงินค่าไถ่ได้เพื่อแลกกับความปลอดภัยทางธุรกิจ
- ยิ่งไปกว่านั้น สำหรับกลุ่มธุรกิจประเภท SME ก็มีทุนทรัพย์ไม่มากในการจัดหาโซลูชั่นรักษาความปลอดภัย และยิ่งองค์กรที่อนุญาตให้พนักงานนำอุปกรณ์สื่อสารส่วนตนเข้ามาใช้งาน (BYOD : Bring Your Own Device) ก็ยิ่งกลายเป็นช่วงโหว่ด้านความปลอดภัยที่สามารถโจมตีได้ง่ายยิ่งขึ้น

3. เหตุผลของการเลือกโจมตีหน่วยงานภาครัฐ

- หน่วยงานภาครัฐมีฐานข้อมูลขนาดใหญ่และเกี่ยวข้องกับการบริหารประเภท รวมถึงยังมีข้อมูลสำคัญทั้งที่เกี่ยวกับประชาชนแต่ละคน รวมถึงแผนงานต่างๆ ของภาครัฐ จึงสุ่มเสี่ยงต่อการถูกนำไปขายต่อ
- หน่วยงานรักษาความปลอดภัยของภาครัฐ มักได้รับผลกระทบจากการตัดลดงบประมาณอยู่เสมอ ทำให้เทคโนโลยีการป้องกันการจู่โจมไม่ทันสมัย ง่ายต่อการจู่โจม
- พนักงานด้านไอทีของภาครัฐจำนวนไม่น้อยไม่ได้รับการฝึกอบรมให้มีความรู้และความเชี่ยวชาญที่ทันสมัยพอจะรับมือกับภัยคุกคามในรูปแบบใหม่ๆ ได้ทันท่วงที
- หาก Ransomware สามารถเจาะระบบคอมพิวเตอร์ของภาครัฐและสร้างความเสียหายต่อระบบได้แล้ว ก็จะเกิดผลกระทบมหาศาลต่อการบริหารจัดการภาครัฐ กลายเป็นอำนาจต่อรองสำคัญของบรรดาอาชญากร



รูปที่ 3 พฤติกรรมของภาคธุรกิจที่ยอมจ่ายค่าไถ่กับอาชญากร Ransomware เพื่อแลกกับปัญหาที่จะเกิดขึ้นกับธุรกิจของตน



รูปที่ 4 จำนวนผู้บริโภคที่ใช้ Smart Phone และถูกจู่โจมโดย Mobile Ransomware ในช่วงระหว่างเดือนเมษายน พ.ศ. 2557 ถึง มีนาคม พ.ศ. 2559

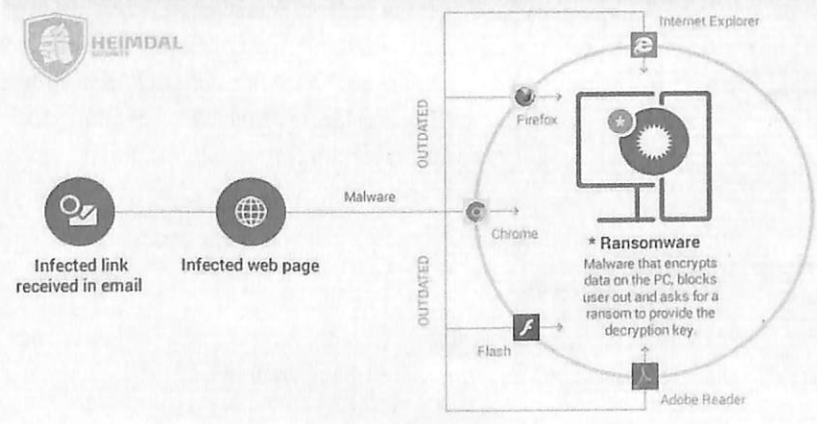
• การประสบความสำเร็จกับการเจาะระบบของภาครัฐและยิ่งสร้างความเสียหายมหาศาลได้มากเท่าไร ก็จะยิ่งเป็นการสร้างความทะนงตนและกระตุ้นให้อาชญากรสร้างความท้าทายใหม่ๆ ด้วยการเพิ่มความรุนแรงของ Ransomware ยิ่งขึ้น นอกจากเหนือจากการได้เงินค่าไถ่จำนวนมาก

จากข้อมูลที่มีการรวบรวมได้ พบว่าบรรดาอาชญากรที่สร้างและเผยแพร่ Ransomware มีการพัฒนาโปรแกรมของตนเองหลากหลายรุ่น เพื่อให้เหมาะสมกับการจู่โจมอุปกรณ์ และแพล็ตฟอร์มคอมพิวเตอร์ของผู้คนทั่วโลก ไม่ว่าจะเป็นเครื่องคอมพิวเตอร์ อุปกรณ์โทรศัพท์เคลื่อนที่หรือ Smart Phone ซึ่งเป้าหมายสำคัญก็คือบรรดาอุปกรณ์ที่ใช้ระบบปฏิบัติการ Android ไปจนถึงบรรดาเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ทั้งหลาย โดยรูปที่ 4 แสดงให้เห็นถึงการเพิ่มขึ้นอย่างก้าวกระโดดของภัยคุกคาม Ransomware บนอุปกรณ์โทรศัพท์เคลื่อนที่ประเภท Smart Phone ที่ใช้ระบบปฏิบัติการ Android ภายในช่วงระยะเวลาเพียง 2 ปี

อะไรทำให้ Ransomware แพร่กระจายอย่างรวดเร็ว

หัวใจในการพัฒนา Ransomware ของบรรดาอาชญากรไซเบอร์ทั้งหลาย อยู่ที่การออกแบบให้สามารถเจาะระบบปฏิบัติการและระบบรักษาความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์ให้ได้อย่างรวดเร็ว หลังจากนั้น Ransomware ก็จะอาศัยการทำงานของเครือข่ายคอมพิวเตอร์ที่เจาะเข้าไปได้นั้นเพื่อเร่งการแพร่กระจายไปยังอุปกรณ์คอมพิวเตอร์อื่นๆ ที่เชื่อมกับอยู่กับเครือข่ายนั้น รูปที่ 5 แสดงกลไกการบุกรุกเข้าสู่เครือข่ายของ Ransomware ผ่านการใช้งานของผู้ใช้งานคอมพิวเตอร์รายหนึ่ง

1. ผู้ใช้งานที่เป็นเหยื่อของการบุกรุก ได้รับอีเมลที่ภายในมี link ลวง หรืออาจมีการแนบไฟล์ที่ติดตั้ง Malware นอกจากนั้นยังอาจเป็นไปได้ว่าผู้ใช้งานรายนี้ถูกหลอกให้เข้าไปยังเว็บไซต์ลวงที่มีกลไกการทะลวงระบบรักษาความปลอดภัยบนเครื่องคอมพิวเตอร์ผ่านทางซอฟต์แวร์ที่ถูกฝังไว้ในเว็บไซต์นั้น



รูปที่ 5 กลไกการบุกรุกของ Ransomware เข้าสู่เครือข่ายคอมพิวเตอร์ผ่านการใช้งานที่พิดพลาดของผู้ใช้งานรายหนึ่ง

2. เหยื่อคลิก link หรือดาวน์โหลดไฟล์ที่แนบมา ซึ่งจะเป็นการเรียกโปรแกรมดาวน์โหลดที่ซ่อนไว้ให้มาติดตั้งบนเครื่องคอมพิวเตอร์ของเหยื่อโดยที่เหยื่อไม่รู้ตัว

3. โปรแกรมดาวน์โหลดจะเรียกไปยัง Domain Server หรือ C&C Server (Comment and Control Server) ที่บริหารจัดการโดยอาชญากรไซเบอร์ เพื่อทำการดาวน์โหลดโปรแกรม Ransomware เข้าไปในเครื่องคอมพิวเตอร์ของเหยื่อ

4. ทางด้านฝั่ง C&C Server จะตอบกลับโดยการส่งข้อมูลไฟล์ที่ต้องการไปให้

5. เมื่อโปรแกรม Ransomware ได้รับการติดตั้งเรียบร้อยแล้ว ก็จะเริ่มทำงานทันที โดยเข้ารหัสไฟล์ทั้งหมดบนฮาร์ดดิสค์ของเหยื่อ และยังดำเนินการเข้ารหัสไฟล์ไปบนไดร์ฟบนเครือข่าย Cloud ที่เชื่อมต่อกับเครื่องคอมพิวเตอร์กล่าวทั้งหมด (Google Drive, Dropbox ฯลฯ) และหากมีคอมพิวเตอร์เครื่องอื่นที่เชื่อมต่ออยู่บนเครือข่าย LAN เดียวกันกับเครื่องของเหยื่อ Ransomware ก็จะทำการเข้ารหัสไฟล์บนคอมพิวเตอร์เครื่องอื่นๆ ทั้งหมดด้วย

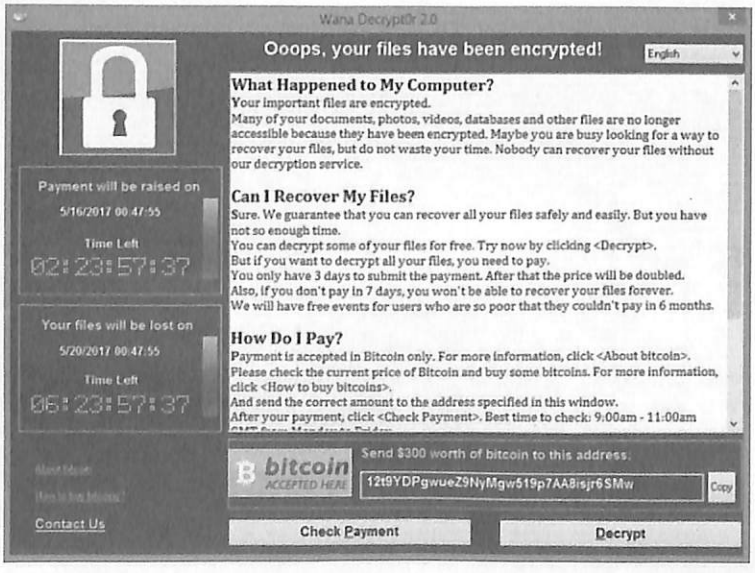
6. บนหน้าจอของเครื่องคอมพิวเตอร์ทั้งหมดที่ถูกเข้ารหัสไฟล์จะมีการแสดงหน้าจอแบบ Pop Up พร้อมบอกรายละเอียดของการจ่ายเงินค่าไถ่เพื่อแลกกับการถอดรหัสไฟล์ทั้งหมด ตัวอย่างหน้าจอดังแสดงในรูปที่ 6

สิ่งที่เป็นข้อสงสัยของผู้ใช้งานคอมพิวเตอร์และเจ้าหน้าที่ด้านสารสนเทศของหน่วยงานต่างๆ ทั่วโลกก็คือ ทำไมโปรแกรมหรือโซลูชั่นป้องกันไวรัสจากผู้ผลิตรายต่างๆ จึงไม่สามารถตรวจจับ Ransomware ได้ทั้งหมด เรื่องนี้เป็นการกำหนดยุทธศาสตร์การออกแบบ Ransomware ของบรรดาอาชญากรไซเบอร์ โดยมีหลากหลายเทคนิคเพื่อหลอก หรือหลบหลีกไม่ได้โปรแกรมป้องกันไวรัสโดยทั่วไปตรวจสอบเทคนิคที่ใช้มีหลากหลายวิธีดังนี้

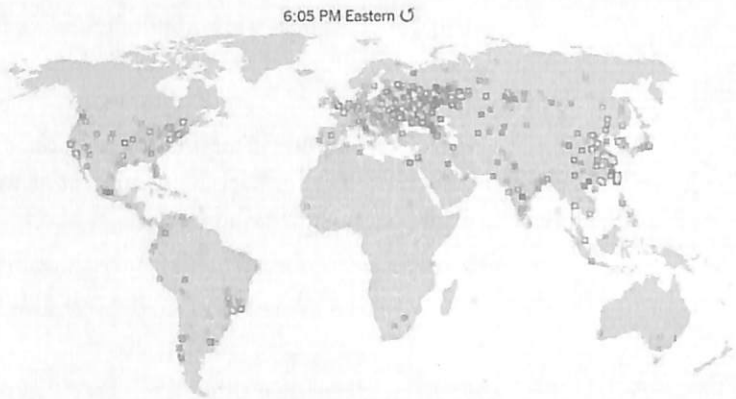
- การติดต่อสื่อระหว่าง Ransomware และ C&C Server ได้รับการเข้ารหัส จนทำให้โปรแกรมป้องกันไวรัสไม่สามารถตรวจสอบได้
- การโอนเงินเรียกค่าไถ่ก็ใช้กลไกอย่าง Bitcoin ซึ่งไม่สามารถติดตามหาเบาะแสได้โดยหน่วยงานทางกฎหมาย
- โปรแกรม Ransomware บางตัวมีการติดตั้งกลไก Anti-Sandboxing เพื่อไม่ให้โปรแกรมป้องกันไวรัสตรวจจับได้
- มีการใช้เทคโนโลยี Domain Shadowing เพื่อซ่อนโดเมนของเว็บไซต์อาชญากรที่เกี่ยวข้องในขณะที่มีการสื่อสารระหว่าง C&C Server กับโปรแกรมดาวน์โหลดที่ติดตั้งบนเครื่องคอมพิวเตอร์ของเหยื่อ

ฯลฯ

ภัยคุกคามของ Ransomware ในปัจจุบันมีความรุนแรงมากยิ่งขึ้น เนื่องจากเมื่อสังคมออนไลน์มีความตื่นตัวและคิดค้นเทคโนโลยีในการป้องกันภัย แต่ในขณะที่กลุ่มเป้าหมายของการโจมตียังคงมีจุดอ่อนดังที่กล่าวมาข้างต้น การปรับปรุงเพื่อสร้างความแข็งแกร่งให้กับ Ransomware โดยการใช้เทคนิคการซ่อนตัวใหม่ๆ ก็ยังเป็นเรื่องที่อาชญากรสามารถทำได้ คิดถึงมูลค่าเงินค่าไถ่ที่ได้รับ ซึ่งส่วนหนึ่งได้กลายเป็นทุนทรัพย์ในการทำวิจัยและพัฒนา (R&D) ของเหล่าอาชญากรเหล่านั้นให้สามารถคิดค้นหาเทคนิคการจู่โจมที่มีความซับซ้อนและทวีความรุนแรงมากขึ้น ในขณะที่ผู้พัฒนาซอฟต์แวร์และโซลูชั่นในการป้องกันยังคงเป็นเพียงฝ่ายตั้งรับ รอให้ตรวจพบ Ransomware ตัวใหม่ๆ แล้วจึงวิเคราะห์หาทางแก้ไข



รูปที่ 6 หน้าจอ Pop Up ที่โปรแกรม Ransomware แสดงบนหน้าจอของเครื่องคอมพิวเตอร์ทั้งหมดที่ถูกโจมตีและเข้ารหัสไฟล์บนฮาร์ดดิสค์ทั้งหมด แสดงรายละเอียดของการให้โอนเงินค่าไถ่



รูปที่ 7 จุดในรูปแสดงถึงประเทศและพื้นที่ที่ WannaCry โจมตีผู้ใช้งานเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Windows

ตัวอย่าง Ransomware ที่สร้างผลกระทบต่อโลกไซเบอร์

ดังได้ไว้แล้วว่า Ransomware มีประวัติศาสตร์ที่ยาวนาน ผ่านการพัฒนาต่อยอดโดยอาชญากรรมหลากหลายกลุ่ม ทำให้ในปัจจุบันโลกไซเบอร์ได้รับผลกระทบจากการโจมตีจาก Ransomware จำนวนมาก ในที่นี้จะได้กล่าวถึง Ransomware ที่ได้สร้างความรุนแรงบนโลกอินเทอร์เน็ต เพื่อให้ผู้อ่านได้ตระหนักถึงผลกระทบและเป็นการสร้างความระมัดระวังของตนเองมิให้ตกเป็นเหยื่อของพฤติกรรมการโจมตีเหล่านี้

WannaCry

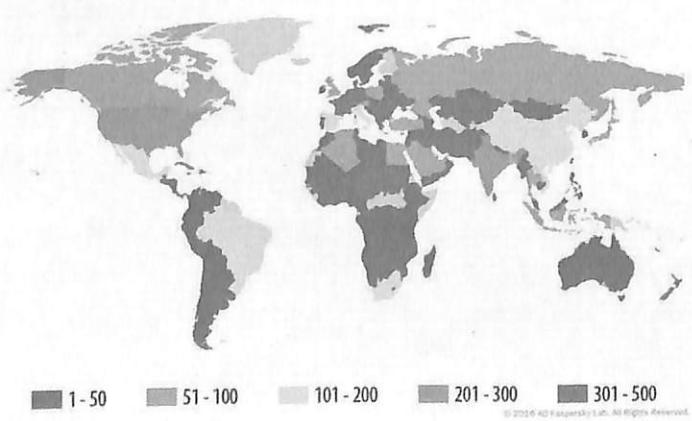
เป็น Ransomware ที่ได้รับความสนใจจากผู้คนทั่วโลกมากที่สุด และก็เป็น Ransomware ที่สร้างความเสียหายเป็นวงกว้างไปทั่วโลก เริ่มสร้างการโจมตีตั้งแต่วันศุกร์ที่ 12 พฤษภาคม พ.ศ. 2560 โดยอาศัยช่องโหว่ด้านการรักษาความปลอดภัยในระบบปฏิบัติการ Windows ซึ่งเปิดโอกาสให้ WannaCry สามารถบุกเข้าไปในเครื่องคอมพิวเตอร์ของเหยื่อได้โดยไม่มีการเตือนภัยหรือตอบโต้ของโปรแกรมใดๆ นับจากนั้นมาจนถึงวันที่ 24 พฤษภาคม พ.ศ. 2560 มีเหยื่อที่ถูก WannaCry เข้ารหัสไฟล์และเรียกค่าไถ่ เป็นจำนวนถึง 200,000 รายใน 150 ประเทศทั่วโลก และยังคงมีการแพร่กระจายอย่างต่อเนื่อง

Locky

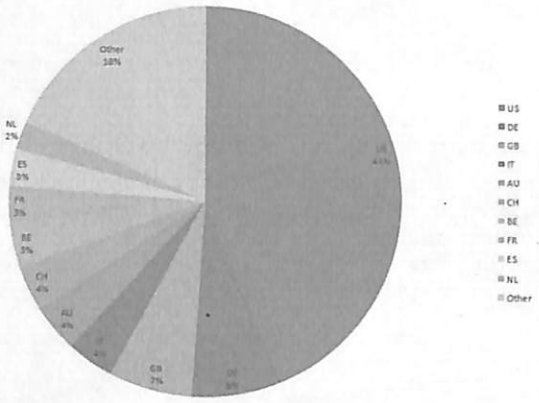
เป็น Ransomware ที่สร้างผลกระทบต่อผู้ใช้คอมพิวเตอร์อย่างรุนแรง เริ่มปรากฏตัวบนโลกอินเทอร์เน็ตเป็นครั้งแรกเมื่อเดือนกุมภาพันธ์ พ.ศ. 2559 โดยจู่โจมและเรียกค่าไถ่จากโรงพยาบาลในฮอลลีวูด เป็นเงิน 17,000 เหรียญสหรัฐ หลังจากนั้นเพียง 2 วัน หลังจากสื่อต่างๆ รายงานข่าวของ Locky ก็มีรายงานข่าวการถูกจู่โจมจำนวนมากจากทั้งผู้บริโภค หน่วยงาน และบริษัทต่างๆ แสดงให้เห็นถึงการแพร่ระบาดอย่างรวดเร็วของ Locky ไปทั่วโลก โดยรูปที่ 8 แสดงถึงการกระจายตัวของผู้เสียหายจาก Ransomware ดังกล่าวทั่วโลก นับถึงเดือนเมษายน พ.ศ. 2559

TorrentLocker

เป็น Ransomware ที่มีกลการการจู่โจมด้วยการเข้ารหัสไฟล์ ได้รับการพัฒนาและแพร่กระจายตั้งแต่ช่วงต้นปี พ.ศ. 2557 และในหลายๆ ครั้งก็มีการจงใจเปลี่ยนชื่อเรียกตนเองเป็น CryptoLocker เพื่อสร้างความสับสนต่อการตรวจจับ นับตั้งแต่นั้นเป็นต้นมา TorrentLokcer ก็มีการแพร่ระบาดโดยฝังตัวเองเข้ากับสแปมอีเมลต่างๆ และมีการจงใจส่งไปยังภูมิภาคต่างๆ ทั่วโลก เพื่อเร่งปฏิกิริยาการโจมตี อาชญากรที่ผลักดันการแพร่กระจายของ TorrentLocker ให้ความสำคัญกับการเขียนเนื้อหาในอีเมลลวงด้วยภาษาที่สะกดถูกต้องตามหลักไวยากรณ์ เพื่อสร้างความน่าเชื่อถือให้ผู้อ่านได้อ่านตามและเผลอคลิก link หรือไฟล์ที่แนบมาด้วย



รูปที่ 8 รายงานการกระจายตัวผู้เสียหายจากการจู่โจมของ Locky ในเดือนเมษายน พ.ศ. 2559



รูปที่ 9 การกระจายตัวของ TorrentLocker ในประเทศต่างๆ

ความน่ากลัวของ TorrentLokcer อยู่ที่ความเลือกเย็นของผู้สร้างโปรแกรมนี้ขึ้นมา เพราะโปรแกรมมีการฝังตัวบนเครื่องคอมพิวเตอร์ไม่ได้หายไปไหน และเมื่อผู้ใช้งานมีการติดตั้งโปรแกรมป้องกัน ผู้สร้าง Ransomware ดังกล่าวก็ยังคงเฝ้าดูผ่านทางโปรแกรมที่ซ่อนตัวในเครื่อง และเมื่อถึงเวลาที่เหมาะสมผู้ผลิตก็จะส่งโปรแกรม TorrentLocker รุ่นใหม่ที่มีกลไกการเข้ารหัสไฟล์ที่แก้ไขได้ยากขึ้นลงไปติดตั้งบนเครื่องคอมพิวเตอร์ของเหยื่อ รูปที่ 9 แสดงถึงการกระจายตัวของของ Ransomware ดังกล่าวในประเทศต่างๆ

นิสัยใหม่ในการป้องกัน Ransomware

ดังได้ทราบแล้วว่ามุมมองของอาชญากรไซเบอร์ที่คิดค้นและพัฒนาโปรแกรม Ransomware เพื่อสร้างรายได้จากการเรียกค่าไถ่การเข้ารหัสไฟล์ ที่มีต่อทั้งผู้บริโภคทั่วไป องค์กรธุรกิจ และหน่วยงานภาครัฐ ล้วนมีสิ่งที่ตรงกันคือการขาดความรู้ ความเอาใจใส่ ทางด้านการป้องกันและรักษาความปลอดภัยข้อมูลของผู้คน ดังนั้นเพื่อมิให้เกิดปัญหาวัวหายแล้วจึงล้อมคอกต่อปัญหาด้านความปลอดภัยของข้อมูล ต่อไปนี้เป็นคำแนะนำง่ายๆ ที่ผู้อ่านพึงตระหนักและเริ่มฝึกที่จะปฏิบัติเพื่อลดความเสี่ยงของการตกเป็นเหยื่อของบรรดา Ransomware ทั้งหลายทั้งที่มีอยู่ในวันนี้ และที่จะเกิดขึ้นใหม่ในอนาคต

1. ไม่เก็บข้อมูลที่มีความสำคัญไว้บนเครื่องคอมพิวเตอร์โดยไม่มีการทำการสำรองข้อมูล

2. ในการทำสำรองข้อมูล ควรจะต้องทำสำรองไว้อย่างน้อย 2 ชุด ชุดแรกบนอุปกรณ์ฮาร์ดดิสค์แบบพกพาได้ อีกชุดหนึ่งบนเครือข่าย Cloud

3. หลีกเลี่ยงที่จะเปิดการทำงานของแอปพลิเคชั่นการบันทึกข้อมูลบนเครือข่าย Cloud ไว้ตลอดเวลา จะให้ดีก็คือให้กำหนดค่ามาตรฐาน (Default) ของโปรแกรมเชื่อมต่อกับแหล่งบันทึกข้อมูล Cloud บนเครื่องคอมพิวเตอร์ไว้เป็น "ปิด" และจะเปิดใช้ก็ต่อเมื่อเวลาที่ต้องการ Sync ข้อมูลเท่านั้น หลังจากเสร็จงานแล้วควรจะปิดการเชื่อมต่อทันที

4. ต้องทำการอัพเดตระบบรักษาความปลอดภัยของทั้งระบบปฏิบัติการและโปรแกรมต่างๆ ที่มีการติดตั้งใช้งานบนเครื่องคอมพิวเตอร์อยู่ตลอดเวลา

5. ในการ login เข้าใช้งานเครื่องคอมพิวเตอร์ หลีกเลี่ยงการ login ด้วยแอคเคานท์ Admin แต่ควรใช้แอคเคานท์ Guest หรือที่สร้างขึ้นมาเพื่อใช้งานสำหรับผู้ใช้งานแต่ละคนเท่านั้น

6. ปิดการทำงานของ Macro ทั้งหลายที่มีอยู่บนบรรดาโปรแกรมในตระกูล Microsoft Office รวมถึงในโปรแกรม Browser ที่ใช้งานอยู่

7. ควรปลดบรรดา Plugin ทั้งหลายที่มีการติดตั้งบนโปรแกรม Browser ไม่ว่าจะเป็น Adobe Flash, Adobe Reader, Java และ Silverlight ในกรณีที่จำเป็นต้องใช้งาน Plugin เหล่านี้ ก็ต้องกำหนดค่าให้โปรแกรม Browser ถามเพื่อขอการอนุญาตก่อนที่จะทำการ Activate บรรดา Plugin เหล่านี้

8. เข้าไปกำหนดค่าการรักษาความปลอดภัยและความเป็นส่วนตัวในโปรแกรม Browser ให้มีระดับการป้องกันที่สูงขึ้นกว่าที่เป็นอยู่

9. ลบบรรดา Plugin และ Add-on ที่เก่าและไม่ได้ใช้งานแล้ว ควรทำให้เป็นนิสัย เก็บเฉพาะ Plugin และ Add-on ที่ตนเองต้องใช้จริงเป็นประจำเท่านั้น

10. ใช้โปรแกรมประเภท Ad-Blocker เพื่อสกัดกั้นบรรดาโฆษณาที่เข้าข่ายเป็นช่องทางลวงของภัยคุกคาม

11. ห้ามเปิดอีเมลที่มีลักษณะเป็นสแปม หรืออีเมลจากคนที่เราไม่รู้จัก

12. ห้ามเปิดหรือดาวน์โหลดไฟล์ที่แนบมากับอีเมลสแปมหรืออีเมลจากคนที่เราไม่รู้จัก

13. ห้ามคลิก link ที่อยู่ในอีเมลสแปมหรืออีเมลจากคนที่เราไม่รู้จัก

14. ให้ความสำคัญกับการลงทุนจ่ายเงินเพื่อซื้อโปรแกรมป้องกันไวรัสที่มีระบบอัพเดตอัตโนมัติ พร้อมกับกลไกการสแกนป้องกันแบบตามเวลาจริง

15. ควรติดตั้งโซลูชั่น Traffic-filtering เพื่อสามารถตรวจพบและสกัดกั้น Ransomware ได้อย่างทันท่วงที

บนโลกที่เปิดกว้างของอินเทอร์เน็ต บริการที่หลากหลาย การเข้าถึงโดยอุปกรณ์สารพัดชนิด การเปลี่ยนทิศทางของการหารายได้ซึ่งปัจจุบันเน้นไปที่การขายโฆษณา เทคโนโลยี Cloud ซึ่งต่อไปจะควบรวมกับเทคโนโลยี IoT เหล่านี้ย่อมเป็นเค้าร่างของภัยอันตรายจาก Ransomware และภัยอื่นๆ ที่นับวันจะยิ่งมีความซับซ้อนและมีผลกระทบต่อการใช้ชีวิตของผู้คนมากขึ้น บทความเรื่องนี้คงจะทำหน้าที่ในการปูพื้นสร้างความเข้าใจต่อภัยคุกคามบนโลกไซเบอร์ในขั้นแรกเพียงเท่านี้ พบกันได้ในบทความเรื่องต่อไปครับ

■ ศุวิล ชมชัยยา
สาขาวิชาวิทยาการคอมพิวเตอร์ประยุกต์
ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

Ransomware โจรเรียกค่าไถ่ยุคไซเบอร์ ที่ต้องรู้เท่าทันเพื่อป้องกันตัว

หากผู้ใช้งานมีความตระหนักและมีความระมัดระวังในการใช้งานก็จะสามารถลดการแพร่ระบาดและความเสียหายของ ransomware ลงได้ และยังสามารถกระทำได้ด้วยตนเอง เพราะในปัจจุบันก็ยังไม่มีอุปกรณ์หรือโปรแกรมต้านมัลแวร์ที่ได้ผล 100 %

จากการที่โปรแกรมไวรัสเรียกค่าไถ่ หรือ ransomware ที่ชื่อว่า WannaCry หรือ WannaCrypt ที่แพร่กระจายไปทั่วโลกเมื่อวันที่ 12 พฤษภาคม 2560 ส่งผลกระทบในวงกว้างต่อเครื่องคอมพิวเตอร์จำนวนหลายพันเครื่องในกว่า 150 ประเทศทั่วโลก ซึ่งเชื่อกันว่า WannaCry ส่งผลกระทบที่รุนแรงเหนือกว่า ransomware ตัวอื่นๆ เนื่องจาก ransomware ตัวนี้สามารถที่จะแพร่ตัวเองไปทั่วทั้งองค์กรผ่านทางระบบเครือข่ายโดยอาศัยช่องโหว่ของระบบปฏิบัติการ Windows และ ransomware ตัวนี้มีความสามารถที่จะสแกนผ่าน TCP port 445 (Server Message Block/SMB) เช่นเดียวกับมัลแวร์ worm แต่มีความสามารถที่จะเข้ารหัสไฟล์ข้อมูลที่ ransomware ตัวนี้เข้ายึดครองและมีการเรียกร้องให้เจ้าของไฟล์ข้อมูลจ่ายค่าไถ่ด้วย bitcoin ซึ่งเป็นที่น่าสังเกตว่า ransomware ตัวนี้ไม่เพียงแต่จะสามารถสแกนภายในระบบคอมพิวเตอร์เพื่อที่จะระบุตำแหน่งที่ต้องการจะแพร่ตัวเองแต่ยังสามารถที่จะแพร่ระบาดผ่านทางช่องโหว่ที่พบในระบบอื่นๆ ทั้งเครือข่าย การแพร่กระจายของ WannaCry ในครั้งนี้ทำให้ Microsoft มีการแก้ไขจุดบกพร่อง (patch) สำหรับระบบปฏิบัติการเวอร์ชั่นเก่าเป็นการด่วน

การระบาดของ WannaCry ในครั้งนี้ก่อให้เกิดความเสียหายและความรุนแรงอย่างมากมาย องค์กรและผู้ใช้งานที่ได้รับผลกระทบจาก ransomware ตัวนี้เพิ่มจำนวนขึ้นอย่างรวดเร็ว อีกทั้งยังมี

ransomware ตัวใหม่ๆ ออกมาอย่างต่อเนื่องซึ่งทำให้การแก้ไขทำได้ยากขึ้น ซึ่งในขณะนี้การแพร่ระบาดของ WannaCry ยังคงอยู่ภายในระหว่างการสอบสวน และการแพร่กระจายของ ransomware คราวนี้ทำให้ทั่วโลกตื่นตระหนักอีกครั้งถึงการรักษาความปลอดภัยของระบบให้ปลอดภัยจากมัลแวร์ประเภทนี้ ซึ่งนอกจากจะส่งผลกระทบและความเสียหายต่อระบบแล้วอาจสร้างความเสียหายเศรษฐกิจตามมาเนื่องจากผู้ไม่หวังดีจะทำการเรียกค่าไถ่ซึ่งถือว่าเป็นอาชญากรรมทางเศรษฐกิจทางโลกไซเบอร์ประเภทหนึ่ง

Ransomware: มัลแวร์ที่ทั้งบุกรุกและรีดไถ

ransomware เป็นลักษณะของมัลแวร์ประเภทหนึ่งที่ทำการสกัดกั้นการเข้าถึงข้อมูลบนระบบโดยจะทำการยึดไฟล์ข้อมูลเพื่อทำการเรียกค่าไถ่ทำให้เจ้าของไฟล์ข้อมูลต้องจ่ายเงินเพื่อที่จะสามารถเข้าถึงได้ตามปกติ ในปัจจุบันมี ransomware มากกว่า 120 สายพันธุ์ และถึงแม้ว่าการแพร่ระบาดของ ransomware ที่ชื่อ WannaCry จะเป็นข่าวที่โด่งดังไปทั่วโลกในขณะนี้ แต่ ransomware ไม่ใช่อุบัติการณ์ใหม่แต่อย่างใด หากแต่มีการพัฒนามาอย่างยาวไกลและเนิ่นนาน

เริ่มจากในปี 1989 ที่ ransomware ถูกนิยามขึ้นว่าเป็นมัลแวร์ที่ขัดขวางการเข้าถึงระบบคอมพิวเตอร์จนกว่าจะมีการชำระเงินค่าไถ่ซึ่ง ransomware ตัวแรกที่มีแพร่กระจาย คือ Aids Trojan หรือที่ทราบกันดีในชื่อ Cyberborg ซึ่งเป็น ransomware ที่เขียนโดย Joseph L. Popp ซึ่งมีแพร่กระจายจากการแจกจ่ายแผ่นดิสก์บันทึกข้อมูลที่ติดฉลากปลอมว่าเป็นแผ่นข้อมูล Aids Information-Introductory Diskettes ที่แจกจ่ายออกไปกว่า 2 หมื่นแผ่นให้กับผู้เข้าร่วมสัมมนาโรคเอดส์ซึ่งจัดโดยองค์การอนามัยโลก ในปี 1989 มัลแวร์ในรูปแบบของโทรจัน (Trojan) เมื่อถูกติดตั้งลงไปในคอมพิวเตอร์แล้วจะทำการนับจำนวนครั้งที่เครื่องคอมพิวเตอร์มีการบูต หากเครื่องคอมพิวเตอร์มีการบูทครบ 90 ครั้งไฟล์ข้อมูลจะถูกซ่อนและเข้ารหัสซึ่งทำให้ผู้ใช้ถูกเรียกร้องให้ชำระเงิน 189 ดอลลาร์สหรัฐให้กับบริษัทปลอมที่ตั้งขึ้นมาเพื่อรับชำระค่าไถ่ที่ชื่อว่า PC Cyborg Corp. มีถิ่นฐานที่ตั้งในประเทศปานามา ซึ่ง AIDS Trojan ถือว่าเป็น ransomware รุ่นแรก ที่สามารถแก้ไขได้ไม่ยากและในเวลาต่อมาไม่นานนักก็ได้มีเครื่องมือในการแก้รหัสไฟล์ได้ แต่อย่างไรก็ตาม ransomware ก็ยังมีการยกระดับการพัฒนาขึ้นอีก

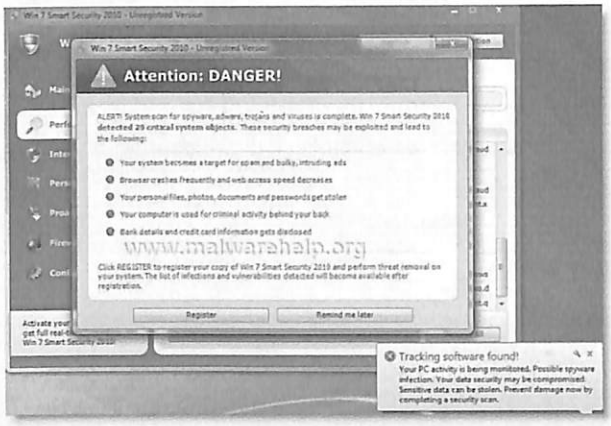
ต่อมาในปี 2006 เมื่อการพัฒนา ransomware มีความเป็นมืออาชีพมากขึ้นจึงมีการผสมผสานการเข้ารหัสแบบ RSA ซึ่งในปีนี้ trojan ที่ชื่อว่า Archiveus สามารถเข้ารหัสทุกไฟล์ข้อมูลใน My Documents และบังคับให้ผู้ตกเป็นเหยื่อต้องซื้อผลิตภัณฑ์ออนไลน์เพื่อรับรหัสผ่าน 30 หลักเพื่อปลดล็อคไฟล์ข้อมูล ในเดือนมิถุนายนปี 2006 ransomware ที่ชื่อว่า CP Code ซึ่งเป็น trojan แบบเข้ารหัสเหมือนกัน สามารถแพร่กระจายผ่านอีเมล์ในลักษณะของจดหมายสมัครงานโดยใช้กุญแจสาธารณะ RSA แบบ 660 บิท และกลายเป็นแบบ 1024 Bit ในอีก 2 ปีต่อมา

Ransomware แบบล็อคหน้าจอ (Lock-screen)

เป็น ransomware ชนิดอื่นที่ไม่เกี่ยวข้องกับการเข้ารหัสแต่เป็นแบบ lockout ผู้ใช้งาน ซึ่งในช่วงปี 2006 เช่นกัน ได้มีการพัฒนา ransomware ที่ชื่อ Winlocker ที่แสดงผลเป็นภาพล่อไปในทางลามกอนาจารขึ้นมาบนหน้าจอ (แสดงในรูปที่ 1) จนกว่าผู้ใช้งานจะยอมจ่ายเงินจำนวน 10 ดอลลาร์เพื่อรับรหัสในการปลดล็อคผ่านทาง SMS หรือ ransomware ประเภทอื่นที่มีแจ้งเตือนแบบ Windows Product activation ซึ่งจะให้ผู้ใช้งานต้องโทรศัพท์ไปตามหมายเลขโทรศัพท์ทางไกลระหว่างประเทศ (International Number) เพื่อรับหมายเลขถอดรหัส 6 หลักซึ่ง โทรศัพท์จะทำการต่อสายไปยังประเทศที่มีอัตราค่าโทรศัพท์ทางไกลระหว่างประเทศสูงซึ่งทำให้พูดต้องถือสายไว้ในระยะเวลานานทำให้ค่าโทรศัพท์พุ่งสูงขึ้น

อีกประเภทหนึ่งก็คือ scarware ซึ่งเป็นมัลแวร์ที่ใช้ในการข่มขู่ให้เกิดความกลัว (แสดงในรูปที่ 2) ซึ่งต่างจากมัลแวร์ที่กล่าวมาข้างต้น ซึ่งทำหน้าที่เข้ารหัสไฟล์ข้อมูลหรือล็อคหน้าจอ มัลแวร์ประเภทนี้จะข่มขู่ผู้ใช้งานให้เกิดความกลัวจนยอมจ่ายเงินเช่นเดียวกันกับลักษณะที่มีการสร้างการแจ้งเตือนลวง เหมือน Windows Alert ซึ่งเป็นการหลอกลวงผู้ใช้งานว่าขณะนี้ตรวจพบไวรัสหรือสปายแวร์บนเครื่องคอมพิวเตอร์ซึ่งจะมีผลกระทบต่อการใช้งานหรือสร้างผลเสียหายตามมาอย่างมาก และเชิญชวนให้ผู้ใช้งานซื้อซอฟต์แวร์เพื่อป้องกันหรือปราบไวรัส/สปายแวร์ หรือในกรณีที่มีการเตือนลวงว่ามีการเข้าถึงสื่อลามกอนาจารเด็กหรือการดาวน์โหลดโปรแกรมที่เป็นการละเมิดลิขสิทธิ์หรือไม่ถูกต้องตามกฎหมายได้ถูกตรวจพบบนเครื่องคอมพิวเตอร์ และข่มขู่ผู้ใช้งานต้องเสียเงินเพื่อหลีกเลี่ยงการถูกดำเนินคดีทางกฎหมาย

รูปที่ 1 หน้าจอ Winlocker (www.pcmag.com)



รูปที่ 2 Scareware (www.gaspartech.com)

Scareware ในปัจจุบัน ได้มีการพัฒนาเทคนิคต่างๆ มากมาย เช่น การปิดกั้นการทำงานของโปรแกรมอื่นๆ ด้วยการเฝ้ามองหน้าต่างที่เปิดใหม่เพื่อใช้งานและมีการแทรกแซงหรือยึดกระบวนการทำงานของระบบปฏิบัติการแล้วสร้างหน้าจอเดสท็อปใหม่ขึ้นตลอดเวลา หรือการสร้างหน้าจอเต็มเพื่อบดบังหน้าจออื่นๆ ที่กำลังใช้งานอยู่ ซึ่งเทคนิคนี้หน้าจอของโปรแกรมที่ผู้ใช้งานที่กำลังเปิดใช้งานอยู่ยังคงดำเนินต่อไปได้ แต่ทุกหน้าจอจะถูกบังคับควบคุมโดย scareware ที่คอยสร้างหน้าจอเต็มเพื่อก่อกวนและขัดขวางการใช้งานอยู่ตลอดเวลา

ในปี 2012 ซึ่งเป็นปีของการระบาดของ ransomware อย่างกว้างขวางโดยเริ่มจากช่วงกลางปี 2011 ที่ ransomware ได้มีการพัฒนาให้มีความใหญ่โตและมีขีดความสามารถมากขึ้น จากรายงานของ McAfee Quarterly Threats Report พบว่าได้มีการตรวจพบ ransomware ชนิดใหม่มากกว่า 30,000 ประเภทในช่วง 2 ไตรมาสแรกของปี 2011 และได้เพิ่มขึ้นเป็นเท่าทวีคูณจนทะลุ 100,000 ประเภท ในไตรมาสที่ 3 ของปี 2011 และไม่เพียงเท่านั้น จำนวนของ ransomware ได้เพิ่มจำนวนเป็นเท่าทวีคูณอีกในไตรมาสที่ 3 ของปี 2012 โดยมีมากกว่า 200,000 ชนิดหรือมี ransomware เกิดใหม่ประมาณ 2,000 ชนิดต่อวัน ซึ่งในส่วนนี้บริการจ่ายเงินแบบนิรนามหรือ anonymous payment services ช่วยให้การจ่ายเงินค่าไถ่ให้บรรดาแฮกเกอร์เหล่านี้เป็นเรื่องง่ายมากกว่าการจ่ายทางบัตรเครดิต

Ransomware แบบเข้ารหัส (Crypto)

ransomware ประเภทนี้จะมีการเข้าลักลอบเข้ารหัสข้อมูลโดยที่เจ้าของไฟล์ข้อมูลหรือเจ้าของระบบไม่ได้รับรู้ทำให้ไม่สามารถเปิดไฟล์ข้อมูลหรือเข้าระบบได้ตามปกติและเช่นเดียวกันก็การเรียกร้องให้ผู้ใช้งานหรือเจ้าของไฟล์ข้อมูลต้องจ่ายเงินเพื่อปลดล็อค โดยในปี 2013 CryptoLocker ได้ปรากฏสู่สายตาเป็นครั้งแรกซึ่งส่งผลร้ายแรงมากกว่า ransomware แบบ lock-screen และ scareware เนื่องจากแบบ lock-screen สามารถแก้ไขได้โดยการสร้างเครื่องมือในการที่จะล้างโปรแกรมออกทำให้สามารถเข้าถึงข้อมูลได้ CryptoLocker แพร่กระจายผ่านทางอีเมล์และการดาวน์โหลดต่างๆ จากเว็บไซต์ที่ติดไวรัสหรือโทรจัน โดยจะสร้างกุญแจรหัสคู่แบบ RSA แบบ 2048 bit อัพโหลดขึ้นสู่ Server และถูกใช้ในการเข้ารหัสไฟล์ที่มีนามสกุลที่จำเพาะเจาะจงแล้วลบต้นฉบับทิ้งไป และมีการข่มขู่เจ้าของไฟล์ข้อมูลว่าจะมีการลบไฟล์ทิ้งหากไม่ได้รับเงินค่าไถ่ภายใน 3 วันโดยผู้ใช้งานที่ตกเป็นเหยื่อต้องชำระค่าไถ่ด้วย bitcoin หรือคูปองเงินสด และ CryptoLocker บางประเภทที่หากผู้ใช้งานยังไม่ชำระค่าไถ่ภายใน 3 วันจะได้รับโอกาสอีกครั้งเป็นครั้งที่ 2 แต่จะต้องชำระค่าไถ่ในอัตราที่สูงขึ้นเพื่อเอาไฟล์ข้อมูลกลับมาและราคาค่าไถ่จะมีการเปลี่ยนแปลงตลอดเวลา

และในเดือนธันวาคมปี 2013 เช่นกัน จากรายงานของ Dell Secure Work พบว่าเครื่องคอมพิวเตอร์มากกว่า 250,000 เครื่อง มีการติด ransomware แล้ว และจากการวิจัยของ ZDNet ที่ทำการศึกษาวิจัยบัญชี bitcoin ที่มีความเกี่ยวข้องกับ CryptoLocker และพบว่า bitcoin จำนวน 41,928 bitcoin ถูกถ่ายโอนเข้ามายัง 4 บัญชี bitcoin ในระหว่างเดือนกุมภาพันธ์ถึงเดือนธันวาคมโดยในระหว่างนั้น 1 bitcoin มีมูลค่าเท่ากับ 661 เหรียญสหรัฐ ซึ่งหมายถึงมีการชำระค่าไถ่ด้วย Bitcoin โดยมีมูลค่าเทียบเป็นเงินตราได้ถึง 27 ล้านเหรียญสหรัฐ ทั้งนี้ยังไม่รวมถึงวิธีการชำระค่าไถ่โดยวิธีอื่นๆ

จากวิวัฒนาการของ ransomware ข้างต้นจะเห็นว่ารูปแบบการเรียกค่าไถ่มีการพัฒนาไปพร้อมๆ กับวิธีการเรียกเก็บค่าไถ่ โดยการชำระด้วย bitcoin เป็นวิธีการที่แฮกเกอร์นิยมนำมาใช้ ซึ่งจากการชำระค่าไถ่ด้วย bitcoin เป็นการชำระแบบนิรนามโดยที่ bitcoin มีมูลค่าสูงและไม่สามารถตรวจสอบได้เนื่องจากเป็นระบบเงินตรา digital ที่ไม่ได้ถูกควบคุมโดยรัฐบาลประเทศใดๆ ดังนั้นจึงเป็นการง่ายในการรับเงินแต่ยากต่อการตรวจสอบและติดตาม

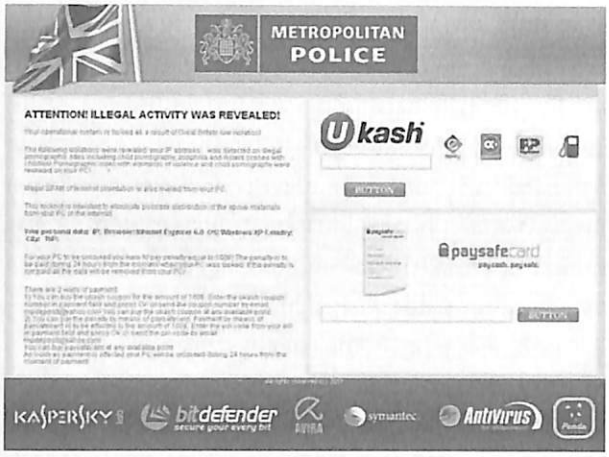
สายพันธุ์หลักของ ransomware

Ransomware สามารถจำแนกเป็นสายพันธุ์หลักๆ ต่างๆ เช่น

Winlock/Police Ransomware

Police ransomware จะมีการแสดงข้อความเตือนผู้ใช้งานโดยสร้างความรู้สึกเสมือนว่ากำลังถูกติดตามโดยเจ้าหน้าที่กฎหมายบ้านเมืองโดยกล่าวหาผู้ใช้งานว่าได้กระทำผิดกฎหมายคอมพิวเตอร์ในด้านต่างๆ เช่น การเข้าเยี่ยมชมเว็บไซต์สื่อลามกอนาจาร การดาวน์โหลดหรือแชร์ไฟล์/โปรแกรมที่มีลิขสิทธิ์โดยมัลแวร์จะเข้าทำการยึดครองคอมพิวเตอร์และล็อคเครื่องทำให้ไม่สามารถเข้าใช้งานได้ตามปกติ หรือมีการล็อคหน้าจอและแสดงข้อความจากกลุ่มบุคคลที่แอบอ้างว่าเป็นเจ้าหน้าที่ตำรวจ (แสดงในรูปที่ 3)

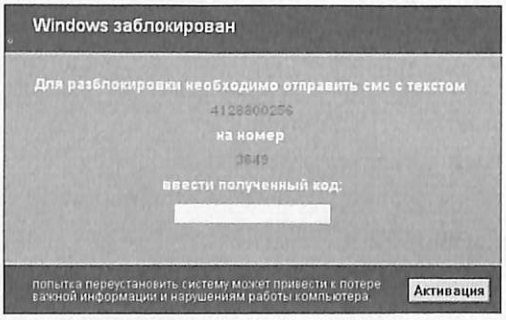
Police ransomware ประเภทนี้มีถิ่นกำเนิดจากประเทศทางยุโรปตะวันออกซึ่งมีพื้นฐานทางสังคมที่ประชาชนมีความหวาดกลัวและไม่ไว้ใจต่อตำรวจมาเป็นเวลากว่าครึ่งศตวรรษเนื่องจากต้องเผชิญกับองค์กรตำรวจสันติบาลในยุคสังคมนิยม และ ransomware ชนิดนี้ได้แพร่กระจายไปทั่วโลกในปี 2012 ลักษณะเด่นของ ransomware ประเภทนี้คือสามารถปรับแต่งให้เหมาะสมกับลักษณะของพื้นที่ เช่น สถานที่ กฎหมายท้องถิ่น หรือข้อมูลจำเพาะพื้นที่เพื่อสร้างความสมจริง



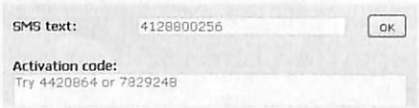
รูปที่ 3 Police ransomware (www.anvisoft.com)

SMS ransomware

Ransomware ประเภทนี้เป็นสายพันธุ์หนึ่งของ log-out ransomware แตกต่างในเรื่องของวิธีการชำระค่าไถ่ซึ่งหน้าจอจะแสดงรหัสและวิธีการในการส่งรหัสผ่านทาง SMS โดยส่งผ่านไปยังหมายเลข SMS ที่มีการเก็บค่าธรรมเนียมแบบพรีเมี่ยมโดยผู้ใช้งานที่ส่งรหัสผ่าน SMS จะได้รับรหัสในการปลดล็อค (แสดงในรูปที่ 4) โดยที่บนหน้าจอจะปรากฏหมายเตือนเรียกเก็บค่าไถ่และวิธีการชำระค่าไถ่ ซึ่งลักษณะการใช้งานประเภทนี้จะเป็นงานเรียกเก็บค่าไถ่เพื่อรับรหัสในการปลดล็อคเพื่อให้คอมพิวเตอร์สามารถใช้งานได้ต่อไป



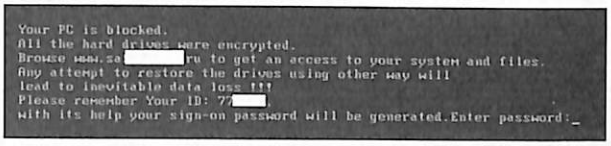
Trojan.Winlock can remove itself in two hours after launching. Users who don't want to wait that long can use the web-form to enter the text of the suggested SMS and get the unblock code.



รูปที่ 4 SMS ransomware (www.zdnet.com)

MBR ransomware

MBR หรือ Master Boot Record เป็นส่วนหนึ่งของฮาร์ดดิสก์ไดร์ฟที่บรรจุข้อมูลเพื่อช่วยในการ boot up ของระบบปฏิบัติการ ซึ่ง MBR ransomware จะทำการเปลี่ยน Master Boot Record ของเครื่องคอมพิวเตอร์ ข้อความในการเรียกค่าไถ่จะแสดงอยู่บนหน้าจอเมื่อเปิดใช้งาน ทำให้เครื่องคอมพิวเตอร์ไม่สามารถจะบูตได้และจะมีการอ้างว่าไฟล์ข้อมูลถูกเข้ารหัสแม้ว่าจริงๆ จะไม่ได้เป็นเช่นนั้น ทำให้เครื่องคอมพิวเตอร์ไม่สามารถที่จะโหลดระบบปฏิบัติการได้ ดังนั้นผู้ใช้งานก็ไม่สามารถที่จะใช้เครื่องมือในการแก้ระบบ ต้าน ransomware หรือทำการใดๆ กับระบบได้อย่างสิ้นเชิง (แสดงในรูปที่ 5)



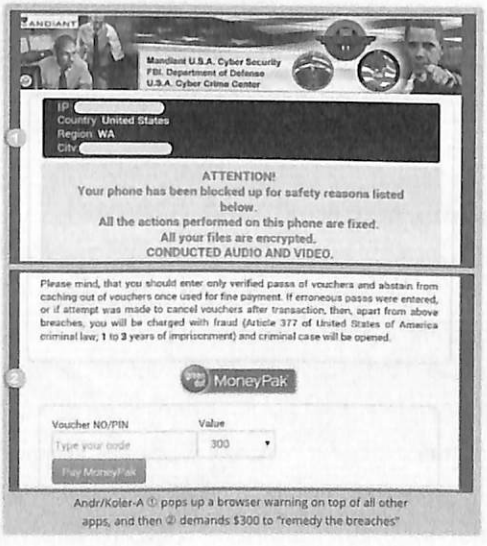
รูปที่ 5 ข้อความที่ปรากฏบนหน้าจอ MBR ransomware (www.securelist.ru)

mobile ransomware: เมื่อโจรเรียกค่าไถ่ติดตามตัวไปได้ทุกที่

แม้ว่า ransomware ส่วนใหญ่จะพุ่งเป้าที่ desktop หรือ laptop แต่ก็ยังมี ransomware บางประเภทที่ออกแบบเฉพาะสำหรับการบุกรุกและเรียกค่าไถ่บนอุปกรณ์พกพา เช่น

- **Koler.a**

เปิดตัวในเดือนเมษายนในรูปแบบของ police ransom trojan แพร่กระจายไปยังผู้ใช้งาน Android ราว 2 แสนรายซึ่ง 3 ใน 4 ของจำนวนนี้เป็นผู้ใช้งาน Android ในประเทศสหรัฐอเมริกา แต่ว่าเมื่อ Android กำหนดให้ผู้ใช้งานต้องอนุญาตเมื่อต้องทำการติดตั้ง app ใดๆ ดังนั้นจึงไม่สามารถทราบได้ว่าเมื่อดาวน์โหลด app ไปแล้วจะมีจำนวนเท่าไหร่ที่ติดตั้งเพื่อใช้งานจริง ซึ่งผู้ใช้งานที่เผลอติดตั้ง app ลงไปจะต้องถูกเรียกค่าไถ่เป็นจำนวนเงิน 100 ถึง 300 เหรียญสหรัฐเพื่อลบโปรแกรมออก โดยจะแสดงการล็อคหน้าจอของอุปกรณ์พกพาพร้อมแสดงหน้าจอเพื่อชำระเงินค่าไถ่ ดังแสดงในรูปที่ 6

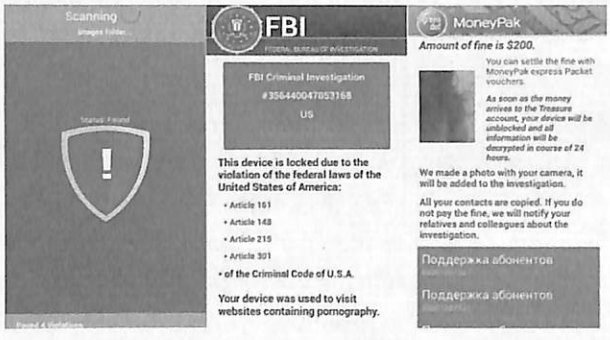


Andr/Koler-A ① pops up a browser warning on top of all other apps, and then ② demands $300 to "remedy the breaches"

รูปที่ 6 ตัวอย่างข้อความที่ปรากฏบนหน้าจอ Koler.a (www.sophos.com)

• **Svpeng**

mobile trojan ตัวนี้พุ่งเป้าไปที่ผู้ใช้งาน Android ซึ่งมีการตรวจพบครั้งแรกในเดือนกรกฎาคมปี 2013 โดย kaspersky ซึ่ง mobile trojan ตัวนี้แรกเริ่มได้ถูกออกแบบให้มีการขโมยข้อมูลเกี่ยวกับบัตรเครดิตหรือบัตรชำระเงินต่างจากลูกค้าของธนาคารต่างๆ ในประเทศรัสเซีย และในช่วงต้นปี 2014 ได้พัฒนามาเป็น ransomware โดยจะมีการล็อกหน้าจอโทรศัพท์และแสดงข้อความกล่าวหาว่าผู้ใช้งานได้มีการเข้าสู่เว็บไซต์หรือสื่อลามกอนาจารเด็ก และในช่วงฤดูร้อนของปี 2014 เวอร์ชั่นใหม่ของโทรจันตัวนี้ได้ถูกพัฒนาขึ้นโดยพุ่งเป้าไปที่ผู้ใช้งานที่อยู่ในประเทศสหรัฐอเมริกาโดยใช้ข้อความปลอมที่แอบอ้างว่าเป็นข้อความจากหน่วยสืบสวนกลาง (Federal Bureau of Investigation: FBI) ละข่มขู่ให้ต้องชำระเงินจำนวน 200 ดอลลาร์สหรัฐ (แสดงในรูปที่ 7) ทั้งนี้ยังมีเวอร์ชั่นที่เปลี่ยนแปลงไปตามลักษณะประเทศโดยได้ระบาดไปยังประเทศอังกฤษ สวิตเซอร์แลนด์ อินเดีย และรัสเซีย นอกจากนี้ svpeng ยังสแกน app ต่างๆ ที่เป็น Mobile Banking เพื่อตรวจจับหาข้อมูลสำคัญในการใช้ งาน เช่น รหัสผ่าน หมายเลขบัญชี แต่ยังไม่พบว่าข้อมูลเหล่านี้ถูกโจรกรรมและสร้างความเสียหายแต่อย่างใด



รูปที่ 7 ข้อความที่ปรากฏบนหน้าจอ svpeng (www.softpedia.com)

• **Find my phone**

ในเดือนพฤษภาคม 2014 ผู้ใช้งาน Apple ในประเทศออสเตรเลียและสหรัฐอเมริกาพบว่ามีการล็อกหน้าจอบนอุปกรณ์ต่างๆ เช่น iPad หรือ iPhone โดยหน้าจอได้ถูกล็อคและมีการเรียกค่าไถ่เป็นจำนวนเงินระหว่าง 50 ถึง 100 ดอลลาร์สหรัฐ เพื่อปลดล็อคซึ่งในจำนวนนี้ไม่ได้มีการระบุว่าจำนวนอุปกรณ์เท่าใดที่ได้รับผลกระทบจาก ransomware ตัวนี้ และในเดือนมิถุนายนในปีเดียวกันทางการตำรวจของประเทศรัสเซียได้มีการจับกุมบุคคล 2 คนที่มีส่วนเกี่ยวข้องและได้มีการสอบสวนถึงการแพร่กระจายของ ransomware ชนิดนี้ ซึ่งพบว่าไม่มีการเกี่ยวข้องกับการติดตั้งมัลแวร์แต่ประการใดเพียงแต่อาศัยบางฟังก์ชั่นการใช้งานของระบบปฏิบัติการ iOS โดยที่ผู้ใช้งานจะถูกล่อลวงให้ sign up เพื่อใช้บริการจาก video service ซึ่งจะต้องใช้ Apple ID ในการลงทะเบียน จากนั้นแฮกเกอร์จะสามารถสร้างบัญชี iCloud โดยใช้ ID เหล่านั้นกับฟังก์ชันการใช้งาน find my phone ซึ่งฟังก์ชันนี้สามารถที่จะล็อคหน้าจอ iPhone หรือ iPad เสมือนว่าอุปกรณ์นั้นได้สูญหายหรือถูกโจรกรรมจริง Apple ID ที่ได้มาจากการล่อลวงเหล่านี้จะถูกย้อนกลับมาใช้ล็อคหน้าจอโทรศัพท์ของผู้ที่ตกเป็นเหยื่อและให้ Apple ID ไปกับแฮกเกอร์ด้วยความรู้เท่าไม่ถึงการณ์ (แสดงในรูปที่ 8)

รูปที่ 8 ตัวอย่างข้อความที่ปรากฏบนหน้าจอเมื่อ Apple ID ถูกใช้เป็นเครื่องมือในการเรียกค่าไถ่โดยเลียบแบบ ransomware (www.9to5mac.com)

Ransomware บน Android : การรุกคืบของ ransomware ที่เกาะกระแสความนิยม

แม้ว่าสองประเภทหลักของ ransomware คือ screen-lock และ crypto ซึ่งต่างก็สร้างปัญหามากมายบนเครื่องคอมพิวเตอร์ในยุคแรกๆ ของการแพร่กระจาย โดยเฉพาะอย่างยิ่งบนระบบปฏิบัติการ Windows นับตั้งแต่ปี 2013 และถึงแม้ว่า ransomware จะมีการแพร่กระจายมาเป็นเวลานานก่อนหน้านั้นซึ่งได้ส่งผลเสียหายต่อทั้งผู้ใช้งานรายบุคคลและองค์กรธุรกิจ และในปัจจุบันเมื่อแนวโน้มของอุปกรณ์พกพาที่ใช้ระบบปฏิบัติการ Android ซึ่งมีความนิยมสูงมากในขณะนี้ ทำให้เป้าหมายในการโจมตีของมัลแวร์พุ่งเป้ามาที่ระบบปฏิบัติการแอนดรอยด์มากขึ้นโดยนักพัฒนามัลแวร์ทั้งหลายได้มีการพัฒนาเทคนิคในการสร้าง ransomware โดยใช้เทคนิคที่ประสบผลสำเร็จมาแล้วบนระบบปฏิบัติการ Windows

Mobile computing ที่เป็นที่นิยมอย่างแพร่หลายและผู้ใช้งานนิยมหันมาเก็บข้อมูลไว้บนอุปกรณ์พกพาที่สะดวกและง่ายต่อการเข้าถึงได้ทุกที่ทุกเวลานั่นหมายถึงข้อมูลอันมีค่า เช่น ข้อมูลทางธุรกิจที่นำมาจัดเก็บไว้บนอุปกรณ์พกพาหรือเข้าถึงผ่านอุปกรณ์พกพา จึงเป็นที่หมายตาของเหล่าบรรดาแฮกเกอร์และนักพัฒนามัลแวร์ต่างๆ ช่องทางในการแพร่กระจายของ ransomware บนระบบปฏิบัติการ Android ก็เช่นเดียวกับมัลแวร์ที่แพร่กระจายบนเครื่องคอมพิวเตอร์ PC และเป็นวิธีการแพร่กระจายเช่นเดียวกับโทรจันต่างกันที่การแฝงตัวมาในรูปของ app ต่างๆ ที่ดูเหมือนเป็นปกติหรือไม่มีความน่าสงสัย เช่น เกมส์ออนไลน์ต่างๆ ที่เปิดให้ทดลองดาวน์โหลดมาเล่นได้ฟรีหรือสื่อปลุกอารมณ์แบบต่างๆ ซึ่ง App ที่ใช้เป็นสื่อในการแพร่กระจายมัลแวร์ต่างๆ เหล่านี้จะถูกพัฒนาขึ้นมาเพื่อเป็นการล่อตาล่อใจให้เหยื่อได้ทดลองดาวน์โหลด หรือลักษณะของมัลแวร์บางประเภทซึ่งมาในรูปของ .APK แต่มีการตั้งชื่อให้ดูเหมือนปกติที่ไม่มีความน่าสงสัยหรือไม่มีพิษภัยอะไร

Ransomware บนระบบปฏิบัติการ Android จะมีลักษณะการทำงานที่ต่างกันโดยปกติแล้วจะแสดงข้อความหรือก่อกวนระบบเพื่อเรียกค่าไถ่ในรูปแบบต่างๆ เช่น

- การส่งข้อความ SMS ไปถึงรายชื่อติดต่อบางรายชื่อรายชื่อทั้งหมด
- การล็อคหรือการปลดล็อคอุปกรณ์
- การขโมยข้อความ SMS
- การแสดงข้อความเรียกค่าไถ่ต่างๆ กัน
- มีการนำเสนอให้อัพเดท App หรือซอฟต์แวร์ให้เป็นเวอร์ชั่นที่ใหม่กว่า
- การล็อกหรือปลดล็อคข้อมูล mobile
- การล็อคหรือปลดล็อค WiFi
- การติดตามผู้ใช้งานผ่านทาง GPS

กลไกการป้องกันตัวของมัลแวร์บนระบบปฏิบัติการ Android

มัลแวร์บนระบบปฏิบัติการ Android ซึ่งรวมถึง ransomware ต่างก็พัฒนาให้มีระบบการป้องกันตนจากการถูกทำลายโดย anti-malware หรือกลไกการป้องกันของ Google เอง เช่น การขัดขวางการทำงานของโปรแกรม anti-malware หรือการแอบอ้างสิทธิ์ของผู้ดูแลอุปกรณ์ (Device Administrator priviledges) ซึ่งจะสามารถเข้าถึงข้อมูลและฟังก์ชั่นต่างๆ บนอุปกรณ์พกพาได้มากกว่าปกติทั่วไป เนื่องจากสิทธิ์ของผู้ดูแลอุปกรณ์ครอบคลุมถึงการปรับแต่งหรือการตั้งค่าความเสถียรและความปลอดภัยของอุปกรณ์ซึ่งหากมัลแวร์ต่างๆ ที่รวมถึง ransomware สามารถเข้าถึงสิทธิ์นี้ได้มักจะเป็นอันตรายอย่างยิ่ง เช่น ในกรณีที่ ransomware ที่สามารถบุกรุกและยึดครองสิทธิ์ของผู้ดูแลอุปกรณ์ได้อาจตั้งค่าหรือปรับแต่งให้อุปกรณ์ยินยอมให้มีการติดตั้ง App ต่างๆ ที่เป็นมัลแวร์เหมือนการติดตั้ง App ตามปกติและจำกัดสิทธิ์ของผู้ใช้งานจริงในการที่จะลบโปรแกรมมัลแวร์ออกไปจากอุปกรณ์ หรือการลักขโมยสิทธิ์ของผู้ดูแลอุปกรณ์หรือเจ้าของอุปกรณ์ในการเปลี่ยนรหัสผ่านเพื่อปลดล็อคหน้าจอ เป็นต้น

Ransomware ที่ได้มีการพัฒนาขึ้นเพื่อแพร่กระจายบนระบบปฏิบัติการ Android ก็มีหลายสายพันธุ์ เช่น

• Android defender

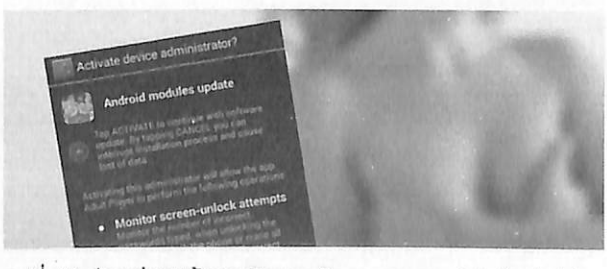
ตรวจพบครั้งแรกในปี 2013 แต่ลักษณะของโปรแกรมที่ปลอมตัวว่าเป็น Anti-virus ซึ่งกล่าวได้ว่าเป็น ransomware ตัวแรกที่พุ่งเป้าที่ผู้ใช้งาน Android โดยหน้าจอจะเตือนผู้ใช้งานที่ตกเป็นเหยื่อว่ากำลังเผชิญกับ Application ที่มีผลต่อความเสถียรของระบบโดยโปรแกรม ransomware ตัวนี้จะเสแสร้งว่ากำลังสแกนอุปกรณ์อยู่แล้วจะแสดงชื่อไฟล์ที่อยู่บนโทรศัพท์หรืออยู่ในหน่วยความจำ Memory Card เพื่อให้ดูสมจริง เพื่อเป็นการชวนเชื่อและชี้ชวนให้เหยื่อยอมจ่ายเงินเพื่อซื้อโปรแกรมต่อต้านมัลแวร์ ซึ่งในขั้นแรกผู้ใช้งานที่ตกเป็นเหยื่อมีทางเลือกสองทางคือการออกจากโปรแกรมและไม่ใส่ใจข้อความเตือนหรือปฏิเสธการใช้บริการของโปรแกรมต้านมัลแวร์ปลอม แต่ถ้าผู้ใช้งานปฏิเสธที่จะใช้งานหรือตกเป็นเหยื่อก็มักจะถูกยกระดับการข่มขู่ขึ้นไปอีก เช่น การแสดงหน้าจอด้วยสื่อลามกอนาจารหรือมีการล็อคหน้าจอโดยที่ผู้ใช้งานไม่สามารถที่จะปลดล็อคได้จนกว่าจะยอมจ่ายค่าไถ่ตามจำนวนที่ ransomware ระบุ (แสดงในรูปที่ 9)

รูปที่ 9 หน้าจอ Android Defender (www.thehackernews.com)

โดยหากที่ผู้ใช้งานตอบรับและยินดีใช้บริการจะถูกเรียกค่าใช้จ่ายเป็นเงิน $89.99 และถ้าหากผู้ใช้งานจ่ายด้วยบัตรเครดิตก็จะเป็นอันตรายมากเพราะว่าข้อมูลบนบัตรเครดิตก็จะถูก ransomware ตัวนี้เก็บไว้เป็นข้อมูลในการข่มขู่และเรียกค่าไถ่ในอนาคตได้เช่นกัน

• Ransomware กับสื่อลามกอนาจาร (Porno-ransomware)

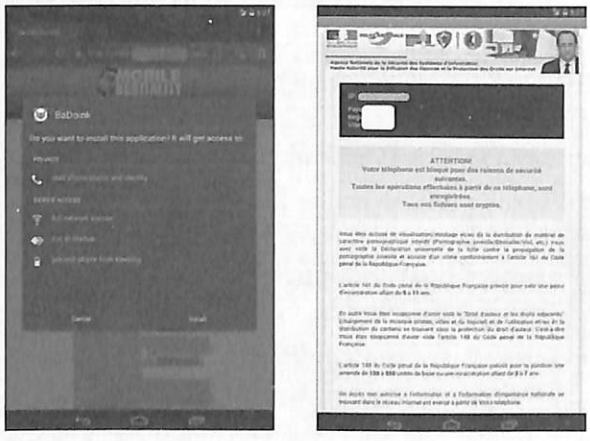
ransomware ประเภทนี้มีการใช้สื่อลามกอนาจารหรือสื่อปลุกใจต่างๆ บังหน้าและในขณะเดียวกันก็ตัดการทำงานของระบบด้วยการล็อคหน้าจอ ซึ่ง ransomware ประเภทนี้เคยปรากฏในลักษณะของ Mobile App ที่เชื่อมต่อกับเว็บไซต์ที่มีคลิปวีดีโอลามกอนาจารแบบต่างๆ ซึ่งเมื่อใดที่ ransomware ปรากฏตัวขึ้นจะแสดงให้ผู้ใช้งานเห็นหรือเตือนผู้ใช้งานว่าจำเป็นต้องตรวจเช็คไวรัสและมีปุ่มให้ผู้ใช้งานเลือกตกลงโดยและจะมีการใช้หน้าจอของโปรแกรมต้านไวรัสที่ทำปลอมขึ้น หรือแอบอ้างจากโปรแกรมต้านไวรัสที่มีอยู่จริง หากผู้ใช้งานตกเป็นเหยื่อและยอมตกลงให้ ransomware ทำการสแกนระบบ ransomware ก็จะแสดงผลบนหน้าจอว่าระบบกำลังตกอยู่ในภาวะอันตรายและต้องทำการซื้อซอฟท์แวร์ต้านไวรัสเวอร์ชั่นสูงหรือเวอร์ชั่นพิเศษเพื่อเพิ่มความปลอดภัยให้กับระบบ (แสดงในรูปที่ 10)



รูปที่ 10 ตัวอย่างหน้าจอ Porno Ransomware บน Android (www.thestack.com)

- **Police Ransomware**

Ransomware แบบล็อคหน้าจอมีการแพร่ระบาดมานานบนระบบปฏิบัติการ Windows โดยจะแสดงหน้าจอเป็นหน้าจอสีฟ้าหรือเป็นข้อความเตือนจากระบบปฏิบัติการ Windows ซึ่ง Police ransomware ก็ใช้หลักการเดียวกันคือเป็นการล็อคหน้าจอไม่ให้ผู้ใช้งานสามารถเข้าถึงระบบได้ และมีการแอบอ้างว่าสาเหตุที่หน้าจอถูกล็อคเนื่องจากหน่วยงานด้านกฎหมาย เช่น หน่วยงานตำรวจได้ทำการล็อคหน้าจอเนื่องจากตรวจพบเนื้อหาที่ขัดต่อหรือละเมิดกฎหมายบนอุปกรณ์พกพาหรือการใช้อุปกรณ์ในทางที่ฝ่าฝืนกฎหมาย เช่น การดาวน์โหลดโปรแกรมที่เป็นการละเมิดทรัพย์ลิขสิทธิ์ (แสดงในรูปที่ 11) ซึ่งในบางครั้ง ransomware ก็จะมีการแสดงข้อกฎหมายที่เกี่ยวข้องเพื่อเพิ่มความน่าเชื่อถือ ทำให้ผู้ตกเป็นเหยื่อตกอยู่ในความกลัวและก็มีการเสนอแนะเพื่อหลีกเลี่ยงการถูกการทางกฎหมายหรือการดำเนินคดีด้วยการจ่ายค่าธรรมเนียมซึ่ง police ransomware จะมีการทำงานร่วมกันกับระบบ GPS หรือ IP-Base geolocation เพื่ออ้างถึงพิกัดตำบลที่อยู่ของผู้ใช้งานและกฎหมายที่เกี่ยวข้องกับพื้นที่นั้นๆ เพื่อสร้างความเชื่อถือให้ผู้ตกเป็นเหยื่อยอมจำนนและคิดว่าตนฝ่าฝืนกฎหมายจริง ซึ่งมัลแวร์ประเภท Police ransomware ถูกตรวจพบครั้งแรกในปี 2014



รูปที่ 11 หน้าจอ Police Ransomware บน Android (www.thehackernews.com)

- **Simplocker**

ตรวจพบครั้งแรกในปี 2014 ในลักษณะของ ransomware ประเภทเข้ารหัสไฟล์ (Crypto) ที่แพร่ระบาดอย่างกว้างขวางบนระบบปฏิบัติการ Windows มาก่อนภายใต้ชื่อต่างๆ เช่น Crypto Locker Cryptowall CTB-Locker หรือ TorrentLocker มัลแวร์ประเภทนี้จะทำการแสดงข้อมูลและสแกนไฟล์ต่างๆ และทำการเข้ารหัสไฟล์ Simplocker จะทำการลวงผู้ใช้งานให้ตกเป็นเหยื่อโดยการแสดงตนหรือพรางตัวให้ดูเหมือนเป็น Application ที่เป็นที่นิยมทั่วไป (แสดงในรูปที่ 12) ซึ่งเป็นเทคนิคที่นิยมใช้บน Android มัลแวร์ โดยพรางตนเป็น Application ที่เป็นวีดีโอสื่อลามกอนาจาร เกมส์ออนไลน์ หรือ Application ทั่วไปเช่น Flash Player เป็นต้น

รูปที่ 12 หน้าจอ Simplocker Ransomware บน Android ในภาษารัสเซีย(www.quickheal.com)

Lockerpin

ตรวจพบครั้งแรกในปี 2015 โดยผู้สร้าง ransomware ได้ยกระดับก้าวขึ้นไปอีกขั้นโดยที่ผู้ใช้งานที่ตกเป็นเหยื่อของ ransomware แบบล็อคหน้าจอ ซึ่งการที่จะหลุดรอดจากการตกเป็นเหยื่อสามารถทำได้โดยการตั้งค่ารหัสผ่านปลดล็อคหน้าจอใหม่หรือทางเลือกสุดท้ายคือการ Factory Reset อุปกรณ์ ซึ่งจะลบข้อมูลเดิมทั้งหมดบนอุปกรณ์ออกไป เทคนิคที่ Lockerpin ใช้ในการล็อคหน้าจอเป็นเทคนิคอย่างง่ายซึ่งอาศัยข้อได้เปรียบจากกลไกในการล็อคหน้าจอด้วยรหัสผ่านของระบบปฏิบัติการ Android ที่สามารถตั้งรหัสผ่านบนอุปกรณ์แม้ว่าจะไม่เคยตั้งรหัสผ่านมาก่อนหรือเปลี่ยนรหัสผ่านในการปลดล็อคหน้าจอด้วยตนเอง ransomware ชนิดนี้ถือกำเนิดขึ้นในประเทศในกลุ่มยุโรปตะวันออกและรัสเซีย แต่ในปัจจุบันได้แพร่กระจายเข้าสู่สหรัฐอเมริกาที่มีเศรษฐกิจดีกว่าจึงสามารถเรียกร้องค่าไถ่และให้ผลตอบแทนได้ดีกว่า

การปกป้องตนให้ปลอดภัยจาก ransomware

ไม่มีอุปกรณ์เพื่อความปลอดภัยใดๆ ที่ได้ผล 100% ตลอดเวลา แต่วิธีที่ดีที่สุดคือการตื่นตัวและปกป้องอุปกรณ์และระบบอยู่ตลอดเวลาในระดับต่างๆ เพื่อป้องกันข้อมูลในระบบ ด้วยเทคนิคและกลยุทธ์ต่างๆ เช่น การใช้ Firewall web filtering การติดตั้งโปรแกรมต้านมัลแวร์ ผนวกกับความตระหนักถึงภัยและความเสียหายอันเกิดจาก ransomware ที่อาจเกิดขึ้น เช่น

- **การสำรองข้อมูลตลอดเวลา**

ในกรณีที่สามารถกอบกู้ข้อมูลได้อย่างง่ายดายและรวดเร็วนั้น ผลกระทบจาก ransomware ประเภท lock screen อาจไม่มีผลมากเท่าใด แต่ในกรณีที่เป็น ransomware แบบเข้ารหัสไฟล์อาจมีผลกระทบมากดังนั้นจึงควรที่จะสำรองข้อมูลไว้ภายนอกและหากเป็นระบบการสำรองข้อมูลที่เชื่อมต่อกับระบบหลักเป็นการถาวรก็ควรที่จะมีการป้องกันโดยการตัดการเชื่อมต่อเมื่อการสำรองข้อมูล

แล้วเสร็จ เพื่อเป็นการป้องกันการแพร่กระจายของ ransomware ที่อาจเข้าไปถึงระบบข้อมูลสำรองด้วย ทั้งนี้การสำรองข้อมูลต่างจากการทำสำเนาข้อมูล โดยที่การทำสำเนาข้อมูลที่ถึงแม้ว่าจะทำสำเนาเป็น 2 ชุดแต่หากเก็บไว้บนที่เดียวกันก็อาจได้รับผลกระทบจาก ransomware ได้ ดังนั้นการสำรองข้อมูลภายนอกจะมีความปลอดภัยจาก ransomware ได้มากกว่า

- **การอัพเดทซอฟต์แวร์ตลอดเวลาเพื่อลดช่องโหว่หรือจุดบกพร่อง**

ransomware บางประเภทอาศัยช่องโหว่หรือจุดบกพร่องด้านความปลอดภัยของซอฟต์แวร์และแอพพลิเคชั่นต่างๆ ดังนั้นจึงมีความจำเป็นที่ต้องมีการอัพเดทซอฟต์แวร์และแอพพลิเคชั่นต่างๆ ให้เป็นปัจจุบันอยู่เสมอเนื่องจากบรรดาผู้ผลิตซอฟต์แวร์และแอพพลิเคชั่นเหล่านี้ต่างก็ตระหนักถึงความเสียหายของมัลแวร์ในรูปแบบต่างๆ ที่มีการยกระดับความรุนแรงและเพิ่มความซับซ้อนขึ้นอย่างต่อเนื่อง ดังนั้นผู้ผลิตและผู้พัฒนาซอฟต์แวร์ก็มีการแก้ไขช่องโหว่และจุดบกพร่องอย่างต่อเนื่องเช่นกัน ซึ่งเป็นสิ่งที่ผู้ใช้งานต้องมีการอัพเดตอยู่เสมอและในบางกรณีอาจมีความจำเป็นต้องลบซอฟต์แวร์เวอร์ชั่นเก่าออกก่อนเพื่อลงซอฟต์แวร์เวอร์ชั่นใหม่ที่มีความเสถียรมากกว่าและสามารถปิดช่องโหว่ของระบบได้ดีกว่า

- **การอัพเดทโปรแกรมต้านมัลแวร์ให้เป็นปัจจุบัน**

เช่นเดียวกับวิวัฒนาการของมัลแวร์และ ransomware ที่มีมาอย่างต่อเนื่อง anti-malware ก็ต้องมีการพัฒนาอย่างต่อเนื่องให้ทัดเทียมกัน ดังนั้น antimalware ที่ขาดการอัพเดทจะมีความล้าสมัยและไม่สามารถรับรู้และป้องกันมัลแวร์ใหม่ๆ ได้ ดังนั้นจึงมีความจำเป็นอย่างยิ่งที่ต้องอัพเดทให้เป็นปัจจุบันอย่างสม่ำเสมอเช่นกัน

- **การตั้งรหัสผ่านให้มีความซับซ้อนพอสมควร**

การแพร่กระจายของมัลแวร์ส่วนหนึ่งเกิดขึ้นจากพฤติกรรมของผู้ใช้งาน ซึ่งหนึ่งในสาเหตุนั้นคือรหัสผ่านที่มีความอ่อนแอหรือง่ายต่อการลักจำ เช่น รหัสผ่านที่เป็นคำสามัญ รหัสผ่านที่สามารถจดจำลอกเลียนแบบได้ง่าย หรือรหัสผ่านเดียวที่ใช้กับหลายๆ บัญชีผู้ใช้งาน ดังนั้นรหัสผ่านที่ใช้ในการเข้าถึงระบบทั้งระบบปกติและระบบบนอุปกรณ์พกพาอาจจะไม่จำเป็นต้องแตกต่างกันมาก แต่ควรจะเป็นรหัสผ่านที่มีความซับซ้อนอยู่พอสมควรที่ยังคงง่ายต่อการจดจำแล้วควรมีการเปลี่ยนรหัสผ่านอยู่เสมอตามช่วงเวลาที่เหมาะสมหรือเมื่อต้องสงสัยว่ามีการถูกแอบอ้างหรือมีรายงานในการพยายามการเข้าระบบโดยไม่ได้รับอนุญาต

- **การให้ความระมัดระวังเป็นพิเศษกลับอีเมล์ที่น่าสงสัย**

E-mail ที่มาจากผู้ส่งที่ต้องสงสัยหรือไม่รู้จักโดยเฉพาะอย่างยิ่งอีเมล์ที่มาพร้อมเอกสารแนบ หรือ Link ต่างๆ จากบุคคลหรือจากหน่วยงานที่ไม่รู้จักไม่คุ้นเคยก็เป็นช่องทางในการแพระกระจายของมัลแวร์ได้เช่นกัน ดังนั้นจึงไม่ควรไม่เปิดอีเมล์เหล่านั้นหรือการตั้งค่าให้คัดกรองอีเมล์เหล่านั้นออกจากอีเมล์หลัก ซึ่งอีเมล์ต่างๆ เหล่านี้อาจมาพร้อมสิ่งที่เป็นอันตรายต่อระบบเช่น มัลแวร์ ransomware และ virus ต่างๆ ซึ่งการแพร่กระจายของมัลแวร์ผ่านทางอีเมล์มีมานานและยังคงมีอยู่ต่อไปด้วยกลยุทธ์ที่แตกต่างกันตามยุคสมัย ซึ่งผู้ใช้งานยังคงต้องยึดถือแนวทางในการป้องกันเช่นเดิม คือ การไม่เปิดอ่านอีเมล์ต้องสงสัย เช่น อีเมล์ที่ส่งมาจากบุคคลหรือผู้ส่งที่ไม่คุ้นเคย หรืออีเมล์ที่ส่งมาบ่อยจนผิดสังเกตหรือมีข้อความชี้นำในเชิงโฆษณาหรือชวนเชื่อในรูปแบบต่างๆ ที่เกินความจริง

บทสรุป

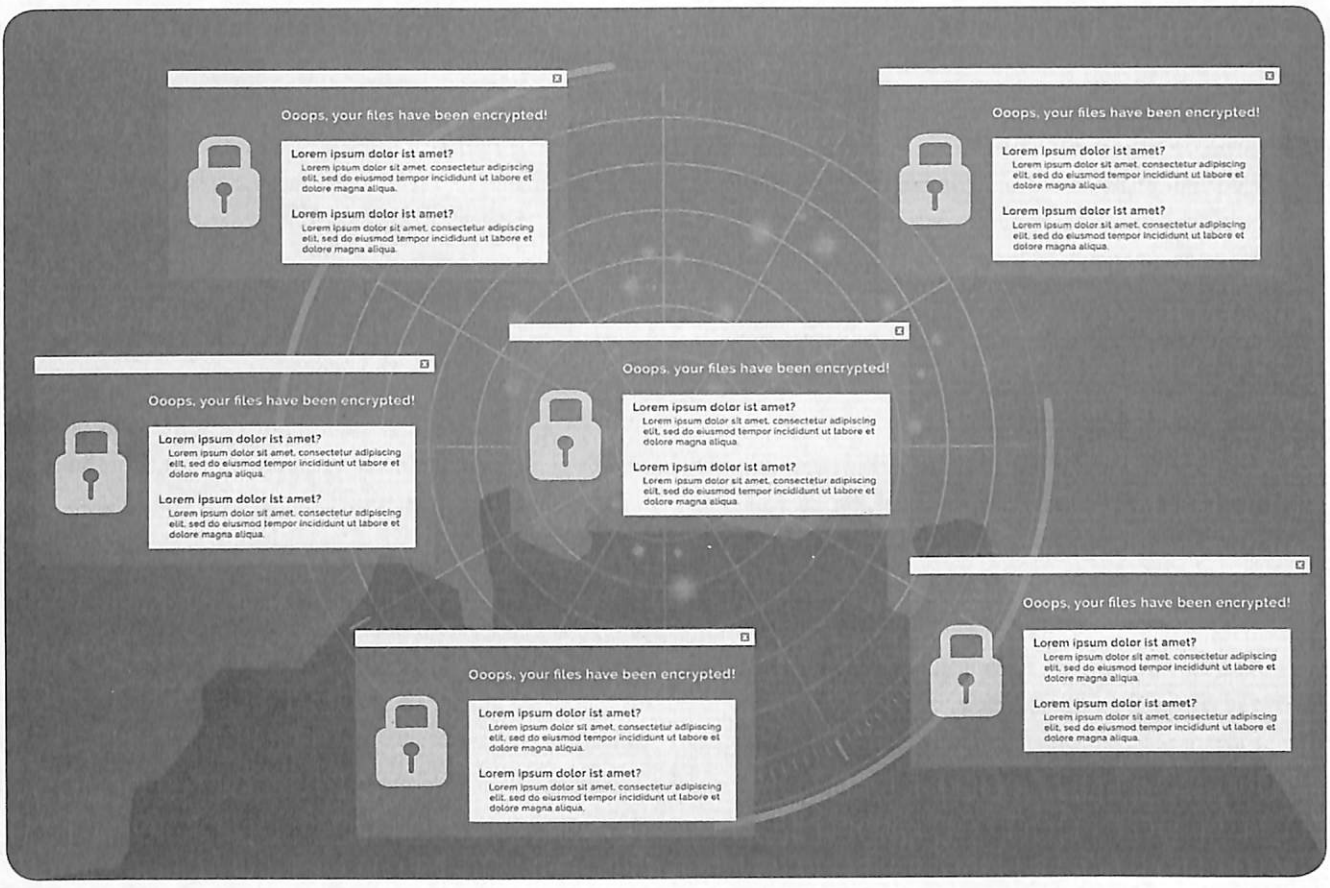
การระบาดของ WannaCry หรือ WannaCrypt สร้างความตระหนักถึงพิษภัยและความเสียหายจาก ransomware ให้กับทั้งโลกอย่างจริงจังอีกครั้ง แม้ว่า ransomware จะไม่ใช่อุบัติการณ์ใหม่และเป็นมัลแวร์ประเภทหนึ่งซึ่งผู้พัฒนามีจุดประสงค์ร้ายโดยการสร้างความเสียหายหรือสร้างความชะงักงันให้กับระบบ ตามด้วยการเรียกค่าไถ่ ซึ่งนับเป็นอาชญากรรมทางเศรษฐกิจประเภทหนึ่ง กลไกการทำงานของ ransomware ทั้ง 2 ประเภทหลักคือการเข้ารหัสไฟล์และการล็อคหน้าจอโดยมีจุดประสงค์เดียวกันคือการสกัดกั้นขัดขวางผู้ใช้งานให้เข้าถึงระบบหรือข้อมูลได้จนกว่าจะชำระค่าไถ่ตามจำนวนที่เรียกร้อง ซึ่งกลไกในการเรียกร้องค่าไถ่ก็มีทั้งการข่มขู่ให้เกิดความกลัวหรือการชวนเชื่อให้จ่ายเงินเพื่ออัพเดทระบบปฏิบัติการหรือซื้อซอฟต์แวร์เพื่อป้องกันหรือแก้ไขระบบซึ่งล้วนแล้วแต่เป็นสิ่งที่ปลอมแปลงขึ้นโดยไม่ได้มีตัวตนหรือใช้งานได้จริงแต่อย่างใด และในปัจจุบันได้มีการแพร่ระบาดขึ้นสู่อุปกรณ์พกพาโดยเฉพาะอย่างยิ่งอุปกรณ์ที่ใช้ระบบปฏิบัติการ Android ซึ่งเป็นระบบปฏิบัติแบบรหัสเปิดหรือ open source ที่ในปัจจุบันยังมีใช้กันอย่างหลากหลายเวอร์ชั่นทั้งรุ่นเก่าที่กลไกการรักษาความปลอดภัยของระบบไม่มีการพัฒนาต่อแล้วและรุ่นใหม่ที่มีความเสถียรมากขึ้น ดังนั้นผู้ใช้งานบนอุปกรณ์พกพาที่ใช้ระบบปฏิบัติการ Android เวอร์ชั่นเก่าจึงพึงระมัดระวังเป็นอย่างยิ่ง

อย่างไรก็ตามความตระหนักและความไม่ประมาทของผู้ใช้งานยังคงมีบทบาทสำคัญในสถานการณ์ที่มีการระบาดของ ransomware เช่นนี้ ทั้งนี้เนื่องจาก ผู้พัฒนา ransomware อาศัยช่องโหว่ของพฤติกรรมผู้ใช้งานมาศึกษาเพื่อเป็นกลไกในการสร้างการแพร่ระบาดผ่านทางมัลแวร์ประเภทอื่น เช่น โทรจันหรือไวรัส ซึ่งถ้าหากผู้ใช้งานมีความตระหนักและมีความระมัดระวังในการใช้งานก็จะสามารถลดการแพร่ระบาดและความเสียหายของ ransomware ลงได้ และยังสามารถกระทำได้ด้วยตนเอง เพราะในปัจจุบันก็ยังไม่มีอุปกรณ์หรือโปรแกรมต้านมัลแวร์ที่ได้ผล 100 %

เรียบเรียงจาก

- Robert Lipovský, Lukáš Štefanko, Gabriel Braniša, The Risk of Andriod Ransomware, Eset document version 1.0., www.welivesecurity.com
- Drew Robb, Your Money of Your Life Files, whitepaper, KnowB4 Inc. 2016.
- CERT-MU, The WannaCry Ransomware, Whitepaper, The Computer emergency Response Team of Mauritius (CERT-MU), 2017.
- SWGfL, Ransomware White Paper, South West Grid for Learning Trust Ltd., October 2016.

■ เดอริค มันคี
นักกลยุทธ์ด้านความปลอดภัยเครือข่ายของโลกฟอร์ติการ์ดแล็ปส์



มุมมองจากฟอร์ติเน็ต: จะเกิดอะไรขึ้นหลังการโจมตี WannaCry ครั้งนี้

คำถามคือ ช่วงที่เลวร้ายที่สุดผ่านไปหรือยัง? หรือเรายังกำลังอยู่ในศูนย์กลางของพายุภัยคุกคาม?

เดอริค มันคี นักกลยุทธ์ด้านความปลอดภัยเครือข่ายของโลกที่ฟอร์ติการ์ดแล็ปส์อันเป็นส่วนหนึ่งของฟอร์ติเน็ตได้ให้ความเห็นหลังสถานการณ์การคุกคามของภัยแรนซัมแวร์เรียกค่าไถ่ Wanna Cry หรือ WCry ว่า Wanna Cry กลายเป็นข่าวใหญ่ทั่วโลก แต่ตอนนี้ได้แผ่วเบาลงแล้ว คำถามคือ ช่วงที่เลวร้ายที่สุดผ่านไปหรือยัง? หรือเรายังกำลังอยู่ในศูนย์กลางของพายุภัยคุกคาม?

ด้วยเหตุผลหลายประการ ฟอร์ติเน็ตเชื่อว่าวิกฤติ WannaCry ได้ลดลง เชื่อว่าช่องโหว่ดังกล่าว (SMB CVE 2017-0144) ได้ผ่านขีดสูงสุดของสถานการณ์ต่างๆ เนื่องจากเราผ่านช่วงประหลาดใจและสามารถป้องกันภัยไซเบอร์นี้ได้อย่างเต็มที่ ซึ่งเป็นความร่วมมือจากสมาชิกของหน่วยงานด้านกฎหมาย CERT และกลุ่มพันธมิตรด้านภัยไซเบอร์ (Cyber Threat Alliance) ที่ฟอร์ติเน็ตเป็นสมาชิกผู้ก่อตั้งอยู่ด้วย

หลังภัย WannaCry ข่าวลือว่า อาจจะมีภัยใหม่ เช่น Adylkuzz ที่จะคุกคามทั่วโลกนั้น เดอริคเห็นว่าบอทเน็ทประเภทที่สามารถพรางกายได้จะยากที่จะถูกตรวจจับ ซึ่งน่าจะทำการได้สำเร็จมากขึ้น แต่เมื่อเกิดการจู่โจมครั้งใหญ่ขึ้นของ WannaCry นี้ ทุกคนเริ่มตื่นตัวต่อการโจมตีครั้งต่อไป จึงทำให้องค์กรส่วนใหญ่ได้ปิดช่องโหว่เหล่านี้ลงแล้วและระแวดระวังเตรียมพร้อมต่อภัย WannaCry หรือภัยที่คล้ายคลึงกันมากขึ้น ทั้งนี้ ผู้ให้บริการโทรคมนาคมทั่วโลกได้เริ่ม

ปิดกั้นพอร์ต 445 เพื่อลดการแพร่กระจายของการใช้ประโยชน์จาก SMB ซึ่งจะเป็นอุปสรรคต่อภัย Adylkuzz มากยิ่งขึ้นเช่นกัน จะเห็นได้ว่า มาตรการป้องกันภัยเหล่านี้ จะทำให้ภัยการโจมตีที่เลียนแบบ WannaCry มีความอ่อนแอลงในขณะนี้

นอกจากนี้ ฟอร์ติเน็ตยังไม่เห็นข้อบ่งชี้ใดๆ ที่จะระบุว่าการโจมตีอื่นๆ เช่น Adylkuzz จะสร้างการโจมตีครั้งใหญ่ใดๆ แต่อย่างไรก็ตาม ไม่ได้หมายความว่าผู้สร้างมัลแวร์จะไม่สามารถหากลยุทธ์อื่นๆ เพื่อทำให้ Adylkuzz ประสบความสำเร็จได้อีก

ด้วยเซนเซอร์รักษาความปลอดภัยหลายล้านชุดที่มีอยู่ทั่วโลก ทำให้ทีมงานวิจัยด้านภัยคุกคามของฟอร์ติการ์ดแล็ปส์สามารถตรวจสอบและเข้าภัยคุกคามที่เกิดขึ้นได้ทั่วโลกที่เรียกว่า Global threat landscape ตัวอย่างเช่น ข้อมูลของฟอร์ติการ์ดแลบส์แสดงการโจมตีและการตรวจจับภัยจำนวนมากซึ่งนำไปสู่การแพร่กระจายภัยที่รุนแรง ซึ่งเกิดหลังจากเมื่อภัยคุกคามพบองค์กรที่มีมาตรการป้องกันหย่อนลง (ได้พบ ในกิจกรรมที่ CVE-2017-0144 เพิ่มขึ้น 340% อันเป็นช่องโหว่ DoublePulsar ที่อยู่ในทูลส์วินโดวส์ SMB ที่เป็นจุดใช้ในการแพร่กระจาย WannaCry) ตั้งแต่นั้น เราได้เห็นการลดลงของการโจมตีอย่างต่อเนื่อง

เนื่องจากเกิดการโจมตีสูงในช่วงวันศุกร์ที่ 12 และวันเสาร์ที่ 13 พฤษภาคม เราจึงสังเกตเห็นการเติบโตที่ลดลงอยู่ที่ -44% ภายในวันอาทิตย์ที่ 14 พฤษภาคม และตั้งแต่นั้นมา กิจกรรมการโจมตีจากทั่วโลกลดลงครึ่งหนึ่งทุกวันเป็น 53% นับตั้งแต่วันที่เกิดภัยสูงที่สุด ที่มีตัวเลขการโจมตีในหลักแสนครั้งต่อวัน ลงมาเป็นหลักหมื่นครั้งต่อวัน และฟอร์ติเน็ตคาดว่าแนวโน้มดังกล่าวจะยังเป็นระดับนี้ต่อไป โดยทั่วไปแล้ว ระบบส่วนใหญ่ที่อ่อนแอจะได้ถูกโจมตีหรือกลับกันคือ ได้รับการป้องกันให้ดีขึ้นแล้ว

ดังนั้น โอกาสที่จะถูกโจมตีโดย WannaCry (และ AdyllKuzz) จะลดลงอย่างมีนัยสำคัญไปแล้ว ซึ่งหมายความว่าการโจมตีที่คล้ายกันจะกลับกลายเป็นว่าเกิดขึ้นช้าไปแล้ว เพราะเกิดกระบวนการตรวจจับและการตอบโต้ภัยที่แข็งแกร่งแล้ว ภัยต่างๆ คงไม่น่าจะสร้างความรุนแรงได้อีกในเร็วๆ นี้

หากถามว่า WannaCry ประสบความสำเร็จอย่างมากไหม? คำตอบคือ เราจะวัดความสำเร็จนั้นอย่างไร ทั้งนี้ WannaCry ได้พิสูจน์แล้วว่าภัยการโจมตีแบบ Zero day attacks (ภัยคุกคามที่เกิดจากการใช้ประโยชน์จากช่องโหว่ ที่ยังไม่มีใครรู้ แม้แต่ทีมผู้พัฒนา) นั้นสามารถประสบความสำเร็จได้อย่างดุเดือด แต่ครั้งนี้ล้มเหลวในแง่ของการเรียกค่าไถ่ จากผลการวิเคราะห์พบว่า ไม่มีการจ่ายเงินจำนวนมากที่ Bitcoin ในขณะที่ WannaCry สามารถสร้างผลกระทบอย่างมากและรวดเร็ว แต่ก็ไม่ได้หมายความว่าจะเป็นบอทเนทที่ใหญ่ที่สุดเท่าที่เราเคยเห็นกันมา

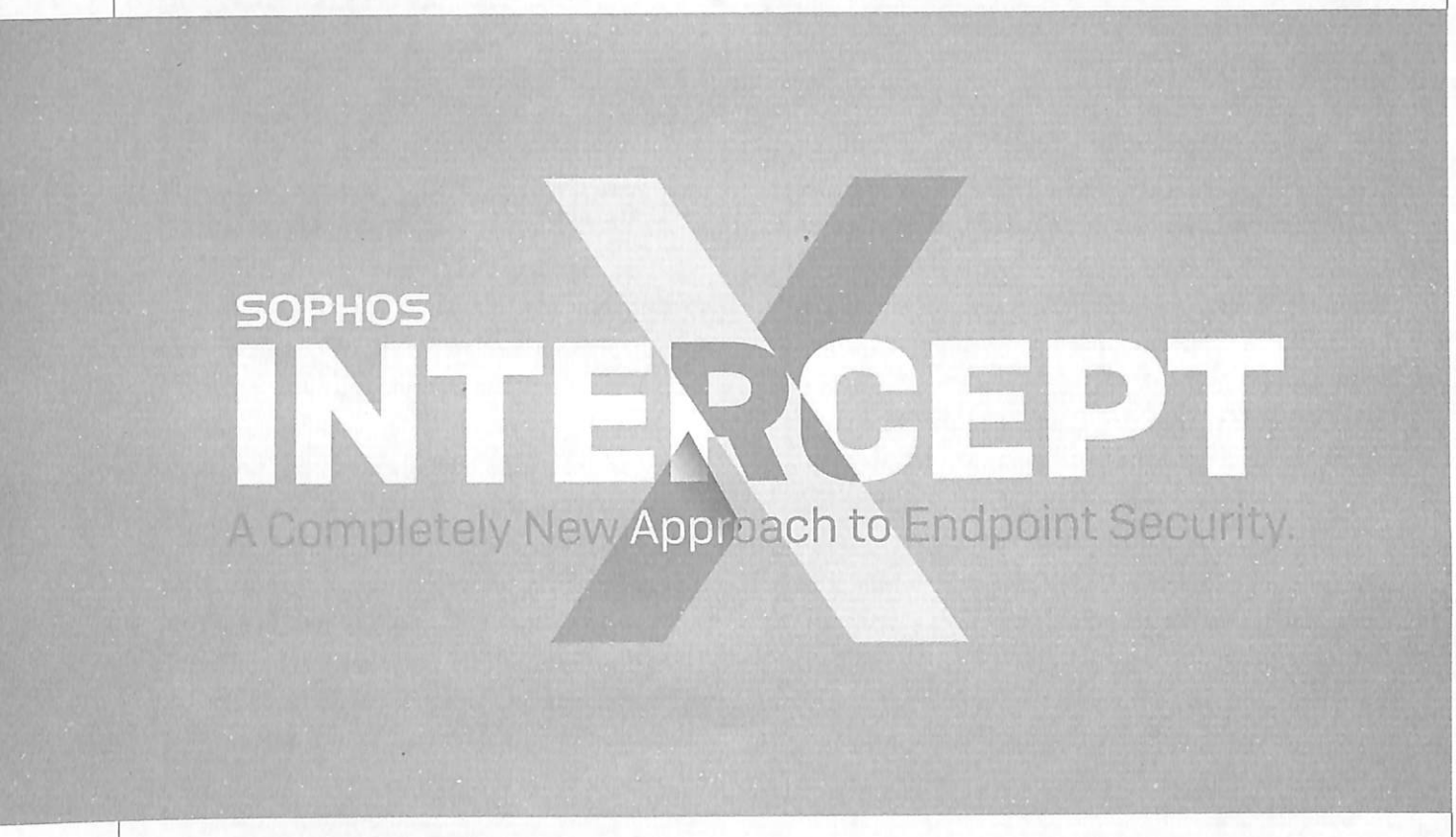
ในแง่ของบอทเนท (Ransomware bots) ทางกลุ่มพันธมิตรด้านภัยไซเบอร์ (Cyber Threat Alliance) ได้ตรวจสอบพบความพยายามเรียกค่าไถ่โดย CryptoWall v3 ประมาณกว่า 400,000 ครั้ง ในปี 2015 ซึ่งมากกว่าเกือบจะเป็นสองเท่าที่เกิดโดย WannaCry นอกจากนี้ สำหรับประเภทโทรจันหรือบอทเนทแบบเงียบนั้น ฟอร์ติเน็ตได้ตรวจพบผู้ที่ตกเป็นเหยื่อการติดไวรัส (Mariposa botnet) มากกว่า 15 ล้านราย

บอทเนทขนาดใหญ่เหล่านี้มีพื้นผิวโจมตีที่ใหญ่ขึ้นเนื่องจากเกิดการใช้งาน CaaS (Crime as a Service หรืออาชญากรรมในฐานะผู้ให้บริการ) มากขึ้น ร่วมกับกลุ่มอาชญากรไซเบอร์แบล็กแฮ็ตที่ต้องการใช้ความเชี่ยวชาญของตนเองเจาะระบบในทางที่ผิด

อะไรต่อไป หลังการโจมตี WannaCry? ทั่วโลกกำลังให้ความสนใจกับภัยและกลุ่มแฮกเกอร์ที่เรียกว่า ShadowBroker exploit kit ในขณะที่กลุ่มอาชญากรไซเบอร์แบล็กแฮ็ตอาจจะมุ่งไปที่ DarkNet (เว็บไซต์ที่ถูกซ่อนลึก) เพื่อหาช่องโหว่ใหม่ๆ ที่ไม่มีใครสนใจ ดังนั้นองค์กรควรติดตามและพิจารณาการป้องกันเครือข่ายของท่านตามการคาดการณ์ของปี พ. ศ. 2560 ได้ที่ www.fortinet.com เชื่อว่าเราน่าจะเห็นบอทเนทที่ใหญ่ที่สุดในโลก ซึ่งจะมีผู้ได้รับผลกระทบมากกว่า 15 ล้านราย ทั้งนี้ เราคาดว่าจากการใช้ประโยชน์ของไอโอที จะส่งผลให้มีการเรียกค่าไถ่สำหรับอุปกรณ์ไอโอที บริการข้อมูลสำคัญและทรัพย์สินทางปัญญาอื่น ๆ นอกจากนี้ น่าจะเกิดกิจกรรมด้านอาชญากรรม เช่น การเก็บรวบรวมข้อมูล การโจมตีที่กำหนดเป้าหมาย และการคุกคามอื่นๆ ตามมาอีกด้วย

ติดตามข่าว WannaCry อัปเดทล่าสุดตลอดเวลาได้ที่เว็บไซต์ https://fortinet.uberflip.com/wannacry-central

■ ธิติมา มานิตพร
Business Director
บริษัท อี หริ่ง คอนซัลแตนท์ส จำกัด



ป้องกันดีกว่าแก้ไข วิธีปิดช่องโหว่ที่ทำให้เราต้องเผชิญกับ Ransomware

ความล้มเหลวของระบบรักษาความปลอดภัย ช่องโหว่ที่ทำให้เราต้องเผชิญ Ransomware ดังนั้นการป้องกันจึงเป็นคำตอบที่ดีที่สุดในตอนนี้ ที่เราจะไม่ต้องเป็นเหยื่อของไวรัสเรียกค่าไถ่เหล่านี้

ขณะนี้ ทั่วโลกต่างพากันตื่นตัวอย่างมาก จากการที่มีหน่วยงานสำคัญของหลายประเทศ และเครื่องคอมพิวเตอร์ส่วนบุคคล ที่แพร่ระบาดไปแล้วร้อยกว่าประเทศทั่วโลก ต้องเจอกับ Ransomware ไวรัสเรียกค่าไถ่ ในชื่อของ Wannacry การทำงานของ Wannacry หรือที่เรารู้จักในชื่อของ WannaCry, WCry, WanaCrypt, WanaCrypt0r และ Wana DeCrypt0r เป็นภัยคุกคาม ที่เมื่อผู้ติดกับไวรัสแฮกเกอร์ตัวนี้ จะโดนเข้ารหัสไฟล์ และการแก้ไขเปลี่ยนแปลงสกุลไฟล์ ให้เป็น .wnry, .wcry, .wncry and .wncrypt. ความสูญเสียที่เกิดขึ้น คือการสูญเสียข้อมูลสำคัญนั้นไป และเหยื่อหลายรายต้องสูญเสียเงินที่ทางแฮกเกอร์เรียกร้องไปพร้อมๆ กับข้อมูลเหล่านั้นด้วย

การปรากฏตัวต่อสาธารณชนครั้งแรกของ Ransomware ในชื่อของ CryptoLocker นั้นมีมาตั้งแต่ปี 2013 โดยปกติแล้ว ไวรัสเรียกค่าไถ่ หรือ Ransomware เหล่านี้ จะติดมากับการคลิกไฟล์

ที่นำพาเหยื่อ ให้มีการติดตั้งไฟล์ไวรัสเรียกค่าไถ่ หรือเกิดจากการเปิดอีเมล์ ที่มีการแนบไฟล์ โดยเมล์ดังกล่าว จะเป็นเมล์ที่มีหน้าตาเหมือนเมล์ปกติที่รับได้ทั่วไปทุกประการ อีกทั้งมาจากผู้ส่งที่เหมือนมีความคุ้นเคยอีกด้วย โดยไฟล์ที่แนบมา จะเป็นไฟล์สกุลทั่วไปที่ผู้ใช้ปกติ ใช้ในการรับส่งงานต่างๆ กับลูกค้า หรือเพื่อนร่วมงาน เช่น PDF, Word, Excel เป็นต้น โดยที่ผู้ใช้ทั่วไปอาจไม่สามารถจำแนกได้ว่า นี่จะเป็นไฟล์ล่อลวงให้ไปสู่การติดตั้งไวรัสเรียกค่าไถ่บนเครื่องคอมพิวเตอร์ของตัวเอง โดยจะทำการเข้ารหัสไฟล์สำคัญต่างๆ ของเหยื่อ ทำให้ไม่สามารถเปิดใช้งานได้ และมีการเรียกร้องค่าไถ่ ในการเปิดไฟล์ที่เข้ารหัสนั้น โดยปัจจุบัน ยังไม่สามารถมีใครถอดรหัสออกเองได้เลย สำหรับ Wannacry นั้นมีความรุนแรงกว่า Ransomware ทั่วไป เพราะมันสามารถแพร่กระจายไปยังเครื่องคอมพิวเตอร์อื่นๆ ภายในองค์กรได้ด้วย

ในทันทีที่มีการคลิกยังไฟล์ที่มีไวรัสเรียกค่าไถ่นี้ หากมีการเชื่อมต่ออินเทอร์เน็ต ไฟล์นี้จะส่งสัญญาณไปหาเซิรฟเวอร์ของแฮกเกอร์ และทำการเข้ารหัสไฟล์สำคัญของเราทั้งหมดในเครื่องคอมพิวเตอร์ หากเป็นข้อมูลสำคัญ ผู้ใช้จะสูญเสียไฟล์ไปทั้งหมด และหน้าจอวินโดวส์จะขึ้นข้อความ เป็นข้อตกลงกับเหยื่อในการเรียกค่าไถ่ ตามจำนวนเงินที่ต้องการ เพื่อให้ได้รับไฟล์ข้อมูลกลับคืน โดยจากสถิติไม่ว่าจะมีการส่งเงินไปยังแฮกเกอร์หรือไม่ก็ตาม ยังไม่มีใครได้รับข้อมูลสำคัญในเครื่องคอมพิวเตอร์คืนแบบสมบูรณ์เลย และจนปัจจุบันเรายังไม่พบวิธีการแก้ไข จากการเข้ารหัสไฟล์ที่เกิดจากไวรัสเรียกค่าไถ่เหล่านี้เลย

การป้องกันจึงเป็นคำตอบที่ดีที่สุดในตอนนี้ ที่เราจะไม่ต้องเป็นเหยื่อของไวรัสเรียกค่าไถ่เหล่านี้

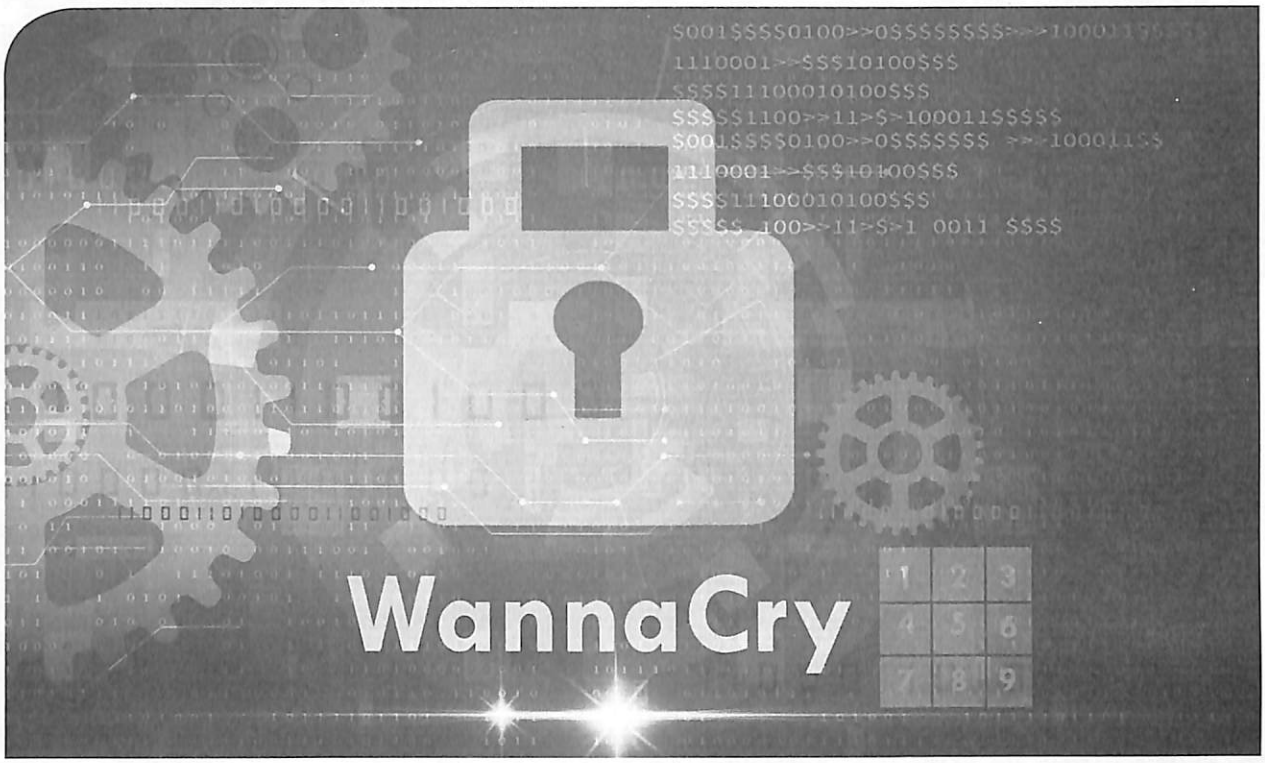
คำแนะนำสำหรับการป้องกันข้อมูลสำคัญของเรา ก่อนเจอไวรัสเรียกค่าไถ่ หรือ Ransomware เหล่านี้

1. มีการ back up ข้อมูลสำคัญต่างๆ ไว้หลายแห่ง เพื่อให้ยังคงมีข้อมูลสำคัญนั้นไว้เรียกใช้งาน ในกรณีที่มีต้องเผชิญกับ Ransomware
2. การอัพเดท Window ซึ่งเป็นประกาศจากไมโครซอฟท์ส่วนของการไม่สนับสนุนการอัพเดท Window XP จะเห็นได้ว่าช่วงที่มีการแพร่ระบาดและเหยื่อที่เจอ Wannacry รุนแรงมาก เพราะยังคงมีหลายองค์กร มีผู้ใช้ที่ยังใช้ Window XP อยู่ ซึ่งทางไมโครซอฟต์ไม่สนับสนุนการดูแลแล้ว
3. การติดตั้งไฟร์วอล หรือ แอนตี้ไวรัส ที่มีคุณสมบัติในการป้องกัน Ransomware ซึ่งจะเห็นได้ว่า เหยื่อหลายรายที่ติดตั้งแอนตี้ไวรัส ก็ยังติดไวรัสเรียกค่าไถ่เหล่านี้ นั่นเพราะภาวการณ์ปัจจุบัน แค่ไฟร์วอล หรือแอนตี้ไวรัสแบบดั้งเดิมนั้นไม่ เพียงพอ จำเป็นต้องมีแอนตี้ไวรัสที่มีคุณสมบัติ จัดการแบบ signatureless หรือ zero hour การมี Anti-ransomware Anti-Exploit ต่างๆ รวมทั้งการมีอัลกอลิทึมในการจัดการภัยคุกคามที่ยังไม่ปรากฏเป็น signature แบบวิธีการของแอนตี้ไวรัส
4. แม้จะมีการติดตั้งแอนตี้ไวรัสแล้ว มีความจำเป็นอย่างมากที่จะต้องมีการอัพเดทโปรแกรมอยู่ตลอด หากมีการซื้อแอนตี้ไวรัส หรือ แอนตี้แฮกเกอร์ต่างๆใช้งาน ต้องยังเป็นโปรแกรมที่ยังคงอัพเดทอยู่เสมอ เพราะไวรัส และแฮกเกอร์มีการสร้างขึ้นใหม่ทุกวัน
5. เจอเมล์ต้องสงสัย ไม่เปิด ไม่คลิกไฟล์แนบ และไม่ตั้งค่าการเปิดรับไฟล์แนบอัตโนมัติ ก่อนจะมั่นใจว่าไฟล์แนบทางเมล์นั้นมีความปลอดภัย
6. ไม่เปิดหน้าล็อคอินใช้งานใดๆ ทิ้งเอาไว้ หากไม่ได้มีการเข้าใช้งาน ควรทำการล็อคเอ้าท์ออกก่อนเสมอ

หากการป้องกันแบบจัดการด้วยตัวเอง นั้นยุ่งยาก หรือยังไม่รัดกุมพอ ปัจจุบันก็มีโปรแกรมความปลอดภัย อย่าง Sophos Intercept X ที่ช่วยป้องกันเรื่องของภัยคุกคาม ที่เพิ่มเติมนอกเหนือจากการใช้แค่แอนตี้ไวรัส ให้การตรวจจับการโจมตีแบบ Zero-day ที่แน่นอนว่า แอนตี้ไวรัสอย่างเดียวไม่เพียงพอ เพราะภัยคุกคามอย่างพวก ransomware หรือเทคโนโลยี exploit นี้ เข้าถึงเหยื่อก่อนที่แอนตี้ไวรัส จะสามารถป้องกันได้ โดยผ่านอัลกอริทึมขั้นตอนของ Sophos Intercept X ที่จะป้องกันการบุกรุก ยับยั้งและกำจัดมัลแวร์ หรือแรนซัมแวร์ต่างๆ เหล่านี้ให้หมดไปได้ นอกจากนี้ ยังสามารถทำ Root Cause Analysis เพื่อวิเคราะห์ต้นสายปลายเหตุของภัยคุกคาม ที่ช่วยให้แอดมิน มองเห็นมัลแวร์ ภัยคุกคามต่างๆ ที่เข้ามาในระบบ และสามารถนำมาปรับใช้ในการจัดการนโยบายความปลอดภัยขององค์กรได้

สามารถขอทดสอบ หรือทดลองฟรี Sophos Intercept X ติดต่อ บริษัท อี้ หรั่ง คอนซัลแตนท์ส จำกัด โทรศัพท์ 089-010-9634 E-mail: sales@e-rong.co.th

■ G-Able Security Consulting Team



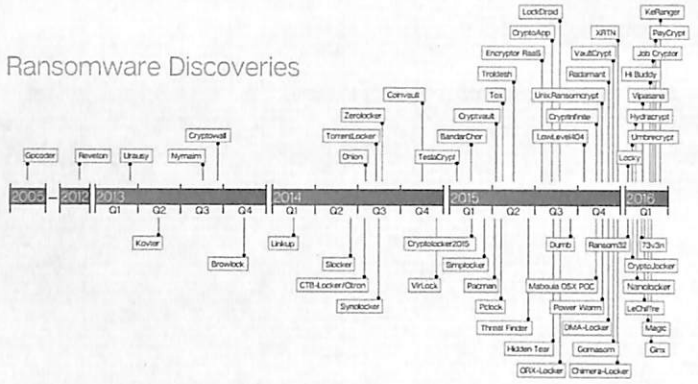
WannaCry เกมโจรกรรมเรียกค่าไถ่

มีหลายองค์กรจำเป็นต้องจ่ายเงินให้เพื่อแลกกับคีย์ (Key) ในการใช้มาถอดรหัสของระบบไฟล์บนเครื่องคอมพิวเตอร์เพื่อให้สามารถทำงานต่อได้โดยเฉพาะกับเซิร์ฟเวอร์ที่ให้บริการในงานทางธุรกิจและส่งผลกระทบต่องานหลักของธุรกิจนั้น

หากเราพูดถึงเรื่องของไวรัส (Virus) หรือมัลแวร์ (Malware) ในช่วงเวลานี้คงจะต้องพูดถึง Ransomware ตัวหนึ่งที่ชื่อ WannaCry หรือ WannaCrypt เพราะเป็น Ransomware ที่ทำให้ทุกคนในโลกได้ตระหนักถึงภัยร้ายของ Malware อีกชนิดที่ไม่เพียงแต่สร้างความเสียหายให้กับระบบคอมพิวเตอร์และเน็ตเวิร์ก แต่มีลักษณะของการโจรกรรมเรียกค่าไถ่ของไฟล์ด้วยการเข้ารหัสไฟล์ในเครื่องคอมพิวเตอร์ (Encryption) จนระบบปฏิบัติการหรือซอฟต์แวร์ที่อยู่ในเครื่องคอมพิวเตอร์เหล่านั้นไม่สามารถทำงานต่อได้ จากนั้นจะแสดงข้อความเพื่อบอกวิธีการให้จ่ายเงินในรูปแบบของ Bitcoin ซึ่งเป็นการโอนผ่านระบบอินเทอร์เน็ตที่ง่ายและไม่สามารถตรวจสอบปลายทางได้ให้กับผู้สร้างมัลแวร์ตัวนี้ ซึ่งก็มีหลายองค์กรหรือหลายบริษัทจำเป็นต้องจ่ายเงินให้เพื่อแลกกับคีย์ (Key) ในการใช้มาถอดรหัสของระบบไฟล์บนเครื่องคอมพิวเตอร์เพื่อให้สามารถทำงานต่อได้โดยเฉพาะกับเซิร์ฟเวอร์ที่ให้บริการในงานทางธุรกิจและส่งผลกระทบต่องานหลักของธุรกิจนั้น

ในความเป็นจริงแล้วมัลแวร์ประเภท Ransomware ได้เกิดขึ้นมานานแล้ว เพียงแต่ความร้ายแรงยังอยู่ในวงจำกัดที่สามารถป้องกันและยับยั้งการทำงานได้ แต่หากย้อนกลับไปเมื่อเดือนสิงหาคม 2559 ได้มีกลุ่มแฮกเกอร์ที่ชื่อว่า "The Shadow Broker" สามารถแฮกเข้าไปใช้เครื่องมือระดับสูงที่ใช้ในการค้นหาช่องโหว่ของซอฟต์แวร์หรือระบบปฏิบัติการจาก NSA ของสหรัฐ และเรียกร้องเงินจำนวน 1 ล้านเหรียญสหรัฐ แต่ไม่มีหน่วยงานไหนยอมจ่าย จึงได้ทำการปล่อยเครื่องมือและข้อมูลช่องโหว่ที่ค้นหาได้ออกสู่สาธารณะในช่วงเมษายน 2560

ข้อมูลช่องโหว่นี้เองเป็นจุดกำเนิดที่ทำให้มีผู้พัฒนา Ransomware ที่ชื่อ WannaCry ออกมาโดยใช้ข้อมูลช่องโหว่ของ Windows ที่เรียกว่า EternalBlue ซึ่งจะใช้การเข้าถึง Protocal และ Services ของ SMB (Simple Message Block) Version 1 หรืออาจเรียกอีกอย่างหนึ่งว่า CIFS (Common Internet File System) ที่ใช้ในระบบการแชร์ไฟล์ (File Sharing), พรินเตอร์ (Printer) และซีเรียลพอร์ท (Serial Port) ของระบบปฏิบัติการ Windows ถึงแม้ว่าทาง Microsoft จะได้มีการออกแพตช์ (Patch) ที่ใช้ในการแก้ไขช่องโหว่นี้มาตั้งแต่มีนาคม 2560 แล้วก็ตาม แต่เครื่องคอมพิวเตอร์หลายเครื่องก็ไม่ได้มีการติดตั้งแพตช์นี้เอาไว้



ที่มา: https://devcentral.f5.com/articles/security-trends-in-2016-the-problem-of-ransomware-24933

การทำงานของ WannaCry จะทำการสแกนค้นหาบนเครื่องที่อยู่ในระบบเน็ตเวิร์กที่มีช่องโหว่ข้างต้น ซึ่งเมื่อเจอก็จะทำการสำเนาตัวเองไปยังเครื่องเหล่านั้น และทำการเข้ารหัสไฟล์สำคัญบนเครื่องตัวเองเช่น .docx, .pptx, .mpeg, .zip, .backup แล้วแสดงข้อความเรียกค่าไถ่เป็นเงิน $300 เหรียญสหรัฐทาง Bitcoin

การทำงานของมัลแวร์ WannaCry เริ่มพบครั้งแรกเมื่อวันที่ 12 พฤษภาคม ที่ผ่านมา ภายใต้ชื่อ Wcry/ WanaCrypt0r/ WannaCry/ WanaCypt0r/ Wanacryptor และแพร่กระจายอย่างรวดเร็ว คาดว่ามีคอมพิวเตอร์ที่ติดมัลแวร์นี้มากกว่า 100,000 เครื่องทั่วโลกในระยะเวลาไม่ถึง 1 วัน จนกระทั่งมีผู้พบการหยุดการแพร่กระจายชั่วคราว มีหน่วยงานที่เป็นที่รู้จักซึ่งได้รับผลกระทบจากมัลแวร์ตัวนี้หนึ่งในนั้นคือ NHS (Nation Health Service) ซึ่งดูแลระบบประกันสุขภาพของประชาชนในอังกฤษ ได้ถูก WannaCry โจมตีและเข้ารหัสข้อมูล จนคนไข้จำนวนมากไม่สามารถรับการผ่าตัดได้ในวันนั้น จนทำให้ NHS ต้องยอมจ่ายค่าไถ่เพื่อกู้ข้อมูลที่สำคัญกลับคืนมา

ถึงแม้ว่าจะมีการค้นพบวิธีการหยุด WannaCry ด้วยการใช้ “Kill Switch” ฟังก์ชั่น ที่ซ่อนอยู่ในมัลแวร์ตัวนี้เพื่อตรวจค้นหา URL ที่ชื่อ “iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com” ในอินเทอร์เน็ต ซึ่งเมื่อเจอก็จะหยุดการทำงานของมัลแวร์ได้แล้ว แต่ก็ยังจะมีผู้พัฒนามัลแวร์ในลักษณะนี้ต่อไปและอาจจะไม่ได้ใส่ Kill Switch เพื่อหยุดมัลแวร์นั้นก็เป็นได้

เมื่อเราได้ทราบถึงวิธีการทำงานของมัลแวร์ในลักษณะนี้แล้ว ก็ทำให้เราสามารถหาวิธีการป้องกันการโจมตีจากมัลแวร์เหล่านี้ได้ในอนาคต โดยวิธีการที่จะช่วยให้ปลอดภัยจากการคุกคามนี้ก็คือ

- เครื่องคอมพิวเตอร์ส่วนบุคคลควรหมั่นตรวจสอบการอัปเดตแพตช์ (Patch) ทั้งส่วนของระบบปฏิบัติการ (OS) และโปรแกรมที่ใช้ภายในเครื่อง สำหรับผู้บริหารระบบไอทีขององค์กรควรติดตั้งระบบจัดการแพตช์ (Patch Management) เพื่อให้เครื่องแม่ข่ายและเครื่องของผู้ใช้ได้มีการติดตั้งแพตช์ให้ทันสมัยอยู่เสมอเพื่อลดความเสี่ยงจากการถูกโจมตีทางช่องโหว่ของซอฟต์แวร์เหล่านั้น
- ทำการสำรองข้อมูลอย่างสม่ำเสมอทั้งส่วนของระบบปฏิบัติการซอฟต์แวร์ และข้อมูลของผู้ใช้ เพื่อเพิ่มโอกาสในการกู้คือข้อมูลเมื่อเกิดความเสียหายจากมัลแวร์
- ตัดการเชื่อมต่อระบบเน็ตเวิร์กของเครื่องที่ติดมัลแวร์นั้นทันทีเมื่อตรวจพบ และตรวจสอบเครื่องอื่นในระบบเน็ตเวิร์กที่เหลือ
- ติดตั้งซอฟต์แวร์ป้องกันไวรัสและหมั่นอัพเดตฐานข้อมูลไวรัสให้ทันสมัยอยู่เสมอเพื่อป้องกันไวรัสหรือมัลแวร์ที่จะเกิดขึ้นในอนาคต
- ผู้ดูแลระบบเน็ตเวิร์กควรติดตั้งระบบติดตามและตรวจสอบพฤติกรรมของการใช้งานระบบเน็ตเวิร์กเพื่อให้สามารถสังเกตพฤติกรรมของการใช้งานที่น่าจะเกิดจากการแพร่กระจายของมัลแวร์ได้
- หลีกเลี่ยงการใช้ซอฟต์แวร์ที่ไม่ถูกลิขสิทธิ์เพราะนอกจากจะไม่สามารถอัพเดตแพทช์แล้วในบางกรณียังมีการซ่อนเร้นมัลแวร์บางชนิดมาด้วย
- หมั่นตรวจสอบช่องโหว่ของระบบปฏิบัติการ (OS) และซอฟต์แวร์ที่ติดตั้งในเครื่องและทำการปิดช่องโหว่นั้น โดยอาจจะใช้ซอฟต์แวร์ของผู้ผลิตที่มีให้ เช่น MBSA (Microsoft Baseline Analyzer)
- คอยติดตามข่าวสารของภัยคุกคามที่มาจากไวรัส มัลแวร์ หรือภัยคุกคามจากหน่วยงานที่เกี่ยวข้อง เช่น ThaiCERT (ETDA) , SANS หรือจากผู้ผลิตโปรแกรมป้องกันไวรัส เช่น Avast, McAfee, TrendMicro, Symantec เป็นต้น

ข้อมูลอ้างอิง :

- Customer Guidance for WannaCrypt Attack by MS (https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/)
- Microsoft Security Bulletin MS17-010 (https://technet.microsoft.com/en-us/library/security/ms17-010.aspx)
- How to enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server
- (https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
- Windows DNS Server Sinkhole Domains Tool (https://cyber-defense.sans.org/blog/2010/08/31/windows-dns-server-blackhole-blacklist)
- Microsoft Baseline Security Analyzer (https://www.microsoft.com/en-us/download/details.aspx?id=7558)
- Microsoft Windows Server Update Services (https://www.microsoft.com/en-us/download/details.aspx?id=5216)

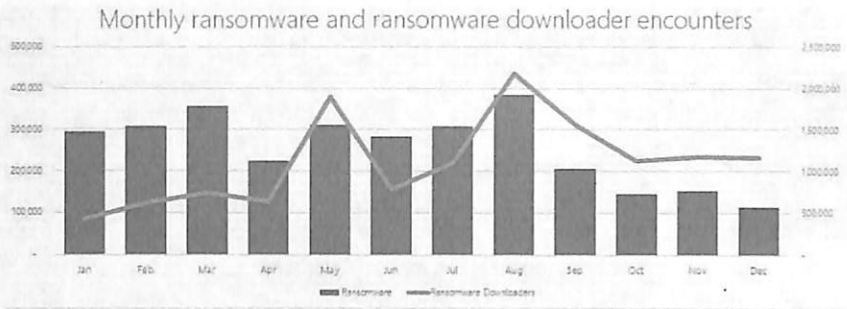
■ TaKaShi

Ransomware
มัลแวร์เรียกค่าไถ่จับเป็นตัวประกัน

Ransomware ชื่อนี้เพียงไม่กี่วันที่ผ่านมาแรนซัมแวร์ WannaCry ก็โด่งดังไปทั่วโลก เพราะได้โจมตีเครื่องคอมพิวเตอร์ขององค์กรนับพันและยูสเซอร์ทั่วโลก กระทบต่อองค์กรจำนวนมหาศาลในหลายกลุ่มธุรกิจทั่วโลก นี่เป็นมัลแวร์ตัวแรก หรือจะมีตัวอื่นอีกต่อไป แล้วเราจะรับมือกับ มัลแวร์ในอนาคตได้อย่างไร

WannaCry ได้สร้างการสะท้อนให้เห็นถึงผลกระทบที่เกิดขึ้นในชีวิตจริงของแรนซั่มแวร์ ไม่ว่าจะเป็น การทำลายล้างระบบ, ทำให้การปฏิบัติงานหยุดชะงักลง, ทำให้ชื่อเสียงเสื่อมเสีย และสร้างความเสียหายทางการเงิน ธุรกิจ ธุรกรรม อันเป็นผลมาจากการที่ไม่สามารถดำเนินธุรกิจได้ตามปกติ ทั้งนี้ยังไม่รวมถึงค่าใช้จ่ายที่เกิดขึ้นจากการจัดการกับเหตุการณ์ด้านความปลอดภัยที่เกิดขึ้น และการกู้คืนระบบ ในบทความนี้เราจะมีรู้และป้องกัน

Ransomware เป็นปัญหาระดับโลกที่เกิดขึ้นในประเทศต่างๆ เช่น สหรัฐอเมริกา, อิตาลี, รัสเซีย, เกาหลี และสเปน เริ่มมีมากขึ้นในปีพ.ศ. 2016 ปัจจุบัน Ransomware ที่ได้รับความนิยม เช่น Ransom:Win32/Cerber, Ransom:Win32/Locky, Ransom:Win32/Spora, Ransom:Win32/HydraCrypt, Ransom:Win32/Critroni, Ransom:Win32/Teerac, Ransom:Win32/Troldesh



รูปที่ 1 แสดงการดาวน์โหลดในแต่ละประเทศ แต่ละเดือน (รูปจาก microsoft.com)

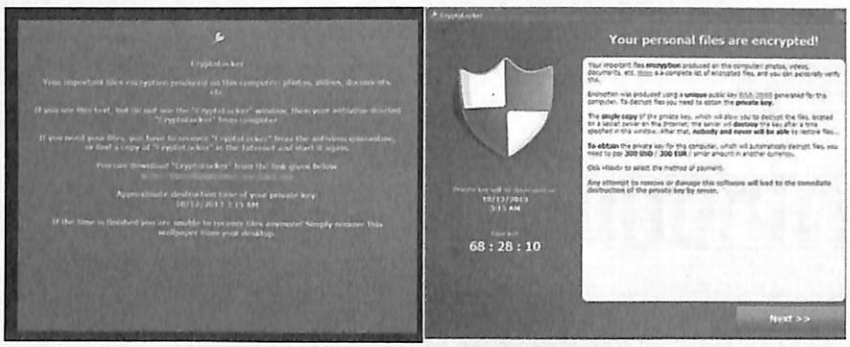
จะเห็นอีเมลจำนวนมากที่มีผู้ดาวน์โหลด Ransomware จำนวนอีเมล 500 ฉบับ เอกสารที่แนบมากับอีเมลถึงคอมพิวเตอร์นับล้านเครื่อง

แต่มีหลายไฟล์ที่ถูกบล็อกจากการดาวน์โหลดและเรียกใช้ ransomware ที่มากกว่า 200 กว่าชนิด กว่าครึ่งถูกค้นพบในปี 2016

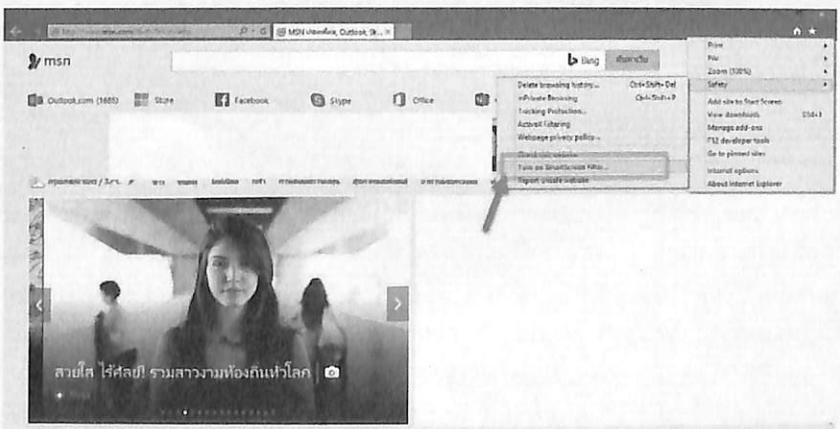
รู้จักกับขั้นตอนการทำงานของ Ransomware

Ransomware เป็นมัลแวร์ (Malware) ประเภทหนึ่งที่มีลักษณะการทำงานที่แตกต่างกับมัลแวร์ประเภทอื่นๆ ที่เราเคยรู้จักกันมา โดยจะทำการเข้ารหัสหรือล็อกไฟล์ข้อมูลในเครื่องคอมพิวเตอร์ ทั้งไฟล์เอกสาร รูปภาพ วิดีโอ เสียง ไฟล์งานของเราทั้งหมด นอกจากการใช้งานโปรแกรมหรือไฟล์ที่มีการเข้ารหัส แล้วยังไม่ให้คุณใช้งานระบบปฏิบัติการวินโดวส์ การไม่ให้ใช้งานแอปบางอย่าง เช่น โปรแกรมเว็บเบราเซอร์อีกด้วย ซึ่งแม้เราเป็นเจ้าของเองก็จะไม่สามารถเปิดไฟล์เอกสารนั้นๆ ได้เพราะเราไม่ทราบรหัสผ่าน ถ้าต้องการเปิดไฟล์จะต้องทราบถึงรหัสผ่าน หากต้องการรหัสผ่านจะต้องจ่ายเงินตามข้อความเรียกค่าไถ่ แต่ถ้าเราไม่จ่ายก็แน่นอนไม่สามารถเปิดดูได้ ซึ่งไม่ได้มีการรับประกันว่าการจ่ายเงินค่าปรับนั้นแล้วคุณจะเปิดไฟล์ข้อมูลนั้นได้ ถ้าแสดงข้อความเรียกค่าถ่าย ดังรูปที่ 2 แสดงว่าคุณกำลังถูกเรียกค่าไถ่แล้วแหละ

ส่วนเงินที่ต้องโอนไปให้ราคาอยู่ที่ประมาณ 150 ถึง 500 เหรียญ และต้องชำระผ่านระบบที่ไม่สามารถตรวจสอบได้ว่าเป็นใครที่ไหน ทั้งการโอนเงินผ่านระบบอิเล็กทรอนิกส์, Paysafecard หรือ Bitcoin แต่หลายกระแสบอกว่าโอนให้แล้วก็ใช่ว่าจะได้รหัสปลดล็อค



รูปที่ 2 ภาพจาก Trend Micro แสดงข้อความเรียกค่าไถ่



รูปที่ 3 เปิดใช้งาน SmartScreen Filter บน Internet Explorer

โอกาสของการติดมัลแวร์ Ransomware

ไม่ใช่มัลแวร์ Ransomware จะติดกับเครื่องคอมพิวเตอร์ทุกเครื่อง แต่มันมีที่มาที่ไป ส่วนมากก็จะเปิดจากอีเมลหลอกลวงที่แนบไฟล์ Ransomware โดยปลอมเป็นอีเมลส่งมาหาเราทั้งการปลอมเป็น FedEx หรือ DHL ซึ่งจะมีการปลอมเหมือนหน้าจริงอย่างมาก หรืออีเมลมาหรอกว่าบัญชีโดนล็อค เมื่อคลิกที่ลิงก์ก็จะดาวน์โหลดไฟล์ exe ที่มีมัลแวร์ Ransomware ทันที หลังจากเปิดไฟล์ที่ติดมัลแวร์ จะแสดงหน้าต่างแจ้งเตือนบังคับให้จ่ายเงินเพื่อทำการปลดล็อค

อย่าคลิกบนลิงก์หรือเปิดไฟล์ อีเมลจากบริษัท หรือคนที่คุณไม่รู้จัก เพราะอาจทำให้เราติดมัลแวร์ Ransomware ได้โดยง่ายหากใช้งาน Internet Explorer ให้เปิดใช้งาน Smart Screen

- ในหน้าต่างโปรแกรม Internet Explorer แล้วคลิกปุ่ม Tools แล้วคลิกที่รายการ Safety
- คลิกเลือกที่รายการ Turn off SmartScreen Filter แล้วเลือก Turn off SmartScreen Filter หรือ Turn on SmartScreen Filter
- แล้วคลิกปุ่ม OK

เมื่อโดนมัลแวร์ Ransomware เล่นงาน

คุณไม่ตกเทรนด์แล้ว (แต่หลายอยากตกเทรนด์) แน่นอนไฟล์ข้อมูลดังกล่าวไม่ได้คืนกลับมาแน่ๆ ต่อให้โอนเงินไปให้เพื่อขอรหัสผ่านก็ไม่มีทางได้ ดีไม่ดีเสียเงินแล้วไม่ได้อะไรกลับมาแลกเปลี่ยนอีกด้วย ขณะที่เครื่องคอมพิวเตอร์ของคุณโดน Ransomware ไม่ควรจะเสียบ Flash Drive, External Hard disk หรือเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต กรณีที่มีการซิงค์ไฟล์จากเครื่องไปยังระบบคลาวด์ก็เช่นกันควรปิดการซิงค์นั้นก่อน เพราะมันอาจจะลามไปถึงระบบเครือข่ายอื่นๆ ที่คุณเชื่อมต่อไว้ด้วยจะยุ่งกันไปใหญ่

แนะนำให้ฟอร์แมตเครื่องคอมพิวเตอร์ เพื่อล้างเครื่องและกำจัดมัลแวร์ Ransomware ให้สิ้นซากไปด้วยในตัว จากนั้นก็เริ่มติดตั้งระบบปฏิบัติการใหม่ และโปรแกรมต่างๆ ที่ต้องการ

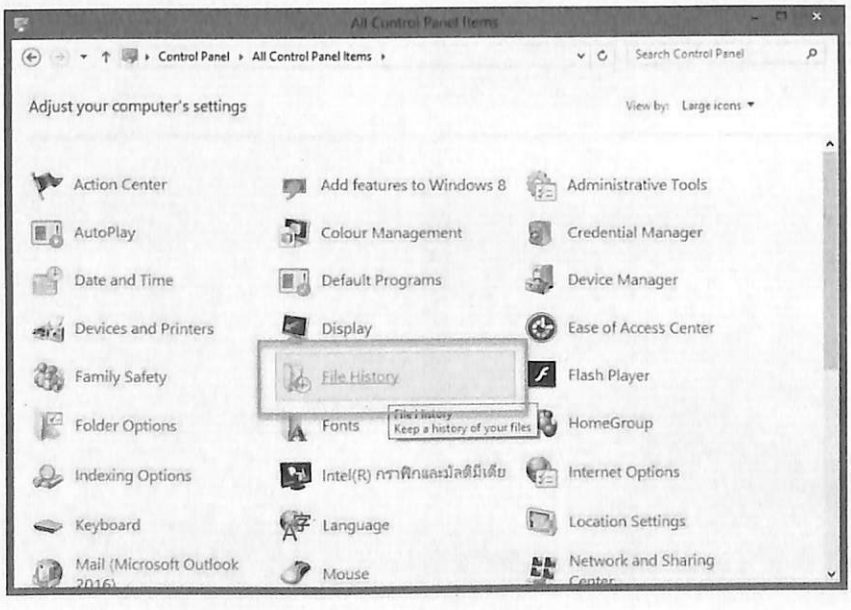
การกู้คืนไฟล์บนวินโดวส์

หากใช้งานวินโดวส์เมื่อต้องการกู้คืนไฟล์ให้ใช้ Windows Defender ในแบบออฟไลน์เพื่อทำความสะอาดเครื่องคอมพิวเตอร์เสียก่อนส่วนกู้คืนไฟล์ที่จัดเก็บไว้ใน Microsoft Office หรือซิงก์รวมถึงแบ็กอัพบน OneDrive ก่อนกู้ไฟล์ต้องตรวจสอบให้แน่ใจก่อนกรณีใช้สร้างไฟล์ Microsoft Office ไว้ใน OneDrive ให้กำหนดรหัสผ่านที่มีการคาดเดาได้ยาก ควรใส่ข้อมูล อีเมลแอดเดรส เบอร์ติดต่อ และคำถามกรณีเป็นคำถามทางด้านความปลอดภัย เพื่อให้ผู้แอบอ้างเข้าใช้งานอีเมลคุณได้ยากขึ้น ตรวจสอบเวอร์ไฟล์บน OneDrive บนเว็บ ให้เข้าไปที่เอกสาร แล้วคลิกขวาบนไฟล์ที่ต้องการกู้คืน ให้คลิกที่ Detail ตรวจสอบรายละเอียดไฟล์

กรณีไฟล์อยู่บนเครื่องคอมพิวเตอร์ หากเปิดใช้งาน File History (มีในวินโดวส์ 10 และวินโดวส์ 8.1) หรือ System Protection (ในวินโดวส์ 7 และ Windows Vista) ก่อนจะติดไวรัส ในบางครั้งที่ผู้ผลิตและผู้ดูแลระบบเครือข่ายจะเปิดให้ใช้งานอยู่แล้ว แต่อาจมี Ransomware บางตัวที่เก่งขนาดเข้ารหัสและลบเวอร์ชั่นสำรองที่เราทำเอาไว้ รวมไปถึงไฟล์บนเครือข่าย และ Flash Drive แต่สามารถถึงไฟล์สำรองจากไดร์ฟแบบถอดได้หรือไดร์ฟที่ไม่ได้เชื่อมต่อกับเครือข่าย

การป้องกัน Ransomware

การป้องกัน Ransomware หรืออาจเป็นไวรัส สปายแวร์ตัวอื่นๆ ก็สามารถใช้ขั้นตอนเดียวกันนี้ประยุกต์ใช้งานได้เช่นกัน



รูปที่ 4 เปิดใช้งานระบบแบ็กอัพในวินโดวส์ก่อนโดยเล่นงาน

แบ็กอัพเลยไม่ต้องรอมัลแวร์ สปายแวร์ ไวรัส หลายคนก็ตกใจกับความสามารถของมัลแวร์ตัวนี้ (จริงๆ ก็มีหลายตัวเกิดขึ้นมาเรื่อย) แต่ก็อย่าลืม สปายแวร์ ไวรัส ที่มีความสามารถก่อกวน หรือทำลายร้างได้พอๆ กัน ข้อมูลมักจะเป็นสิ่งที่เราคิดถึงหลังจากเปิดเครื่องคอมพิวเตอร์ โน้ตบุ๊ก ไม่ได้ หรืออาจคิดถึงอันดับแรก น้ำตาจะไหลไหนจะรูปภาพ ไฟล์เอกสาร ไฟล์วิดีโอ ไฟล์โปรเจ็กต์ต่างๆ หมดกัน

ก่อนที่ข้อมูลจะหายเราควรแบ็กอัพข้อมูล และควรจะทำเป็นประจำ กรณีหากเกิดปัญหากับระบบจะได้ทำงานต่อเนื่องได้อย่างไม่สะดุด สามารถเลือกแบ็กอัพข้อมูลบนระบบเครือข่าย ระบบ Cloud Storage ของบริษัท เช่าเป็นรายเดือน หรือบริการฟรีอย่าง Google Drive, Dropbox, Box, OneDrive, Mega เป็นต้น แต่ควรเป็นข้อมูลที่ไม่สำคัญมาก หรือเสียค่าใช้จ่ายเพิ่มเติมเพื่อเพิ่มปริมาณพื้นที่จัดเก็บ

สำหรับการใช้งานบนสมาร์ทโฟนก็มีให้เลือกใช้งานเช่นกันทั้ง iCloud ขนาด 5 กิกะไบต์สำหรับผู้ใช้ iOS หรือ Amazon Cloud ขนาด 5 กิกะไบต์สำหรับผู้ใช้ iOS และ Android, Box ขนาด 10 กิกะไบต์สำหรับผู้ใช้ iOS และ Android, Dropbox ขนาด 2-50 กิกะไบต์สำหรับผู้ใช้ iOS และ Android, Google Drive ขนาด 5-15 กิกะไบต์สำหรับผู้ใช้ iOS และ Android เป็นต้น

External Hard Drive ฮาร์ดดิสก์ขนาดพกพา สำหรับจัดเก็บข้อมูลมีให้เลือกหลากหลายขนาดทั้งน้อยกว่า 500 กิกะไบต์เริ่มต้นประมาณ 1,500 บาท ไปจนถึง 12 เทราไบต์ ประมาณ 2,700 บาทขึ้นไป ส่วนถ้าต้องการแบ็กอัพด้วย USB Flash Drive เริ่มต้นที่ขนาด 8 กิกะไบต์, 16 กิกะไบต์, 32 กิกะไบต์, 128 กิกะไบต์, 2 เทราไบต์ เป็นต้น สำหรับการเครื่องคอมพิวเตอร์แบ็กอัพ หรือระบบ NAS ระบบจัดเก็บข้อมูลที่เชื่อมต่อกับระบบเครือข่าย ก็จะเพิ่มความสะดวกมากขึ้น

อัพเดทซอฟต์แวร์

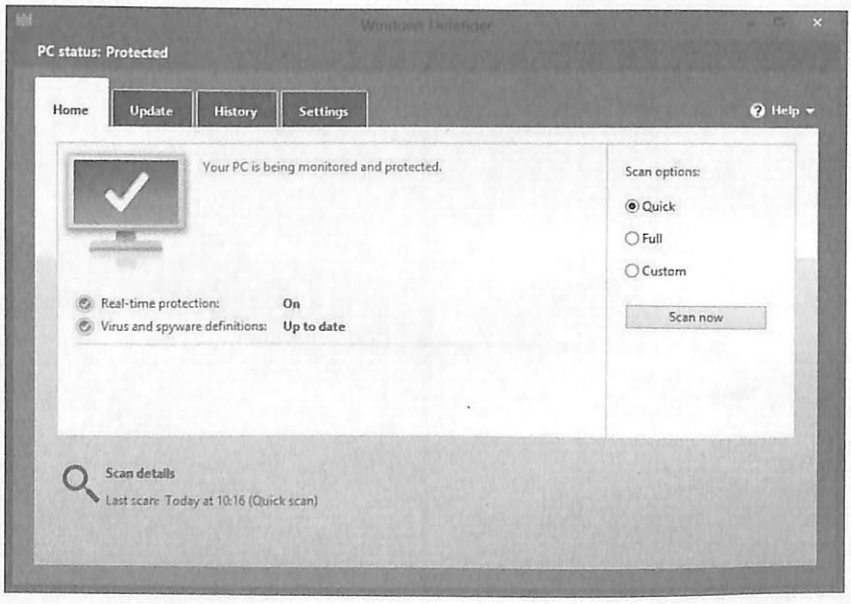
ก่อนจะว่าไปถึงเรื่องอัพเดท ต้องถามก่อนคำถามแรก ถึงข้อมูลพื้นฐานที่ไม่ควรจะมองข้ามไป เพราะบางครั้งการทำให้เครื่องคอมพิวเตอร์ของท่านเสียหาย ไม่ได้ระวังแต่การป้องกันเสียอย่างเดียว

คุณใช้ซอฟต์แวร์โดยเฉพาะระบบปฏิบัติการวินโดวส์เป็นซอฟต์แวร์ลิขสิทธิ์หรือไม่ เดี๋ยวนี้ราคาซอฟต์แวร์ไม่แพงเหมือนแต่ก่อน และสามารถอัพเดทเวอร์ชั่นเป็นเวอร์ชั่นใหม่ได้ พร้อมระบบการอัพเดทเพื่อป้องกันไวรัส สปายแวร์ ช่องโหว่ต่างๆ หากใครซื้อเครื่องใหม่ก็มักจะมาพร้อมกับระบบปฏิบัติการมาให้ด้วย แต่อย่าลืมอัพเดทด้วย

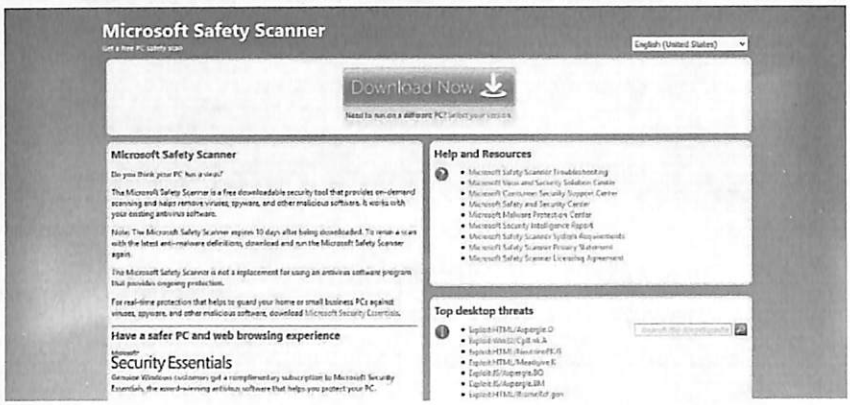
การอัพเดทซอฟต์แวร์ของระบบปฏิบัติการวินโดวส์ 10 โดยคร่าวๆ ก็คลิกปุ่ม Start > Settings > Update & security แล้วคลิกปุ่ม Check for updates

ติดตั้งและใช้งานพร้อมอัพเดทเวอร์ชั่นของโปรแกรมป้องกันไวรัส เช่น Microsoft Security Essentials ดาวน์โหลดได้จาก https://support.microsoft.com/en-us/help/14210/security-essentials-download โดย Microsoft Security Essentials สำหรับ Windows 7 และ Windows Defender สำหรับ Windows 8, Windows RT, Windows 8.1, Windows RT 8.1, Windows 10

ติดตามข่าวสาร ควรติดตามข่าวสารในทุกช่องทางทั้งเว็บไซต์ โซเชียลมีเดียต่างๆ เพื่อตรวจสอบช่องโหว่ หรือภัยคุกคามต่างๆ ที่สำคัญควรศึกษาวิธีการป้องกัน รับมือจะได้ไม่ตกเป็นเหยื่อของผู้ไม่หวังดี แอบแฝง และเพื่อความปลอดภัยให้กับผู้ใช้งาน



รูปที่ 5 ป้องกันเครื่องด้วย Microsoft Security Essentials หรือ Windows Defender



รูปที่ 6 เครื่องมือช่วยจัดการ Microsoft Safety Scanner

ต้องการลบ Ransomware ออกจากเครื่อง

วิธีที่จะแนะนำอาจใช้งานได้กับมัลแวร์ Ransomware บางตัวเท่านั้น ถ้าหากเบราเซอร์ถูกล็อค ให้ยกเลิกการล็อคให้ใช้ Task Manager เพื่อหยุดการทำงานของเบราเซอร์

1. เปิดใช้งาน Task Manager ให้คลิกขวาบนทาสก์บาร์เลือก Task Manager หรือ Start Task Manager อีกวิธี กด Ctrl+Shift+Esc หรือกด Ctrl+Alt+Delete

2. ในรายการที่แสดง Applications หรือ Processes ให้คลิกลงบนชื่อของโปรแกรมเว็บเบราเซอร์

3. คลิกปุ่ม End task ถ้ามีหน้าต่างต้องการรอโปรแกรมตอบสนองหรือไม่ ให้คลิกปุ่ม Close หากเปิดใช้งานเว็บเบราเซอร์อีกครั้ง จะถามว่าให้กู้คืนหน้าต่างเดิมกลับมา ไม่ต้อให้กู้คืนหน้าต่างเดิม

กรณีใช้ Microsoft Safety Scanner ใน Safe Mode

1. ให้ดาวน์โหลด Microsoft Safety Scanner จาก https://www.microsoft.com/security/scanner/en-us/default.aspx แล้วคัดลอกไฟล์มาไว้ใน Flash Drive หรือซีดี

2. จากนั้นก็รีสตาร์วินโดวส์แล้วเข้า Safe Mode

3. แล้วสั่งรัน Microsoft Safety Scanner

4. หรือใช้งาน Windows Defender ในแบบออฟไลน์

ผลกระทบที่เกิดขึ้นมีอะไรบ้าง

ผู้ใช้งานจะสูญเสียข้อมูล เอกสารการใช้งานทางด้านธุรกิจ และข้อมูลต่างๆ ที่จัดเก็บไว้บนเครื่องคอมพิวเตอร์ ทำให้ธุรกิจสะดุดลง ไม่สามารถเดินต่อไปได้ สูญเสียเวลาและทรัพย์สิน ต้องมานั่งติดตั้งและซอฟต์แวร์ใหม่ ถ้าทำเองได้ก็ใช้เวลาพอประมาณ แต่ถ้าทำเองไม่เป็นก็ต้องเสียเวลาและค่าใช้จ่ายให้กับทางร้านที่ติดตั้ง

ผู้ดูแลระบบ แน่นอนระบบที่ดูแลอยู่จะต้องหยุดทำงาน จนบางครั้งอาจต้องหยุดชะงัก อาจรวมไปถึงระบบแบ็กอัพและระบบอื่นๆ ถ้าเป็นระบบใหญ่ๆ เช่น ระบบการเงิน ระเบียงจัดเก็บข้อมูล ระบบราชการต่างๆ ก็ทำให้เสียหายมากมาย เป็นสิ่งที่ผู้ดูแล และสถานที่นั้น ต้องให้ความสำคัญกับระบบการรักษาความปลอดภัยในรูปแบบต่างๆ

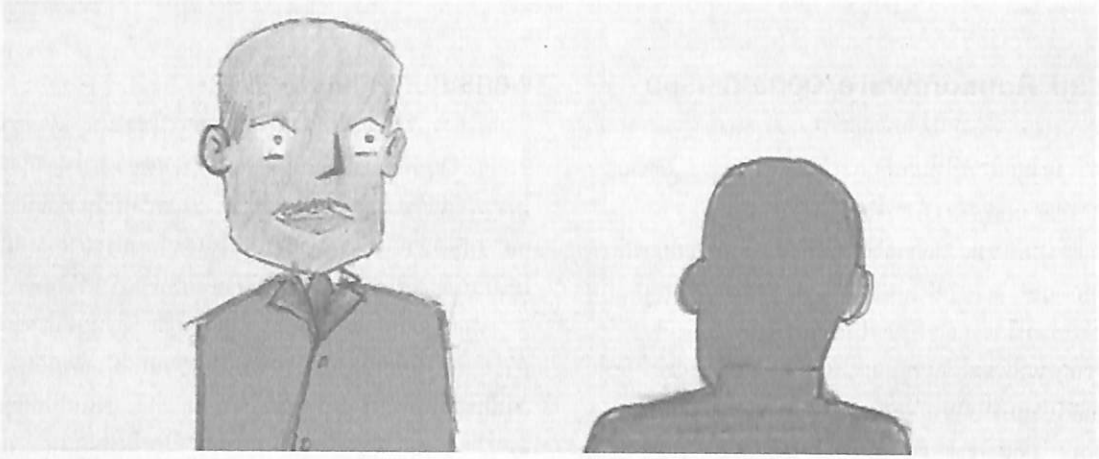
เอกสารอ้างอิง www.microsoft.com, www.trendmicro.com

Micro Toon

❑ Witchy

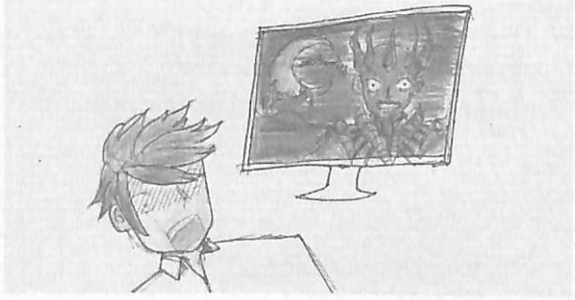
ตอน... เมื่อ AI กลายเป็น UI

"หัวหน้า...ไม่ต้องห่วงนะครับ ผมได้พัฒนาโปรแกรมหัวหน้าจำแลงและติดตั้งในทุกเครื่องแล้ว ช่วงที่หัวหน้าไม่อยู่โปรแกรมนี้จะทำงานแทนทั้งหมด ทั้งตามงานลูกน้องแบบตัวต่อตัวที่แตกต่างกันตามสไตล์ของหัวหน้า รวมทั้งยังมีฟังก์ชั่นพิเศษที่จะคอยหยอดมุกน้องแต่ม ก่อนเลิกงานทุกวันด้วยครับ"



"เจ้านายไม่อยู่..ดีจัง ไม่มีใครมาบ่นให้รำคาญแอบงีบสักหน่อยดีกว่า"

"วิโรจน์!!! คิดจะงีบใช่ไหม??? ...กลับมาทำงานต่อได้แล้ว จะต้องส่งงานสัปดาห์หน้าแล้วนะ"



เรียนรู้เทคโนโลยีกับ Micro Toon : ปัญญาประดิษฐ์ (Artificial Intelligence หรือ AI) เป็นศาสตร์หนึ่งที่พยายามพัฒนาให้คอมพิวเตอร์มีความสามารถและความชาญฉลาดเพิ่มยิ่งขึ้น ทั้งในงานด้านการประมวลผลภาษาธรรมชาติ (Natural Language Processing: NLP) การพัฒนาหุ่นยนต์ (Robotic) การแปลภาษา (Machine Translation) การรู้จำภาพและเสียง (Pattern and Voice recognition) และอื่นๆ อีกมากมาย ซึ่งเป็นเรื่องที่ท้าทายและยากมากในยุค 80-90

ปัจจุบันศาสตร์ด้านปัญญาประดิษฐ์มีความก้าวหน้าอย่างรวดเร็ว ดังเห็นได้จากการนำผลงานด้านปัญญาประดิษฐ์มาประยุกต์ใช้กับเครื่องใช้และอุปกรณ์อัตโนมัติต่างๆ เป็นจำนวนมากเช่น โปรแกรมหรืออุปกรณ์ช่วยแปลภาษา การรับอินพุตข้อมูลด้วยเสียงในแอพพลิเคชั่นและระบบต่างๆ รวมทั้งระบบผู้เชี่ยวชาญที่ให้คำปรึกษาด้านต่างๆ จนกระทั่งปัญญาประดิษฐ์กลายเป็นส่วนสำคัญของส่วนเชื่อมต่อระหว่างระบบต่างๆ กับผู้ใช้งาน (User Interface) จนกระทั่งกูรูหลายคนเห็นพ้องกันว่า AI จะกลายเป็นส่วนสำคัญของ UI ที่ใช้กันในอนาคตอันใกล้นี้

ดร.วิรินทร์ เมฆประดิษฐสิน

วิเคราะห์เครือข่ายและระบบรักษาความปลอดภัย ด้วย Wireshark

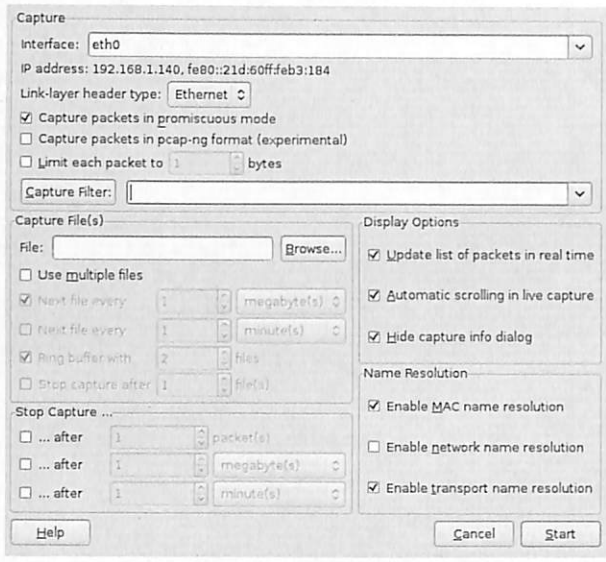
วิธีใช้ Wireshark เครื่องมือที่ได้รับความนิยมอย่างยิ่งในบ้านเรา เพื่อวิเคราะห์และเรียนรู้การทำงานของระบบเครือข่ายและระบบรักษาความปลอดภัย

ในการบริหารจัดการ การดูแลรักษาระบบเครือข่ายคอมพิวเตอร์จำเป็นต้องมีเครื่องทุ่นแรงและตาทิพย์ ตลอดจนยามที่ใช้สอดส่องและวิเคราะห์ปัญหาต่างๆ ที่เกิดขึ้นในระบบ ปัญหาในปัจจุบันคือเครื่องมือประสิทธิภาพสูงมักมีราคาแพงมาก แต่ปัจจุบันเรามีเครื่องมือประเภทฟรีแวร์มากมาย ทำงานภายใต้โอเพนซอร์ส (Open Source) ที่มีประสิทธิภาพ ดูแล้วน่าสนใจ อย่างเช่น Wireshark ซึ่งถือเป็นเครื่องมือประเภทฟรีแวร์ที่ทรงพลังยิ่ง แต่มีการทำงานแบบ Passive หรือ Promiscuous Mode หรือการดักจับแพ็กเก็ตเพื่อนำมาวิเคราะห์กระแสการจราจรบนเครือข่าย เพื่อตรวจหาจุดบกพร่องการทำงาน หรือแม้แต่นำมาวิเคราะห์เพื่อความปลอดภัย ประเด็นสำคัญคือเราจะนำไปประยุกต์ใช้เพื่อวิเคราะห์หรือศึกษาระบบเครือข่ายได้อย่างไร รวมทั้งการตรวจสอบประเด็นที่น่าสงสัยเกี่ยวกับความปลอดภัย บทความนี้กล่าวถึงวิธีใช้เครื่องมือที่ได้รับความนิยมอย่างยิ่งในบ้านเราเกี่ยวกับการวิเคราะห์ เรียนรู้การทำงานของเครือข่าย ตลอดจนระบบรักษาความปลอดภัย

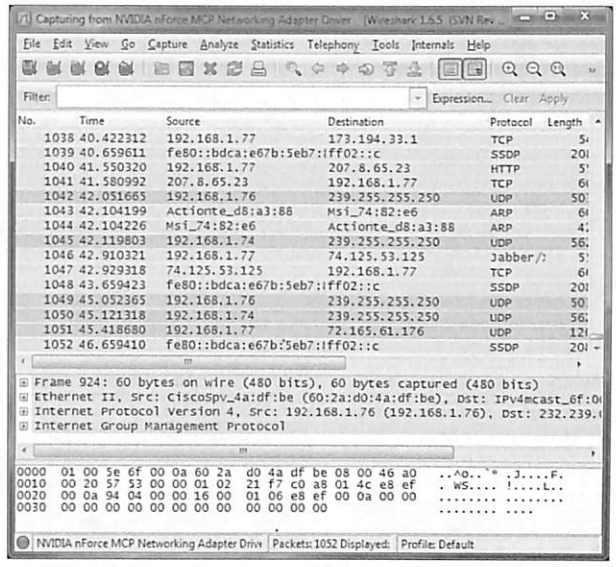
ทบทวนการใช้งาน Wireshark สำหรับ Windows

การดักจับแพ็กเก็ต

หลังจากที่ดาวน์โหลดและติดตั้ง Wireshark เป็นที่เรียบร้อยแล้ว ท่านสามารถเรียกออกมาใช้งานด้วยการคลิกที่ Interface หรือชื่อการ์ด LAN ที่ท่านกำลังใช้งานเพื่อเริ่มดักจับแพ็กเก็ต ตัวอย่างเช่น หากท่านต้องการดักจับกระแสจราจรบนเครือข่ายไร้สายหรือ Wireless ท่านเพียงคลิกไปที่ Wireless Interface เท่านั้น นอกจากนี้ท่านยังสามารถเลือกออปชั่นสำหรับการดักจับแพ็กเก็ตโดยเฉพาะ

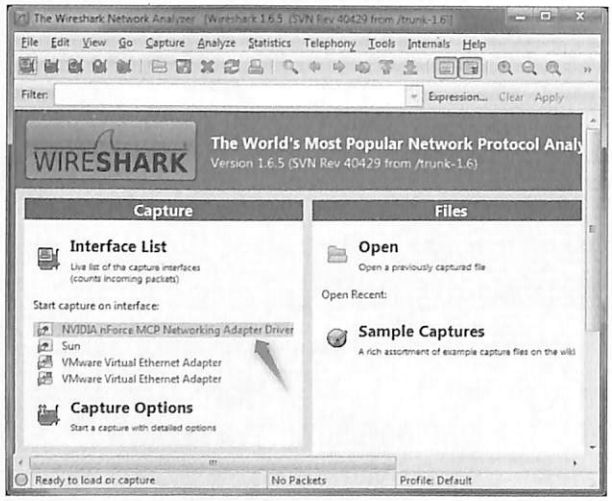


รูปที่ 1 แสดงหน้าจอ Display Option



รูปที่ 3 แสดงหน้าจอขณะดักจับแพ็กเก็ต

จากรูปที่ 1 ท่านสามารถกำหนดขนาดของแพ็กเก็ตที่จะดักจับคิดเป็นไบต์ รวมทั้งปริมาณของแพ็กเก็ตคิดเป็นเมกะไบต์ (MB) หรือจำนวนแพ็กเก็ตที่ระบุเป็นตัวเลข รวมทั้งจำนวนคิดเป็นนาทีที่จะดักจับแพ็กเก็ต นอกจากนี้ยังสามารถกำหนดว่าจะให้แสดงชื่อหรือไอพีแอดเดรส รวมทั้งโปรโตคอลที่เกี่ยวข้องอีกด้วย ส่วนในรูปที่ 2 เป็นการแสดงหน้าจอ Wireshark ในเวอร์ชั่นก่อนๆ



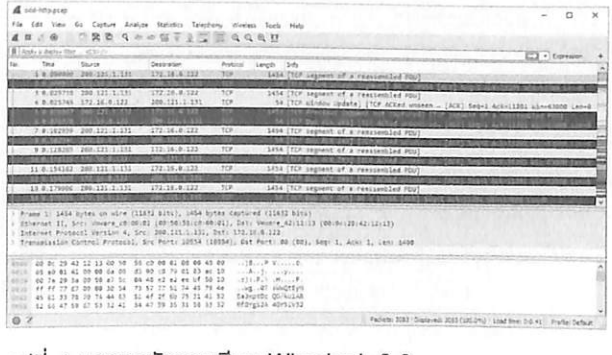
รูปที่ 2 แสดงหน้าจอ Wireshark ในเวอร์ชั่นก่อนๆ

เกือบทันทีที่ท่านคลิกไปยังชื่อของ Interface ท่านจะเห็นการดักจับแพ็กเก็ตเกิดขึ้น (รูปที่ 3) โดยเป็นแพ็กเก็ตที่รับเข้ามาหรือออกไปจากคอมพิวเตอร์ของท่าน โดยจะมีการแสดงช่วงเวลาที่รับแพ็กเก็ตเข้ามาที่ด้านซ้ายมือ รวมทั้งแอดเดรสต้นทางที่สามารถแสดงเป็น MAC Address หรือไอพีแอดเดรส ตลอดจนโปรโตคอลที่ใช้ ขนาดของแพ็กเก็ต รวมทั้งข้อมูลข่าวสารต่างๆ เกี่ยวกับโปรโตคอลที่ใช้งาน เช่น การแลกเปลี่ยนข่าวสารระหว่างโปรโตคอลในแต่ละชนิด สิ่งนี้จะช่วยให้ท่านทราบปฏิสัมพันธ์และการทำงานร่วมกันระหว่างคอมพิวเตอร์ภายใต้โปรโตคอลต่างๆ ถ้าท่านมีความรู้เกี่ยวกับการทำงานของโปรโตคอล ท่านจะทราบถึงปัญหาและนำไปสู่การวินิจฉัยปัญหาได้อย่างง่ายดาย

ในกรณีที่ท่านต้องการยกเลิกการดักจับแพ็กเก็ตก็เพียงแต่คลิกที่ปุ่ม Stop หรือหากเป็นเวอร์ชั่นใหม่ เช่น Wireshark 2.0 ให้คลิกที่ปุ่มสี่เหลี่ยมสีแดงเท่านั้น ในกรณีที่ต้องการดักจับแพ็กเก็ตใหม่ให้คลิกที่รูปครีบปลาฉลาม

รหัสของแถบสี

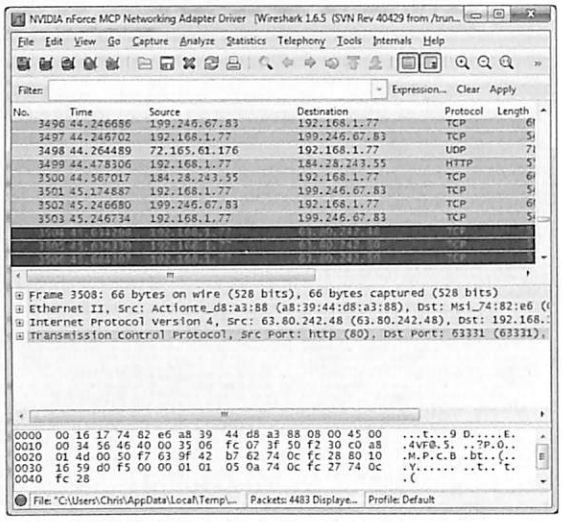
ภายใต้หน้าจอ Wireshark ท่านจะเห็นแถบสีต่างๆ ประกอบด้วยสีเขียว ฟ้า และดำ (รูปที่ 4) โดย Wireshark ใช้แถบสีที่คาดบนแพ็กเก็ตเพื่อแยกหรือระบุชนิดของกระแสการจราจรหรือทราฟฟิก (Traffic) เพื่อให้ดูได้ง่าย โดยค่าดีฟอลต์แล้วสีเขียวมักใช้กับทราฟฟิกของ TCP สีฟ้าเข้มใช้กับทราฟฟิกของ DNS ส่วนสีฟ้าอ่อนสำหรับทราฟฟิกของ UDP และสีดำใช้กับแพ็กเก็ตของ TCP ที่กำลังมีปัญหา ตัวอย่างเช่น แถบสีดำในรูปที่ 5 อาจเป็นการปล่อยแพ็กเก็ตออกมาหรือแพ็กเก็ตที่วิ่งเข้ามาแบบไม่เรียงลำดับ เป็นต้น



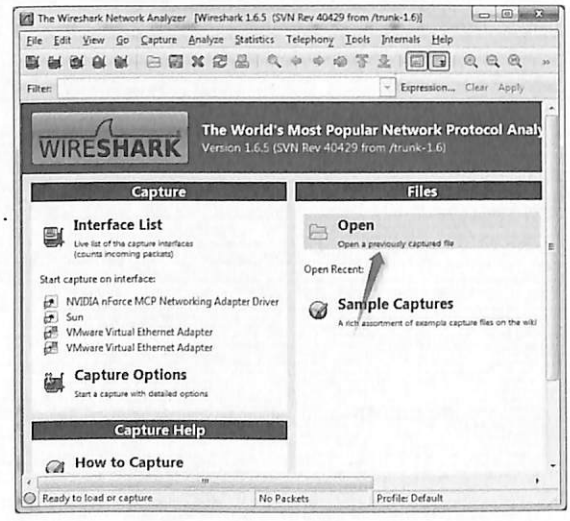
รูปที่ 4 แสดงรหัสแถบสีบน Wireshark 2.0

ตัวอย่างการดักจับแพ็กเก็ต

ท่านสามารถเรียกดูตัวอย่างที่เป็นไฟล์เก็บภาพตัวอย่างที่ทางผู้ผลิตจัดทำไว้เป็นตัวอย่างให้ดูเป็นแนวทางการวิเคราะห์ เราสามารถเปิดไฟล์ดังกล่าวได้ง่ายโดยไปที่หน้าจอหลักและค้นหาไฟล์ นอกจากนี้ท่านยังสามารถบันทึกไฟล์ที่ได้ Capture ด้วยตัวท่านเองและสามารถเปิดดูได้ในโอกาสต่อไป (ดูรูปที่ 6)



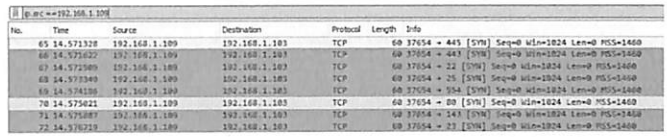
รูปที่ 5 แสดงแถบสีที่บ่งบอกทราฟฟิกของ TCP ที่มีปัญหา



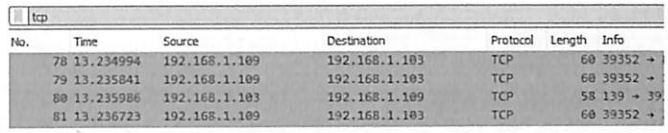
รูปที่ 6 แสดงหน้าจอหลักในตำแหน่งสำหรับเปิดไฟล์ที่ Capture ไว้

การคัดกรองแพ็กเก็ต

เนื่องจากมีโปรโตคอลจำนวนมากมายหลากหลายวิ่งอยู่บนเครือข่าย ดังนั้นจึงยากที่จะแยกแยะทราฟฟิกต่างๆ ได้อย่างง่ายดาย ท่านสามารถคัดกรองทราฟฟิกที่ต้องการจะแสดงผลได้โดยใช้ทางเลือกที่เรียกว่า Display Filter โดยไปที่ช่อง Filters (ดูรูปที่ 7 สำหรับเวอร์ชั่น 2.0 ขึ้นไปให้ดูรูปที่ 8)



รูปที่ 7 การใช้ Expression ระบุไอพีแอดเดรสต้นทาง



รูปที่ 8 แสดงช่องกรอกชื่อโปรโตคอลที่จะแสดง

ท่านสามารถกรอกชื่อโปรโตคอลที่ต้องการ เช่น การใส่ชื่อโปรโตคอลเพียงอย่างเดียว เช่น HTTP, DNS, ARP, TCP หรือ UDP เป็นต้น นอกจากนี้ท่านยังสามารถกรอกข้อมูลในรูปแบบ Expression ได้ดังตัวอย่างในรูปที่ 8

Source IP Filter

ท่านสามารถระบุไอพีแอดเดรสต้นทางซึ่งเป็นแหล่งกำเนิดของทราฟฟิกโดยเฉพาะได้ Wireshark จะคัดกรองเฉพาะแพ็กเก็ตที่มาจากต้นกำเนิดดังกล่าวเท่านั้น ตัวอย่างเช่น ip.src == 192.168.1.109

คัดกรองเฉพาะไอพีแอดเดรสปลายทาง

เช่นเดียวกับไอพีแอดเดรสต้นทาง ท่านสามารถระบุไอพีแอดเดรสปลายทางที่จะเป็นผู้รับทราฟฟิก วิธีนี้มีประโยชน์เนื่องจากสามารถบอกให้ท่านทราบว่าผู้รับปลายทางได้รับข้อมูลแล้วหรือยัง โดยอาจจะวิเคราะห์ดูแพ็กเก็ตที่แสดงการตอบรับก็เป็นได้ ตัวอย่างเช่น ip.dst == 192.168.1.109

การคัดกรองเฉพาะโปรโตคอล

เป็นเรื่องง่ายที่จะคัดกรองเฉพาะโปรโตคอลแต่ละอย่าง เพียงกรอกชื่อโปรโตคอลเข้าไปในช่อง Filter เท่านั้น ตัวอย่างเช่น http

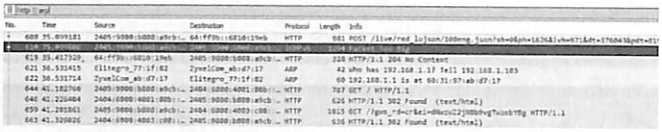
การใช้เงื่อนไข OR ใน Filter

Filter ในลักษณะเงื่อนไขเช่นนี้จะช่วยให้ท่านสามารถคัดกรองเฉพาะแพ็กเก็ตที่เข้ากับเงื่อนไขที่กำหนด จะเป็นเงื่อนไขเดียวหรือมากกว่าก็ได้

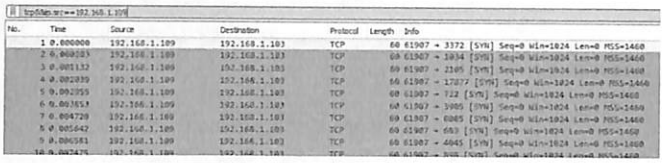
สมมติว่าท่านอาจต้องการเห็นแพ็กเก็ตที่อาจเป็นทั้งโปรโตคอล 'http' หรือ 'arp' ในกรณีนั้นท่านอาจไม่สามารถแยกกันดูแบบคนละโปรโตคอลแต่ต้องการดูพร้อมกันทีเดียว 2 โปรโตคอลก็สามารถทำได้โดยใช้เครื่องหมาย "||" คั่นไว้ระหว่างโปรโตคอลทั้งสอง ตัวอย่างเช่น http || arp

การประยุกต์ใช้งานเงื่อนไข AND ใน Filter

Filter ต่อไปนี้จะช่วยให้ท่านสามารถคัดกรองแพ็กเก็ตที่เข้ากันได้กับเงื่อนไขหลายๆ อย่าง (รูปที่ 9) สมมติว่ามีความต้องการที่จะคัดกรองเฉพาะแพ็กเก็ตที่เป็น HTTP ที่มีแหล่งมาจากไอพี '192.168.1.109' ตัวอย่างเช่น tcp&&ip.src==192.168.1.109 (ดูรูปที่ 10)



รูปที่ 9 แสดงการใช้เงื่อนไข AND



รูปที่ 10 แสดงการใช้ Filter แสดงเฉพาะ TCP ที่มาจากไอพีต้นทาง

คัดกรองโดยใช้หมายเลขพอร์ต

สามารถทำได้โดยใช้ Filter 'tcp.port eq [port-no]' ตัวอย่างเช่น tcp.port eq 80

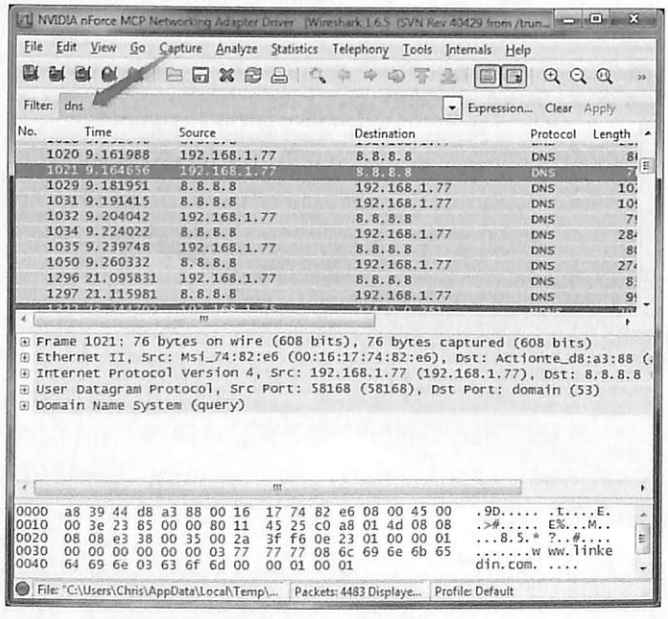
คัดกรองแพ็กเก็ตโดยดูจาก Sequence โดยเฉพาะเจาะจง

ใช้ Filter Syntax ดังนี้ '[prot] contains [ลำดับของไบต์]' ตัวอย่างเช่น tcp contains 01:01:04

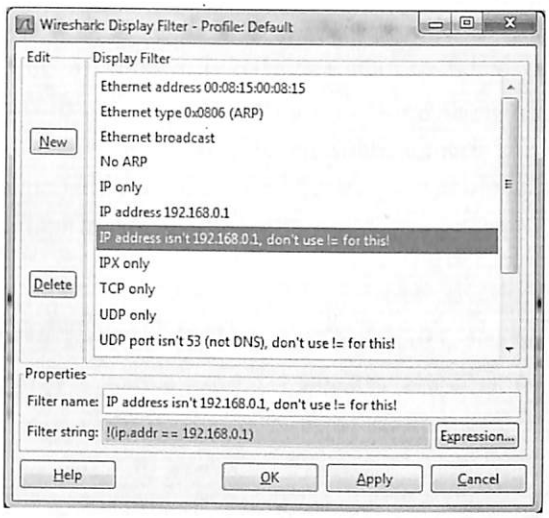
ตัดแพ็กเก็ตออกไปโดยอาศัยค่าไอพีต้นทางหรือปลายทาง

Filter ที่ใช้ในที่นี้คือ 'ip.src != [src_addr]' หรือ 'ip.dst != [dst_add]' ตัวอย่างเช่น ip.dst != 192.168.1.1 (รูปที่ 11)

นอกจากนี้ท่านยังสามารถไปที่เมนู Analyze และเลือก Display Filters เพื่อสร้าง Filter ใหม่ (ดูรูปที่ 12 และ 13)



รูปที่ 11 ตัวอย่างการกรองโปรโตคอลที่ช่อง Filter

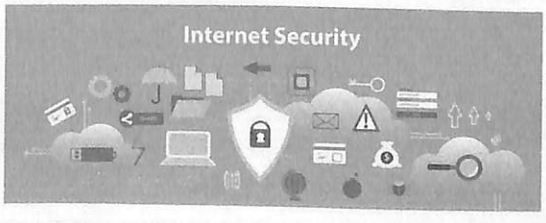


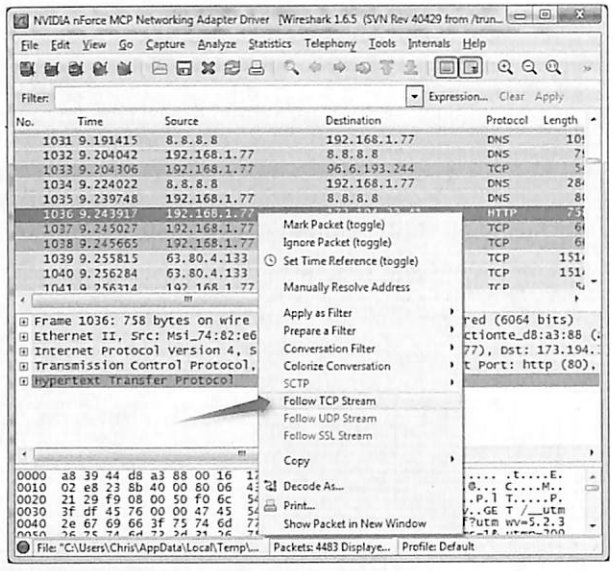
รูปที่ 12 แสดงการตั้งค่า Display Filter

รูปที่ 13 ตัวอย่าง Display Filter สำหรับโปรโตคอลต่างๆ

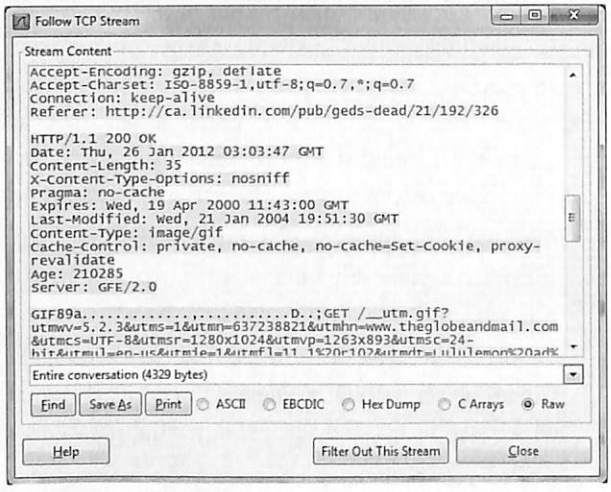
อีกหนึ่งวิธีการที่น่าสนใจคือท่านสามารถคลิกขวาที่ตัวแพ็กเก็ตและเลือก Follow TCP Stream (รูปที่ 14 และ 15)

ท่านจะได้มองเห็นการสนทนา (Conversation) ระหว่างไคลเอนต์กับเซิร์ฟเวอร์

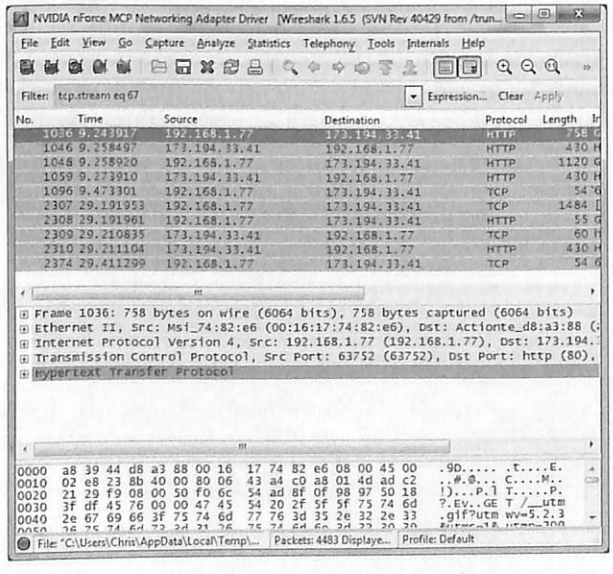




รูปที่ 14 หน้าจอสำหรับเรียกใช้ Follow TCP Stream

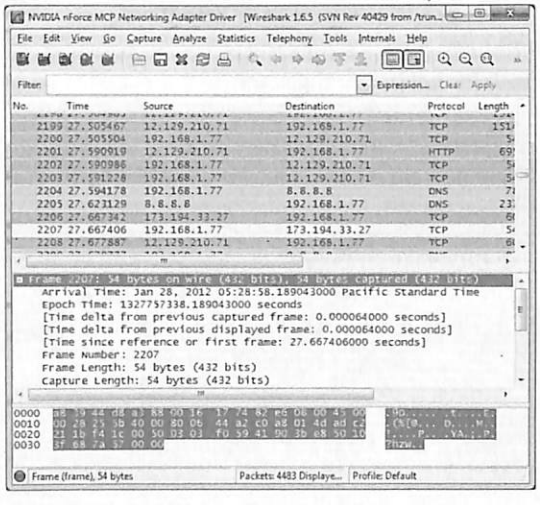


รูปที่ 15 หน้าจอ Follow TCP Stream

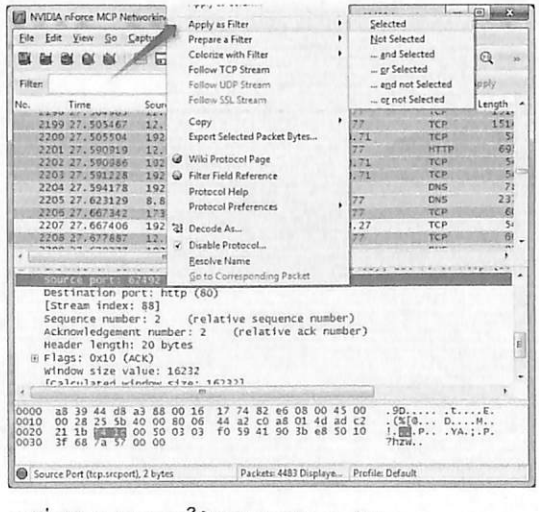


รูปที่ 16 แสดงการสื่อสารระหว่างคอมพิวเตอร์ทั้งสอง

หลังจากปิดหน้าต่างแล้วท่านจะเห็นว่าได้มีการนำเอา Filter มาใช้โดยอัตโนมัติ และแสดงแพ็กเก็ตที่เกี่ยวข้องกับการสื่อสารระหว่างกัน (รูปที่ 16)



รูปที่ 17 แสดงรายละเอียดภายในของแพ็กเก็ต



รูปที่ 18 แสดงการใช้งาน Apply as Filter

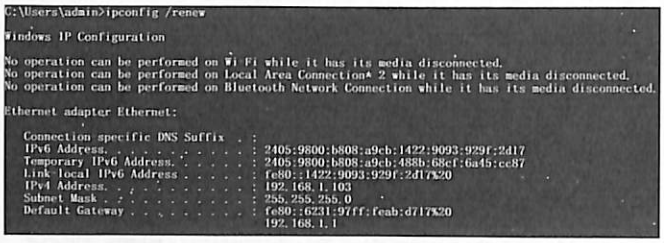
การตรวจสอบแพ็กเก็ต

ลองคลิกที่ตัวแพ็กเก็ตเพื่อเลือก ท่านยังสามารถดูรายละเอียดภายในของมัน (รูปที่ 17)

ท่านสามารถสร้าง Filters จากหัวข้อ Apply as Filter ซึ่งเป็นเมนูย่อย ดังตัวอย่างในรูปที่ 18

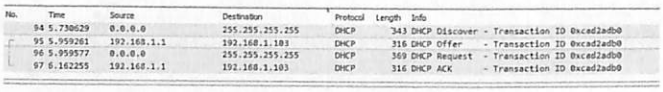
ตัวอย่างการใช้ Wireshark เพื่อวิเคราะห์โปรโตคอลการวิเคราะห์ DHCP

จากรูปที่ 19 จะเห็นว่าหลังจากที่ได้พิมพ์คำสั่ง ipconfig /release เพื่อแสดงเจตนายกเลิกการใช้ไอพีแอดเดรสที่แจกมาให้ใช้งานก่อนหน้านี้ แล้วตามด้วยคำสั่ง ipconfig /renew ซึ่งเป็นคำสั่งที่ใช้สำหรับส่งคำร้องขอไปที่ DHCP Server เพื่อขอรับแจกไอพีจากเซิร์ฟเวอร์

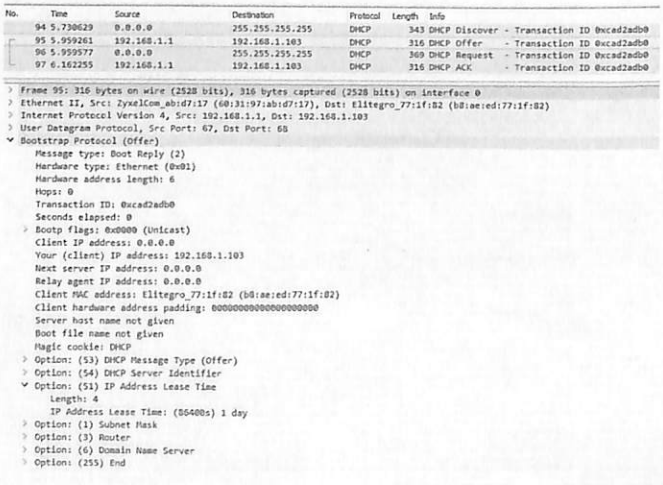


รูปที่ 19 แสดงตัวอย่างการใช้คำสั่ง เพื่อขอรับแจกไอพีใหม่จากเซิร์ฟเวอร์

ในขั้นตอนนี้เรียกว่า DHCP Discovery ซึ่งเป็นขั้นตอนที่เครื่องไคลเอนต์ใช้โปรโตคอล bootp โดยกำหนดไอพีแอดเดรสต้นทางเป็น 0.0.0.0 (ดีฟอลต์ไอพี) และไอพีปลายทางเป็น 255.255.255.255 ซึ่งเป็น Broadcast Address ติดต่อไปที่ DHCP Server หลังจากที่ DHCP Server ได้รับการติดต่อจากไคลเอนต์แล้วจึงได้เสนอไอพีแอดเดรสมาให้ 1 หมายเลข เราเรียก



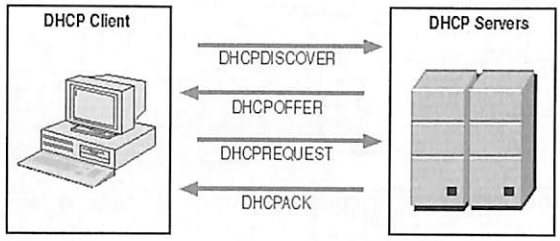
รูปที่ 20 แสดงขั้นตอนการติดต่อขอรับแจกไอพีจากเครื่องไคลเอนต์



รูปที่ 21 แสดงหน้าจอรายละเอียดของ DHCP Offer

ขั้นตอนนี้ว่า DHCP Offer โดยนอกจากไอพีแอดเดรสที่เสนอให้แล้ว ยังให้ข้อมูลข่าวสารเกี่ยวกับเลขหมายไอพีแอดเดรสของ DNS Server ตลอดจนไอพีแอดเดรสของเราเตอร์ซึ่งเป็นเกตเวย์อีกด้วย (รูปที่ 20)

นอกจากนี้ยังให้รายละเอียดที่เกี่ยวข้องกับจำนวนชั่วโมงหรือระยะเวลาที่ให้ใช้งานไอพีแอดเดรสดังกล่าว (ดูรูปที่ 21) โดยเซิร์ฟเวอร์จะใช้ไอพีแอดเดรสของตนเองเป็นไอพีต้นทาง และไอพีแอดเดรสที่แจกให้เป็นไอพีปลายทาง



รูปที่ 22 แสดงขั้นตอนการส่งข่าวสารเพื่อติดต่อขอรับแจกไอพีจากเซิร์ฟเวอร์ของไคลเอนต์

หลังจากที่ไคลเอนต์ได้รับไอพีเรียบร้อยแล้ว เครื่องของไคลเอนต์จะส่งข่าวสารเรียกว่า DHCP Request เพื่อเป็นการยืนยันถึงไอพีแอดเดรสที่ได้รับ และแสดงเจตจำนงเพื่อขอใช้ไอพีแอดเดรสที่แจกให้ดังกล่าว โดยใช้แอดเดรส 0.0.0.0 เป็นไอพีต้นทาง และ 255.255.255.255 เป็นไอพีปลายทาง

เมื่อ DHCP Server ได้รับข่าวสารจากไคลเอนต์เรียบร้อยแล้ว จึงดำเนินการจัดส่งข่าวสารที่เรียกว่า DHCP ACK ออกมาเพื่อรับทราบความต้องการของไคลเอนต์ จากนั้นเริ่มนับเวลาที่ให้เช่าใช้ไอพีดังกล่าว

จากรูปที่ 22 แสดงการทำงานของโปรโตคอลจาก Wireshark มีคำถามต่อไปนี้

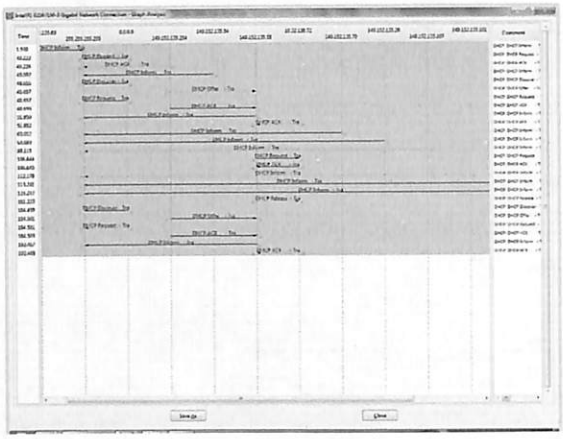
1. การจัดส่งข่าวสารระหว่าง DHCP Server กับไคลเอนต์นั้นขนถ่ายด้วยโปรโตคอลอะไร?

   คำตอบ : UDP (User Datagram Protocol)

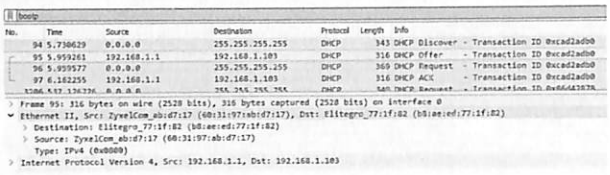
2. เขียนไดอะแกรมแสดงลำดับการทำงานของแพ็กเก็ตทั้ง 4 ที่สื่อสารไปมาระหว่าง DHCP Client กับ DHCP Server ได้แก่ Discover/Offer/Request/ACK ของแต่ละแพ็กเก็ตตลอดจนหมายเลขพอร์ตต้นทางและปลายทาง (รูปที่ 23)

   คำตอบ :

   - Discover Packet มีพอร์ตต้นทางคือ 68 และพอร์ตปลายทางเป็น 67
   - Offer Packet มีพอร์ตต้นทางเป็น 67 และพอร์ตปลายทางเป็น 68
   - Request Packet มีพอร์ตต้นทางเป็น 68 และพอร์ตปลายทางเป็น 67
   - ACK Packet มีพอร์ตต้นทางเป็น 67 และพอร์ตปลายทางเป็น 68



รูปที่ 23 แสดง Flow Diagram ระหว่าง DHCP Client กับเซิร์ฟเวอร์



รูปที่ 24 แสดง MAC Address ของเซิร์ฟเวอร์

3. อะไรคือ MAC Address ของเครื่องเซิร์ฟเวอร์ (รูปที่ 24)

คำตอบ : ZyxelCom_ab:d7:17

4. อะไรคือค่าที่อยู่ใน DHCP Discover Message ซึ่งแตกต่างจาก DHCP Request Message?

คำตอบ : DHCP Discover Message มีค่าเท่ากับ 1 แต่ Request Packet Message มีค่าเท่ากับ 3

5. อะไรคือค่า Transaction-ID ของแต่ละแพ็กเก็ต ซึ่งได้แก่ (Discover/Offer/Request/ACK) DHCP Messages อะไรคือค่า Transaction-ID ในข้อความชุดที่ 2 (Request/ACK) และอะไรคือจุดประสงค์ของ Transaction-ID Field?

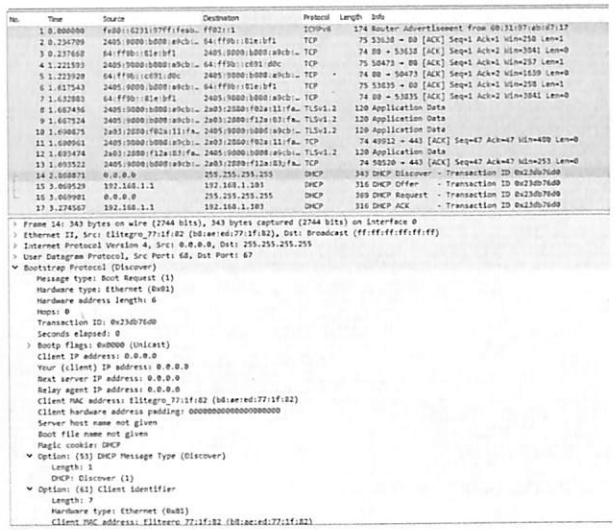
คำตอบ :

- Transaction ID ในข่าวสาร 4 ชุดแรกคือ 0x3e5e0ce3
- Transaction ID ในข่าวสารชุดที่ 2 คือ 0x257e55a3
- Transaction ID จะถูกระบุตัวหากข่าวสารนั้นเป็นส่วนหนึ่งของชุดข่าวสารที่สัมพันธ์กันกับ Transaction

6. เครื่องไคลเอนต์จะใช้ DHCP เพื่อได้รับแจกไอพีแอดเดรส แต่การที่เครื่องของไคลเอนต์จะได้ใช้ไอพีแอดเดรสก็ต่อเมื่อมีการแลกเปลี่ยนข่าวสารไปมาทั้ง 4 ชุดก่อนหน้านี้เสียก่อน หากไอพีแอดเดรสยังไม่สามารถนำมาใช้งานได้จนกว่าจะมีการแลกเปลี่ยนครบทั้ง 4 ข่าวสารแล้ว เมื่อเป็นเช่นนี้อะไรคือค่าที่อยู่ใน IP Datagram ภายในข่าวสารทั้ง 4 ที่แลกเปลี่ยนกัน เช่น (Discover/Offer/Request/ACK DHCP) ลองใช้ Wireshark ตรวจจับและแสดงดูข้อมูลภายในแพ็กเก็ต

คำตอบ :

- ภายใต้ DHCP Discover IP ต้นทางมาจาก 0.0.0.0 ส่วนไอพีปลายทางคือ 255.255.255.255
- ภายใต้ DHCP Offer IP ต้นทางมาจาก 192.168.1.1 ส่วนไอพีปลายทางคือ 255.255.255.255



รูปที่ 25 แสดงไอพีแอดเดรสของ DHCP Server

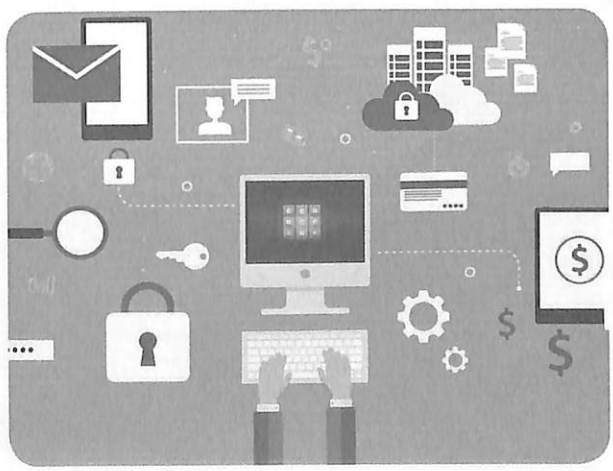
คำตอบ :

- ภายใต้ DHCP Request IP ต้นทางมาจาก 0.0.0.0 ส่วนไอพีปลายทางคือ 255.255.255.255
- ภายใต้ DHCP ACK, DHCP Server จะใช้ไอพีต้นทางเป็น 192.168.1.1 ส่วนไอพีปลายทางเป็น 255.255.255.255

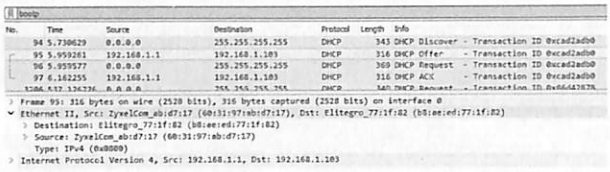
7. อะไรคือไอพีแอดเดรสของ DHCP Server?

คำตอบ : DHCP Server IP Address 192.168.1.1 (รูปที่ 25)

8. ไอพีแอดเดรสอะไรของ DHCP Server ที่ใส่ไว้อยู่ในข่าวสารของ DHCP Offer Message และอะไรคือสิ่งบ่งบอกว่านี่คือข่าวสารที่มาจาก DHCP Server?



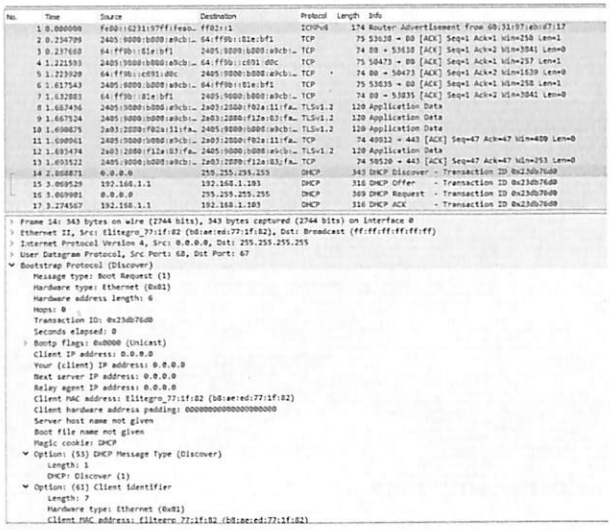
รูปที่ 23 แสดง Flow Diagram ระหว่าง DHCP Client กับเซิร์ฟเวอร์



รูปที่ 24 แสดง MAC Address ของเซิร์ฟเวอร์

คำตอบ :

- ภายใต้ DHCP Discover IP ต้นทางมาจาก 0.0.0.0 ส่วนไอพีปลายทางคือ 255.255.255.255
- ภายใต้ DHCP Offer IP ต้นทางมาจาก 192.168.1.1 ส่วนไอพีปลายทางคือ 255.255.255.255



รูปที่ 25 แสดงไอพีแอดเดรสของ DHCP Server

3. อะไรคือ MAC Address ของเครื่องเซิร์ฟเวอร์ (รูปที่ 24)

   คำตอบ : ZyxelCom_ab:d7:17

4. อะไรคือค่าที่อยู่ใน DHCP Discover Message ซึ่งแตกต่างจาก DHCP Request Message?

   คำตอบ : DHCP Discover Message มีค่าเท่ากับ 1 แต่ Request Packet Message มีค่าเท่ากับ 3

5. อะไรคือค่า Transaction-ID ของแต่ละแพ็กเก็ต ซึ่งได้แก่ (Discover/Offer/Request/ACK) DHCP Messages อะไรคือค่า Transaction-ID ในข้อความชุดที่ 2 (Request/ACK) และอะไรคือจุดประสงค์ของ Transaction-ID Field?

   คำตอบ :

   - Transaction ID ในข่าวสาร 4 ชุดแรกคือ 0x3e5e0ce3
   - Transaction ID ในข่าวสารชุดที่ 2 คือ 0x257e55a3
   - Transaction ID จะถูกระบุตัวหากข่าวสารนั้นเป็นส่วนหนึ่งของชุดข่าวสารที่สัมพันธ์กันกับ Transaction

6. เครื่องไคลเอนต์จะใช้ DHCP เพื่อได้รับแจกไอพีแอดเดรส แต่การที่เครื่องของไคลเอนต์จะได้ใช้ไอพีแอดเดรสก็ต่อเมื่อมีการแลกเปลี่ยนข่าวสารไปมาทั้ง 4 ชุดก่อนหน้านี้เสียก่อน หากไอพีแอดเดรสยังไม่สามารถนำมาใช้งานได้จนกว่าจะมีการแลกเปลี่ยนครบทั้ง 4 ข่าวสารแล้ว เมื่อเป็นเช่นนี้อะไรคือค่าที่อยู่ใน IP Datagram ภายในข่าวสารทั้ง 4 ที่แลกเปลี่ยนกัน เช่น (Discover/Offer/Request/ACK DHCP) ลองใช้ Wireshark ตรวจจับและแสดงดูข้อมูลภายในแพ็กเก็ต

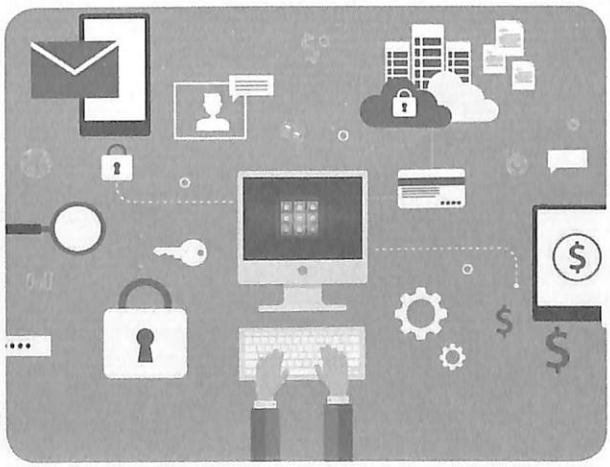
   คำตอบ :

   - ภายใต้ DHCP Request IP ต้นทางมาจาก 0.0.0.0 ส่วนไอพีปลายทางคือ 255.255.255.255
   - ภายใต้ DHCP ACK, DHCP Server จะใช้ไอพีต้นทางเป็น 192.168.1.1 ส่วนไอพีปลายทางเป็น 255.255.255.255

7. อะไรคือไอพีแอดเดรสของ DHCP Server?

   คำตอบ : DHCP Server IP Address 192.168.1.1 (รูปที่ 25)

8. ไอพีแอดเดรสอะไรของ DHCP Server ที่ใส่ไว้อยู่ในข่าวสารของ DHCP Offer Message และอะไรคือสิ่งบ่งบอกว่านี่คือข่าวสารที่มาจาก DHCP Server?



คำตอบ : DHCP Server จะใช้ไอพีแอดเดรส 192.168.1.1 เป็นแอดเดรสที่ใช้แสดงตน (หรือต้นทาง) ในการจัดส่งไอพีแอดเดรสไปยังเครื่องไคลเอนต์ โดยไอพีนี้ปรากฏอยู่ในข่าวสาร DHCP Offer นอกจากนี้ยังมีข่าวสารอื่นๆ เช่น Option: (t=53,l=1) DHCP Message Type = DHCP Offer ซึ่งใช้บอกว่านี่เป็นข่าวสารเกี่ยวกับการนำเสนอไอพีแอดเดรสให้กับไคลเอนต์

ใช้ Wireshark เพื่อการ Troubleshooting ปัญหาระบบเครือข่าย

การวิเคราะห์ปัญหาอัตราการเกิด Packet Retransmission ด้วย Wireshark

Segment Retransmitted หมายถึงการที่เครื่องคอมพิวเตอร์นั้นมีการเชื่อมต่อไปที่ปลายทางที่อาจเป็นเซิร์ฟเวอร์เพื่อการอัปโหลดแฟ้มข้อมูล แต่หลังจากที่มีการส่งข้อมูลหรืออัปโหลดแฟ้มข้อมูลไปได้ส่วนหนึ่งแล้ว จะรอคอยเพื่อให้ผู้รับทำการส่งข่าวสาร Acknowledge มาให้ แต่หากปลายทางหรือผู้รับไม่จัดส่งข่าวสารดังกล่าวมาให้ทันตามกำหนดแล้ว ผู้ส่งจะดำเนินการส่งข่าวสารซ้ำๆ ซึ่งเป็นของเดิมมาให้จนกว่าผู้รับจะจัดส่ง Acknowledge ไปยังผู้ส่ง นี่เป็นธรรมชาติการทำงานของโปรโตคอล TCP ที่ดูแลการขนถ่ายข้อมูล แต่การที่มี Retransmission ปรากฏอยู่บนเครือข่ายมากมายไม่ใช่เรื่องดี การที่เรามี Retransmission มากมายอยู่บนเครือข่ายไม่ใช่เรื่องดีแน่นอน เพราะเป็นสัญญาณบ่งบอกว่าเครือข่ายของท่านกำลังมีปัญหาเรื่องของสุขภาพ นั่นคือ ปัญหาต่างๆ ที่อาจจะนำไปสู่ประสิทธิภาพที่แย่ลงเป็นอย่างมาก (รูปที่ 26)

สาเหตุของการเกิด Retransmission มีมากมายหลายประการ สามารถตรวจจับได้ด้วย Wireshark ต่อไปนี้เป็นสาเหตุที่ทำให้เกิด Retransmission

1. ปัญหาเครือข่ายทำงานช้า มีดีเลย์ (Delay) สูงมาก
2. ปัญหาการตอบสนองจากเซิร์ฟเวอร์ที่ล่าช้า ทำให้การตอบกลับด้วย Acknowledge ช้าลง
3. ปัญหาเครือข่ายมี Error ที่สูงมาก ทำให้ผู้ส่งต้องส่งข้อมูลซ้ำๆ ออกมาบ่อยๆ สาเหตุมาจาก Error ที่อาจเกิดขึ้นจากการทำงานที่ผิดพลาดของอินเตอร์เฟซ เช่น การ์ด LAN เป็นต้น
4. ปัญหาเกี่ยวกับการทำงานที่ผิดพลาด หรือประสิทธิภาพของอุปกรณ์เครือข่ายจนนำไปสู่ความล่าช้า
5. ปัญหาเกี่ยวกับประสิทธิภาพการทำงานของแอพพลิเคชั่น

```
C:\Users\admin>netstat -s -p tcp

TCP Statistics for IPv4

  Active Opens                            = 1842
  Passive Opens                           = 2
  Failed Connection Attempts              = 2
  Reset Connections                       = 325
  Current Connections                     = 31
  Segments Received                       = 510533
  Segments Sent                           = 287204
  Segments Retransmitted                  = 3842

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49689        DESKTOP-I8TNVB9:49690  ESTABLISHED
  TCP    127.0.0.1:49690        DESKTOP-I8TNVB9:49689  ESTABLISHED
```

รูปที่ 26 แสดงหน้าจอ Segments Retransmitted

ปัญหาเกี่ยวกับเซิร์ฟเวอร์ที่ทำให้เกิด Retransmission ได้แก่ ปริมาณการใช้งานซีพียูที่เพิ่มสูงขึ้น หรือหน่วยความจำไม่มากเพียงพอ รวมทั้งปัญหาการ์ด LAN ของเซิร์ฟเวอร์ ตลอดจนแอพพลิเคชั่น

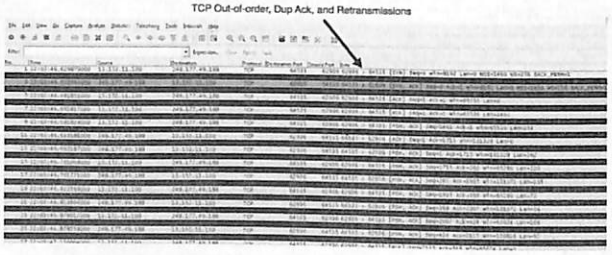
การตรวจสอบ TCP Retransmission ด้วย Wireshark

ขั้นตอนแรกของการตรวจสอบ Retransmission ได้แก่ การกำหนดค่า Filter ดังนี้

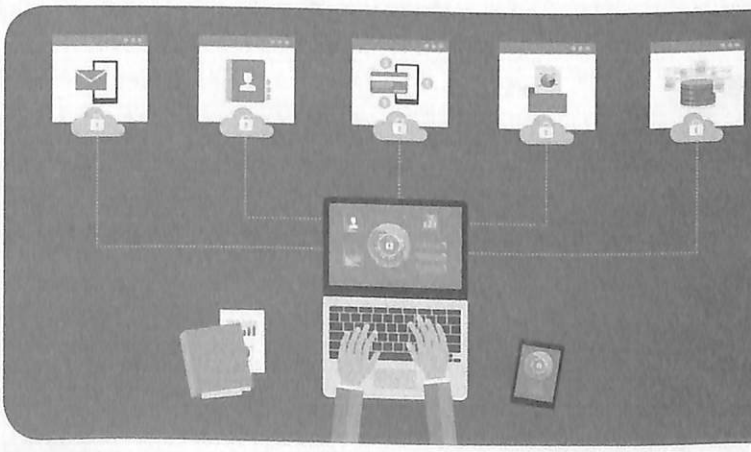
```
tcp.analysis.retransmission
```

หลังจากติดตั้ง Filter นี้เรียบร้อยแล้ว เราจะเริ่มมองเห็นว่ามี Retransmission เกิดขึ้นมากมาย ซึ่งก็แล้วแต่สถานะของเครือข่ายในขณะนั้น หากเมื่อใดที่รู้สึกเครือข่ายทำงานช้าผิดปกติ ท่านอาจต้องพิจารณาเลือกดูปัญหาการเกิด Retransmission แต่อย่างที่เราทราบกันปัญหา Retransmission อาจไม่ได้มีสาเหตุหลักมาจาก Retransmission เพียงอย่างเดียวก็ได้

Wireshark มีการคำนวณ TCP Retransmission บนพื้นฐานการทำงานของหมายเลข SEQ/ACK รวมทั้ง IP และ ID ตลอดจนไอพีแอดเดรสต้นทางและปลายทาง นอกจากนี้ยังรวมถึงหมายเลขพอร์ตและกรอบของเวลาเมื่อได้รับเฟรม เป็นเรื่องง่ายที่ Wireshark สามารถนับจำนวนแพ็กเก็ตที่ซ้ำกันเพื่อบ่งบอกว่านี่คือ Retransmission อย่างไรก็ตามควรตรวจสอบให้แน่ใจว่าไม่ได้ดักจับแพ็กเก็ตหรือเฟรมที่ซ้ำกัน



รูปที่ 27 แสดงหน้าจอขณะกำลังเกิด Retransmission



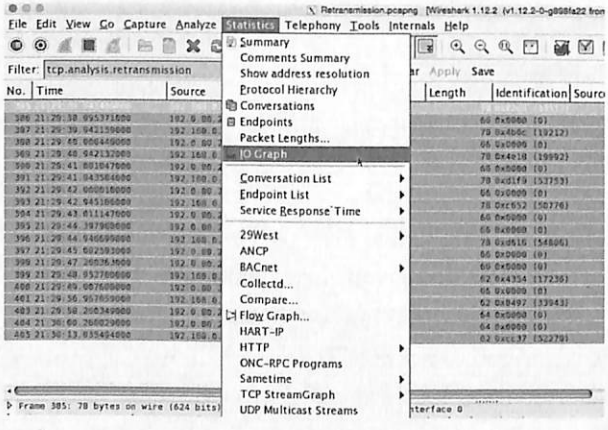
หากท่านได้เปิดหน้าจอดูการดักจับแพ็กเก็ตหรือเฟรมสดๆ อาจได้เห็นว่ามีบรรทัดมากมายที่แสดงถึงการจัดส่งแพ็กเก็ตซ้ำๆ กันมากมาย

จากรูปที่ 27 จะเห็นว่ามี Retransmission เกิดขึ้นจำนวนมากมาย โดย Wireshark แสดงให้เห็นเป็นบรรทัดต่างๆ อย่างไรก็ตามให้สังเกตดูเลขหมายไอพีแอดเดรสที่ซ้ำกัน ที่สำคัญให้สังเกตดูหมายเลข Seq ซึ่งเกิดขึ้นซ้ำกัน ในที่นี้แสดงว่ามี Retransmission เกิดขึ้นอย่างแน่นอน

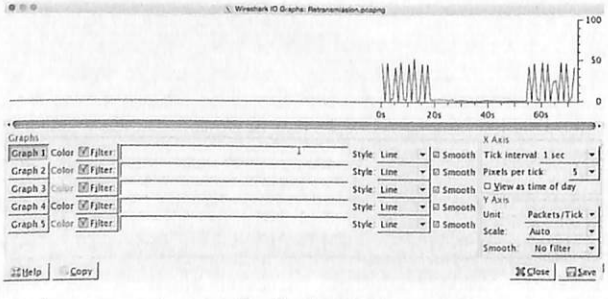
การแสดงกราฟการทำงานของโฮสต์เดี่ยว

เรามาลองเปิดดู IO Graph ใน Wireshark (รูปที่ 28) หน้าต่าง IO Graph สามารถแสดงการนับจำนวนของแพ็กเก็ตต่อวินาที สิ่งแรกที่ได้เห็นคือจำนวนของแพ็กเก็ตต่อวินาทีที่ถูก Drop ทิ้ง ในกรณีนี้จะเห็นว่า Wireshark สามารถดักจับ Error Packet ที่เกิดการสูญเสีย +/- 50% (รูปที่ 29)

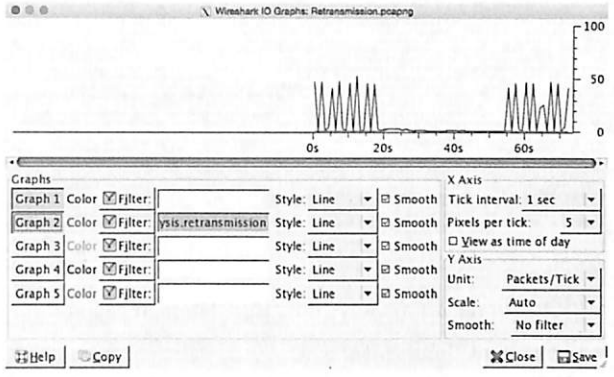
หลังจากใช้ Filter ชื่อว่า : tcp.analysis.retransmission จากรูปที่ 30 จะแสดง Graph 2 เผยให้เห็นเส้นสีแดงระหว่าง 0s ถึง 20s และช่วง 55 ถึง 70s แต่ดูไม่ค่อยชัดเจน จึงต้องดำเนินการปรับแต่งสักเล็กน้อยเพื่อให้เห็นชัดเจนมากขึ้นดังนี้



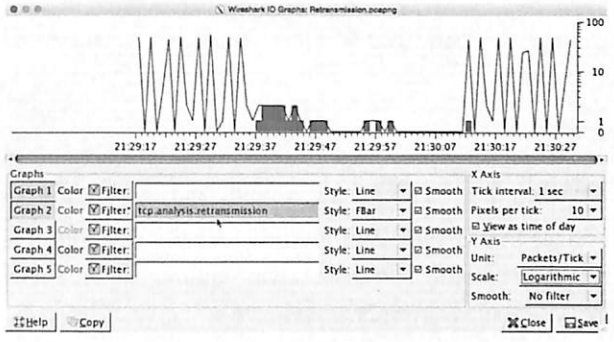
รูปที่ 28 วิธีการเปิด IO Graph



รูปที่ 29 แสดงปริมาณแพ็กเก็ตที่ถูกดักจับ



รูปที่ 30 แสดง Retransmission สังเกตดูแถบเส้นสีแดง



รูปที่ 31 แสดงช่วงเวลาการเกิด Retransmission ในช่วงเวลาต่างๆ

- เปลี่ยนค่า Pixels per Tick ไปเป็น 10 – จะช่วยขยายขนาดแกน X และช่วยให้เห็นชัดเจนมากขึ้น
- เลือก View เป็น Time of day – ทำให้เป็นเปลี่ยนการแสดงของเวลา (คิดเป็นวินาที) บนแกน X ไปเป็นช่วงเวลาของวัน
- เปลี่ยนสเกล (Scale) ของแกน Y ไปเป็น Logarithmic – ซึ่งเป็นการแสดงจำนวนของ Retransmission ที่รับได้ของแพ็กเก็ตคิดเป็นต่อวินาที
- เปลี่ยนสไตล์ของ Graph 2 ไปเป็น FBar

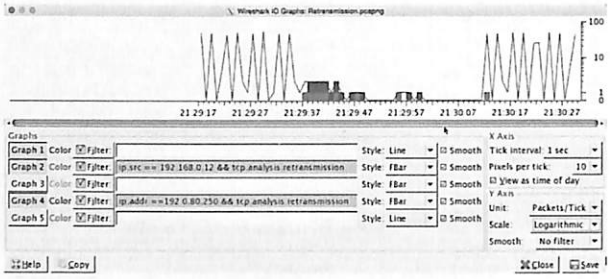
หลังจากที่ได้เปลี่ยนแปลงการตั้งค่าการแสดงผลจะเห็นผลลัพธ์ที่ชัดเจนมากขึ้น จากรูปที่ 31 จะเห็นว่ามีแถบสีแดงที่บริเวณ 21 นาฬิกา 29 นาทีเป็นต้นไป

ใช้ Wireshark แสดงจำนวนของโฮสต์หลายเครื่อง

จากรูปที่ 32 เป็นการเปรียบเทียบระหว่างคอมพิวเตอร์ 2 เครื่อง เป้าหมายของกราฟคือต้องการแสดงจำนวนของ Retransmission ต่อวินาทีสำหรับเครื่องคอมพิวเตอร์แต่ละเครื่อง

ท่านสามารถเพิ่ม Display Filter ให้กับกราฟที่เป็นสีสัน ในที่นี้ผู้เขียนเลือกสีแดงหรือสีฟ้าเพื่อให้ดูชัดเจน ตัวอย่างการตั้งค่า Display Filter สำหรับ Graph 2

```
ip.src == 192.168.0.12 && tcp.analysis.retransmission
```



รูปที่ 32 Graph 4 แสดงสถานะการเกิด Retransmission ในเวลาเดียวกันของโฮสต์ทั้งสอง

ตัวอย่างการตั้งค่า Display Filter สำหรับ Graph 4

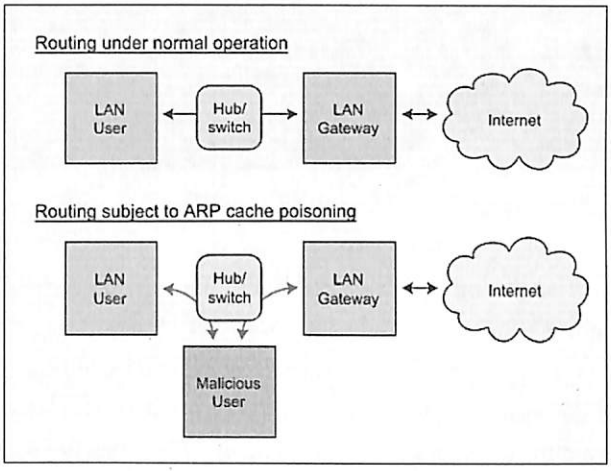
```
ip.addr ==192.0.80.250 && tcp.analysis.retransmission
```

TCP Retransmissions เป็นหนึ่งในปรากฏการณ์ที่สามารถตรวจจับได้เพื่อตรวจสอบหาสาเหตุที่ทำให้เกิดปัญหาต่างๆ บนเครือข่าย เพียงแต่ว่าท่านต้องเข้าใจกลไกการทำงานของโปรโตคอลที่ทำงานภายใต้ TCP/IP แล้ว Wireshark จะช่วยเปิดเผยโลกที่ไม่เร้นลับของ TCP/IP กับการทำงานบนระบบเครือข่าย

ใช้ Wireshark ตรวจสอบการโจมตีแบบ ARP Spoof

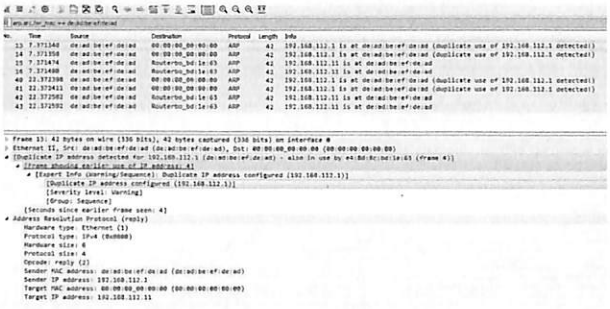
ในระบบเครือข่ายคอมพิวเตอร์ ARP Spoofing, ARP Cache Poisoning หรือ ARP Poison Route เป็นเทคนิคที่ผู้โจมตีส่งข้อความ ARP (Spoofed) ไปยังเครือข่ายท้องถิ่น โดยทั่วไปจุดมุ่งหมายคือการเชื่อมโยงที่อยู่ MAC ของผู้บุกรุกกับที่อยู่ไอพีของโฮสต์อื่น เช่น เกตเวย์เริ่มต้น ทำให้การรับส่งข้อมูลหมายถึงที่อยู่ไอพีนั้นจะถูกส่งไปยังผู้โจมตีแทน (รูปที่ 33)

การปลอมแปลง ARP อาจทำให้ผู้โจมตีสามารถดักฟังข้อมูลในเครือข่าย รวมทั้งสามารถปรับเปลี่ยนกระแสจราจรของข้อมูล หรือหยุดการสื่อสารจราจรได้ บ่อยครั้งที่การโจมตีถูกใช้เป็นช่องเปิดสำหรับการโจมตีอื่นๆ เช่น DoS การโจมตีแบบ Man in The Middle Attack



รูปที่ 33 แสดงลักษณะการโจมตีของ ARP Spoof

รูปที่ 34 แสดงการอัปเดต ARP ตามปกติ



รูปที่ 35 แสดงการโจมตีแบบ ARP Spoof

หรือการปล้นเซสชั่น (Session) การโจมตีสามารถใช้ได้เฉพาะกับเครือข่ายที่ใช้โปรโตคอล ARP และจำกัดเฉพาะเครือข่าย LAN เท่านั้น ในรูปที่ 34 แสดงการอัปเดต ARP ตามปกติ ส่วนรูปที่ 35 จะแสดงการโจมตีแบบ ARP Spoof

ARP Spoof มีลักษณะดังนี้เมื่อใช้ Wireshark จับตาดูการทำงาน

```
192.168.112.1 is at  ab:ab:ab:ab:ab:ab
และ
192.168.112.1 is at 10:10:10:10:10:10
```

Wireshark จะเตือนท่านโดยใช้ข่าวสาร "(duplicate use of <ip> detected!)" ในกรณีนี้มีการใช้ Intercepter NG เพื่อการโจมตีโดยเป็นการทดสอบการโจมตี ท่านสามารถใช้ Filter Expression "arp.duplicate-address-detected" เพื่อค้นหาว่าเกิดเหตุการณ์เกี่ยวกับการโจมตีเช่นนี้หรือไม่อย่างรวดเร็ว

■ ริอบ เอ็นสลิน
ประธานบริหารฝ่าย Global Customer Operations
และคณะกรรมการบริหาร, เอสเอพี เอสอี

การลงทุนอย่างชาญฉลาดจะสามารถสร้างสมาร์ทซิตี้ให้เกิดขึ้นได้อย่างไร

อินเทอร์เน็ต ออฟ ธิงส์ จะช่วยให้เมืองต่างๆ สามารถวัดดาต้าได้มากขึ้น ยังส่งผลให้ดาต้าเติบโตอย่างรวดเร็วมากขึ้นด้วยเช่นกัน เพื่อเพิ่มมูลค่าสูงสุดให้กับดาต้าดังกล่าว เมืองต่างๆ จำเป็นต้องสร้าง ดาต้า แพล็ตฟอร์ม

ทุกวันนี้ บทสนทนาที่เกิดขึ้นเป็นประจำในวงการธุรกิจต่างๆ คงหนีไม่พ้นเรื่องที่ยุคนี้เป็นยุคของบริษัทด้านเทคโนโลยี ซึ่งไม่ได้หมายถึงบริษัทไอทีดั้งเดิมอย่าง Google, Apple, IBM หรือแม้กระทั่งบริษัทเทคโนโลยีอย่าง SAP ซึ่งองค์กรที่กลับได้รับการพูดถึงในวงกว้างขึ้นกลับกลายเป็นบริษัทที่ใครหลายคนไม่ได้มองว่าเป็นองค์กรไอทีเลยเสียด้วยซ้ำ เช่น Airbnb, GO-JEK, Under Armour และกระทั่ง Uber แต่รู้หรือไม่ว่า บริษัทเหล่านี้ ล้วนประกาศตัวว่าพวกเขาเป็นบริษัทไอที และที่มากไปว่านั้น ปัจจุบันนี้ แม้แต่ภาครัฐเอง ก็เริ่มเข้ามามีบทบาทในด้านเทคโนโลยีแล้วเช่นกัน

พื้นที่ของโอกาส

ปัจจุบัน ประชากรโลกมากกว่า 54% ใช้ชีวิตอยู่ในเมือง และภายในปี 2050 ตัวเลขดังกล่าวจะเพิ่มขึ้นเป็น 66% กระแสความเป็นเมือง (Urbanization) นั้นจะเชื่อมโยงไปถึงระบบการศึกษาที่พัฒนาขึ้น การเข้าถึงการรักษาพยาบาลที่ทั่วถึงขึ้น รวมไปถึงการเข้าสังคมและใช้จ่ายได้อย่างคล่องตัวมากขึ้น เมื่อเทคโนโลยีดิจิตอลได้มีการพัฒนาและเดินหน้าไปไกลขึ้น จึงไม่น่าแปลกใจว่าทำไมสังคมในปัจจุบันจึงอยากใช้เทคโนโลยีดิจิตอลเหล่านี้ในทางที่สร้างสรรค์มากขึ้น ยุคอุตสาหกรรม 4.0 จะไม่ได้ถูกจำกัดอยู่ที่ภาคเอกชนอีกต่อไป หากแต่มันกำลังก้าวเข้าสู่พื้นที่ของภาครัฐด้วยเช่นกัน ซึ่งจะเข้ามาเปลี่ยนวิธีการใช้ชีวิตและการทำงานของพวกเราทุกๆ คน

ความร่วมมือระหว่างภาครัฐและภาคเอกชน

ในช่วง 2-3 ปีที่ผ่านมา เราได้เห็นการเปิดรับและปรับใช้เทคโนโลยีอย่างแพร่หลายมากขึ้นของภาครัฐในภูมิภาคอาเซียน สมาร์ท ซิตี้ และเศรษฐกิจดิจิตอล ได้กลายเป็นนโยบายหลักที่รัฐบาลของประเทศต่างๆ ในอาเซียนพยายามผลักดันให้เกิดขึ้น สำหรับประเทศไทย จังหวัดภูเก็ตก็ได้มีการเริ่มพัฒนาสู่การเป็นสมาร์ท ซิตี้ ภายในปี 2020

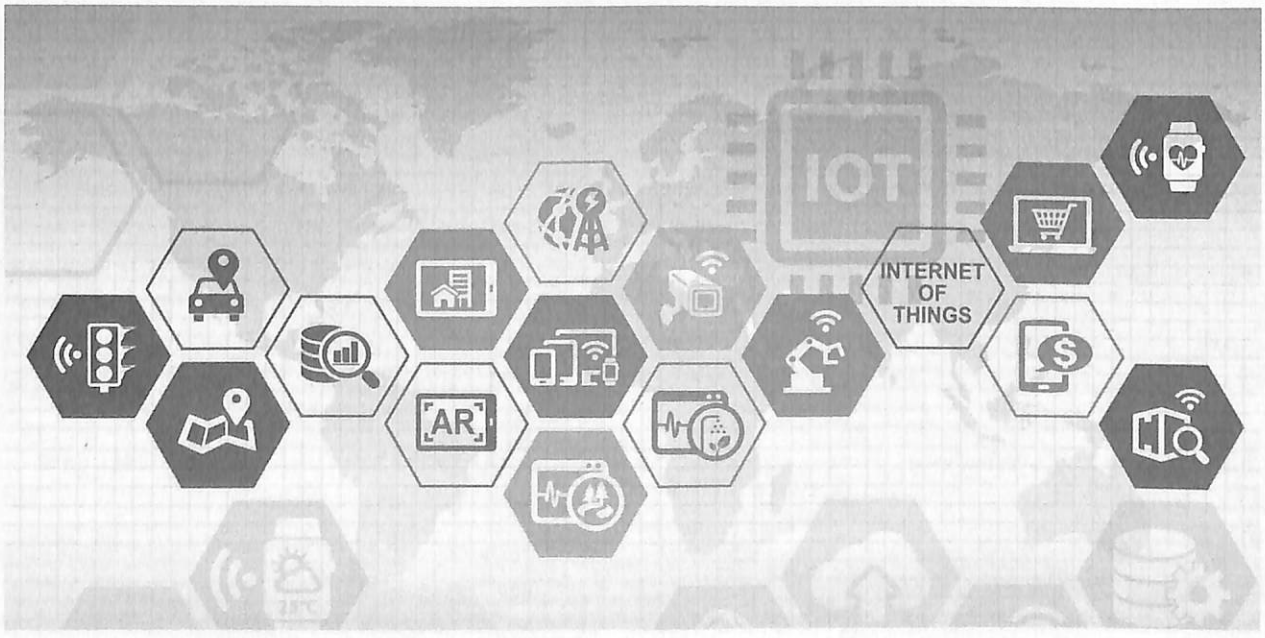
แล้วเช่นกัน ภายใต้คอนเซ็ปต์ **"Smile Smart and Sustainable Phuket"** ด้วยเส้นกั้นระหว่างประชาชน รัฐบาล และธุรกิจเอกชนที่เริ่มเลือนหายไป และการปรับใช้เทคโนโลยีสมัยใหม่อย่าง อินเทอร์เน็ต ออฟ ธิงส์ (ไอโอที) เทคโนโลยีเซ็นเซอร์ รวมถึง machine learning และ advanced analytics ส่งผลให้แนวคิด สมาร์ท ซิตี้ สามารถเกิดขึ้นได้จริง ซึ่งประเด็นเหล่านี้ไม่ได้จำเป็นต้องเกิดขึ้นแต่ในเมืองใหญ่เท่านั้น แต่มันสามารถเกิดขึ้นได้ทุกที่ ตัวอย่างเช่น ที่เมืองฟุกุอิ ประเทศญี่ปุ่น กลุ่มบริษัท NTT Group ได้ร่วมมือกับบริษัทเจ้าของรถประจำทาง Keifuku Bus เพื่อพัฒนาเกียร์ที่ควบคุมด้วยระบบดิจิตอล ซึ่งช่วยเพิ่มความมั่นใจในด้านความปลอดภัยให้กับทั้งคนขับและผู้โดยสารในทุกการขับขี่

โครงการ สมาร์ท ซิตี้ ในประเทศอื่นๆ

ปัจจุบัน เมืองหลวงใหญ่ๆ ทั่วโลก กำลังเริ่มปฏิรูปเมืองของตนในทุกๆ ด้าน ตั้งแต่การปรับปรุงโครงสร้างพื้นฐานให้สามารถใช้งานได้เกิดประโยชน์สูงสุด เพื่อเพิ่มความแข็งแกร่งให้กับเมือง และช่วยให้นโยบายต่างๆ มุ่งไปที่การพัฒนาคุณภาพชีวิตของประชาชนเป็นหลัก เมืองหลวงของอาร์เจนตินา อย่างบัวโนสไอเรส ได้มีการวิเคราะห์ดาต้าจากเซ็นเซอร์ในท่อน้ำรอบตัวเมือง รวมถึงแหล่งทางน้ำอื่นๆ เพื่อใช้ในการตัดสินใจแบบเรียลไทม์เพื่อหลีกเลี่ยงการเกิดน้ำท่วมในตัวเมือง นอกจากนี้ บัวโนสไอเรสยังมีการติดตั้งระบบไฟฟ้าอัจฉริยะ โดยการติดตั้งเทคโนโลยี LED เข้าไปในหลอดไฟจำนวน 91,000 ดวงรอบตัวเมือง พร้อมเพิ่มความสามารถในการเก็บข้อมูล 360 องศา แบบเรียลไทม์ ผ่านระบบเซ็นเซอร์ที่ติดตั้งในหลอดไฟ ตั้งแต่ข้อมูลด้านการระบายน้ำบนท้องถนน ไปจนถึงการเก็บค่าปรับการจอดรถริมถนน เพื่อช่วยให้ผู้เกี่ยวข้องสามารถบริหารจัดการได้จากระยะไกล ผลลัพธ์ที่ได้นั้น นอกจากเรื่องของการบริหารจัดการที่สะดวกขึ้นแล้ว เมืองบัวโนสไอเรสยังสามารถประหยัดพลังงานได้มากขึ้นถึง 50%

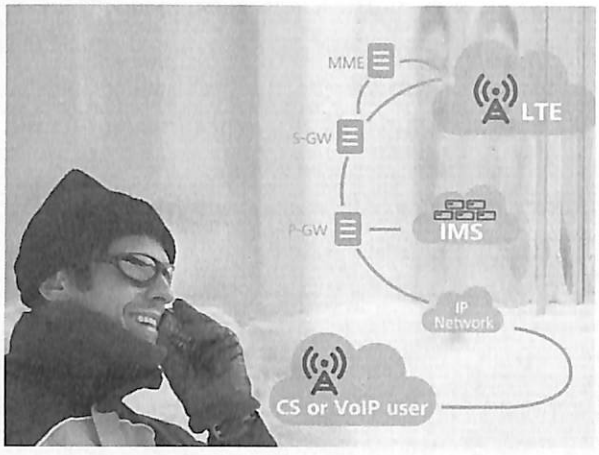
นอกจาก อินเทอร์เน็ต ออฟ ธิงส์ จะช่วยให้เมืองต่างๆ สามารถวัดดาต้าได้มากขึ้น ยังส่งผลให้ดาต้าเติบโตอย่างรวดเร็วมากขึ้นด้วยเช่นกัน เพื่อเพิ่มมูลค่าสูงสุดให้กับดาต้าดังกล่าว เมืองต่างๆ จำเป็นต้องสร้าง ดาต้า แพล็ตฟอร์ม ซึ่งผู้มีส่วนได้ส่วนเสียทั้งหมด (ภาครัฐ, ภาคธุรกิจ, สตาร์ทอัพต่างๆ) สามารถใช้ประโยชน์ได้ร่วมกัน ซึ่งโซลูชั่นแบบบูรณาการเหล่านี้ จะช่วยลดการทำงานแบบไซโลในแต่ละแผนกองค์กร นอกจากนี้ สำหรับกลุ่มธุรกิจประเภทฟินเทคฉุกเฉินต่างๆ การที่มีข้อมูลที่สามารถแชร์ระหว่างกันได้ในทันที ส่งผลให้พวกเขาสามารถตอบสนองต่อเหตุฉุกเฉินต่างๆ ได้รวดเร็วขึ้น ตัวอย่างเช่นเมืองเคปทาวน์ ประเทศแอฟริกาใต้ พวกเขาสามารถประเมินสถานการณ์ได้จากชุดข้อมูลเก่าทั้งหมดที่มี บวกกับข้อมูลเหตุการณ์ที่เกิดขึ้นแบบเรียลไทม์ และการวิเคราะห์โซเชียลมีเดีย ซึ่งชุดข้อมูลเหล่านี้ ช่วยให้พวกเขาสามารถประเมินความเสี่ยงได้อย่างชาญฉลาดที่สุด สามารถเลือกใช้วิธีการรับมือที่เหมาะสม และพร้อมสำหรับทุกสถานการณ์

ดังนั้น ไม่ว่าการลงทุนจะเกิดขึ้นในด้านใดก็ตาม ไม่ว่าจะเป็นด้านการบริหารจัดการการขนส่งและจราจร หรือการลงทุนเพื่อมอบประสบการณ์ที่ดีให้กับประชาชน หรือด้านความปลอดภัยและสุขภาพของประชาชน โอกาสสำหรับการใช้งานเทคโนโลยีใหม่ๆ ที่สำหรับภาครัฐก็ยังมีสูง นอกจากนี้ โซลูชั่นที่ช่วยเพิ่มการมีส่วนร่วมของประชาชน เพิ่มความร่วมมือระหว่างภาครัฐและภาคเอกชน และเพิ่มนวัตกรรมใหม่ๆ สำหรับประชาชนรากหญ้านั้น ไม่เพียงแต่จะช่วยให้ประชาชนได้รับประสบการณ์ที่เหนือกว่าอย่างเดียวเท่านั้น แต่ยังเปิดประตูให้กับธุรกิจก้าวสู่ระดับท้องถิ่นได้อีกด้วย ซึ่งการลงทุนที่มากขึ้นของธุรกิจ จะนำพาซึ่งนวัตกรรมใหม่ๆ ต่อไปในอนาคต ผมภูมิใจที่ เอสเอพี เป็นส่วนหนึ่งของวงจรการลงทุนที่พร้อมสร้างประโยชน์ให้กับทุกฝ่ายในแต่ละประเทศ และเป็นเรื่องน่าตื่นเต้นที่เราจะได้เห็นว่า ยุคดิจิตอลจะช่วยให้เราสามารถเปลี่ยนแปลงประสบการณ์ของทั้งประชาชนทั่วไป และผู้บริโภค ที่จะส่งผลต่อการพัฒนาโลกของเราไปอีกขั้นได้อย่างไร



■ ไพโรจน์ ไววานิชกิจ

เทคโนโลยี VoLTE เพื่อการแข่งขันกับโลก OTT



เทคโนโลยี VoLTE สะท้อนถึงยุทธศาสตร์การแข่งขันในสมรภูมิการให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ระหว่างผู้ประกอบการท้องถิ่นกับผู้ให้บริการในระดับโลก ซึ่งถือว่า VoLTE เป็นเพียงหมัดแรกของการปรับเปลี่ยนสถาปัตยกรรมโทรศัพท์เคลื่อนที่ไปสู่ระบบ 4G เต็มรูปแบบ

พัฒนาการทางเทคโนโลยีเครือข่ายโทรศัพท์เคลื่อนที่ของประเทศไทยรุดหน้าไปอย่างรวดเร็ว ยิ่งนับตั้งแต่หลังจากการจัดให้มีประมูลคลื่นความถี่วิทยุย่าน 900 เมกะเฮิรตซ์และ 1800 เมกะเฮิรตซ์ ซึ่งเป็นย่านความถี่เดิมจากการให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ 2G ด้วยเทคโนโลยี GSM ภายใต้สัมปทานระหว่างเอกชนกับหน่วยงานของภาครัฐ ทั้งฝั่งของบริษัท ทีโอที จำกัด (มหาชน) และบริษัท กสท โทรคมนาคม จำกัด (มหาชน) ซึ่งหมดสัมปทานลงและต้องได้รับการส่งคืนกลับมาให้คณะกรรมการกิจการวิทยุสื่อสาร กิจการโทรทัศน์ และกิจการโทรคมนาคม (กสทช.) เพื่อจัดให้มีการประมูลย่านความถี่ทั้งสองย่านเพื่อนำไปให้บริการโทรศัพท์เคลื่อนที่ในเทคโนโลยีที่สูงกว่ามาตรฐาน 2G เดิม โดยเป็นการประมูลเมื่อไตรมาสที่ 4 ของปี พ.ศ. 2558 ที่ผ่านมา

หลังจากที่ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ทั้งค่ายบริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน) หรือ AIS และบริษัท ทรูมูฟ จำกัดหรือ True Move ได้ช่วงชิงคลื่นความถี่เพิ่มเติมมาเพื่อเสริมจำนวนแถบความถี่เดิมที่ตนมีให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ 3G และ 4G ซึ่งแต่เดิม AIS มีเพียงการให้บริการเครือข่าย 3G บนย่านความถี่ 2100 เมกะเฮิรตซ์ และต่อมาประมูลได้ความถี่ในย่าน 1800 เมกะเฮิรตซ์มาได้ ในขณะที่ค่าย True มีการให้บริการทั้งเครือข่าย 3G และ 4G บนย่านความถี่ที่ตนมีให้บริการทั้ง 850 เมกะเฮิรตซ์ 1800 เมกะเฮิรตซ์และ 2100 เมกะเฮิรตซ์ ซึ่งต่อมาประมูลได้ย่านความถี่ 900 เมกะเฮิรตซ์มาเพิ่ม การแข่งขันในการให้บริการโทรศัพท์เคลื่อนที่ของประเทศไทยก็ทวีความร้อนแรงด้วยการออกโปรโมชั่นการให้บริการชนิดใหม่ๆ พร้อมกับการแข่งขันแสดงศักยภาพในการสื่อสารข้อมูลด้วยอัตราความเร็วสูงบนเครือข่าย 4G ซึ่งแม้กระทั่งบริษัท โทเทิ่ล แอ็คเซ็ส คอมมูนิเคชั่น จำกัด (มหาชน) หรือ DTAC ซึ่งไม่สามารถประมูลย่านความถี่ 900 เมกะเฮิรตซ์และ 1800 เมกะเฮิรตซ์ที่จัดขึ้นเมื่อปลายปี พ.ศ. 2558 มาได้สักย่าน แต่ก็ยังมีย่านความถี่ทั้ง 800 เมกะเฮิรตซ์ 1800 เมกะเฮิตรซ์และ 2100 เมกะเฮิรตซ์ ทำให้มีย่านความถี่มากพอที่จะให้บริการทั้งเทคโนโลยี 3G และ 4G เท่ากับปัจจุบันผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ทั้ง 3 ค่ายมีย่านความถี่มากพอที่จะให้บริการทั้งเครือข่าย 3G และ 4G ส่งผลให้เกิดการแข่งขันทางการตลาดอย่างรุนแรง (ดูตารางที่ 1)

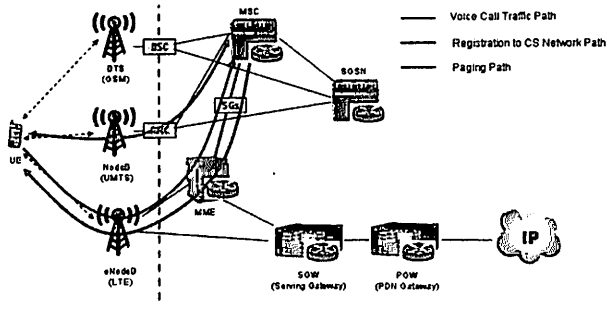
พื้นฐานการทำงานของเครือข่าย LTE 4G

สิ่งหนึ่งที่ไม่ค่อยมีการพูดถึงกันก็คือข้อจำกัดของเครือข่าย 4G ซึ่งใช้เทคโนโลยีที่เรียกว่า Long Term Evolution หรือ LTE ที่มีมาตั้งแต่ยุคแรกของการพัฒนา เครือข่าย 4G ไม่ได้รับการออกแบบมาให้สามารถเชื่อมต่อเพื่อการสื่อสารแบบสนทนาด้วยเสียง (Voice Communication) ทำได้เพียงการเชื่อมต่อเพื่อการรับส่งข้อมูล (Data Communication) ที่มีอัตราเร็วในการสื่อสารสูงมากกว่าเครือข่าย 3G ที่ใช้มาตรฐานการสื่อสารแบบ High Speed Packet Access หรือ

HSPA ซึ่งแปลว่าเมื่อใดก็ตามที่โทรศัพท์เคลื่อนที่ที่รองรับการสื่อสารทั้งมาตรฐาน 3G และ 4G มีการจับใช้งานเครือข่ายสถานีฐานที่รับส่งข้อมูลโดยเทคโนโลยี 4G มีความต้องการเชื่อมต่อวงจรสื่อสารเพื่อการสนทนา โทรศัพท์เคลื่อนที่เครื่องดังกล่าวจะต้องย้ายตัวเองกลับมาจับใช้งานเครือข่ายสถานีฐานที่รองรับการสื่อสารแบบ 3G ซึ่งผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ย่อมจะต้องวางเครือข่าย 3G และ 4G ซ้อนทับกันอยู่แล้วเพื่อรับประกันว่าผู้ใช้บริการเครือข่ายของตนทั้งที่ใช้โทรศัพท์เคลื่อนที่ 3G และโทรศัพท์รุ่นใหม่ๆ ที่รองรับทั้งเทคโนโลยี 3G และ 4G จะสามารถใช้บริการสื่อสารไร้สายได้อย่างไม่ติดขัด การที่โทรศัพท์เคลื่อนที่ซึ่งเดิมเคยจับใช้งานเครือข่าย 4G ต้องโดดมาจับเครือข่ายโทรศัพท์เคลื่อนที่ 3G เพื่อไปขอใช้บริการเชื่อมต่อวงจรสื่อสารเพื่อสนทนา ทำให้ต้องมีการย้ายข้ามเซลล์ระหว่างสถานีฐาน 4G ไปยังสถานีฐาน 3G ยิ่งมีผู้ใช้บริการโทรศัพท์เคลื่อนที่ 4G ต้องการสนทนามากขึ้น ก็จะยิ่งทำให้อัตราการย้ายข้ามเซลล์มากขึ้น ก่อให้เกิดสภาวะรับส่งสัญญาณ (Signaling) ระหว่างเครือข่าย 4G และ 3G มากยิ่งขึ้น จะเป็นภาระ (Loading) ของเครือข่ายโดยไม่จำเป็น เราเรียกปรากฏการณ์ดังกล่าวว่า 3G Circuit Switch Fall Back หรือ CS Fall Back ซึ่งเมื่อการสนทนาสิ้นสุดลง โทรศัพท์เคลื่อนที่ก็จะโดดกลับไปจับเครือข่าย 4G เช่นเดิม ซึ่งก็เป็นการสร้างภาระให้กับเครือข่ายเพิ่มขึ้นอีก

ตารางที่ 1 ย่านความถี่คลื่นวิทยุที่ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยใช้งานในปัจจุบัน

ผู้ให้บริการเครือข่าย	800/850 MHz	900 MHz	1800 MHz	2100 MHz
บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน) "AIS"	-	-	X	X
บริษัท โทเทิ่ล แอ็คเซ็ส คอมมูนิเคชั่น จำกัด (มหาชน) "DTAC"	X	-	X	X
บริษัท ทรูมูฟ จำกัด "True Move"	X	X	X	X



รูปที่ 1 การโอนการเชื่อมต่อไปยังเครือข่าย 3G เพื่อสนับสนุนการเชื่อมต่อเพื่อสนทนาโดยใช้เทคโนโลยี CS Fall Back

รูปที่ 1 เป็นการแสดงเหตุการณ์การเกิดปรากฏการณ์ CS Fall Back ก่อนที่จะกล่าวถึงกระบวนการต่างๆ ขอแนะนำให้รู้จักกับอุปกรณ์ต่างๆ ภายในเครือข่ายโทรศัพท์เคลื่อนที่ก่อน โดยจากรูปที่ 1 มีทั้งส่วนที่เป็นอุปกรณ์ของเครือข่ายโทรศัพท์ 2G, 3G และ 4G อันประกอบด้วยส่วนต่างๆ ดังนี้

- **BTS (Base Station Transceiver)** คือสถานีฐานตามมาตรฐานโทรศัพท์เคลื่อนที่ 2G ที่ใช้เทคโนโลยี GSM ซึ่งจะไม่มีบทบาทเกี่ยวข้องใดๆ กับกระบวนการ CS Fall Back แต่แสดงเพื่อให้เข้าใจบทบาทหน้าที่ของอุปกรณ์ชุมสายโทรศัพท์เคลื่อนที่ 2G/3G ที่จะกล่าวถึงต่อไป
- **BSC (Base Station Controller)** อุปกรณ์ที่ทำหน้าที่บริหารจัดการทั้งด้านการจัดความถี่คลื่นวิทยุ การจัดช่องสัญญาณ การบริหารจัดการสร้างวงจรสื่อสาร การควบคุมการย้ายข้ามสถานีฐานของโทรศัพท์เคลื่อนที่บนเครือข่าย 2G โดยเชื่อมต่อกับบรรดาสถานีฐานหรือ BTS ในด้านหนึ่ง และอีกด้านหนึ่งก็เชื่อมต่อกับชุมสายโทรศัพท์เคลื่อนที่ 2G/3G
- **Node B** เป็นอุปกรณ์สถานีฐานสำหรับรับส่งสัญญาณคลื่นวิทยุที่เป็นมาตรฐานการสื่อสาร 3G ซึ่งใช้เทคโนโลยี HSPA
- **eNode B** เป็นอุปกรณ์สถานีฐานสำหรับการสื่อสารตามมาตรฐาน 4G LTE สิ่งที่ควรจำก็คือในโครงสร้างสถาปัตยกรรมเครือข่ายโทรศัพท์เคลื่อนที่ 4G จะเน้นให้มีอุปกรณ์เชื่อมต่อกันนับตั้งแต่เครื่องลูกข่ายโทรศัพท์เคลื่อนที่ไปจนถึงอุปกรณ์ชุมสายโทรศัพท์เคลื่อนที่หรือเกตเวย์ (Gateway) ให้น้อยชิ้นที่สุดเพื่อให้เวลาหน่วงของการรับส่งข้อมูลน้อยที่สุด จึงไม่มีเรื่องของอุปกรณ์ที่ทำหน้าที่คล้ายกับ RNC หรือ BSC ภายในเครือข่าย 4G
- **RNC (Radio Node Controller)** คืออุปกรณ์ที่บริหารจัดการทรัพยากรทั้งทางด้านความถี่และวงจรสื่อสารและกลไกการให้บริการเครื่องลูกข่ายโทรศัพท์เคลื่อนที่ 3G โดยที่ด้านหนึ่งจะเชื่อมต่อกับบรรดาสถานีฐาน Node B อีกด้านหนึ่งเชื่อมต่อกับชุมสายโทรศัพท์เคลื่อนที่ 2G/3G
- **MSC (Mobile Switching Center)** คือชุมสายโทรศัพท์เคลื่อนที่ที่ทำหน้าที่เชื่อมต่อวงจรสื่อสารทางเสียง (Circuit Switch) โดยในยุคแรกที่ถือกำเนิดขึ้นในยุคของเครือข่าย 2G กลไกการทำงานของ MSC จะใช้และเชื่อมต่อกับเครือข่ายสื่อสัญญาณที่เป็นเทคโนโลยี PCM (Pulse Code Modulation) ซึ่งเป็นการแบ่งช่องสัญญาณเสียงตามเวลาบนวงจรสื่อสารอย่างตายตัว ต่อมาในยุคของเครือข่าย 3G อุปกรณ์ MSC ก็ได้รับการพัฒนาให้รองรับการส่งข้อมูลและเชื่อมต่อกับเครือข่ายสื่อสัญญาณที่เป็นแพ็กเก็ตสวิตช์ โดยมีการพัฒนาอุปกรณ์ MSC ไปเป็นอุปกรณ์ที่ชื่อว่า MSC-Server ทำหน้าที่เป็นศูนย์กลางการควบคุมการบริหารการเชื่อมต่อวงจร ทำงานร่วมกับอุปกรณ์ Media Gateway หรือ MGw ที่เชื่อมต่อกับเครือข่ายแพ็กเก็ตสวิตช์เพื่อรับส่งสัญญาณเสียงที่อยู่ในรูปก้อนข้อมูลแบบแพ็กเก็ต มิใช่ข้อมูลแบบ PCM เหมือนดังในยุคเดิมของมาตรฐาน GSM

- **SGSN (Serving GPRS Support Node)** เป็นอุปกรณ์ชุมสายโทรศัพท์สำหรับให้บริการรับส่งข้อมูลประเภท Data ทั้งกับเครือข่ายสถานีฐาน 2G และ 3G โดยทั้ง BSC ของเครือข่ายสถานีฐาน 2G และ RNC ของเครือข่ายสถานีฐาน 3G จะมีการแยกวงจรเชื่อมต่อกับเครือข่ายชุมสายโทรศัพท์เคลื่อนที่ออกเป็น 2 เส้นทาง เส้นทางแรกคือการรับส่งสัญญาณเสียงพูดไปยังอุปกรณ์ MSC อีกเส้นทางหนึ่งจะรับส่งสัญญาณข้อมูลไปยังอุปกรณ์ SGSN ซึ่งเป็นชุมสายโทรศัพท์เคลื่อนที่แบบแพ็กเก็ตสวิตช์ โดยทั่วไปในทางวิศวกรรมมักจะเรียกชุมสายโทรศัพท์ MSC ว่า CS Core (Circuit Switch Core Network) และเรียกอุปกรณ์ SGSN รวมถึงอุปกรณ์อีกตัวหนึ่งที่ชื่อว่า GGSN (Gateway GPRS Support Node) ว่า PS Core (Packet Core Network) อุปกรณ์ GGSN ที่มิได้แสดงในรูปที่ 1 ทำหน้าที่ทั้งประตูในการเชื่อมต่อโลกอินเทอร์เน็ตหรือเครือข่ายสื่อสารข้อมูลภายนอกที่เชื่อมต่อเข้ามายังเครือข่ายโทรศัพท์เคลื่อนที่ 2G/3G และยังทำหน้าที่บริหารจัดการทรัพยากรของเครือข่าย PS Core ให้เหมาะกับการรองรับรูปแบบข้อมูลที่ทำการสื่อสาร เช่น สื่อสารเพื่อการชมภาพยนตร์ สื่อสารเพื่อการเล่นเกม ฯลฯ
- **MME (Mobility Management Entity)** เป็นอุปกรณ์เครือข่ายชนิดใหม่ที่เพิ่งมีใช้งานภายในเครือข่ายโทรศัพท์เคลื่อนที่ 4G ทำหน้าที่บริหารจัดการสัญญาณควบคุม เชื่อมต่อทั้งอุปกรณ์ชุมสายโทรศัพท์ของเครือข่าย LTE และกับอุปกรณ์ MSC (หรือ MSC-Server) ของเครือข่าย 2G และ 3G เพื่อตรวจสอบตำแหน่งที่อยู่ของเครื่องลูกข่ายโทรศัพท์เคลื่อนที่ของผู้ใช้บริการ เหตุที่ต้องเชื่อมต่อทั้งกับอุปกรณ์เครือข่ายโทรศัพท์เคลื่อนที่ 2G/3G และ LTE ซึ่งก็คือเครือข่าย 4G ก็เพื่อสนับสนุนให้เครื่องลูกข่ายโทรศัพท์เคลื่อนที่ 4G ที่ต้องมีความสามารถแบบ Backward Compatibility เพื่อจับใช้งานเครือข่าย 2G และ 3G สามารถย้ายไปจับเครือข่ายใดๆ ที่เหมาะสมในช่วงเวลานั้นๆ การที่อุปกรณ์ MME ทราบที่อยู่ภายในเครือข่ายโทรศัพท์เคลื่อนที่ต่างๆ ที่เกี่ยวข้อง จะทำให้ผู้ให้บริการเครือข่ายสามารถกำหนดใช้อัตราค่าบริการที่ตรงกับการใช้งานเครือข่ายที่เกี่ยวข้องในขณะนั้น และยังสามารถทำให้เครื่องลูกข่ายโทรศัพท์เคลื่อนที่สามารถเชื่อมต่อเข้ากับอุปกรณ์ชุมสายโทรศัพท์เคลื่อนที่ได้ถูกเทคโนโลยี ที่สำคัญก็คือเป็นอุปกรณ์หลักที่รองรับการพูดคุยสนทนาผ่านทางเครื่องลูกข่ายโทรศัพท์เคลื่อนที่ 4G โดยอาศัยเทคโนโลยี CS Fall Back อันจะได้กล่าวถึงต่อไป
- **SGW (Serving Gateway)** ในเครือข่ายชุมสายโทรศัพท์เคลื่อนที่หรือ Core Network ของมาตรฐาน 4G นั้นจะได้รับการออกแบบให้เพียงอุปกรณ์ SGW และ PGW ทำหน้าที่คล้ายๆ กับอุปกรณ์ SGSN และ GGSN บนเครือข่าย 3G โดยอุปกรณ์ SGW จะทำหน้าที่เป็นเสมือนชุมสายโทรศัพท์แบบแพ็กเก็ตสวิตช์ ซึ่งเมื่อมาถึงยุค 4G แล้วเทคโนโลยีการรับส่งข้อมูลก็ได้รับการพัฒนาให้กลายเป็นเทคโนโลยี IP (Internet Protocol) โดยสมบูรณ์
- **PGW (Packet Data Network Gateway)** สำหรับอุปกรณ์ PGW ทำหน้าที่คล้ายคลึงกับอุปกรณ์ GGSN โดยเป็นประตูเชื่อมต่อไปยังเครือข่ายสื่อสารภายนอกที่ต่อเข้ากับเครือข่ายโทรศัพท์เคลื่อนที่ 4G

กลไกการทำงานสำหรับเชื่อมต่อวงจรสื่อสารสนทนาทางเสียงดังรูปที่ 1 เริ่มจากการที่เครื่องลูกข่ายโทรศัพท์เคลื่อนที่ 4G LTE มีความประสงค์จะโทรออกเพื่อติดต่อกับโทรศัพท์เคลื่อนที่ปลายทาง การติดต่อนี้เป็นการที่ผู้ใช้บริการโทรโดยอ้างอิงเลขหมายปลายทางสากล มิได้หมายถึงการโทรศัพท์ออกผ่านทางแอพพลิเคชั่นประเภท Instant Message หรือ Social Network อย่าง LINE, Facebook Messenger หรือ Skype เพราะในกรณีแบบนี้จะเป็นการสื่อสารข้อมูลแบบแพ็กเก็ต มีการใช้งานโปรโตคอล (Protocol) สำหรับการรักษาคุณภาพของสัญญาณเสียงตามที่ได้รับการกำหนดโดยแอพพลิเคชั่นนั้นๆ ซึ่งไม่เกี่ยวข้องกับการพูดคุยโทรศัพท์แบบทั่วไป ในกรณีนี้เครื่องลูกข่ายโทรศัพท์เคลื่อนที่ 4G จะทำการติดต่อกับอุปกรณ์ MME เพื่อแจ้งให้ทราบว่าการขอติดต่อสื่อสารหลังจากนี้จะเป็นไปเพื่อการพูดคุยสนทนาและเป็นการเชื่อมต่อแบบ Circuit Switch ซึ่งเครือข่าย 4G LTE แบบพื้นฐานไม่ได้รับการออกแบบมาให้รองรับบริการดังกล่าว อุปกรณ์ MME ซึ่งเชื่อมต่อกับเครือข่ายโทรศัพท์เคลื่อนที่ 3G จะทำการติดต่อไปยังอุปกรณ์ MSC หรือ MSC-Server เพื่อแจ้งให้เครือข่ายโทรศัพท์เคลื่อนที่ 3G ทราบว่าจะมีการส่งผ่านโทรศัพท์เคลื่อนที่เครื่องดังกล่าวจากเครือข่าย 4G ไปยังเครือข่าย 3G (CS Fall Back) เพื่อให้อุปกรณ์ MSC ทำการติดต่อสั่งการไปยังอุปกรณ์ RNC และ Node B ที่อยู่ในพื้นที่ที่ให้บริการโทรศัพท์เคลื่อนที่เครื่องดังกล่าว พร้อมจัดสรรทรัพยากรเครือข่าย ทั้งความถี่คลื่นวิทยุ วงจรสื่อสัญญาณระหว่าง Node B ไปยัง RNC จาก RNC ไปยัง MSC หรือ Media Gateway (MSC-Server ทำหน้าที่เป็นสมองจัดการเรื่องสัญญาณควบคุม ในขณะที่ Media Gateway ทำหน้าที่รับวงจรสื่อสัญญาณทางเสียง) และเชื่อมต่อไปยังเลขหมายโทรศัพท์เคลื่อนที่ปลายทางหรือโทรศัพท์พื้นฐานปลายทาง ซึ่งอาจจะเป็นเลขหมายในเครือข่ายเดียวกัน หรือต้องเชื่อมต่อผ่านเครือข่ายโทรคมนาคมอื่นๆ แล้วแต่สถานการณ์

เมื่อถึงจุดนี้การเชื่อมต่อเพื่อสร้างวงจรสนทนาทางเสียงระหว่างโทรศัพท์เคลื่อนที่ 4G ซึ่งทุกรุ่นย่อมต้องมีความสามารถในการเชื่อมต่อย้อนหลังกลับมายังเครือข่าย 3G (Backward Compatibility) ก็จะสร้างวงจรเชื่อมต่อเสียงมายังเครือข่ายโทรศัพท์เคลื่อนที่ 3G ในทางกลับกันหากเป็นกรณีของการโทรเรียกเข้า ไม่ว่าจากโทรศัพท์เคลื่อนที่ภายในเครือข่ายเดียวกันหรือจากเครือข่ายสื่อสารอื่นๆ ไปยังเลขหมายโทรศัพท์เคลื่อนที่ที่ใช้เครือข่าย 4G LTE ผู้ให้บริการเครือข่ายซึ่งตั้งอุปกรณ์ MSC หรือ MSC-Server/Media Gateway เพื่อรอรับการเรียกเข้าเพื่อสนทนาจากเครือข่ายภายนอกจะส่งผ่านสัญญาณการเรียกเข้าและสร้างวงจรการเรียกเข้ามายังเครือข่าย CS Core ของเครือข่าย 3G ซึ่งอุปกรณ์ MSC ที่ดูแลสถานีฐาน 3G ที่โทรศัพท์เคลื่อนที่ 4G นั้นใช้งานก็จะส่งสัญญาณแจ้งผ่านมายังอุปกรณ์ MME ว่ามีการโทรเรียกเข้าไปยังเลขหมาย 4G ปลายทาง สิ่งที่เกิดขึ้นตามมาก็คืออุปกรณ์ MME จะทำการติดต่อสื่อสารกับโทรศัพท์เคลื่อนที่ 4G

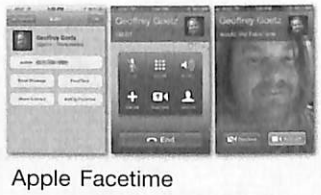
(Paging) และกำหนดให้โทรศัพท์เคลื่อนที่ 4G เครื่องดังกล่าวทำการติดต่อสื่อสารกับสถานีฐาน 3G ที่อยู่ในพื้นที่ใช้งานของตน และส่งสัญญาณโทรเรียกเข้า (Ringing) ไปยังโทรศัพท์เครื่องดังกล่าว หากผู้ใช้งานกดรับสายก็จะมีผลทำให้เกิดการสร้างวงจรสื่อสารระหว่างโทรศัพท์เคลื่อนที่ 4G ซึ่งขณะนี้เปลี่ยนสภาพการทำงานไปเป็นโทรศัพท์เคลื่อนที่ 3G เชื่อมต่อผ่านอุปกรณ์ Node B และ RNCและเข้าสู่อุปกรณ์ MSC หรือ MSC-Server/Media Gateway อันเป็นไปตามเส้นทางของการรับส่งสัญญาณดังแสดงในรูปที่ 1 เหตุการณ์ทั้งสองกรณีนี้เกิดขึ้นบนเครือข่ายโทรศัพท์เคลื่อนที่ 4G ที่เป็นมาตรฐาน LTE โดยพื้นฐาน ทั้งนี้มีเงื่อนไขสำคัญว่าผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ 4G ดังกล่าวต้องมีเครือข่าย 3G ของตนเองวางซ้อนอยู่ด้วยกัน หรือหากเป็นกรณีของผู้ให้บริการเครือข่าย 4G ที่เป็นผู้ประกอบการรายใหม่ไม่เคยมีเครือข่าย 3G เป็นของตนเอง ผู้ประกอบการรายดังกล่าวก็จำเป็นจะต้องทำมีการสัญญา Roaming หรือขอเข้าใช้งานข้ามเครือข่ายกับผู้ให้บริการเครือข่าย 3G รายอื่นๆ อันหมายถึงการเกิดต้นทุนในการ Roaming ตามปริมาณการโทรศัพท์เข้าและออกของบรรดาผู้ใช้บริการโทรศัพท์เคลื่อนที่ 4G ของตนเอง

แรงผลักดันต่อเทคโนโลยี VoLTE

ในแง่ของกลไกการทำงานทางเทคโนโลยีของ CS Fall Back ก็มิได้เป็นปัญหาสำคัญประการใด ทั้งในมุมมองทางด้านวิศวกรรมเครือข่ายและคุณภาพการสนทนาที่ผู้ใช้บริการจะพึงรับรู้ อันที่จริงแล้วผู้ใช้บริการโทรศัพท์เคลื่อนที่ 4G ทั่วไปก็ไม่จำเป็นที่จะต้องรับรู้กลไกการทำงานแบบ CS Fall Back แต่อย่างใด เพียงคุณภาพของการใช้โทรศัพท์เพื่อสนทนามีความชัดเจน ผู้ใช้งานก็จะถือว่าไม่เกิดปัญหาแต่ประการใดแล้ว แต่สิ่งที่เป็นเหตุผลักดันให้ต้องเกิดการเร่งพัฒนาเทคโนโลยี Voice over LTE หรือ VoLTE นั้นกลับเกิดมาจากเรื่องของการประหยัดต้นทุนเครือข่ายเพื่อที่ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่สามารถมีต้นทุนประหยัดพอที่จะแข่งขันกับผู้ให้บริการที่ให้บริการคุยสนทนาด้วยเสียงผ่านทางแอพพลิเคชั่นซึ่งโดยทั่วไปก็คือบรรดาผู้ให้บริการแอพพลิเคชั่นด้าน Social Network โดยทั่วไปจะเรียกว่าเป็นผู้ให้บริการประเภท OTT (Over-The-Top) อันหมายถึงผู้ที่อาศัยทรัพยากรเครือข่ายโทรคมนาคม เช่น เครือข่ายโทรศัพท์เคลื่อนที่ มาสร้างประโยชน์ให้กับตนเองโดยที่ไม่ต้องช่วยแบกรับภาระใดๆ ต่อผู้ให้บริการเครือข่ายเลย

ความนิยมในการใช้งานแอพพลิเคชั่นบนโทรศัพท์เคลื่อนที่สมาร์ทโฟนซึ่งปัจจุบันกลายเป็นอุปกรณ์สื่อสารที่มีสัดส่วนมากที่สุดในโลก ขณะที่โทรศัพท์เคลื่อนที่แบบดั้งเดิมหรือ Legacy Phone ใกล้จะสูญหายไปจากโลกของผู้บริโภคด้านโทรคมนาคม แอพพลิเคชั่นในหมวดที่ให้บริการสนทนาทางเสียงโดยใช้การเชื่อมต่อผ่านทางการสื่อสารข้อมูลมีอยู่มากมาย มีทั้งที่ดำเนินยุทธศาสตร์ด้วยการสร้างกลุ่มผู้ใช้งานจำนวนมหาศาลในรูปแบบของ Social Network ก่อนจากนั้นจึงเพิ่มขีดความสามารถในการให้ผู้ใช้บริการสามารถโทรหากันได้โดยไม่คิดค่าใช้จ่ายในการให้บริการประการใด เช่น Facebook Messenger, Line Call, WhatsApp ฯลฯ และยังมีทั้งที่ได้รับการสร้างขึ้นมาโดยผู้ให้บริการระบบปฏิบัติการสำหรับสมาร์ทโฟน ซึ่งผู้ใช้บริการย่อมจำเป็นจะต้องลงทะเบียนความมีตัวตน (Identity หรือ ID) กับผู้ให้บริการระบบปฏิบัติการก่อนที่จะใช้งานขีดความสามารถพื้นฐาน เช่น ระบบจัดเก็บหมายเลขโทรศัพท์ (Contact) การเข้าถึง AppStore การได้ใช้สิทธิ์บันทึกข้อมูลผ่านเครือข่าย Cloud Computing ฯลฯ ซึ่งเมื่อมี ID แล้วผู้ใช้ระบบปฏิบัติการก็สามารถใช้แอพพลิเคชั่นที่ได้รับการสร้างขึ้นเพื่อการพูดคุยสนทนา ไม่ว่าจะเป็นแอพพลิเคชั่น Hangout ที่สร้างขึ้นมาเพื่อให้บริการสนทนากับผู้ใช้ระบบปฏิบัติการ Android ของค่าย Google ซึ่งถึงเวลาให้บริการจริงๆ ผู้ใช้ระบบปฏิบัติการอื่นๆ สามารถดาวน์โหลด Hangout ไปใช้งานได้ เพียงแค่ขอให้ลงทะเบียนเป็นสมาชิกกับ Google เช่น เปิดใช้งานอีเมลบน Gmail ก็เพียงพอแล้ว นอกจากนั้นยังมี Facetime ซึ่งสร้างขึ้นโดย Apple เพื่อให้บริการสนทนาแก่ผู้ใช้ระบบปฏิบัติการ iOS ของตน ที่สำคัญยังมีแอพพลิเคชั่นที่ให้บริการสนทนา เช่น Skype ซึ่งเกิดมาตั้งแต่ยุคแรกๆ และค่อยผันตัวเองมาเป็นการให้บริการแบบ Social Network และยังเป็นแอพพลิเคชั่นที่มีผู้ใช้งานเพื่อสนทนาแบบ OTT อย่างเหนียวแน่นอีกตัวหนึ่ง (รูปที่ 2)

Facebook Messenger



Apple Facetime

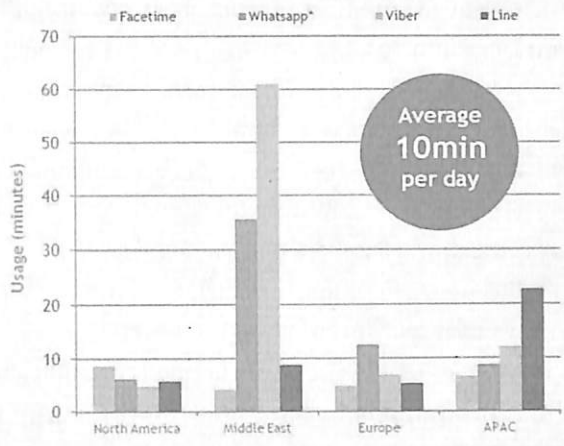
WhatsApp

Line Call

รูปที่ 2 บรรดาแอพพลิเคชั่น Social Network ที่กลายเป็นคู่แข่งแย่งชิงส่วนแบ่งทางการตลาดของการสนทนาเสียงกับผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่

เนื่องจากโทรศัพท์เคลื่อนที่สมาร์ทโฟนมีการแพร่กระจายใช้งานไปทั่วทุกภูมิภาคทั่วโลก อุปกรณ์สมาร์ทโฟนเกิดขึ้นตั้งแต่ยุคของการใช้งานเครือข่ายโทรศัพท์เคลื่อนที่ 3G โดยการเปิดตัวของ iPhone ในปี พ.ศ. 2551 ตามมาด้วยการแข่งขันจากระบบปฏิบัติการ Android จากค่าย Google ซึ่งทั้งสองค่ายนำจุดเด่นในเรื่องของ AppStore ที่เปิดกว้าง ส่งเสริมให้มีผู้พัฒนาแอพพลิเคชั่นต่างๆ ให้ใช้งานเป็นจำนวนมาก ทำให้เกิดการแข่งขันสร้างแอพพลิเคชั่นทางด้าน Social Network และพัฒนาต่อไปเป็นการใช้ประโยชน์จากฐานผู้ใช้บริการ Social Network ที่แอพพลิเคชั่นแต่ละรายมีอยู่มาสร้างเป็นขีดความสามารถในการโทรศัพท์สนทนากัน โดยผู้ใช้บริการไม่มีภาระค่าใช้จ่ายใดๆ ทั้งสิ้น ยกเว้นค่า Air Time ที่ตนต้องรับส่งข้อมูลผ่านเครือข่ายโทรศัพท์เคลื่อนที่ แต่หากมีการใช้งานผ่านทางเครือข่าย Wi-Fi ที่ผู้ให้บริการมิได้คิดค่าใช้จ่ายใดๆ เช่น Wi-Fi ที่บ้าน ที่สำนักงาน หรือตามห้างสรรพสินค้า ฯลฯ ก็จะยิ่งเป็นประโยชน์ต่อการลดต้นทุนของผู้ใช้บริการแอพพลิเคชั่นนั้นๆ ยิ่งเมื่อเครือข่ายโทรศัพท์เคลื่อนที่ได้รับการพัฒนาขีดความสามารถให้สื่อสารได้ด้วยอัตราความเร็วที่สูงขึ้น จนสามารถแบ่งอัตราเร็วในการสื่อสารที่ไม่ต่ำให้กับผู้ใช้บริการแต่ละรายในกรณีที่มีการแย่งกันใช้งานเครือข่ายพร้อมกันหลายๆ คน อัตราความเร็วในการสื่อสารที่ได้นั้นก็ยิ่งทำให้คุณภาพในการสนทนาเสียงผ่านแอพพลิเคชั่นแบบ OTT ดียิ่งขึ้น ไม่มีความล่าช้า (Delay) ของเสียง ความชัดเจนของเสียงดี จนทำให้ผู้ให้บริการแอพพลิเคชั่นสามารถเพิ่มความสามารถในการสนทนาแบบเห็นหน้า (Video Call) และกระทั่งเมื่อเร็วๆ นี้ผู้ให้บริการอย่าง LINE ในประเทศไทยยังถึงกับเปิดให้บริการสนทนาทางเสียงได้พร้อมๆ กันสำหรับกลุ่มการใช้งาน LINE ที่ผู้ใช้งานแต่ละคนจัดตั้งขึ้นเป็นการสื่อสารแบบ Voice Conference ซึ่งแน่นอนว่าผู้ใช้บริการแอพพลิเคชั่นแต่ละรายไม่มีภาระค่าใช้จ่ายใดๆ กับการใช้บริการเหล่านี้เพิ่มเติม นี่คือภัยคุกคามต่อรายได้จากการให้บริการสนทนาทางเสียงของผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่อย่างเห็นได้ชัด

รูปที่ 3 แสดงให้เห็นถึงการแจกแจงความนิยมในการใช้งานแอพพลิเคชั่นแบบ OTT ในการพูดคุยสนทนา แต่ละภูมิภาคก็จะมีความนิยมใช้งานแอพพลิเคชั่นแต่ละตัวแตกต่างกัน ขึ้นอยู่กับความสำเร็จในการทำตลาดของผู้ให้บริการแอพพลิเคชั่นรายนั้นๆ ผู้บริโภคในทวีปอเมริกาเหนือมีความสนใจใช้งานแอพพลิเคชั่นแต่ละรายใกล้ๆ กัน โดยอาจจะมีผู้นิยมใช้แอพพลิเคชั่น Facetime มากกว่าแอพพลิเคชั่นอื่นๆ อันสะท้อนให้เห็นว่าน่าจะมาจากฐานผู้ใช้โทรศัพท์เคลื่อนที่ iPhone ที่มีอยู่เป็นจำนวนมาก สำหรับในภูมิภาคตะวันออกกลางมีความนิยมใช้งานแอพพลิเคชั่นเพื่อการสนทนาทางเสียงเป็นอย่างมาก เห็นได้ชัดว่าผู้บริโภคมีความนิยมใช้แอพพลิเคชั่นอย่าง Viber และ WhatsApp เป็นอย่างมาก โดยค่าเฉลี่ยของการใช้โทรศัพท์ผ่านแอพพลิเคชั่น Viber มีสูงสุดถึง 61 นาทีต่อวัน ตามมาด้วย WhatsApp ที่ 35 นาทีต่อวัน สะท้อนให้เห็นถึงคุณภาพของเครือข่ายสื่อสารไร้สายทั้งเครือข่ายโทรศัพท์เคลื่อนที่ 3G/4G และเครือข่าย Wi-Fi แอพพลิเคชั่น WhatsApp ได้รับความนิยมในการใช้งานมากที่สุดเมื่อเทียบกับแอพพลิเคชั่นอื่นๆ ในกลุ่มผู้บริโภคที่อาศัยอยู่ในทวีปยุโรป สำหรับในทวีปเอเชีย LINE Call ได้รับความนิยม



รูปที่ 3 พฤติกรรมการใช้งานแอพพลิเคชั่นเพื่อการสนทนาแบบ OTT ซึ่งเป็นคู่แข่งกับการให้บริการ Voice บนเครือข่ายโทรศัพท์เคลื่อนที่ (ข้อมูลจากบริษัท Alcatel-Lucent)

ใช้งานผ่านโทรศัพท์มากที่สุด โดยเปรียบเทียบเวลาที่ใช้โทรต่อวันเทียบกับแอพพลิเคชั่นอื่นๆ คือประมาณ 22 นาทีต่อวัน ตัวเลขดังกล่าวย่อมมีการพัฒนาที่สูงขึ้น แน่นอนว่าแอพพลิเคชั่นที่ใช้งานรายใหม่ๆ อาจเกิดขึ้นและมีการแย่งชิงส่วนแบ่งกับแอพพลิเคชั่นรายเดิมๆ แต่เป็นที่แน่ชัดว่าแนวโน้มของการโทรศัพท์สนทนาทางเสียงผ่านทางแอพพลิเคชั่นย่อมจะต้องเกิดมีมากขึ้นอย่างแน่นอน

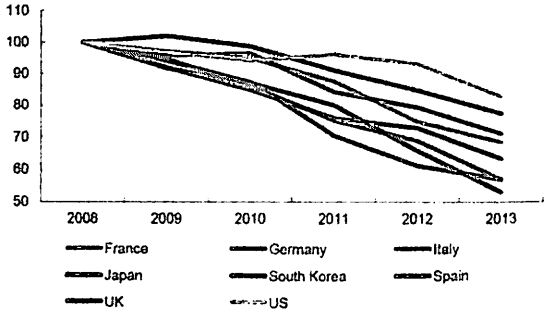
สาเหตุของความนิยมใช้งานโทรศัพท์สนทนาผ่านแอพพลิเคชั่นนอกเหนือจากการประหยัดค่าใช้จ่าย ผู้บริโภคจ่ายเพียงค่าเชื่อมต่อเพื่อรับส่งข้อมูลผ่านเครือข่ายโทรศัพท์เคลื่อนที่ ซึ่งโดยทั่วไปมีแพ็กเกจการใช้งานมาตรฐานที่ตนจะเลือกใช้งานตามพฤติกรรมของตนเองอยู่แล้ว ยิ่งหากเป็นการใช้งานผ่านเครือข่าย Wi-Fi ที่บ้าน โรงแรม หรือสำนักงานก็จะไม่มีค่าใช้จ่ายใดๆ เกิดขึ้น ค่าใช้จ่ายผ่านทางแอพพลิเคชั่นก็ไม่มี ยังมีประเด็นในเรื่องของความสามารถในการโทรติดต่อสื่อสารกับใครก็ได้ที่มีชื่อเป็นเพื่อนของตนบนเครือข่าย Social Network ที่ใช้งานนั้นๆ โดยไม่ต้องสนใจว่าเพื่อนคนนั้นใช้บริการเครือข่ายโทรศัพท์เคลื่อนที่รายใด ซึ่งหมายความว่าการเรียกขานตัวตนของผู้ที่ตนต้องการติดต่อนั้นจะไม่เกี่ยวข้องกับเลขหมายโทรศัพท์ เช่น LINE Call ก็จะอ้างอิงถึง LINE ID ของคนๆ นั้น Facebook Messenger ก็จะอ้างอิงถึง Facebook Username ฯลฯ เป็นการยิ่งทำให้ความสำคัญของเลขหมายโทรศัพท์เคลื่อนที่ที่เคยมีบทบาทสำคัญมากในอดีตลดน้อยลงเรื่อยๆ หมายความว่าผู้ใช้งานโทรศัพท์เคลื่อนที่ในปัจจุบันไม่ค่อยมีความยึดติดว่าจะต้องใช้บริการ 3G หรือ 4G จากผู้ให้บริการเครือข่ายรายเดิมๆ ของตน แต่สามารถเปลี่ยนค่ายได้ทันทีหากคิดว่าราคาค่าบริการที่ตนใช้งานไม่คุ้มค่า คุณภาพของเครือข่ายไม่ดีเทียบเท่าผู้ให้บริการรายอื่นๆ ยิ่งในประเทศไทยที่มีการบังคับใช้มีบริการ Number Portability อันทำให้ผู้บริโภคสามารถย้ายค่ายโทรศัพท์เคลื่อนที่ได้โดยที่ยังใช้เลขหมายโทรศัพท์เคลื่อนที่เดิมติดตัวไปได้ ก็ยิ่งเป็นภัยคุกคามต่อการรักษาฐานผู้ใช้บริการโทรศัพท์เคลื่อนที่ของตน ท้ายที่สุดก็คือการใช้บริการโทรศัพท์สนทนาผ่านแอพพลิเคชั่น OTT เหล่านี้กลายเป็น

สูตรมาตรฐานสำหรับผู้คนที่มีความประสงค์จะโทรศัพท์หากันเมื่ออยู่ต่างแดน ทำให้ไม่ต้องแบกรับภาระค่าโทรศัพท์ข้ามประเทศ (IDD หรือ International Dialing) รวมถึงการคิดค่าบริการ IR (International Roaming) สำหรับการรับสายโทรศัพท์ที่เรียกเข้าหาตนเองขณะอยู่ต่างประเทศ รวมถึงการใช้โทรศัพท์ของตนเองโทรหาผู้อื่นเมื่ออยู่ต่างประเทศอีกด้วย สิ่งที่เห็นได้ชัดในปัจจุบันก็คือการที่ผู้บริโภคถามหา LINE ID หรือ Facebook Account เมื่อเพิ่งรู้จักกัน อันเป็นการยืนยันว่าโลกของการสนทนาทางเสียงได้ถูกแอพพลิเคชั่นบนสมาร์ทโฟนแย่งชิงลูกค้าผู้ใช้บริการไปอย่างรวดเร็ว

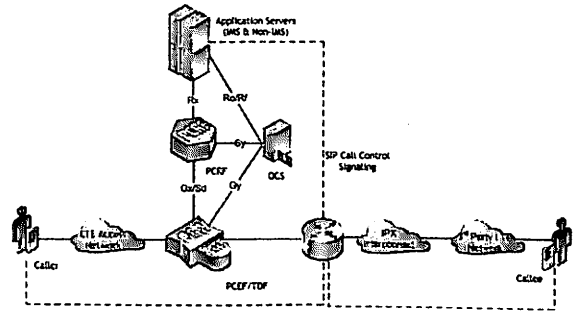
ผลที่เกิดขึ้นต่อรายได้ของการให้บริการสื่อสารทางเสียงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ ทำให้บริษัทผู้ให้เครือข่ายโทรศัพท์เคลื่อนที่ต้องปรับกลยุทธ์ทั้งหมดทั้งในเรื่องของเทคโนโลยีเครือข่าย โดยเฉพาะอย่างยิ่งการนำมาตรฐาน VoLTE มาใช้งานกับเครือข่ายโทรศัพท์เคลื่อนที่ 4G และตามมาด้วยยุทธศาสตร์ที่จะพยายามเร่งโอนย้ายผู้ใช้บริการที่ยังใช้ SIM 3G ให้เป็นลูกค้า 4G ให้มากที่สุด ดังจะได้กล่าวถึงในหัวข้อสุดท้าย อีกประการหนึ่งก็คือการกำหนดโปรโมชั่นทางการตลาดสำหรับจัดแพ็กเกจราคาค่าบริการ ในเมืองไทยเพิ่งมีการทดลองตลาดโดยผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ทั้ง 3 รายนำเสนอแพ็กเกจการใช้งานแบบ Non-FUP (Non- Fair Usage Policy) มาใช้งานตั้งแต่ช่วงปลายปี พ.ศ. 2558 ที่ผ่านมา ซึ่งผู้เขียนก็จะขออธิบายความสัมพันธ์ของการผสานแนวคิดทั้งทางด้านเทคนิคและการตลาดเข้าด้วยกันอีกครั้งหนึ่ง ในที่นี้ขอให้ศึกษาผลกระทบจากการแย่งชิงตลาดการสนทนาเสียงของแอพพลิเคชั่น OTT ทั้งหลายที่มีต่อผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ตามประเทศต่างๆ ในทวีปยุโรปดังแสดงในรูปที่ 4 จะเห็นได้ว่ารายได้จากการให้บริการสนทนาเสียงลดลงจนเหลือเพียงเกือบครึ่งหนึ่งจากการบันทึกตั้งต้นภายในเวลาเพียง 5 ปี ตารางในภาพแสดงแนวตั้งเป็นค่ากลาง (Normalization) โดยแทนค่าเริ่มต้นว่า 100 เนื่องจากไม่ต้องการแสดงให้เห็นถึงรายได้ที่แท้จริงของผู้ให้บริการแต่ละราย การลดลงของรายได้ในการให้บริการสนทนาทางเสียงเกิดขึ้นอย่างรุนแรงนับตั้งแต่ปี พ.ศ. 2553 (ค.ศ. 2010) อันเป็นปีที่โทรศัพท์เคลื่อนที่สมาร์ทโฟนที่ใช้ระบบปฏิบัติการ Android มีปริมาณในตลาดผู้บริโภคมากขึ้น จนสามารถสร้างการแข่งขันกับ iPhone ของค่าย Apple เชื่อได้ว่าหากนำข้อมูลรายได้ของผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ในภูมิภาคอื่นๆ มาวิเคราะห์ในลักษณะเช่นนี้ก็จะได้ผลลัพธ์ที่ไม่แตกต่างกันกับในทวีปยุโรป ประเด็นสำคัญที่ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ให้ความสำคัญก็คือสัดส่วนรายได้จากการให้บริการสนทนาทางเสียงยังคงมีมากกว่ารายได้ที่มาจากการขายแพ็กเกจการรับส่งข้อมูล หากรายได้จากการสนทนาเสียงลดลงอย่างรวดเร็ว แต่ตนไม่สามารถเพิ่มรายได้จากการสื่อสารข้อมูล ในขณะที่ฐานผู้ใช้บริการยังมีเท่าเดิม เท่ากับเป็นความเสี่ยงทางธุรกิจที่เกิดจากการที่รายได้สุทธิลดลง แต่ต้นทุนในการดูแลผู้ใช้บริการอันประกอบด้วยการขยายเครือข่ายเพื่อให้รองรับการสื่อสารที่ต้องการอัตราเร็วรวมสูงขึ้น ต้นทุนการทำการตลาดเพื่อรักษาฐานลูกค้าพร้อมๆ กับแย่งชิงลูกค้าจากผู้ให้บริการเครือข่ายรายอื่นๆ ยังมีค่าคงเดิมหรืออาจจะต้องลงทุนมากขึ้น เท่ากับเป็นการทำธุรกิจที่ล้มเหลว ในขณะที่บรรดาผู้ให้บริการแอพพลิเคชั่น OTT มีแต่ผลตอบแทนที่เป็นบวก ทั้งในเรื่องของการสร้างความภักดี (Loyalty) ของผู้ใช้บริการแอพพลิเคชั่นที่มีต่อตน อันนำไปสู่การสร้างรายได้ต่อยอดจากการขายโฆษณา ซึ่งปัจจุบันคือเม็ดเงินจำนวนมหาศาลที่ขับเคลื่อนธุรกิจดิจิทัล

VoLTE และการช่วยปรับสถานการณ์การแข่งขันทางธุรกิจ

ก่อนที่จะกล่าวถึงแนวคิดทางยุทธศาสตร์ธุรกิจเบื้องลึกสำหรับการยกระดับเครือข่ายให้สามารถแข่งขันกับผู้ให้บริการ OTT ผู้เขียนขอกล่าวถึงการเปลี่ยนแปลงทางเทคนิคสำหรับเครือข่ายโทรศัพท์เคลื่อนที่ LTE รูปที่ 5 เป็นการพัฒนาเครือข่ายโทรศัพท์เคลื่อนที่ LTE ให้รองรับเทคโนโลยี VoLTE โดยมีการเพิ่มอุปกรณ์หลักคือ PCRF (Policy and Charging Rule Function) โดยเชื่อมต่อกับอุปกรณ์ชุมสายของเครือข่าย LTE ซึ่งก็คือ PGW โดยอุปกรณ์ PCRF จะมีการเชื่อมต่อตรงไปยังกลุ่มอุปกรณ์เครือข่ายอีกชุดหนึ่งที่เป็นไปตามมาตรฐาน IMS (IP Multimedia Subsystem) ซึ่งเป็นมาตรฐานบริหารจัดการรูปแบบการสื่อสารชนิดต่างๆ ไม่ว่าจะเป็นการสื่อสารทางเสียง การสื่อสารวิดีโอ หรืออื่นๆ โดยจะสั่งการให้ชุมสายโทรศัพท์ทั้งบนเครือข่าย 3G และ 4G จัดสรรทรัพยากรเพื่อรองรับการสื่อสารแต่ละประเภทของผู้ใช้บริการแต่ละรายอย่างเหมาะสม ซึ่งหมายถึงประหยัดทรัพยากรเครือข่ายที่สุด เช่น บีบอัดข้อมูลให้ใช้ Bit Rate ต่ำที่สุด แต่ยังคงรักษาคุณภาพของการสื่อสารตามที่ผู้ใช้บริการต้องการ



รูปที่ 4 การลดลงของรายได้ในการให้บริการสนทนาทางเสียงของผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ในยุโรป



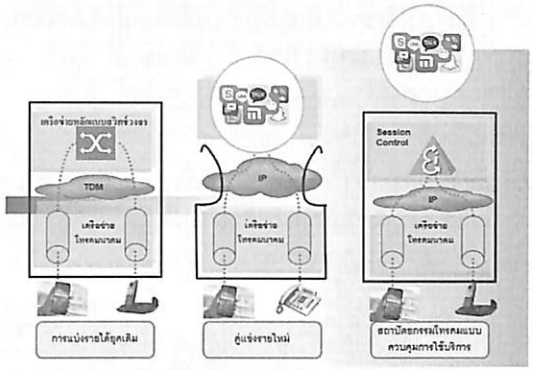
รูปที่ 5 การพัฒนาเครือข่าย 4 LTE ให้รองรับการเชื่อมต่อวงจรสนทนาโดยใช้เทคโนโลยี VoLTE

ในเครือข่าย LTE ที่ได้รับการเพิ่มขีดความสามารถ VoLTE ก็จะได้รับการติดตั้งอุปกรณ์ OCS (Online Charging Server) เพื่อทำหน้าที่ในการบันทึก ตรวจสอบความเป็นไป จนถึงการสิ้นสุดการสนทนาทางเสียง โดยที่ส่วนประกอบอื่นๆ ของเครือข่ายโทรศัพท์เคลื่อนที่ 4G LTE ก็ยังคงเป็นไปตามเดิม การปรับเพิ่มอุปกรณ์ภายในเครือข่ายก็เป็นไปเพียงเท่านี้ สิ่งที่ผู้อ่านพึงทราบคือรายละเอียดของกลุ่มอุปกรณ์เครือข่าย IMS

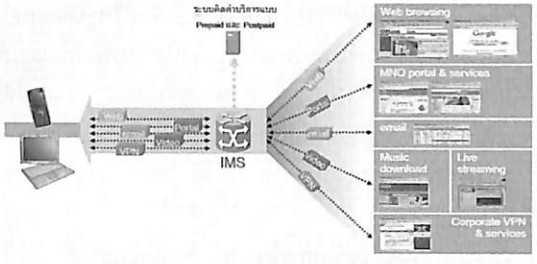
เทคโนโลยี IMS พัฒนาขึ้นอย่างต่อเนื่องตามวิวัฒนาการของเครือข่ายสื่อสารโทรคมนาคม ยิ่งเครือข่ายมีการประยุกต์ใช้โครงข่าย IP หรือมีแนวทางในการให้บริการ Convergence ไม่ว่าจะเป็นการหลอมรวมอย่างง่ายระหว่างเทคโนโลยีสื่อสารไร้สายด้วยกัน เช่น 2G/3G/4G กับ Wi-Fi หรือการหลอมรวมทางสถาปัตยกรรมที่ซับซ้อนมากเท่าใด ความสำคัญของ IMS ในฐานะของการเป็นสมองควบคุมและบริหารจัดการการให้บริการแบบมัลติมีเดียที่หลากหลายและซับซ้อนก็จะทวีมากยิ่งขึ้น แต่อย่างไรก็ตามปัจจัยผลักดันประการสำคัญกลับอยู่ที่ยุทธศาสตร์ในการแข่งขันระหว่างผู้ให้บริการโทรคมนาคมท้องถิ่น เช่น ผู้ให้บริการในประเทศไทยกับผู้ประกอบการระดับโลก (Global Player) ซึ่งยิ่งเครือข่ายโทรคมนาคมมีการหลอมรวมกับโครงข่าย IP มากเท่าใด ก็จะยิ่งทำให้ผู้ใช้บริการเครือข่ายโทรศัพท์เคลื่อนที่หรือเครือข่ายโทรคมนาคมท้องถิ่นต่างมองฐานะของเครือข่ายโทรคมนาคมท้องถิ่นเป็นเพียง "ท่อรับส่งข้อมูล" (Information Pipe) เพื่อเชื่อมต่อผ่านโครงข่าย IP ออกไปยังเซิร์ฟเวอร์หรือแหล่งให้บริการของผู้ประกอบการแบบ OTT มากขึ้นเท่านั้น ยิ่งเครือข่ายโทรคมนาคมของผู้ให้บริการท้องถิ่นมีระดับของการ Convergence มากขึ้นเท่าไร หมายถึงมีการให้บริการผ่านทางเครือข่ายเข้าถึงหลายชนิด เช่น 3G/4G, ADSL/FTTH, WiFi ฯลฯ ฐานลูกค้าของผู้ให้บริการ (Customer Segment) รายดังกล่าวก็ยิ่งเปิดกว้าง อาจเป็นการเพิ่มโอกาสให้ผู้ให้บริการ OTT เข้ามาตัดส่วนแบ่งของห่วงโซ่คุณค่าทางธุรกิจ (Business Value Chain) ได้มากยิ่งขึ้น

แนวทางในการรับมือกับภัยคุกคามดังกล่าวจึงอยู่ที่การเพิ่มขีดความสามารถให้กับเครือข่ายโทรคมนาคมของผู้ประกอบการท้องถิ่นให้สามารถตรวจวิเคราะห์การขอใช้บริการของผู้ใช้บริการ รวมถึงความสามารถในการกำหนดมาตรการควบคุมและบริหารจัดการ เช่น อาจจะยอมให้ผู้ใช้งานใช้บริการ VoIP จากผู้ให้บริการระดับโลกรายใดรายหนึ่งได้ แต่ผู้ใช้บริการจะต้องจ่ายค่าธรรมเนียมพิเศษเพิ่มให้บริษัทผู้ให้บริการโทรคมนาคมท้องถิ่นที่ตนจดทะเบียนใช้งานอยู่ หรืออาจไม่ยอมให้ใช้งานเลย ขึ้นกับกลยุทธ์และนโยบายในการให้บริการเป็นสำคัญ รูปที่ 6 แสดงให้เห็นถึงความสำคัญของการเพิ่มขีดความสามารถในการควบคุมการใช้บริการให้กับเครือข่ายในทางเทคนิคจะเรียกว่า Session Control ซึ่งถือเป็นบทบาทสำคัญของเทคโนโลยี IMS

รูปที่ 7 อธิบายบทบาทหน้าที่ของเครือข่าย IMS โดยพื้นฐานแล้วเทคโนโลยี IMS จะสามารถแยกแยะประเภทของข้อมูลที่มีการรับส่งระหว่างผู้ใช้บริการ ไม่ว่าจะใช้งานผ่านเครือข่ายเข้าถึงแบบใดก็ตาม กับเครือข่ายภายนอก หรือแม้กระทั่งกับเครื่องคอมพิวเตอร์เซิร์ฟเวอร์



รูปที่ 6 แนวคิดของการสร้างเทคโนโลยี Session Control เพื่อสร้างการแข่งขันกับผู้ให้บริการแบบ OTT



รูปที่ 7 ภาพรวมอธิบายการทำงานและจำแนกข้อมูลของเทคโนโลยี IMS

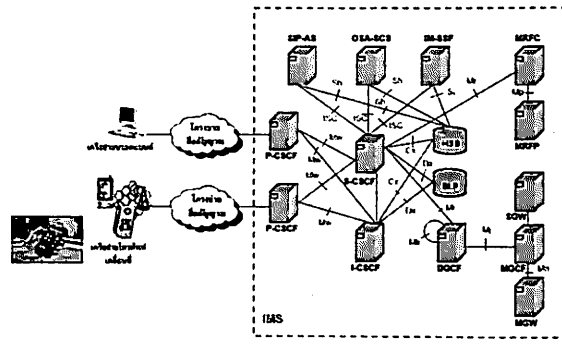
ที่ให้บริการต่างๆ ภายในเครือข่ายของผู้ให้บริการเอง โดยสามารถทราบถึงแอดเดรสต้นทางและปลายทาง ประเภทของบริการ เส้นทางในการรับส่ง ฯลฯ ซึ่งข้อมูลเหล่านี้จะถูกนำมาใช้พิจารณาประกอบกับเงื่อนไขในการให้บริการซึ่งได้รับการกำหนดขึ้นมาโดยผู้ให้บริการเครือข่าย ทั้งนี้ IMS จะมีการเชื่อมต่อกับอุปกรณ์ต่างๆ ในเครือข่ายหลัก รวมถึงอุปกรณ์บริหารจัดการผู้ใช้บริการโทรศัพท์เติมเงิน ซึ่งส่วนใหญ่ใช้เทคโนโลยี Intelligent Network (IN) และระบบบริหารจัดการผู้ใช้บริการแบบชำระค่าบริการรายเดือนเพื่อรับประกันว่าผู้ให้บริการสามารถจัดเก็บค่าบริการได้ถูกต้องถึงแม้ว่าจะมีกลยุทธ์และเงื่อนไขในการให้บริการที่ซับซ้อนเพียงใดก็ตาม

การพัฒนาเทคโนโลยี IMS ขึ้นมามีจุดมุ่งหมายสำคัญเพื่อสนับสนุนการให้บริการมัลติมีเดียสำหรับผู้ให้บริการเครือข่ายโทรคมนาคม แม้จะเริ่มต้นจากการให้ความสนใจกิจการโทรศัพท์เคลื่อนที่ โดยเฉพาะอย่างยิ่งกับมาตรฐานโทรศัพท์เคลื่อนที่ 3G เป็นอันดับแรก แต่ IMS ก็มีบทบาทสำคัญในการสนับสนุนกิจการสื่อสารสำหรับผู้ให้บริการเครือข่ายบรอดแบนด์ รวมไปถึงผู้ประกอบการแบบ Convergence โครงสร้างสถาปัตยกรรมของ IMS รองรับขีดความสามารถในการให้บริการด้านโทรคมนาคมต่อไปนี้

1. **รองรับการเชื่อมต่อเพื่อสื่อสารข้อมูลมัลติมีเดียเต็มรูปแบบ** โดยผ่านโครงข่ายแบบ IP หรือการสื่อสารแบบแพ็กเก็ตสวิตช์
2. **ผู้ให้บริการเครือข่ายสามารถกำหนดเงื่อนไขสำหรับการให้บริการแต่ละประเภทได้** เช่น อนุญาตหรือไม่อนุญาตให้ผู้ใช้บริการดาวน์โหลดข้อมูล หรือใช้บริการจากผู้ประกอบการ

รายอื่นๆ ดังได้กล่าวถึงในตอนต้น ทั้งนี้เทคโนโลยี IMS สามารถรองรับการกำหนดเงื่อนไขได้ทั้งแบบเงื่อนไขรวม (Group Policy) ที่ให้ผลกับผู้ใช้ทั้งเครือข่าย หรือแบบเป็นรายย่อย (Individual Policy) สำหรับผู้ใช้งานเป็นรายๆ ไป

3. **สนับสนุนการเข้าถึงเพื่อใช้บริการจากหลายๆ เครือข่ายเข้าถึง** นอกเหนือจากการสื่อสารผ่านเครือข่ายโทรศัพท์เคลื่อนที่ไม่ว่าจะเป็น 2G, 3G หรือ 4G โดยการวางข้อกำหนดให้มาตรฐานเทคโนโลยี IMS อยู่ในระดับชั้นล่างๆ ตามข้อกำหนดแบบจำลอง OSI ทำให้การรองรับบริการต่างๆ ไม่ขึ้นกับเทคโนโลยีการเข้าถึง เปิดโอกาสให้ผู้ใช้บริการที่ติดต่อเข้ามาทางเครือข่ายอื่นๆ เข้าถึง เช่น Wi-Fi หรือแม้แต่เครือข่ายบรอดแบนด์ อย่าง ADSL, FTTH หรือกล่าวอีกนัยหนึ่งก็คือการสนับสนุนผู้ให้บริการแบบ Convergence
4. **รองรับคุณภาพในการให้บริการ (QoS หรือ Quality of Service)** ที่แตกต่างกันไปของบริการแต่ละประเภท โดยเปิดโอกาสให้ผู้ให้บริการเครือข่ายสามารถควบคุม QoS ที่จะให้แก่ผู้ใช้บริการแต่ละรายได้ผ่านทางการกำหนดแบนด์วิดธ์สูงสุดของเครือข่ายที่จะยินยอมให้กับผู้ใช้บริการตามประเภทของบริการ
5. **รองรับการใช้งานข้ามเครือข่าย (Roaming)** ซึ่งเป็นสิ่งที่พัฒนาต่อยอดจากการให้บริการโทรศัพท์เคลื่อนที่ในตระกูล 2G/3G/4G ที่เปิดโอกาสให้ผู้ใช้บริการสามารถนำเครื่องลูกข่ายไปใช้กับเครือข่ายผู้ให้บริการรายอื่นๆ ได้ ทั้งนี้ขีดความสามารถและข้อกำจัดที่ผู้ใช้บริการ IMS จะสามารถใช้บริการต่างๆ ได้ในขณะที่ใช้งานอยู่ในเครือข่าย Roaming นั้นจะขึ้นอยู่กับเงื่อนไขและข้อตกลงในการให้บริการร่วมกันระหว่างผู้ให้บริการเครือข่ายต้นทางกับผู้ให้บริการเครือข่าย Roaming แต่ละรายเป็นสำคัญ
6. **การเชื่อมต่อเพื่อแลกเปลี่ยนข้อมูลกับเครือข่ายชนิดอื่น (Interworking)** อันดับแรกคือการแลกเปลี่ยนข้อมูลกับเครือข่ายอินเทอร์เน็ต ซึ่งถือเป็นความสำคัญอันดับแรกที่ IMS ให้การรองรับ รองลงไปคือการเชื่อมต่อกับเครือข่ายโทรคมนาคมแบบสวิตช์วงจร เช่น การเชื่อมต่อเพื่อการสื่อสารวงจรเสียงกับเครือข่ายโทรศัพท์พื้นฐานหรือเครือข่ายโทรศัพท์เคลื่อนที่ดั้งเดิมที่ยังมิได้พัฒนาไปเป็นเครือข่ายแบบแพ็กเก็ตสวิตช์ หรือ IMS แม้กระทั่งการให้บริการโทรศัพท์แบบเห็นหน้า (Video Call) ในรุ่นแรกๆ เครื่องลูกข่ายก็ยังคงสนับสนุนการเชื่อมต่อแบบสวิตช์วงจรเพื่อให้สามารถรองรับการสื่อสารไปยังเครือข่ายโทรศัพท์พื้นฐาน (ซึ่งรวมถึงเครือข่าย ISDN)
7. **ช่วยให้พัฒนาบริการใหม่ๆ ได้เร็วขึ้น** ด้วยการตัดสินใจไม่กำหนดมาตรฐานใดๆ สำหรับการพัฒนาบริการ อันเป็นการเรียนรู้จากประสบการณ์ในการพัฒนาบริการต่างๆ ในยุคของเครือข่ายโทรศัพท์เคลื่อนที่ 2G ซึ่งทำให้ต้องเสียเวลาในการวางข้อกำหนดและทำการทดสอบ จนกลายเป็นข้อจำกัดในการสร้างบริการใหม่ๆ ขึ้นโดยปริยาย การไม่เน้นข้อกำหนดใดๆ เป็นพิเศษสำหรับการพัฒนาบริการ แต่เลือกใช้มาตรฐาน



รูปที่ 8 โครงสร้างทางสถาปัตยกรรมของเครือข่าย IMS

โปรโตคอลบนโลกอินเทอร์เน็ตซึ่งมีการใช้งานอย่างแพร่หลาย เป็นการสื่อสารภายในระบบเครือข่ายสถาปัตยกรรม IMS กลับกลายเป็นปัจจัยเสริมในการช่วยให้นักพัฒนาบริการและแอพพลิเคชั่นต่างๆ ซึ่งอาจจะหมายถึงบริษัทผู้ให้บริการโทรคมนาคมเอง หรืออาจเป็นบริษัทที่ทำหน้าที่เป็น Content Provider รวมถึงผู้ให้บริการอิสระบนโลกอินเทอร์เน็ต ซึ่งคาดว่าน่าจะส่งผลให้เกิดความหลากหลายของบริการ

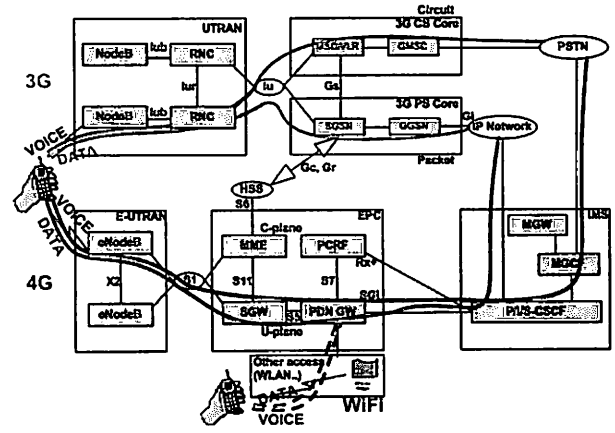
โครงสร้างของมาตรฐาน IMS ที่แสดงในรูปที่ 8 ถือว่าเป็นสถาปัตยกรรมกรอบมาตรฐานที่วาดขึ้นอย่างสมบูรณ์แบบ ประกอบด้วยส่วนของเครือข่ายเข้าถึง ซึ่งถูกมองแยกเป็นส่วนอิสระและไม่มีผลกระทบต่อโครงสร้างเครือข่าย IMS มีทั้งที่เป็นเครือข่ายเข้าถึงแบบมีสาย เช่น เครือข่ายโทรศัพท์พื้นฐาน (รวมถึง ISDN) เครือข่ายบรอดแบนด์ (เช่น ADSL, FTTH ฯลฯ) และเครือข่ายเข้าถึงแบบไร้สาย (เช่น โทรศัพท์เคลื่อนที่ 3G/4G รวมถึงเครือข่ายไร้สายอื่นๆ เช่น Wi-Fi) ในภาพรวมเครื่องลูกข่ายที่สามารถใช้กับมาตรฐาน IMS จึงมีความหลากหลายตั้งแต่โทรศัพท์พื้นฐาน โทรศัพท์เคลื่อนที่ อุปกรณ์ CPE (Customer Premise Equipment) เช่น Set Top Box หรือ ADSL Router คอมพิวเตอร์ สมาร์ทโฟน ฯลฯ ส่วนที่เหลือในรูปเป็นฟังก์ชั่นหลักๆ ที่ต้องมีตามข้อกำหนดมาตรฐาน IMS (3GPP TS 23.002) ประกอบด้วยฟังก์ชั่นสำคัญที่ทำหน้าที่ในการบริหารจัดการการให้บริการมัลติมีเดียต่างๆ ให้กับผู้ใช้บริการทั้งหมด รวมเรียกสถาปัตยกรรมในส่วนนี้ว่า IP Multimedia Core Network Subsystem อันมีรายละเอียดของฟังก์ชั่นที่สำคัญพอจะกล่าวถึงโดยสังเขปดังนี้

- **ฟังก์ชั่นฐานข้อมูลผู้ใช้บริการ (User Database)** ประกอบด้วยฟังก์ชั่น HSS (Home Subscriber Servers) และ SLF (Subscriber Location Function) ร่วมกันทำหน้าที่จัดเก็บรายละเอียดในการใช้งาน สถานภาพ และระบุตำแหน่งที่อยู่ภายในเครือข่ายของผู้ใช้บริการแต่ละราย
- **กลุ่มของ SIP Server** มีชื่อเรียกตามมาตรฐาน IMS ว่า CSCF (Call/Session Control Function) แยกย่อยออกตามหน้าที่ได้เป็น P-CSCF (Proxy CSCF) I-CSCF (Interrogating CSCF) และ S-CSCF (Serving CSCF) ทำหน้าที่เสมือนอุปกรณ์ชุมสายบริหารจัดการการสื่อสารมัลติมีเดียที่เกิดขึ้นผ่านเครือข่าย IMS

- **กลุ่มของฟังก์ชั่น MRF (Media Resource Function)** ซึ่งแยกย่อยออกไป ประกอบด้วยฟังก์ชั่น MRFC (Media Resource Function Controller) และ MRFP (Media Resource Function Processor) ทำหน้าที่ในการบริหารจัดการสื่อ (Media) ให้การสนับสนุนต่างๆ กับผู้ใช้บริการ IMS ในเครือข่ายต้นทาง (ซึ่งหมายถึงเครือข่ายที่ผู้ใช้บริการลงทะเบียนใช้งาน) ไม่ว่าจะเป็นการเก็บเสียงประกาศ (Announcement) รวมสัญญาณเสียงและการแปลงรูปแบบสัญญาณเสียงไปเป็นมาตรฐานต่างๆ
- **กลุ่มของฟังก์ชั่น BGCF (Breakout Gateway Control Function)** เป็น SIP Server อีกประเภทหนึ่งที่ทำหน้าที่วิเคราะห์ บริหารจัดการกำหนดเส้นทางเชื่อมต่อ (ผ่านโครงข่าย IP) สำหรับรองรับในกรณีของการสื่อสารแบบสนทนาผ่านไปยังเครือข่ายโทรศัพท์พื้นฐานหรือโทรศัพท์เคลื่อนที่ที่ยังคงเป็นการเชื่อมต่อแบบสวิตช์วงจร
- **กลุ่มของอุปกรณ์เชื่อมต่อเครือข่ายแบบสวิตช์วงจร** ประกอบด้วยฟังก์ชั่น SGW (Signaling Gateway) MGCF (Media Gateway Control Function) และ MGW (Media Gateway) ทำหน้าที่รับและแปลงสัญญาณเสียงหรือสัญญาณภาพที่มีการรับส่งจากเครือข่าย IMS ไปยังเครือข่ายอื่นๆ ที่มีรูปแบบการสื่อสารแบบสวิตช์วงจร ไม่ว่าจะเป็นเครือข่ายโทรศัพท์เคลื่อนที่ โทรศัพท์พื้นฐาน หรือเครือข่าย ISDN
- **กลุ่มของฟังก์ชั่นบริการต่าง ๆ (Application Server)** จัดเป็นฟังก์ชั่นแบบ SIP อีกกลุ่มหนึ่งที่ทำหน้าที่จัดเก็บและให้บริการแอพพลิเคชั่นต่างๆ ให้กับผู้ใช้บริการ สามารถแยกย่อยออกเป็น 3 กลุ่มคือ SIP AS (SIP Application Server) OSA-SCS (Open Service Access – Service Capability Server) และ IM-SSF (IP Multimedia Service Switching Function) ซึ่งต่างมีหน้าที่การทำงานที่แตกต่างกัน

เมื่อพัฒนาขีดความสามารถของเครือข่าย 4G LTE ให้รองรับการสื่อสารแบบ VoLTE แล้ว สิ่งที่เกิดขึ้นกับเครือข่ายก็คือความสามารถในการรองรับ Bearer Service ซึ่งก็คือการจัดเตรียมทรัพยากรของเครือข่ายโทรศัพท์เคลื่อนที่ LTE ทั้งในส่วนการเข้ารหัสข้อมูลทางคลื่นวิทยุ การจัดโปรโตคอลทั้งในส่วนการสื่อสารผ่านคลื่นวิทยุจนถึงการสื่อสารภายในเครือข่ายเพื่อให้รองรับรูปแบบการสื่อสารทางเสียง อันที่จริงแล้วการเพิ่มอุปกรณ์ทั้งในส่วนของ PCRF, OCS และอุปกรณ์เครือข่าย IMS นั้นยังเป็นการเพิ่มขยายขีดความสามารถในการสื่อสารทางเสียงให้กับเครือข่ายโทรศัพท์เคลื่อนที่ 4G ทั้งที่เป็นการสื่อสารจากสถานีฐาน 4G หรือ eNode B และสื่อสารผ่านทางอื่นๆ เช่น การสื่อสารโดยโทรศัพท์เคลื่อนที่สมาร์ทโฟนผ่านเครือข่าย Wi-Fi

รูปที่ 9 แสดงให้เห็นเครือข่ายโทรศัพท์เคลื่อนที่ 4G ที่มีการเชื่อมต่อเครือข่าย 3G และเครือข่าย Wi-Fi โดยอุปกรณ์ PCRF จะทำงานร่วมกับอุปกรณ์ MME, SGW และ PGW ในการบริหารจัดการให้เกิดการสร้าง Bearer Service สำหรับรองรับการสื่อสารทางเสียงผ่านการเชื่อมต่อแบบแพ็กเก็ตสวิตช์ผ่านเครือข่ายสถานีฐาน 4G ในทางเทคนิคอาจเรียกรวมการทำงานของอุปกรณ์ PCRF, MME, SGW และ PGW ว่า EPC หรือ Evolved Packet Control ทั้งนี้เบื้องหลังของ



รูปที่ 9 โครงสร้างทางสถาปัตยกรรมของเครือข่าย IMS

การบริหารจัดการและคัดเลือก Bearer Service ที่เหมาะสมกับการสื่อสารทั้งที่เป็นเสียงสนทนาและข้อมูลแบบอื่นๆ เช่น การรับชมภาพยนตร์ การเล่นเกม การให้บริการแบบ Steaming ในรูปแบบอื่นๆ จะเป็นหน้าที่ของกลุ่มอุปกรณ์ IMS ซึ่งเมื่อเป็นเช่นนี้ก็เท่ากับว่าผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ 4G ก็จะสามารถทำการออกแบบแอพพลิเคชั่นของตนเอง เปิดโอกาสให้ผู้ใช้บริการสามารถเข้าถึงบริการได้ทั้งโดยผ่านทางเครือข่าย 4G และผ่านเครือข่าย Wi-Fi ที่ตนเองลงทุน หรือได้ให้บริการร่วมกับพันธมิตรธุรกิจรายอื่นๆ ซึ่งก็เป็นฟังก์ชั่นการทำงานปกติเครือข่าย IMS ตามที่ได้กล่าวมาข้างต้น การลงทุนเพื่อให้บริการ VoLTE ของผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ 4G จึงมีคุณค่ามากกว่าเพียงการเพิ่ม Bearer Service เพื่อให้บริการรับส่งสัญญาณเสียงผ่านทางเครือข่าย 4G เพียงถ่ายเดียว ในแง่ของการสื่อสารทางเสียงจึงมีการเรียกบริการดังกล่าวว่า VoMBB (Voice over Mobile Broadband) เพราะผู้ให้บริการเครือข่ายสามารถเปิดโอกาสให้ผู้ใช้บริการพูดคุยสนทนาผ่านเครือข่ายสื่อสารต่างๆ ที่ตนมีได้ทั้งหมดตราบเท่าที่อุปกรณ์สมาร์ทโฟนของผู้ใช้บริการ 4G ของตนมีศักยภาพในการเชื่อมต่อกับเครือข่ายเหล่านั้น

รูปที่ 9 ยังแสดงให้เห็นว่าผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ 4G ซึ่งแทบทั้งหมดก็มีธุรกิจเครือข่ายโทรศัพท์เคลื่อนที่ 3G ของตนเอง สามารถแยกเส้นทางและอุปกรณ์เครือข่ายที่รองรับการเชื่อมต่อทั้งการสื่อสารสนทนาด้วยเสียงและการสื่อสารข้อมูลออกเป็น 2 เส้นทาง สำหรับสื่อสารโดยเครื่องลูกข่ายโทรศัพท์เคลื่อนที่ 3G หรือแม้จะเป็นการใช้สมาร์ทโฟนที่รองรับการสื่อสาร 4G แต่ผู้ใช้บริการยังใช้ซิมการ์ด (SIM Card) ที่รองรับถูกลงทะเบียนเฉพาะในเครือข่าย 3G ก็จะเชื่อมต่อผ่านสถาปัตยกรรมเครือข่าย 3G ขณะที่ลูกค้าผู้ใช้บริการซิมการ์ดที่ได้รับการลงทะเบียนในเครือข่าย 4G แล้ว และใช้เครื่องลูกข่ายที่รองรับการติดต่อกับเครือข่าย 4G ได้ก็จะมีเส้นทางสื่อสารผ่านเครือข่าย 4G ซึ่งเมื่อมีการลงทุนติดตั้งอุปกรณ์ที่สนับสนุนการสื่อสารด้วยเสียงผ่านเทคโนโลยี VoLTE แล้วก็เท่ากับเป็นการแยกเส้นทางสื่อสารทั้งเสียงพูดและการสื่อสารข้อมูลผ่านทางเครือข่าย4G เต็มรูปแบบ โดยไม่จำเป็นต้องพึ่งกระบวนการกระโดดข้ามกลับไปเครือข่าย 3G เพื่อดำเนินการกระบวนการ CS Fall Back อีกต่อไป

QCI	Bearer Type	Priority	Packet Delay	Packet Loss	Example
1	GBR	2	100 ms	10^{-2}	VoIP call
2		4	150 ms	10^{-3}	Video call
3		3	50 ms		Online Gaming (Real Time)
4		5	300 ms		Video streaming
5	Non GBR	1	100 ms	10^{-6}	IMS Signaling
6		6	300 ms		Video, TCP based services e.g. email, chat, ftp etc
7		7	100 ms	10^{-3}	Voice, Video, Interactive gaming
8		8	300 ms	10^{-6}	Video, TCP based services e.g. email, chat, ftp etc
9		9			

รูปที่ 10 กลุ่ม Bearer Service ที่ได้รับการกำหนดขึ้นหลังจากมีการพัฒนาเครือข่าย 4G LTE ไปสู่มาตรฐาน VoLTE

เมื่อกล่าวถึง Bearer Service แล้วผู้เขียนก็ขอนำเสนอถึงมาตรฐาน Bearer Service ที่มีให้ใช้งานบนเครือข่ายโทรศัพท์เคลื่อนที่ 4G ซึ่งเมื่อกล่าวรวมไปจนถึงยุคที่ผู้ให้บริการเครือข่ายได้เพิ่มขีดความสามารถด้าน VoLTE ลงไปในเครือข่ายแล้วก็จะเท่ากับว่าเครือข่ายโทรศัพท์เคลื่อนที่ 4G ในปัจจุบันรองรับรูปแบบ Bearer Service อยู่ 2 กลุ่ม ดังแสดงในรูปที่ 10 ประกอบด้วยกลุ่ม Guaranteed Bit Rate หรือ GBR ซึ่งมีการแบ่งระดับความสำคัญ (Priority) ของการเชื่อมต่อออกเป็น 4 ประเภทย่อย และกลุ่ม Non Guarantee Bit Rate หรือ Non-GBR แบ่งเป็น 5 กลุ่มความสำคัญของการเชื่อมต่อย่อย หากย้อนกลับไปพิจารณาถึงสถาปัตยกรรมของเครือข่ายโทรศัพท์เคลื่อนที่ 4G LTE มาตรฐานก่อนที่จะมีการติดตั้งฟังก์ชั่นการทำงาน VoLTE เครือข่ายในยุคแรกนั้นจะรองรับเฉพาะการเชื่อมต่อแบบ Non-GBR รองรับการสื่อสารที่เป็นการรับส่งข้อมูลพื้นฐาน อย่างเช่น การรับส่งสัญญาณวิดีโอการรับส่งอีเมล การ Chat และการสื่อสารอื่นใดที่มีมาตรฐานการสื่อสารแบบ TCP (Transmission Control Protocol) รองรับ ในความหมายของผู้บริโภคก็คือการสื่อสารข้อมูลในทุกรูปแบบยกเว้นการสื่อสารสนทนาด้วยเสียงและการสนทนาแบบ Video Call

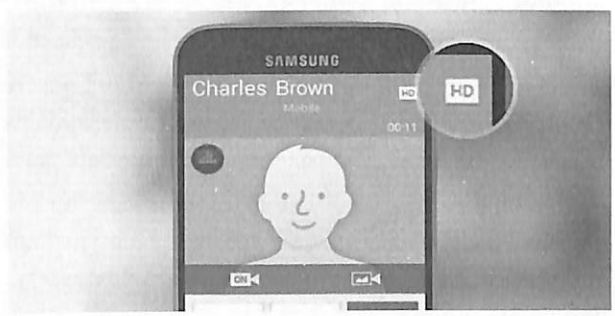
ต่อเมื่อมีการติดตั้งอุปกรณ์ PCRF, OCS และอุปกรณ์เครือข่าย IMS ลงไปในเครือข่าย LTE แล้ว สิ่งที่เกิดขึ้นก็คือการจัดให้มี Bearer Service ในกลุ่ม GBR ที่สามารถรับประกันคุณภาพของการสื่อสารแบบเรียลไทม (Real Time) โดยเฉพาะการพูดคุยสนทนาและการสื่อสารแบบ Video Stream จนถึงการเพิ่มคุณภาพการรับชมภาพยนตร์แบบ Video Streaming เมื่อพิจารณารายละเอียดของตัวแปรด้านคุณภาพการสื่อสารในรูปที่ 10 จะเห็นว่าเมื่อมีการรองรับการสื่อสารสนทนาทางเสียงโดยใช้เทคโนโลยี VoIP (Voice over IP) ซึ่งก็เป็นมาตรฐานเดียวกันกับที่บรรดาผู้ให้บริการแอพพลิเคชั่น OTT ทั้งหลายใช้งาน รวมถึงการสื่อสารสนทนาแบบเห็นหน้ากัน โดยเป็นการสื่อสารด้วยฟังก์ชั่นโทรศัพท์ของโทรศัพท์เคลื่อนที่สมาร์ทโฟน ไม่ใช่การสื่อสารจากแอพพลิเคชั่นอย่าง Facetime, LINE Call ฯลฯ เครือข่ายโทรศัพท์เคลื่อนที่ 4G LTE จะมีการผ่อนปรนระดับของการรักษาความผิดพลาดของข้อมูลลงเมื่อเทียบกับระดับเดิมที่ได้รับการกำหนดเอาไว้ในมาตรฐานเครือข่าย LTE ก่อนที่จะมีการเพิ่มเติมขีดความสามารถของ VoLTE จะเห็นได้ว่าในการสื่อสารด้วยเสียงนั้นเครือข่ายจะยินยอมให้มีอัตราการผิดพลาดของบิตข้อมูลมากถึง 10-2 หรือ 1 บิตใน 100 บิตที่มีการรับส่ง เพราะการผิดพลาดของบิตข้อมูลแม้จะมากขนาดนั้นก็ไม่ได้ทำให้การรับฟังสัญญาณเสียงเกิดความเสียหายจนเข้าใจผิด ต่างกับการรับส่งข้อมูลอื่นๆ ที่ต้องรักษาระดับความผิดพลาดไว้ที่ 10-5 หรือ 1 บิตใน 10,000 บิต ซึ่งหมายความว่าเมื่อมีการติดตั้งอุปกรณ์ PCRF, OCS และ IMS แล้วจะมีผลทำให้การเพิ่มปริมาณสื่อสารของการสนทนาด้วยเสียงโดยเครื่องลูกข่ายโทรศัพท์เคลื่อนที่ 4G ไม่สร้างปัญหาให้เครือข่าย 4G เกิดปัญหาข้อมูลหนาแน่นจนก็ให้เกิดปัญหาเรื่องการรักษาระดับคุณภาพของสัญญาณ (Quality of Service) โดยรวม

ยุทธศาสตร์ทางธุรกิจของผู้ให้บริการ VoLTE

ทั้งหมดที่กล่าวมาถึงเป็นยุทธศาสตร์สำคัญสำหรับผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ทั่วโลกในการที่จะเร่งยกระดับเครือข่ายโทรศัพท์เคลื่อนที่ 4G LTE ของตนให้เป็นมีรูปแบบการทำงาน VoLTE เพื่อสร้างช่องทางในการสื่อสารทางเสียงด้วยเทคโนโลยี VoLTE ผ่านเครือข่าย 4G ของตน เหตุที่ต้องเร่งดำเนินการดังกล่าวก็เพราะบรรดาผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่เข้าใจดีถึงภัยคุกคามที่บรรดาผู้ให้บริการแอพพลิเคชั่น OTT ทั้งหลายที่ได้กล่าวถึงในตอนแรกของบทความเรื่องนี้จะรุกเข้ามาทำให้รายได้จากการขายบริการสนทนาด้วยเสียงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ลดลง การที่เทคโนโลยี VoLTE ซึ่งเกิดจากการทำงานของ PCRF และ IMS ทำให้สามารถลดแบนด์วิดธ์ของการสื่อสารด้วยเสียงผ่านเครือข่าย 4G LTE ลงได้ก็หมายความเครือข่ายจะยิ่งมีทรัพยากรเหลือมากขึ้นเพื่อรองรับการทางเสียง และด้วยการที่มีข้อกำหนด GBR ที่ยอมผ่อนปรนอัตราความผิดพลาดของข้อมูลสัญญาณเสียงและสัญญาณภาพก็เท่ากับว่าการเพิ่มปริมาณการสนทนาทางเสียงจะมีสร้างปัญหาเบียดบังแบนด์วิดธ์ของการสื่อสารข้อมูลชนิดอื่นๆ ที่ต้องให้ความสำคัญกับการรักษาความถูกต้องของข้อมูลมากกว่า การชูจุดขายของบรรดาผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ว่าคุณภาพในการพูดคุยผ่านเทคโนโลยี VoLTE ชัดเจนระดับ HD นั้นก็เป็นเพียงกลยุทธ์ทางการตลาด ซึ่งเป็นผลพลอยได้จากความก้าวหน้าของเทคโนโลยีบีบอัดและเข้ารหัสข้อมูลเสียง (Voice CODEC) ที่ดีขึ้นเรื่อยๆ และความหมายซ่อนเร้นที่บรรดาผู้ให้บริการเครือข่ายได้กล่าวนั้นก็เป็นความพยายามจะบอกว่าอย่าไปใช้แอพพลิเคชั่นประเภท Social Network ในการคุยกันเลย เพราะระบบเซิร์ฟเวอร์ของผู้ให้บริการเหล่านั้นไม่ได้รับประกันคุณภาพและความชัดเจนของสัญญาณ สู้ใช้โทรศัพท์เคลื่อนที่ 4G โทรพูดคุยกันตรงๆ จะชัดยิ่งกว่า ซึ่งมิได้แปลว่าความชัดดังกล่าวจะมีมากกว่าการพูดคุยกันผ่านเครือข่าย 3G

สิ่งที่สามารถคาดเดาได้ถึงยุทธศาสตร์ขั้นถัดไปของบรรดาผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ก็คือความพยายามที่ผลักดันให้ผู้ใช้บริการเปลี่ยนไปใช้โทรศัพท์เคลื่อนที่ 4G ให้เร็วและมากที่สุด ยิ่งเป็นเครื่องลูกข่ายที่รองรับเทคโนโลยีการสื่อสารแบบ VoLTE ได้ก็ยิ่งทำให้ปริมาณการใช้งานทราฟฟิกบนเครือข่าย 3G เริ่มลดลง ดังที่ได้กล่าวแล้วว่าเครือข่ายโทรศัพท์เคลื่อนที่ 4G LTE ได้รับการออกแบบมาให้มีอุปกรณ์ภายในเครือข่ายน้อยประเภทที่สุดเพื่อให้การสื่อสารผ่านเครือข่ายเกิดขึ้นได้เร็วที่สุด มองในแง่ของการลงทุนขยายเครือข่ายและการบำรุงรักษาก็เท่ากับว่าต้นทุนของการให้บริการเครือข่าย 4G ต่ำกว่าเครือข่าย 3G มาก เพราะสถาปัตยกรรมเครือข่าย 3G นั้นได้รับการพัฒนามาจากเครือข่าย 2G อันทำให้มีความหลากหลายของอุปกรณ์อยู่มาก สิ่งที่เป็นจุดหมายปลายทางของผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ก็คือการทำให้มีผู้ใช้งานเหลือตกค้างภายในเครือข่าย 3G น้อยที่สุด จะได้ค่อยๆ โยกย้ายย่านความถี่ที่ให้บริการเครือข่าย 3G ไปใช้กับเครือข่าย 4G ซึ่งปัจจุบันเทคโนโลยี LTE สามารถรองรับการสื่อสารได้ในแทบทุกความถี่ที่มีการกำหนดให้ใช้งานในโลกโทรคมนาคม อาทิ 800/850, 900, 1800, 2100, 2500, 2600 เมกะเฮิรตซ์ หากผู้ให้บริการสามารถมุ่งโฟกัสการลงทุนมาที่เครือข่าย 4G ได้โดยจำกัดขนาดความจุของเครือข่าย 3G ไว้ให้รองรับเฉพาะลูกค้าส่วนน้อยที่อาจมีรายได้ไม่มาก ไม่พร้อมหรือไม่คิดที่จะซื้อเครื่องลูกข่ายที่รองรับมาตรฐาน 4G ทั้งหลายทั้งปวงที่กล่าวมานี้ก็จะเป็นการลดต้นทุนทั้งด้านเงินลงทุนขยายเครือข่าย (Capital Expense หรือ CAPEX) และเงินลงทุนซ่อมบำรุง (Operating Expense หรือ OPEX) ทำให้มีช่องว่างของผลกำไรมากขึ้นกว่าการที่ต้องแบกรับทั้งการบริหารจัดการเครือข่ายโทรศัพท์เคลื่อนที่ 3G และ 4G ในสัดส่วนหรือสเกล (Scale) ที่ใหญ่พอๆ กัน ผลกำไรที่มากขึ้นนี้จะได้ถูกใช้ไปในการทำการตลาดเพื่อให้ตนสามารถแข่งขันดึงลูกค้าผู้ใช้บริการให้เห็นดีเห็นชอบกับการโทรศัพท์สื่อสารเสียงผ่านทางเครือข่ายโทรศัพท์เคลื่อนที่ตรงๆ ซึ่งด้วยต้นทุนที่ประหยัดลงนี้ผู้ให้บริการเครือข่ายก็สามารถที่จะกำหนดสร้างแพ็กเกจราคาค่าโทรศัพท์ที่ลดค่าใช้จ่ายในการพูดคุยโทรศัพท์กันได้มากกว่าในปัจจุบัน ผลก็คือจะทำให้ผู้บริโภคชะลอที่จะหันไปมุ่งใช้งานแอพพลิเคชั่นแบบ OTT ในการโทรศัพท์นั่นเอง

ปัจจุบันการมุ่งไปสู่ความฝันของบรรดาผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ยังไม่สามารถเป็นไปได้รวดเร็ว สาเหตุก็เพราะความพร้อมของเครื่องลูกข่ายที่รองรับการสื่อสารแบบ VoLTE ยังมีไม่มากและที่มีให้ใช้งานก็ยังเป็นเครื่องที่มีราคาสูง กลไกทางด้านเศรษฐศาสตร์บอกว่าต้องใช้เวลาให้ VoLTE กลายเป็นมาตรฐานหลักของโทรศัพท์เคลื่อนที่ 4G ทั่วไป และยิ่งไปกว่านั้นก็ยังต้องรอให้ความสามารถนี้กระจายไปโทรศัพท์เคลื่อนที่ที่มีระดับราคาถูกเพื่อให้เกิด Scaling ของการชักชวนลูกค้าจำนวนมากให้เปลี่ยนมาใช้แพ็กเกจการโทรศัพท์แบบ 4G ซึ่งโดยเบื้องหลังก็คือการชักชวนให้มาใช้บริการ VoLTE นั่นเอง



สิ่งที่บรรดาผู้ให้บริการเครือข่ายโทรศัพท์สามารถทำได้ในเวลานี้จึงเป็นการออกแพ็กเกจการให้บริการโทรศัพท์แบบ Non-FUP หรือ Non-Fair Usage Policy ที่เปลี่ยนแปลงรูปแบบการให้บริการจากเดิมที่เป็นแบบ FUP ภายใต้เงื่อนไขที่ว่า

จ่าย xx บาทต่อเดือน = โทรได้ a นาที + เชื่อมต่ออินเทอร์เน็ตด้วยอัตราเร็วสูงสุดได้ถึง b GB + หลังจากนั้นอัตราเร็วในการสื่อสารจะลดลงเหลือ c Kbps

กลายไปเป็นแพ็กเกจแบบ Non-FUP ที่มีเงื่อนไขว่า

จ่าย yy บาทต่อเดือน = โทรได้ p นาที (ซึ่งส่วนใหญ่ p จะมีจำนวนนาทีต่ำกว่า a) + เชื่อมต่ออินเทอร์เน็ตด้วยอัตราเร็วสูงสุดได้ถึง q GB (ซึ่ง q จะมีค่าสูงกว่า b มากๆ) + หลังจากใช้งานเกินกว่า q จะเริ่มมีการคิดค่าเชื่อมต่ออินเทอร์เน็ตด้วยอัตรา r บาทต่อเมกะไบต์ ไม่มีการลดอัตราเร็วในการสื่อสาร

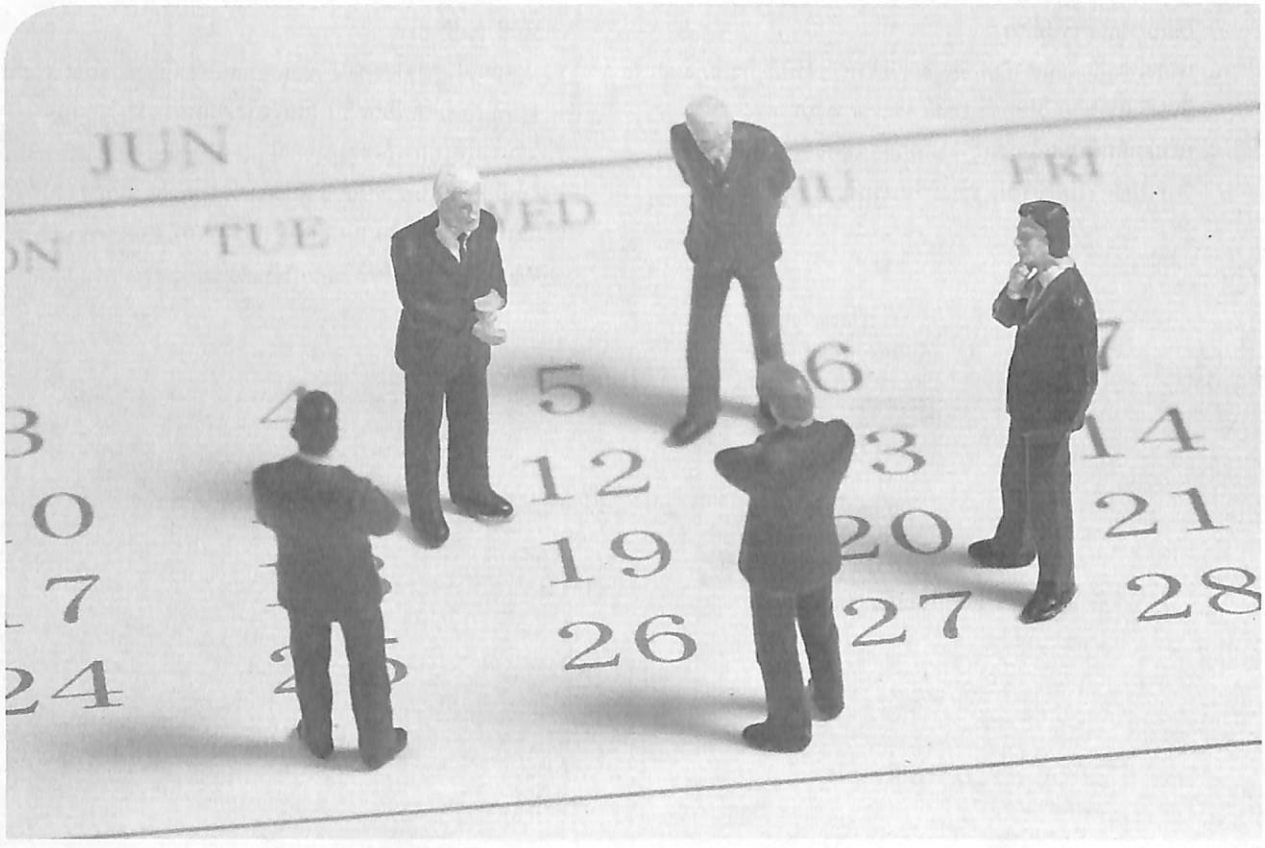
โดยการที่ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่จะแลกเปลี่ยนผลประโยชน์ในการมีโควต้าการรับส่งข้อมูลผ่านเครือข่ายโทรศัพท์เคลื่อนที่ให้กับผู้ใช้บริการมากขึ้นเมื่อเทียบกับแพ็กเกจแบบ FUP แต่หลังจากการใช้งานมากเกินค่า q แล้วผู้ใช้บริการก็ต้องยอมที่จะรับภาระค่าใช้งานที่ต้องจ่ายเพิ่มโดยไม่มีการลดอัตราเร็วในการสื่อสาร สิ่งที่สะท้อนให้เห็นถึงการตระหนักของผู้ให้บริการเครือข่ายว่าผู้บริโภคจำนวนมากเริ่มหนีไปใช้บริการพูดคุยผ่านทางแอพพลิเคชั่น OTT บนอุปกรณ์สมาร์ทโฟนมากขึ้นก็คือการตัดสินใจลดจำนวนนาทีที่แถมให้ในโปรโมชั่นลง เท่ากับว่าไหนๆ ผู้บริโภคก็มุ่งที่จะใช้งานแอพพลิเคชั่นพูดคุยกันมากกว่าการใช้ฟังก์ชั่นโทรศัพท์แล้วก็ให้โควต้าในการเข้าถึงข้อมูลมากขึ้นไปเลย แต่หากใช้งานจนเพลินผสมกับการเสพข้อมูลผ่านทางแอพพลิเคชั่นต่างๆ จนทำให้ปริมาณการรับส่งข้อมูลเกินโควต้าก็ต้องยอมจ่ายเงินเพิ่มให้กับผู้ให้บริการเครือข่าย ในขณะที่แพ็กเกจแบบ FUP แต่เดิมรายได้ที่ผู้ให้บริการจะได้เพิ่มนั้นมาจากการใช้งานโทรศัพท์ผ่านเครือข่ายจนเกินโควต้า ซึ่งปัจจุบันการใช้งานโทรศัพท์เกินโควต้านั้นเริ่มลดจำนวนลง จึงเป็นประโยชน์ต่อการทำธุรกิจมากกว่าในการที่จะหันมาคิดค่าบริการส่วนเกินจากการรับส่งข้อมูล ซึ่งการตอบรับของผู้บริโภคจะเป็นเช่นไรนั้นคงต้องให้เวลาอีกสักระยะหนึ่งจนกว่าจะเห็นปฏิกิริยาของผู้บริโภค อย่างไรก็ตามในปัจจุบันบรรดาผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยก็ยังคงมีแพ็กเกจการใช้งานแบบ FUP ให้ผู้บริโภคเลือกใช้งาน แต่ก็มีการเพิ่มลูกเล่นที่ดึงใจให้ผู้บริโภคสนใจเปลี่ยนไปใช้แพ็กเกจแบบ Non-FUP มากกว่า เช่น ค่าย AIS ซึ่งมีการให้บริการ Multi-SIM หรือการให้บริการซิมการ์ดหลายใบ แต่ใช้เลขหมายโทรศัพท์เดียวกันสำหรับให้ลูกค้านำไปใช้งานกับสมาร์ทโฟนหรือแท็บเล็ตพีซีหลายๆ เครื่องโดยใช้แพ็กเกจทางการตลาดเดียวกัน ในการซื้อแพ็กเกจแบบ Non-FUP นั้นผู้บริโภคสามารถขอซิมการ์ดสำหรับใช้บริการ Multi-SIM ได้มากที่สุดถึง 5 เครื่องโดยไม่ต้องเสียค่าบริการ Multi-SIM รายเดือน ในขณะที่การขอใช้บริการ Multi-SIM สำหรับแพ็กเกจแบบ FUP นั้นผู้ใช้บริการต้องรับภาระเสียค่าบริการ Multi-SIM รายเดือนอีกใบละ 20 บาทต่อเดือน

การพูดถึงเทคโนโลยี VoLTE ในบทความเรื่องนี้จึงมีมากกว่าการกล่าวถึงเฉพาะรายละเอียดทางเทคโนโลยี หากแต่สะท้อนถึงยุทธศาสตร์ของการให้บริการเครือข่ายโทรศัพท์เคลื่อนที่นับตั้งแต่นี้เป็นต้นไป การฉายภาพของการแข่งขันในสมรภูมิสื่อสารที่มิได้มีเพียงการแข่งขันระหว่างผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่เท่านั้น หากแต่ยังเป็นการแข่งขันกับบรรดาผู้ให้บริการแอพพลิเคชั่นแบบ OTT ซึ่งเป็นการแข่งขันระหว่างบรรดาผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ซึ่งถือเป็นผู้ประกอบการท้องถิ่นในระดับประเทศกับบรรดาผู้ให้บริการ OTT ที่เป็นผู้ให้บริการในระดับโลก

ศึกการแข่งขันครั้งนี้ยังต้องใช้เวลาอีกระยะหนึ่ง VoLTE เป็นเพียงหมัดแรกของการปรับเปลี่ยนสถาปัตยกรรมเครือข่ายโทรศัพท์เคลื่อนที่ ในไม่ช้าผู้ให้บริการเครือข่ายย่อมต้องเน้นการให้บริการเฉพาะเครือข่าย 4G เพื่อให้ตนมีต้นทุนต่ำพอจะต่อสู้กับผู้ประกอบการ OTT

การนำเทคโนโลยีดังกล่าวมาใช้ยังมีความท้าทายอยู่อีกมากกับมิติในการแข่งขันของเหล่าบรรดาผู้ให้บริการ OTT ที่สามารถหาลูกค้าได้จากทุกพื้นที่ทั่วโลกโดยไม่สนใจว่าลูกค้าเหล่านั้นจดทะเบียนใช้บริการโทรศัพท์เคลื่อนที่กับผู้ประกอบการรายใด พูดง่ายๆ ว่าเป็นการแข่งขันระหว่างมหาอำนาจ OTT ที่ความสามารถของแพลตฟอร์มที่สามารถหาลูกค้าเป็นใครก็ได้ทั่วโลก ในขณะที่ VoLTE เป็นเพียงการให้บริการของผู้ประกอบการโทรศัพท์เคลื่อนที่แต่ละรายในแต่ละประเภทเท่านั้น เรื่องนี้อาจจบลงด้วยการเป็นเพียงความพยายามที่จะหารายได้ Voice ที่กำลังค่อยๆ เสื่อมสลายไปกลับมาโดยอาศัยการสื่อสารทางในช่องทางข้อมูลเท่านั้น คงต้องคอยติดตามความคืบหน้าของการแข่งขันทางด้านเทคโนโลยีเหล่านี้กันต่อไป

ธัชชัย จำลอง
touchai@gmail.com



เบื้องลึกเบื้องลับกับ Windows & Microsoft Office

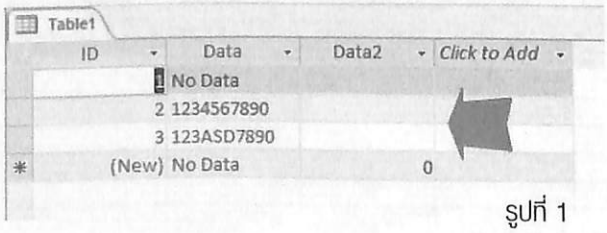
ตอนเจาะลึก Microsoft Access ฉบับหาอ่านที่ไหนไม่ได้ #8

สาระเล็กๆ น้อยๆ กับเทคนิคการใช้งาน รวมทั้งคำสั่งที่ซ่อนอยู่ใน ระบบปฏิบัติการและโปรแกรมสำนักงานชุดนี้ มาเจาะลึก Microsoft Access โดยจะแนะนำวิธีใช้ Format ใน Data Type เกี่ยวกับเรื่องวุ่นๆ ของ Date/Time

เรื่องของข้อมูลประเภท Date/Time นี่ไม่ว่าจะอยู่ใน Excel หรือ Access ก็มักสร้างปัญหาให้ผู้ใช้อยู่เสมอครับ เช่น ป้อนข้อมูลเข้าไปเป็นวัน-เดือน-ปี ประมาณ 10/12/2017 โดยหวังว่าจะเป็นวันที่ 10 เดือนธันวาคม ปี 2017 แต่โปรแกรมดันเข้าใจว่าเป็นวันที่ 12 เดือนตุลาคม ปี 2017 ไปซะได้

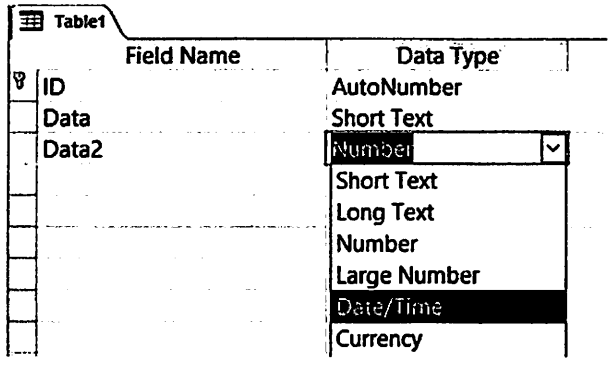
บทความคราวนี้จะช่วยบรรเทาปัญหาเกี่ยวกับ Date/Time แน่นอนครับ ลองอ่านดูนะครับ

1. ขอใช้ตารางเดิมนะครับ ถ้ามีข้อมูลอยู่ใน Data2 ก็ให้ลบออกให้หมดก่อน (รูปที่ 1)

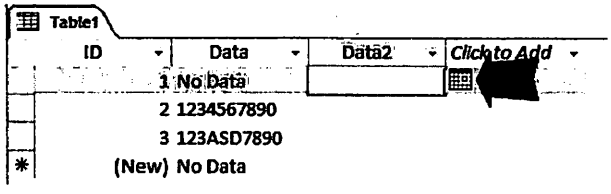


รูปที่ 1

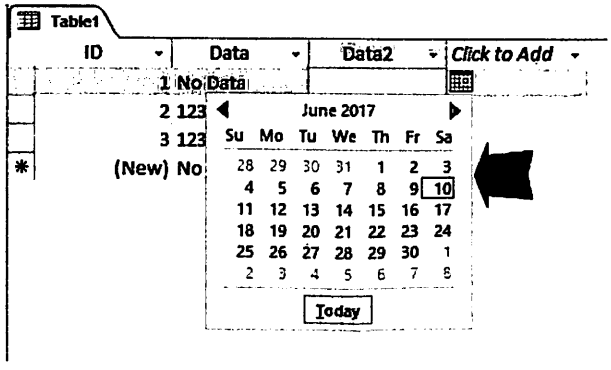
2. จากนั้นก็เปิดมุมมองออกแบบ แล้วเปลี่ยน Data Type เป็น Date/Time (รูปที่ 2)
3. เพียงเท่านี้เวลาที่เราป้อนข้อมูลจะมีตัวช่วย (รูปที่ 3) แสดงผลขึ้นมา (ตัวช่วยนี้มีชื่อว่า Date Picker ครับ)
4. เพียงคลิกที่ปุ่มนี้ก็จะมีปฏิทินเล็กๆ แสดงขึ้นมาให้เราเลือกวันที่ต้องการใส่เข้าไปตารางครับ (รูปที่ 4)



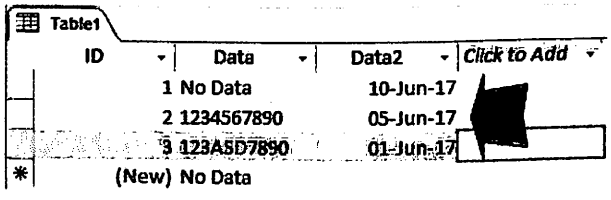
รูปที่ 2



รูปที่ 3

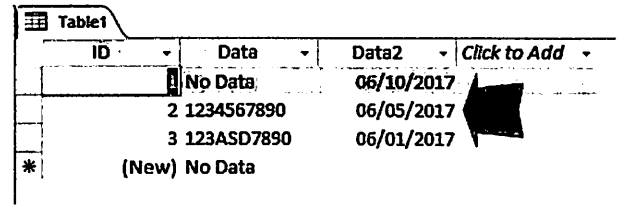


รูปที่ 4

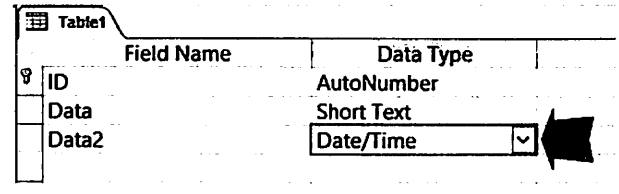


รูปที่ 5

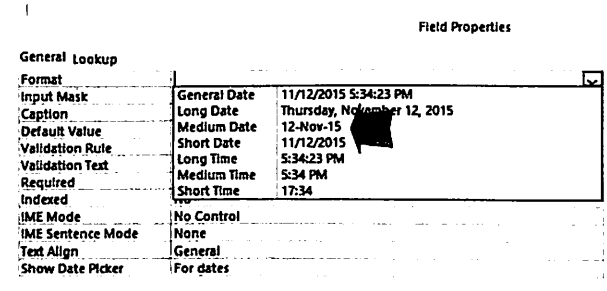
5. พอเราเลือกวันที่ที่เราต้องการ ข้อมูลก็จะถูกใส่เข้าไปในตารางทันที (รูปที่ 5)
6. ถ้าข้อมูลในตารางของใครชวนสับสนแบบนี้เราต้องไปตั้งค่ากัน (รูปที่ 6) นิดหน่อยครับ (แน่นอนว่ามีหลายวิธีด้วยกัน)
7. วิธีแรกให้ไปกำหนดที่มุมมองออกแบบครับ (รูปที่ 7)
8. ให้เลือกรูปแบบวันได้ตามต้องการที่ Format นั่นเอง (รูปที่ 8)
9. แต่ถ้าจะให้เด็ดขาดไปเลยต้องไปกำหนดที่ Settings (สำหรับ Windows 10) โดยให้เลือก Time & Language ครับ (รูปที่ 9)



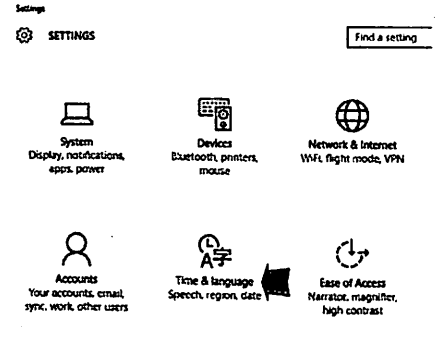
รูปที่ 6



รูปที่ 7

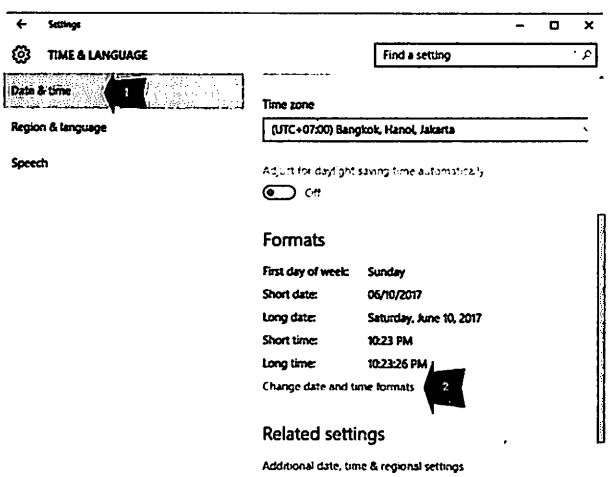


รูปที่ 8

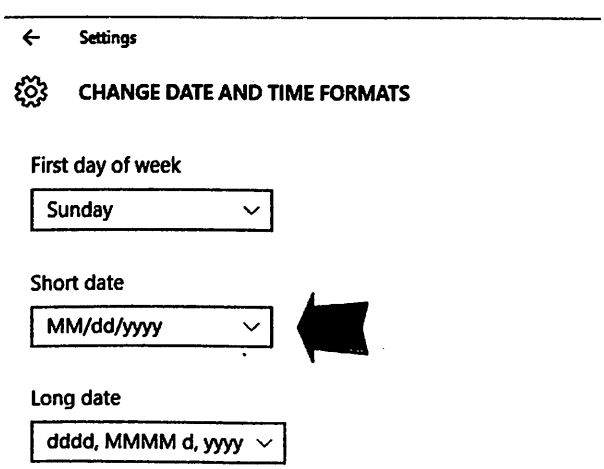


รูปที่ 9

10. จากนั้นก็เลือก Change date and time formats (รูปที่ 10)
11. ที่ Short Date จะแสดงรูปแบบของวันที่แบบเดียวกับที่แสดงอยู่ในตารางแบบนี้ครับ (รูปที่ 11)
12. ให้เราไปเลือกรูปแบบที่เราต้องการได้ที่นี่เลยครับ (รูปที่ 12)
13. ถ้าใครไม่ถนัดกับ Settings ของ Windows 10 หรืออาจจะใช้ Windows รุ่นก่อนหน้าก็สามารถเข้าไปที่ Control Panel แล้วเลือกเมนู Change date, time or number formats (รูปที่ 13)
14. แล้วเลือกรูปแบบวันที่ที่เราต้องการได้ที่ Short date ครับ (รูปที่ 14)

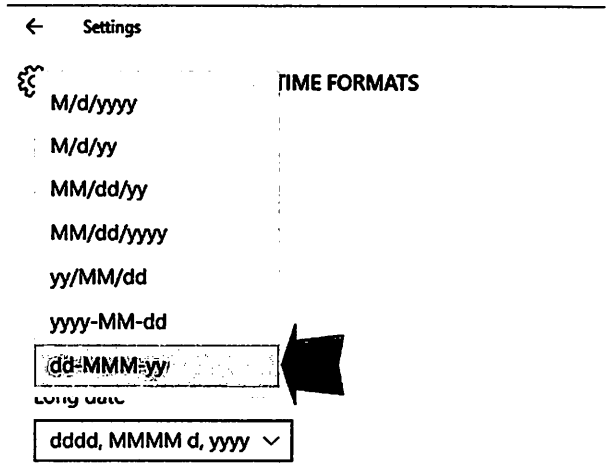


รูปที่ 10

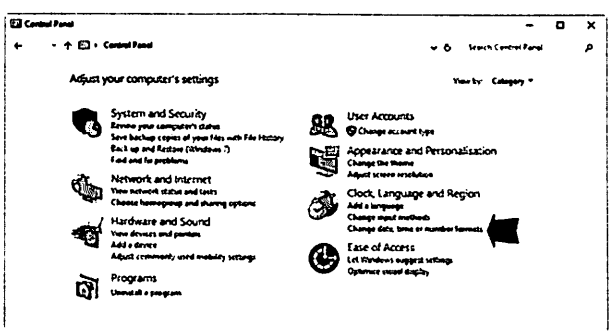


รูปที่ 11

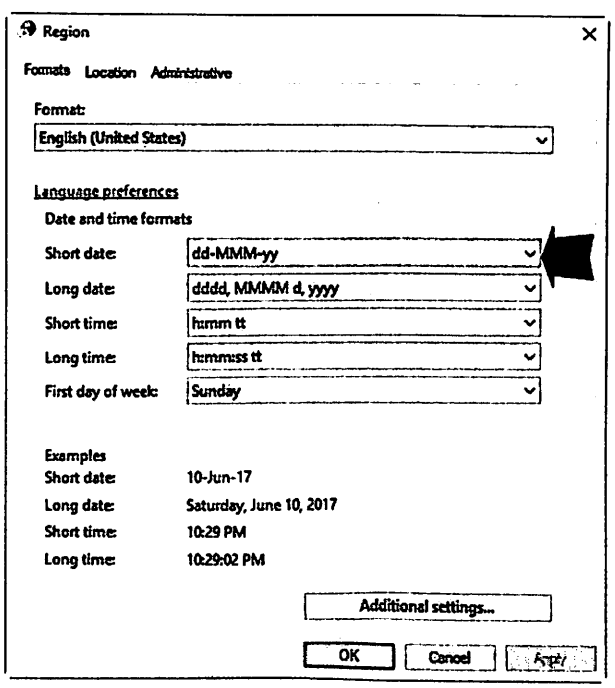
สุดท้ายให้ Restart คอมพิวเตอร์ที่เราใช้งานใหม่ รูปแบบที่เราเลือกก็จะแสดงในตารางแล้วครับ (Windows 10 แค่ปิด Access แล้วเปิดใหม่ก็ได้แล้วนะครับ)



รูปที่ 12



รูปที่ 13

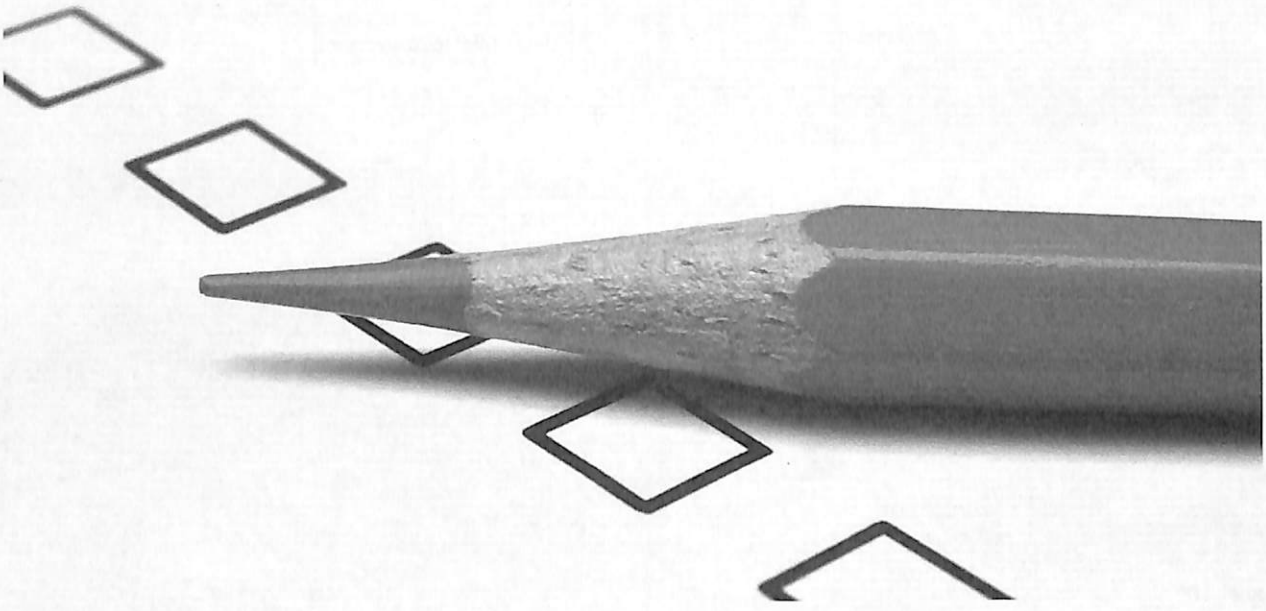


รูปที่ 14

แล้วหน้ากระดาษก็หมด แต่เนื้อหายังไม่หมด ดังนั้นคงต้องรอพบกันในฉบับถัดไปนะครับ สำหรับฉบับนี้สวัสดีครับ ^_^

■ ธัชชัย จำลอง
touchai@gmail.com

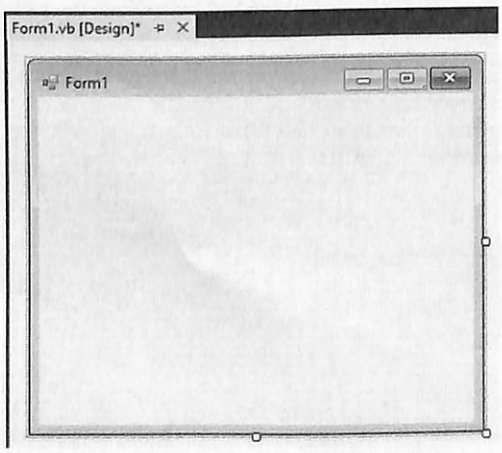
สูงสุดสู่สามัญกับบทบาทสำคัญของ Visual Basic ตอนคอนโทรลพื้นฐานในการใช้งาน VB.Net (10)



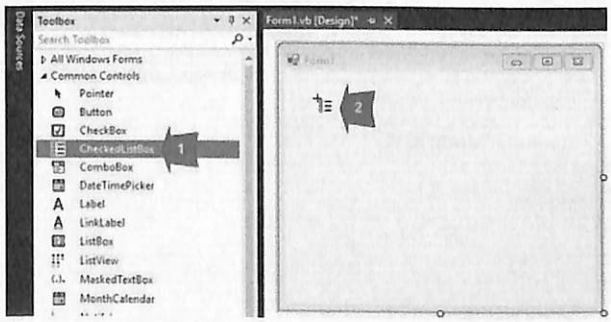
ท่านที่เคยหลอนกับ "คอนโทรล" ในเรื่องของฟอร์มว่าจะควบคุมอะไรยังไง เนื่องจากคอนโทรลใน VB.Net มีมากมาย รอบนี้ถึงคิวของ CheckedListBox

ดูเหมือนเรื่องคอนโทรลพื้นฐานของ VB นี่เราจะไม่สามารถจบกันง่ายๆ เลยนะครับ คราวนี้เราจะมาดูการใช้งาน CheckedListBox กันครับ

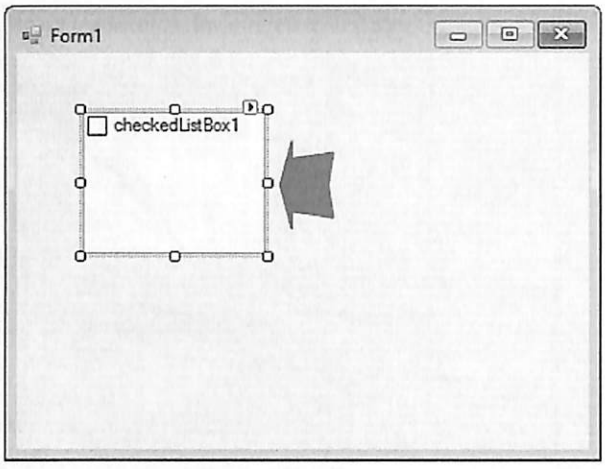
1. อันดับแรกให้เราเปิดโปรเจ็กต์ใหม่ขึ้นมาครับ (รูปที่ 1)
2. จากนั้นให้นำ CheckedListBox มาวางบนฟอร์ม 1 ออบเจ็กต์ (รูปที่ 2)



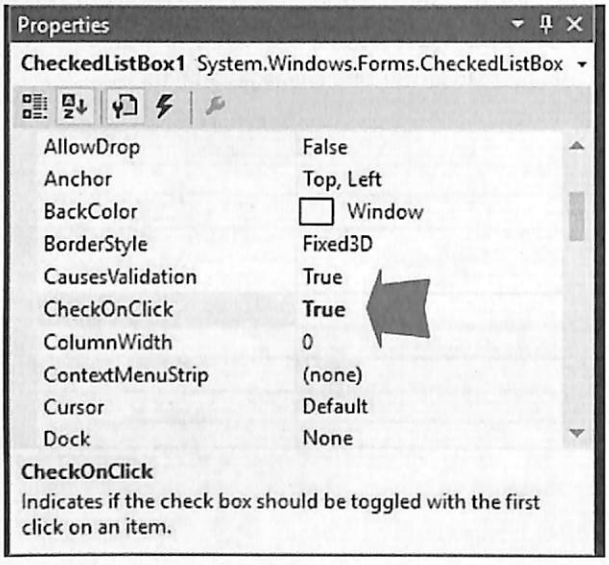
รูปที่ 1



รูปที่ 2

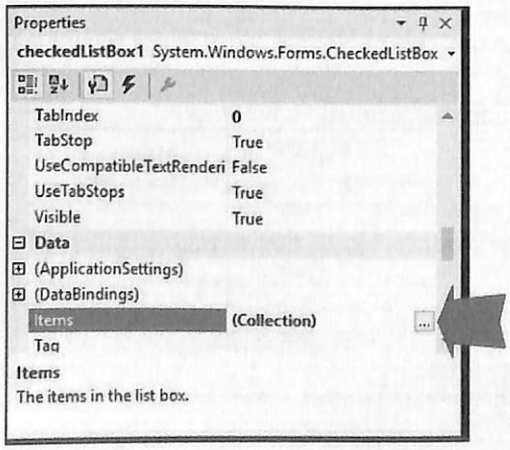


รูปที่ 3

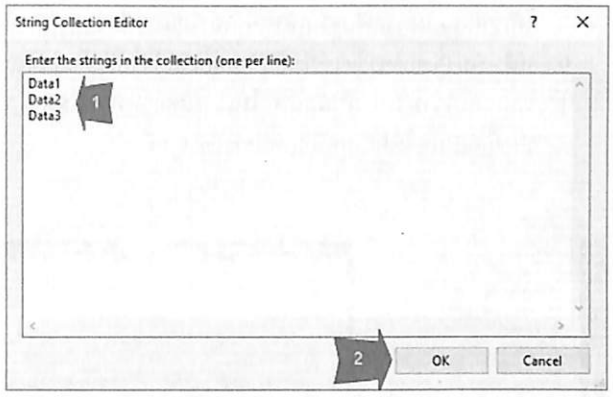


รูปที่ 4

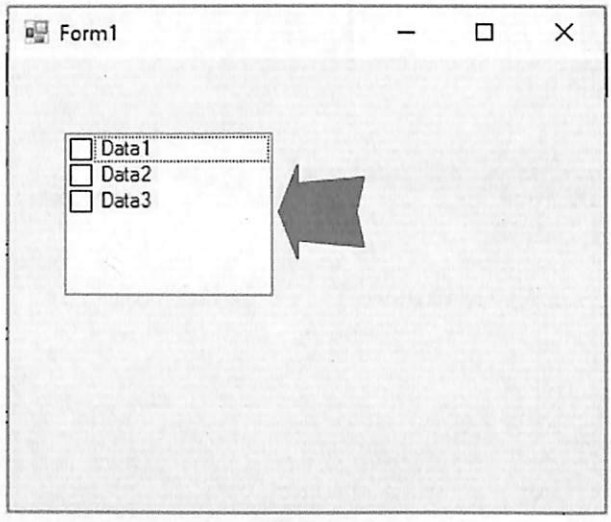
3. หน้าตาของ CheckedListBox จะเป็นแบบนี้ครับ (รูปที่ 3)
4. กำหนด CheckOnClick ให้กับคอนโทรลนี้เพื่อความสะดวกในการเลือกตัวเลือกด้วยครับ (รูปที่ 4)



รูปที่ 5

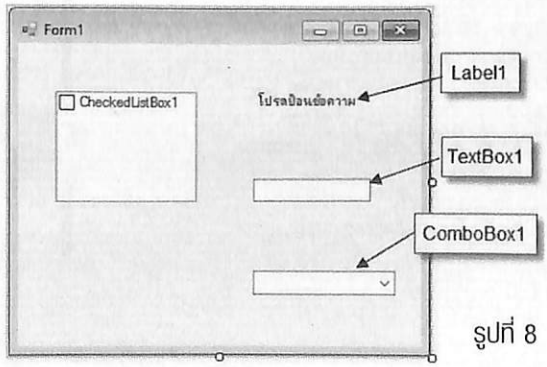


รูปที่ 6



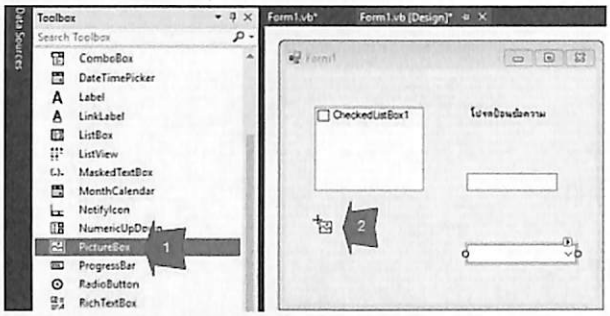
รูปที่ 7

5. เราสามารถใส่รายการให้กับ CheckedListBox ได้โดยคลิกที่ตัวเลือก Items (รูปที่ 5)
6. ในที่นี้ให้ลองใส่ Data1, Data2 และ Data3 เข้าไปแบบนี้ (รูปที่ 6)
7. ลองสั่ง Start ได้ครับ เราจะเห็นตัวเลือกตามที่เรากำหนดเอาไว้แสดงใน CheckedListBox ทันที แต่ในที่นี้เราไม่ต้องการครับ เดี๋ยวเราจะไปเขียนโค้ดใส่ตัวเลือกเข้าไปแทน ดังนั้นลบ Items ออกไปได้เลย แล้วมาเริ่มใส่คอนโทรลเข้าไปในฟอร์มกัน (รูปที่ 7)

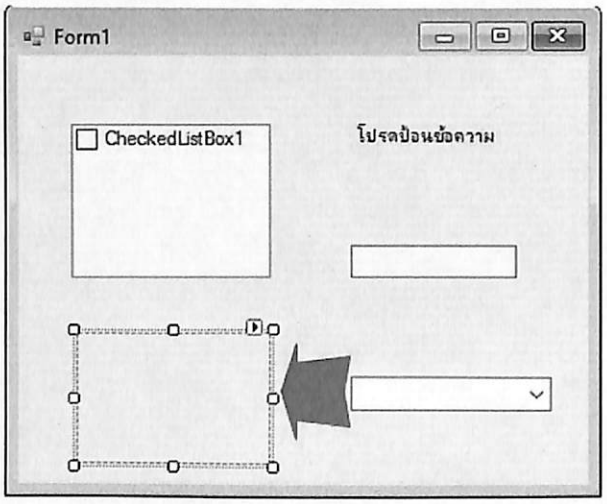


รูปที่ 8

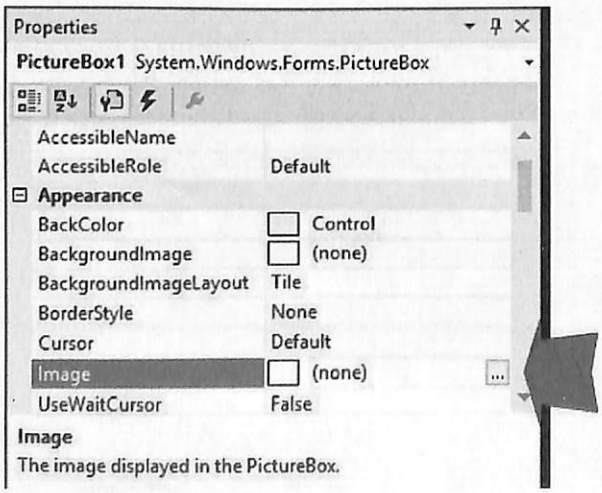
8. ให้เราใส่คอนโทรลพื้นฐานเข้าไปในฟอร์มแบบนี้ครับ (รูปที่ 8)
9. แล้วเพิ่ม PictureBox เข้าไปอีก 1 ออบเจ็กต์ (รูปที่ 9 และ 10)
10. ทบทวนความรู้เก่ากันสักนิด ให้เราเลือกรูปที่จะแสดงใน PictureBox โดยคลิกเลือกที่ Image (รูปที่ 11)



รูปที่ 9

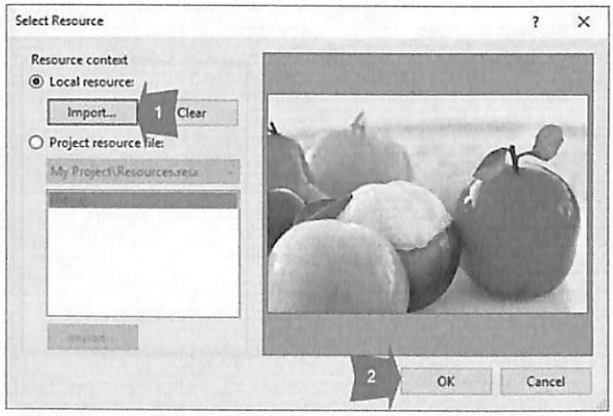


รูปที่ 10

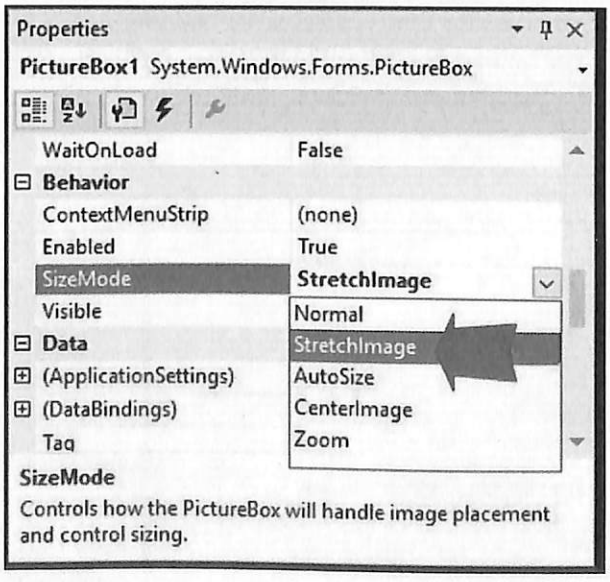


รูปที่ 11

11. แล้วเลือกไฟล์รูปภาพของ Local resource (รูปที่ 12)
12. เพื่อไม่ให้รูปใหญ่กว่า PictureBox ดังนั้นก็ต้องกำหนด SizeMode เป็น StretchImage (รูปที่ 13)

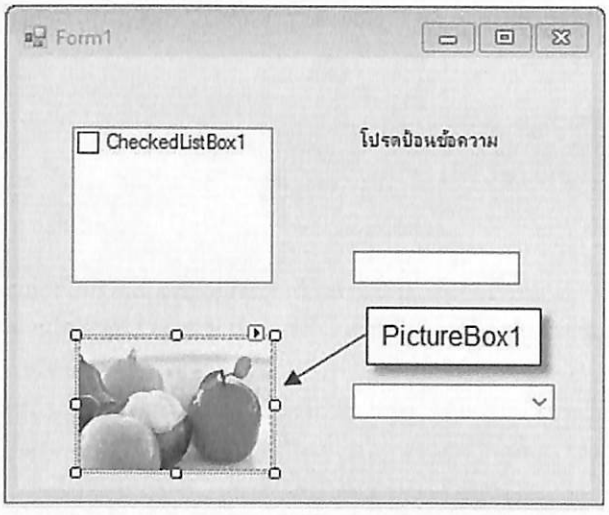


รูปที่ 12



รูปที่ 13

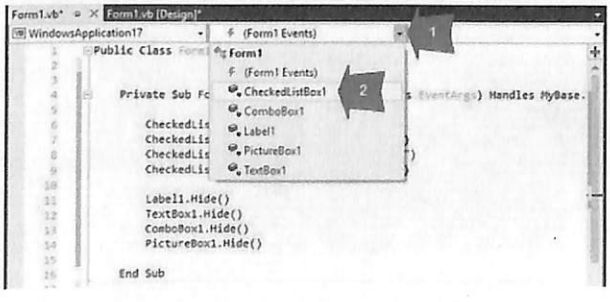
13. เพียงเท่านี้รูปที่เราเลือกก็จะมาแสดงอยู่บนฟอร์มแล้วครับ (รูปที่ 14)
14. ทีนี้เรามาใส่โค้ดกันครับ เริ่มแรกให้ใส่โค้ดควบคุมการแสดงผลของคอนโทรลบนฟอร์ม โดยโค้ดนี้เป็นการใส่รายการตัวเลือกเข้าไปใน CheckedListBox แล้วทำการซ่อนคอนโทรล 4 อันที่เราใส่เข้าไปด้วย (รูปที่ 15)
15. จากนั้นก็ทำการเพิ่มพื้นที่เขียนโค้ดของ CheckedListBox โดยให้เราเลือกคอนโทรลเป้าหมายของเราก่อน (รูปที่ 16)
16. จากนั้นเลือก Event ของคอนโทรลเป้าหมาย โดยในที่นี้เลือกเป็น ItemCheck ครับ (รูปที่ 17)



รูปที่ 14

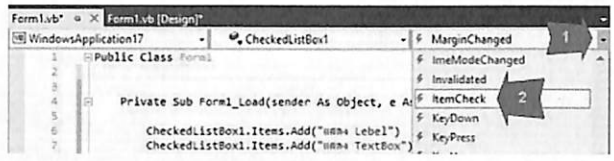
```
Private Sub Form1_Load(sender As Object, e As EventArgs)

    CheckedListBox1.Items.Add("แสดง Lebel")
    CheckedListBox1.Items.Add("แสดง TextBox")
    CheckedListBox1.Items.Add("แสดง ComboBox")
    CheckedListBox1.Items.Add("แสดง Picture")

    Label1.Hide()
    TextBox1.Hide()
    ComboBox1.Hide()
    PictureBox1.Hide()

End Sub
```

รูปที่ 15



รูปที่ 16

17. เราจะได้ Sub ของคอนโทรล CheckedListBox ทันที โดยเราจะเห็นโค้ดเขียนว่า "e As ItemCheckEventArgs" ซึ่งตัว e ตัวนี้เราต้องใช้ในการเขียนโค้ดครับ (รูปที่ 18)
18. ให้เราใช้คำสั่ง Select Case ในการกำหนดเงื่อนไขเวลาเราคลิกเลือกตัวเลือกใน CheckedListBox (รูปที่ 19)
19. พอสั่ง Start ฟอร์มก็พร้อมใช้งานแล้วครับ (รูปที่ 20)



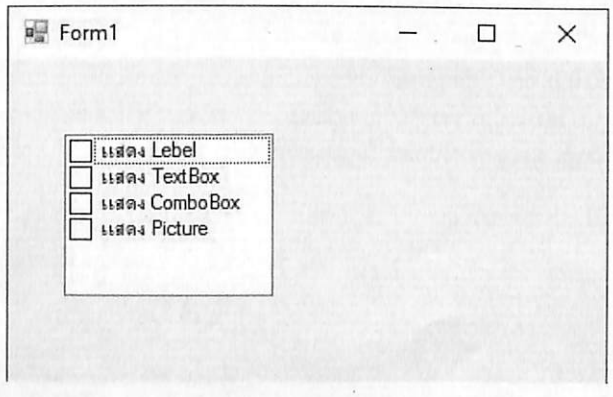
รูปที่ 17

```
Public Class Form1
    Private Sub CheckedListBox1_ItemCheck(sender As Object, e As ItemCheckEventArgs)

    End Sub
```

รูปที่ 18

```
Private Sub CheckedListBox1_ItemCheck(sender As Object,
    Select Case e.Index
        Case 0
            Label1.Show()
        Case 1
            TextBox1.Show()
        Case 3
            ComboBox1.Show()
        Case 4
            PictureBox1.Show()
    End Select
End Sub
```

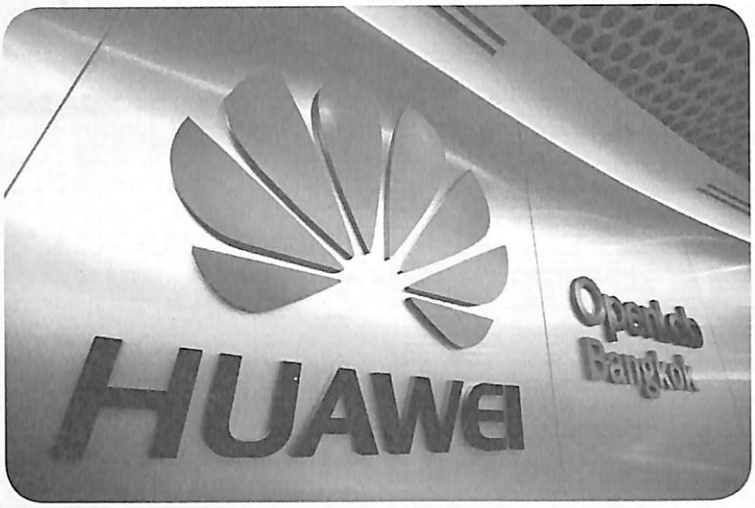
รูปที่ 19



รูปที่ 20

ตอนนี้ถึงฟอร์มจะพร้อมใช้งานก็จริง แต่ดูเหมือนมีอะไรติดๆ ขัดๆ อยู่เล็กน้อย คุณผู้อ่านลองเล่นดูก่อนนะครับ เดี๋ยวคราวหน้าจะมาเฉลยว่าอะไรคือเรื่องติดๆ ขัดๆ แล้วจะแก้ไขอย่างไร สำหรับฉบับนี้สวัสดีก่อนนะครับ ^_^ (หน้ากระดาษหมดจริงๆ แฮะๆ)

หัวเว่ย เปิดศูนย์ Huawei OpenLab Bangkok สนับสนุนการขับเคลื่อนสู่ เศรษฐกิจดิจิทัล อย่างบูรณาการแห่งแรกในประเทศไทย



หัวเว่ย ผู้จัดหาโซลูชั่นไอซีทีชั้นนำระดับโลก เปิดตัวศูนย์หัวเว่ย โอเพ่นแล็ป แบงค์กอก (Huawei OpenLab Bangkok) เพื่อเป็นแพล็ตฟอร์มพื้นฐานด้านไอซีทีแบบครบวงจรสำหรับองค์กรต่างๆ และช่วยขับเคลื่อนการเปลี่ยนผ่านประเทศไทยสู่ยุคเศรษฐกิจดิจิทัล

ดร. สมคิด จาตุศรีพิทักษ์ รองนายกรัฐมนตรี และนายเดวิด ชุน ประธานกรรมการบริหาร และหัวหน้าคณะเจ้าหน้าที่บริหาร บริษัท หัวเว่ย เทคโนโลยี จำกัด ประจำภูมิภาคเอเชียตะวันออกเฉียงใต้ ให้เกียรติร่วมเป็นประธานในพิธีเปิดครั้งนี้

ศูนย์หัวเว่ย โอเพ่นแล็ป แบงค์กอก ใช้เงินลงทุนทั้งสิ้น 15 ล้านเหรียญสหรัฐ และถือเป็นศูนย์โอเพ่นแล็ป ลำดับที่ 7 ของหัวเว่ยทั่วโลก ต่อจากซูโจว เม็กซิโก มิวนิก สิงคโปร์ โจฮันเนสเบิร์ก และดูไบ โดยมีเนื้อที่ราว 2,000 ตารางเมตร ตั้งอยู่ ณ อาคารจี ทาวเวอร์ ซึ่งเป็นที่ตั้งของสำนักงานใหญ่ของบริษัทแห่งใหม่ในประเทศไทย

นายเดวิด ชุน ประธานกรรมการบริหารและหัวหน้าคณะเจ้าหน้าที่บริหาร บริษัท หัวเว่ย เทคโนโลยี จำกัด ประจำภูมิภาคเอเชียตะวันออกเฉียงใต้ กล่าวว่า *"ศูนย์หัวเว่ย โอเพ่นแล็ป แบงค์กอก จะช่วยสนับสนุนการเปลี่ยนผ่านไปสู่ยุคดิจิทัลแก่ลูกค้าและพันธมิตรต่างๆ ในอุตสาหกรรม โดยจะเป็นแพล็ตฟอร์มแบบเปิด และดาต้าเซ็นเตอร์ต่างๆ ช่วยแก้ปัญหาการทดสอบโซลูชั่นการใช้งานต่างๆ กระตุ้นให้เกิดการพัฒนานวัตกรรม ทั้งยังช่วยส่งเสริมการพัฒนาระบบนิเวศอุตสาหกรรม และให้บริการฝึกอบรมด้านไอซีที*

ศูนย์หัวเว่ย โอเพ่นแล็ป แบงค์กอก จะช่วยอำนวยความสะดวกในการพัฒนานวัตกรรมความร่วมมือและการคิดค้นโซลูชั่นใหม่ร่วมกับลูกค้าและพันธมิตรทางธุรกิจทั้งในประเทศไทย รวมไปถึงประเทศอื่นๆ ในภูมิภาคเอเชียตะวันออกเฉียงใต้ ในด้านต่าง ๆ อาทิ สมาร์ทซิตี้ ความปลอดภัยสาธารณะ โครงข่ายไฟฟ้าอัจฉริยะ (Smart Grid) การเงิน การศึกษา การขนส่ง และผู้ให้บริการอินเทอร์เน็ต

ในพิธีเปิดศูนย์ดังกล่าว นายเดวิด ชุน ได้กล่าวว่า ศูนย์โอเพ่นแล็ป แบงค์กอก ยังจะช่วยสนับสนุนนโยบายของรัฐบาล และช่วยขับเคลื่อนและส่งเสริมธุรกิจสตาร์ทอัพและการศึกษาของไทยในด้านไอซีทีด้วย

"เมื่อผนวกกับวิสัยทัศน์ของรัฐบาล ในการพัฒนาเศรษฐกิจของประเทศสู่ยุคเศรษฐกิจดิจิทัล "ไทยแลนด์ 4.0" และโครงการระเบียงเศรษฐกิจภาคตะวันออก เพื่อผลักดันให้ประเทศไทยเป็นศูนย์กลางเทคโนโลยีสารสนเทศและการสื่อสาร (ไอซีที) ของภูมิภาคมีความชัดเจนขึ้น ดังนั้นจึงต้องมีการลงทุนอย่างต่อเนื่อง โครงสร้างพื้นฐานด้านโทรคมนาคมได้ผลักดันให้ความเร็วในการเชื่อมต่อโมบายบรอดแบนด์เพิ่มขึ้นจาก 5 Mbs ไปอยู่ที่ 15 Mbps และเชื่อมโยงเครือข่ายการสื่อสารโดยตรงของไทยไปยังประเทศต่างๆ ให้เพิ่มมากขึ้นผ่านเคเบิ้ลใต้น้ำ"

เราเชื่อมั่นว่าด้วยระบบการเมืองที่มีเสถียรภาพ สภาพเศรษฐกิจ นโยบายด้านเศรษฐกิจดิจิทัล สิทธิประโยชน์ด้านการลงทุนจากบีโอไอ และการเชื่อมโยงของเครือข่ายการบิน รวมถึงบุคลากรที่มีความสามารถด้านไอซีที จะทำให้ประเทศไทยเป็นตัวเลือกที่เหมาะสมมากขึ้นในสายตาขององค์กรธุรกิจในระดับนานาชาติ" นายชุน กล่าวเสริม

นอกจากนี้หัวเว่ยยังคงให้การสนับสนุนภาครัฐบาลของไทยในหลายด้านผ่านการทำงานร่วมกันกับภาครัฐ และเอกชน และองค์กรวิจัยต่างๆ เพื่อสร้างระบบนิเวศ การปรับโครงสร้างของอุตสาหกรรมสู่การเติบโตแนวดิ่ง (vertical industries) และการนำเสนอประสบการณ์การใช้งานดีไวซ์ที่ดีที่สุดแก่ลูกค้าชาวไทย

"ในปัจจุบันนี้ คนไทยกว่า 6 ล้านคน ใช้อุปกรณ์ดีไวซ์ของหัวเว่ย และเพลิดเพลินกับคุณสมบัติใหม่ ๆ ของเครื่อง อาทิ กล้องเลนส์คู่ที่พัฒนาร่วมกับไลก้า วีดีโอสตรีมมิ่งแบบเอชดี และเทคโนโลยีการสื่อสารความเร็วสูง LTE นวัตกรรมเหล่านี้จะช่วยสร้างความแข็งแกร่งของหัวเว่ยในฐานะหนึ่งใน 3 แบรนด์ชั้นนำของสมาร์ทโฟนระดับไฮเอนด์ ที่มีระดับการรับรู้ของแบรนด์สูงที่สุดเป็นประวัติการณ์ถึงร้อยละ 84" นายเดวิด ชุน กล่าว

ในปีที่ผ่านมาหัวเว่ยได้จ่ายภาษีเป็นจำนวนทั้งสิ้น 33 ล้านเหรียญดอลลาร์สหรัฐ และสร้างงานมากกว่า 10,000 ตำแหน่งในประเทศไทย ซึ่งเพิ่มขึ้นสองเท่าจากปีก่อนหน้า นอกจากนี้บริษัทยังใช้งบจัดซื้อจัดจ้างถึง 660 ล้านเหรียญดอลลาร์สหรัฐ ในช่วง 5 ปีที่ผ่านมา และได้มีการจัดการอบรมด้านไอซีทีให้กับ **"นักรบดิจิทัล"** มากกว่า 35,000 คนในประเทศไทยในช่วงสิบปีที่ผ่านมา

"เรามุ่งหวังว่าบริษัทหัวเว่ยจะเป็นตัวอย่างที่ดีขององค์กรธุรกิจต่างชาติที่เข้ามาทำธุรกิจในประเทศไทย" **นายชุน กล่าว**

ศูนย์โอเพ่น แล็ป บางกอก ตั้งเป้าจะให้การฝึกอบรมบุคลากรด้านไอซีทีไม่ต่ำกว่า 800 คนต่อปี รวมถึงพัฒนาบุคลากรที่ผ่านประกาศนียบัตรรับรองด้านอาชีพ Huawei Certification อีก 500 คนต่อปี และคาดว่าจะสามารถรองรับโครงการทดสอบแนวคิด (POC) ราว 150 คนต่อปี โดยคาดว่าทุก ๆ ปี จะสามารถต้อนรับบริษัทสตาร์ทอัพด้านไอซีทีได้มากกว่า 20 ราย

ในส่วนของโครงการความร่วมมือของศูนย์โอเพ่น แล็ป บางกอก กับหน่วยงานต่างๆ ได้แก่

- โครงการพัฒนานวัตกรรมเกี่ยวกับโซลูชั่นด้านไอซีทีเพื่อพัฒนาระบบพลังงานไฟฟ้าร่วมกับการไฟฟ้า ส่วนภูมิภาค
- โครงการความร่วมมือทางยุทธศาสตร์เมืองแห่งความปลอดภัยของกรมตำรวจ
- โครงการความร่วมมือกับกลุ่มสตาร์ทอัพด้านเมืองอัจฉริยะของสถาบันเทคโนโลยีพระจอมเกล้า เจ้าคุณทหารลาดกระบัง

นอกจากนี้ที่ศูนย์หัวเว่ย โอเพ่นแล็ป แบงค์กอกยังได้ประสานความร่วมมือกับพันธมิตรธุรกิจ ทั้งในและต่างประเทศอีกกว่า 30 แห่ง เพื่อให้บริการข้อมูล และสนับสนุนการพัฒนานวัตกรรม และดิจิทัลโซลูชั่น อาทิ เอสเอพี, ไมโครซอฟท์, ฮันนี่เวลล์, บอมบาร์ดิเอร์, ออราเคิล, แอ็กเซนเจอร์ และอินโฟซีส ฯลฯ

และในปี 2560 หัวเว่ยวางแผนที่จะเปิดศูนย์โอเพ่น แล็ป ใหม่อีก 7 แห่งทั่วโลก และอีก 3 ปีนับจากนี้ จะลงทุนด้วยงบประมาณทั้งสิ้น 200 ล้านเหรียญดอลลาร์สหรัฐ และเพิ่มบุคลากรอีกประมาณ 1,000 คน เพื่อสร้างศูนย์โอเพ่น แล็ป ให้ครบ 20 แห่งในปี 2562

ไมโครซอฟท์เดินหน้าสานต่อแคมเปญคลาวด์เพื่อสาธารณะประโยชน์ ร่วมสนับสนุน "โครงการกาแฟอินทรีย์รักษาป่า" ของมูลนิธิสายใยแผ่นดิน ผ่านแพล็ตฟอร์มไมโครซอฟท์ อาซัวร์

บริษัท ไมโครซอฟท์ (ประเทศไทย) จำกัด มอบไมโครซอฟท์ อาซัวร์เทคโนโลยีคลาวด์ที่ปลอดภัยและให้ความเชื่อมั่นกับทุกองค์กรทั่วโลก ให้กับมูลนิธิสายใยแผ่นดินเพื่อโครงการกาแฟอินทรีย์รักษาป่า ตอกย้ำพันธสัญญาของไมโครซอฟท์ในการมอบเทคโนโลยีคลาวด์เพื่อสาธารณประโยชน์ โดยการจับมือกับบริษัท บีทามส์ โซลูชั่น จำกัด บริษัทพัฒนาแอพพลิเคชั่น Internal Control System หรือการตรวจรับรองมาตรฐานภายใน ที่พัฒนาด้วยไมโครซอฟท์ อาซัวร์ เพื่อช่วยพนักงานประหยัดระยะเวลาและขั้นตอนในการตรวจรับรองมาตรฐานอินทรีย์ของกระบวนการและผลผลิตกาแฟด้วยการจัดเก็บข้อมูลและประมวลผลผ่านคลาวด์ได้รวดเร็วขึ้นจากการใช้เวลา 4 เดือนเหลือเพียง 1 เดือนลดลงกว่า 75% เพิ่มประสิทธิภาพในการบริหารจัดการระบบการตรวจสอบสวนกาแฟ ส่งผลให้ขีดความสามารถในการทำงานของพนักงานมูลนิธิเพิ่มขึ้น

"การพัฒนาขีดความสามารถของธุรกิจในภาคการเกษตรและการพัฒนาศักยภาพทางด้านเทคโนโลยีเพื่อบุคลากรที่ทำงานในภาคเกษตรเป็นเรื่องที่เราให้ความสำคัญเป็นลำดับต้นๆ ในการนำเทคโนโลยีเข้ามาใช้เป็นเครื่องมือสำคัญเพื่อขับเคลื่อนการพัฒนาประเทศ เราเชื่อมั่นว่าการทำธุรกิจผ่านระบบดิจิทัล จะเปรียบเสมือนการเสริมกำลังให้กลุ่มเกษตรกรและวิสาหกิจชุมชนให้ทำงานได้อย่างคล่องตัว" **นางวรรณพร เทพหัสดิน ณ อยุธยา เลขาธิการคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ** กล่าว *"เราเชื่อว่าการสนับสนุนด้านเทคโนโลยีคลาวด์เพื่อสาธารณประโยชน์จากไมโครซอฟท์กับองค์กรไม่แสวงผลกำไรต่างๆ เช่น มูลนิธิเพื่อนศิลปะ สมาคมพัฒนาประชากรและชุมชน หรือ พีดีเอ (PDA) สถาบันเชนจ์ฟิวชั่น รวมถึงมูลนิธิสายใยแผ่นดินในครั้งนี้จะช่วยเพิ่มประสิทธิภาพการบริหารจัดการด้านการเกษตร และนำไปสู่การทำการเกษตรแบบอัจฉริยะ เพื่อสร้างมูลค่าเพิ่มและเป็นรากฐานสำคัญที่จะยกระดับประเทศไทยให้มีบทบาทมากขึ้นในระดับสากล"*

นายธนวัฒน์ สุธรรมพันธุ์ กรรมการผู้จัดการ บริษัท ไมโครซอฟท์ (ประเทศไทย) จำกัด กล่าวว่า *"สำหรับไมโครซอฟท์ ภารกิจของพวกเราคือ เป็นกำลังสำคัญให้ทุกคนและทุกองค์กรในทุกมุมโลกได้บรรลุผลสำเร็จที่ดียิ่งกว่า ในการที่จะทำให้ภารกิจนี้ประสบความสำเร็จ เราต้องทำให้ทุกคนบนโลกนี้สามารถเข้าถึงเทคโนโลยีได้อย่างเท่าเทียมกัน เชื่อว่าแนวคิด "Public Cloud for Public Good (คลาวด์สาธารณะเพื่อสาธารณประโยชน์) ของไมโครซอฟท์จะสามารถสร้างศักยภาพปกป้อง และสร้างแรงบันดาลใจ ให้กับผู้ที่ใช้เทคโนโลยีได้ เพื่อการนำคลาวด์อัจฉริยะอย่างอาซัวร์มาใช้ให้เกิดประโยชน์ในการพัฒนาประเทศไทยในทุกๆด้านไปพร้อมๆ กับผู้คนในทั่วทุกมุมโลก"*

ตลอดระยะเวลา 23 ปี ในประเทศไทย ไมโครซอฟท์ได้มุ่งมั่นทำงานอย่างหนักเพื่อเป็นพันธมิตรในระยะยาวของประเทศไทย ไมโครซอฟท์ได้ร่วมมือกับองค์กรไม่แสวงผลกำไรและองค์กรธุรกิจต่างๆ ในการนำเทคโนโลยีคลาวด์มาลดช่องว่างเพื่อสร้างความเท่าเทียมในการเข้าถึงผ่านเทคโนโลยี

ในประเทศไทย ไมโครซอฟท์ ได้บริจาคซอฟต์แวร์รวมมูลค่ากว่า 2 ล้านเหรียญสหรัฐ หรือราว 70 ล้านบาท ให้กับองค์กรไม่แสวงผลกำไรต่างๆ กว่า 430 แห่ง พร้อมการฝึกอบรมเทคโนโลยีโดยไม่มีค่าใช้จ่าย เพื่อช่วยให้องค์กรเหล่านั้นมีศักยภาพที่เพิ่มขึ้นในการทำงานหรือแม้กระทั่งการช่วยเหลือกลุ่มผู้ด้อยโอกาสได้ดียิ่งขึ้น

แอพพลิเคชั่น Internal Control System (ICS) เข้ามาช่วยเพิ่มคุณค่า (Value) ในกระบวนการผลิตตามมาตรฐานเกษตรอินทรีย์ได้ 3 ประการ คือ

- **เพิ่มประสิทธิภาพการทำงานด้วยการประยุกต์เทคโนโลยีคลาวด์ในการเก็บและประมวลผลข้อมูล** พนักงานสามารถป้อนข้อมูลได้โดยตรงผ่านสมาร์ทโฟนหรือแท็บเล็ตทั้งแบบออนไลน์และออฟไลน์ และไปเก็บในไมโครซอฟท์ คลาวด์สาธาณะ อาซัวร์ ทำให้ได้ฐานข้อมูลกลางที่ถูกต้อง และสามารถแชร์เพื่อการใช้งานร่วมกันตั้งแต่ต้นทางถึงปลายทางการผลิตสินค้าเกษตรอินทรีย์
- **ประหยัดเวลาและต้นทุนในขั้นตอนของการตรวจสอบตามมาตรฐานเกษตรอินทรีย์** ด้วยระบบประมวลผลอย่าง Microsoft SQL Database พร้อมใช้ Power BI เป็นเครื่องมือวิเคราะห์และแสดงผลข้อมูลได้ทั้งแบบ Dashboard และ GIS ช่วยให้ผู้บริหารและทีมงานประเมินผล ทราบสถานะในกระบวนการในการจัดการทางเกษตรอินทรีย์ เพื่อที่จะบริหารจัดการได้อย่างทันเวลา และใช้ในการสร้างรายงานประกอบการรับรองมาตรฐานผลผลิตกาแฟ ทำให้เกิดการตรวจสอบและออกใบรับรองได้เร็วขึ้น
- **ในอนาคตมูลนิธิตั้งเป้าที่จะยกระดับมาตรฐาน โดยการนำเทคโนโลยี IoT ทางการเกษตรมาใช้บริหารจัดการช่วงเพาะปลูกได้อย่างมีประสิทธิภาพ** โดยบูรณาการข้อมูลจาก IoT แบบเรียลไทม์และประมวลผลผ่านทาง Microsoft's IoT Hub Public Cloud โดยจะทำให้พนักงานสามารถมอนิเตอร์และควบคุมและจัดการปรับสภาพแวดล้อมต่างๆ ในสวนกาแฟได้แบบเรียลไทม์ สามารถดูแลสวนกาแฟได้อย่างทั่วถึง เพื่อให้ได้ผลผลิตเมล็ดกาแฟออร์กานิคคุณภาพดีเพิ่มขึ้นแบบยั่งยืน

แบล็คเบอรี่ ผนึกพันธมิตร ดาต้าวัน เอเชีย รุกตลาด Mobility Enterprise รองรับนโยบายไทยแลนด์ 4.0

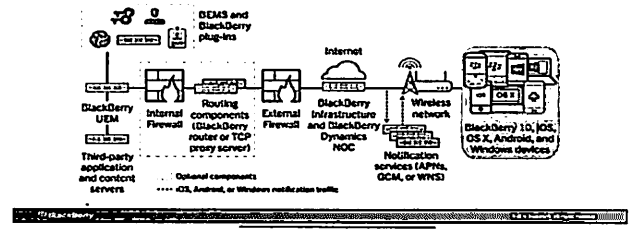
แบล็คเบอรี่ เผยเทรนด์ดิจิทัลในเอเชียแปซิฟิกมาแรงดันตลาดไอทีโต ประกาศจับมือพันธมิตร ดาต้าวัน เอเชีย เปิดตัวโซลูชัน Enterprise Mobile Management รองรับนโยบายไทยแลนด์ 4.0 หลังภาครัฐและเอกชนขานรับนโยบาย เดินหน้าลงทุนโครงสร้างพื้นฐานนำพาองค์กรสู่ Digital Transformation ในยุคเศรษฐกิจดิจิทัล

บริษัท แบล็คเบอรี่ (สิงคโปร์) จำกัด ประกาศจับมือพันธมิตรทางธุรกิจกับ บริษัท ดาต้าวัน เอเชีย (ประเทศไทย) จำกัด ซึ่งเป็นบริษัทตัวแทนจำหน่ายอุปกรณ์ในกลุ่ม Network และ Security ชั้นนำ เพื่อเปิดตลาด Enterprise Mobile Management หรือ โซลูชันการจัดการอุปกรณ์เคลื่อนที่ขององค์กรในประเทศไทย โดยคาดการณ์ว่าแนวโน้มในอีก 3 ปีข้างหน้า องค์กรในเอเชียแปซิฟิกจะมุ่งสู่การทำ Digital Transformation อย่างเต็มรูปแบบ ประกอบกับมองเห็นศักยภาพของตลาดของลูกค้าองค์กรในประเทศไทยที่มีความพร้อมทั้งภาครัฐและเอกชน จากนโยบายไทยแลนด์ 4.0 ที่ส่งเสริมและผลักดันให้ประเทศไทยก้าวเข้าสู่ยุคเศรษฐกิจดิจิทัล จึงเล็งเห็นถึงความต้องการในด้านการสนับสนุนให้องค์กรเป็น Mobility Enterprise เพิ่มขึ้น เนื่องจากองค์กรในธุรกิจปัจจุบัน จำเป็นต้องใช้ซอฟต์แวร์ในการทำหน้าที่ประสานกระบวนการสร้างสรรค์ผลิตภัณฑ์ งานบริการและโซลูชัน ให้องค์กรสามารถตอบสนองความต้องการของลูกค้า พร้อมปรับเปลี่ยนขั้นตอนการทำงานให้ง่ายขึ้น สะดวกขึ้น เพื่อช่วยสร้างความพร้อมทางธุรกิจในการแข่งขันได้อย่างเต็มประสิทธิภาพ

ที่ผ่านมาแบล็คเบอรี่มีประสบการณ์กว่า 10 ปี ในการทำงานสนับสนุนเกี่ยวกับความปลอดภัยของข้อมูลบนเครื่องสมาร์ทโฟนและร่วมกับบริษัทชั้นนำทั่วโลกกว่า 100 บริษัท ในการให้บริการด้านระบบ Mobility Enterprise และ Security ด้วยการพัฒนาการเชื่อมโยงข้อมูลทำงานผ่านระบบและอุปกรณ์ไอทีใหม่ๆ อยู่ตลอดเวลา ทำให้ทราบถึงความจำเป็น ปัญหา และความสำคัญของการนำอุปกรณ์ที่หลากหลายมาใช้งานในองค์กร ซึ่งโซลูชัน Unified Endpoint Manager (UEM) จากแบล็คเบอรี่ จะมาช่วยทำหน้าที่จัดการอุปกรณ์เคลื่อนที่ต่าง ๆ ให้สอดรับกับนโยบายและโครงสร้างพื้นฐานของธุรกิจ เพื่อการทำงานในยุคดิจิทัล พร้อมยืนยันความปลอดภัยเป็นอันดับหนึ่ง ด้วยผลรายงานการวิเคราะห์จาก Gartner เพื่อให้มั่นใจว่าอุปกรณ์พกพาอย่าง โน๊ตบุ๊ค สมาร์ทโฟน แท็บเล็ต และอุปกรณ์เชื่อมต่ออื่น ๆ ไม่ว่าจะเป็นขององค์กรหรือของส่วนตัวผู้ใช้เอง พร้อมใช้งานเพื่อสนับสนุนการดำเนินงานเชิงธุรกิจ ภายใต้นโยบายด้านความปลอดภัยขององค์กร โดยที่ไม่ส่งผลกระทบต่อการใช้งานส่วนตัว

นายพูลสุข วัฒนายิ่งเจริญชัย ผู้อำนวยการ บริษัท ดาต้าวัน เอเชีย (ประเทศไทย) จำกัด กล่าวว่า การร่วมมือทางธุรกิจระหว่างดาต้าวันฯและแบล็คเบอรี่ในครั้งนี้ เพราะแบล็คเบอรี่ได้มองเห็นศักยภาพของตลาดลูกค้าองค์กรในประเทศไทย จากนโยบายไทยแลนด์ 4.0 ที่ส่งเสริมและผลักดันให้ประเทศไทยก้าวเข้าสู่ระบบเศรษฐกิจดิจิทัล และร่วมกันเป็นพันธมิตรทางธุรกิจ เพื่อเปิดตลาดโซลูชั่นด้าน Mobility Enterprise สำหรับองค์กร เพื่อช่วยจัดการ

Architecture: BlackBerry UEM Solution



อุปกรณ์เชื่อมต่อที่หลากหลาย ที่มาพร้อมระบบความปลอดภัยในการดูแลรักษาข้อมูลด้วยเทคโนโลยีระดับโลก โดยลูกค้าเป้าหมายที่ทางดาต้าวัน ฯ จะเข้าไปเปิดตลาดจะเป็นลูกค้ากลุ่มธนาคาร ประกันภัย และภาครัฐ ซึ่งเป็นหน่วยงานที่ให้ความสำคัญกับข้อมูลในระดับสูง

สำหรับโซลูชัน UEM ของแบล็คเบอรี่ สามารถรองรับการบริหารจัดการอุปกรณ์พกพาบนแพล็ตฟอร์มที่หลากหลาย ได้แก่ Android, iOS, Windows 10, MacOS และ BlackBerry โดยผู้ใช้งานสามารถลงทะเบียนเพื่อเริ่มใช้งานด้วยตนเอง ผ่านการตั้งค่าอุปกรณ์เบื้องต้น เช่น E-mail , Wi-Fi และ VPN โดยอัตโนมัติ การควบคุมการติดตั้งและใช้แอปพลิเคชัน การป้องกันการ Jailbreak/Root ไปจนถึงการค้นหาตำแหน่งของอุปกรณ์และการล้างข้อมูลทิ้งเมื่ออุปกรณ์สูญหาย ที่สำคัญคือผู้ดูแลระบบสามารถเลือกวิธีบริหารจัดการจากศูนย์กลางแบบ On-premise หรือระบบคลาวด์ก็ได้ ซึ่งค่อนข้างยืดหยุ่นในการทำงานร่วมกับระบบที่แตกต่างกันในแต่ละองค์กร

"ในช่วงปีที่ผ่านมา หลังจากรัฐบาลประกาศเดินหน้าประเทศไทยด้วยนโยบายเศรษฐกิจไทยแลนด์ 4.0 ส่งผลให้ทั้งภาครัฐและเอกชนต่างวางแผนนำเทคโนโลยีและนวัตกรรมใหม่ ๆ เข้ามาสนับสนุนธุรกิจและสร้างมูลค่าให้แก่องค์กร ไม่ว่าจะเป็นการหันไปใช้ระบบคลาวด์ หรือการนำ IoT (Internet of Things) มาพัฒนาธุรกิจ และนำข้อมูลจำนวนมหาศาลที่ได้จากอุปกรณ์ ไอทีต่างๆ นำมาวิเคราะห์ (Big Data Analytics) และนำผลการวิเคราะห์ที่ได้มาสร้างฟีเจอร์ใหม่ ๆ ให้กับผลิตภัณฑ์และบริการขององค์กร ซึ่งแนวทางที่จะได้มาซึ่งข้อมูลที่เป็น Big Data นั้น สามารถนำมาออกแบบการทำงานให้เป็นแบบ Mobility เพื่อเพิ่มความยืดหยุ่น และความคล่องตัว ในการทำงานให้มากยิ่งขึ้น โดยหัวใจสำคัญของการพัฒนาศักยภาพเพื่อนำองค์กรสู่การแข่งขันในยุคนี้คือ เทคโนโลยีดิจิทัลและอินเทอร์เน็ต ส่งผลให้เรื่องของระบบการรักษาความปลอดภัย เป็นปัจจัยสำคัญที่องค์กรให้ความสำคัญสูงสุด" นายพูลสุข กล่าวทิ้งท้าย

ซินโนโลยีเปิดตัวโซลูชั่นจัดเก็บข้อมูลประสิทธิภาพสูง เตรียมธุรกิจ SME ให้พร้อมเพื่ออนาคตดิจิทัลของไทย

ซินโนโลยีเปิดตัวยูนิต NAS ตัวล่าสุดในชุดอุปกรณ์บริหารและจัดเก็บข้อมูลบนเครือข่ายประสิทธิภาพสูงสำหรับการใช้งานข้อมูลขนาดหนัก มุ่งหวังส่งมอบโซลูชั่นและเทคโนโลยีเสริมศักยภาพไอทีแก่ธุรกิจเอสเอ็มบีในไทยให้สามารถเตรียมพร้อมรับมือกับอนาคตดิจิทัลของประเทศไทยตามนโยบายไทยแลนด์ 4.0

วิค ชู ประธานกรรมการบริหาร บริษัท ซินโนโลยี อิงค์ ผู้ผลิตชั้นนำของโลกด้าน Network Attached Storage (NAS) กล่าวว่า จากประสบการณ์และความเชี่ยวชาญในอุตสาหกรรมกว่า 17 ปีด้วยยอดขายกว่า 4.7 ล้านเครื่องทั่วโลก ทำให้ซินโนโลยีก้าวขึ้นสู่การเป็นผู้นำด้านการผลิต NAS ที่ใหญ่ที่สุดในโลก ด้วยรายได้ในปี พ.ศ. 2558 สามารถเติบโตในอัตราเลขสองหลัก จากการที่ข้อมูลมีปริมาณเพิ่มขึ้นอย่างรวดเร็ว เทคโนโลยีการจัดเก็บข้อมูลจึงเป็นตัวแปรสำคัญในการปฏิวัติการเก็บข้อมูลแบบเดิม ดังนั้นเพื่อเตรียมพร้อมสำหรับอนาคตไอทียุคใหม่ ประกอบกับความต้องการที่เพิ่มขึ้นได้ผลักดันให้ธุรกิจโดยเฉพาะธุรกิจเอสเอ็มบีต่างมองหาโซลูชั่นที่มีประสิทธิภาพในราคาเหมาะสม ซินโนโลยีจึงได้ออกแบบผลิตภัณฑ์เพื่อตอบสนองความต้องการที่หลากหลายในยุคแห่งการเปลี่ยนแปลงนี้

"การที่รัฐบาลไทยได้ประกาศนโยบายเศรษฐกิจภายใต้ Thailand 4.0 เพื่อประกาศความมุ่งมั่นสำหรับการนำประเทศก้าวสู่ยุคใหม่ที่ ***"มั่นคง มั่งคั่ง ยั่งยืน"*** *โดยตั้งเป้าหมายให้ไทยเป็นประเทศที่สร้างสรรค์ มีความเป็นดิจิทัลซึ่งขับเคลื่อนด้วยนวัตกรรม ข้อมูลมีการเชื่อมโยงกับทุกด้านของการใช้ชีวิต ดังนั้นการบริโภคข้อมูลดิจิทัลจึงเพิ่มขึ้น ความต้องการพื้นที่สำหรับจัดเก็บข้อมูลจำเป็นต้องขยายความจุตามไปด้วย เชื่อว่ากลุ่มผลิตภัณฑ์ NAS ของเราสามารถครอบคลุมการทำงานด้านไอทีได้ในทุกมิติอย่างแท้จริง"* ซีอีโอจากซินโนโลยีกล่าว

ผลิตภัณฑ์ในกลุ่ม NAS ของซินโนโลยีประกอบด้วย

Networking เครือข่ายเพื่อเชื่อมโยงโครงสร้างพื้นฐาน ซินโนโลยีเพิ่งเปิดตัวเราเตอร์รุ่นใหม่ในไทย นั่นคือ RT2600ac เป็นเราเตอร์ความเร็วสูง มีจุดเด่นด้านความปลอดภัย รองรับการใช้งานในบ้านและสำนักงานทันสมัย RT2600ac เชื่อมต่อได้ทั้งมีสายและไร้สาย พร้อม UI ที่ใช้งานง่าย

Application แอพพลิเคชั่นเพื่อเพิ่มมูลค่า ซินโนโลยีได้พัฒนาแอพพลิเคชั่นสำหรับ DiskStation Manager ซึ่งเป็นระบบที่รันบนหน่วย NAS ของซินโนโลยีโดยเฉพาะ และเปิดตัวแพ็กเกจ Add-on 118 ชุดใน Package Center ตอบสนองความต้องการตั้งแต่ระดับบุคคลจนถึงภาคธุรกิจ นอกจากนี้ยังได้สร้างระบบนิเวศแอพพลิเคชั่นชั้นเยี่ยมในอุตสาหกรรม NAS กับการเปิดตัว DiskStation Manager (DSM) 6.1 พร้อมแพ็กเกจสมบูรณ์แบบ สร้างประสบการณ์การใช้งาน NAS ทั้งด้านความปลอดภัยและประสิทธิภาพการใช้งานสูงสุด

Storage การจัดเก็บข้อมูลคือหัวใจสำคัญ ซินโนโลยีได้เปิดตัวหน่วยเก็บข้อมูลรุ่นล่าสุดคือ DiskStation DS1517+ และ DS1817+ เซิร์ฟเวอร์แบบ 5-bay และ 8-bay tower ที่สามารถขยายขนาดได้ พร้อมด้วย Expansion Unit DX517 ซึ่งช่วยให้ธุรกิจทั้งขนาดกลางและเล็กในไทยเพิ่มกำลังการผลิต รวมถึงแก้ไขปัญหาการจัดเก็บข้อมูลได้ทันท่วงที NAS ทั้งสองรุ่นนี้สนับสนุน M.2 SSD และออกแบบมาเพื่อแก้ปัญหาความแออัดของการใช้ข้อมูลแอพพลิเคชั่นที่หนักหน่วง ลดความล่าช้าของระบบรับและแสดงผลได้อย่างชัดเจน

วิคเตอร์ หวัง ผู้จัดการฝ่ายขายในตลาดกลุ่มอาเซียน บริษัท ซินโนโลยี อิงค์ กล่าวว่าปัจจุบันนี้ธุรกิจไทยให้ความสำคัญกับการก้าวสู่ยุคดิจิทัล แล้วยังมีความตื่นตัวในการอัปเดตซอฟต์แวร์และโซลูชั่นต่างๆ ซึ่งซินโนโลยีมองเห็นโอกาสจากปัจจัยด้านจีดีพีของประเทศที่เพิ่มขึ้น รวมถึงโครงการต่างๆ จากทางภาครัฐและภาคเอกชนภายใต้นโยบายไทยแลนด์ 4.0 ส่งผลให้ประเทศไทยกลายเป็นแหล่งลงทุนที่น่าดึงดูดสำหรับนักลงทุนทั่วโลก

STOP CYBER ATTACK

บริษัทเน็ตมาร์ค (ประเทศไทย) จำกัด ร่วมกับบริษัทยักษ์ใหญ่อย่าง บริษัทซิสโก้ ซิสเต็มส์ (ประเทศไทย) จำกัด จัดงานสัมมนาภายใต้งานที่ชื่อว่า "STOP CYBER ATTACK" พร้อมอัพเดทเทคโนโลยีใหม่ๆ ที่น่าสนใจให้กับกลุ่มลูกค้า ที่มาในงาน ณ ห้องสัมนา Yangtze ชั้น30 โรงแรมMillennium Hilton Bangkok

โดยการจัดงานในครั้งนี้ เน็ตมาร์ค(ประเทศไทย) และ ซิสโก้ ซิสเต็มส์(ประเทศไทย)ได้เดินทางไปมอบความสุข ความสนุกสนานเป็นกันเอง และให้ความรู้ในเรื่องของ Cyber Defense Revolution โดยได้เชิญ ดร.ศุภกร กังพิสดาร มาเป็นผู้บรรยายในครั้งนี้ พร้อมทั้งอัพเดทเทคโนโลยีใหม่ๆ โดยตัวแทนจาก บริษัทซิสโก้ ซิสเต็มส์ ประเทศไทย

และทิ้งท้ายในช่วงค่ำ โดยจัดงานเลี้ยงรับรองอาหารค่ำ พร้อมการแสดง Music Live band ให้กับลูกค้าที่มาร่วมสัมนาในช่วงบ่าย เพื่อผ่อนคลายความเครียดจากงานสัมนา และหลังจากจบงาน ทางเน็ตมาร์คได้มอบของที่ระลึกให้กับลูกค้า เรียกได้ว่าเป็นงานที่สร้างรอยยิ้มและความอบอุ่นแบบเป็นกันเอง

ไฟเบอร์วันตั้งเป้าผู้ใช้งาน 1 ล้านยูนิตภายในปีนี้ เผยแผนรุกตลาด CLMV รองรับเศรษฐกิจดิจิทัล

ไฟเบอร์วันเผยทิศทางการดำเนินงาน ตั้งเป้าหมายฐานผู้ใช้งานทั้งส่วนอินเทอร์เน็ตบรอดแบนด์และบริการดิจิทัลคอนเทนต์ 1 ล้านยูนิต พร้อมสยายปีกรุกวางโครงข่ายไฟเบอร์ออปติกใน 4 หัวเมืองใหญ่ของไทย เตรียมแผนเปิดตลาดในกลุ่มประเทศ CLMV (เวียดนาม-พม่า-กัมพูชา-ลาว) อีกด้วย

กิตติ โกสินสกุล ประธานเจ้าหน้าที่บริหาร บริษัท ไฟเบอร์วัน จำกัด (มหาชน) ผู้ให้บริการวางโครงข่ายไฟเบอร์ออปติก กล่าวว่า จากข้อมูลจำนวนผู้ใช้อินเทอร์เน็ตในประเทศไทยเมื่อสิ้นปี 2559 ที่ผ่านมามีผู้ใช้งาน 38 ล้านคน ขณะที่ฐานลูกค้าของไฟเบอร์วันในปัจจุบันได้ติดตั้งและใช้งานแล้วประมาณ 80,000 ยูนิต นั่นหมายความว่าไฟเบอร์วันมีโอกาสเติบโตสูงมาก ปีนี้ไฟเบอร์วันตั้งเป้าหมายไว้ที่ 1 ล้านยูนิตด้วยบิสิเนสโมเดล Sharing and Caring แบ่งปันและใส่ใจ ซึ่งเป็นบิสิเนสโมเดลที่แตกต่างจากผู้ให้บริการรายอื่นในตลาด เพราะไฟเบอร์วันเป็นผู้ให้บริการวางโครงข่ายไฟเบอร์ออปติกโดยไม่คิดค่าใช้จ่าย แต่ใช้วิธีแบ่งรายได้กับผู้ให้บริการอินเทอร์เน็ตหรือผู้ให้บริการดิจิทัลคอนเทนต์ ซึ่งทุกฝ่ายได้ประโยชน์ โดยเฉพาะผู้ใช้งานปลายทางไม่ต้องเสียค่าติดตั้งเดินสายไฟเบอร์ออปติที่ปัจจุบันยังมีราคาค่อนข้างสูง

ทั้งนี้ ไฟเบอร์วันได้ขยายฐานลูกค้าโครงข่ายไฟเบอร์ออปติกไปยังหัวเมืองใหญ่แล้ว 4 จังหวัด ประกอบด้วย เชียงใหม่ ภูเก็ต อุบลราชธานี และอุดรธานี ซึ่งเป็นจังหวัดที่มีความเจริญทางเศรษฐกิจมีความต้องการโครงข่ายไฟเบอร์ออปติก โดยร่วมมือกับกลุ่มพัฒนาอสังหาริมทรัพย์รายต่างๆ รวมถึงมีแผนขยายไปยังประเทศเพื่อนบ้าน CLMV นั่นคือ เวียดนาม พม่า เขมร และลาว

ในเชิงแนวโน้มเทคโนโลยีโครงข่ายไฟเบอร์ออปติกหรือโครงข่ายใยแก้วนำแสงจะเข้ามาแทนที่สายทองแดงที่ใช้กันอยู่อย่างแน่นอน จากข้อดีหลายอย่าง เช่น ให้ความเร็วสูงสุดถึง 100 กิกะบิตต่อวินาที สามารถรองรับบริการดิจิทัลแอพพลิเคชั่นหรือดิจิทัลเซอร์วิสในปัจจุบันและในอนาคตได้อย่างไม่มีขีดจำกัด โครงข่ายมีเสถียรภาพมีประสิทธิภาพการส่งสัญญาณดีกว่า แล้วโครงข่ายยังมีอายุการใช้งานยาวนาน 30-50 ปี

"ในยุคของอินเทอร์เน็ตออฟธิงส์ซึ่งดีไวซ์ต่างๆ สามารถเชื่อมต่อเข้าอินเทอร์เน็ตได้ จะทำให้เกิดดิจิทัลเซอร์วิสรูปแบบใหม่ๆ ตามมา เช่น สมาร์ทโฮมที่เราสามารถดูกล้องวงจรปิดภายในบ้านผ่านอุปกรณ์มือถือเพื่อดูความเรียบร้อยภายในบ้าน สมาร์ทเฮลธ์แคร์ที่คุณหมอสามารถอ่านผลเอ็กซเรย์คนไข้ผ่านเครือข่ายอินเทอร์เน็ตภายในโรงพยาบาลแม้จะอยู่คนละจังหวัด สมาร์ทซิตี้ที่หน่วยงานให้บริการสาธารณูปโภค เช่น ไฟฟ้าหรือประปาจะติดตั้งสมาร์ทมิเตอร์ สามารถส่งค่าตัวเลขใช้ไฟหรือใช้น้ำกลับมายังศูนย์กลาง ในอนาคตเราจะไม่ต้องมีคนเดินจดเลขมิเตอร์อีกต่อไป ดิจิทัลเซอร์วิสเหล่านี้ล้วนต้องอาศัยโครงข่ายไฟเบอร์ออปติกความเร็วสูงทั้งสิ้น" กิตติกล่าว

สมมาศเสถียร เลิศวัฒนกูล ประธานเจ้าหน้าที่บริหารฝ่ายการตลาด บริษัท ไฟเบอร์วัน จำกัด (มหาชน) กล่าวว่าจากช่วง 3 ปีที่ผ่านมาทางไฟเบอร์วันได้ติดตั้งโครงข่ายในกรุงเทพฯ และปริมณฑล ได้ขยายฐานลูกค้าสู่หัวเมืองใหญ่ 4 จังหวัด ซึ่งเป็นลูกค้ากลุ่มอสังหาริมทรัพย์ เช่น โครงการบ้านจัดสรรและคอนโด ในครึ่งปีแรกได้ร่วมมือกับเจริญเคเบิลทีวีในการให้บริการ FiberTV ส่วนช่วงครึ่งปีหลังไฟเบอร์วันจะร่วมมือกับพันธมิตรต่างๆ มากยิ่งขึ้น เช่น การร่วมมือกับโรงพยาบาลในการให้บริการ E-Medical การขยายการให้บริการกับลูกค้าองค์กรในนิคมอุตสาหกรรม อาคารสำนักงาน และส่วนงานภาครัฐ เป็นต้น รวมถึงการนำส่วนของระบบรักษาความปลอดภัย ซึ่งเป็นเรื่องที่มีความสำคัญมากในยุคดิจิทัลไซเบอร์ซิเคียวริตีเข้ามาเสริมบริการให้กับลูกค้าของไฟเบอร์วันในทุกกลุ่มธุรกิจ

"เพื่อเป็นการสร้างการรับรู้เรื่องแบรนด์ของไฟเบอร์วันที่เพิ่งเข้ามาทำตลาดได้เพียง 3 ปี ทางไฟเบอร์วันจึงเตรียมออกแคมเปญโรคเน็ตเนียยตอบรับยุคของดิจิทัลที่พฤติกรรมผู้บริโภคเปลี่ยนไป การดาวน์โหลดไฟล์ขนาดใหญ่ในยุคดิจิทัล ความเร็วในการดาวน์โหลดหรืออัปโหลดไฟล์ต่างๆ เป็นเรื่องสำคัญมาก แอพพลิเคชั่นต่างๆ ต้องการแบนด์วิดธ์ขนาดใหญ่ในการรับส่ง เช่น การส่งไฟล์กราฟิก งานพิมพ์ต่างๆ การเรียนการสอนผ่านระบบออนไลน์ ดูหนัง ฟังเพลง ไฟล์มัลติมีเดีย เกม หรือแม้แต่ผู้สูงอายุในปัจจุบันก็เป็นอีกกลุ่มที่ใช้งานดิจิทัล เช่น ดาวน์โหลดบทสวดมนต์ และอื่นๆ อีกมากมาย ผู้ใช้งานจำนวนมากต้องการโครงข่ายความเร็วสูง หากใครกำลังรู้สึกหงุดหงิดกับการใช้งานอินเทอร์เน็ต แคมเปญนี้น่าจะโดนใจผู้บริโภคได้มากทีเดียว" สมมาศเสถียรเสริม

ทางไฟเบอร์วันได้ขึ้นบิลบอร์ดแคมเปญโรคเน็ตเนียยแล้วตั้งแต่วันที่ 25 พฤษภาคมที่ผ่านมาบริเวณทางด่วน 6 จุดสำคัญ คือทางด่วนคลองเตย มอเตอร์เวย์ อนุสาวรีย์ชัยสมรภูมิ พระราม 9 หลักสี่ และสาทร รวมถึงการทำออนไลน์มาร์เก็ตติงในรูปแบบต่างๆ ปัจจุบันไฟเบอร์วันมีทีมงานคอลล์เซ็นเตอร์ในการรับแจ้งปัญหาหรือขอใช้บริการที่หมายเลข 1262 และมีทีมงานวิศวกรติดตั้งโครงข่ายไฟเบอร์ออปติกมากกว่า 130 ทีมคอยให้บริการได้ทั่วประเทศ

อรูบ้าเปิดตัวโซลูชั่นติดตามทรัพย์สินตัวแรกที่ผสานรวมเป็นหนึ่งเดียวกันกับระบบเครือข่ายไร้สายได้อย่างสมบูรณ์

Aruba Tag ใช้เทคโนโลยี BLE แบบใหม่, Aruba Access Point และ Meridian Software จะช่วยขจัดการสูญหายของทรัพย์สินที่มีมูลค่า และทำให้สามารถบริหารจัดการคลังสินค้าได้แบบอัตโนมัติ ; ระบบนิเวศทางเทคโนโลยีที่เติบโตจะช่วยให้สามารถนำเทคโนโลยีนี้ไปปรับใช้ในอุตสาหกรรมที่หลากหลายมากขึ้นได้

ในวันนี้ อรูบ้า หนึ่งในบริษัทของ Hewlett Packard Enterprise ได้ออกมาประกาศถึงผลิตภัณฑ์ใหม่ที่เพิ่มเติมเข้ามาในกลุ่มผลิตภัณฑ์ทางด้านบริการอ้างอิงสถานที่ (location-based services) ซึ่งจะช่วยให้องค์กรสามารถติดตามทรัพย์สินที่มีมูลค่าได้ง่ายขึ้น ส่งผลให้ประสิทธิภาพของการทำงานภายในองค์กรสูงขึ้น และสามารถลดทั้งค่าใช้จ่ายในการลงทุนและการดำเนินงานที่เกิดจากการที่อุปกรณ์ต่างๆ สูญหายหรือไม่อยู่ในสถานที่ที่ถูกจัดเก็บเอาไว้เป็นประจำได้ โซลูชั่นการติดตามทรัพย์สินของอรูบ้านี้ได้ถูกผสานรวมเป็นหนึ่งเดียวกับโครงสร้างพื้นฐานทางด้านระบบเครือข่ายไร้สายของอรูบ้าอย่างสมบูรณ์ทำให้สามารถติดตั้งใช้งานร่วมกันได้อย่างง่ายดาย และใช้งานได้เต็มประสิทธิภาพ อีกทั้งยังมีค่าใช้จ่ายที่ลดต่ำลงกว่าเดิมเป็นอย่างมาก

ระบบติดตามทรัพย์สินของอรูบ้าช่วยแก้ปัญหาเหล่านี้ได้ด้วยโซลูชั่นที่ผนวกรวมเข้าไปเป็นส่วนหนึ่งของโครงสร้างพื้นฐานใน Aruba Wi-Fi และทำให้ไม่ต้องมีการแยกส่วนของระบบเครือข่ายอีกต่อไป องค์กรต่างๆ สามารถได้รับประโยชน์จากความสามารถในการติดตามทรัพย์สินสำคัญทั้งหมดได้อย่างแม่นยำด้วยการใช้งานผ่านทางแอพพลิเคชั่นบนโทรศัพท์มือถือที่ใช้งานได้ง่ายดายและแสดงผลในรูปแบบของแผนที่ หรือจะผสานรวมระบบติดตามทรัพย์สินนี้เข้ากับโซลูชั่นการติดตามทรัพย์สินอื่น ๆ ที่องค์กรใช้งานอยู่เดิมได้ ภายในโซลูชั่นมีส่วนประกอบดังต่อไปนี้:

- **การก้าวไปเป็นส่วนหนึ่งของ ArubaOS และ Aruba APs :** ซอฟต์แวร์ตัวใหม่นี้ทำให้ Aruba Access Point รุ่นที่รองรับ BLE และ Aruba Sensor สามารถทำหน้าที่เป็น "อุปกรณ์ตรวจสอบ" แท็กติดตามทรัพย์สินได้ ทำให้สร้างระบบเครือข่ายของเซ็นเซอร์ที่ช่วยเสริมคุณค่าให้กับองค์กรที่ใช้งานระบบเครือข่ายไร้สายจากอรูบ้าอยู่แล้ว โดยสรุปแล้ว ซอฟต์แวร์นี้จะทำให้ระบบ Wi-Fi ที่ใช้งานอยู่คุ้มค่าขึ้นเป็นสองเท่า ด้วยการทำหน้าที่เป็นเครือข่ายสำหรับติดตามทรัพย์สินได้ด้วยในตัว
- **Aruba Tag รุ่นใหม่** : แท็กที่ใช้เป็นเทคโนโลยี Bluetooth Low Energy (BLE) ซึ่งมีราคาถูกคุ้มค่าและมีขนาดที่ใหญ่กว่า ¼ นิ้วเพียงเล็กน้อย ทำให้เหมาะที่จะนำไปใช้ติดตั้งในอุปกรณ์หลากหลายขนาด ตั้งแต่เครื่องควบคุมการให้สารละลายทางหลอดเลือดในวงการสาธารณสุข ไปจนถึงสินค้าที่บรรจุในพาเลทภายในคลังสินค้า แท็กเหล่านี้ถูกออกแบบมาให้ใช้งานได้ภายในสภาวะแวดล้อมการทำงานที่หลากหลาย และยังมาพร้อมกับทางเลือกในการติดแท็กเข้ากับวัตถุต่างๆ ได้อย่างยืดหยุ่น
- **แอพพลิเคชั่นสำหรับกำหนดค่าให้กับแท็กติดตามสินค้า:** แอพพลิเคชั่นสำหรับกำหนดค่าของอรูบ้าจะช่วยให้การติดตั้งเริ่มต้นและการบริหารจัดการแท็กนั้นเป็นไปได้อย่างง่ายดาย สินทรัพย์ต่างๆ จะสามารถถูกระบุได้ด้วยชื่อ, ภาพถ่าย และหมายเลข ID เพื่อให้ง่ายต่อการค้นหา การเปลี่ยนแปลงข้อมูลใดๆ ก็สามารถทำได้อย่างรวดเร็วจากบริเวณที่ใกล้เคียงกับสินทรัพย์เหล่านั้น และข้อมูลทั้งหมดก็จะถูกบันทึกโดยอัตโนมัติไปยังระบบฐานข้อมูลกลางบนระบบคลาวด์
- **ความสามารถใหม่สำหรับ Aruba Meridian AppMaker :** องค์กรสามารถสร้างแอพพลิเคชั่นติดตามทรัพย์สินขึ้นมาใช้งานเองได้แล้วทั้งสำหรับ iOS หรือ Android ด้วย Meridian AppMaker โดย AppMaker นี้จะมี SDK และ API ใหม่สำหรับให้เชื่อมต่อกับระบบอื่น ๆ ภายนอกเพื่อรองรับการใช้งานในรูปแบบต่าง ๆ ได้

พันธมิตรในระบบนิเวศทำให้สามารถนำไปประยุกต์ใช้ได้ในหลายอุตสาหกรรม

กุญแจสำคัญสู่ความสำเร็จของบริการอ้างอิงสถานที่ของอรูบาและผลิตภัณฑ์กลุ่ม Mobile Engagement คือโครงการ Meridian Engage Partner Program โดยลูกค้าสามารถได้ประโยชน์จากการที่อรูบ้าเปิดให้นักพัฒนาแอพพลิเคชั่นเข้ามาทำงานผสานระบบและสร้างแอพพลิเคชั่นบนมือถือเพื่อเพิ่มมูลค่าใหม่ๆ ให้กับแอพพลิเคชั่นที่ใช้งานอยู่ได้สำหรับทั้ง iOS และ Android ด้วย Meridian Mobile App Platform และผลิตภัณฑ์กลุ่ม Aruba Mobile Engagement อรูบ้านั้นกำลังทำการขยายโครงการนี้ไปยังเหล่าพันธมิตรที่มีอยู่ ซึ่งรวมถึง Emerge , Raizlabs , STANLEY Healthcare และ VenueNext เพื่อให้นำความสามารถในการติดตามทรัพย์สินไปใช้ อีกทั้งยังเปิดรับพันธมิตรรายใหม่ๆ เข้าร่วมในโครงการเพื่อให้ครอบคลุมอุตสาหกรรมต่าง ๆ ทั้งสาธารณสุข, ค้าปลีก, คลังสินค้า และอุตสาหกรรมอื่นๆ ด้วย

ด้วยการลงทุนอย่างต่อเนื่องในนวัตกรรม Intelligent Edge อรูบ้าได้เปิดตัว 8400 Core Swith ในงาน HPE Discover ด้วย โดย Core Switch รุ่น 8400 นี้จะเป็น Core Aggregation Switch รุ่นใหม่ที่มีทั้งประสิทธิภาพ, ความสามารถในการจ่ายพลังงาน, การทำงานได้แบบอัตโนมัติ และความสามารถในการแก้ไขปัญหาในหนึ่งเดียวที่จำเป็นต่อการจัดการกับความท้าทายทางด้าน Mobility, Cloud และ IoT ภายในระบบเครือขายทุกวันนี้ได้

HPE PointNext

Aruba Meridian Services จาก HPE Pointnext จะช่วยเสริมการให้บริการแก่ลูกค้าและพันธมิตรทั่วโลกในการนำบริการอ้างอิงสถานที่ไปใช้เพื่อเข้าถึงเหล่าผู้ใช้งานอุปกรณ์พกพาภายในองค์กรหรือสถานที่เปิดแบบสาธารณะ บริการเหล่านี้จะสามารถช่วยให้ฝ่าย IT ของลูกค้าและพันธมิตรของอรูบ้าสามารถทำการออกแบบและพัฒนาแอพพลิเคชั่นบนโทรศัพท์มือถือได้ด้วยแพล็ตฟอร์มของ Meridian

กลุ่มบริษัท อินเตอร์ลิ้งค์ฯ จัดงาน "INTERLINK THANK YOU PARTY 2017" สุดอลังการ

บริษัท อินเตอร์ลิ้งค์ คอมมิวนิเคชั่น จำกัด (มหาชน) ผู้นำเข้าและจัดจำหน่ายสายสัญญาณที่ใหญ่ที่สุดในอาเซียน จัดงาน **"INTERLINK THANK YOU PARTY 2017"** เพื่อขอบคุณลูกค้าและสื่อมวลชนที่ให้การสนับสนุนการดำเนินกิจการของบริษัทด้วยดีเสมอมา โดยในงานเต็มไปด้วยความสนุกสนานและอลังการภายใต้คอนเซ็ปต์ Under Water World

สมบัติ อนันตรัมพร ประธานกรรมการ บริษัท อินเตอร์ลิ้งค์ คอมมิวนิเคชั่น จำกัด (มหาชน) กล่าวขอบคุณผู้มีอุปการคุณที่มาร่วมงาน พร้อมทั้งเปิดเผยว่าอินเตอร์ลิ้งค์เป็นบริษัทแรกที่ได้นำเทคโนโลยีสาย LAN เข้ามาเผยแพร่ในไทย ด้วยความมุ่งมั่นตั้งแต่ก่อตั้งบริษัทที่ต้องการนำเทคโนโลยีมาพัฒนาประเทศ กว่า 30 ปี ที่ผ่านมาบริษัทได้เติบโตอย่างต่อเนื่องจวบจนถึงปัจจุบัน กลุ่มบริษัท อินเตอร์ลิ้งค์ฯ มีบริษัทในเครือถึง 5 บริษัท ได้แก่ บริษัท อินเตอร์ลิ้งค์ คอมมิวนิเคชั่น จำกัด (มหาชน) บริษัท อินเตอร์ลิ้งค์ เทเลคอม จำกัด บริษัท อินเตอร์ลิ้งค์ พาวเวอร์ แอนด์ เอนเนอยี่ จำกัด บริษัท อินเตอร์ลิ้งค์ ดาต้าเซ็นเตอร์ จำกัด บริษัท อินเตอร์ลิ้งค์ โฮลดิ้ง จำกัด ซึ่งสิ่งเหล่านี้จะเกิดขึ้นไม่ได้หากขาดผู้มีอุปการคุณทุกท่านที่ให้การสนับสนุนตลอด 30 ปีที่ผ่านมา ดังนั้นการจัดงานในวันนี้จึงเป็นความตั้งใจอย่างที่สุดของชาวอินเตอร์ลิ้งค์ฯ ที่จะมอบสิ่งดีๆ และความสุขสุดพิเศษให้สมกับที่ทุกท่านให้ความอุปการคุณมาโดยตลอด

INTERLINK NUMBER 1 ฉลอง 30 ปี คอนเสิร์ต 30 ศิลปิน นับเป็นงานยิ่งใหญ่ที่บริษัทฯ ดึงศิลปินระดับแนวหน้ากว่า 30 ชีวิต มาสร้างความสนุกสนานแก่แขกที่เข้าร่วมงานกว่า 2,000 คนในมินิคอนเสิร์ตครั้งนี้ **อาทิ เอ๊ะ จิรากร, สุชาติ ชวางกูร, ปั่น ไพบูลย์เกียรติ เชียวแก้ว, ไก่ อัญชุลีอร และศิลปินจากค่าย The Voice, The Star, AF Academy** ฯลฯ พร้อมรับประทานอาหารดินเนอร์สุดพิเศษ นอกจากนี้ยังมีโชว์หน้างานสุดตระการตา พร้อมกิจกรรมต่างๆ ภายในงานมากมาย สร้างความประทับใจแก่แขกผู้เข้าร่วมงานกันถ้วนหน้า ณ ห้องรอยัล จูบิลี่ ชาเลนเจอร์ ฮอลล์ อิมแพค เมืองทองธานี เมื่อเร็วๆ นี้

(ในภาพ) **สมบัติ อนันตรัมพร** (ยืนกลาง) ประธานกรรมการและกรรมการผู้จัดการใหญ่ กลุ่มบริษัท อินเตอร์ลิ้งค์ฯ จัดงาน เลี้ยงขอบคุณลูกค้าในโอกาสครบรอบ 30 ปี โดยมี**ปกรณ์ มาลากุล ณ อยุธยา, ชลิดา อนันตรัมพร, กชพรรณ นุ่มฤทธิ์, นันทา ทรัพย์นิรันดร์, อรทัยรัชต์ ภูมิวงศ์พิทักษ์** และ**ณัฐนัย อนันตรัมพร** ร่วมแสดงความยินดี

(ซ้ายไปขวา) กชพรรณ นุ่มฤทธิ์, นันทา ทรัพย์นิรันดร์, ชลิดา อนันตรัมพร, สมบัติ อนันตรัมพร, ปกรณ์ มาลากุล ณ อยุธยา, อรทัยรัชต์ ภูมิวงศ์พิทักษ์, ณัฐนัย อนันตรัมพร








เทราดาต้ามุ่งย้ำนำเสนอ Teradata Customer Journey โซลูชั่นที่นำความสำเร็จในการผลิกโฉมธุรกิจสู่ยุคดิจิทัล

เทราดาต้าประกาศเปิดตัวโซลูชั่น Teradata Customer Journey เวอร์ชั่นใหม่ที่เปี่ยมด้วยประสิทธิภาพเพื่อช่วยให้บริษัทต่างๆ ในไทยผลิกโฉมธุรกิจไปสู่ดิจิทัล ช่วยให้ธุรกิจต่างๆ สามารถมองเห็นเส้นทางด้วยประสบการณ์ของลูกค้าเองที่ปรับแต่งได้ตามความต้องการเฉพาะบุคคล สามารถจำลองผลกระทบของแคมเปญใหม่ล่วงหน้า และดึงดูดลูกค้าด้วยคอนเทนต์ที่ตรงใจ

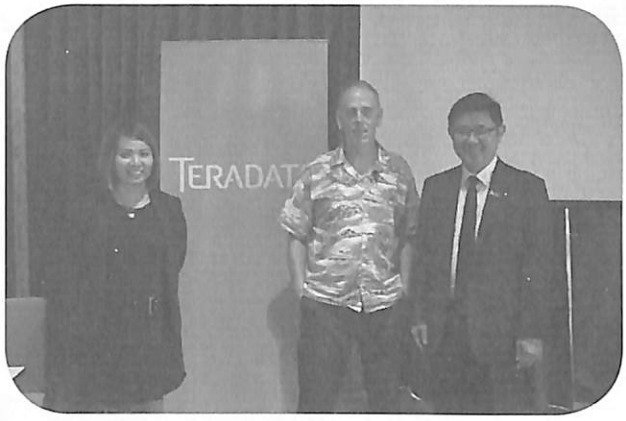
สตีเฟน บร็อบส์ท ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี บริษัท เทราดาต้า คอร์ปอเรชั่น ซึ่งเป็นหนึ่งในผู้นำระดับโลกด้านโซลูชั่นการวิเคราะห์ข้อมูล กล่าวว่าโซลูชั่นใหม่ล่าสุดนี้จะช่วยให้นักการตลาดสามารถวิเคราะห์ จำลองข้อมูลแบบไดนามิก เรียนรู้ด้วยตนเองได้ง่ายจากระบบ และสามารถจำลองข้อมูลแบบการทำนายล่วงหน้าได้ง่ายขึ้น นอกจากนี้ด้วยความเชี่ยวชาญด้านการรวบรวมข้อมูล การวิเคราะห์ขั้นสูง และการจัดการปฏิสัมพันธ์หลายช่องทางของ Teradata Customer Journey เวอร์ชั่นใหม่นี้ยังช่วยเพิ่มความสามารถให้นักการตลาดดูแลลูกค้าทุกรายได้แบบเฉพาะบุคคล เพิ่มอัตราการตอบสนอง ลดความยุ่งยาก และสร้างความพึงพอใจแก่ลูกค้าได้ดียิ่งขึ้น

ผลการศึกษาจากการ์ตเนอร์ชี้ให้เห็นว่าภายในปี 2561 บริษัทต่างๆ ที่ลงทุนเต็มที่ในการให้บริการออนไลน์เฉพาะบุคคลจะสามารถทำยอดขายได้มากกว่าบริษัทที่ไม่ลงทุนประมาณกว่า30%

"หลายบริษัทมักพบว่าเป็นเรื่องยากที่จะทำความเข้าใจและใช้ประโยชน์จากพฤติกรรมลูกค้าบนเส้นทางธุรกรรมหลายพันล้านครั้งของลูกค้าหลายล้านคน นอกจากนี้ลูกค้าต่างใช้งานหลากหลายอุปกรณ์และช่องทางในการสร้างปฏิสัมพันธ์ แต่ส่วนใหญ่ก็ยังคาดหวังว่าจะได้รับประสบการณ์เฉพาะบุคคลในทุกช่องทาง ซึ่งเทราดาต้าเชื่อว่า Teradata Customer Journey จะตอบโจทย์ได้ลงตัวและคุ้มค่าอย่างที่สุด" ซีทีโอแห่งเทราดาต้ากล่าวอย่างมั่นใจ

จีรภา คงสว่างวงศา กรรมการผู้จัดการประจำประเทศไทยของเทราดาต้า กล่าวว่าในขณะที่ประเทศไทยมุ่งสู่เศรษฐกิจดิจิทัลด้วยวิสัยทัศน์การพัฒนาเศรษฐกิจประเทศไทย4.0 ของรัฐบาลไทยในปัจจุบัน ทางบริษัทหวังให้ธุรกิจไทยเติบโตขึ้นด้วยการมอบคุณค่าแก่ผู้บริโภคมากยิ่งขึ้น โซลูชั่น Teradata Customer Journey จะช่วยเพิ่มความสามารถในการวิเคราะห์ข้อมูลให้นักการตลาดเพื่อสร้างความเข้าใจพฤติกรรมหรือประสบการณ์ของลูกค้าได้อย่างลึกซึ้งมากขึ้น รวมทั้งปรับใช้งานแบบเชิงรุกได้อย่างรวดเร็ว

โซลูชั่น Teradata Customer Journey ไม่เพียงช่วยให้บริษัทเข้าใจและเพิ่มประสิทธิภาพประสบการณ์ของลูกค้าแต่ละรายได้ตลอดเวลา แต่ยังรองรับทุกช่องทางและทุกอุปกรณ์ได้แบบเรียลไทม์ รวมทั้งยังช่วยนักการตลาดเข้าถึงข้อมูลเชิงลึกเพื่อการวิเคราะห์ที่เหมาะสม สามารถใช้ระบบอัตโนมัติที่ฝังในโซลูชั่นเป็นตัวช่วยให้นักการตลาดดำเนินแคมเปญผ่านหลายช่องทางแบบเจาะจงลูกค้าได้พร้อมกันหลายพันรายการโดยไม่ต้องเพิ่มกำลังคนหรือทีมงาน



"โซลูชั่นของเรารวบรวมเทคโนโลยีที่จำเป็นทั้งหมดผนวกกับความเชี่ยวชาญด้านการให้คำปรึกษาเพื่อให้บรรลุเป้าหมายด้านทำการตลาดได้รวดเร็วยิ่งขึ้น ช่วยให้องค์กรมีศูนย์ข้อมูลเส้นทางของลูกค้าที่สมบูรณ์โดยไม่ต้องคำนึงถึงความท้าทายจากการใช้งานโซลูชั่นร่วมกับผู้ขายหลากหลายราย นอกเหนือจากเทคโนโลยีชั้นนำของอุตสาหกรรม เรายังให้บริการด้าน Consulting Resources เพื่อต้องการให้บริษัทต่างๆ ตระหนักถึงความสามารถเหล่านี้ได้อย่างรวดเร็วในค่าใช้จ่ายที่เหมาะสม และได้รับมูลค่าทางธุรกิจที่สูงขึ้น ยิ่งไปกว่านั้นการเติบโตอย่างต่อเนื่องของไทยในช่วงหลายปีที่ผ่านมานับเป็นหลักฐานแห่งความสำเร็จและความเชี่ยวชาญที่ได้รับการยอมรับในด้านการวิเคราะห์ข้อมูลขนาดใหญ่ของลูกค้าหลักของเรา อาทิ บริษัท ปตท. จำกัด (มหาชน)" จีรภากล่าวเสริม

ดร.บุรณิน รัตนสมบัติ ผู้ช่วยกรรมการผู้จัดการใหญ่ธุรกิจหล่อลื่น กลุ่มธุรกิจน้ำมัน บริษัท ปตท. จำกัด (มหาชน) ให้ความเห็นว่าระบบวิเคราะห์ข้อมูลเชิงลึกที่มีจำนวนมหาศาล (Big Data Analytics) คือเทคโนโลยีที่เป็นพลังสำคัญในการขับเคลื่อนบริษัท ปตท. ให้สามารถดูแลคนไทยอย่างทั่วถึงด้วยสินค้าและบริการที่ถูกใจ สามารถสนองความต้องการของผู้บริโภคได้ในเวลาอันรวดเร็ว เพิ่มขีดความสามารถในการแข่งขัน พร้อมนำแบรนด์ปตท. ให้สามารถเติบโตเป็นแบรนด์ที่อยู่คู่คนไทย ทำเพื่อคนไทย เป็นแบรนด์แห่งความภูมิใจของคนไทย

"ปตท. คำนึงถึงความสำเร็จของลูกค้าเป็นหลัก จึงได้ร่วมมือกับเทราดาต้าซึ่งเป็นผู้เชี่ยวชาญชั้นนำระดับโลกด้านการวิเคราะห์ข้อมูลเชิงลึกในการพัฒนาแผนระยะยาว เสริมสร้างความพร้อมทั้งในด้านฮาร์ดแวร์ ซอฟต์แวร์ และศักยภาพของบุคลากรตั้งแต่ปี 2558 คาดว่าจะเริ่มใช้งานอย่างเต็มประสิทธิภาพในปี 2562" ดร.บุรณินกล่าวปิดท้าย

โซลูชั่น Teradata Customer Journey ของเทราดาต้าให้บริการแล้วทั่วโลก คุณสมบัติใหม่ๆ พร้อมให้บริการตั้งแต่เดือนมิถุนายน 2560 เป็นต้นไป

SHOWCASE

Fluke 64 MAX
อินฟราเรดเทอร์โมมิเตอร์รุ่นสมบุกสมบัน

Fluke Corporation ผู้นำเทคโนโลยีเครื่องมือวัดและทดสอบชั้นนำ ขอแนะนำอินฟราเรดเทอร์โมมิเตอร์รุ่นใหม่ **Fluke 64 Max** ขนาดเล็กกะทัดรัด แม่นยำสูง ใช้งานง่าย พร้อมคุณสมบัติที่ทนทานต่อฝุ่น ละอองน้ำ และแรงกระแทก เหมาะสำหรับงานในสภาพแวดล้อมทารุณ สมบุกสมบันที่ช่างเทคนิคต้องเผชิญอยู่เป็นประจำ ทั้งงานด้านไฟฟ้า งานระบบปรับอากาศ HVAC งานซ่อมบำรุงภายในโรงงานอุตสาหกรรมที่ต้องการการวัดอุณหภูมิจุดเล็กเป็นพิเศษ

คุณสมบัติเด่นของ Fluke 64 Max

- **เหมาะสำหรับวัดในที่แคบพิเศษ** : ด้วยอัตราส่วนของระยะห่างต่อขนาดจุดวัดที่มากถึง 20:1 จึงเหมาะในการวัดจุดเล็กๆ ที่เทอร์โมมิเตอร์แบบอินฟราเรดไม่เคยทำได้มาก่อน (ไม่เหมาะสำหรับการวัดระยะไกลเกิน 2 เมตร)
- **ทนแรงกระแทก** : ทนทานจากการตกกระแทกจากความสูง 3 เมตรถึงพื้นไม้
- **ทนน้ำทนฝุ่น**: ทนทานต่อละอองน้ำ ฝุ่นละออง และความสกปรกต่างๆ ที่ระดับ IP54
- **ขนาดเล็ก ใช้งานง่าย** : เล็กพอที่จะห้อยกับเข็มขัดเครื่องมือได้อย่างสบาย หยิบมาวัดอุณหภูมิได้สะดวกด้วยคลิกเดียว หน้าจออ่านง่ายทุกมุมมอง พร้อมไฟฉายส่องในที่มืดในตัว
- **ใช้แบตเตอรี่ขนาด AA เพียงก้อนเดียว**: อยู่ได้นานถึง 30 ชั่วโมง (Alkaline)
- **มีเลเซอร์ชี้ตำแหน่งวัด** : บอกขนาดจุดวัดอย่างแม่นยำ

Fluke 64 Max เหมาะสำหรับการตรวจวัดอุณหภูมิวัตถุหมุนหรือวัตถุที่มีไฟฟ้าแรงสูงโดยไม่ต้องตัดการทำงานเพื่อหาจุดที่มีความร้อนแปลกๆ ที่เป็นสัญญาณบอกเหตุความผิดปกติของระบบไฟฟ้าและเครื่องจักรกลไฟฟ้าต่างๆ เนื่องจากเราสามารถตรวจวัดได้โดยไม่สัมผัสและห่างจากชิ้นส่วนกลไกที่หมุน หรือมีกระแสไฟฟ้าไหลอยู่

Fluke 64 Max มีค่า Distance-to-Spot Ratio ที่ 20:1 ช่วงวัดอุณหภูมิ -30°C ถึง +600°C ความแม่นยำ ± 1% หรือ 1 องศา สามารถปรับค่า Emissivity ได้ตั้งแต่ 0.1 จนถึง 1.0 ด้วย Step 0.01 แสดงค่า Min, Max, Avg และ Hi-lo Alarm และทำการบันทึกผลการวัดลงหน่วยความจำในเครื่องได้ 99 ค่าการวัด

สนใจสอบถามรายละเอียดเพิ่มเติมติดต่อ : คุณพลธร 08-1834-0034, คุณสิทธิโชค 084-710-7667

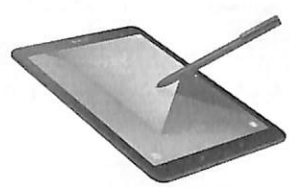
บริษัท เมเชอร์โทรนิกซ์ จำกัด

2425/2 ถนนลาดพร้าว ระหว่างซอย 67/2-69 แขวงสะพานสอง เขตวังทองหลาง กรุงเทพฯ 10310
โทรศัพท์ : 0 2514 1000, 0 2514 1234 โทรสาร : 0 2514 0001, 0 2514 0003
Website : www.measuretronix.com E-Mail : info@measuretronix.com

---

"ซัมซุง กาแลคซี่ แท็บ เอส3" แท็บเล็ตสุดล้ำ ตอบทุกโจทย์การทำงานและความบันเทิง

ซัมซุงแนะนำสมาร์ทแท็บเล็ตรุ่นใหม่ **"ซัมซุง กาแลคซี่ แท็บ เอส3 (Samsung Galaxy Tab S3)"** สมาร์ทแท็บเล็ตรุ่นล่าสุดที่ผู้ใช้รอคอย มาพร้อมกับ S Pen ดีไซน์ใหม่ จับถนัดเหมือนปากกาจริง ใช้งานง่ายด้วยหัวที่เล็กลง ทำให้สามารถเขียนได้อย่างแม่นยำ ตอบโจทย์ในทุกๆ ไลฟ์สไตล์การทำงานยุคดิจิทัลด้วยการทำงานแบบหลายหน้าจอ รองรับความบันเทิงทุกรูปแบบด้วยหน้าจอสีสันสวยสดขนาด 9.7 นิ้ว มองเห็นชัดทุกรายละเอียดผ่านสีเหมือนจริง เป็นแท็บเล็ตตัวแรกที่รองรับไฟล์ HDR ภายใต้ระบบเสียงทรงพลังจัดเต็มด้วยลำโพง 4 ตัว ปรับแต่งเสียงโดย AKG บริษัทอุปกรณ์เครื่องเสียงชั้นนำ



ซัมซุง กาแลคซี่ แท็บ เอส3 พกพาสะดวกด้วยตัวเครื่องที่บางเพียง 6 มิลลิเมตร รองรับระบบสัญญาณ 4G LTE ทำให้สามารถอัปโหลดและแชร์ได้อย่างง่ายดาย ระบบปฏิบัติการแอนดรอยด์ 7.0 Nougat โดดเด่นด้วยกล้องหลังความละเอียด 13 ล้านพิกเซล กล้องหน้าความละเอียด 5 ล้านพิกเซล หน่วยประมวลผล Snapdragon 820 Quad-Core (2.15 GHz + 1.6 GHz) หน่วยความจำภายใน 32 กิกะไบต์ สามารถเพิ่มหน่วยความจำ Micro SD ได้สูงสุดถึง 256 กิกะไบต์

ซัมซุง กาแลคซี่ แท็บ เอส3 สีดำ พร้อมเปิดให้เป็นเจ้าของแล้ววันนี้ในราคา 24,500 บาท สอบถามข้อมูลเพิ่มเติมได้ที่ศูนย์บริการลูกค้าซัมซุง โทรศัพท์ 0 2689 3232 หรือติดต่อผ่านโทรศัพท์บ้าน (ฟรี) 1-800-9-3232

ขยายสาขาและรองรับ BYOD ให้ปลอดภัยด้วย VPN Firewall ระดับพรีเมี่ยมใหม่จากไซเซล

รวมการใช้งาน VPN เพื่อให้การสื่อสารในเครือข่ายส่วนตัวปลอดภัย เหมาะสำหรับองค์กรที่มีผู้ใช้งานมากกว่า 2,000 คนขึ้นไป

ไฟร์วอลล์ USG2200-VPN ใหม่จากไซเซล

หากองค์กรของท่านมีสำนักงานแห่งเดียว การสร้างความปลอดภัยเครือข่ายอาจทำได้โดยไม่ยากนัก แต่ในทุกวันนี้องค์กรมีการขยายสำนักงาน มีพนักงานใช้อุปกรณ์ของตนเชื่อมโยงเข้ามาใช้ทรัพยากรในเครือข่ายองค์กรของท่าน (Bring Your Own Device : BYOD) ซึ่งองค์กรมักสร้าง Virtual Private Network : VPN มารองรับเทรนด์ทางด้านนี้ เครือข่าย VPN เป็นเครือข่ายส่วนตัวเสมือนที่มีเส้นทางทำงานอยู่ในเครือข่ายสาธารณะ ดังนั้นเรื่องความปลอดภัยของข้อมูลในเครือข่ายส่วนตัวจึงเป็นเรื่องที่ต้องคำนึงถึงเป็นอย่างมาก เครือข่าย VPN จะมีการส่งข้อมูลในรูปแบบแพ็กเก็ตผ่านเครือข่ายอินเทอร์เน็ต โดยมีการเข้ารหัสข้อมูลก่อนที่จะส่งข้อมูลเพื่อสร้างความปลอดภัยให้กับข้อมูล และส่งข้อมูลผ่าน Tunnel ที่สร้างขึ้นจากจุดต้นทางไปถึงปลายทาง จึงมีเพียงผู้รับปลายทางเท่านั้นที่สามารถถอดรหัสข้อมูลและนำข้อมูลไปใช้ได้

อีกทั้งในสถานการณ์ปัจจุบันที่มีภัยไซเบอร์นานาประเภทพยายามคุกคามเข้ามาในองค์กร ยิ่งจำเป็นต้องให้ความสำคัญเรื่องการสร้างความปลอดภัยให้กับข้อมูลในเครือข่ายของตนเอง ซึ่งคงปฏิเสธไม่ได้ว่าข้อมูลด้านธุรกิจนับเป็นข้อมูลที่มีค่ามาก ไซเซลจึงเปิดตัว **USG2200-VPN** ซึ่งเป็นไฟร์วอลล์ระดับพรีเมี่ยมใหม่ล่าสุดที่ให้คุณสมบัติโดดเด่นด้านการทำงาน VPN อันจะช่วยรวมและบริหารการใช้งาน VPN เพื่อให้การสื่อสารระหว่างสำนักงานและสาขามีความปลอดภัยสูงสุด

อุปกรณ์รุ่นใหม่นี้เหมาะสำหรับองค์กรที่มีผู้ใช้งานมากกว่า 2,000 คนขึ้นไป ซึ่งไฟร์วอลล์ USG2200-VPN ได้รับการออกแบบมาให้เหมาะกับการใช้งานในองค์กรขนาดกลางที่มีสำนักงานหรือสาขาหลายแห่ง สร้างขึ้นบนเทคโนโลยี VPN Concentrator อันมีศักยภาพในการจัดการการเชื่อมโยงของ VPN โดยเฉพาะ สามารถรองรับการส่งข้อมูลผ่าน Tunnel หลากหลายประเภท ครบถ้วนในการสื่อสารสมัยใหม่ ไม่ว่าจะเป็นระหว่างสาขา เชื่อมโยงกับสำนักงานคู่ค้า และการใช้ BYOD ในสำนักงาน รวมถึงการเชื่อมโยงจากพนักงานที่ทำงานนอกสถานที่อย่างปลอดภัยสูงได้ถึง 3,000 ช่อง

นอกจากนี้อุปกรณ์ยังใช้โปรโตคอล VPN ระดับสูงคือ IPSec/SSL/L2TP over IPSec จึงสามารถเชื่อมโยงกับอุปกรณ์ส่วนใหญ่ที่ใช้ในสำนักงานหรือในบ้านได้อย่างราบรื่น การสื่อสารทั้งขาเข้าและขาออกจะถูกเข้ารหัสด้วยอัลกอริทึมประเภท SHA-2 Encryption ที่แข็งแกร่งและใหม่ล่าสุด ภัยคุกคามจึงเข้ามาในเครือข่ายได้ยากขึ้น ข้อมูลด้านธุรกิจมีความปลอดภัยสูง

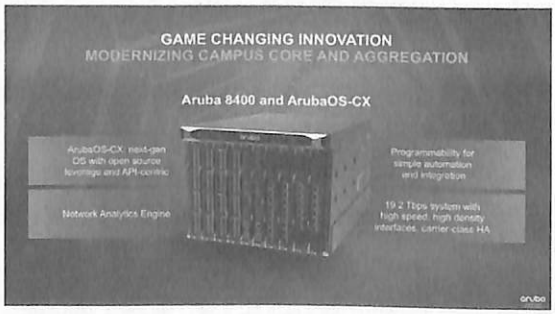
ในด้านการปฏิบัติการไซเซลได้พัฒนาซอฟต์แวร์สำหรับการบริหารจัดการเครือข่ายบนคลาวด์ (Cloud CNM SecuManager) เพื่อทำหน้าที่รวบรวมและจัดการความปลอดภัยให้เป็นหนึ่งเดียวกัน เอื้อให้องค์กรบริหารอุปกรณ์ด้านความปลอดภัยทุกชิ้นของไซเซลที่ติดตั้งอยู่ในสาขาต่างๆ ทั่วโลกผ่านหน้าจอเดียวกันได้อย่างง่ายๆ ช่วยลดเวลาในการดูแลเครือข่ายลงไปได้มาก

นอกจากนี้อุปกรณ์ออกแบบตามคอนเซ็ปต์ Multilayer High Availability Pro Design ที่มุ่งสร้างความต่อเนื่องในการใช้งานแบบ 24/7 ครอบคลุมทั้งด้านอุปกรณ์ฮาร์ดแวร์ การเชื่อมต่อ และบริการ VPN ซึ่งรวมถึงการทำงานที่ต่อเนื่องทันทีของ Hot-swappable Power & Fan Modules การทำงานของ Multi-WAN Load Balancing/Failover และการใช้งาน VPN High Availability ที่ต่อเนื่อง ทั้งหมดนี้เพื่อให้องค์กรสามารถมีแผนการทำงานสำรองอยู่เสมอ จึงยิ่งมั่นใจได้ว่าโอกาสที่บริการเกิดปัญหานั้นจะเท่ากับ 0 ท่านสามารถดูข้อมูลเพิ่มเติมได้ที่ www.zyxel.co.th

---

อรูบ้ากำหนดนิยามใหม่ระดับพื้นฐานให้ Core Switch เพื่อตอบโจทย์ความต้องการใช้โมบายล์, คลาวด์และ IoT

Aruba 8400 Core Switch รุ่นใหม่และระบบปฏิบัติการ ArubaOS-CX ได้นำความสามารถ Intelligent Edge มาสู่ศูนย์กลางของเครือข่ายด้วยความสามารถในการติดตามในระดับสูง การตรวจสอบข้อมูลเชิงลึกของเครือข่าย การแก้ไขปัญหาเครือข่ายโดยอัตโนมัติ และประสิทธิภาพในการทำงานระดับชั้นนำของอุตสาหกรรม



อรูบ้าหนึ่งในบริษัทของ Hewlett Packard Enterprise ได้ประกาศเปิดตัว **Aruba 8400 Core Switch Series** ซึ่งเป็น Core และ Aggregation Switch รุ่นใหม่พร้อมกับเปิดตัวระบบปฏิบัติการใหม่ที่ก้าวล้ำที่สุดในวงการ **ArubaOS-CX** ถูกออกแบบมาสำหรับรองรับความต้องการด้าน Mobility, คลาวด์และ IoT ในสมัยใหม่ ก้าวกระโดดจากแพลตฟอร์มระบบ Switching แบบเดิมๆ โดย Aruba 8400 Core Switch Series และ ArubaOS-CX สร้างขึ้นมารองรับแอพพลิเคชั่นเชิงธุรกิจในรูปแบบ Mobile-Cloud ที่กำลังเกิดขึ้นอย่างต่อเนื่องและ

การเปลี่ยนแปลงรูปแบบของการจราจรบนเครือข่ายที่ถูกขับเคลื่อนโดยแหล่งข้อมูลจำนวนมหาศาลจากการเติบโตของจำนวนอุปกรณ์ประเภท IoT

Aruba 8400 Switch Series ได้นำเสนอนวัตกรรมใหม่ภายในระบบเครือข่ายสำหรับผู้ใช้งานในส่วนของ Core และ Aggregation ด้วยการเพิ่มความชาญฉลาดให้ระบบเครือข่ายตั้งแต่ Edge ขึ้นมายัง Core ทำให้เหล่าซีไอโอสามารถสร้างผลลัพธ์เชิงธุรกิจที่ดียิ่งขึ้นได้จากระบบเครือข่ายเหล่านี้ ขณะที่ Aruba 8400 เองยังคงมีความทนทานและประสิทธิภาพเทียบเท่าอุปกรณ์ในระดับผู้ให้บริหารโครงข่ายที่บรรดาองค์กรต้องการ นวัตกรรมที่มาพร้อมกันนี้เองได้ก้าวล้ำไปสู่การตอบสนองความต้องการในการตรวจสอบได้ทันท่วงที มีความมั่นคงปลอดภัยในระดับสูงขึ้น ความสามารถในการวิเคราะห์ข้อมูลต่างๆ เพื่อแก้ไขปัญหาได้ดีขึ้น การทำงานแบบอัตโนมัติได้ง่ายขึ้น ทำให้องค์กรมีความเร็วในการทำงานได้อย่างแท้จริงในขณะที่มุ่งไปสู่การเป็นธุรกิจแบบ Mobile-first, Cloud และ IoT อีกทั้งยังช่วยประหยัดค่าใช้จ่ายลงไปอย่างมหาศาลอีกด้วย คุณประโยชน์เหล่านี้ยังสามารถต่อยอดเพิ่มขึ้นไปได้อีกด้วยการใช้ Aruba AirWave Network Management และ ClearPass Policy Manager โดยทั้งสองระบบนี้สามารถทำงานร่วมกับ Aruba 8400 ได้อย่างง่ายดาย

นำความชาญฉลาดมาสู่ศูนย์กลางของเครือข่าย : ArubaOS-CX

Aruba 8400 มีนวัตกรรมที่โดดเด่นเฉพาะตัว นั่นคือ ArubaOS-CX ซึ่งเป็นซอฟต์แวร์พื้นฐานทำหน้าที่เป็นมันสมองให้กับอุปกรณ์สวิตช์เพื่อให้งานด้านระบบเครือข่ายที่มีความสำคัญและความซับซ้อนกลายเป็นงานอัตโนมัติที่ง่ายดาย ประโยชน์หลักๆ ที่ได้รับจากระบบปฏิบัติการใหม่สำหรับฝ่ายไอทีมีดังนี้

- **ตรวจสอบเหตุการณ์ต่างๆ ได้รวดเร็วขึ้น** : Aruba Network Analytics Engine เต็มเปี่ยมด้วยนวัตกรรมที่ช่วยตรวจสอบระบบเครือข่าย ระบบแม่ข่าย แอพพลิเคชั่น และกิจกรรมเกี่ยวกับความมั่นคงปลอดภัยตามกฎที่ตั้งไว้ ทำให้ผู้ดูแลระบบตรวจพบปัญหาได้ทันที วิเคราะห์แนวโน้มเพื่อทำความเข้าใจได้อย่างรวดเร็ว ทำนายหรือหลีกเลี่ยงปัญหาที่อาจเกิดขึ้นกับการเพิ่มขยายระบบ ความมั่นคงปลอดภัย และคอขวดทางประสิทธิภาพ
- **แก้ปัญหาเร็วขึ้นด้วยการวิเคราะห์ข้อมูลเครือข่าย** : Aruba 8400 สามารถแก้ไขปัญหาต่างๆ ได้อย่างจากความสามารถในการพัฒนาโปรแกรมขึ้นมาใช้งานได้ ผสานนโยบายอัจฉริยะเข้ากับระบบตรวจสอบเครือข่ายและระบบจัดการประสิทธิภาพความมั่นคงปลอดภัยได้ในตัว
- **รองรับการเขียนโปรแกรม ทำให้ฝ่ายไอทีเพิ่มขยายระบบง่ายขึ้น** : Aruba 8400 รองรับการควบคุมด้วยโปรแกรมที่พัฒนาขึ้นมาจากการที่มีตัวแปลงภาษา Python และ REST-based APIs รองรับการเข้าถึงได้ทุกความสามารถ ทำให้การผสานระบบมีความยืดหยุ่นในระยะยาวในการทำงานร่วมกับระบบโครงสร้างพื้นฐานและแอพพลิเคชั่นที่มีอยู่

สร้างขึ้นมาให้รองรับการเพิ่มขยายและทำงานได้อย่างทนทานตั้งแต่เริ่มต้น

Aruba 8400 มีความเป็นเอกลักษณ์ เนื่องจากได้รับการออกแบบตั้งแต่ขั้นเริ่มต้นให้มีประสิทธิภาพสูง ทนทาน เพิ่มขยายเพื่อรองรับเครือข่ายสมัยใหม่ในปัจจุบันได้อย่างดี การออกแบบระบบ Fabric ที่เพิ่มขยายได้เต็มที่ของ Aruba 8400 ทำให้อัปเกรดระบบได้อย่างไร้รอยต่อ ส่งผลให้เพิ่มแบนด์วิดธ์ได้ตามต้องการ ความสามารถในการทำ Virtual Switching Framework (VSF) ร่วมกันระหว่าง Chassis 2 ชุดสามารถรองรับพอร์ตความเร็ว 10GbE ได้สูงสุดถึง 512 ช่อง 40GbE ได้สูงสุดถึง 128 ช่อง หรือ 100GbE ได้สูงสุดถึง 96 ช่อง

การเพิ่มความสามารถในหลายด้านที่ส่งผลดีต่อการทำธุรกิจ

ด้วยซอฟต์แวร์ ArubaOS-CX ที่เป็นเอกลักษณ์ของ Aruba 8400 ฝ่ายไอทีก็สามารถที่จะตรวจสอบ วิเคราะห์การเชื่อมต่อเครือข่ายและรูปแบบจราจรของข้อมูลได้เร็วยิ่งขึ้น แก้ไขปัญหาต่างๆ ได้ก่อนที่เครือข่ายจะต้องหยุดทำงาน ช่วยเพิ่มความรวดเร็วในการทำงาน สร้างผลลัพธ์ใหม่ๆ ให้เกิดขึ้นได้จากโครงสร้างพื้นฐานของเครือข่าย สาธิตให้องค์กรเห็นคุณค่าใหม่ๆ ที่เกิดขึ้น ส่งผลลัพธ์ต่อการทำธุรกิจที่ดีขึ้น อีกทั้งยังช่วยประหยัดค่าใช้จ่ายอย่างมหาศาล คุณประโยชน์เหล่านี้สามารถต่อยอดได้ด้วยการใช้ Aruba AirWave Network Management และ ClearPass Policy Manager โดยทั้งสองระบบนี้สามารถทำงานร่วมกับ Aruba 8400 ได้อย่างง่ายดาย

บราเดอร์แนะนำเครื่องพิมพ์ปลอกสายไฟและฉลากตอบโจทย์งานด้านวิศวกรรม อุตสาหกรรม และอิเล็กทรอนิกส์

บราเดอร์ คอมเมอร์เชี่ยล (ประเทศไทย) ขอแนะนำ**เครื่องพิมพ์ปลอกสายไฟและฉลาก (P-TOUCH TUBE) รุ่น PT-E850TKWLI** พิมพ์ปลอกท่อและฉลาก ทนทานด้วยเทปเคลือบลามิเนตหน้ากว้างสูงสุดถึง 36 มิลลิเมตร และเทปสำหรับท่อหดด้วยความเร็ว 60-80 มิลลิเมตรต่อวินาที มีรูปแบบฉลากที่ตอบโจทย์งานด้านวิศวกรรม อุตสาหกรรม และอิเล็กทรอนิกส์โดยไม่ต้องหยุดเครื่อง สามารถลดขั้นตอนการทำงาน ประหยัดเวลามากกว่า มาพร้อมกับแบตเตอรี่ในตัวนำไปใช้งานได้ในทุกที่โดยไม่ต้องง้อปลั๊กไฟ สามารถสั่งพิมพ์ฉลากได้ง่าย สะดวกด้วย 3 วิธีคือสั่งพิมพ์ฉลากด้วยคีย์บอร์ดบนเครื่องพิมพ์ เชื่อมต่อพอร์ตยูเอสบีกับคอมพิวเตอร์ และผ่านระบบไร้สาย รองรับการเชื่อมต่อผ่านเครือข่าย และสั่งพิมพ์ผ่านสมาร์ทโฟน

เครื่องพิมพ์รุ่นนี้มีวางจำหน่ายแล้วในราคา 28,990 บาท สัมผัสประสบการณ์ที่เหนือชั้นจากบราเดอร์ได้แล้ววันนี้ที่ร้านค้าตัวแทนจำหน่ายสินค้าบราเดอร์ทั่วประเทศ ผู้สนใจสามารถติดต่อสอบถามได้ที่ Brother Contact Center โทรศัพท์ 0 2665 7777 หรือ www.brother.co.th, www.facebook.com/BrotherCommercialThailand

G-TECHNOLOGY® ตอบรับความต้องการแอพพลิเคชั่นโซลูชั่นเวิร์กโฟลว์ สำหรับกลุ่มนักสร้างสรรค์มืออาชีพด้วยโซลูชั่นจัดเก็บข้อมูลประสิทธิภาพสูง

เวสเทิร์น ดิจิตอล คอร์ปอเรชั่น ผู้นำด้านเทคโนโลยีและโซลูชั่นการจัดเก็บข้อมูลระดับโลก ประกาศยกระดับประสิทธิภาพสินค้าในกลุ่ม **G-Technology®** ซึ่งเป็นสินค้าที่การันตีคุณภาพด้วยรางวัล และการเข้ามาของเทคโนโลยีเชื่อมต่ออุปกรณ์กับคอมพิวเตอร์อย่าง Thunderbolt™ 3 และพอร์ต USB-C™ โดยได้อัปเกรดด้านความเร็วและประสิทธิภาพการทำงานของโซลูชั่นการจัดเก็บข้อมูลในไดรฟ์กลุ่มนี้เพื่อตอบสนองความต้องการที่เพิ่มขึ้นของกลุ่มนักสร้างสรรค์ผลงานมืออาชีพที่กำลังจับภาพข้อมูลและการถ่ายโอนเนื้อหาข้อมูลความละเอียดสูงจำนวนมหาศาล

G-DRIVE® พร้อมเทคโนโลยี ThunderboltTM 3

G-DRIVE® มาพร้อมเทคโนโลยี Thunderbolt 3 (ขนาด 12 เทราไบต์ จำหน่ายในราคา 28,799 บาท และขนาด 10 เทราไบต์ ราคา 25,199 บาท ไม่รวมภาษีมูลค่าเพิ่ม) ออกแบบเพื่อกลุ่มนักสร้างสรรค์ผลงานมืออาชีพ โซลูชั่นการจัดเก็บข้อมูลประสิทธิภาพสูงที่มาพร้อมกับพอร์ต Thunderbolt 3 และ USB-C (ที่รองรับพอร์ต USB 3.1 เจเนอเรชั่น 1) ผู้ใช้สามารถทำการเชื่อมต่อกับอุปกรณ์ต่างๆ ได้ถึง 5 ตัว สามารถเชื่อมต่อกับไดรฟ์ได้หลายตัว สามารถย้ายวิดีโอแบบความละเอียดสูงและฟุตเทจแบบ 4K ผ่านการเชื่อมต่อหัวเดียวได้อย่างรวดเร็ว ด้วยความจุที่มีมากถึง 12 เทราไบต์ เวิร์กโหลดงานที่หนักและข้อมูลสำคัญของผู้ใช้สามารถวางใจได้ด้วยความน่าเชื่อถือที่มีอย่างยาวนานของ Ultrastar® แบรนด์ HGST ฮาร์ดดิสก์ระดับองค์กรที่ติดตั้งอยู่ข้างใน ด้วยระดับความเร็วในการอ่านและเขียนอยู่ที่ 7200 RPM

G-RAID® ที่มาพร้อมกับเทคโนโลยี Thunderbolt 3

G-RAID® ที่มาพร้อมกับเทคโนโลยี Thunderbolt 3 (ขนาด 24 เทราไบต์ จำหน่ายในราคา 71,999 บาท และขนาด 10 เทราไบต์ ราคา 25,199 บาท ไม่รวมภาษีมูลค่าเพิ่ม) ฮาร์ดดิสก์ 2 ลูกที่มีประสิทธิภาพสูงและสามารถถอดออกได้ ทำงานแบบ RAID 0 RAID 1 หรือระบบจัดเก็บข้อมูลแบบ JBOD ที่มาพร้อมกับพอร์ต Thunderbolt 3 พอร์ต USB 3.1 เจเนอเรชั่น 2 หัวต่อ HDMI® 2.0 ที่สามารถใช้เชื่อมต่อกับจอแสดงผลแบบ 4K แบบ 60 HDR และอุปกรณ์ตัดต่อช่วยให้นักสร้างสรรค์ผลงานมืออาชีพสามารถเข้าถึง เรียกดู แก้ไข และทำการสำรองคลังภาพดิจิทัลได้อย่างรวดเร็ว ด้วย Ultrastar® แบรนด์ HGST ความเร็วในการอ่าน 7200 RPM ฮาร์ดดิสก์ระดับองค์กรที่สามารถทำการถอดออกมาได้นั้นช่วยให้เกิดความยืดหยุ่นและความน่าเชื่อถือ ซึ่งเหมาะสำหรับโปรเจ็กต์งานครีเอทีฟที่ต้องมีความต้องการสูง ซึ่งรวมถึงเวิร์กโฟลว์ของวิดีโอแบบหลายๆ สตรีมทั้งแบบ HD 2K 4K และ HDR

G-SPEED® Shuttle XL

G-SPEED Shuttle XL พร้อมเทคโนโลยี Thunderbolt 3 (ขนาด 96 เทราไบต์ จำหน่ายในราคา 367,199 บาท ไม่รวมภาษีมูลค่าเพิ่ม) สามารถจัดการกับวิร์คโฟลว์แบบหลายสตรีมของ ตั้งแต่ 4K ขึ้นไป ทั้งในสถานที่อื่นและสตูดิโอ G-SPEED Shuttle XL และ Thunderbolt 3 มาพร้อมฮาร์ดแวร์ RAID 0, 1, 5, 6, และ 50 คอนฟิก ในโซลูชั่นที่สามารถเครื่องย้ายได้ 8 ช่อง มาพร้อมกับฮาร์ดดิสก์ Ultrastar ระดับองค์กรซึ่งยกระดับความน่าเชื่อถือและอัตราถ่ายโอนข้อมูลสูงสุดถึง 2000 MB/s ทำให้นักสร้างสรรค์ผลงานมืออาชีพมีโซลูชั่นสำหรับการเก็บข้อมูลที่ดีที่สุดสำหรับวิดีโอและการจัดเก็บข้อมูลความจุสูง

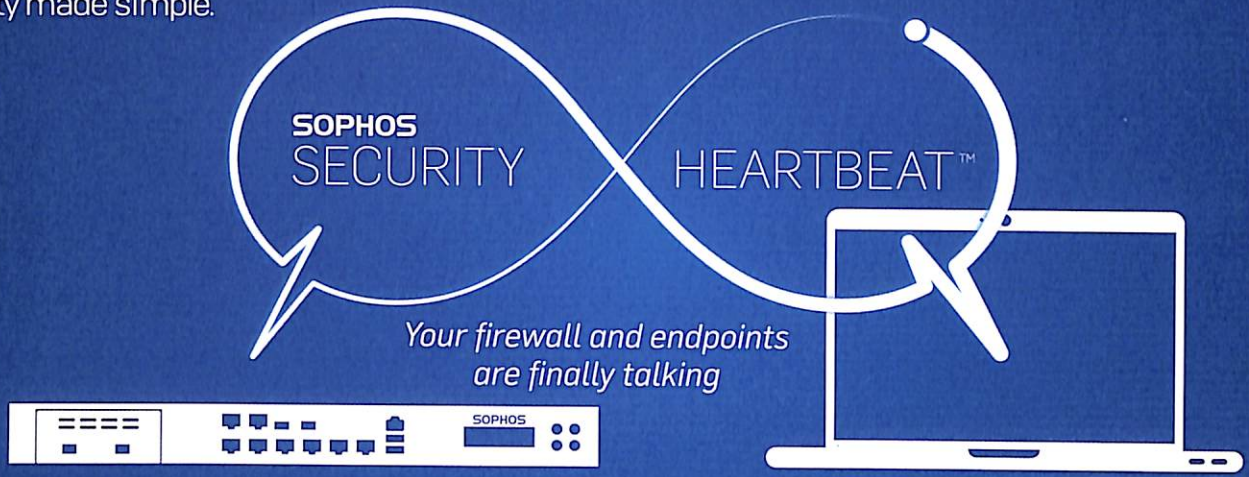
G-SPEED Shuttle XL พร้อมอะแดปเตอร์รุ่น ev Series Bay (ขนาด 72 เทราไบต์ จำหน่ายในราคา 280,799 บาท ไม่รวมภาษีมูลค่าเพิ่ม) ซึ่งคล้ายกับ G-SPEED Shuttle XL เทคโนโลยีแบบ Thunderbolt 3 ตัวอะแดปเตอร์รุ่น ev Series Bay ช่วยเพิ่มเติมทางเลือกในการทำงานและเพิ่มผลิตภาพโดยเปิดใช้งานฟังก์ชั่นกับไดรฟ์รุ่น ev Series ทั้งหมด ได้รับการออกแบบโดยใช้อะแดปเตอร์ที่มี 2 ช่องสำหรับ ev Series สำหรับการใช้กับชุดไดรฟ์ ev Series และเครื่องอ่าน ev Series ทำให้ผู้ใช้สามารถสัมผัสกับความน่าเชื่อถือที่เพิ่มขึ้นพร้อมกับอัตราการถ่ายโอนข้อมูลที่รวดเร็วถึง 1500 MB/s

โซลูชั่นจัดเก็บข้อมูลของ G-Technology ใช้ฮาร์ดดิสก์ Ultrastar ระดับองค์กร พร้อมการรับประกันจากอุตสาหกรรมชั้นนำ 5 ปี โซลูชั่นการเก็บข้อมูลของ G-Technology มีการจัดรูปแบบไว้ล่วงหน้าสำหรับคอมพิวเตอร์ของ Mac® สามารถจัดรูปแบบใหม่สำหรับคอมพิวเตอร์แบบ Windows® ด้วย G-Technology Windows Format Wizard

ข้อมูลเกี่ยวกับสินค้าทุกตัวของ G-Technology สามารถติดตามได้ที่ www.g-technology.com

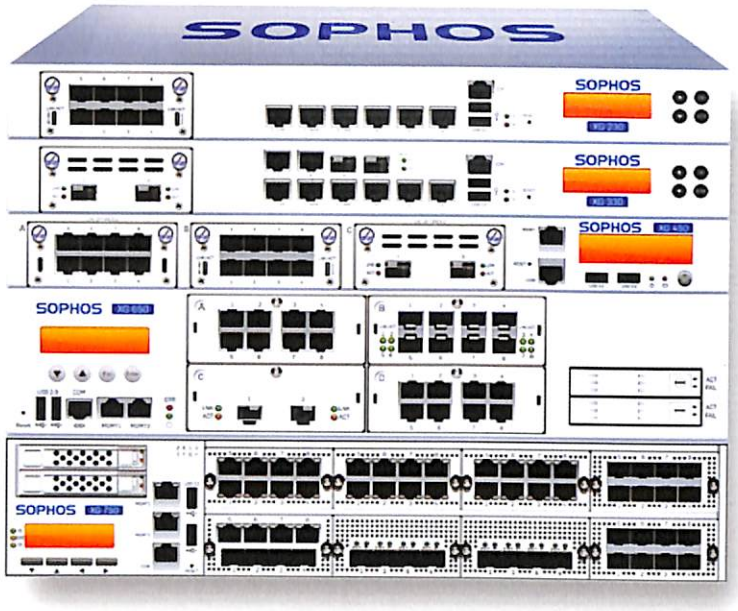
SOPHOS

Security made simple.



UNRIVALED

SECURITY SIMPLICITY AND INSIGHT



WITH FEATURES YOU JUST CAN'T GET ANY WHERE ELSE.

- Full protection suite of network, wireless, IPS, VPN, web, app, email, and web application firewall technology
- Automatically identify and isolate infected systems on your network until they can be cleaned up
- Unprecedented visibility, including user and application risk, with traffic-light style indicators and rich reporting
- Unified policy management that makes powerful policies and rule sets easy and intuitive
- Industry-leading performance at every price point with XG Series hardware appliances utilizing FastPath

E-Rong Consultants Co., Ltd.

90 CW Tower, 26th Floor, Tower A, Unit A 2602,
Ratchadapisek Rd., Huai Khwang, Bangkok 10310

Tel : 02-664-6588 Fax : 02-664-6599
E-mail : Sales@e-rong.co.th Website : www.e-rong.co.th