ข่าวสั้นและบทความ

CYBER THREATS 2018

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

WWW.ETDA.OR.TH ETDA THAILAND
ETDA
สพธอ

ข่าวสั้นและบทความ

CYBER THREATS 2018

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

WWW.ETDA.OR.TH ETDA THAILAND
ETDA สพธอ

ชื่อเรื่อง	ข่าวสั้นและบทความ CYBER THREATS 2018
เรียบเรียงโดย	สุรางคณา วายุภาพ, ชัยชนะ มิตรพันธ์, ศุภโชค จันทรประทิน, อุรัชฎา เกตุพรหม, พรพรหม ประภากิตติกุล, วีรชัย ประยูรพฤกษ์, Martijn Van Der Heide, สัญญา คล่องในวัย,อารยะ สวัสดิชัย, กรรณิกา ภัทรวิศิษฏ์สัณธ์, ทรงศักดิ์ ยงยิงศักดิ์ถาวร, ณัฐโชติ ดุสิตานนท์, ฉัตรชัย จันทร์อินทร์, ยุทธนา ชนวัฒน์, เสฏฐวุฒิ แสนนาม, ปวริศ จอมสถาน, จักรวาล องค์ทองคา, นันทพงศ์ บุญถนอม, รุ่งวิทย์ จิตรส่องแสง, ธนชัย แสงไพฑูรย์, สิริณัฐ ตั้งธรรมจิต, ภูรินทร์ หวังกีรติกานต์, วรรณิศา อนุรัตน์, พีร์นิธิ ฐานิวัฒนานนท์
ISBN	978-616-7956-45-9
พิมพ์ครั้งที่ 1	พฤษภาคม 2562
พิมพ์จำนวน	500 เล่ม
ราคา	300 บาท

จัดพิมพ์และเผยแพร่โดย

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

Thailand Computer Emergency Response Team (ThaiCERT)

Electronic Transactions Development Agency (ETDA)

Ministry of Digital Economy and Society

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี)

ชั้น 20 เลขที่ 33/4ถนนพระราม 9 แขวงห้วยขวาง

เขตห้วยขวาง กรุงเทพมหานคร 10310

โทรศัพท์: 0 2123 1212

คำนำ

ทุกวันนี้ ประชาชนส่วนใหญ่ล้วนต้องพึ่งพาอาศัยเทคโนโลยีสารสนเทศอย่างหลีกเลี่ยงไม่ได้เพื่ออำนวยความสะดวกและพัฒนาคุณภาพชีวิตในด้านต่าง ๆ ซึ่งเทคโนโลยีสารสนเทศที่ช่วยขับเคลื่อนทั้งเศรษฐกิจและสังคมนี้ จำเป็นต้องได้รับการปกป้องและดูแลที่เหมาะสมเพื่อป้องกันภัยคุกคามไซเบอร์ ที่มีรูปแบบหลากหลายและเปลี่ยนแปลงอย่างรวดเร็ว

ในปี 2561 เราพบการโจมตีทางไซเบอร์ในประเทศไทยที่มีผลประโยชน์ทางการเงินในรูปแบบต่าง ๆ เช่น การสวมรอยผู้ใช้ Line หรือ Facebook หลอกคนรู้จักของเหยื่อให้โอนเงิน การสร้างเว็บไซต์ธนาคารปลอม การเผยแพร่มัลแวร์เรียกค่าไถ่ การเจาะระบบเพื่อฝังโค้ดขุดสกุลเงินดิจิทัล ตัวอย่างกรณีการโจมตีที่ส่งผลกระทบรุนแรงต่อประเทศไทย อาทิ การแพร่ระบาดของมัลแวร์ขุดสกุลเงินดิจิทัล Monero ที่ประเทศไทยมีจำนวนดาวน์โหลดมากที่สุดในโลกถึงกว่า 3.5 ล้านครั้ง เป็นระยะเวลาต่อเนื่องกว่า 4 เดือน ทั้งนี้ คาดว่ายังคงพบการโจมตีในลักษณะนี้อย่างต่อเนื่องในปี 2562 ผู้ประสงค์ร้ายพยายามหาวิธีการใหม่ ๆ เพื่อโจมตีบริการทางการเงิน เช่น กรณีขโมยเงินในบัญชีธนาคารที่ผูกกับแอปพลิเคชัน e-Wallet

ประเทศไทยผลักดันเศรษฐกิจดิจิทัล โดยส่งเสริมให้มีบริการออนไลน์ในรูปแบบต่าง ๆ เพื่ออำนวยความสะดวกต่อประชาชน เช่น ระบบเสนอขายโทเคนดิจิทัลเพื่อระดมทุน (Initial CoinOffering Portal : ICO Portal) ระบบโครงการพัฒนาโครงสร้างพื้นฐานการยืนยันตัวตนอิเล็กทรอนิกส์ (National Digital ID) ฯลฯ จึงเป็นเรื่องที่หน่วยงานกำกับและผู้ให้บริการที่เกี่ยวข้องจำเป็นต้องช่วยกันดูแลอย่างใกล้ชิดและแจ้งเตือนผู้รับบริการให้หลีกเลี่ยงการตกเป็นเหยื่อ

ไทยเซิร์ตรวบรวมเหตุการณ์โจมตีทางไซเบอร์และสรุปสถิติที่สำคัญ การแจ้งเตือนช่องโหว่ แนวทางปฏิบัติในการป้องกันภัยคุกคามไซเบอร์ กฎหมาย ระเบียบที่เกี่ยวข้อง

ในรูปแบบข่าวสั้นและบทความผ่านช่องทางโซเชียลมีเดีย เพื่อสร้างความตระหนักรู้ให้กับประชาชนและยกระดับความรู้ให้กับผู้ดูแลระบบ โดยหวังเป็นอย่างยิ่งว่าหนังสือเล่มนี้จะช่วยให้ผู้อ่านเข้าใจรูปแบบภัยคุกคามไซเบอร์และพร้อมที่จะรับมือเมื่อเกิดเหตุการณ์ทางไซเบอร์ สร้างความเชื่อมั่นในการใช้เทคโนโลยีสารสนเทศเพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ และผลักดันประเทศไทยไปสู่สังคมเศรษฐกิจดิจิทัลอย่างแท้จริง

สุรางคณา วายุภาพ
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

สารบัญ

Awareness

Fraud

Incident

สารบัญ

Law & Policy

Malware

Privacy

Standard & Guideline

Statistic

สารบัญ

Vulnerability & Patch

สารบัญ


01
02
03
04


01
02
03
04


Awareness

ระวัง พิจารณาก่อนเล่นเกมทันใจ (Instant Game) บน Facebook อาจเปิดเผยข้อมูลส่วนตัวโดยไม่ตั้งใจได้

เมื่อวันที่ 9 พฤศจิกายน 2561 มีการเผยแพร่ข้อมูลผ่าน social media ว่า แอปพลิเคชัน OMG ซึ่งเป็นเกมทำนายนิสัย อาจขโมยข้อมูลส่วนบุคคลของผู้ใช้งานได้

ไทยเซิร์ตได้ตรวจสอบแล้วพบว่า OMG เป็นแอปพลิเคชันเกมจากผู้พัฒนาภายนอก ที่เล่นผ่านแพลตฟอร์มของ Facebook โดยตัวเกมถูกพัฒนาขึ้นมาในลักษณะ เกมทันใจ (Instant Game) รูปแบบของการเล่นเกมประเภทดังกล่าวคือเมื่อผู้ใช้กดปุ่มเล่นเกม จะมีการมอบสิทธิ์ในการเข้าถึงข้อมูลส่วนบุคคล ทั้งข้อมูลที่เป็นสาธารณะ เช่น ชื่อ รูปโพรไฟล์ หรือโพสต์ที่ถูกตั้งค่าให้เห็นแบบสาธารณะ และข้อมูลที่สามารถเข้าถึงได้เฉพาะเจ้าของบัญชี เช่น รายชื่อเพื่อน, สถานะการจ่ายเงินใน Messenger

ระบบ เกมทันใจ เป็นคุณสมบัติที่ Facebook พัฒนาขึ้นมาเพื่อให้ผู้ใช้สามารถเล่นเกมกับเพื่อนผ่าน Facebook Messenger หรือ News Feed ได้อย่างรวดเร็ว จึงมีความแตกต่างจากแอปพลิเคชันปกติที่ต้องมีการขออนุญาตสิทธิ์การเข้าถึงข้อมูลก่อน ทั้งนี้ การอนุญาตให้แอปพลิเคชันเข้าถึงข้อมูลส่วนบุคคลอาจมีผลต่อการนำข้อมูลนั้นไปใช้เพื่อการโฆษณา หรือเพื่อจุดประสงค์อย่างอื่นได้ ปัจจุบันไทยเซิร์ตอยู่ระหว่างการเฝ้าระวัง หากพบความผิดปกติจะแจ้งให้ทราบในภายหลัง

เนื่องจากแอปพลิเคชันประเภท เกมทันใจ นั้นมีการให้สิทธิ์บางอย่างโดยไม่ได้ขออนุญาต และไม่ได้มีการแจ้งข้อมูลโดยละเอียดก่อนเล่นเกมว่าจะอนุญาตให้เข้าถึงสิทธิ์อะไรบ้าง ผู้ที่มีความกังวลเรื่องความเป็นส่วนตัวควรพิจารณาก่อนเล่นเกมประเภทนี้ ทั้งนี้ หากผู้ใช้ได้เล่นเกมดังกล่าวแล้วมีความกังวลเรื่องข้อมูลส่วนตัว สามารถเข้าไปที่หน้าจอตั้งค่าแอปพลิเคชันที่ผู้กับบัญชี Facebook และลบแอปพลิเคชันนี้ออกได้

กระบวนการทำงานของไทยเซิร์ต หากพบแอปพลิเคชันที่เป็นอันตราย จะแจ้งเตือนสังคม ประสานงานกับผู้ให้บริการ และประสานงานกับเครือข่าย CERT เพื่อแลกเปลี่ยนข้อมูล

ThaiCERT
http://thcert.co/cM12q7
7/11/2561

Microsoft ออก Sysinternals ProcDump เวอร์ชัน Linux

Sysinternals เป็นชุดเครื่องมือสำหรับผู้ดูแลระบบปฏิบัติการ Windows ที่ Microsoft เผยแพร่ให้ดาวน์โหลดได้ฟรี ตัวอย่างเครื่องมือหลักๆ ที่นิยมใช้กันเช่น Autoruns, ProcDump, Process Explorer, Process Monitor เป็นต้น เมื่อต้นเดือนพฤศจิกายน 2561 ทาง Microsoft ได้แจ้งว่ากำลังพัฒนาเครื่องมือเหล่านี้ให้สามารถทำงานได้บนระบบปฏิบัติการ Linux ด้วย โดยเบื้องต้นได้ปล่อยโปรแกรม ProcDump ออกมาให้ดาวน์โหลดได้ฟรีแล้ว

ProcDump เป็นเครื่องมือที่ใช้สำหรับ dump ข้อมูลของ process ออกมาจาก memory รวมถึงสามารถใช้เฝ้าระวังการทำงานของ process, สร้างไฟล์ crash dump, หรือเชื่อมต่อกับโปรแกรม debugger ได้ ตัวอย่างคำสั่งที่ใช้ใน ProcDump สามารถศึกษาได้จากเว็บไซต์ของ Microsoft (https://docs.microsoft.com/en-us/sysinternals/downloads/procdump) อย่างไรก็ตาม สำหรับเวอร์ชัน Linux นี้อาจมีรูปแบบคำสั่งบางอย่างที่แตกต่างออกไป

โปรแกรม ProcDump เวอร์ชัน Linux มีให้ดาวน์โหลดทั้งแบบ binary พร้อมติดตั้ง และ source code สำหรับนำไป compile เอง โดยโปรแกรมรองรับ Linux Kernel เวอร์ชัน 3.5 ขึ้นไป ผู้ดูแลระบบที่สนใจใช้งานโปรแกรมนี้สามารถดาวน์โหลดได้จาก GitHub ของ Microsoft

Bleeping Computer
http://thcert.co/6lvMoO
7/11/2561

US-CERT เผยแพร่ข้อแนะนำในการทำลายข้อมูลก่อนทิ้งหรือส่งต่ออุปกรณ์อิเล็กทรอนิกส์

หน่วยงาน US-CERT ได้เผยแพร่ข้อแนะนำในการทำลายข้อมูลก่อนทิ้งหรือส่งต่ออุปกรณ์อิเล็กทรอนิกส์ โดยเนื่องจากปัจจุบันมีอุปกรณ์จำนวนมากที่สามารถเก็บบันทึกข้อมูลไว้ข้างในได้ หากไม่มีกระบวนการทำลายข้อมูลที่ดีพอแล้วนำอุปกรณ์ดังกล่าวไปทิ้ง ขายต่อ หรือบริจาค ก็อาจถูกผู้ไม่หวังดีกู้คืนข้อมูลสำคัญออกมาได้ รายการอุปกรณ์ในข้อแนะนำนี้ประกอบไปด้วยคอมพิวเตอร์ สมาร์ตโฟน แท็บเล็ต อุปกรณ์ดิจิทัลที่สามารถบันทึกข้อมูลได้เช่นกล้องหรือเครื่องเล่นเพลง อุปกรณ์เชื่อมต่อภายนอกที่สามารถรับส่งข้อมูลได้เช่นเครื่องพิมพ์หรือฮาร์ดดิสก์แบบพกพา และสุดท้ายคือเครื่องเล่นเกมคอนโซล

กระบวนการทำลายข้อมูล ตาม
ข้อแนะนำมีดังนี้

1. สำรองข้อมูลสำคัญออกมาจากตัวอุปกรณ์ เพื่อป้องกันข้อมูลสูญหาย รวมถึงเพื่อตรวจสอบว่าในอุปกรณ์นี้มีข้อมูลใดบ้างที่ผู้ประสงค์ร้ายอาจกู้คืนออกมาได้หากไม่ได้ถูกทำลายด้วยวิธีการที่เหมาะสม

2. สั่งลบข้อมูลในอุปกรณ์ โดยหากเป็นคอมพิวเตอร์ให้ใช้เครื่องมือประเภท secure erase หรือ disk wiping หากเป็นสมาร์ตโฟนหรือแท็บเล็ต กล้องดิจิทัล เครื่องเล่นเพลง เครื่องเกมคอนโซล หรืออุปกรณ์สำนักงาน เช่น เครื่องพิมพ์ เครื่องแฟกซ์ สั่ง factory reset จากนั้นถอดซิมการ์ด ฮาร์ดดิสก์ หรือการ์ดหน่วยความจำออกจากเครื่อง (หากทำได้)

3. เพื่อให้แน่ใจว่าผู้ประสงค์ร้ายจะไม่สามารถกู้คืนข้อมูลสำคัญออกมาจากอุปกรณ์ได้ อาจใช้วิธีเขียนทับสื่อบันทึกข้อมูลด้วยการ zero fill (เขียนทับทุก sector ด้วยค่า 0) หรือ random fill (เขียนทับทุก sector ด้วยค่า 0 หรือ 1 แบบสุ่ม)

4. หากอุปกรณ์ใดมีข้อมูลที่สำคัญมากๆ อยู่และไม่ต้องการให้ผู้อื่นใช้งานอุปกรณ์นั้นต่อ ควรทำลายทั้งเครื่องหรือทำลายชิ้นส่วนสำคัญให้ไม่สามารถใช้งานได้อีกต่อไป เช่น ทุบหรือเผา ทั้งนี้วิธีการทำลายอาจแตกต่างกันไปในแต่ละอุปกรณ์ เช่น ฮาร์ดดิสก์แบบจานแม่เหล็กอาจต้องใช้เครื่องทำลายสนามแม่เหล็ก ส่วนแผ่นซีดีอาจต้องใช้วิธีบดทำลาย เป็นต้น

ผู้ที่สนใจสามารถศึกษาข้อมูลเพิ่มเติมได้จากเว็บไซต์ US-CERT

ZDNet
http://thcert.co/wd4me9
US-CERT
http://thcert.co/hd2cVa
5/11/2561

ข้อแนะนำในการชอปปิงออนไลน์อย่างมั่นคงปลอดภัย

ปฏิเสธไม่ได้ว่าการชอปปิงออนไลน์นั้นอาจมีความเสี่ยงด้านความมั่นคงปลอดภัย ไม่ว่าจะเป็นการถูกขโมยข้อมูลส่วนตัวหรือข้อมูลบัตรเครดิต ข้อแนะนำเหล่านี้สามารถช่วยให้ผู้ที่ใช้บริการช็อปปิ้งแบบออนไลน์สามารถมีความปลอดภัยมากขึ้นได้

เว็บไซต์ชอปปิงออนไลน์นั้นเป็นเว็บไซต์จริงหรือไม่อาจทำได้ยาก วิธีที่ง่ายกว่าคือการช็อปปิ้งผ่านแอปพลิเคชันของผู้ให้บริการ ซึ่งควรดาวน์โหลดจาก App Store หรือ Play Store ไม่ควรติดตั้งแอปพลิเคชันช็อปปิ้งออนไลน์จากแหล่งซอฟต์แวร์ภายนอก เพราะอาจเป็นมัลแวร์ได้

1. ไม่แชร์ข้อมูลส่วนตัวกับผู้ขายหรือเว็บไซต์ซื้อขายสินค้า เนื่องจากอาจมีผู้ประสงค์ร้ายปลอมตัวเป็นเข้ามาขายสินค้าเพื่อหลอกถามหรือเก็บรวบรวมข้อมูล ทางที่ดีอีเมลสำหรับใช้ช็อปปิ้งออนไลน์ควรแยกออกมาต่างหากกับอีเมลหลักที่ใช้งานประจำ โดยเฉพาะอย่างยิ่งไม่ควรเป็นอีเมลที่ใช้สมัคร social media เพราะผู้ประสงค์ร้ายอาจใช้อีเมลดังกล่าวย้อนกลับมาหาข้อมูลส่วนบุคคลได้ ที่สำคัญทุกบัญชีควรตั้งรหัสผ่านที่คาดเดาได้ยากและเปิดใช้งานการยืนยันตัวตนแบบหลายชั้น

2. หากต้องการช็อปปิ้งออนไลน์ในขณะที่เชื่อมต่อกับ Wi-Fi สาธารณะควรเปิดใช้งาน VPN ก่อนทุกครั้ง เพื่อป้องกันไม่ให้ผู้ประสงค์ร้ายที่อยู่ในเครือข่าย Wi-Fi เดียวกันสามารถดักขโมยข้อมูลสำคัญออกไปได้ ทางที่ดีไม่ควรทำธุรกรรมที่อาจมีการส่งข้อมูลสำคัญเช่นบัตรเครดิตในขณะเชื่อมต่อกับ Wi-Fi สาธารณะ

3. ควรจ่ายเงินผ่านระบบของเว็บไซต์ที่ให้บริการช็อปปิ้ง ไม่ควรโอนเงินให้กับผู้ขายโดยตรง เพราะความปลอดภัยและการรับผิดชอบความเสียหายนั้นแตกต่างกัน

4. ก่อนล็อกอินหรือจ่ายเงิน ตรวจสอบว่า URL ของเว็บไซต์ถูกต้องและเชื่อมต่อผ่าน HTTPS ทางที่ดีควรพิมพ์ URL ของเว็บไซต์โดยตรง ไม่คลิกจากลิงก์ในอีเมลหรือเว็บไซต์อื่น

5. ไม่ควรใช้บัตรเครดิตหลักที่มีวงเงินสูงในการช็อปปิ้งออนไลน์ ควรใช้วิธีสร้างบัตรเสมือนหรือบัตรเครดิต/เดบิตแบบชั่วคราวสำหรับใช้ช็อปปิ้งในวงเงินจำกัด เช่น จ่ายได้ไม่เกินครั้งละ 2,000 บาท เป็นต้น เพื่อจำกัดความเสียหายหากเกิดเหตุการณ์ข้อมูลรั่วไหล

6. ตรวจสอบข้อมูลการใช้จ่ายบัตรเครดิตอย่างสม่ำเสมอ โดยปกติผู้ให้บริการบัตรเครดิตมักมีบริการแจ้งเตือนรายการซื้อขายล่าสุดผ่านทาง SMS, อีเมล หรือแอปพลิเคชัน ซึ่งหากพบรายการซื้อขายที่ไม่แน่ใจหรือคาดว่าถูกขโมยข้อมูลบัตรเครดิตไปใช้งานควรติดต่อธนาคารโดยเร็ว

TripWire
http://thcert.co/xCbEWH
26/10/2561

NIST เผยแพร่เอกสารข้อมูลภาพรวมด้านเทคนิคของเทคโนโลยี Blockchain เน้นสร้างความเข้าใจให้บุคคลทั่วไปและผู้บริหาร

ในช่วงหลายปีที่ผ่านมา คำว่า blockchain นั้นถูกพูดถึงในสื่อกระแสหลักอยู่เป็นระยะ ทั้งในแง่ของการเป็นเทคโนโลยีที่สามารถแก้ไขปัญหาหลายอย่างของระบบการเก็บข้อมูลแบบเดิมได้ หรือการที่เป็นเทคโนโลยีเบื้องหลังของระบบ cryptocurrency ที่ทั้งผู้ใช้งานและนักเก็งกำไรต่างให้ความสนใจ อย่างไรก็ตาม เทคโนโลยี blockchain เองก็มีข้อจำกัดและอาจไม่ได้เหมาะสมกับงานทุกประเภท เมื่อเดือนตุลาคม 2561 ทางหน่วยงาน NIST ของสหรัฐอเมริกาได้เผยแพร่เอกสาร NISTIR 8202 หัวข้อ Blockchain Technology Overview ซึ่งตัวเอกสารนี้เน้นการให้ข้อมูลภาพรวมในเรื่องหลักการทำงานของ blockchain โดยจุดประสงค์ของเอกสารจะเน้นไปที่การสร้างความเข้าใจให้กับผู้ที่ยังไม่มีพื้นฐาน และผู้บริหารที่สนใจใช้งาน blockchain ในองค์กร

โครงสร้างเนื้อหาของเอกสารนี้ จะไล่ตั้งแต่ที่มาและจุดประสงค์ของเทคโนโลยี blockchain รูปแบบการทำงาน องค์ประกอบต่างๆ ของตัวระบบ การยืนยันความถูกต้องของข้อมูล ความปลอดภัย รวมถึงข้อจำกัดและสิ่งที่คนทั่วไปมักจะเข้าใจผิดเกี่ยวกับ blockchain และข้อควรตระหนักก่อนนำ blockchain มาใช้ในองค์กร ตัวเอกสารมีทั้งหมด 59 หน้า แบ่งเป็น 9 หัวข้อ ผู้ที่สนใจสามารถดาวน์โหลดเอกสารนี้ได้ฟรีจากเว็บไซต์ของ NIST

https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

NIST
http://thcert.co/4yJWRl
8/10/2561

ความมั่นคงปลอดภัยไซเบอร์ กับหน่วยงานภาคสาธารณสุข

จากเหตุการณ์ข้อมูลรั่วไหลหลายครั้งที่เกิดกับตัวองค์กรสาธารณสุข และ vendor ที่หน่วยงานจ้าง ในช่วงที่ผ่านมา เช่น หน่วยงาน Legacy Health ถูกโจมตีด้วยฟิชชิง ส่งผลให้ข้อมูลผู้ป่วย 38,000 รายการรั่วไหล*

แสดงให้เห็นถึงความสนใจของผู้ประสงค์ร้ายที่มีต่อข้อมูลส่วนบุคคลของหน่วยงานในภาคส่วนนี้ มีการนำข้อมูลไปขายใน Dark Web ซึ่งเป็นเว็บไซต์รูปแบบนึงที่มีลักษณะซ่อนตัวจากการค้นหาทั่วไป โดยตัวอย่างข้อมูลที่ขาย เช่น ข้อมูล 1 เซ็ตของบุคคล 1 คนประกอบด้วยชื่อ วันเกิด หมายเลขบัตรประชาชน ข้อมูลทางการแพทย์ ถูกขายในราคาสูงถึง 50 ดอลล่าร์ หรือประมาณ 1500 บาท มีราคามากกว่าข้อมูลบัตรเครดิตซึ่งถูกขายในราคา 1-3 ดอลล่าร์ หรือ 50-150 บาท ผู้ประสงค์ร้ายที่ซื้อข้อมูลอาจนำไปใช้ในการสวมรอยหรือหลอกลวงผู้อื่น

ด้วยความที่เป้าหมายหลักของหน่วยงานภาคสาธารณสุขคือการรักษาคน อาจส่งผลให้หน่วยงานไม่ได้ให้ความสนใจด้านความมั่นคงปลอดภัยในระบบไอทีเท่าที่ควร ไม่ได้มีการอัปเดตระบบ จึงเป็นสาเหตุให้ถูกโจมตีจากบุคคลภายนอก สาเหตุอีกส่วนมาจากการกระทำของพนักงานภายในจากรายงาน 2018 Verizon Protected Health Information Data Breach**

ซึ่งสำรวจ 27 ประเทศ (ข้อมูลสามในสี่เป็นของหน่วยงานในสหรัฐฯ) พบว่าสาเหตุหลักส่วนหนึ่งของข้อมูลรั่วไหลเกิดจากการกระทำที่ตั้งใจจากพนักงานภายในซึ่งอาจเป็นเพราะจุดประสงค์ต่าง ๆ ตั้งแต่ความสะดวกส่วนตัว จนถึงจุดประสงค์ทางการเงิน หรือเพื่อแก้แค้น โดย 66% เป็นการเข้าถึงข้อมูลโดยที่ไม่ควรมีสิทธิเข้าถึง (privilege abuse)

ดังนั้น หน่วยงานภาคสาธารณสุขอาจพิจารณามาตรการด้านความมั่นคงปลอดภัย เช่น การสร้างความตระหนักรู้ให้กับเจ้าหน้าที่, การเข้ารหัสลับข้อมูลข้อมูลสำคัญ, การใช้งานการยืนยันตัวตนแบบหลายขั้นตอนในระบบสำคัญ, บังคับใช้นโยบายการให้สิทธิเท่าที่จำเป็น

ด้วยการโจมตีด้านไซเบอร์ที่เพิ่มขึ้นต่อภาคสาธารณสุขในประเทศสหรัฐฯ จึงมีมาตรการทางกฎหมายเข้ามากำกับ เช่น Health Insurance Portability and Accountability Act (HIPAA) หรือ the Health Information Technology for Economic and Clinical Health (HITECH) Act ถือเป็นเพียงมาตรการขั้นต่ำที่หน่วยงานต้องทำตาม ซึ่งหน่วยงานจำเป็นต้องเสริมสร้างศักภาพอย่างต่อเนื่องเพื่อรับมือภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว

* https://www.healthcareitnews.com/news/phishing-attack-breaches-38000-patient-records-legacy-health

**http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf

Securityweek
http://thcert.co/H7UVHc
2018-09-18-01

บทบาทของทีมรับมือภัยคุกคามกับมาตรฐานด้านความมั่นคงปลอดภัยของ ICS

ICS หรือ Industrial Control System เป็นระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรมต่าง ๆ ซึ่งระบบเหล่านี้ที่ถูกใช้งานในปัจจุบันอาจจะเก่าและไม่ได้ถูกออกแบบโดยคำนึงถึงความมั่นคงปลอดภัย เช่น ทำการอัปเดตได้ยาก ไม่มีระบบจัดการอุปกรณ์ (asset management) หรือการเฝ้าระวังภัยคุกคาม เป็นอุปสรรคที่ท้าทายในการจะทำให้หน่วยงานปฏิบัติตามมาตรฐานหรือข้อบังคับด้านความมั่นคงปลอดภัย อย่างไรก็ตาม ทีมที่มีหน้าที่รับมือภัยคุกคามอาจพิจารณา 5 หัวข้อเป็นแนวทาง โดยมีรายละเอียดดังนี้

1. Asset Management ทำการระบุ จัดแยกประเภท ระบบ ICS รวมถึงข้อมูลที่ระบบจัดเก็บ

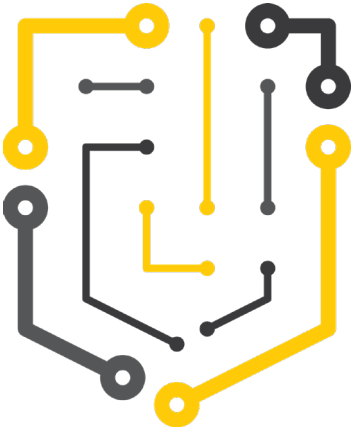
2. Identify and access management ในการเข้าถึงระบบ ต้องมีการยืนยันตัวตน จำกัดและควบคุมสิทธิ

3. Risk assessment, Vulnerability management, and change management มีการประเมินความเสี่ยง ตรวจสอบหาช่องโหว่ของระบบ รวมถึงจัดการและบันทึกการแก้ไขค่าต่างๆ รวมถึงการอัปเดตของระบบ

4. Security controls ควบคุมเพิ่มความมั่นคงปลอดภัย เช่น แยกเครือข่าย ICS ออกจากเครือข่ายที่ใช้งานทั่วไป เข้ารหัสลับข้อมูล มีการเฝ้าระวังและบันทึกทราฟิค

5. Physical security เนื่องจากอุปกรณ์ ICS มักมีข้อจำกัดเรื่องความสามารถด้านความมั่นคงปลอดภัย จึงจำเป็นต้องจำกัดการเข้าถึงอุปกรณ์ทางภาพอย่างเข้มงวด

ทีมที่รับมือคุกคามมีบทบาทสำคัญในการทำให้องค์กรปฏิบัติตามมาตรฐานด้านความมั่นคงปลอดภัย ไม่ว่าจะเป็น การเฝ้าระวังเพื่อตรวจจับภัยคุกคามให้เร็วที่สุด การวิเคราะห์ตรวจสอบภัยคุกคามที่พบ เช่น สาเหตุ ความเสียหาย แนวทางแก้ไข นอกจากนี้ยังรวมถึงการทำเอกสารขั้นตอนการรับมือ ดังนั้นหน่วยงานจึงควรให้ความสำคัญในการสร้างทีมรับมือภัยคุกคาม ซึ่งส่วนใหญ่มักจะเป็นเจ้าหน้าที่ปฏิบัติการที่ดูแลระบบ ICS



สำหรับผู้ที่สนใจสามารถศึกษาแนวทางด้านความมั่นคงปลอดภัยสำหรับ ICS ได้จากเอกสาร Recommended Practice: Creating Cyber Forensics Plan for Control Systems* Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability** รวมถึงตามข้อมูลจากเว็บไซต์ของ National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems (https://ics-cert.us-cert.gov) ซึ่งเป็นหน่วยงานที่ส่งเสริมความมั่นคงปลอดภัยของ ICS ของประเทศสหรัฐฯ

*https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Forensics_RP.pdf

**https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf

DarkReading
http://thcert.co/bBV36R
10/9/2561

Malvertising กับการโจมตีผ่านวงจรธุรกิจโฆษณาออนไลน์

ก่อนหน้านี้ไทยเซิร์ตได้อธิบายเกี่ยวกับการแพร่กระจายมัลแวร์ผ่านทางโฆษณาในหน้าเว็บไซต์หรือ Malvertising ซึ่งเกิดจากผู้ประสงค์ร้ายซื้อพื้นที่โฆษณาสำหรับใช้โจมตี (https://www.thaicert.or.th/newsbite/2016-06-27-02.html) อย่างไรก็ตามบริษัทด้านความมั่นคงปลอดภัยพบว่ามีผู้ประสงค์ร้ายได้เจาะระบบเว็บไซต์ที่ใช้งาน Wordpress เวอร์ชันเก่า (4.7.1) มากกว่า 10,000 เว็บไซต์ เพื่อขายพื้นที่โฆษณาให้กับผู้ประสงค์ร้ายที่ต้องการเผยแพร่มัลแวร์ด้วย

สำหรับวงจรธุรกิจโฆษณาออนไลน์นั้นสามารถแบ่งเป็นส่วนประกอบ 4 ส่วน คือ

1. ผู้ที่มีเนื้อหาที่ต้องการโฆษณา (Advertiser)

2. เจ้าของเว็บไซต์ที่เตรียมพื้นที่สำหรับโฆษณาออนไลน์ (Publisher)

3. บริษัทกลางที่ติดต่อซื้อพื้นที่โฆษณา Publisher จำนวนมากและแบ่งขายให้กับ Advertisers ด้วยระบบประมูล (Ad-Networks)

4. ในบางรูปแบบธุรกิจ จะมีบริษัทที่รับซื้อพื้นที่โฆษณาจาก Ad-Networks เพื่อขายต่อให้กับ Advertiser อีกที (Reseller)

การโจมตีที่พบนั้น ผู้ประสงค์ร้ายได้เจาะระบบเว็บไซต์จำนวนมากแล้วขายพื้นที่โฆษณาบนเว็บไซต์ให้กับ Ad-Networks และผู้ประสงค์ร้ายที่ต้องการเผยแพร่มัลแวร์จะเลือกซื้อพื้นที่โฆษณาบนเว็บไซต์ของผู้ประสงค์ร้ายคนดังกล่าว ในขณะที่ Ad-Networks และ Reseller อยู่ในฐานะคนกลางที่อาจรู้เห็นในการกระทำผิดแต่ได้รับผลประโยชน์ทางธุรกิจ ซึ่งสภาพแวดล้อมในรูปแบบนี้ทำให้ยากต่อการหยุดยั้งการโจมตี อีกทั้งยังตรวจจับการโจมตีได้ยากเนื่องจากผู้ประสงค์ร้ายอาจเลือกเผยแพร่มัลแวร์เมื่อพบเป้าหมายผู้เยี่ยมชมเว็บไซต์ที่มีคุณสมบัติตรงตามลักษณะเฉพาะที่กำหนด เช่น เวอร์ชันระบบปฏิบัติการหรือเบราว์เซอร์ที่ใช้งาน

เพื่อป้องกันการถูกโจมตี ทั้งเจ้าของเว็บไซต์และผู้ที่เยี่ยมชมเว็บไซต์ควรอัปเดตระบบปฏิบัติการและซอฟต์แวร์ที่ให้งานเป็นประจำ สำหรับผู้ดูแลระบบอาจใช้ข้อมูลรายการโดเมนต้องสงสัย และหมายเลขไอพีของเครื่องผู้ประสงค์ร้าย (134.249.116.78) เป็นข้อมูลประกอบในการเฝ้าระวังการโจมตีหรือตรวจสอบเครื่องที่ติดมัลแวร์

Checkpoint
http://thcert.co/ZiYI6h
2/8/2561

จุดอ่อนของโปรแกรม สร้างความตระหนักรู้ในองค์กร

หากพูดถึงหนึ่งในมาตรการเสริมสร้างด้านความมั่นคงปลอดภัยที่องค์กรนำมาปฏิบัติ ก็มักจะนึกถึงการสร้างความตระหนักรู้ให้กับพนักงานในองค์กร ทำให้พนักงานรู้จักรูปแบบภัยคุกคาม เช่น รู้จักสังเกตลักษณะของอีเมลหลอกลวง เพื่อให้รู้เท่าทันหลีกเลี่ยงการตกเป็นเหยื่อ แต่โปรแกรมเหล่านี้อาจยังไม่ช่วยป้องกันได้อย่างสมบูรณ์ เนื่องจาก สุดท้ายแล้วขึ้นอยู่กับการตัดสินใจของพนักงานเองว่าการกระทำที่พบเป็นการหลอกลวงหรือไม่ ซึ่งกลไกที่มาช่วยเติมเต็มในส่วนนี้คือการมีกระบวนการที่ชัดเจน

ยกตัวอย่าง เช่น การหลอกลวงติดต่อไปยัง HR เพื่อขอข้อมูลส่วนบุคคลของพนักงาน หากให้ HR เป็นผู้พิจารณาเองก็มีโอกาสที่ HR จะตกเป็นเหยื่อ แต่หากมีกระบวนการที่ดี กำหนดชัดเจนว่าใครที่สามารถขอข้อมูลเหล่านี้ได้ และมีการลงนามเพื่อยืนยันตัวตน ผู้ประสงค์ร้ายต้องใช้ความพยายามปลอมเป็นผู้มีอำนาจในการเข้าถึงข้อมูล ถือเป็นการยกระดับการปกป้องกัน ช่วยลดความเสี่ยงได้มาก

อีกตัวอย่างเป็นเรื่องของ กลไก เรื่องเหตุการณ์ทดสอบหลอกให้ยามออกตราป้ายเพื่อเข้าถึงข้อมูลสำคัญ ซึ่งองค์กรของยามนั้นไม่มีกระบวนการที่ชัดเจนในการกำกับการออกป้าย ยิ่งไปกว่านั้นคือไม่มีการบันทึก ทำให้ไม่รู้ว่าเป็นยามคนไหนที่ออกป้าย ซึ่งผู้รับผิดก็คือหัวหน้าผู้จัดการที่ดูแลเรื่องความปลอดภัย

สุดท้ายเป็นเรื่องของ การสูญหายของ Thumb Drive ที่เก็บข้อมูล ซึ่งองค์กรมักจะบอกพนักงานว่าให้ระวังไม่ให้สูญหาย แต่วิธีที่ดีกว่านั้นคือการกำหนดว่าข้อมูลสำคัญระดับใดที่สามารถเก็บใส่ Thumb Drive ได้ หรือคำนึงถึงเผื่อกรณีสูญหาย ให้เข้ารหัสลับไว้หากต้องถ่ายข้อมูลสำคัญลง Thumb Drive โดยวิธีง่ายวิธีหนึ่งคือการเก็บในรูปแบบไฟล์สกุล zip ที่ใส่รหัสลับไว้

ดังนั้นแล้ว จึงเป็นเรื่องที่ดีที่องค์กรควรตรวจสอบว่าส่วนใดที่ต้องพึ่งการใช้วิจารณญาณของพนักงาน กล่าวคือ พนักงานต้องระวังในเรื่องใด เพื่อไม่ให้ตกเป็นเหยื่อ แล้วลองคิดว่าจะหากระบวนการใดมาชดเชยเพื่อลดความเสี่ยง แทนที่จะบอกให้ระวังอย่างเดียว ก็จะช่วยเสริมให้องค์กรมีความมั่นคงปลอดภัยมากขึ้น

Dark Reading
http://thcert.co/6bc1gi
20/7/2561

ความมั่นคงปลอดภัยของข้อมูลบนโซเชียลมีเดีย

ในโลกโซเชียลมีเดียที่เรียกได้ว่าหลายคนใช้เวลาอยู่ในโลกแห่งนี้มากกว่าโลกแห่งความจริง แต่คำถามที่คนส่วนใหญ่ไม่ได้นึกถึงคือ ข้อมูลของเราบนโซเชียลมีเดียมีความมั่นคงปลอดภัยแค่ไหน ซึ่งหากพูดถึงความมั่นคงปลอดภัย เราสามารถจำกัดความของคำนี้ด้วยคุณสมบัติ 3 ด้านคือ

การรักษาความลับของข้อมูล (Confidentiality)

นั่นหมายถึงผู้ใช้สามารถกำหนดว่าใครสามารถเข้าถึงข้อมูลได้บ้าง ใน Facebook ผู้ใช้สามารถกำหนดได้ว่าให้ใครก็ตาม เพื่อน หรือ กลุ่มคนที่เฉพาะ ให้สามารถอ่านโพสต์ที่สร้างไว้ สำหรับ Instagram ข้อความต่าง ๆ จะเป็นรูปแบบที่ใครก็ตามสามารถอ่านได้ แต่ก็มีช่องทาง direct message สำหรับสื่อสารในรูปแบบตัวต่อตัว

ข้อมูลไม่ถูกใครแอบมาแก้ไข (Integrity)

ในโซเชียลมีเดีย ไม่ค่อยมีปัญหาในด้านนี้ เพราะข้อมูลจะถูกแสดงในรูปแบบที่เราโพสต์ โดยเป็นเรื่องยากที่จะมีคนอื่นมาแก้ไข แต่ในฐานะผู้ที่อ่านโพสต์ควรระลึกไว้ว่าข้อความที่โพสต์นั้นที่เห็นอยู่ อาจถูกแก้ไขก่อนหน้าโดยเจ้าของโพสต์เอง ซึ่งไม่ใช่ปัญหาของ Integrity และในกรณีของ Facebook ผู้ที่อ่านโพสต์ สามารถตรวจสอบดูประวัติการแก้ไขของโพสต์ได้

ข้อมูลพร้อมใช้งาน (Availability)

หมายความว่าผู้ใช้สามารถอ่านหรือแชร์ข้อความหรือรูปในโซเชียลเมื่อต้องการ แต่ในแง่มุมนึงอาจจะพูดถึงคุณสมบัติการดึงข้อมูลบนโซเชียลมีเดีย เช่น รูป หรือคลิป มาเก็บไว้บนเครื่องเพื่อใช้งานในเวลาที่ไม่สามารถเข้าถึงโซเชียลมีเดียได้ ซึ่งผู้ใช้ Facebook สามารถเรียกใช้งานความสามารถนี้ได้ที่ https://www.facebook.com/settings?tab=your_facebook_information

การที่เรารู้จักใช้วิธีควบคุม และรู้จักเลือกกำหนดการเข้าถึงข้อมูลให้เหมาะสมกับข้อมูลที่จะโพสต์ จะทำให้ข้อมูลมีความมั่นคงปลอดภัยมากขึ้น ใน Facebook หรือโซเชียลมีเดียต่าง ๆ อาจมีการอัปเดตเปลี่ยนแปลงรูปแบบการกำหนดดังกล่าว ผู้ใช้จึงควรเช็คเป็นประจำ หากต้องการข้อมูลเพิ่มเติม ผู้ใช้สามารถศึกษาข้อแนะนำในการใช้โซเชียลมีเดียได้จาก Infographic ของไทยเซิร์ต

https://www.thaicert.or.th/downloads/files/BROCHURE_Social_Network.jpg

Trend Micro
http://thcert.co/z4Cg7t
2/7/2561

แนวทางการเตรียมตัวและรับมือกรณีข้อมูลรั่วไหลสำหรับหน่วยงานเก็บข้อมูลส่วนบุคคลในออสเตรเลีย

เมื่อเดือนกุมภาพันธ์ หน่วยงานภาครัฐของประเทศออสเตรเลีย Office of the Australia Information Commissioner ได้เผยแพร่เอกสารชื่อ Data breach preparation and response - A guide to managing data breaches in accordance with the Privacy Act 1988 ซึ่งเป็นแนวทางการเตรียมตัวและรับมือกรณีข้อมูลรั่วไหลสำหรับหน่วยงานที่เก็บข้อมูลส่วนบุคคล ซึ่งสอดคล้องกับกฎหมายคุ้มครองความเป็นส่วนตัว Privacy Act 1988 โดยได้แนะนำกฎหมายการรั่วไหลของข้อมูลและกฎหมายคุ้มครองความเป็นส่วนตัว (Data breaches and the Australian Privacy Act) และกฎหมาย the Privacy Act 1988 รวมถึงเนื้อหาส่วนหนึ่งระบุถึงแนวทาง 13 ประการในการจัดการข้อมูลส่วนบุคคล มีเนื้อหา เช่น การเก็บข้อมูลส่วนบุคคลสามารถเก็บได้มากน้อยแค่ไหน การจัดการข้อมูลส่วนบุคคลที่ไม่จำเป็นต้องใช้แล้ว แนวทางการรักษาความมั่นคงปลอดภัยของข้อมูล

(https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/)

นอกจากนี้ยังพูดถึง The Notifiable Data Breaches (NDB) scheme ซึ่งเป็นข้อบังคับให้หน่วยงานต้องแจ้งผู้ได้รับผลกระทบและหน่วยงานที่กำกับดูแล เมื่อข้อมูลส่วนบุคคลรั่วไหลหรือถูกขโมย และคาดว่าจะส่งผลกระทบร้ายแรงกับผู้ที่เกี่ยวข้อง และหน่วยงานไม่สามารถควบคุมหรือจัดการได้ นอกจากนี้หน่วยงานบางหน่วยงานอาจจำเป็นต้องปฏิบัติตามข้อบังคับเพิ่มเติม เช่น General Data Protection Regulation ของสหภาพยุโรป

เนื้อหาอีกส่วนที่น่าสนใจคือการเตรียมแผนรับมือเมื่อเกิดเหตุข้อมูลรั่วไหล (Preparing a data breach response plan) อธิบายส่วนประกอบของแผน เช่น มีการประเมิน จำกัดความเสียหาย และจัดการเหตุตั้งแต่ต้นจนจบ ครอบคลุมข้อกำหนดทางกฎหมาย กำหนดบทบาทและหน้าที่ ในเอกสารได้แนบเช็คลิสต์ในการสร้างแผนไว้ด้วย ผู้สนใจสามารถค้นหาในเอกสารด้วยคำว่า Data breach response plan quick checklist รวมถึงการรับมือเมื่อเกิดเหตุข้อมูลรั่วไหล 4 ขั้นตอน ได้แก่

1) จำกัดความเสียหาย
2) ประเมินผลกระทบ
3) แจ้งผู้ที่ผู้ได้รับผลกระทบและหน่วยงานกำกับที่เกี่ยวข้อง
4) ทบทวนแนวทางการรับมือและหาวิธีการป้องกันไม่ให้เกิดขึ้นอีก

Notifiable Data Breach (NDB) Scheme อธิบายข้อกำหนดของหน่วยงานที่จำเป็นต้องรายงานเมื่อเกิดเหตุข้อมูลรั่วไหล เช่น เป็นหน่วยงานที่มีรายรับประจำปีมากกว่า 72 ล้านบาท หรือหน่วยงานที่ซื้อขายข้อมูลส่วนบุคคล หรือหน่วยงานที่เก็บข้อมูลส่วนบุคคลทางการแพทย์ และบทบาทของหน่วยงานที่รับรายงาน

แหล่งข้อมูลอื่นๆ ที่เกี่ยวข้อง ได้แก่ รายการหน่วยงานให้คำปรึกษาในกรณีเกิดเหตุข้อมูลบางชนิดรั่วไหล เช่น หากข้อมูลส่วนบุคคลทางการแพทย์รั่วไหล จำเป็นต้องดูข้อแนะนำของ Australian Digital Health Agency รวมถึงข้อแนะนำ มาตรฐาน อื่นๆ ในการรับมือและป้องกันเหตุภัยคุกคาม

ปัจจุบันหน่วยงานที่เก็บข้อมูลส่วนบุคคลมักจะตกเป็นเป้าของการโจมตี จึงจำเป็นต้องมีการเตรียมพร้อมวางแผน ซักซ้อมรับมือเมื่อเกิดเหตุเพื่อให้แน่ใจว่าแผนที่เตรียมไว้สามารถใช้งานได้จริง รวมถึงอาจสร้างเครือข่ายกับหน่วยงานประเภทเดียวกันแลกเปลี่ยนข้อมูล เพื่อแลกเปลี่ยนประสบการณ์ ความรู้

Office of the Australia Information Commissioner
http://thcert.co/uezJTF
18/4/2561

10 ข้อแนะนำ เพิ่มความมั่นใจ ใช้งานมือถือ Android อย่างปลอดภัย

Malwarebytes แนะนำ 10 ข้อที่ช่วยให้อุปกรณ์ระบบปฏิบัติการ Android มีความมั่นคงปลอดภัยมากขึ้น โดยมีรายละเอียดดังนี้

1. ทำความรู้จักฟีเจอร์หรือค่าต่างๆ ที่เกี่ยวกับความมั่นคงปลอดภัยหรือความเป็นส่วนตัว เช่น ฟีเจอร์ที่เปิดให้ระบุตำแหน่งพิกัด GPS หรือลบข้อมูลในมือถือกรณีที่อุปกรณ์สูญหาย*ตรวจสอบความมั่นคงปลอดภัยและความเป็นส่วนตัว เช่น มีการล็อกหน้าจอด้วยรหัสผ่านหรือไม่ รวมถึงตรวจสอบจากบริการ Security Checkup ของ Google*

2. กำหนดในปฏิทินเตือนให้ตรวจสอบความมั่นคงปลอดภัยและความเป็นส่วนตัวทุก 12 เดือน

3. เนื่องจากการสื่อสารบางช่องทาง เช่น SMS อาจไม่ได้มีการเข้ารหัสลับข้อมูล มีความเสี่ยงให้ผู้ประสงค์ร้ายดักข้อมูลได้ ในการสื่อสารที่สำคัญและเป็นความลับ ควรใช้งานแอปพลิเคชันแชตที่มีการเข้ารหัสลับข้อมูลแบบ end-to-end ซึ่งป้องกันการดักข้อมูล บุคคลที่สามรวมถึงผู้ให้บริการแอปพลิเคชันไม่สามารถอ่านข้อมูลได้ ตัวอย่างแอปพลิเคชัน เช่น Signal (https://ssd.eff.org/en/module/how-use-signal-android)

4. ควรหลีกเลี่ยงการแชร์ตำแหน่งของมือถือบนโซเชียลมีเดียที่ไม่จำเป็น และจำกัดการใช้แอปพลิเคชันที่มีสิทธิอ่านข้อมูลตำแหน่งของมือถือ

5. ปิดการใช้ Wi-Fi และ Bluetooth เมื่อไม่ใช้งานมือถือ

6. ตรวจสอบรายการอุปกรณ์ที่ผูกกับบัญชี Google (https://myaccount.google.com/device-activity) หากพบรายการอุปกรณ์ที่ไม่รู้จักให้ทำการลบรายการ และเปลี่ยนรหัสผ่าน

7. ระวังแอปพลิเคชันหลอกลวงที่เลียนแบบใช้ไอคอนหรือชื่อคล้ายแอปพลิเคชันจริง ซึ่งอาจมีพฤติกรรมไม่พึงประสงค์ เช่น ขโมยข้อมูล, แสดงโฆษณา ซึ่งผู้ใช้อาจพิจารณาความน่าเชื่อถือของแอปพลิเคชันจากจำนวนครั้งที่แอปพลิเคชันถูกดาวน์โหลดหรือพิจารณาจากรีวิว

8. หลีกเลี่ยงการทำธุรกรรมสำคัญเมื่อใช้ Wi-Fi ฟรี ตามสถานที่ต่างๆ โดยเฉพาะ Wi-Fi ที่ไม่มีการตั้งรหัสผ่าน การจำเป็นต้องใช้งานก็อาจพิจารณาใช้ VPN ที่น่าเชื่อถือ

9. เมื่อได้รับข้อความจากอีเมล โซเชียลมีเดีย SMS หยุดคิดซักนิดถึงความน่าเชื่อถือของข้อความหรือผู้ส่งก่อนตกลงกระทำการใดๆ

*https://myaccount.google.com/security-checkup

Malwarebytes
http://thcert.co/C3CeeU
5/4/2561

ผลสำรวจเผย 2 บทบาท ผู้บริหาร เจ้าหน้าที่ฝ่ายเทคนิค มีความเห็นด้านการรับมือภัยคุกคามต่าง และส่งผลต่อองค์กรอย่างไร

บริษัท Centrify เผยแพร่รายงานผลสำรวจด้านความมั่นคงปลอดภัยที่ทำกับผู้บริหารและเจ้าหน้าที่ฝ่ายเทคนิคเพื่อเปรียบเทียบมุมมองความเห็นของทั้ง 2 ฝ่าย พบความเห็นแตกต่างที่น่าสนใจหลายประเด็น ดังนี้

1. ผู้บริหารส่วนใหญ่ (65%) คิดว่าภัยคุกคามที่รุนแรงมากที่สุดคือมัลแวร์ แต่เจ้าหน้าที่ฝ่ายเทคนิคส่วนใหญ่ (35%) กลับคิดว่าเป็นการแฮกบัญชีผู้ใช้งาน ซึ่งเกิดจากสาเหตุ เช่น ผู้ใช้งานตั้งรหัสผ่านที่คาดเดาง่าย หรือใช้รหัสผ่านตั้งต้นที่ได้รับตั้งแต่เริ่มใช้งานโดยไม่ได้เปลี่ยน ซึ่งสอดคล้องกับความเห็นผู้บริหารส่วนใหญ่ที่เคยถูกโจมตีมาแล้วอย่างน้อย 1 ครั้ง และสอดคล้องกลับรายงาน Verizon 2017 Data Breach Investigations จากบริษัท Verizon ก็แสดงให้เห็นว่า 81% ของการโจมตีเกิดจากรหัสผ่านถูกขโมยหรือตั้งรหัสผ่านที่คาดเดาง่าย

2. จากความเห็นที่แตกต่างในแง่ของประเภทภัยคุกคามที่รุนแรงและควรให้ความสำคัญของทั้งสองฝ่าย ก็สะท้อนมาถึงเรื่องการลงทุน โดยผู้บริหารส่วนใหญ่ (60%) คิดว่าควรลงทุนเพื่อป้องกันมัลแวร์

3. ผู้บริหาร (15%) มากกว่าเจ้าหน้าที่เทคนิค (8%) คิดว่าภัยคุกคามที่เกิดในองค์กรส่งผลกระทบรุนแรง แสดงให้เห็นว่าเจ้าหน้าที่อาจไม่ได้รับทราบถึงความเสียหายบางอย่าง การสูญเสียลูกค้า หรือราคาหุ้นขององค์กรตก ซึ่งเป็นเรื่องต้องผู้บริหารอาจพิจารณาสื่อสารให้เข้าใจถึงผลกระทบให้ตรงกัน

4. ในแง่ของอะไรที่เป็นจุดเปลี่ยนให้องค์กรหันมาใส่ใจในเรื่องการรับมือและป้องกันภัยคุกคาม ผู้บริหารส่วนคิดว่า เมื่อเกิดภัยคุกคามขนาดใหญ่ขึ้นกับหน่วยงานของตน (56%) หรือ เมื่อเกิดเหตุการณ์ที่เป็นข่าวใหญ่โต (51%) ในขณะที่เจ้าหน้าที่ฝ่ายเทคนิคส่วนใหญ่ (38%) คิดว่าควรพิจารณาจากงานวิจัยหรือผลสำรวจเกี่ยวกับความเสี่ยงของภัยคุกคามในการอ้างอิง

ผลสำรวจนี้อาจสะท้อนว่าผู้บริหารส่วนใหญ่ให้ความสำคัญในแง่ผลกระทบของบริษัท เช่น ราคาหุ้น ให้ความสำคัญจากข่าวต่างๆ ที่ออกสื่อ ในขณะที่เจ้าหน้าที่เทคนิคจะสนใจในแง่ของความเสี่ยงของการถูกโจมตีในเชิงเทคนิค

5. ผู้บริหารส่วนใหญ่ (54%) ให้ความสำคัญกับคุณภาพการให้บริการลูกค้า และกังวลกับมาตรการด้านความมั่นคงปลอดภัยที่มาส่งผลกระทบ เช่น มาตรการยืนยันตัวตนแบบ 2 ขั้นตอน ซึ่งเป็นมาตรสำคัญที่ช่วยลดความเสี่ยงจากการถูกโจมตีได้มาก ในขณะที่เจ้าหน้าที่เทคนิคในสัดส่วนที่น้อยกว่าที่เห็นด้วย เนื่องจากปัจจุบันมาตรการยืนยันตัวตนแบบ 2 ขั้นตอนสามารถทำให้หลายรูปแบบ เช่น การยืนยันตัวตนด้วยลายนิ้วมือ หรือใบหน้า ซึ่งง่ายต่อผู้ใช้งาน

จะเห็นได้ว่าความแตกต่างของความเห็นระหว่างผู้บริหารกับเจ้าหน้าที่ทางเทคนิค อาจส่งผลถึงการรักษาความมั่นคงปลอดภัยขององค์กร หากทั้งสองฝ่ายลองสื่อสารกันในแง่มุมของตนเพื่อปรับความเข้าใจให้ตรงกัน ก็อาจสามารถช่วยให้องค์กรรับมือภัยคุกคามได้อย่างมีประสิทธิภาพมากขึ้น

Malwarebytes
http://thcert.co/C3CeeU
5/4/2561

MCafee เผยแพร่ข้อแนะนำป้องกันสมาร์ตโฟนถูกแฮก

บริษัทด้านความมั่นคงปลอดภัย MCafee เผยแพร่ข้อแนะนำง่ายๆ สำหรับผู้ใช้ทั่วไปเพื่อป้องกันสมาร์ตโฟนจากการถูกแฮกโดยมีข้อมูลดังนี้

1. ติดตั้งแอปพลิเคชันจากแหล่งที่น่าเชื่อถือ เช่น Google Play หรือ App Store

2. ล็อกมือถือด้วยรหัสผ่าน (Passcode) และเปิดฟังก์ชัน Find my Devices สำหรับอุปกรณ์ระบบปฏิบัติการ Android และฟังก์ชัน Find my iPhone สำหรับอุปกรณ์ระบบปฏิบัติการ iOS เผื่อกรณีอุปกรณ์สูญหาย

3. ล็อกเอาต์หรือจากระบบทุกครั้ง เมื่อเสร็จสิ้นการใช้งาน หลีกเลี่ยงการใช้งานฟังก์ชันจดจำข้อมูลและเติมข้อมูลอัตโนมัติ (Auto-fill)

4. หมั่นทำการอัพเดตเฟิร์มแวร์ซอฟต์แวร์ระบบสม่ำเสมอ เพื่อเพิ่มความปลอดภัยการใช้งาน

5. หลีกเลี่ยงคลิกลิงก์ใด ๆ ที่มีการส่งมายังมือถือของผู้ใช้ หากไม่ทราบแหล่งที่มาอย่างชัดเจน

ข้อแนะนำเหล่านี้ดูเหมือนเป็นเรื่องง่ายๆ แต่เรื่องง่ายๆ เหล่านี้ก็อาจทำให้ผู้ใช้ละเลยไม่ได้ปฏิบัติตาม เช่น การเปิดฟังก์ชันเพื่อค้นหาอุปกรณ์ การล็อกมือถือด้วยรหัสผ่าน มิฉะนั้นเมื่อเกิดเหตุอุปกรณ์สูญหายหรือถูกขโมย ก็อาจส่งผลให้ผู้ประสงค์ร้ายได้ข้อมูลหรือสวมรอยเพื่อกระทำการหลอกลวงผู้อื่นได้ ผู้ใช้สามารถศึกษาข้อแนะนำกรณีอุปกรณ์สูญหายได้จากอินโฟกราฟิกของไทยเซิร์ตได้ที่

https://www.thaicert.or.th/downloads/files/Security_Tips_When_Losing_Mobile.png

Mcafee
http://thcert.co/DX63Nc
13/2/2561

ภาพหลุด เผยรหัสผ่านบนกระดาษแปะหน้าเครื่องคอมห้องปฏิบัติการเฝ้าระวังของหน่วยงานรับมือเหตุฉุกเฉินมลรัฐฮาวาย

เมื่อเดือนมกราคม 2561 ได้มีการเผยแพร่รูปถ่ายบน Twitter ซึ่งเป็นรูปห้องปฏิบัติการเฝ้าระวังเหตุฉุกเฉินของหน่วยงานรับมือเหตุฉุกเฉินในเขตฮาวาย (Hawaii Emergency Management Agency) ประเทศสหรัฐฯ โดยเครื่องคอมพิวเตอร์ที่เฝ้าระวังในรูปพบว่ามีรหัสผ่านเขียนใส่กระดาษแปะไว้

จากเหตุการณ์ดังกล่าวทำให้เกิดความสงสัยในการรักษาความมั่นคงปลอดภัยของหน่วยงาน เนื่องจากก่อนหน้านี้ ได้เกิดเหตุผิดพลาดแจ้งเตือนประชาชนถึงการโจมตีด้วยขีปนาวุธ

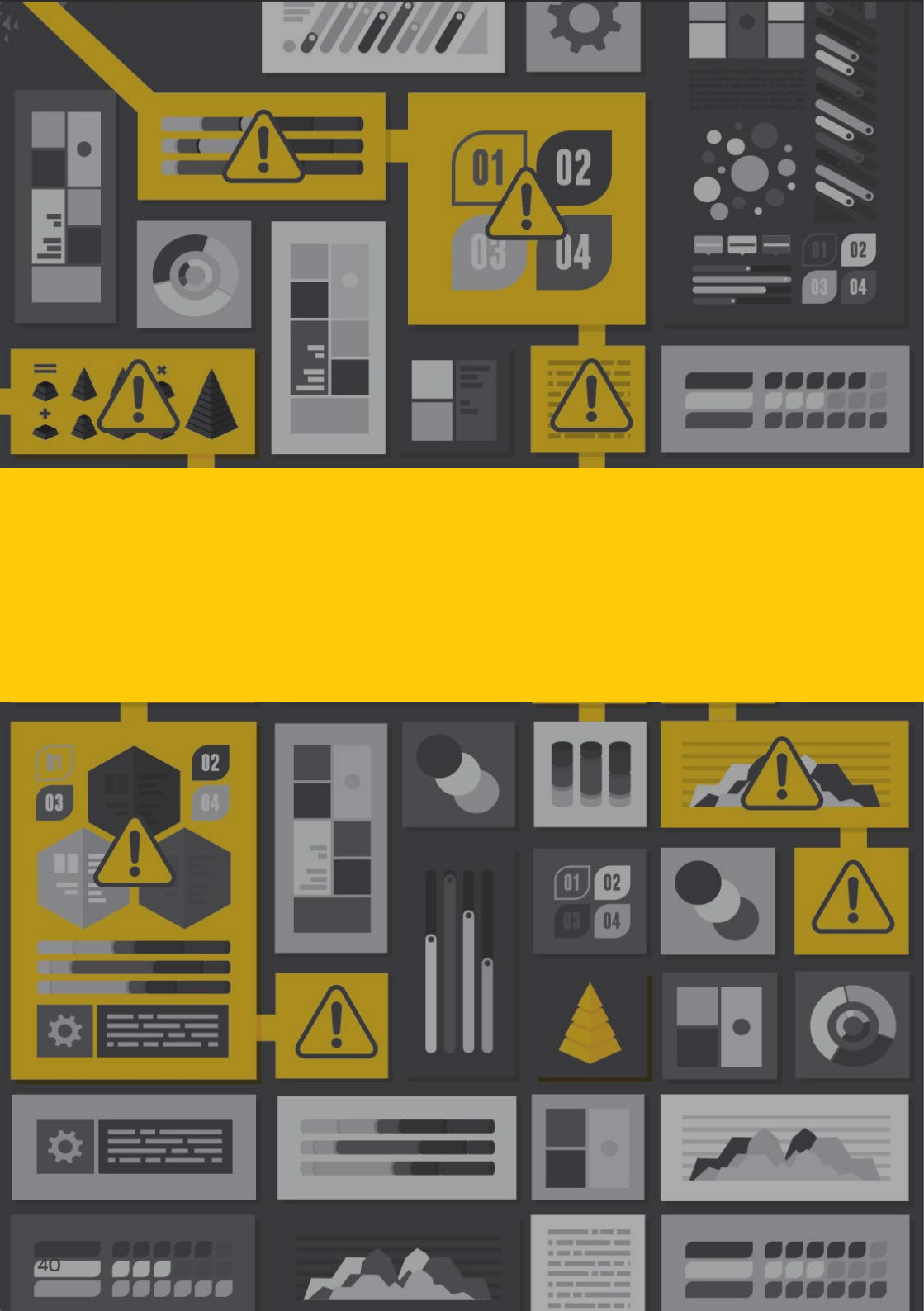
อย่างไรก็ตามทางผู้แทนหน่วยงานได้ชี้แจงว่าความผิดพลาดของการแจ้งเตือนเกิดจากการกดปุ่มผิดของผู้ควบคุมระบบ ส่วนรูปที่เผยแพร่นั้นถูกถ่ายในเดือนกรกฎาคม 2560 และรหัสผ่านในรูปเป็นรหัสผ่านสำหรับแอปพลิเคชันภายใน ซึ่งเชื่อว่าไม่ได้ใช้งานแล้ว และไม่มีส่วนเกี่ยวข้องกับการแจ้งเตือนที่ผิดพลาด

กรณีนี้เป็นตัวอย่างที่ดีในการแสดงให้เห็นว่านอกจากจะมีการระบบป้องกันที่ดี องค์กรควรสร้างความตระหนักให้พนักงานรู้จักเก็บรักษารหัสผ่าน และระวังการเผยแพร่ข้อมูลภายในหน่วยงานสู่สาธารณะ โดยองค์กรเองอาจมีการตรวจสอบเป็นระยะว่าข้อมูลเกี่ยวกับองค์กรที่เผยแพร่อยู่บนอินเทอร์เน็ต มีข้อมูลที่เป็นความลับหรือไม่

สำหรับผู้ที่สนใจสามารถศึกษาคำแนะนำเกี่ยวกับการจัดการรหัสผ่านได้จากอินโฟกราฟิกของไทยเซิร์ต

https://www.thaicert.or.th/downloads/files/info_ThaiCERT_Password_Awareness.pdf

Intelligent Business Insider
http://thcert.co/udCwHu
18/1/2561


01
02
03
04
40


Fraud

แจ้งเตือน อย่าหลงเชื่ออีเมลหลอกลวง อ้างว่าแฮกบัญชีได้และมีรูปแอบถ่ายจากกล้องเว็บแคม ข่มขู่ให้จ่ายเงินด้วย Bitcoin

เมื่อช่วงกลางเดือนตุลาคม 2561 ไทยเซิร์ตได้รับรายงานการแพร่กระจายอีเมลหลอกลวง โดยมีเนื้อหาอ้างว่าผู้ประสงค์ร้ายสามารถเข้าถึงอีเมลของเหยื่อ รายชื่อผู้ติดต่อ บัญชีโซเชียลมีเดีย รวมถึงได้ติดตั้งมัลแวร์และได้แอบถ่ายภาพผ่านกล้องเว็บแคมของเครื่องคอมพิวเตอร์ โดยผู้ประสงค์ร้ายข่มขู่ว่าจะเผยแพร่ข้อมูลดังกล่าวหากไม่จ่ายเงินจำนวน 500 ดอลลาร์ไปยังบัญชี Bitcoin ภายในเวลาที่กำหนด ตัวอย่างข้อความในอีเมลหลอกลวงปรากฏดังรูป

Hello!

My nickname in darknet is gonzalo80.
I hacked this mailbox more than six months ago,
through it I infected your operating system with a virus (trojan) created by me and have been monitoring you for a long time.

If you don't belive me please check 'from address' in your header, you will see that I sent you an email from your mailbox.

Even if you changed the password after that - it does not matter, my virus intercepted all the caching data on your computer
and automatically saved access for me.

I have access to all your accounts, social networks, email, browsing history.
Accordingly, I have the data of all your contacts, files from your computer, photos and videos.

I was most struck by the intimate content sites that you occasionally visit.
You have a very wild imagination, I tell you!

During your pastime and entertainment there, I took screenshot through the camera of your device, synchronizing with what you are watching.
Oh my god! You are so funny and excited!

I think that you do not want all your contacts to get these files, right?
If you are of the same opinion, then I think that $533 is quite a fair price to destroy the dirt I created.

Send the above amount on my BTC wallet (bitcoin): 19D67Tgb3neJiTHd8pZDEBYmUn2qSjxEeB
As soon as the above amount is received, I guarantee that the data will be deleted, I do not need it.

Otherwise, these files and history of visiting sites will get all your contacts from your device.
Also, I'll send to everyone your contact access to your email and access logs, I have carefully saved it!

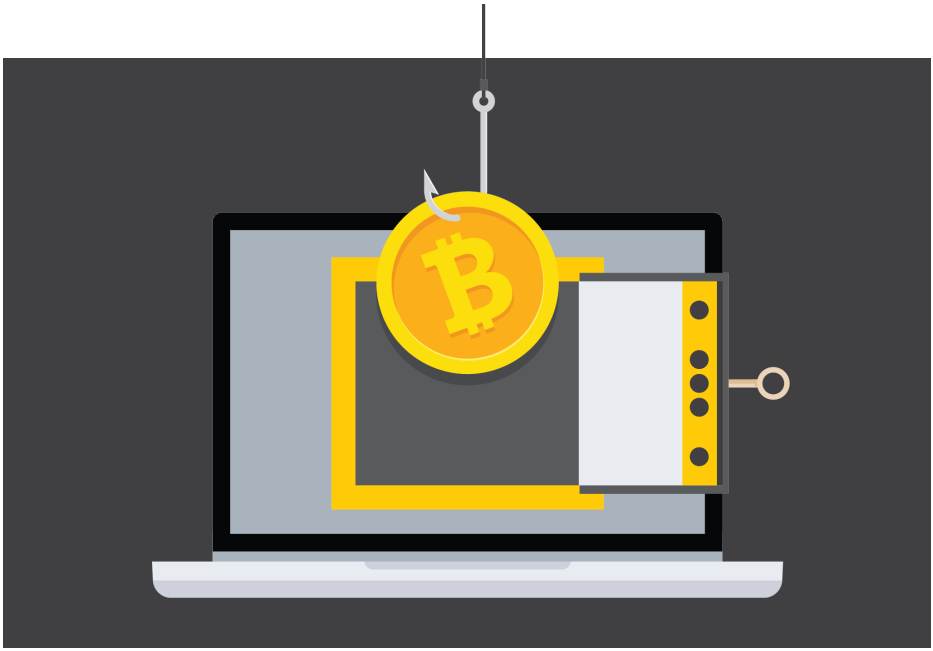
Since reading this letter you have 50 hours!
After your reading this message, I'll receive an automatic notification that you have seen the letter.

I hope I taught you a good lesson.
Do not be so nonchalant, please visit only to proven resources, and don't enter your passwords anywhere!
Good luck!

ThaiCERT
http://thcert.co/3Vrg2x
17/10/2561t

ไทยเซิร์ตได้ดำเนินการตรวจสอบพบว่าอีเมลดังกล่าวเป็นอีเมลหลอกลวง โดยใช้วิธีการปลอมแปลงชื่อผู้ส่ง ซึ่งโปรแกรมป้องกันสแปมส่วนใหญ่จะสามารถคัดกรองอีเมลลักษณะนี้ได้ อย่างไรก็ตาม ในบางระบบอาจมีอีเมลลักษณะนี้หลุดรอดเข้ามาได้ ผู้ดูแลระบบอาจพิจารณาตรวจสอบอีเมลที่มีลักษณะผิดปกติและแจ้งเตือนไปยังผู้ใช้ภายในหน่วยงานของท่านเพื่อไม่ให้หลงเชื่อและดำเนินการจ่ายเงินตามที่ได้มีการข่มขู่ เนื่องจากพบรายงานว่ามีผู้ตกเป็นเหยื่อโอนเงินไปยังบัญชีของผู้ประสงค์ร้ายแล้ว

การส่งอีเมลหลอกลวงเพื่อข่มขู่ให้จ่ายเงินนั้นไม่ใช่เรื่องใหม่ อีกทั้งการปลอมชื่อและที่อยู่ของผู้ส่งอีเมลนั้นก็ไม่ได้ใช้เทคนิคที่ซับซ้อน ผู้ดูแลระบบควรตรวจสอบว่าระบบคัดกรองอีเมลนั้นยังสามารถทำงานได้เพื่อลดความเสี่ยง ในส่วนของผู้ใช้ อาจต้องใช้ความตระหนักและพิจารณาก่อนเชื่อข้อความที่มีลักษณะข่มขู่ให้จ่ายเงิน



ระวัง! เพื่อนเก่า

เป็น friend กันอยู่ จู่ ๆ มาขอแอดใหม่

ถ้ากดรับ อาจเจอดี

- **คิดให้ดีก่อนกดรับ**
  เพราะอาจเป็นผู้ไม่หวังดีนำรูปและข้อมูลโปรไฟล์ของเพื่อนในเฟซบุ๊กมาสวมรอยสร้างบัญชีใหม่
- **หากกดรับอาจเจอ**
  - **โดนส่งสแปม**
    เช่น โฆษณาขยะก่อกวน
  - **หลอกดูข้อมูล**
    ที่ตั้งไว้ให้เห็นได้เฉพาะเพื่อน
  - **ยืมเงินหรือขอให้โอนเงิน**
    ซึ่งเจอบ่อย ๆ

แล้วทำไงดี

- **ถามเพื่อนคนนั้นก่อน** เพราะเขาอาจลืมพาสเวิร์ด หรือบัญชีเก่าถูกแฮกไปเลยตั้งใหม่
- **บล็อกหรือเลิกเป็นเพื่อน**
  บัญชีเก่าที่เขาเลิกใช้หรือถูกแฮกไปแล้ว
- **แนะนำเพื่อน** ว่าก่อนตั้งบัญชีใหม่ เฟซบุ๊กมีบริการช่วยเหลือ
  - จำพาสเวิร์ดไม่ได้
    เข้าไปที่ https://www.facebook.com/help/213395615347144?helpref=faq_content
  - โดนแฮก เข้าไปที่
    https://www.facebook.com/hacked

เพื่อนบอกไม่ใช่บัญชีเขา

- **กด report (แสดงความคิดเห็นหรือรายงานโปรไฟล์นี้)**
  โดยรายงานว่าเป็น "บัญชีปลอม"
- **กดบล็อก**

ป้องกันเรา ป้องกันเพื่อน

- **ตั้งค่าเพื่อนเป็น เป็น "เฉพาะฉัน"**
  (only me) เพื่อไม่ให้ผู้ไม่หวังดีเห็นโปรไฟล์เพื่อนเรา
- **โพสต์อะไร ก็ตั้งเป็นเฉพาะเพื่อน**
  ก็พอ เพื่อเซฟได้อีกระดับนึง

ที่มา: ThaiCERT

ThaiCERT ETDA

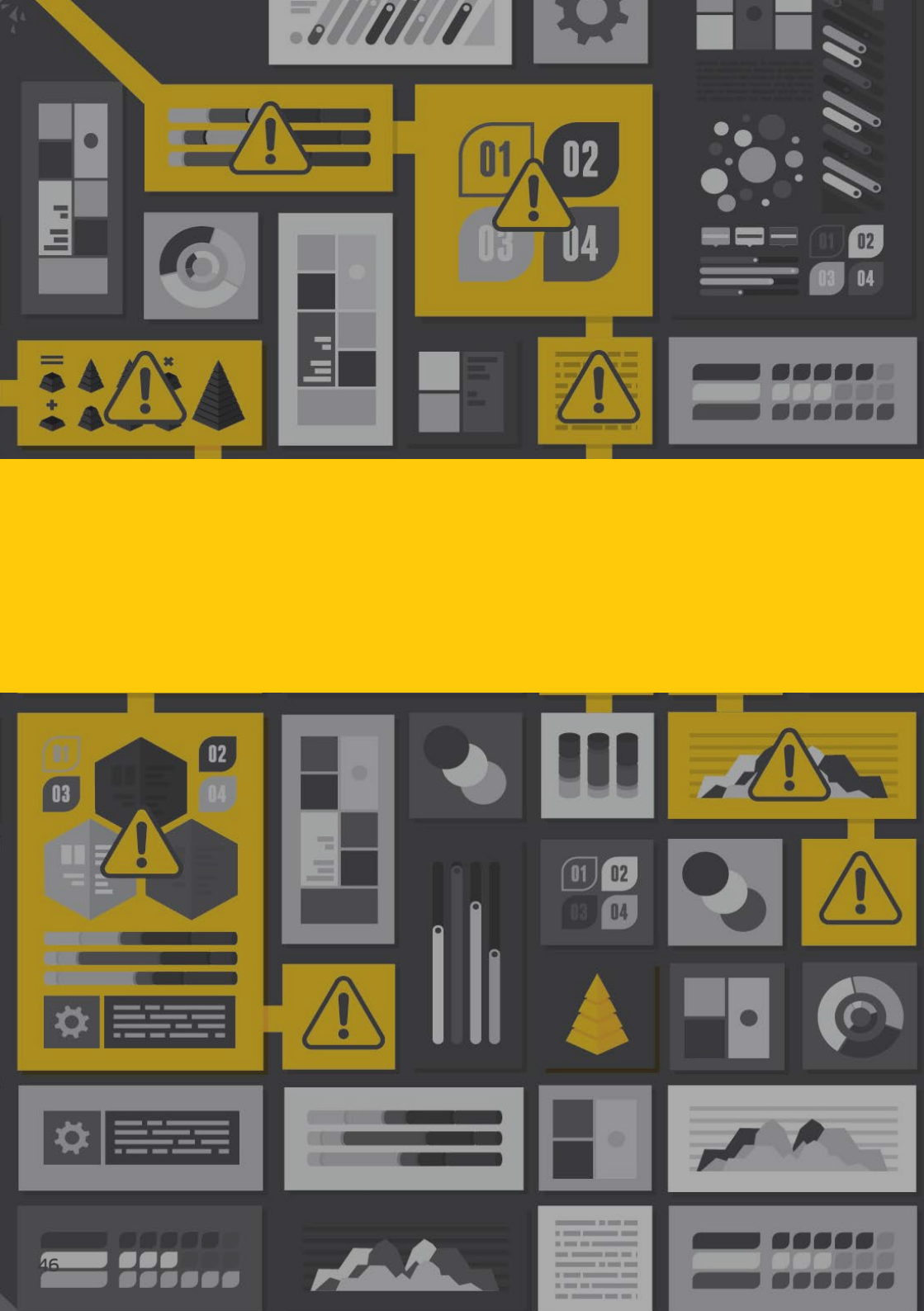
ระวัง พิจารณาก่อนกดรับเพื่อน อาจเป็นผู้ไม่หวังดีสวมรอยสร้างโพรไฟล์เพื่อนใน Facebook เพื่อหลอกยืมเงิน/ขโมยข้อมูล

ผู้ใช้ Facebook ที่ได้รับคำขอเป็นเพื่อนจากคนที่เคยเป็นเพื่อนใน Facebook อยู่แล้ว ควรพิจารณาให้ถี่ถ้วนก่อนกดรับ เนื่องจากมีรายงานว่าผู้ไม่หวังดีใช้วิธีนำรูปและข้อมูลโพรไฟล์ของเพื่อนใน Facebook ของเหยื่อมาสวมรอยสร้างบัญชีใหม่ แล้วกดขอเป็นเพื่อนกับเหยื่อ จุดประสงค์ของการกระทำนี้มีตั้งแต่เพื่อใช้ส่งสแปม หลอกดูข้อมูลที่ถูกตั้งไว้ให้เห็นได้เฉพาะเพื่อน ไปจนถึงหลอกขอให้โอนเงิน ซึ่งกรณีหลังสุดนี้มีรายงานผู้ได้รับความเสียหายมาอยู่เรื่อยๆ

อย่างไรก็ตาม เป็นไปได้ว่าเพื่อนของเราอาจลืมรหัสผ่านเข้าใช้งานบัญชี หรือบัญชีถูกแฮก จึงจำเป็นต้องสร้างบัญชีใหม่ขึ้นมาเพื่อใช้งาน ในกรณีนี้ ควรตรวจสอบให้แน่ใจว่าบัญชีที่ติดต่อเข้ามาขอเพิ่มเป็นเพื่อนใหม่นั้นเป็นของเพื่อนเราจริงๆ และอาจพิจารณาบล็อคหรือเลิกเป็นเพื่อนกับบัญชีที่ถูกแฮกหรือไม่มีการใช้งานแล้ว เพื่อป้องกันปัญหาข้อมูลรั่วไหล ทั้งนี้ ทาง Facebook มีบริการช่วยเหลือในกรณีที่บัญชีถูกแฮกหรือลืมรหัสผ่าน ซึ่งอาจแนะนำให้เพื่อนลองติดต่อกับทาง Facebook เพื่อแก้ไขปัญหาก่อนที่จะสร้างบัญชีใหม่ขึ้นมาเพิ่ม

ในกรณีที่พบว่ามีการสร้างบัญชีปลอมสวมรอยเป็นเพื่อน สามารถบล็อคและแจ้งรายงานให้ทาง Facebook ทราบ โดยระบุว่าเป็นบัญชีปลอม เพื่อให้ตรวจสอบและระงับบัญชีดังกล่าว ก่อนที่จะเกิดความเสียหายกับบุคคลอื่น

Naked Security
http://thcert.co/q2lNUs
11/10/2561


01
02
03
04


Incident

แจ้งเตือนการโจมตีทางไซเบอร์ Operation Sharpshooter มุ่งเป้าเจาะระบบหน่วยงานด้านความมั่นคงและโครงสร้างพื้นฐานสำคัญของประเทศ

เมื่อวันที่ 12 ธันวาคม 2561 บริษัท McAfee ได้เผยแพร่รายงาน Operation Sharpshooter ระบุถึงการโจมตีทางไซเบอร์ที่มุ่งเป้าไปยังหน่วยงานด้านนิวเคลียร์ การเงิน ความมั่นคง และพลังงาน โดยทาง McAfee พบว่ามัลแวร์แพร่กระจายไปยังหน่วยงาน 87 แห่งทั่วโลกรวมถึงประเทศไทย ตั้งแต่ช่วงเดือนตุลาคมถึงพฤศจิกายน ส่วนใหญ่เป็นหน่วยงานด้านความมั่นคงหรือหน่วยงานที่มีความเกี่ยวข้องกับรัฐบาล (อยู่ระหว่างตรวจสอบเพื่อยืนยันข้อมูลหน่วยงานที่ได้รับผลกระทบ)

รูปแบบการโจมตีจะใช้วิธีหลอกให้เหยื่อเปิดไฟล์ Microsoft Word ที่หลอกว่าเป็นเอกสารที่เกี่ยวข้องกับการรับสมัครงาน ช่องทางแพร่กระจายจะอัปโหลดไฟล์ Microsoft Word ขึ้นไปไว้บน Dropbox โดยในไฟล์ Word จะมีโค้ดอันตรายฝังอยู่ หากผู้ใช้เปิดไฟล์ดังกล่าวและอนุญาตให้มีการใช้งาน Macro โค้ดอันตรายจะถูกเรียกขึ้นมาทำงานเพื่อดาวน์โหลดไฟล์มัลแวร์จากเซิร์ฟเวอร์ภายนอกมาติดตั้งลงในเครื่องอีกทีหนึ่ง ตัวมัลแวร์นี้ทาง McAfee ตั้งชื่อว่า Rising Sun มีความสามารถในการฝังตัวเพื่อขโมยข้อมูลและส่งออกไปยังเซิร์ฟเวอร์ภายนอก ตัวอย่างข้อมูลที่ถูกส่งออกไปโดยหลัก ๆ จะเป็นรายละเอียดเบื้องต้นของเครื่องที่ติดมัลแวร์ เช่น ชื่อเครื่อง ชื่อบัญชีผู้ใช้ ที่อยู่ไอพี เวอร์ชันของระบบปฏิบัติการ เป็นต้น โดยข้อมูลที่ถูกส่งออกไปจะถูกเข้ารหัสลับเพื่อไม่ให้สามารถถูกตรวจจับความผิดปกติได้

ทาง McAfee ได้เผยแพร่ข้อมูล IOC สำหรับใช้ตรวจสอบและป้องกันการโจมตี โดยประกอบด้วยค่าแฮชของไฟล์ที่เกี่ยวข้อง ที่อยู่ไอพีและโดเมนของเซิร์ฟเวอร์ที่ใช้ควบคุมและสั่งการเครื่องที่ติดมัลแวร์ หน่วยงานที่อยู่ในกลุ่มเสี่ยงที่ว่ามีโอกาสตกเป็นเป้าหมายของการโจมตีควรเฝ้าระวัง อัปเดตข้อมูลสำหรับใช้ในการตรวจจับการโจมตีและอัปเดตระบบอย่างสม่ำเสมอ

McAfee
http://thcert.co/E3sMX0
McAfee
http://thcert.co/O1lDmk
14/12/2561

Facebook แถลงเพิ่มเติมเรื่องข้อมูลหลุด มีผลกระทบประมาณ 30 ล้านบัญชี

จากเหตุการณ์ผู้ใช้ Facebook กว่า 50 ล้านบัญชีถูกแฮก ส่งผลให้มีโอกาสข้อมูลรั่วไหล (ข่าวเก่า https://www.thaicert.or.th/newsbite/2018-10-01-01.html) เมื่อวันที่ 12 ตุลาคม 2561 ทาง Facebook ได้ออกแถลงการณ์เพิ่มเติมเรื่องผลกระทบจากกรณีดังกล่าว โดยจากการตรวจสอบพบว่ามีจำนวนผู้ได้รับผลกระทบอยู่ที่ประมาณ 30 ล้านบัญชี ข้อมูลที่หลุดรั่วออกไปส่วนใหญ่เป็นข้อมูลที่เฉพาะเจ้าของบัญชีเท่านั้นถึงจะมีสิทธิ์เห็น เช่น ข้อมูลผู้ใช้ที่ถูกตั้งค่าไว้เป็นส่วนตัว วันเกิด หมายเลขโทรศัพท์ รายชื่อบุคคลที่คุยด้วยใน Messenger ข้อความที่ค้นหาล่าสุด เป็นต้น อย่างไรก็ตาม ข้อมูลสำคัญอื่นๆ เช่น รหัสผ่าน หรือ หมายเลยบัตรเครดิตไม่ได้หลุดรั่วออกไปด้วย ทั้งนี้ ผู้ใช้แต่ละคนอาจได้รับผลกระทบไม่เท่ากัน ซึ่งทาง Facebook แจ้งว่าจะส่งข้อความแจ้งเตือนไปยังผู้ใช้ที่ถูกแฮกตามผลกระทบที่ได้รับ

อ้างอิงข้อมูลจากเว็บไซต์ TechCrunch ผู้ที่ไม่แน่ใจว่าบัญชีของตนเองเข้าข่ายได้รับผลกระทบหรือไม่ สามารถตรวจสอบได้จากหน้าเว็บไซต์ (https://www.facebook.com/help/securitynotice) โดยเลื่อนลงมาด้านล่างสุด หากพบข้อความ

Is my Facebook account impacted by this security issue?

Based on what we've learned so far, your Facebook account has not been impacted by this security incident. If we find more Facebook accounts were impacted, we will reset their access tokens and notify those accounts.

แสดงว่าไม่ได้รับผลกระทบจากเหตุการณ์นี้ แต่หากพบว่าเป็นหนึ่งในผู้ที่ได้รับผลกระทบ ทาง Facebook จะแจ้งว่ามีข้อมูลใดหลุดบ้างและควรดำเนินการอย่างไรต่อไป เช่น ติดต่อธนาคารหรือผู้ให้บริการโทรศัพท์มือถือในกรณีที่ข้อมูลส่วนตัวรวมถึงหมายเลขโทรศัพท์รั่วไหล

Facebook
http://thcert.co/9bF0cJ
TechCrunch
http://thcert.co/4MNrVh
12/10/2561

บัญชี Facebook ถูกแฮกเกือบ 50 ล้านบัญชี จากช่องโหว่การใช้งาน View As

เมื่อวันที่ 25 กันยายน 2561 ที่ผ่านมา ทีมวิศวกรของ Facebook ตรวจพบช่องโหว่ ซึ่งมีผลกระทบต่อบัญชีผู้ใช้เกือบ 50 ล้านบัญชี จากการตรวจสอบพบว่าผู้ประสงค์ร้ายได้โจมตีผ่านช่องโหว่การใช้งาน View As ซึ่งเป็นคุณลักษณะที่ช่วยให้เจ้าของบัญชีสามารถมองเห็นว่าโปรไฟล์ของตนเองมีลักษณะอย่างไรกับผู้อื่น ทำให้ผู้ประสงค์ร้ายขโมย access token ของบัญชี Facebook ได้

สิ่งที่ Facebook ได้ดำเนินการ

1. แก้ไขช่องโหว่ดังกล่าว และแจ้งผู้บังคับใช้กฎหมาย

2. ดำเนินการ reset access token เกือบ 50 ล้านบัญชีที่พบว่าได้รับผลกระทบ และอีก 40 ล้านบัญชีที่ตรวจสอบแล้วพบว่ามีการใช้งาน View As ในรอบปีผ่านมา ทำให้มีจำนวนทั้งสิ้น 90 ล้านบัญชีที่ต้องลงชื่อเข้าใช้งานใหม่

3. ปิดการใช้งาน View As เพื่อตรวจสอบอย่างละเอียด

ทั้งนี้ผู้ใช้ Facebook ไม่จำเป็นต้องเปลี่ยนรหัสผ่าน เพราะ Facebook แก้ไขช่องโหว่แล้ว แต่ผู้ที่มีปัญหาในการลงชื่อหรือล็อกอิน เช่น ลืมรหัสผ่าน สามารถดูรายละเอียด เพื่อเข้าถึงบัญชีได้ที่ Help Center https://www.facebook.com/help/105487009541643

Facebook
http://thcert.co/p4eV5J
1/10/2561

Tech Bureau บริษัทให้บริการแลกเปลี่ยนสกุลเงินคริปโตญี่ปุ่นถูกโจมตี สูญเงินมูลค่ากว่า 1,900 ล้านบาท

เมื่อเดือนกันยายน 2561 Tech Bureau บริษัทญี่ปุ่นที่ให้บริการแลกเปลี่ยนสกุลเงินคริปโตได้รายงานว่า บริษัทถูกโจมตีทางไซเบอร์และถูกขโมยเงินมูลค่ากว่า 1,900 ล้านบาท โดยการโจมตีเกิดเมื่อวันที่ 14 ถูกตรวจพบในวันที่ 17 และบริษัทรายงานการโจมตีให้หน่วยงานภาครัฐรับทราบในวันที่ 20 กันยายน

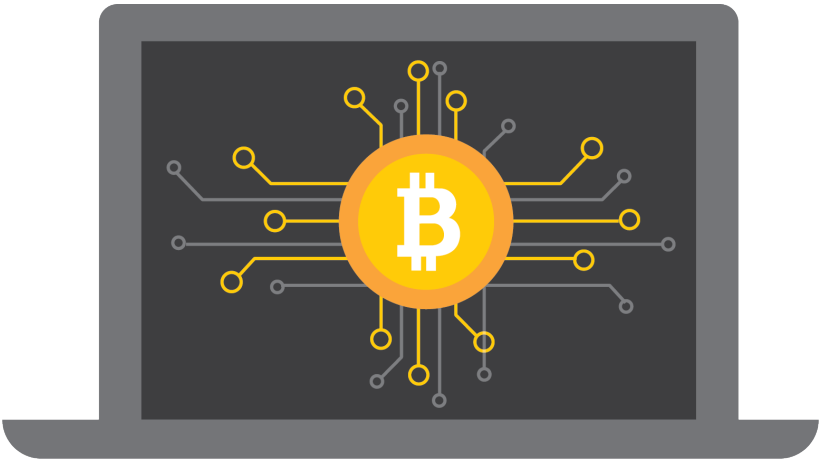
ญี่ปุ่นเป็นประเทศแรกที่รัฐบาลให้ความสำคัญและเริ่มกำกับดูแลการแลกเปลี่ยนสกุลเงินคริปโต บริษัทที่ต้องการให้บริการดังกล่าวต้องได้รับอนุญาตและขึ้นทะเบียนจาก FSA หรือ Financial Service Agency โดย FSA แจ้งว่ามี 160 กว่าหน่วยงานที่สนใจให้บริการ แต่ตั้งแต่เดือนธันวาคม 2561 ไม่พบว่า FSA อนุมัติบริษัทใด ๆ ให้เปิดบริการ

ก่อนหน้าที่ Tech Bureau Corp จะถูกโจมตี หน่วยงานกำกับได้ออกคำสั่ง เพื่อปรับปรุงการให้บริการ 2 ครั้ง และหลังจากเกิดการโจมตีดังกล่าวหน่วยงานกำกับได้เข้ามาตรวจสอบอย่างเร่งด่วนในการจัดการความมั่นคงปลอดภัยของบริษัทอื่นที่ให้บริการสกุลคริปโต

บริษัทแลกเปลี่ยนสกุลเงินคริปโตเป็นหนึ่งในเป้าหมายการโจมตีทางไซเบอร์เพื่อจุดประสงค์ทางการเงิน ก่อนหน้านี้เมื่อเดือนมกราคม 2561 Coincheck บริษัทญี่ปุ่นที่ให้บริการนี้ก็ถูกโจมตีและถูกขโมยเงินมูลค่ากว่า 17,000 ล้านบาท ผู้ที่ให้บริการจึงควรให้ความสำคัญกับการดูแลความมั่นคงปลอดภัย ในขณะที่ผู้ใช้บริการก็ควรพิจารณาความเสี่ยง นำเงินออกจากเว็บไซต์หลังจากแลกเปลี่ยนสกุลเงินเสร็จ เพื่อลดโอกาสการถูกขโมยเงิน

ในประเทศไทยเริ่มมีผู้ให้บริการแลกเปลี่ยนสกุลเงินคริปโตแล้ว มีหลายหน่วยงานเริ่มสนใจที่จะให้บริการด้านนี้ และหน่วยงานภาครัฐมีการกำกับดูแลเช่นกัน เช่น เมื่อวันที่ 24 กันยายน บริษัท ซุปเปอร์ริช เคอเรน ซี่ เอ็กซ์เชนจ์ (1965) จำกัด (Superrich สีส้ม) ได้ประกาศว่ากำลังเตรียมความพร้อม โดยอยู่ระหว่างการขออนุมัติจากสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์หรือ ก.ล.ต ซึ่งที่ผ่านมา ก.ล.ต. ได้อนุมัติผู้ให้บริการเว็บไซต์แลกเปลี่ยนสกุลเงินคริปโต 8 รายการ

นอกจากนี้สำหรับผู้ที่สนใจสามารถศึกษาข้อมูลพื้นฐานเกี่ยวกับสกุลเงินคริปโตได้จากเอกสาร Digital Currency Series Vol.1
https://www.bot.or.th/Thai/MonetaryPolicy/ArticleAndResearch/FAQ/FAQ_124.pdf



Reuters
<http://thcert.co/RBwV7S>
efinianceThai
<http://thcert.co/xT9Yx5>
27/9/2561

พบการโจมตีครั้งใหม่จากกลุ่ม Cobalt มุ่งเป้าธนาคารในรัสเซียและโรมาเนีย

ในเดือนสิงหาคม นักวิจัยได้ค้นพบการโจมตีอีกครั้งจากกลุ่มแฮกเกอร์ที่ชื่อ Cobalt โดยมุ่งเป้าโจมตีธนาคารในประเทศรัสเซียและโรมาเนีย โดยใช้รูปแบบการส่งอีเมลไปยังเป้าหมายเพื่อเผยแพร่มัลแวร์

กลุ่มแฮกเกอร์ดังกล่าวเริ่มปฏิบัติการตั้งแต่ปี 2559 โดยมุ่งเป้าไปที่หน่วยงานภาคการเงิน จากข้อมูลของ Europol พบว่ามีความเกี่ยวข้องกับการโจมตีกับธนาคารอย่างน้อย 100 แห่งและขโมยเงินประมาณ 1 พันล้านยูโรหรือ 40,000 ล้านบาท

สำหรับการโจมตีในเดือนสิงหาคมที่พบเป็นรูปแบบ Spear Phishing* แฮกเกอร์ได้เลือกเหยื่อไว้ล่วงหน้าซึ่งเป็นเจ้าหน้าที่ธนาคารเพื่อส่งอีเมลหลอกลวง ในอีเมลมี 2 ลิงก์ คือลิงก์สำหรับดาวน์โหลดไฟล์เอกสารนามสกุล doc ซึ่งมีสคริปต์ VBA ที่ผู้ประสงค์ร้ายฝังไว้ เมื่อเปิดไฟล์ด้วย Microsoft Word จะปรากฏข้อความถามเพื่อเปิดใช้งาน Macro หากเหยื่อตกลงก็จะทำให้สคริปต์ดังกล่าวทำงานและดาวน์โหลดมัลแวร์มายังเครื่อง ส่วนลิงก์ที่โหลดสำหรับดาวน์โหลดไฟล์ที่ดูเหมือนเป็นไฟล์รูปภาพ มีนามสกุลเป็น jpg แต่ที่จริงแล้วเป็นไฟล์โปรแกรมซึ่งหากเปิดไฟล์ก็จะทำให้ติดมัลแวร์เช่นกัน

มัลแวร์ที่แอบอยู่ในเครื่องจะรับคำสั่งและส่งข้อมูลไปให้แฮกเกอร์ เรียนรู้สภาพแวดล้อมของระบบต่าง ๆ และเครือข่ายขององค์กร เพื่อหาช่องทางในการเจาะระบบสำคัญหรือบัญชีที่มีสิทธิระดับสูง เพื่อดำเนินการขโมยเงินผ่านระบบ SWIFT หรือ ATM ต่อไป

รูปแบบการเผยแพร่มัลแวร์ด้วยสคริปต์ที่ฝังอยู่ใน microsoft word เป็นหนึ่งในการรูปแบบการโจมตีที่ค่อนข้างพบ ในระดับองค์กรอาจพิจารณาควบคุมไม่ให้พนักงานเปิดใช้งาน Macro หากไม่ได้มีการใช้งาน ผู้ที่สนใจสามารถศึกษารายละเอียดการโจมตี รวมถึงข้อมูลที่ใช้การตรวจจับการโจมตี (IoC) ในครั้งนี้ได้จากที่มา

https://www.thaicert.or.th/papers/general/2012/pa2012ge007.html

Bleeping Computer
http://thcert.co/98jxSR
Arbor
http://thcert.co/Q3ZmFR
31/8/2561

FBI ออกโรงเตือนอาชญากรไซเบอร์ หลอกขโมยรหัสผ่านเข้าระบบ HR เพื่อเปลี่ยนบัญชีธนาคารรับเงินเดือน

เอฟบีไอได้แจ้งเตือนการเพิ่มขึ้นของอาชญากรทางอินเทอร์เน็ตเพื่อเข้าถึงข้อมูลเงินเดือนของพนักงานบริษัท ในปี 2560 พบเหยื่อ 17 ราย แต่ในเดือนกรกฎาคม 2561 ที่ผ่านมา ได้พบเหยื่อ 47 ราย ถูกหลอกโอนเงิน มีมูลค่าความเสียหายรวมประมาณ 1 ล้านเหรียญสหรัฐหรือ 33 ล้านบาท และหน่วยงานต่าง ๆ มีโอกาสที่จะได้รับผลกระทบนี้ ไม่จำกัดเฉพาะกลุ่มของ มหาวิทยาลัย โรงเรียน ระบบการดูแลสุขภาพ และการขนส่งทางอากาศ

โดยเอฟบีไอได้ตั้งข้อสังเกตพบว่ามีสองวิธี ที่กลุ่มอาชญากรใช้เพื่อเข้าถึง และแก้ไขข้อมูลการเงินของพนักงานได้ คือ ผ่านทางฟิชชิงอีเมล และผ่านการชักชวนทางโทรศัพท์ (ลักษณะคล้ายแก๊งค์คอลเซ็นเตอร์ หลอกถามข้อมูล หรือหลอกให้โอนเงิน)

รูปแบบวิธีการที่อาชญากรนำมาใช้

อาชญากรใช้วิธีการเปลี่ยนแปลงบัญชีเงินเดือนปลายทางเพื่อรับโอนเงินจากบริษัทเป้าหมาย โดยการใช้ข้อมูลส่วนตัวของพนักงานเพื่อเข้าถึงระบบจ่ายเงินเดือน เปลี่ยนแปลงข้อมูลหมายเลขบัญชีธนาคารที่รับเงินเดือนหรือสั่งจ่ายไปยังบัญชีบัตรเติมเงินปลายทางที่อาชญากรสามารถควบคุมได้

รูปแบบแรก เป็นวิธีการได้มาของข้อมูลประจำตัวของเหยื่อมีการเจาะจงเป้าหมายโดยการส่งอีเมลที่มีลิงก์ไปยังฟิชชิ่งเว็บไซต์หรือแนบไฟล์เอกสารนามสกุล pdf เพื่อหลอกให้ผู้ใช้เข้าไปยังฟิชชิ่งเว็บไซต์ ในกรณีนี้ส่วนใหญ่มีการปลอมแปลงลักษณะหน้าเว็บไซต์ให้คล้ายกับบริการซอฟต์แวร์ที่ฝ่ายบุคคลใช้งาน เพื่อให้เหยื่อหลงเชื่อและป้อนรหัสผ่านสำหรับล็อกอินเข้าสู่ระบบของตน จากนั้นอาชญากรนำรหัสผ่านที่ได้ ล็อกอินเข้าใช้บัญชีของพนักงาน และเปลี่ยนแปลงหมายเลขบัญชีธนาคารสำหรับรับเงินเดือน ทำให้เงินเดือนถูกโอนไปยังบัญชีธนาคารปลายทางตามข้อมูลที่ระบุ

รูปแบบที่สอง การใช้วิธีการทาง Social Engineer ด้วยการติดต่อไปยังบริการสายด่วนพนักงาน เพื่อขอให้บริษัททำการรีเซ็ตรหัสผ่าน โดยการแจ้งหมายเลขประจำตัวลูกจ้าง และหมายเลขประกันสังคมสี่ตัวสุดท้ายของเหยื่อเพื่อใช้สำหรับเข้าถึงข้อมูลทางการเงินของเหยื่อต่อไป

จากการตรวจสอบพบว่ามีการจ่ายเงินเดือนจำนวน 205 รายการ ที่โอนเงินไปยังบัตรเติมเงินของอาชญากรไซเบอร์ นอกจากนี้ ยังพบว่าระยะเวลาเฉลี่ยตั้งแต่เปิดใช้งานบัตรเติมเงินเพื่อรับโอนเงินฝากคือ 54 วัน และอย่างน้อยที่สุดคือ 1 วัน

ข้อแนะนำสำหรับองค์กรเพื่อป้องกัน

1. ควรแจ้งเตือนพนักงานให้ทราบถึงรูปแบบการหลอกลวงของภัยคุกคามนี้ เพื่อให้รู้ทัน

2. เมื่อระบบพบการร้องเพื่อขอเปลี่ยนแปลงข้อมูลบัญชีธนาคารเพื่อรับเงินเดือน ควรมีการตรวจสอบอย่างเข้มงวด

ให้ความรู้แก่บุคลากรเกี่ยวกับการดำเนินการเชิงป้องกัน และการแก้ไขที่เหมาะสมกับแผนการก่ออาชญากรรมที่มาในรูปแบบของ Social Engineer

3. แนะนำพนักงานในกรณีได้รับอีเมลที่ขอข้อมูลสำหรับเข้าสู่ระบบ เช่น รหัสผ่าน ไอดี ให้หลีกเลี่ยงการให้ข้อมูล และดำเนินการส่งต่อข้อมูลที่น่าสงสัยเกี่ยวกับการร้องขอข้อมูลส่วนบุคคลไปที่แผนกไอที หรือแผนกทรัพยากรบุคคล ให้ช่วยตรวจสอบ

แนะนำพนักงานให้ตั้งรหัสผ่านของระบบที่ใช้สำหรับการจ่ายเงินเดือน แตกต่างจากรหัสผ่านที่ใช้ในบัญชีทั่วไป

4. ตรวจสอบการเข้าสู่ระบบของพนักงานที่เกิดขึ้นนอกเวลาทำการปกติ

5. จำกัดการเข้าถึงอินเทอร์เน็ตในระบบจัดการข้อมูลที่สำคัญ

6. สำหรับระบบและข้อมูลสำคัญ ควรใช้งานรูปแบบการยืนยันตัวตนแบบสองขั้นตอน

7. พนักงานสามารถดำเนินการจัดการข้อมูลที่สำคัญได้ บนระบบที่อนุญาตเท่านั้น เช่น เครื่อง Terminal ที่เตรียมไว้ให้

FBI
http://thcert.co/Rubrcm
17/8/2561

FBI แจ้งเตือนปฏิบัติการ Unlimited เจาะระบบธนาคารเพื่อปลดล็อกการจำกัดจำนวนถอนเงินผ่านตู้ ATM

เมื่อช่วงต้นเดือนสิงหาคม FBI ได้แจ้งเตือนปฏิบัติการโจมตีทางไซเบอร์ที่ชื่อ Unlimited เพื่อขโมยเงินจากธนาคาร โดยการโจมตีเริ่มจากผู้ประสงค์ร้ายเจาะระบบธนาคารเพื่อ

1) ปลดล็อกการควบคุม เช่น การจำกัดจำนวนเงินหรือจำนวนครั้งที่สามารถถอนได้จากตู้ ATM
2) เปลี่ยนจำนวนเงินในบัญชีและมาตรการควบคุมเพื่อให้สามารถถอนเงินได้อย่างไม่จำกัดจากตู้ ATM ต่าง ๆ อย่างรวดเร็ว

จากนั้นผู้ประสงค์ร้ายขโมยข้อมูลบัตร ATM หรือบัตรเครดิตของลูกค้า เพื่อนำไปสร้างบัตรแล้วนำไปถอนเงินตามตู้ ATM ในประเทศต่าง ๆ โดยมีการทำงานเป็นทีม นัดหมายกันเพื่อถอนเงินจากตู้ ATM ต่าง ๆ ในวันเวลาที่กำหนด โดยมักเริ่มปฏิบัติการในช่วงวันหยุดสุดสัปดาห์ โดยเฉพาะวันเสาร์ ช่วงเวลาธนาคารใกล้ปิดทำการ

การแจ้งเตือนของ FBI นี้มีความสัมพันธ์กับเหตุการณ์ ธนาคาร Cosmos ประเทศอินเดียถูกโจมตีด้วยปฏิบัติการดังกล่าวในช่วงวันที่ 11 ถึง 13 สิงหาคม 2561 ถูกขโมยเงินผ่านตู้ ATM ในประเทศแคนาดา ฮ่องกง และอินเดีย จำนวน 12,000 ครั้ง รวมเงินที่ถูกขโมยเป็นจำนวนประมาณ 940 ล้านรูปีหรือ 450 ล้านบาท และก่อนหน้านี้พบแฮกเกอร์เจาะระบบธนาคาร Blacksburg ซึ่งเป็นธนาคารแห่งชาติของประเทศสหรัฐฯ ในสาขาเล็ก เพื่อเข้าถึงระบบจัดการบัตรเครดิตและเดบิตที่ผูกกับบัญชีลูกค้า และได้ขโมยเงิน 2 ครั้ง จากการถอนเงินตู้ ATM รวมมูลค่า 2.4 ล้านดอลล่าร์หรือ 80 ล้านบาท ในช่วงระหว่างเดือนพฤษภาคม 2560 ถึงเดือนมกราคม 2561

ทาง FBI ได้ให้คำแนะนำแก่ธนาคารดังนี้

1. แยกหน้าที่ผู้ที่มีหน้าที่เพิ่มจำนวนเงินที่ถอนได้สูงสุดต่อวันหรือปรับจำนวนเงินในบัญชี ออกจากการทำหน้าที่อื่น รวมถึงเฝ้าระวังบัญชีของผู้ที่มีสิทธิดังกล่าว

2. จำกัดให้เฉพาะรายการแอปพลิเคชันที่กำหนดไว้เท่านั้นที่สามารถทำงานได้ (application whitelisting) เพื่อป้องกันไม่ให้มัลแวร์ทำงาน

3. เฝ้าระวังเครื่องมือของผู้ประสงค์ร้ายที่แอบวางไว้ในระบบเพื่อเชื่อมต่อเข้ามาควบคุมหรือสั่งการเครื่องจากระยะไกล เช่น Powershell, Cobalt Strike และ TeamViewer

4. เฝ้าระวังทราฟฟิคการเชื่อมต่อรูปแบบ SSL หรือ TLS ด้วยพอร์ตหมายเลขที่ไม่ได้ใช้งานทั่วไป (non-standard port)

5. เฝ้าระวังทราฟฟิคขาออกจากธนาคารไปยังปลายทางที่น่าสงสัย

หากผู้ใช้พบเห็นการถอนเงินจำนวนมากจากตู้ ATM เกินจำกัดอย่างผิดปกติ สามารถแจ้งไทยเซิร์ตได้ที่ 02-123-1212 เพื่อประสานงานดำเนินการตรวจสอบต่อไป

KrebsOnSecurity
http://thcert.co/Xytp7C
17/8/2561

พบกลุ่มปฏิบัติการโจมตีใหม่ Rancor มุ่งเป้าโจมตีเฉพาะเพื่อขโมยข้อมูลในประเทศสิงค์โปร์และกัมพูชา

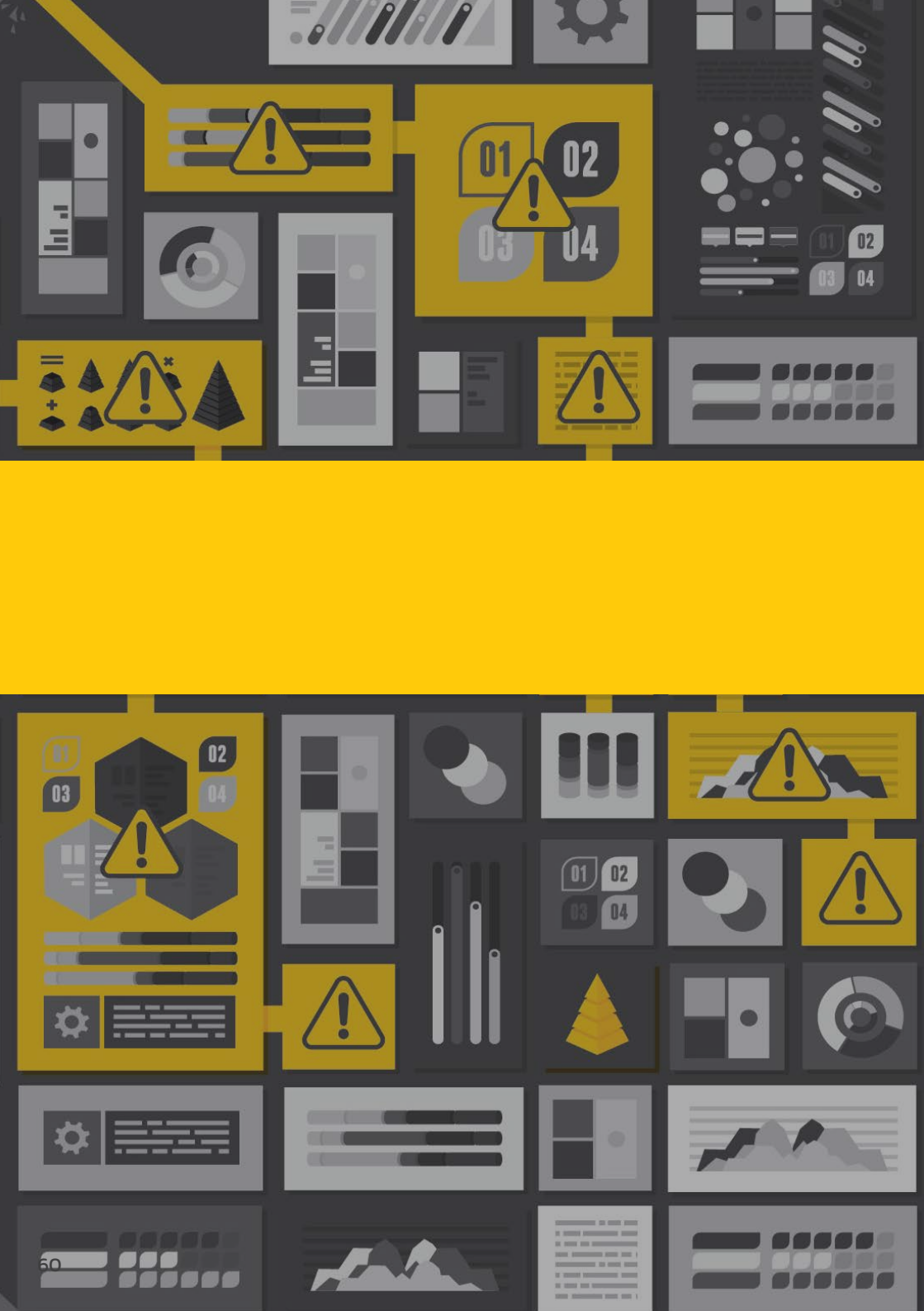
บริษัท Palo Alto ได้เผยแพร่การค้นพบปฏิบัติการโจมตีทางไซเบอร์โจมตีในประเทศสิงคโปร์ และกัมพูชา โดยตั้งชื่อกลุ่มผู้โจมตีว่า Rancor เชื่อว่ากลุ่มดังกล่าวมีเป้าหมายเฉพาะโจมตีหน่วยงานหรือบุคคลที่เกี่ยวข้องกับการเมืองเพื่อขโมยข้อมูล

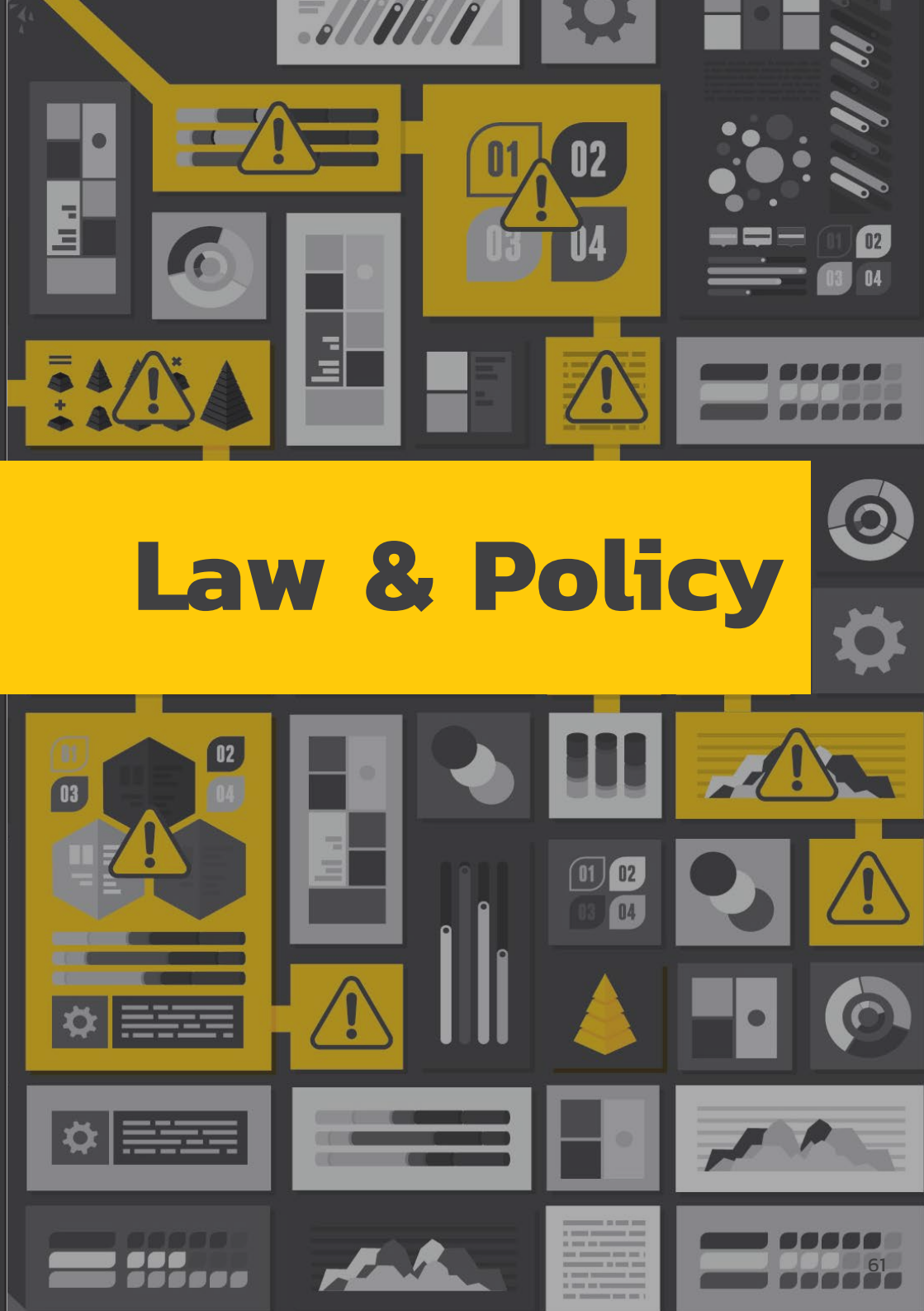
ผู้ประสงค์ร้ายได้ใช้ไฟล์ 3 ประเภท ในการเริ่มต้นโจมตีเพื่อดาวน์โหลดมัลแวร์ ได้แก่ไฟล์เอกสารประเภท Excel ที่มีโค้ดอันตรายในรูปแบบ Macro หากผู้ใช้เปิดไฟล์และเปิดใช้งาน Macro ก็จะประมวลผลโค้ดอันตรายดังกล่าวไฟล์แนบอีเมลประเภท .hta (HTML Application File) เมื่อเปิดไฟล์ดังกล่าว จะดาวน์โหลดมัลแวร์และรูปภาพที่มีข้อมูลเกี่ยวกับการเมืองไฟล์ประเภท DDL Loader ถูกพบในเว็บไซต์ของรัฐบาลกัมพูชา

ในรายงานระบุมัลแวร์ที่ถูกดาวน์โหลด 2 สายพันธุ์คือ Loader และ PLAINTEE สำหรับผู้ดูแลระบบที่สนใจสามารถนำข้อมูลเกี่ยวกับมัลแวร์ในรายงาน เช่น ค่า แฮช ของมัลแวร์หรือหมายไอพีที่มัลแวร์ติดต่อมาใช้ตรวจสอบการบุกรุกของระบบ

ในช่วงหลายปีที่ผ่านมา เริ่มมีการพบการโจมตีแบบมุ่งเป้าหมาย เพื่อแอบแฝงและขโมยข้อมูลในระบบขององค์กรในประเทศแถบอาเซียนอยู่หลายครั้ง องค์กรจึงควรใส่ใจในเรื่องความมั่นคงปลอดภัยไซเบอร์และสร้างความตระหนักให้พนักงานในองค์กรของตนรู้จักระวังการเปิดไฟล์หรือลิงก์ที่ได้รับตามช่องทางต่าง ๆ โดยเฉพาะรู้จักความเสี่ยงในการเปิดไฟล์เอกสารและเปิดใช้งาน Macro ซึ่งเป็นช่องทางที่ผู้ประสงค์ร้ายนิยมใช้ในการเผยแพร่มัลแวร์ และหากพบความผิดปกติหรือน่าสงสัยควรแจ้งเจ้าหน้าที่ไอที

Palo Alto
http://thcert.co/cc1Crs
28/6/2561


01
02
03
04


Law & Policy

รัฐบาลสหราชอาณาจักรประกาศแผนพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เริ่มใช้ต้นปี 2562

รัฐบาลสหราชอาณาจักรได้ประกาศแผนการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ซึ่งสอดคล้องตามยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Strategy) เพื่อแก้ไขปัญหาการขาดแคลนบุคลากรที่มีความเชี่ยวชาญในด้านนี้

แผนการพัฒนาบุคลากรฯ ประกอบด้วย 4 หัวข้อหลัก ดังนี้

1. กำหนดโครงสร้างตำแหน่งงานและเส้นทางสายวิชาชีพที่ชัดเจน

เนื่องจากเทคโนโลยีมีการเปลี่ยนแปลงอย่างรวดเร็วและความเชี่ยวชาญของแต่ละสายงานในด้านความมั่นคงปลอดภัยไซเบอร์นั้นมีความแตกต่างกันค่อนข้างสูง ทำให้ทักษะที่จำเป็นต้องใช้ในการทำงานแต่ละสายนั้นมีความแตกต่างกันตามไปด้วย การกำหนดโครงสร้างตำแหน่งงานและความก้าวหน้าที่ชัดเจนจะช่วยให้การพัฒนาบุคลากรเป็นไปได้อย่างมีประสิทธิภาพมากขึ้น และช่วยให้ได้บุคลากรที่มีทักษะตรงตามความต้องการของสายงานตามไปด้วย ทั้งนี้ ทักษะที่จำเป็นนั้นมีทั้งด้านเทคนิคและด้านที่ไม่ใช่เทคนิค (เช่น ทักษะการบริการหรือทักษะการสื่อสาร)

2. ปรับปรุงสภาพแวดล้อมของการสอนและการฝึกอบรม

แบ่งแนวทางการพัฒนาทักษะออกเป็น 2 ส่วน คือการฝึกอบรมบุคลากรที่ทำงานในด้านนี้อยู่แล้ว และปรับปรุงหลักสูตรการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์เพื่อให้มีผู้ที่จะเข้ามาทำงานในด้านนี้มากขึ้น โดยในระดับมัธยมศึกษา ทางรัฐบาลมีแผนที่จะเพิ่มทักษะความรู้ของอาจารย์ผู้สอนในสาย STEM (วิทยาศาสตร์ เทคโนโลยี วิศวกรรมศาสตร์ และคณิตศาสตร์) เพื่อปูพื้นฐานสำหรับการสอนในเรื่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยฯ ส่วนในระดับมหาวิทยาลัย จะมีทั้งการเตรียมความพร้อมสำหรับปฏิบัติงานจริง (หลักสูตร ป.ตรี) และการฝึกปฏิบัติงานกับหน่วยงานในภาคอุตสาหกรรม (หลักสูตร ป.โท และ ป.เอก) นอกจากนี้ ทางรัฐบาลยังมีแผนพัฒนาความรู้สำหรับผู้ที่ไม่ได้ศึกษาในระดับมหาวิทยาลัยหรือศึกษาอยู่ในระดับสายอาชีพด้วย โดยจะมีทั้งการอบรมหลักสูตรพิเศษเพื่อเพิ่มทักษะ และการจัดสอนเนื้อหาที่เกี่ยวข้องกับความมั่นคงปลอดภัยฯ

3. เสริมสร้างทักษะด้านความมั่นคงปลอดภัยฯ ให้กับบุคคลทั่วไป

การแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์นั้นไม่ได้เป็นแค่หน้าที่ของผู้ที่ทำงานด้านนี้เท่านั้น แต่เป็นความรับผิดชอบของทุกภาคส่วน รวมถึงผู้ใช้งานทั่วไปด้วย ดังนั้น การเสริมสร้างทักษะความรู้ที่จำเป็น เช่น การสร้างความตระหนัก จึงเป็นอีกหนึ่งช่องทางที่จะสามารถแก้ไขปัญหาการขาดแคลนบุคลากรได้ แนวทางการดำเนินงานตามแผนนี้ เช่น เปิดหลักสูตรความรู้พื้นฐานด้านทักษะดิจิทัลให้บุคคลทั่วไปเข้ามาเรียนได้ ซึ่งเนื้อหาจะครอบคลุมเรื่องความปลอดภัยและความเสี่ยงในโลกออนไลน์ รวมถึงมีการจัดอบรมให้ความรู้กับผู้ประกอบธุรกิจขนาดเล็กไปจนถึงหน่วยงานขนาดใหญ่เพื่อให้สามารถเข้าใจและรับมือกับภัยคุกคามทางไซเบอร์ได้

4. เป็นผู้นำในด้านการพัฒนาและรักษาบุคลากร

สร้างความร่วมมือกับภาคส่วนต่างๆ เพื่อดึงดูดบุคลากรที่มีความสามารถ พัฒนาทักษะของผู้ที่ทำงานอยู่ในปัจจุบัน และรักษาผู้มีความเชี่ยวชาญให้ยังอยู่ทำงานต่อ ซึ่งงานในส่วนนี้จำเป็นต้องได้รับความร่วมมือจากหลายภาคส่วน ตั้งแต่ระดับปฏิบัติการไปจนถึงระดับผู้บริหาร โดยทางรัฐบาลมีแผนที่จะสร้างเครือข่ายเพื่อดึงดูดบุคลากรจากประเทศอื่นๆ ให้เข้ามาทำงานในสหราชอาณาจักรด้วย ทั้งนี้จะมีการจัดตั้งหน่วยงาน National Cyber Security Programme (NCSP) เพื่อทำหน้าที่ในส่วนนี้ภายในช่วงปลายปี 2564

แผนการพัฒนาบุคลากรฯ นี้จะเริ่มดำเนินการในช่วงต้นปี 2562 รายละเอียดการดำเนินการและเอกสารต่างๆ จะมีการเผยแพร่ผ่านทางเว็บไซต์ของ NCSC ผู้ที่สนใจสามารถติดตามรายละเอียดได้จากเว็บไซต์ดังกล่าว

Healthcare IT News
http://thcert.co/cXmFzt
NIST
http://thcert.co/oyKDcO
26/12/2561

รัฐบาลออสเตรเลียออกข้อแนะนำความมั่นคงปลอดภัย เสนอให้ผู้ดูแลระบบบล็อกโฆษณาในเว็บไซต์, ปิด Flash Player, Java, และ Office Macro

หน่วยงาน Australian Cyber Security Centre (ACSC) ของรัฐบาลออสเตรเลียได้เผยแพร่เอกสาร Australian Government Information Security Manual เพื่อใช้เป็นคู่มือสำหรับการปฏิบัติงานและการตั้งค่าความมั่นคงปลอดภัยให้กับระบบในหน่วยงานภาครัฐ ตัวเอกสารมีหลายหัวข้อ ครอบคลุมตั้งแต่การแบ่งลำดับหน้าที่การทำงาน การจัดทำเอกสาร การรักษาความมั่นคงปลอดภัยทั้งตัวอุปกรณ์ บุคลากร และระบบเครือข่าย ไปจนถึงแนวทางการตั้งค่าระบบและการพัฒนาซอฟต์แวร์ให้มีความมั่นคงปลอดภัย

ตัวเอกสารนี้ได้มีการปรับปรุงอยู่เรื่อยๆ ทุกปี โดยเอกสารฉบับล่าสุดของปี 2018 ได้ถูกเพิ่มข้อแนะนำการตั้งค่าความมั่นคงปลอดภัยให้กับเครื่องคอมพิวเตอร์ของหน่วยงาน ตัวอย่างเช่น ปิดไม่ให้มีการแสดงผลโฆษณาในหน้าเว็บไซต์ ปิดการใช้งาน Adobe Flash Player ปิดไม่ให้ Java เชื่อมต่อกับอินเทอร์เน็ต รวมถึงปิดไม่ให้มีการใช้งาน Microsoft Office Macro จากไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต เป็นต้น นอกจากนี้ยังมีการเพิ่มข้อกำหนดอื่นๆ อย่างเช่น ต้องมีการตรวจสอบสิทธิ์บัญชีผู้ใช้ในระบบอย่างสม่ำเสมอ ปรับปรุงกระบวนการสำรองและกู้คืนข้อมูล ปรับปรุงการส่งข้อมูลข้ามหน่วยงาน เป็นต้น

ข้อแนะนำส่วนใหญ่ออกมาในแนวภาพรวมแบบกว้างๆ โดยอ้างอิงมาตรฐานสากลอย่างเช่น NIST โดยบางข้อกำหนดมีข้อมูลหรือแนวทางการปฏิบัติเพิ่มเติมได้สามารถศึกษาต่อได้ด้วย ผู้ที่สนใจสามารถดูเอกสารนี้ได้จาก

https://cyber.gov.au/infrastructure/publications/australian-government-information-security-manual-ism/pdf/Australian_Government_Information_Security_Manual.pdf

IT News
http://thcert.co/4Szuys
13/12/2561

รัฐบาลสหราชอาณาจักรออกข้อแนะนำแนวทางปฏิบัติด้านความมั่นคงปลอดภัยสำหรับการผลิตและใช้งานอุปกรณ์ IoT

รัฐบาลสหราชอาณาจักร โดยกระทรวงดิจิทัล วัฒนธรรม สื่อ และกีฬา ได้เผยแพร่ฉบับปรับปรุงของเอกสารแนวทางปฏิบัติด้านความมั่นคงปลอดภัยสำหรับอุปกรณ์ IoT (Code of Practice for Consumer Internet of Things (IoT) Security) โดยปรับปรุงล่าสุดเมื่อวันที่ 14 ตุลาคม 2561 ตัวชุดเอกสารแบ่งเป็นข้อแนะนำสำหรับผู้ผลิตและผู้ใช้งาน ตัวอย่างข้อแนะนำสำหรับผู้ผลิต เช่น รหัสผ่านเริ่มต้นของแต่ละอุปกรณ์ควรแตกต่างกัน มีนโยบายการรับแจ้งปัญหาความมั่นคงปลอดภัย มีความรับผิดชอบปรับปรุงซอฟต์แวร์ของตัวอุปกรณ์ มีนโยบายรักษาข้อมูลส่วนบุคคล เป็นต้น ตัวอย่างข้อแนะนำสำหรับผู้ใช้งาน เช่น ไม่ตั้งรหัสผ่านที่สามารถคาดเดาได้ง่าย พิจารณาก่อนตั้งค่าให้สามารถเข้าใช้งานหรือจัดการอุปกรณ์ได้จากเครือข่ายภายนอก เป็นต้น

ปัญหาความมั่นคงปลอดภัยของอุปกรณ์ IoT นั้นเป็นเรื่องที่หลายประเทศทั่วโลกกำลังให้ความสำคัญ เนื่องจากอุปกรณ์เหล่านี้ส่วนใหญ่จะเชื่อมต่ออินเทอร์เน็ตอยู่ตลอดเวลา และมีความสามารถพอที่จะใช้ประมวลผลการทำงานเสมือนเป็นเครื่องคอมพิวเตอร์ได้ แต่ที่ผ่านมาลักษณะการผลิตและใช้งานอุปกรณ์เหล่านี้ยังไม่ได้มีการให้ความสำคัญกับเรื่องความมั่นคงปลอดภัยมากพอ ทำให้ตกเป็นเป้าหมายการโจมตีทั้งการเจาะระบบหรือถูกฝังมัลแวร์เพื่อใช้เป็นฐานการโจมตีระบบอื่นต่อได้ ศึกษาข้อมูลเพิ่มเติมได้จากบทความของไทยเซิร์ต

https://www.thaicert.or.th/papers/general/2016/pa2016ge001.html

จากปัญหาที่เกิดขึ้น ที่ผ่านมาได้มีความพยายามที่จะจัดทำมาตรฐานความมั่นคงปลอดภัยของอุปกรณ์ IoT จากหลายส่วน ซึ่งชุดเอกสารข้อแนะนำแนวทางปฏิบัติของรัฐบาลสหราชอาณาจักรก็เป็นการศึกษาและรวบรวมข้อมูลเหล่านี้มาจัดทำเป็นแนวทางในภาพรวม โดยมีการแสดงความเชื่อมโยงข้อกำหนดแนวปฏิบัติจากเอกสารอื่นๆ ด้วย สำหรับผู้ที่ใช้งานอุปกรณ์ IoT ควรศึกษาข้อมูลเหล่านี้เพื่อเป็นแนวทางป้องกันไม่ให้ตกเป็นเหยื่อจากการถูกโจมตี

UK Government
http://thcert.co/NCu8a6
17/10/2561

การบังคับให้เปิดเผยรหัสผ่านเพื่อสืบสวนคดี

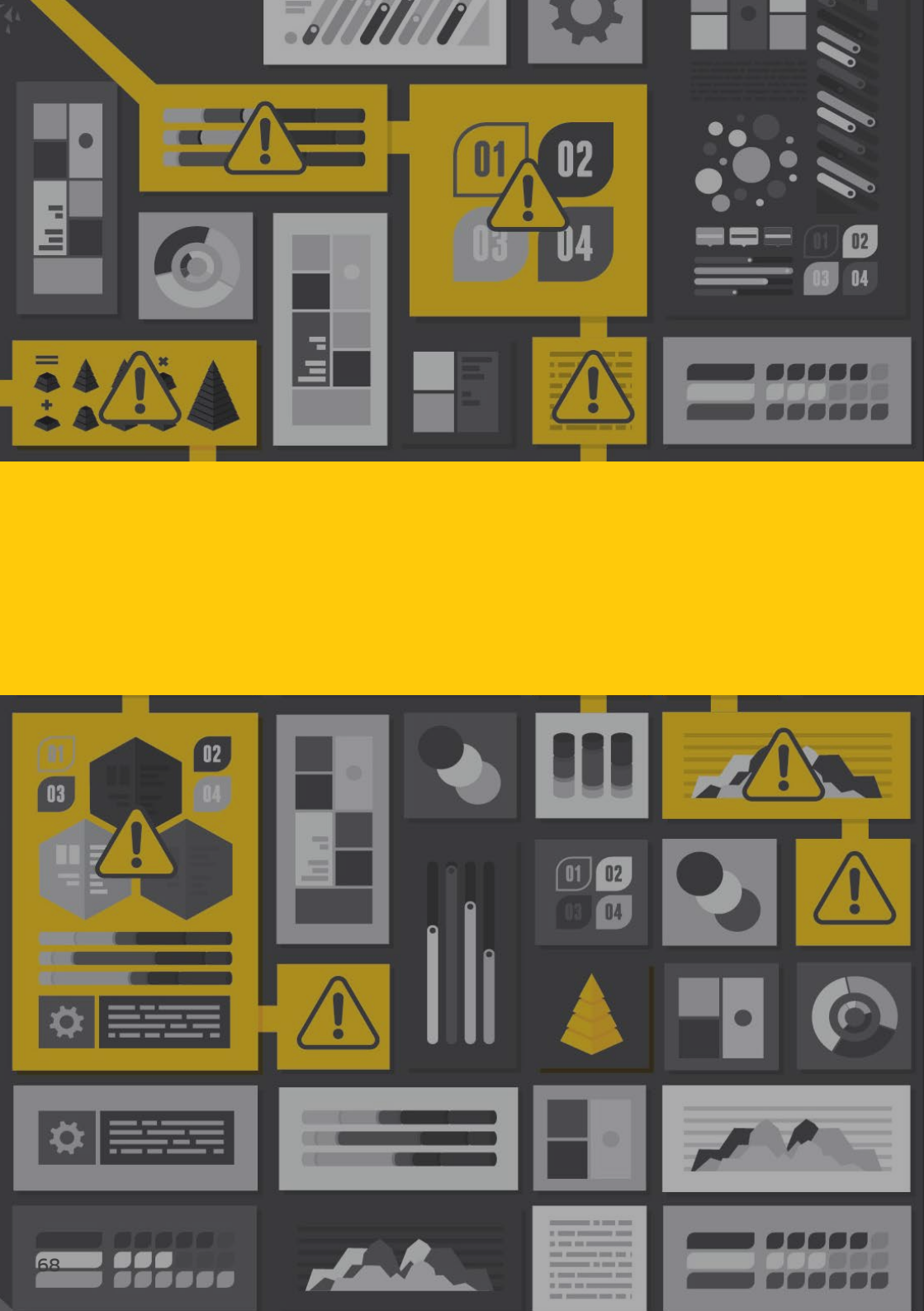
ในวันที่ 31 สิงหาคม 2561 ผู้ต้องหาคดีฆาตกรรมถูกสั่งจำคุก 14 เดือน เนื่องจากไม่ยอมเปิดเผยรหัสผ่านบัญชี Facebook ให้กับเจ้าหน้าที่สืบสวนคดีฆาตกรรมเด็กผู้หญิงอายุวัย 13 ปี การตัดสินดังกล่าวเป็นไปตามกฎหมาย RIPA (Regulation of Investigation Powers Act 2000) ของประเทศสหราชอาณาจักร

RIPA เป็นหนึ่งใน 2 กฎหมายของประเทศสหราชอาณาจักรที่มอบอำนาจให้เจ้าหน้าที่สามารถบังครับให้เปิดเผยกุญแจเข้ารหัสลับหรือข้อมูลสำหรับถอดรหัสลับข้อมูล ซึ่งหากไม่ปฏิบัติตามอาจจะถูกลงโทษด้วยการจำคุกสูงสุด 2 ปีหรือ 5 ปีในกรณีที่เป็นคดีที่เกี่ยวข้องกับความมั่นคงของชาติหรือการอนาจารเด็ก อีกกฎหมายเป็น Terrorism Act 2000 ซึ่งบังคับใช้กับนาย Muhammad Rabbani เพื่อเข้าถึงข้อมูลในอุปกรณ์ ซึ่งคาดว่ามีข้อมูลเกี่ยวข้องกับเหตุการณ์ทรมานของชายคนหนึ่งระหว่างถูกกักคุมตัวในประเทศสหรัฐฯ

สำหรับประเทศสหรัฐ ไม่ได้มีกฎหมายที่ให้อำนาจโดยตรงเหมือนสหราชอาณาจักร แต่ขึ้นอยู่กับดุลพินิจของผู้พิพากษา เช่น ในกรณีที่ตัดสินสั่งจำคุกอดีตตำรวจอย่างไม่มีกำหนดจนกว่าจะให้สิทธิเข้าถึงข้อมูลในฮาร์ดดิสก์เนื่องจากถูกกล่าวหาเก็บรูปภาพอนาจารเด็กไว้ หรืออีกกรณีที่ศาลยกฟ้องกรณีที่บังคับให้จำเลยปลดล็อกไอโฟนเนื่องจากขัดต่อหลักกฎหมายด้านสิทธิที่ชื่อ Fifth Amendment

ในบางกรณีที่สืบสวนคดีที่มีผลกระทบสูงก็อาจจำเป็นต้องเข้าถึงข้อมูลของผู้ต้องหาเพื่อค้นหาความจริงและยืนยันการกระทำผิด ในประเทศสหรัฐฯ และสหราชอาณาจักรมีกรณีที่ใช้กฎหมายเพื่อสนับสนุนเจ้าหน้าที่ในส่วนนี้ โดยเฉพาะคดีที่เกี่ยวข้องกับการอนาจารเด็ก ในขณะเดียวกันในบางกรณีก็อาจมองเป็นเรื่องของการละเมิดสิทธิเสรีภาพ แต่ละประเทศจึงอาจจำเป็นต้องหาจุดสมดุลหรือแนวทางที่สังคมของประเทศยอมรับได้

Nakedsecurity
http://thcert.co/xB81A4
7/9/2561


01
02
03
04


Malware

พบแอปพลิเคชันหลอกลวงใน iOS App Store หลอกให้ผู้ใช้สแกนลายนิ้วมือเพื่อจ่ายเงิน

มีรายงานว่าแอปพลิเคชันชื่อ Fitness Balance และ Calories Tracker บน iOS App Store เป็นแอปพลิเคชันหลอกลวงที่ทำขึ้นมาเพื่อขโมยเงินจากผู้ใช้ โดยแอปพลิเคชันดังกล่าวอ้างว่าสามารถตรวจสอบการเผาผลาญแคลอรีและตรวจการลดน้ำหนักได้โดยการให้ผู้ใช้วางนิ้วลงบนปุ่ม Home ของเครื่อง อย่างไรก็ตาม ตัวแอปพลิเคชันไม่ได้ตรวจสอบข้อมูลร่างกายจริงตามที่กล่าวอ้าง แต่หลังจากที่ผู้ใช้กดปุ่มเพื่อเปิดการสแกนลายนิ้วมือ ตัวแอปพลิเคชันจะแสดงหน้าจอยืนยันการจ่ายเงินผ่าน in-app purchase (ราคาประมาณ 100 ดอลลาร์) จากนั้นจะลดแสงหน้าจอลงต่ำสุดเพื่อไม่ให้ผู้ใช้มองเห็น หากผู้ใช้หลงเชื่อ รวมทั้งตั้งค่าให้สามารถจ่ายเงินได้ด้วยการสแกนลายนิ้วมือ ระบบก็จะยืนยันการจ่ายเงินทันที หลังจากพฤติกรรมหลอกลวงของทั้งสองแอปพลิเคชันถูกเผยแพร่ออกไป ทาง Apple ก็ได้ลบทั้งสองแอปพลิเคชันออกจาก iOS App Store พร้อมเปิดให้ผู้ใช้สามารถขอคืนเงินได้

Bleeping Computer
http://thcert.co/OHglbJ
We Live Security
http://thcert.co/KuFnWM
6/12/2561

การที่แอปพลิเคชันเหล่านี้ผ่านการตรวจสอบและสามารถปรากฏอยู่บน iOS App Store ได้ เกิดจากการอาศัยช่องโหว่ของกระบวนการตรวจสอบ คือ Apple อนุญาตให้แอปพลิเคชันเรียกเก็บเงินผ่าน in-app purchase ได้ แต่ไม่ได้ห้ามการเปลี่ยนราคา (ไม่ว่าจะเพิ่มหรือลดราคา) ในแบบที่มีความแตกต่างกันอย่างชัดเจน อีกหนึ่งกรณีศึกษาที่น่าสนใจคือแอปพลิเคชันนี้มีการจ้างรีวิวปลอมจำนวนมากเพื่อโหวตคะแนนระดับ 5 ดาว ทำให้คะแนนเฉลี่ยของทั้งสองแอปพลิเคชันดูมีความน่าเชื่อถือสูง

จากกรณีที่เกิดขึ้นในทำให้เห็นว่าระบบความมั่นคงปลอดภัยของ iOS ยังมีช่องโหว่ให้สามารถใช้ในการหลอกลวงได้ (ในกรณีคือช่องโหว่ของกระบวนการตรวจสอบแอปพลิเคชันและช่องโหว่ในกระบวนการจ่ายเงินผ่าน in-app purchase) ในอนาคตทาง Apple น่าจะมีมาตรการที่เข้มงวดขึ้น ระหว่างนี้ผู้ใช้สามารถป้องกันตัวเองเบื้องต้นได้ด้วยการปิดไม่ให้มีการยืนยันจ่ายเงินโดยการสแกนลายนิ้วมือ ให้ใช้วิธีการพิมพ์รหัสผ่านแทน

พบเครื่องที่ใช้ Docker จำนวนมาก มีการตั้งค่าไม่ปลอดภัย อาจถูกแฮกฝังมัลแวร์ขุดเงินดิจิทัล

บริษัท Juniper Networks รายงานการโจมตีเครื่องคอมพิวเตอร์ที่ใช้งาน Docker เพื่อฝังมัลแวร์ โดยผู้ประสงค์ร้ายใช้วิธีสแกนพอร์ตที่เครื่องเปิดอยู่ จากนั้นเชื่อมต่อไปยังพอร์ตที่ใช้สำหรับบริหารจัดการ Docker (ปกติจะเป็นพอร์ต 2375 และ 2376) โดยหากมีการตั้งค่าที่ไม่ปลอดภัย เช่น เปิดให้เข้าไปจัดการ container ข้างในได้โดยไม่มีการยืนยันตัวตน ผู้ประสงค์ร้ายก็สามารถเพิ่ม container เข้ามาแล้วติดตั้งมัลแวร์สำหรับขุดเงินดิจิทัลได้ (ส่วนมากใช้ขุดเงินสกุล Monero) ทำให้เครื่องคอมพิวเตอร์ทำงานหนักขึ้นโดยไม่จำเป็น

ในเว็บไซต์ของ Juniper Networks มีรายละเอียดว่ามัลแวร์ติดเข้ามาในเครื่องได้อย่างไร รวมถึงตัวอย่าง log และสคริปต์ที่ถูกใช้ในการโจมตี ซึ่งผู้ที่ใช้งาน Docker สามารถตรวจสอบข้อมูลได้ ข้อแนะนำเพิ่มเติมเพื่อให้ระบบมีความมั่นคงปลอดภัยมากยิ่งขึ้นคือการเปิดใช้งาน Docker ผ่าน TLS (https://docs.docker.com/engine/security/https/) ซึ่งจะช่วยทั้งในเรื่องของการยืนยันตัวตนและการเข้ารหัสลับข้อมูลที่รับส่ง

Bleeping Computer
http://thcert.co/uZtuTv
Juniper
http://thcert.co/1jP84k
16/11/2561

เจ้าหน้าที่หน่วยงานรัฐในอเมริกาใช้คอมสำนักงานเปิดดูเว็บโป๊ มัลแวร์ติดแพร่ไปทั้งเครือข่าย

หน่วยงานสืบสวนของสหรัฐฯ ออกรายงานผลการตรวจสอบปัญหามัลแวร์แพร่ระบาดในสำนักงานสำรวจธรณีวิทยา (U.S. Geological Survey) โดยพบว่าสาเหตุเกิดจากเจ้าหน้าที่ใช้คอมพิวเตอร์และอินเทอร์เน็ตของสำนักงานเข้าชมเว็บไซต์ลามก

เมื่อกลางเดือนตุลาคม 2561 ทางหน่วยงานสืบสวนของสหรัฐฯ ได้รับแจ้งว่าพบทราฟฟิกอินเทอร์เน็ตผิดปกติในหน่วยงาน จึงขอให้ช่วยตรวจสอบ ซึ่งภายหลังพบว่าสาเหตุเกิดจากระบบในเครือข่ายติดมัลแวร์ขโมยข้อมูล เมื่อตรวจสอบต่อไปเรื่อยๆ พบว่าคอมพิวเตอร์เครื่องหนึ่งของหน่วยงานถูกใช้เข้าชมเว็บไซต์ลามกจำนวนหลายพันหน้า ซึ่งเว็บไซต์เหล่านั้นมีมัลแวร์ฝังอยู่ นอกจากนี้ยังพบว่าผู้ใช้เครื่องคอมพิวเตอร์ดังกล่าวนำ USB มาเสียบกับเครื่องเพื่อบันทึกรูปภาพ รวมถึงนำโทรศัพท์มือถือ Android มาเชื่อมต่อกับคอมพิวเตอร์ ทำให้มีมัลแวร์เข้าไปติดอยู่ในโทรศัพท์มือถือด้วย

ภายหลังการตรวจวิเคราะห์ ทางหน่วยงานสืบสวนได้แนะนำให้หน่วยงานเพิ่มมาตรการความมั่นคงปลอดภัยโดยปิดกั้นการเชื่อมต่ออุปกรณ์ USB ที่ไม่ได้รับอนุญาต บล็อกเว็บไซต์ที่เป็นอันตราย และควรตรวจสอบการใช้อินเทอร์เน็ตของพนักงานด้วย

TripWire
http://thcert.co/Cn3hjS
OIG
http://thcert.co/mNEZtb
2/11/2561

ระวัง อันตรายจากการใช้โทรศัพท์มือถือ Android ราคาถูก อาจมีมัลแวร์สอดแนม ขโมยข้อมูลฝังมาตั้งแต่โรงงาน

ปัจจุบันในท้องตลาดมีโทรศัพท์มือถือ Android ให้เลือกซื้อเป็นจำนวนมาก ตั้งแต่ยี่ห้อที่เป็นที่รู้จักและได้รับความนิยม ไปจนถึงโทรศัพท์มือถือราคาถูกจากบริษัทรับจ้างผลิต หรือแม้กระทั่งโทรศัพท์มือถือที่ทำรูปร่างหน้าตาออกมาให้ดูคล้ายยี่ห้อดังแต่ที่จริงแล้วเป็นของเลียนแบบ ซึ่งสินค้าเหล่านี้อาจไม่ได้มีการตรวจสอบคุณภาพหรือมาตรการด้านความมั่นคงปลอดภัยที่ดีพอ ทำให้ผู้ใช้อาจตกอยู่ในความเสี่ยงได้

ตัวอย่างปัญหาที่อาจจะเกิดขึ้นได้จากการที่ผู้ผลิตไม่ได้ให้ความสำคัญกับเรื่องความเป็นส่วนตัวหรือความมั่นคงปลอดภัยตั้งแต่แรก เช่น นักพัฒนาเขียนโค้ดแบบไม่ปลอดภัย ถูกแอบฝังมัลแวร์มาในโทรศัพท์ตั้งแต่ตอนผลิต ถูกฝังมัลแวร์ลงในโทรศัพท์ระหว่างที่ขนย้ายจากโรงงานมายังร้านค้า หรือไม่มีการอัปเดตแก้ไขช่องโหว่ของซอฟต์แวร์หลังจากที่วางจำหน่าย เป็นต้น

เว็บไซต์ Naked Security รายงานพบมัลแวร์ขโมยข้อมูลฝังมากับโทรศัพท์มือถือราคาถูกยี่ห้อหนึ่ง โดยมัลแวร์ดังกล่าวปลอมเป็นแอปพลิเคชันบันทึกเสียง ตัวมัลแวร์มีความสามารถในการแอบบันทึกและส่งต่อข้อมูลส่วนตัวของผู้ใช้ เช่น เสียงบันทึก ตำแหน่งที่อยู่ หรือ SMS ไปยังเซิร์ฟเวอร์ภายนอกโดยไม่ได้ขออนุญาตจากผู้ใช้ จากการตรวจสอบเพิ่มเติมพบว่าโทรศัพท์รุ่นดังกล่าวสามารถหาซื้อได้ในประเทศไทยแต่ไม่ได้มีตัวแทนจำหน่ายในไทยอย่างเป็นทางการเหตุการณ์กรณีที่มีมัลแวร์ฝังมากับโทรศัพท์มือถือราคาถูกนั้นมีการรายงานอยู่อย่างสม่ำเสมอ

(ตัวอย่างเหตุการณ์ที่เคยเกิดขึ้นในไทย https://www.thaicert.or.th/newsbite/2016-06-20-03.html)

เนื่องจากปัจจุบันนี้รูปแบบการใช้งานโทรศัพท์มือถือนั้นไม่ได้มีเพียงแค่การโทรศัพท์หรือรับส่งข้อความ แต่ยังรวมถึงการจ่ายเงินซื้อสินค้าหรือการทำธุรกรรมทางการเงินผ่านโทรศัพท์ด้วย ผู้ที่ต้องการความปลอดภัยในการทำธุรกรรมออนไลน์จึงควรตระหนักและพิจารณาการเลือกใช้งานอุปกรณ์ที่มีกระบวนการตรวจสอบรับรองความมั่นคงปลอดภัยด้วย เพื่อป้องกันไม่ให้เกิดปัญหา

ตัวอย่างแนวทางการพิจารณา เช่น ไม่ควรซื้อโทรศัพท์มือถือที่เป็นของเลียนแบบไม่ได้วางขายผ่านตัวแทนจำหน่ายอย่างเป็นทางการ ไม่มีแนวทางการอัปเดตหรือแก้ไขปัญหาซอฟต์แวร์ที่ชัดเจนเพียงพอ หรือไม่มีช่องทางการติดต่อที่ชัดเจนในกรณีที่พบปัญหา เป็นต้น ทั้งนี้ ผู้ใช้ควรเพิ่มมาตรการป้องกัน เช่น ตั้งรหัสผ่านที่คาดเดาได้ยาก หรือเปิดใช้การยืนยันตัวตนแบบหลายขั้นตอน ควบคู่ไปอีกชั้นหนึ่ง

Naked Security
http://thcert.co/385hPb
19/10/2561

สหรัฐอเมริกาเผยข้อมูลสำหรับตรวจจับมัลแวร์สายพันธุ์ใหม่จากปฏิบัติการโจมตี HIDDEN COBRA

เมื่อวันที่ 14 มิถุนายน 2561 US-CERT ประกาศแจ้งเตือนและเผยแพร่รายงานวิเคราะห์มัลแวร์ซึ่งเกิดจากความร่วมมือระหว่าง Federal Bureau of Investigation (FBI) และ Department of Homeland Security (DHS) ของสหรัฐอเมริกา ในรายงานระบุมัลแวร์ประเภทโทรจัน สายพันธุ์ TYPEFRAME ซึ่งรัฐบาลประเทศเกาหลีเหนือใช้ในปฏิบัติการโจมตีทางไซเบอร์ชื่อ HIDDEN COBRA

รายงานนี้มีบทวิเคราะห์ตัวอย่างมัลแวร์ 11 รายการ เป็น executable file บน Windows ทั้ง 32-bit และ 64-bit และไฟล์เอกสาร Microsoft Word ซึ่งมี VBA Macro โดยไฟล์เหล่านี้มีความสามารถดาวน์โหลดและติดตั้งมัลแวร์ ติดตั้ง proxy และ Remote Access Trojans (RATs) สามารถเชื่อมต่อกับเซิร์ฟเวอร์ของผู้ประสงค์ร้าย (command and control server : C2) เพื่อรับคำสั่งเพิ่มเติม รวมถึงตั้งค่าใน firewall ของเหยื่อให้เปิดรับการเชื่อมต่อจากภายนอก

ในรายงานมีข้อมูลที่องค์กรสามารถนำไปใช้ในการตรวจจับมัลแวร์ดังกล่าว รวมถึงข้อแนะนำในการป้องกัน ผู้ใช้สามารถอ่านรายงานการวิเคราะห์มัลแวร์ดังกล่าวฉบับเต็มได้ที่

https://www.us-cert.gov/ncas/analysis-reports/AR18-165A

และศึกษาข้อแนะนำในการรับมือและจัดการมัลแวร์เพิ่มเติมจากคู่มือของ NIST

https://www.nist.gov/publications/guide-malware-incident-prevention-and-handling-desktops-and-laptops

หากตรวจพบมัลแวร์ ผู้ใช้สามารถติดต่อไทยเซิร์ตเพื่อขอคำแนะนำและความช่วยเหลือในการรับมือภัยคุกคาม โดยติดต่อได้ที่ 0-2123-1212

US-CERT
http://thcert.co/IrgCIJ
15/6/2561

Stresspaint มัลแวร์สายพันธุ์ใหม่ มุ่งเป้าขโมยรหัสผ่านบัญชี Facebook แพร่ระบาดไปยังผู้ใช้มากกว่า 35,000 ราย

เมื่อต้นเดือนเมษายน นักวิจัยค้นพบมัลแวร์สายพันธุ์ที่ชื่อ Stresspaint มีความสามารถขโมยรหัสผ่านบัญชีที่เก็บไว้ใน Chrome และส่งให้ผู้ประสงค์ร้าย ซึ่งพบว่ามีความพยายามรวบรวมข้อมูลผู้ใช้งาน Facebook โดยได้นำรหัสผ่าน Facebook ที่ขโมย มาล็อกอินเพื่อเข้าถึงข้อมูลต่างๆ เช่น จำนวนเพื่อน, เพจที่สร้าง, มีการจ่ายเงินผ่านทาง Facebook หรือไม่ มัลแวร์ดังกล่าวแพร่ระบาดไปยังผู้ใช้มากกว่า 35,000 ราย ส่วนใหญ่พบในประเทศเวียดนาม รัสเซีย และปากีสถาน

สำหรับช่องทางการแพร่กระจายมัลแวร์นักวิจัยเชื่อว่าผู้ประสงค์ร้ายได้ใช้ช่องทางอีเมลและ Facebook เพื่อหลอกให้เหยื่อเข้าเว็บไซต์และดาวน์โหลดแอปพลิเคชัน Relieve Stress Paint ซึ่งมีมัลแวร์ซ่อนอยู่ เหยื่อสามารถติดตั้งและใช้งานโปรแกรมตามปกติ ในขณะที่มัลแวร์ที่ซ่อนอยู่ได้ถูกติดตั้งและแอบขโมยข้อมูล

ถึงแม้ว่ามัลแวร์ดังกล่าวจะถูกตรวจจับโดยแอนติไวรัสส่วนใหญ่ได้แล้ว แต่ก่อนหน้านี้ในช่วงเริ่มต้นแพร่กระจาย มัลแวร์สามารถหลีกเลี่ยงการตรวจจับ โดยแทนที่จะเข้าถึงอ่านไฟล์ที่เก็บรหัสผ่านโดยตรงซึ่งถูกเฝ้าระวังโดยแอนติไวรัสส่วนใหญ่ มัลแวร์ใช้วิธี Copy ไฟล์และอ่านข้อมูลในไฟล์ดังกล่าวแทน

จะเห็นได้ว่าบัญชี Facebook ถือเป็นหนึ่งในข้อมูลสำคัญที่ผู้ประสงค์ร้ายพยายามที่จะขโมย จึงจำเป็นที่ผู้ใช้ต้องตระหนักถึงความเสี่ยงและรู้จักป้องกัน แอนติไวรัสสามารถช่วยป้องกันมัลแวร์ได้ในระดับนึง ผู้ใช้ต้องรู้เท่าทันการโจมตีและวิธีรับมือด้วย เช่น รู้จักสังเกตความผิดปกติของอีเมลที่ได้รับ หรือตั้งการยืนยันตัวตนแบบ 2 ขั้นตอน ซึ่งช่วยให้บัญชีมีความมั่นคงปลอดภัยมากขึ้น

US-CERT
http://thcert.co/lrgCIJ
27/4/2561

รายงานเผย พบแฮกเกอร์ใช้มัลแวร์สายพันธุ์ใหม่โจมตีองค์กรในกลุ่มประเทศเอเชียตะวันออกเฉียงใต้

บริษัทด้านความมั่นคงปลอดภัย ESET เผยแพร่รายงานการค้นพบมัลแวร์ใหม่ที่ถูกใช้โดยกลุ่มแฮกเกอร์ Oceanlotus ซึ่งเป็นกลุ่มที่มุ่งเป้าโจมตีองค์กรภาครัฐและเอกชนในกลุ่มประเทศเอเชียตะวันออกเฉียงใต้

สำหรับรูปแบบการเผยแพร่มัลแวร์แฮกเกอร์ใช้วิธีส่งอีเมลหลอกลวงแนบไฟล์ที่เป็นมัลแวร์โดยมีตัวอย่างชื่อไฟล์ เช่น

20170905-Evaluation Table.xls.exe, CV_LeHoangThing.doc.exe ซึ่งเป็นการตั้งชื่อไฟล์ให้ดูเหมือนไฟล์เอกสาร แต่ที่จริงแล้วเป็นไฟล์สกุล exe หากถูกเปิดก็จะทำให้เครื่องติดมัลแวร์ และอีกรูปแบบคือการเผยแพร่ผ่านเว็บไซต์ โดยหลอกให้ดาวน์โหลดและเปิดไฟล์ติดตั้งโปรแกรม (Installer) ซึ่งที่จริงคือมัลแวร์เช่นกัน

ในการติดตั้งมัลแวร์ แฮกเกอร์ได้ใช้เทคนิคหลีกเลี่ยงการตรวจจับของแอนติไวรัส เช่น การเปลี่ยนแปลงโค้ดในมัลแวร์ทำให้ยากต่อการระบุลักษณะหรือพฤติกรรมที่น่าสงสัย (Code Obfucastion) หรือ การที่มัลแวร์มาในรูปแบบ 2 ไฟล์ คือ ไฟล์แรกสกุล exe ที่เป็นไฟล์ที่ถูกใช้งานทั่วไปและถูกรับรองโดยบริษัทน่าเชื่อถือ ซึ่งไฟล์ดังกล่าวได้โหลดและเรียกใช้งานไฟล์ที่สองสกุล DLL ซึ่งมีโค้ดประสงค์ร้ายแฝงอยู่ โดยเทคนิคนี้เรียกว่า DLL side-loading ซึ่งในการโจมตีของกลุ่มแฮกเกอร์ OceanLotus ได้ใช้ไฟล์ RasTlsc.exe จากบริษัท Symantec และ mcoemcpy.exe จาก McAfee บังหน้าเพื่อหลีกเลี่ยงการตรวจจับ ซึ่งไฟล์ทั้งสองจะไปเรียกใช้งานไฟล์ rastls.dll ซึ่งมีโค้ดประสงค์ร้ายแฝงอยู่อีกที

มัลแวร์ที่ถูกติดตั้งเป็นมัลแวร์ประเภท Backdoor ซึ่งจะติดต่อเครื่องของผู้ประสงค์ร้ายเพื่อส่งข้อมูลเบื้องต้น เช่น ชื่อคอมพิวเตอร์ ชื่อบัญชีผู้ใช้ เวอร์ระบบปฏิบัติการ และรอคำสั่งจากผู้ประสงค์ร้ายต่อไป

จะเห็นได้ว่าผู้ประสงค์ร้ายมีความพยายามในการใช้เทคนิคต่าง ๆ หลีกเลี่ยงการตรวจจับการติดมัลแวร์ ซึ่งเราไม่อาจพึ่งกลไกในการตรวจจับของแอนติไวรัสเพียงอย่างเดียว ผู้ใช้ควรมีความระวังและรู้จักสังเกตสกุลไฟล์ที่แนบในอีเมล ซึ่งหากพบไฟล์ที่อ้างว่าเป็นเอกสาร แต่เป็นไฟล์ประเภท exe ควรแจ้งผู้ดูแลระบบเพื่อตรวจสอบ

ในขณะเดียวกันผู้ดูแลระบบอาจเพิ่มกลไกในการป้องกันเพิ่มเติม เช่น การตั้งค่าจำกัดให้ผู้ใช้สามารถเปิดโปรแกรมทตามรายการที่กำหนดอนุญาตไว้เท่านั้น

ผู้ดูแลระบบสามารถศึกษาข้อมูลไฟล์และหมายเลขไอพีที่กลุ่มแฮกเกอร์ใช้เพื่อโจมตีได้จากรายงานในที่มาของข่าว เพื่อใช้ตรวจสอบความผิดปกติในเครื่องและเครือข่ายขององค์กร

ESET
https://www.thaicert.or.th/newsbite/2018-04-04-01.html
04/4/2561

Palo Alto เตือนภัย พบไทยคลิกลิงก์อันตรายที่แพร่มัลแวร์ขุดเงินดิจิทัล Monero สูงสุด

ปลายเดือนมกราคมที่ผ่านมา บริษัท Paloalto ได้เปิดเผยการพบลิงก์อันตรายซึ่งใช้สำหรับแพร่กระจายมัลแวร์กว่า 250 ตัวอย่าง ที่ใช้ขุดเหรียญ Monero ซึ่งเป็นสกุลเงินหนึ่งของเงินดิจิทัลประเภท Cryptocurrency (ตัวอย่าง Cryptocurrency ที่เราอาจจะคุ้นเคยคือ Bitcoin)

จากวิเคราะห์พบว่ามีผู้คนคลิกลิงก์ดังกล่าวมากกว่า 15 ล้านครั้ง และประเทศที่คลิกลิงก์ดังกล่าวมากที่สุดคือประเทศไทย เป็นจำนวน 3.5 ล้านครั้ง และพบการเผยแพร่มัลแวร์ดังกล่าวนานมากกว่า 4 เดือน

สำหรับรูปแบบการโจมตี ผู้ประสงค์ร้ายใช้เว็บไซต์ที่ให้บริการย่อลิงก์ให้สั้น เช่น Bitly หรือ Adfly ในการสร้างลิงก์สำหรับเผยแพร่มัลแวร์ ซึ่งหากเหยื่อคลิกลิงก์จะส่งผลให้ไฟล์ที่เป็นมัลแวร์ถูกดาวน์โหลดลงในเครื่อง โดยชื่อไฟล์ที่พบ เป็นลักษณะชื่อของผู้ให้บริการอัปโหลดไฟล์ ตามด้วยหมายเลข เช่น [RapidFiles]_2343.exe หรือ [File4org]_421064.exe

หากเหยื่อคลิกรันไฟล์ดังกล่าว จะส่งผลให้มัลแวร์ทำงาน โดยลักลอบใช้การประมวลผล CPU เพื่อขุดเหรียญ ทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง

ปัจจุบัน การโจมตีเพื่อแอบขุดเงินในเครื่องของเหยื่อเริ่มพบได้ทั่วไป โดยมีหลากหลายรูปแบบ เช่น การที่เว็บไซต์ต่างๆ แอบแฝงโค้ดสำหรับขุดเงิน เพียงแค่เหยื่อเข้าเว็บไซต์ก็จะถูกใช้เครื่องในการขุดเงิน

สำหรับการเผยแพร่มัลแวร์ในครั้งนี้ จากการตรวจสอบจากไฟล์มัลแวร์ 250 ตัวอย่าง พบว่าสามารถถูกตรวจจับโดยแอนติไวรัสส่วนใหญ่ได้แล้ว อย่างไรก็ตามผู้ประสงค์ร้ายอาจสร้างดัดแปลงมัลแวร์เพื่อหลบเลี่ยงการตรวจจับ ผู้ใช้จึงควรระมัดระวังไฟล์ต่าง ๆ ที่ดาวน์โหลดจากเครือข่ายอินเทอร์เน็ต โดยเฉพาะหากต้องการดาวน์โหลดไฟล์งานต่าง ๆ เช่น เอกสาร เพลง หากไฟล์ที่ดาวน์โหลดมานั้น เป็นสกุล exe ไม่ควรคลิกรันในระบบ หรือควรหลีกเลี่ยงการใช้งานไฟล์ จากแหล่งที่มาไม่ชัดเจน

ทั้งนี้ผู้ที่สนใจสามารถศึกษาข้อแนะนำทั่วไปในการระวัง ป้องกัน มัลแวร์ ได้ที่
https://www.facebook.com/thaicert/videos/660657847415685/

Paloalto Networks
http://thcert.co/Hz6meP
26/1/2561


01
02
03
04


01
02
03
04


Privacy

ฐานข้อมูลของ SingHealth กลุ่มผู้ให้บริการสาธารณสุขที่ใหญ่สุดในสิงคโปร์ถูกเจาะ กระทบข้อมูลผู้ป่วย 1.5 ล้านคน

เมื่อวันที่ 20 กรกฎาคม 2561 SingCERT ซึ่งเป็นหน่วยงานประสานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ของสิงคโปร์ได้แจ้งเตือนเหตุการณ์ที่ข้อมูลของผู้ป่วยที่ใช้บริการของ SingHealth ถูกขโมยไปจากฐานข้อมูล SingHealth ซึ่งเป็นกลุ่มสถานให้บริการสาธารณสุขที่ใหญ่สุดในประเทศสิงค์โปร์ ข้อมูลที่ถูกขโมยมีสองส่วน ส่วนแรกเป็นข้อมูลส่วนบุคคลของผู้ป่วย 1.5 ล้านคน ที่มาใช้บริการระหว่างวันที่ 1 พฤษภาคม 2558 ถึง 4 กรกฎาคม 2561 ซึ่งข้อมูลประกอบไปด้วย ชื่อ นามสกุล ที่อยู่ เพศ เชื้อชาติ หมายเลขบัตรประจำตัวประชาชน และวันเกิด และในส่วนที่สองเป็นข้อมูลการจ่ายยาผู้ป่วยนอกจำนวน 160,000 คนจากผู้ป่วย 1.5 ล้านคน ทั้งนี้นายกรัฐมนตรีสิงคโปร์ได้โพสต์ข้อความผ่าน Facebook ว่าข้อมูลของตนก็ได้รับผลกระทบจากเหตุการณ์ครั้งนี้เช่นเดียวกัน

เหตุการณ์นี้ทำให้รัฐบาลสิงคโปร์สั่งให้ผู้ให้บริการสาธารณะสุขตรวจสอบระบบทั้งหมด และชะลอโครงการระเบียนผู้ป่วยอิเล็กทรอนิกส์ ตลอดจนให้แยกเครือข่ายที่พนักงานจำนวน 28,000 คนของ SingHealth ที่เชื่อมต่อกับอินเทอร์เน็ตออกจากเครือข่ายภายในของหน่วยงาน หลักการ Network separation นี้จะใช้กับหน่วยบริการสาธารณสุขอื่น ๆ ในสิงคโปร์ด้วย อย่างไรก็ตาม ถึงแม้ว่าข้อมูลส่วนบุคคลบางส่วนจะถูกขโมยออกมาแต่ข้อมูลผู้ป่วยทั้งหมดยังใช้งานได้ตามปกติ โดย SingHelath จะติดต่อผู้ป่วยทุกคนที่มาใช้บริการระหว่างวันที่ 1 พฤษภาคม 2558 – 4 กรกฎาคม 2561 เพื่อแจ้งว่าข้อมูลของตนถูกขโมยหรือไม่ หรือผู้ที่สงสัยว่าจะได้รับผลกระทบจากเหตุการณ์นี้ สามารถตรวจสอบได้ผ่านแอปพลิเคชันบนโทรศัพท์มือถือ (mobile application) หรือเว็บไซต์ของ SingHealth องค์กรด้านสาธารณะสุข เช่น โรงพยาบาล มักจะเป็นหนึ่งในเหยื่อที่มีแนวโน้มตกเป็นเป้าการโจมตี เนื่องจากเก็บข้อมูลส่วนบุคคลจำนวนมาก ของผู้ป่วยอาจพิจารณาจัดทำรายการบริการโครงสร้างพื้นฐานหรือข้อมูลสำคัญ เพื่อยกระดับการเฝ้าระวังในส่วนดังกล่าวเมื่ออยู่ภาวะเสี่ยงต่อการถูกโจมตี

รวมถึงสร้างความตระหนักรู้ให้กับบุคลากรและจัดซ้อมรับมือภัยคุกคาม หน่วยงานอื่นๆ ที่เก็บข้อมูลส่วนบุคคลของลูกค้าก็จำเป็นต้องทบทวนเสริมมาตรการป้องกันให้เพียงทั้งในด้านกระบวนการ เทคโนโลยี และบุคคลากร

คำแนะนำของไทยเซิร์ตเกี่ยวกับการปกป้องข้อมูล ผู้ดูแลระบบควรจัดทำรายการข้อมูลในระบบสารสนเทศและทบทวนสิทธิการเข้าถึงข้อมูลในระบบทั้งหมด ยืนยันมาตรการตรวจสอบสิทธิการเข้าถึงข้อมูล พร้อมทั้งเฝ้าระวังและตรวจจับพฤติกรรม การเข้าถึงข้อมูลที่ผิดปกติ

หน่วยงานควรแจ้งให้บุคลากรของหน่วยงานระมัดระวังในการเปิดไฟล์แนบอีเมล หรือคลิกลิงก์ที่ได้รับ ผ่านช่องทางต่าง ๆ ถ้าสงสัยว่าเป็นไฟล์หรือลิงก์ได้รับจะมีความผิดปกติ ให้ตรวจสอบและยืนยัน กับผู้ส่ง เพื่อป้องกันการติดมัลแวร์ปรับปรุงซอฟต์แวร์ให้เป็นปัจจุบันอย่างสม่ำเสมอ และติดตามข้อมูลข่าวสารเกี่ยวกับภัยคุกคาม ไซเบอร์ทางเว็บไซต์ https://www.thaicert.or.th หรือ Facebook page https://th-th.facebook.com/thaicert

หากพบความผิดปกติหรือมีข้อสงสัยเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ สามารถติดต่อศูนย์ประสานกลางรักษาความมั่นคงปลอดภัยไซเบอร์ (24x7) ทางโทรศัพท์หมายเลข 1212 หรือ 0-2123-1212 หรืออีเมลที่ report@thaicert.or.th (ดำเนินการโดยไทยเซิร์ต สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม)

Ministry of Health
http://thcert.co/y67uDx
The Straits Times
http://thcert.co/1cZNCo
31/7/2561

เซิร์ฟเวอร์ของ Unicef Thailand ที่เก็บข้อมูลผู้บริจาค 20,000 รายถูกเจาะระบบ แจ้งเตือนผู้ที่ได้รับผลกระทบแล้ว

Unicef Thailand ได้ประกาศผ่านทางเว็บไซต์ทางการแจ้งเตือนว่าเซิร์ฟเวอร์ของหน่วยงานถูกโจมตีทางไซเบอร์ พร้อมชี้แจงว่าไม่พบหลักฐานที่ชี้ว่ามีการเข้าถึงข้อมูลที่สำคัญ เซิร์ฟเวอร์ดังกล่าวได้จัดเก็บข้อมูลของผู้บริจาคที่บริจาคผ่านเว็บไซต์ www.unicef.or.th โดยเป็น ชื่อ ช่องทางการติดต่อ และวันเดือนปีเกิด ของผู้บริจาคจำนวนประมาณ 20,000 คน และมีข้อมูลบัตรเครดิตของผู้บริจาคประมาณ 400 ราย ซึ่งส่วนใหญ่เป็นบัตรที่หมดอายุแล้ว และธนาคารได้ดำเนินการออกบัตรใบใหม่ให้แก่ผู้บริจาคที่บัตรอาจยังไม่หมดอายุเป็นที่เรียบร้อยแล้ว โดยยูนิเซฟได้ทำการแจ้งไปยังผู้บริจาคที่เกี่ยวข้องทั้งหมดแล้ว

Unicef Thailand ได้รายงานเหตุการณ์นี้กับหน่วยงานที่เกี่ยวข้องและได้ดำเนินการร่วมกับผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์เพื่อตรวจสอบสิ่งที่เกิดขึ้น รวมถึงกำลังดำเนินการอย่างเต็มที่เพื่อป้องกันไม่ให้เกิดเหตุการณ์เช่นนี้ขึ้นอีก โดยกรณีที่มีข้อสงสัยเพิ่มเติมที่เกี่ยวข้อง ทาง Unicef Thailand ได้จัดเตรียมช่องทางติดต่อไว้ที่เบอร์โทรศัพท์ 02-080-5686

เจ้าของข้อมูลที่ได้รับผลกระทบอาจเสี่ยงที่จะถูกโจมตี เช่น ได้รับอีเมลที่มีจุดประสงค์เพื่อหลอกขโมยข้อมูลหรือเผยแพร่มัลแวร์ สำหรับผู้ที่สนใจสามารถศึกษาวิธีสังเกตอีเมลที่น่าสงสัยได้จากคลิปของไทยเซิร์ต

https://www.facebook.com/thaicert/videos/663973140417489/

Unicef
http://thcert.co/cYy6tT
04/4/2561

ข้อมูลลูกค้า True Move H กว่า 46,000 ไฟล์ หลุดรั่วจาก cloud service

เมื่อวันที่ 13 เมษายน 2561 นักวิจัยด้านความมั่นคงปลอดภัย Niall Merrigan ได้รายงานข้อมูลผู้ใช้บริการ True Move H รั่วไหล เนื่องจากมิได้มีมาตรการเพียงพอสำหรับปกป้องข้อมูลที่อยู่ใน Amazon S3 bucket ส่งผลให้บุคคลภายนอกสามารถเข้าถึงและดาวน์โหลดข้อมูลดังกล่าวออกมาได้

ข้อมูลที่หลุดออกมามีทั้งไฟล์ JPG และ PDF โดยเป็นไฟล์สแกนสำเนาบัตรประชาชน ใบขับขี่ และพาสปอร์ตของผู้ใช้บริการ ปริมาณข้อมูลที่อยู่บนเซิร์ฟเวอร์ดังกล่าวมีประมาณ 46,000 ไฟล์ รวมแล้วกว่า 32GB (อย่างไรก็ตาม ยังไม่ยืนยันจำนวนผู้ได้รับผลกระทบ) นักวิจัยเผยว่าได้ติดต่อประสานไปยัง True Move H เมื่อต้นเดือนมีนาคม 2561 และปัญหานี้ได้รับการแก้ไขแล้วเมื่อวันที่ 12 เมษายน 2561

ปัญหาข้อมูลรั่วไหลในลักษณะนี้เคยเกิดขึ้นมาแล้วหลายครั้ง หน่วยงานหรือนักพัฒนาที่นำข้อมูลสำคัญ (โดยเฉพาะข้อมูลส่วนบุคคล) ฝากไว้บน Amazon S3 bucket ควรรักษาความมั่นคงปลอดภัยของข้อมูลโดยอาจเข้ารหัสลับข้อมูล จำกัดการเข้าถึงจากบุคคลภายนอก รวมถึงตรวจสอบการใช้งานที่ผิดปกติ โดยสามารถศึกษาข้อมูลเพิ่มเติมได้จากเว็บไซต์ของ Amazon

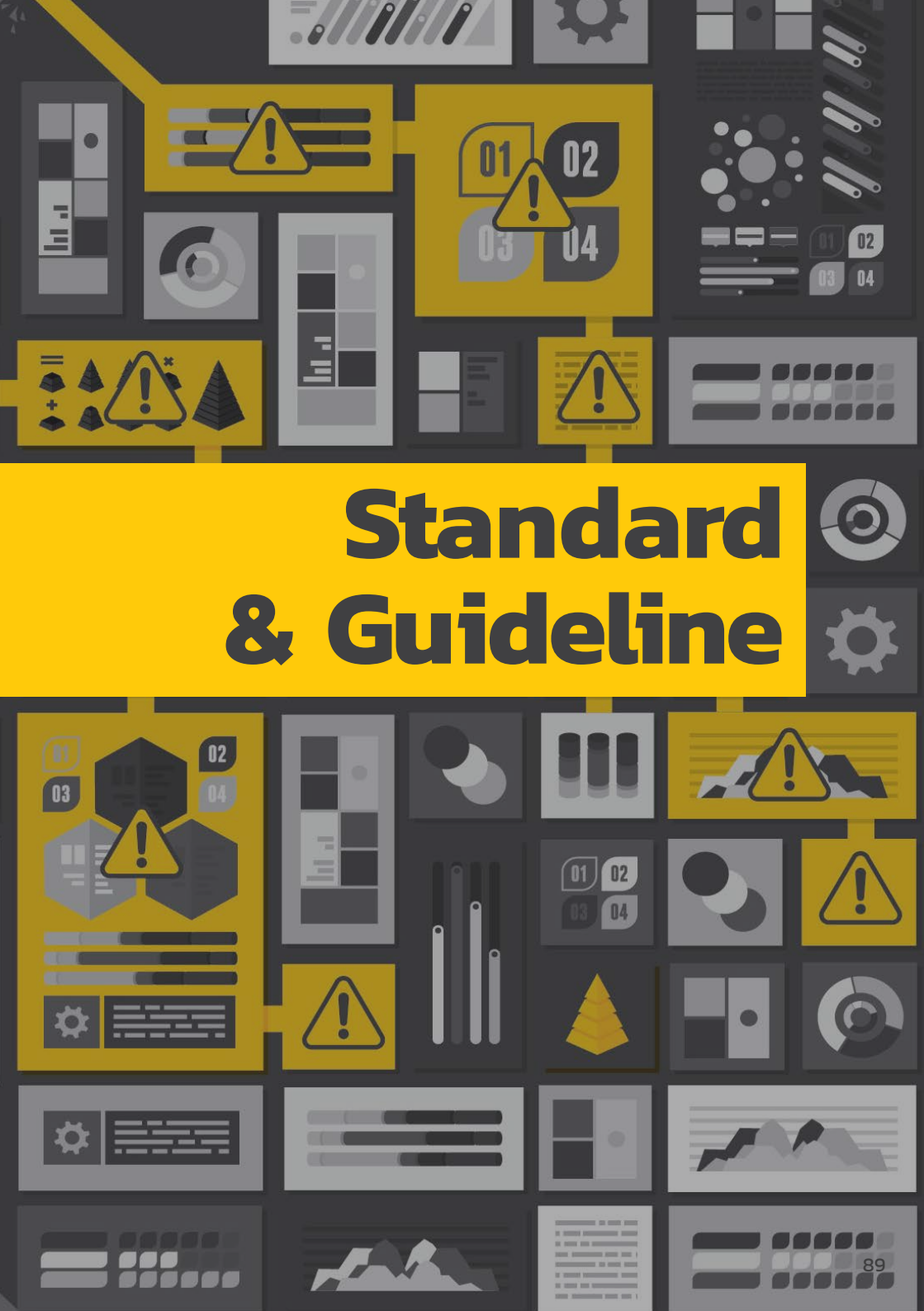
(https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/)

สำหรับผู้ใช้บริการ True Move H ปัจจุบันทางไทยเซิร์ตอยู่ระหว่างการประสานงานเพื่อยืนยันความถูกต้องของข้อมูล โดยในระหว่างนี้ควรตรวจสอบว่าใช้ข้อมูลใดในการลงทะเบียนกับผู้ให้บริการ รวมถึงอาจพิจารณาแจ้งความลงบันทึกประจำวันไว้เป็นหลักฐานในกรณีหากเกิดเหตุการณ์ผู้ประสงค์ร้ายนำข้อมูลที่หลุดรั่วออกไปใช้ในการสวมรอยหรือปลอมแปลงตัวบุคคล ซึ่งอาจส่งผลกระทบทางกฎหมายได้

The Register
http://thcert.co/Zld1fd
Niall Merrigan
http://thcert.co/i1t2x5
14/4/2561


01
02
03
04


01
02
03
04
88


Standard
& Guideline

NIST เผยแพร่เอกสาร Risk Management Framework 2.0 ครอบคลุมด้านความมั่นคงปลอดภัย ความเป็นส่วนตัว และห่วงโซ่อุปทาน

หน่วยงาน NIST ของสหรัฐอเมริกาได้เผยแพร่เอกสาร NIST Special Publication (SP) 800-37 Revision 2 ชื่อเต็มคือ Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (ชื่อย่อ RMF 2.0) โดยเอกสารนี้เป็นฉบับปรับปรุงจากเวอร์ชันก่อนหน้า

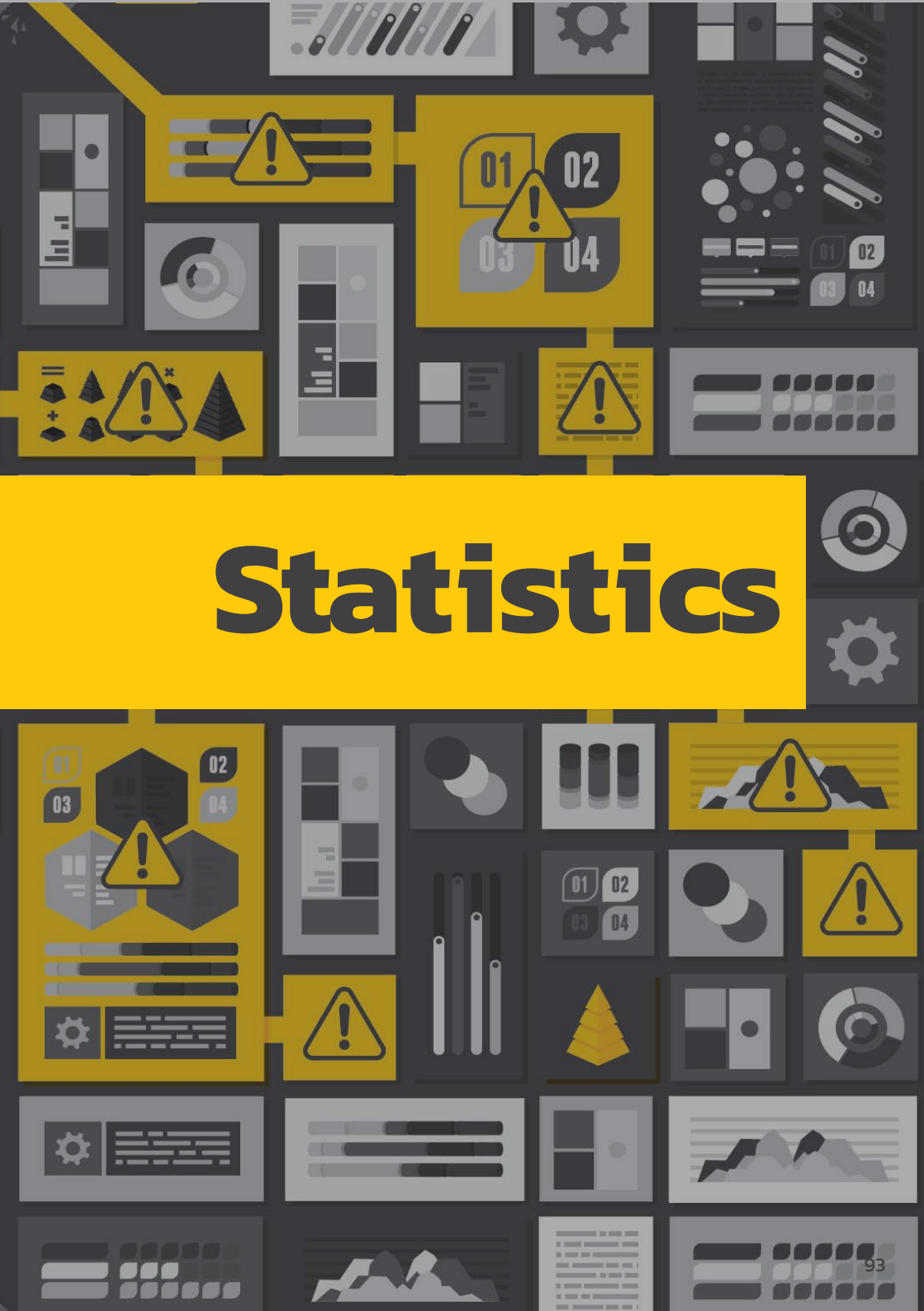
ทาง NIST เผยว่า RMF 2.0 นี้เป็นกรอบการทำงานที่ครอบคลุมทั้งด้านความมั่นคงปลอดภัย ความเป็นส่วนตัว และห่วงโซ่อุปทาน จุดประสงค์หลักเพื่อใช้เป็นแนวทางบริหารจัดการความเสี่ยงของระบบสารสนเทศภายในองค์กร โดยเนื้อหาจะมีตั้งแต่เรื่องแนวคิด โครงสร้าง กระบวนการทำงาน การควบคุม การประเมินผล และการเฝ้าระวัง ตัวเอกสารมีทั้งหมด 183 หน้า ผู้ที่สนใจสามารถดาวน์โหลดได้จากเว็บไซต์ของ NIST

https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Healthcare IT News
http://thcert.co/cXmFzt
NIST
http://thcert.co/oyKDcO
26/12/2561


01
02
03
04


01
02
03
04


Statistics

สถานศึกษาใน UK ประสบปัญหาข้อมูลรั่วไหลมากกว่า 700 ครั้ง ในปี 2559-2560

หน่วยงาน Information Commissioners Office (ICO) ของสหราชอาณาจักรได้เปิดเผยว่าในช่วงปี 2559-2560 มีรายงานว่าสถานศึกษาประสบปัญหาข้อมูลรั่วไหลทั้งหมด 703 ครั้ง โดยส่วนใหญ่เป็นโรงเรียน เนื่องจากมีข้อมูลทางการเงินเก็บบันทึกไว้เป็นจำนวนมากแต่ไม่ได้มีงบประมาณในการดูแลด้านความมั่นคงปลอดภัยของข้อมูลที่เพียงพอ นอกจากโรงเรียนแล้ว สถานศึกษาแหล่งอื่นเช่นสถานรับเลี้ยงเด็กหรือมหาวิทยาลัยก็มีรายงานความเสียหายจากเหตุการณ์ข้อมูลรั่วไหลเพิ่มขึ้นมากเช่นกัน

การเจาะระบบเพื่อขโมยข้อมูลจากสถานศึกษานั้นส่งผลกระทบทั้งในแง่ชื่อเสียงและข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งข้อมูลส่วนตัวของเด็กและข้อมูลทางการเงินของผู้ปกครอง เนื่องจากปัจจุบันนี้ข้อมูลส่วนใหญ่จะถูกเก็บบันทึกในรูปแบบอิเล็กทรอนิกส์ ผู้ที่เก็บบันทึกข้อมูลเหล่านี้ควรตรวจสอบเพื่อให้แน่ใจว่ามาตรการและวิธีการป้องกันข้อมูลนั้นเพียงพอรวมถึงมีช่องทางการตรวจสอบและรายงานให้กับผู้เสียหายและหน่วยงานที่ดูแลหากเกิดเหตุการณ์ข้อมูลรั่วไหล

UHY-UK
http://thcert.co/QE21TS
26/11/2561

ผู้บริโภคกว่า 1 ใน 5 บอกว่าจะไม่กลับไปเป็นลูกค้าของบริษัทที่ทำข้อมูลรั่วไหล ส่วนใหญ่มองว่าเป็นความผิดของบริษัทมากกว่าคนเจาะระบบ

ผลสำรวจจากบริษัท PCI Pal เผยข้อมูลความสำคัญของปัญหาด้านความมั่นคงปลอดภัยและความเชื่อมั่นของลูกค้าต่อธุรกิจ โดยพบว่า 44% ของผู้บริโภคในสหรัฐอเมริกาเคยประสบปัญหาจากเหตุการณ์ข้อมูลรั่วไหลหรือระบบถูกแฮก หนึ่งในข้อมูลที่สำคัญคือผู้บริโภคกว่า 1 ใน 5 บอกว่าจะไม่กลับไปเป็นลูกค้าของบริษัทที่ทำข้อมูลรั่วไหล ผลสำรวจนี้เป็นข้อมูลสนับสนุนที่ดีว่าการลงทุนทางด้านความมั่นคงปลอดภัยไซเบอร์นั้นช่วยลดความเสียหายด้านธุรกิจได้มาก อีกหนึ่งเรื่องที่มีความสำคัญไม่แพ้กันคือนโยบายการรักษาข้อมูลของลูกค้า โดยผลสำรวจพบว่าผู้บริโภค 45% จะไม่ค่อยซื้อสินค้าจากบริษัทที่มีแนวโน้มว่าไม่มีมาตรการปกป้องข้อมูลของลูกค้าที่ดีพอ ในขณะที่ผู้บริโภค 26% บอกว่าบริษัทไหนที่ดูแลข้อมูลของลูกค้าไม่ดีจะไม่ใช้บริการเลย นอกจากเรื่องความมั่นคงปลอดภัยในการซื้อขายสินค้าออนไลน์แล้ว ผู้บริโภค 42% ยังบอกว่าไม่สะดวกใจที่จะให้ข้อมูลสำคัญเช่นหมายเลขบัตรเครดิตผ่านทางโทรศัพท์ ซึ่งสิ่งนี้เป็นเรื่องที่ศูนย์บริการลูกค้าควรต้องนำไปพิจารณาปรับปรุงกระบวนการทำงาน

ก่อนหน้านี้ ผลสำรวจจากบริษัท RSA ก็ให้มุมมองคล้ายๆ กัน โดยเป็นการสอบถามข้อมูลจากผู้บริโภคทั้งสหรัฐอเมริกา สหราชอาณาจักร ฝรั่งเศส เยอรมนี และอิตาลี โดยพบว่าผู้บริโภค 69% จะยกเลิกการเป็นลูกค้าของบริษัทที่ไม่มีการรักษาข้อมูลส่วนบุคคลที่ดีพอ โดยผู้บริโภคกว่าครึ่ง (62%) มองว่าหากเกิดเหตุการณ์ข้อมูลรั่วไหลจะเป็นความผิดของบริษัทที่หละหลวมด้านความมั่นคงปลอดภัยมากกว่าจะมองว่าเป็นความผิดของผู้เจาะระบบ ข้อมูลจากผลสำรวจเหล่านี้มีหลายประเด็นที่เป็นเรื่องสำคัญซึ่งบริษัทที่มีการเก็บข้อมูลส่วนบุคคลของลูกค้าควรตระหนักและพิจารณา

Infosecurity magazine
http://thcert.co/k6r3sl
Infosecurity magazine
http://thcert.co/cEj1mM
30/10/2561

สถิติข้อมูลรั่วไหลทั่วโลก ครึ่งแรกของปี 2018 มีข้อมูลหลุดกว่า 4.5 พันล้านรายการ เกินครึ่งเป็นการขโมยข้อมูลจากบุคคลภายนอก

บริษัท Gemalto เปิดเผยรายงานสถิติข้อมูลรั่วไหล (data breach) ตลอดครึ่งปี 2018 โดยพบว่าจำนวนข้อมูลที่หลุดรั่วออกไปรวมแล้วมีมากกว่า 4.5 พันล้านรายการ โดยประเภทขององค์กรที่พบปัญหาข้อมูลรั่วไหลมากที่สุดคือหน่วยงานด้านสาธารณสุข

รูปแบบของการโจมตีที่พบมากที่สุดคือการขโมยตัวตน (identity theft) ช่องทางการโจมตีที่พบมากที่สุดคือการบุกรุกจากบุคคลภายนอก (malicious outsider) นอกจากนี้ จากสถิติมีข้อมูลสำคัญอีกอย่างหนึ่งคือในบรรดาข้อมูลที่หลุดรั่วออกไปนั้น มีไม่ถึง 3% ที่ถูกเข้ารหัสลับข้อมูลไว้ ซึ่งจะช่วยให้ผู้ที่ได้ข้อมูลไปจะนำไปใช้งานต่อได้ลำบากหรืออาจไม่ได้เลย

ทาง Gemalto เผยแพร่ข้อมูลสถิติทั้งแบบ infographics และรายงานฉบับเต็ม ผู้ที่สนใจสามารถดาวน์โหลดได้จากเว็บไซต์

https://breachlevelindex.com

Naked Security
http://thcert.co/I5izER
Help Net Security
http://thcert.co/vrwDLh
11/10/2561

รายงานเผยแอปไม่พึงประสงค์บนมือถือเพิ่ม 12,000 รายการในไตรมาส 2 พบแอปปลอมหลอกผู้ใช้ MyEtherWallet เพื่อขโมยสกุลเงินคริปโต

รายงาน Mobile Threat Landscape Q2 2018 โดยบริษัท RiskIQ ได้เปิดเผยสถิติแอปพลิเคชันไม่พึงประสงค์ที่ถูกตรวจพบจากแหล่งดาวน์โหลดแอปพลิเคชันมากกว่า 120 แห่ง โดยพบว่า ตรวจพบแอปพลิเคชันไม่พึงประสงค์เพิ่มขึ้น 12,000 รายการในไตรมาสที่ 2 เทียบกับไตรมาสที่ 1 และตรวจพบใน Google Play เป็นจำนวนสูงถึง 28,533 รายการ ตัวอย่างแอปพลิเคชันไม่พึงประสงค์ที่ถูกตรวจพบที่น่าสนใจ เช่น

1. แอปพลิเคชันปลอมเป็นแอปพลิเคชันทางการของ MyEtherWallet ซึ่งให้บริการบัญชีออนไลน์เก็บสกุลเงินคริปโต ในแอปพลิเคชันปลอมมีหน้าเว็บไซต์ปลอมเพื่อขโมยรหัสผ่านบัญชีออนไลน์ดังกล่าว

2. แอปพลิเคชันช่วยประหยัดแบตเตอรี่ของเครื่องโทรศัพท์มือถือ ซึ่งขอสิทธิเกินความจำเป็น เช่น การอ่าน SMS ตำแหน่ง GPS และหมายเลขโทรศัพท์มือถือ การตั้งค่าระบบ พบว่าแพร่กระจายในเครื่องเป็นจำนวนมากกว่า 60,000 เครื่อง

3. Firebase เป็นบริการฐานข้อมูลสำหรับผู้พัฒนาเว็บไซต์หรือแอปพลิเคชันเพื่อใช้เก็บข้อมูลต่าง ๆ เช่น ข้อมูลของผู้ที่เข้าเว็บไซต์หรือใช้งานแอปพลิเคชัน บริษัทด้านความมั่นคงปลอดภัยของแอปพลิเคชัน Appthority พบว่ามีฐานข้อมูล 2,300 แห่งที่ถูกใช้โดย 3000 แอปพลิเคชัน ที่เปิดให้สาธารณะเข้าถึงได้ เนื่องจากเป็นค่าเริ่มต้น โดยพบว่าเป็นข้อมูลรหัสผ่านและไอดี 2.6 ล้านรายการ

จะเห็นได้ว่าภัยคุกคามบนโทรศัพท์มือถือมีแนวโน้มเพิ่มขึ้น และมีการโจมตีที่หลากหลาย ก่อนหน้านี้ในประเทศไทย เคยพบแอปพลิเคชันปลอมของธนาคาร

(https://www.thaicert.or.th/alerts/user/2014/al2014us008.html)

ผู้ใช้จึงควรระวังตรวจสอบกับองค์กรให้แน่ใจว่าเป็นแอปพลิเคชันขององค์กรจริง รวมถึงตรวจสอบสิทธิที่แอปพลิเคชันขอก่อนติดตั้งว่ามีการขอสิทธิเกินความจำเป็นหรือไม่ ในขณะที่ผู้พัฒนาแอปพลิเคชันควรป้องกันฐานข้อมูลไม่เปิดให้สาธารณะเข้าถึง

สำหรับผู้ที่สนใจสามารถอ่านรายงานฉบับเต็มได้จากที่มา

RiskIQ
http://thcert.co/5hCcao
24/9/2561

รายงานแนวโน้มภัยคุกคามไซเบอร์ในยุโรป ของ Europol เผย มัลแวร์เรียกค่าไถ่เริ่มชะลอตัวแต่คงเป็นภัยคุกคามหลัก

ในเดือนกันยายน 2561 Europol ได้เผยแพร่รายงาน the 2018 Internet Organised Crime Threat Assessment(IOCTA) ซึ่งเป็นรายงานแนวโน้มภัยคุกคามไซเบอร์ที่พบในกลุ่มประเทศอียูประจำปี 2561 มีสาระสำคัญที่น่าสนใจดังนี้

1. ถึงแม้การเพิ่มขึ้นของการแพร่กระจายมัลแวร์เรียกค่าไถ่จะชะลอตัวลง แต่ก็ยังคงเป็นภัยคุกคามไซเบอร์หลักที่มีจุดประสงค์ด้านการเงิน และยังคงมีแนวโน้มเป็นภัยคุกคามหลักในอีกหลายปี

2. พบการเผยแพร่เนื้อหาลามกอนาจารเด็กเพิ่มมากขึ้น โดยเผยแพร่บนเว็บไซต์ประเภท Darknet พบว่ามีการถ่ายทอดสดเนื้อหาซึ่งการสืบสวนทำได้ยากด้วยเทคโนโลยีที่ซับซ้อนรวมถึงระบบที่ต้องการเข้าไปตรวจสอบไม่อยู่ในขอบเขตอำนาจของหน่วยงาน

3. ยังคงพบการโจมตีรูปแบบ DDoS ทั้งในภาคเอกชนและภาครัฐ ถือเป็นการโจมตีที่พบบ่อยที่สุด มีแนวโน้มที่การโจมตีรูปแบบนี้จะมีค่าใช้จ่ายที่ถูกลง เสี่ยงต่อการถูกจับน้อยลง และทำได้ง่ายขึ้น

4. การปลอมบัตรเครดิตยังคงเป็นปัญหาที่พบอย่างต่อเนื่องถึง แม้ว่าจะลดลงในปีแล้วด้วยมาตรการ Geoblocking ซึ่งผู้ใช้สามารถตั้งค่าบล็อกการใช้งานบัตรในประเทศที่มีความเสี่ยง เพื่อป้องกันกรณีผู้ประสงค์ร้ายขโมยข้อมูลบัตรของเหยื่อและสร้างบัตรเครดิตปลอมแล้วถอนในเงินในต่างประเทศ

5. พบการใช้สกุลเงินคริปโต โดยเฉพาะ Bitcoin ในการดำเนินการก่ออาชญากรรม เช่น การฟอกเงิน รวมถึงผู้ใช้ ผู้ขุด ผู้ให้บริการแลกเปลี่ยนเงินสกุลคริปโต ก็ตกเป็นเหยื่อก็การโจมตีเพื่อขโมยเงินหรือข้อมูลส่วนบุคคล

6. แนวโน้มภัยคุกคามใหม่ที่พบคือการเจาะระบบเว็บไซต์ฝังโค้ดไม่พึงประสงค์ ส่งผลให้เครื่องที่มาเยี่ยมชมเว็บไซต์ถูกใช้ขุดสกุลเงินคริปโตให้ผู้ประสงค์ร้าย หรือการเผยแพร่มัลแวร์ที่แอบขุดสกุลเงินดังกล่าวในเครื่องเหยื่อ

7. เว็บไซต์ Darknet ยังคงถูกใช้เป็นช่องทางในการซื้อขายของผิดกฎหมายถึง แม้ว่าเมื่อปีที่ผ่านมาได้มีการใช้อำนาจทางกฎหมายปิด 3 เว็บไซต์ใหญ่คือ AlphaBay, Hansa และ RAMP

ในรายงานยังได้พูดถึงความสำเร็จปฏิบัติการรับมือภัยคุกคามไซเบอร์ ซึ่งเกิดจากความร่วมมือระหว่างหน่วยงานตำรวจ หน่วยงานเอกชน และหน่วยงานภาควิชาการ ในขณะที่ในปี 2561 มีการใช้งานกฎหมายหลายฉบับ เช่น General Data Protection Regulation (GDPR), Network and Information Security (NIS) directive and 5G technology ซึ่งส่งผลกระทบต่อความสามารถในการสืบสวน ผู้ที่สนใจสามารถศึกษารายงานฉบับเต็มได้จากที่มา

Europol
http://thcert.co/Yg3mEB
24/9/2561

รายงานเผย 6 เดือน เกิดโจรกรรมสกุลเงินคริปโตกว่า 1.1 พันล้านดอลลาร์ ส่วนใหญ่มุ่งเป้าเว็บไซต์แลกเปลี่ยนสกุลเงิน

เนื่องจากความนิยมในการใช้งานสกุลเงินคริปโต เช่น Bitcoin ที่เพิ่มขึ้นอย่างมากในหลายปีที่ผ่านมา ทำให้การโจมตีเพื่อขโมยสกุลเงินดังกล่าวเริ่มพบมากขึ้นเรื่อย ๆ ยกตัวอย่างเช่น กรณี ในเดือนมิถุนายน เว็บไซต์แลกเปลี่ยนสกุลเงินคริปโตของประเทศเกาหลีที่ชื่อ Coilrail ซึ่งเป็นหนึ่งในร้อยระบบบริการแลกสกุลเงินที่ถูกใช้งานสูงสุด ถูกขโมยเงินเกิดความสูญเสียหลายสิบล้านดอลล่าร์

เมื่อเดือนมิถุนายน บริษัทด้านความมั่นคงปลอดภัย Carbon Black ได้เผยแพร่รายงาน Cryptocurrency Gold Rush on the Dark Web ระบุข้อมูลแนวโน้มการโจมตีไซเบอร์ที่เกี่ยวกับสกุลเงินครีปโตจาก dark web ซึ่งเป็นเว็บไซต์ที่มีลักษณะซ่อนตัว ไม่ปรากฏในผลการค้นหาเว็บไซต์ มักถูกใช้ในการแลกเปลี่ยนซื้อของ หรือการกระทำอื่น ๆ ที่ผิดกฎหมาย โดยในรายงานมีสาระสำคัญดังนี้

1. ในช่วง 6 เดือนที่ผ่านมา พบการขโมยเงินสกุลคริปโตรวมมูลค่า 1.1 พันล้านดอลล่าร์

2. อาชญากรไซเบอร์นิยมใช้สกุลเงิน Monero ในการทำธุรกรรมซื้อขายที่ผิดกฎหมายมากกว่า Bitcoin เนื่องจากทำธุรกรรมได้เร็วกว่ามีความเป็นส่วนตัว ยากแก่การตรวจสอบ และเสียค่าใช้จ่ายในการทำธุรกรรมน้อยกว่า

3. รูปแบบการโจมตีเพื่อขโมยเงินสกุลเงินคริปโต อาชญากรไซเบอร์ส่วนใหญ่จะโจมตีโดยใช้มัลแวร์เพื่อขโมยเงิน โดยพบ dark web กว่า 12,000 เว็บไซต์ แสดงข้อเสนอขายมัลแวร์เพื่อที่ใช้ในการขโมยเงินสกุลคริปโตกว่า 34,000 รายการ ซึ่งส่วนใหญ่ ออกแบบสำหรับบุคคลที่ไม่มีความเชี่ยวชาญทางเทคนิค ให้สามารถใช้งานเครื่องมือได้ง่าย และใช้โจมตีระบบที่มีช่องโหว่สูง ราคาตั้งแต่ 1 - 1,000 ดอลล่าร์ ตลาดโดยรวมในการซื้อขายมัลแวร์มูลค่ากว่า 6.7 ล้านดอลล่าร์

4. ในการโจมตีส่วนใหญ่ที่พบเกิดกับเว็บไซต์ให้บริการแลกเปลี่ยนสกุลเงินคริปโต (27%) รองลองมาได้แก่ บริษัท (21%) บุคคลทั่วไป (14%) และหน่วยงานรัฐ (7%)

จะเห็นได้ว่า มัลแวร์ได้ถูกออกแบบให้ใช้งานได้ง่าย ทำให้การขโมยสกุลเงินคริปโตเริ่มทำได้ง่ายขึ้น ผู้ใช้ทั่วไปและบริษัทที่ใช้งานสกุลเงินคริปโตควรมีมาตรการป้องกันที่ดี อัปเดตระบบเพื่อปิดช่องโหว่ อาจพิจารณาแยกเครื่องทำธุรกรรมเกี่ยวกับสกุลเงินคริปโตออกจากเครื่องที่ใช้งานทั่วไปเพื่อลดความเสี่ยง ในส่วนการใช้งานเว็บไซต์แลกเปลี่ยนสกุลเงิน ควรตั้งค่ายืนยันตัวตนแบบ 2 ขั้นตอน ไม่ใช้รหัสผ่านที่คาดเดาง่าย และนำเงินออกจากเว็บไซต์หลังจากที่แลกเปลี่ยนเสร็จ ไม่ใช้เป็นที่เก็บเงินถาวร

Bank Info Security
http://thcert.co/QMZU19
Carbon Black
http://thcert.co/sDIpTL
13/6/2561


01
02
03
04


01
02
03
04
01
02
03
04
102


Vulnerability
& Patch

อัปเดตด่วน พบการใช้ช่องโหว่ร้ายแรงใน Internet Explorer ที่ทำให้เครื่องถูกแฮกได้

เมื่อวันที่ 19 ธันวาคม 2561 บริษัท Microsoft ได้ออกแพตช์แก้ไขช่องโหว่ความร้ายแรงระดับวิกฤติ (Critical) ในโปรแกรม Internet Explorer โดยช่องโหว่นี้อยู่ในไลบรารี Scripting Engine ที่ใช้สำหรับประมวลผลสคริปต์ในหน้าเว็บไซต์ ตัวช่องโหว่นี้เป็นประเภท remote code execution มีผลให้ผู้ประสงค์ร้ายสามารถติดตั้ง สั่งเรียกใช้งานโปรแกรม หรือควบคุมเครื่องคอมพิวเตอร์ของเหยื่อได้ การโจมตีจะใช้วิธีหลอกให้เหยื่อเข้าไปยังเว็บไซต์ที่มีคำสั่งอันตรายฝังอยู่ หากใช้ Internet Explorer เวอร์ชันที่มีช่องโหว่เปิดเข้าไปยังเว็บไซต์ดังกล่าวก็อาจถูกแฮกเครื่องได้ทันที ช่องโหว่นี้มีรหัส CVE-2018-8653

การเผยแพร่แพตช์ในครั้งนี้เป็นแบบเร่งด่วน อยู่นอกเหนือจากรอบการอัปเดตตามปกติ เนื่องจากพบว่ามีการใช้ช่องโหว่นี้โจมตีแล้ว อย่างไรก็ตาม รายละเอียดการโจมตีนั้นยังไม่ได้เปิดเผยสู่สาธารณะ

ผู้ใช้และผู้ดูแลระบบควรติดตั้งแพตช์โดยเร็วที่สุด หากยังไม่สามารถทำได้ อาจใช้วิธีแก้ปัญหาเฉพาะหน้า (Workarounds) ด้วยการจำกัดสิทธิ์ไลบรารี Scripting Engine เพื่อลดผลกระทบหากถูกโจมตี โดยศึกษาวิธีการตั้งค่าได้จากเว็บไซต์ของ Microsoft (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8653)

ทั้งนี้ วิธีแก้ปัญหาแบบเฉพาะหน้าอาจมีปัญหากับบางเว็บไซต์ทำให้ไม่สามารถใช้งานได้ตามปกติงานสกุลเงินคริปโตควรมีมาตรการป้องกันที่ดี อัปเดตระบบเพื่อปิดช่องโหว่ อาจพิจารณาแยกเครื่องทำธุรกรรมเกี่ยวกับสกุลเงินคริปโต ออกจากเครื่องที่ใช้งานทั่วไปเพื่อลดความเสี่ยง

ในส่วนการใช้งานเว็บไซต์แลกเปลี่ยนสกุลเงิน ควรตั้งค่ายืนยันตัวตนแบบ 2 ขั้นตอน ไม่ใช้รหัสผ่านที่คาดเดาง่าย และนำเงินออกจากเว็บไซต์หลังจากที่แลกเปลี่ยนเสร็จ ไม่ใช้เป็นที่เก็บเงินถาวร

The Register
http://thcert.co/gB3iAW
20/12/2561

Microsoft และ Adobe ออกแพตช์ประจำเดือนธันวาคม 2018 แก้ไขช่องโหว่ร้ายแรงที่ถูกใช้ในการโจมตีจริงแล้ว

เมื่อวันที่ 11 ธันวาคม 2561 ทาง Microsoft และ Adobe ได้ออกแพตช์แก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยประจำเดือนธันวาคม โดยมีการแก้ไขช่องโหว่ระดับวิกฤติ (Critical) ที่เคยถูกใช้ในการโจมตีหน่วยงานในต่างประเทศมาแล้ว ผู้ดูแลระบบควรตรวจสอบและอัปเดตระบบที่ใช้งานอยู่เพื่อลดโอกาสที่จะเกิดความเสียหาย

แพตช์ของ Microsoft แก้ไขช่องโหว่ทั้งหมด 39 จุด โดยมี 9 จุดเป็นช่องโหว่ระดับวิกฤติแต่ยังไม่พบว่าเคยถูกใช้ในการโจมตีมาก่อน อย่างไรก็ตาม มีช่องโหว่ 1 จุดที่เป็นระดับ Important แต่เคยถูกใช้ในการโจมตีมาแล้ว คือช่องโหว่รหัส CVE-2018-8611 ที่เป็นประเภทยกระดับสิทธิ์จากผู้ใช้ทั่วไปเป็นผู้ดูแลระบบ (Elevation of Privilege) ก่อนหน้านี้มีรายงานว่าพบมัลแวร์ที่ใช้เทคนิคนี้ในการโจมตีมาแล้ว

สำหรับแพตช์ของ Adobe หลักๆ จะเน้นการแก้ไขช่องโหว่ของ Adobe Acrobat และ Adobe Reader เป็นหลัก โดยแก้ไขช่องโหว่ทั้งหมด 9 จุด ซึ่งมี 6 จุดเป็นช่องโหว่ระดับวิกฤติที่ส่งผลให้ผู้ประสงค์ร้ายสามารถสั่งประมวลผลคำสั่งอันตรายบนเครื่องของเหยื่อได้

Krebs on Security
http://thcert.co/qgCJY8
Bleeping Computer
http://thcert.co/q2Qcx2
13/12/2561

Adobe ออกแพตช์แก้ไขช่องโหว่ร้ายแรงใน Flash Player หลังถูกพบใช้โจมตีหน่วยงานในรัสเซีย

เมื่อวันที่ 5 ธันวาคม 2561 บริษัท Adobe ได้ออกอัปเดตโปรแกรม Flash Player เวอร์ชัน 32.0.0.101 เพื่อแก้ไขช่องโหว่ร้ายแรงที่ส่งผลให้ผู้ประสงค์ร้ายสามารถติดตั้งมัลแวร์ลงในเครื่องของเหยื่อได้ โดยช่องโหว่นี้มีรหัส CVE-2018-15982

เมื่อปลายเดือนพฤศจิกายน 2561 บริษัทด้านความมั่นคงปลอดภัยไซเบอร์จากประเทศจีนได้รายงานการโจมตีหน่วยงานในประเทศรัสเซีย โดยผู้ประสงค์ร้ายใช้วิธีส่งอีเมล ที่ข้างในมีไฟล์แนบเป็น .rar เมื่อแตกไฟล์ออกมาจะพบ 2 ไฟล์คือ .docx และ .jpg โดยหากเปิดไฟล์ .docx ขึ้นมา ในไฟล์ดังกล่าวจะมีสคริปต์สำหรับโจมตีช่องโหว่ของ Flash Player ซึ่งจุดประสงค์ของสคริปต์นี้คือการสกัดมัลแวร์ออกมาจากไฟล์ .jpg แล้วติดตั้งลงในเครื่องของเหยื่อ (ดูภาพประกอบอธิบายกระบวนการโจมตีได้จากที่มา) ภายหลังจากที่ทาง Adobe ได้รับแจ้งก็ได้เร่งออกอัปเดตมาเพื่อแก้ไขปัญหาทันที ทั้งนี้ ตัวอัปเดตที่ถูกปล่อยออกมาได้มีการแก้ไขช่องโหว่รหัส CVE-2018-15983 ด้วย แต่ยังไม่มีรายงานการโจมตีโดยใช้ช่องโหว่ดังกล่าว

หากผู้ใช้ติดตั้ง Google Chrome, Microsoft Edge, หรือ Internet Explorer 11 อัปเดตของ Flash Player จะถูกดาวน์โหลดมาติดตั้งโดยอัตโนมัติพร้อมกับตัวเบราว์เซอร์เวอร์ชันใหม่ แต่หากผู้ใช้มีการดาวน์โหลด Flash Player มาติดตั้งเอง ก็สามารถดาวน์โหลดอัปเดตเวอร์ชันล่าสุดได้จากเว็บไซต์ของ Adobe หรือจากหน้าอัปเดตของตัวโปรแกรม

(https://helpx.adobe.com/security/products/flash-player/apsb18-42.html)

Softpedia
http://thcert.co/21aR2T
Security Affairs
http://thcert.co/xZ855O
Malwarebytes
http://thcert.co/YsaION
6/12/2561

พบบั๊กใน Gmail ผู้ประสงค์ร้ายสามารถปลอมอีเมลว่าถูกส่งออกมาจากบัญชีของเหยื่อได้ อาจถูกใช้ในการหลอกลวง

นักพัฒนาซอฟต์แวร์ชื่อ Tim Cotten ได้รายงานข้อผิดพลาดใน Gmail โดยพบว่าถ้ามีอีเมลที่ถูกปลอมชื่อผู้ส่งให้เป็นอีเมลเจ้าของบัญชี อีเมลฉบับดังกล่าวอาจจะไม่เข้าไปอยู่ในส่วน Inbox เพราะระบบมองว่าที่อยู่อีเมลกับไอพีของเครื่องที่ส่งมาไม่ตรงกัน แต่อีเมลฉบับนี้จะไปอยู่ในส่วน Sent เพราะระบบของ Gmail ไม่ได้ตรวจสอบความถูกต้องของข้อมูลผู้ส่ง (ตรวจสอบแค่ว่าชื่อผู้ส่งตรงกับที่อยู่อีเมลเจ้าของบัญชี) ผลกระทบจากข้อผิดพลาดนี้ทำให้ผู้ประสงค์ร้ายสามารถปลอมอีเมลให้เหมือนกับว่าถูกส่งออกมาจากบัญชีของเหยื่อได้

ตัวอย่างผลกระทบที่อาจเกิดขึ้นได้จากการอาศัยข้อผิดพลาดนี้ เช่น ผู้ประสงค์ร้ายส่งอีเมลโดยแนบลิงก์หรือไฟล์ที่มีอันตรายมาด้วย โดยอีเมลฉบับดังกล่าวจะปลอมชื่อผู้ส่งว่าถูกส่งออกมาจากบัญชี Gmail ของเหยื่อ จากนั้นส่งอีเมลปกติไปสอบถามความคืบหน้าหรือขอข้อมูลเพิ่มเติมโดยอ้างว่าเป็นเรื่องต่อเนื่องจากอีเมลที่ได้รับมาก่อนหน้านี้ เมื่อเหยื่อได้รับอีเมลก็อาจเปิดดูรายการอีเมลในช่อง Sent หากพบอีเมลต้องสงสัยที่ตนเองไม่ได้เป็นผู้ส่งก็อาจคลิกลิงก์หรือเปิดดูไฟล์ข้างในได้ อีกหนึ่งกรณีที่เป็นไปได้คือผู้ประสงค์ร้ายอาจใช้ช่องทางนี้ในการหลอกลวงว่าสามารถแฮกอีเมลของเหยื่อได้โดยแอบอ้างว่าสามารถส่งอีเมลออกจากบัญชีของเหยื่อทั้งที่ไม่ได้ทำจริง เป็นต้น

ผู้ที่ค้นพบข้อผิดพลาดนี้แจ้งว่าได้รายงานให้ทางทีม Gmail ทราบแล้ว โดยสถานะปัจจุบันยังไม่ยืนยันว่าเป็นเฉพาะบนเว็บไซต์หรือแอปพลิเคชันบนมือถือด้วย ระหว่างที่รอการตรวจสอบและแก้ไข ผู้ใช้ Gmail อาจต้องใช้ความระมัดระวังโดยการพิจารณาอีเมลที่อยู่ในช่อง Sent โดยหากพบอีเมลที่ไม่แน่ใจว่าตนเองเป็นผู้ส่งไม่ควรคลิกลิงก์หรือเปิดไฟล์แนบในอีเมลฉบับดังกล่าว หากสงสัยว่าบัญชี Gmail ถูกเข้าถึงโดยไม่ได้รับอนุญาตจริงหรือไม่สามารถตรวจสอบเพิ่มเติมได้ที่

https://myaccount.google.com/intro/security

HackRead
http://thcert.co/ioNaRO
Tim Cotten
http://thcert.co/p24XTB
Hacker News
http://thcert.co/sZN9ek
20/11/2561

Microsoft ปล่อยอัปเดตแก้ไขช่องโหว่ประจำเดือนพฤศจิกายน 2561 หลายช่องโหว่มีโค้ดโจมตีเผยแพร่สู่สาธารณะแล้ว

Microsoft ปล่อยอัปเดตด้านความมั่นคงปลอดภัยประจำเดือนพฤศจิกายน 2561 ให้กับซอฟต์แวร์หลายชุด เช่น Windows, Internet Explorer, Edge, รวมถึง Microsoft Office โดยในรอบนี้แก้ไขช่องโหว่ไปทั้งหมด 62 รายการ ปัญหาสำคัญที่ถูกแก้ไขในอัปเดตรอบนี้คือช่องโหว่ประเภท remote code execution ใน Microsoft Edge ที่ส่งผลให้ผู้ประสงค์ร้ายสามารถควบคุมเครื่องของเหยื่อได้ด้วยการหลอกให้เข้าไปยังเว็บไซต์ที่มีโค้ดอันตรายฝังอยู่ นอกจากนี้ยังมีการแก้ไขปัญหาช่องโหว่ที่ถูกเปิดเผยรายละเอียดวิธีการโจมตีมาก่อนหน้าที่จะมีแพตช์ด้วย ซึ่งหลายช่องโหว่ถูกนำมาใช้ในการโจมตีจริงแล้ว ผู้ใช้งานผลิตภัณฑ์ของ Microsoft ควรติดตั้งอัปเดตล่าสุด โดยสามารถศึกษาข้อมูลเพิ่มเติมได้จากเว็บไซต์ของ Microsoft

The Register
http://thcert.co/9sYON5
Microsoft
http://thcert.co/pkRNbO
15/11/2561

Cisco ออกอัปเดตแก้ไขช่องโหว่ร้ายแรงใน WebEx บน Windows ที่อาจส่งผลให้ถูกแฮกควบคุมเครื่องได้

นักพัฒนาซอฟต์แวร์ชื่อ Tim Cotten ได้รายงานข้อผิดพลาดใน Gmail โดยพบว่าถ้ามีอีเมลที่ถูกปลอมชื่อผู้ส่งให้เป็นอีเมลเจ้าของบัญชี อีเมลฉบับดังกล่าวอาจจะไม่เข้าไปอยู่ในส่วน Inbox เพราะระบบมองว่าที่อยู่อีเมลกับไอพีของเครื่องที่ส่งมาไม่ตรงกัน แต่อีเมลฉบับนี้จะไปอยู่ในส่วน Sent เพราะระบบของ Gmail ไม่ได้ตรวจสอบความถูกต้องของข้อมูลผู้ส่ง (ตรวจสอบแค่ว่าชื่อผู้ส่งตรงกับที่อยู่อีเมลเจ้าของบัญชี) ผลกระทบจากข้อผิดพลาดนี้ทำให้ผู้ประสงค์ร้ายสามารถปลอมอีเมลให้เหมือนกับว่าถูกส่งออกมาจากบัญชีของเหยื่อได้

ตัวอย่างผลกระทบที่อาจเกิดขึ้นได้จากการอาศัยข้อผิดพลาดนี้ เช่น ผู้ประสงค์ร้ายส่งอีเมลโดยแนบลิงก์หรือไฟล์ที่มีอันตรายมาด้วย โดยอีเมลฉบับดังกล่าวจะปลอมชื่อผู้ส่งว่าถูกส่งออกมาจากบัญชี Gmail ของเหยื่อ จากนั้นส่งอีเมลปกติไปสอบถามความคืบหน้าหรือขอข้อมูลเพิ่มเติมโดยอ้างว่าเป็นเรื่องต่อเนื่องจากอีเมลที่ได้รับมาก่อนหน้านี้ เมื่อเหยื่อได้รับอีเมลก็อาจเปิดดูรายการอีเมลในช่อง Sent หากพบอีเมลต้องสงสัยที่ตนเองไม่ได้เป็นผู้ส่งก็อาจคลิกลิงก์หรือเปิดดูไฟล์ข้างในได้ อีกหนึ่งกรณีที่เป็นไปได้คือผู้ประสงค์ร้ายอาจใช้ช่องทางนี้ในการหลอกลวงว่าสามารถแฮกอีเมลของเหยื่อได้โดยแอบอ้างว่าสามารถส่งอีเมลออกจากบัญชีของเหยื่อทั้งที่ไม่ได้ทำจริง เป็นต้น

ผู้ที่ค้นพบข้อผิดพลาดนี้แจ้งว่าได้รายงานให้ทางทีม Gmail ทราบแล้ว โดยสถานะปัจจุบันยังไม่ยืนยันว่าเป็นเฉพาะบนเว็บไซต์หรือแอปพลิเคชันบนมือถือด้วย ระหว่างที่รอการตรวจสอบและแก้ไข ผู้ใช้ Gmail อาจต้องใช้ความระมัดระวังโดยการพิจารณาอีเมลที่อยู่ในช่อง Sent โดยหากพบอีเมลที่ไม่แน่ใจว่าตนเองเป็นผู้ส่งไม่ควรคลิกลิงก์หรือเปิดไฟล์แนบในอีเมลฉบับดังกล่าว หากสงสัยว่าบัญชี Gmail ถูกเข้าถึงโดยไม่ได้รับอนุญาตจริงหรือไม่สามารถตรวจสอบเพิ่มเติมได้ที่

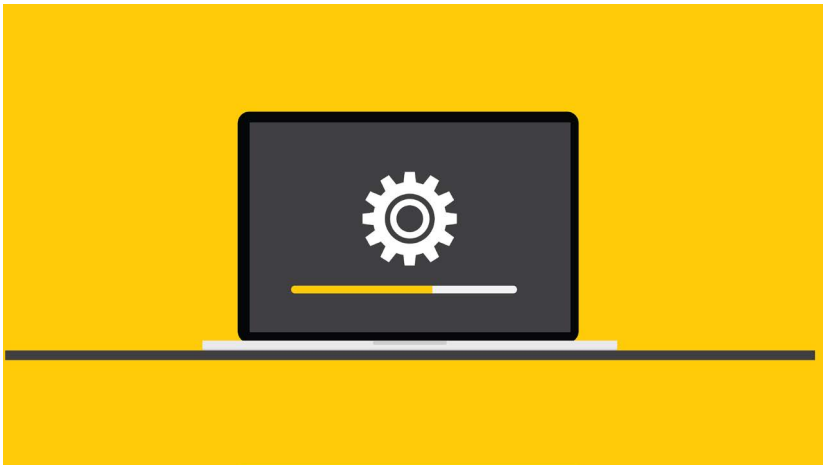
https://myaccount.google.com/intro/security

Cisco
http://thcert.co/TLBrTv
WebExec
http://thcert.co/c4NxtX
SkullSecurity
http://thcert.co/BNS8UY
25/10/2561

แจ้งเตือนผู้ใช้ Drupal รีบอัปเดต พบช่องโหว่ส่งผลให้ถูกควบคุมเครื่องได้

เมื่อวันที่ 17 ตุลาคม 2561 เว็บไซต์ทางการของ Drupal ได้ประกาศอัปเดตปิดช่องโหว่หลายรายการในซอฟต์แวร์ดังกล่าว ซึ่งส่วนหนึ่งเป็นช่องโหว่ส่งผลให้ผู้ประสงค์ร้ายสามารถสั่งประมวลผลคำสั่งอันตรายจากระยะไกลเพื่อควบคุมเครื่อง (Remote Code Execution)

ช่องโหว่เหล่านี้ส่งผลกระทบต่อ Drupal เวอร์ชัน 7 และ 8 ผู้ดูแลเว็บไซต์ที่ใช้งานซอฟต์แวร์ดังกล่าวควรอัปเดตเป็นเวอร์ชันล่าสุด (7.6, 8.5.8 และ 8.6.2) เพื่อปิดช่องโหว่



Drupal
http://thcert.co/MXQykK
19/10/2561

Tech Bureau บริษัทให้บริการแลกเปลี่ยนสกุลเงินคริปโตญี่ปุ่นถูกโจมตี สูญเงินมูลค่ากว่า 1,900 ล้านบาท

Microsoft ได้ออกแพตช์แก้ไขช่องโหว่ประจำเดือนตุลาคม 2561(https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/aa99ba28-e99f-e811-a978-000d3a33c573) โดยหนึ่งในนั้นเป็นการแก้ไขปัญหาร้ายแรงในเบราว์เซอร์ Microsoft Edge ที่อาจส่งผลให้ผู้ประสงค์ร้ายสามารถควบคุมเครื่องคอมพิวเตอร์ของเหยื่อได้โดยการหลอกให้เปิดหน้าเว็บไซต์ที่มีโค้ดอันตรายฝังอยู่ ช่องโหว่นี้มีรหัส CVE-2018-8495 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8495)

สาเหตุของช่องโหว่เกิดจากฟังก์ชันที่ใช้ในการจัดการโพรโทคอลนั้นสามารถเรียกใช้งานแอปพลิเคชันอื่นพร้อมส่งพารามิเตอร์ไปได้ด้วย ทำให้ผู้ประสงค์ร้ายสามารถใช้ช่องทางนี้ในการสั่งเปิดโปรแกรม Windows Script Host แล้วสั่งให้ประมวลผลสคริปต์อันตรายได้ ซึ่งสคริปต์ดังกล่าวอาจมีไว้เพื่อสั่งการควบคุมเครื่องคอมพิวเตอร์ของเหยื่อจากระยะไกล อย่างไรก็ตาม การจะโจมตีผ่านช่องโหว่นี้ได้สำเร็จ ผู้ใช้จำเป็นต้องคลิกอนุญาตให้มีการรันโปรแกรมจากภายนอกด้วย

นักวิจัยที่ค้นพบช่องโหว่นี้ได้เปิดเผยรายละเอียดและข้อมูลช่องโหว่ภายหลังจากที่ Microsoft ได้แก้ไขปัญหานี้แล้ว เนื่องจากข้อมูลการโจมตีถูกเผยแพร่สู่สาธารณะ อาจมีผู้ประสงค์ร้ายนำวิธีนี้ไปใช้โจมตีได้ ผู้ใช้งานระบบปฏิบัติการ Windows ควรติดตั้งอัปเดตเพื่อ ลดผลกระทบและแก้ไขปัญหา

Bleeping Computer
http://thcert.co/4qfELY
Abdulrahman Al-Qabandi
http://thcert.co/spHyuY
12/10/2561

แจ้งเตือน กล้องวงจรปิดหลายล้านเครื่องที่เข้าดูข้อมูลได้ผ่าน XMEye P2P Cloud มีช่องโหว่ร้ายแรง อาจถูกแฮกฝังมัลแวร์/แอบส่องดูภาพวิดีโอ

บริษัท SEC Consult รายงานว่ากล้องวงจรปิดและเครื่องบันทึกวิดีโอ (DVR) จำนวนหลายล้านเครื่องทั่วโลกมีช่องโหว่ที่ส่งผลให้ผู้ประสงค์ร้ายสามารถแฮกเข้ามาควบคุมอุปกรณ์ได้ โดยอุปกรณ์ส่วนใหญ่ที่มีปัญหานี้ถูกผลิตจากบริษัท Xiongmai ประเทศจีน สาเหตุเกิดจากอุปกรณ์เหล่านี้มีฟีเจอร์ชื่อ P2P Cloud ที่เปิดให้ผู้ใช้สามารถเข้ามาดูข้อมูลหรือตั้งค่าอุปกรณ์ได้ผ่านอินเทอร์เน็ต โดยการใช้แอปพลิเคชัน XMEye ในสมาร์ตโฟนหรือแอปพลิเคชัน VMS จากคอมพิวเตอร์

ทาง SEC Consult พบปัญหาสำคัญ 3 ประการที่ทำให้ผู้ใช้งานตกอยู่ในความเสี่ยง โดยปัญหาแรกคือข้อมูล (เช่น ภาพวิดีโอ) ของกล้องวงจรปิดนั้นถูกส่งขึ้นไปยังเซิร์ฟเวอร์ใน cloud โดยไม่มีการเข้ารหัสลับข้อมูล ไม่มีนโยบายการรักษาข้อมูลส่วนตัวที่ชัดเจน อีกทั้งช่องทางที่ใช้ส่งข้อมูลออกไปนั้นยังเปิดให้ผู้ประสงค์ร้ายเชื่อมต่อกลับเข้ามายังระบบเครือข่ายภายในได้ด้วย ปัญหาที่สองคือตัวอุปกรณ์นั้นมีทั้งการใช้รหัสผ่านเริ่มต้นที่ไม่ปลอดภัย และมีบัญชีผู้ดูแลระบบที่สามารถล็อกอินได้โดยไม่ต้องใส่รหัสผ่าน ทำให้ใครก็ตามที่รู้หมายเลขไอพีของอุปกรณ์ก็สามารถเชื่อมต่อเข้ามาดูข้อมูลหรือเปลี่ยนแปลงการตั้งค่าของเครื่องได้ง่าย ปัญหาสุดท้ายคือระบบอัปเดตเฟิร์มแวร์ไม่มีการตรวจสอบความถูกต้องของข้อมูล ทำให้สามารถฝังมัลแวร์เข้าในเครื่องได้

นอกจากนี้ ทาง SEC Consult ยังได้พบว่า กล้องวงจรปิดและเครื่องบันทึกวิดีโอที่ผลิตโดยบริษัท Xiongmai นั้นถูกวางจำหน่ายในชื่อบริษัทอื่นๆ อีกเป็นจำนวนมาก ตัวอย่าง เช่น Goodeye, iCSee Pro, JFeye ซึ่งทาง SEC Consult ได้จัดทำรายชื่อยี่ห้ออุปกรณ์ที่มีปัญหา รวมถึงวิธีตรวจสอบเบื้องต้นว่าอุปกรณ์ยี่ห้อใดถูกผลิตโดยบริษัท Xiongmai บ้าง ผู้ที่ใช้งานกล้องวงจรปิดและเครื่องบันทึกวิดีโอที่ถูกผลิตจากประเทศจีนควรตรวจสอบรายชื่ออุปกรณ์จากเว็บไซต์ของ SEC Consult

ทั้งนี้ ทาง SEC Consult แจ้งว่า ได้พยายามติดต่อกับผู้ผลิตเพื่อรายงานปัญหาให้ทราบแล้ว แต่ไม่ได้รับการตอบรับ ปัจจุบันยังไม่มีวิธีแก้ไขปัญหา ผู้ที่ใช้งานอุปกรณ์ที่มีปัญหาด้านความมั่นคงปลอดภัยควรประเมินความเสี่ยงหากยังต้องการใช้งานต่อ ตัวอย่างความเสี่ยงเช่น ผู้ประสงค์ร้ายสามารถดูภาพจากกล้องได้ ส่งผลให้รู้ว่าไม่มีคนอยู่ในบ้าน หรืออาจถูกบันทึกภาพวิดีโอเหตุการณ์ในบ้านไปเผยแพร่หรือข่มขู่แบล็คเมล์ในภายหลัง

SEC Cunsult
http://thcert.co/2tfrVY
Krebs on Security
http://thcert.co/5e5oD7
11/10/2561

แจ้งเตือนช่องโหว่ระดับร้ายแรงในเราเตอร์ MikroTik ถูกแฮกควบคุมเครื่องได้ รีบแพตช์ด่วน

ทีมนักวิจัยจากบริษัท Tenable ได้แจ้งเตือนช่องโหว่ของระบบปฏิบัติการ RouterOS ที่ถูกใช้งานในเราเตอร์ MikroTik ซึ่งเป็นหนึ่งในยี่ห้อเราเตอร์ที่นิยมใช้กันทั่วโลกรวมถึงประเทศไทย โดยช่องโหว่ที่ถูกแจ้งเตือนนี้ไม่ใช่ช่องโหว่ใหม่ แต่เป็นช่องโหว่เดิมที่เคยถูกค้นพบและแก้ไขไปแล้ว อย่างไรก็ตาม ในตอนที่ค้นพบครั้งแรกนั้นตัวช่องโหว่นี้เปิดโอกาสให้ผู้ประสงค์ร้ายอ่านไฟล์สำคัญจากตัวเราเตอร์ได้โดยไม่จำเป็นต้องยืนยันตัวตน ทำให้ความร้ายแรงของช่องโหว่นี้ถูกจัดให้อยู่ในระดับปานกลาง แต่นักวิจัยได้คนพบวิธีใหม่ในการโจมตีช่องโหว่นี้จนได้สิทธิ์ควบคุมทุกอย่างในตัวอุปกรณ์ ส่งผลให้ปัจจุบันช่องโหว่ดังกล่าวถูกจัดให้อยู่ในระดับความรุนแรงสูง

ที่ผ่านมาได้มีรายงานการโจมตีเราเตอร์ MikroTik เป็นจำนวนมาก โดยหลังจากที่ผู้ประสงค์ร้ายสามารถควบคุมเราเตอร์ได้แล้วได้มีการติดตั้งมัลแวร์เพื่อใช้โจมตีระบบหรือแก้ไขข้อมูลการตั้งค่า DNS เพื่อเปลี่ยนเส้นทางส่งผู้ใช้เข้าไปยังเว็บไซต์ปลอมถึงแม้ตัวผู้ใช้จะพิมพ์ที่อยู่ของเว็บไซต์จริง

ทาง MikroTik ได้ออกอัปเดตเฟิร์มแวร์ RouterOS เวอร์ชัน 6.40.9, 6.42.7 และ 6.43 มาเพื่อแก้ไขปัญหาดังกล่าวแล้ว ผู้ที่ใช้งานอุปกรณ์เราเตอร์ MikroTik ควรรีบอัปเดตโดยเร็ว รวมถึงควรเปลี่ยนรหัสผ่านสำหรับล็อกอินเข้าใช้งานระบบตั้งค่าเราเตอร์ด้วย เนื่องจากตัวอย่างโค้ดสำหรับใช้ทดสอบการโจมตีช่องโหว่ได้ถูกเผยแพร่สู่สาธารณะแล้ว (https://mikrotik.com/download/changelogs/bugfix-release-tree)

The Hacker News
http://thcert.co/3T79rF
Tenable
http://thcert.co/In7fF1
9/10/2561

Apple ออกอัปเดต iOS 12.0.1 แก้ปัญหา ปลดล็อคหน้าจอได้โดยไม่ต้องใส่รหัส

เมื่อวันที่ 8 ตุลาคม 2561 บริษัท Apple ได้ออกอัปเดตระบบปฏิบัติการ iOS เวอร์ชัน 12.0.1 โดยได้มีการแก้ไขปัญหาสำคัญหลายอย่าง หนึ่งในนั้นคือปิดช่องโหว่ที่ทำให้ผู้ประสงค์ร้ายข้ามหน้าจอล็อคได้โดยไม่ต้องใส่รหัสผ่าน ส่งผลให้สามารถเข้าถึงรูปภาพ รายชื่อผู้ติดต่อ อ่านอีเมล หรือข้อมูลอื่นๆ ในเครื่องได้

ผู้ที่ใช้งานระบบปฏิบัติการ iOS สามารถกดอัปเดตเป็นเวอร์ชันใหม่ได้ผ่านตัวเครื่องโดยตรง หรือเชื่อมต่อกับคอมพิวเตอร์เพื่ออัปเดตผ่านโปรแกรม iTunes

US-CERT
http://thcert.co/5cf260t
Bleeping Computer
http://thcert.co/k3lLzR
9/10/2561

Google เตรียมปรับปรุงความปลอดภัย Chrome extension แก้ปัญหาถูกแฮกเบราว์เซอร์

ที่ผ่านมา ปัญหาการแฮกเบราว์เซอร์ด้วยการหลอกให้ติดตั้งส่วนเสริม (extension หรือ add-on) นั้นมีมาอยู่เรื่อยๆ เนื่องจากส่วนเสริมที่ติดตั้งลงในเบราว์เซอร์นั้นได้รับสิทธิ์ในการอ่านและแก้ไขเปลี่ยนแปลงข้อมูลทุกอย่างในหน้าเว็บไซต์ ทำให้ผู้ประสงค์ร้ายใช้ช่องทางนี้ในการควบคุมเบราว์เซอร์ของเหยื่อเพื่อจุดประสงค์สร้างความเสียหาย ตัวอย่าง เช่น เปลี่ยนเส้นทางของเว็บไซต์ให้เข้าไปยังเว็บไซต์ปลอมถึงแม้ผู้ใช้จะพิมพ์ที่อยู่ของเว็บไซต์จริง หรือสวมรอยสิทธิ์ในการเข้าใช้งานเว็บไซต์เพื่อแพร่กระจายมัลแวร์ เป็นต้น

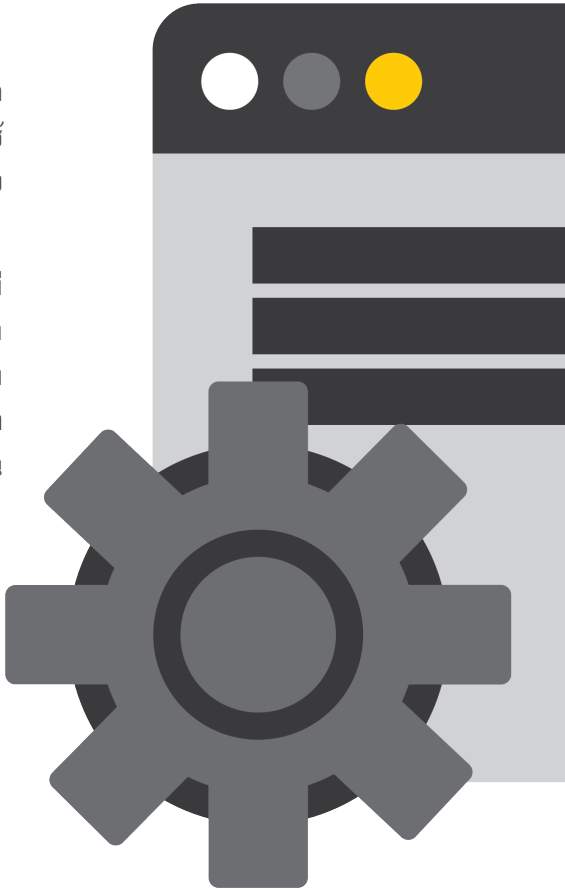
การแฮกเบราว์เซอร์ด้วยการติดตั้งส่วนเสริมที่เป็นอันตรายนั้นสามารถทำได้หลายวิธี ตั้งแต่การหลอกให้ผู้ใช้ติดตั้งส่วนเสริมนั้นลงในเครื่องโดยตรง แอบติดตั้งมาพร้อมกับโปรแกรมอื่น หรือส่งส่วนเสริมที่เป็นอันตรายนั้นขึ้นไปยัง store โดยตรง ซึ่งในกรณีหลังสุดนี้ ที่ผ่านมาก็เคยมีทั้งแบบที่ผู้ประสงค์ร้ายเผยแพร่ส่วนเสริมที่เป็นอันตรายขึ้นไปบน store ด้วยตนเอง หรือบัญชีของผู้พัฒนาส่วนเสริมถูกขโมยสิทธิ์ในการอัปโหลดข้อมูลขึ้น store ทำให้ผู้ประสงค์ร้ายสามารถแก้ไขโค้ดของไฟล์ให้ทำอันตรายกับเครื่องของเหยื่อได้ จากปัญหาเหล่านี้ ทางผู้พัฒนาเบราว์เซอร์ก็ได้มีการพยายามแก้ไขปัญหากันอยู่เป็นระยะๆ ตั้งแต่การปิดไม่ให้ติดตั้งส่วนเสริมจากภายนอก ไปจนถึงเพิ่มมาตรการตรวจสอบส่วนเสริมของเบราว์เซอร์ก่อนเผยแพร่บน store อย่างไรก็ตาม ผู้ประสงค์ร้ายก็ยังคงสามารถหาวิธีหลบเลี่ยงมาตรการป้องกันได้อยู่เรื่อยๆ

เมื่อวันที่ 1 ตุลาคม 2561 ทาง Google ได้ประกาศปรับปรุงนโยบายการพัฒนาส่วนเสริมของเบราว์เซอร์ Chrome เพื่อให้มีความมั่นคงปลอดภัยมากขึ้น โดยสิ่งที่จะเปลี่ยนในฝั่งของผู้ใช้คือส่วนขยายจำเป็นต้องขอสิทธิ์ในการแก้ไขเปลี่ยนแปลงข้อมูลบนหน้าเว็บไซต์และได้รับอนุญาตจากผู้ใช้ก่อนเท่านั้นถึงจะสามารถดำเนินการได้ ซึ่งสิทธิ์นี้สามารถระบุแบบเฉพาะบางเว็บไซต์ได้ ส่วนการเปลี่ยนแปลงในฝั่งของนักพัฒนาคือทาง Google

https://www.thaicert.or.th/alerts/user/2016/al2016us001.html)

Google ยังได้บังคับว่าบัญชีที่นักพัฒนาใช้ในการส่งโค้ดขึ้น store นั้นจะต้องเปิดใช้งานการยืนยันตัวตนแบบ 2 ขั้นตอนด้วย เพื่อเพิ่มความปลอดภัยให้กับบัญชีดังกล่าว

การประกาศนโยบายใหม่นี้อาจไม่มีผลกระทบกับผู้ใช้ทั่วไปมากนักในแง่ของการใช้งาน แต่สำหรับนักพัฒนาส่วนเสริมของเบราว์เซอร์ Chrome อาจจำเป็นต้องศึกษาการเปลี่ยนแปลงในจุดนี้เพื่อป้องกันไม่ให้เกิดปัญหาในอนาคต



Google
http://thcert.co/Qp0dz5
ZDNet
http://thcert.co/CMqqKg
4/10/2561

อัปเดตปิดช่องโหว่ใน Apache Tomcat ผู้ประสงค์ร้ายสามารถขโมยข้อมูลสำคัญได้

เมื่อวันที่ 3 ตุลาคม 2561 Apache Software Foundation ได้เผยแพร่แพตช์อัปเดตปิดช่องโหว่ใน Apache Tomcat เพื่อปิดช่องโหว่รหัส CVE-2018-11784 อาศัยช่องโหว่ดังกล่าวผู้ประสงค์ร้ายสามารถสร้าง URL พิเศษเพื่อเข้าถึงข้อมูลสำคัญได้

เวอร์ชันที่ได้รับผลกระทบคือ 9.0.0.M1-9.0.0.11, 8.5.0-8.5.33 และ 7.0.23-7.0.90 ผู้ที่ใช้งานซอฟต์แวร์ดังกล่าวสามารถอัปเดตเป็นเวอร์ชันล่าสุดคือ 9.0.0.12, 8.5.34 และ 7.0.91 เพื่อแก้ไขช่องโหว่

US-CERT
http://thcert.co/vN39PE
Apache
http://thcert.co/Citbcd
5/10/2561

Western Digital ออกแพตช์แก้ไขช่องโหว่ร้ายแรงในอุปกรณ์ My Cloud ที่เปิดให้ผู้ไม่ได้รับอนุญาตสามารถล็อกอินเป็นผู้ดูแลระบบได้

เมื่อวันที่ 18 กันยายน 2561 นักวิจัยด้านความมั่นคงปลอดภัยจากบริษัท Securify ได้รายงานช่องโหว่ร้ายแรงใน Western Digital My Cloud ซึ่งเป็นอุปกรณ์ NAS สำหรับใช้บริหารจัดการไฟล์ผ่านระบบเครือข่าย ช่องโหว่นี้เปิดโอกาสให้ผู้ไม่ได้รับอนุญาตสามารถเชื่อมต่อเข้ามาเป็นผู้ดูแลระบบของตัวอุปกรณ์ได้โดยไม่จำเป็นต้องใส่รหัสผ่าน ซึ่งทำให้ผู้ประสงค์ร้ายสามารถเข้าถึงไฟล์ที่อยู่ข้างในรวมถึงควบคุมและเปลี่ยนแปลงการทำงานของตัวอุปกรณ์ได้ ช่องโหว่นี้มีรหัส CVE-2018-17153

ภายหลังจากที่นักวิจัยได้รายงานช่องโหว่พร้อมตัวอย่างโค้ดสำหรับใช้โจมตี ทาง Western Digital ได้ออกอัปเดตให้กับอุปกรณ์ My Cloud เพื่อแก้ไขปัญหา โดยเป็นเวอร์ชัน 2.30.196 อัปเดตนี้สามารถติดตั้งได้ผ่านระบบ OTA ของตัวอุปกรณ์ หรือสามารถดาวน์โหลดเฟิร์มแวร์มาติดตั้งด้วยตนเองได้จากเว็บไซต์ของ Western Digital ผู้ใช้งานอุปกรณ์ Western Digital My Cloud ควรตรวจสอบรุ่นที่ได้รับผลกระทบและวิธีการอัปเดตจากเว็บไซต์ของผู้ผลิต

https://nvd.nist.gov/vuln/detail/CVE-2018-17153
https://support.wdc.com/knowledgebase/answer.aspx?ID=25952

Securify
http://thcert.co/mMi1Sj
ZDNet
http://thcert.co/w5zSbo
1/10/2561

แจ้งเตือนช่องโหว่ร้ายแรงใน Apache Struts 2 อาจถูกยึดเครื่องได้ มีโค้ดสาธิตการโจมตีแล้ว

เมื่อวันที่ 22 สิงหาคม 2561 US-CERT ได้แจ้งเตือนช่องโหว่ใน Apache Struts 2 (https://struts.apache.org) ซึ่งเป็นช่องโหว่ประเภท Remote Code Execution ส่งผลให้ผู้ประสงค์ร้ายสามารถเข้าควบคุมเครื่องจากระยะไกล ช่องโหว่นี้มีผลกระทบกับ Apache Struts 2 ตั้งแต่เวอร์ชัน 2.3 - 2.3.34 หรือ 2.5 - 2.5.16 และได้มีการเผยแพร่โค้ดสาธิตการโจมตีแล้ว ผู้ดูแลเว็บไซต์ที่มีการใช้งาน Apache Struts 2 ควรตรวจสอบและอัปเดตแก้ไขช่องโหว่ทันที โดยสามารถศึกษาข้อมูลเพิ่มเติมได้จากเว็บไซต์ของ Apache

https://cwiki.apache.org/confluence/display/WW/S2-057

US-CERT
http://thcert.co/vN39PE
Apache
http://thcert.co/Citbcd
5/10/2561

Microsoft ปล่อยอัปเดตประจำเดือน มิถุนายน ปิดช่องโหว่ของ Windows

Microsoft เผยแพร่อัปเดตด้านความมั่นคงปลอดภัยประจำเดือนมิถุนายน 2561 สำหรับระบบปฏิบัติการ Windows เพื่อปิดช่องโหว่ 50 รายการ โดยแบ่งระดับรุนแรง 11 รายการและระดับสำคัญ 39 รายการ โดยมีช่องโหว่ 3 รายการที่ค่อนข้างส่งผลกระทบ ได้แก่

1. ช่องโหว่ใน Microsoft Internet Explorer (หมายเลขช่องโหว่ CVE-2018-8267) เป็นช่องโหว่ประเภท Remote Code Execution ส่งผลให้ผู้ประสงค์ร้ายสั่งประมวลผลคำสั่งอันตรายจากระยะไกลเพื่อควบคุมเครื่องของเหยื่อ ช่องโหว่ดังกล่าวเกิดจากความผิดพลาดในการจัดการ error ในซอฟต์แวร์

2. ช่องโหว่ใน Windows Domain Name Server API หรือ DNSAPI (หมายเลขโหว่ช่องโหว่ CVE-2018-8225) ใน DNS ซึ่งเป็นบริการสำคัญใน Windows เป็นหนึ่งในส่วนประกอบที่จำเป็นที่ถูกเรียกใช้ เมื่อผู้ใช้ต้องการเข้าถึงเว็บไซต์ต่าง ๆ

3. ช่องโหว่นี้เป็นช่องโหว่ประเภท Remote Code Execution เช่นกัน ผู้ประสงค์ร้ายสามารถโจมตีโดยส่ง DNS reponse ที่มีโค้ดอันตรายไปยังเครื่องเหยื่อที่มีช่องโหว่ เพื่อควบคุมเครื่องของเหยื่อ

4. ช่องโหว่ใน HTTP Protocol Stack (Http.sys) (หมายเลขช่องโหว่ CVE-2018-8231) เป็นช่องโหว่ประเภท Remote Code Execution เช่นกัน เกิดจากข้อผิดพลาดการจัดการข้อมูล object ในเมมโมรี

นอกจากนี้ยังมีช่องโหว่อื่นในซอฟต์แวร์ต่าง ๆ เช่น Microsoft Office, Adobe Flash Player รวมถึงส่วนประกอบอื่น ๆ ใน Windows ซึ่งผู้ใช้ควรติดตั้งอัปเดตล่าสุดเพื่อปิดช่องโหว่

Microsoft
http://thcert.co/wddb6w
15/6/2561

Red Hat แจ้งเตือนพบช่องโหว่ในระบบปฏิบัติการ ส่วนจัดการ DHCP ส่งผลให้เครื่องถูกควบคุมได้

เมื่อวันที่ 15 พฤษภาคม 2561 บริษัทผู้พัฒนา Redhat ประกาศแจ้งเตือนช่องโหว่หมายเลข CVE-2018-1111 ในระบบปฏิบัติการ Red Hat Enterprise Linux 6 และ 7 ซึ่งส่งผลให้ผู้ประสงค์ร้ายสามารถส่งคำสั่งอันตรายจากระยะไกลไปยังเครื่องเหยื่อให้ทำการประมวลผลเพื่อทำการควบคุมเครื่อง (Remote Code Execution)

ช่องโหว่ดังกล่าวอยู่ในสคริปต์ที่ใช้จัดการ DHCP ซึ่งเป็นโปรโตคอลที่ใช้ในการแจกค่า Network Setting เช่น หมายเลขไอพี ให้กับเครื่องที่มาเชื่อมต่อเครือข่าย เพื่อให้สามารถติดต่อสื่อสารกับเครื่องอื่น ๆ ได้ ขั้นตอนการทำงานของ DHCP โดยเบื้องต้น เริ่มจากเครื่องที่มาเชื่อมต่อเครือข่ายส่งคำร้องขอ (DHCP Request) จากนั้น DHCP เซิร์ฟเวอร์จึงส่งข้อมูลกลับไป (DHCP Response) ซึ่งเป็นค่า Network Setting ดังที่ระบุไปในข้างต้น

สคริปต์ที่มีช่องโหว่ อยู่ในเครื่องที่มาเชื่อมต่อเครือข่าย มีหน้าที่จัดการ DHCP response ซึ่งนักวิจัยพบว่าสคริปต์ดังกล่าวไม่สามารถกลั่นกรองข้อมูลได้ดีพอ ทำให้สคริปต์นำคำสั่งอันตรายที่ผู้ประสงค์ร้ายส่งแฝงมาใน DHCP response มาประมวลผล เนื่องจากสคริปต์นี้ใช้สิทธิ root ในการทำงาน ส่งผลให้ผู้ประสงค์ร้ายได้สิทธิสูงสุดและสามารถควบคุมเครื่อง

ทางผู้พัฒนา Red Hat ได้ออกแพตช์เพื่อปิดช่องโหว่แล้ว นอกจากนี้ระบบปฏิบัติการรุ่นอื่น เช่น Fedora, CentOS ก็พบช่องโหว่นี้เช่นกัน ผู้ใช้งานควรตรวจสอบจากเว็บไซต์ทางการว่ารุ่นที่ใช้งานได้รับผลกระทบหรือไม่ และควรอัปเดตเพื่อปิดช่องโหว่ ดูสามารถศึกษาวิธีการได้จากเว็บไซต์ทางการของผู้พัฒนา

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/chap-keeping_your_system_up-to-date

Redhat
http://thcert.co/shqNrY
17/5/2561

แจ้งเตือนผู้ใช้ Drupal พบช่องโหว่ใหม่ ถูกใช้โจมตี 5 ชม. หลังแพตช์ถูกปล่อย

เมื่อวันที่ 25 เมษายน เว็บไซต์ทางการ Drupal ประกาศแพตช์ปิดช่องโหว่หมายเลข CVE-2018-7602 เป็นช่องโหว่ลักษณะ Remote Code Execution ซึ่งเปิดโอกาสให้ผู้ประสงค์ร้ายเข้ามาควบคุมระบบ โดยสั่งประมวลผลคำสั่งอันตรายจากระยะไกล ช่องโหว่ดังกล่าวถูกนำมาใช้เป็นช่องทางในการโจมตีหลังจากแพตช์ถูกประกาศ 5 ชั่วโมง

ผู้ดูแลเว็บไซต์ที่ใช้ Drupal ควรอัปเดตเป็นเวอร์ชันล่าสุด (Drupal 7.59, 8.5.3, 8.4.8) ผู้ที่ยังใช้เวอร์ชัน 8.4.x ควรพิจารณาอัปเกรดเป็นเวอร์ชันที่ใหม่กว่า เนื่องจากผู้พัฒนา Drupal ยุติการสนับสนุนเวอร์ชันดังกล่าวแล้ว

จะเห็นได้ว่าผู้ประสงค์ร้ายมองหาโอกาสในการโจมตีอยู่ตลอดเวลา เมื่อมีการประกาศแพตช์อัปเดตช่องโหว่ ก็พยายามศึกษาค้นคว้ารายละเอียดช่องโหว่เพิ่มเติม และพัฒนาโค้ดสำหรับโจมตี ซึ่งในกรณีนี้พบการโจมตีหลังจากแพตช์ของช่องโหว่ถูกแผยแพร่เพียง 5 ชั่วโมง ผู้ดูและระบบจึงควรติดตามการเผยแพร่ข้อมูลแพตช์จากเว็บไซต์ทางการ และติดตามข่าวสารเพื่อรับทราบสถานการณ์ว่ามีการโจมตีผ่านช่องโหว่ในผลิตภัณฑ์ที่ใช้หรือไม่ รวมถึงพิจารณาอัปเดตแพตช์โดยเร็วที่สุด

Drupal
http://thcert.co/TFqVTm
BleepingComputer
http://thcert.co/YiX61J
26/4/2561

Adobe ปล่อยอัปเดตปิดช่องโหว่ 0-day ใน Adobe Flash Player พบถูกใช้โจมตีเพื่อควบคุมเครื่องเหยื่อ

เมื่อต้นเดือนกุมภาพันธ์ หน่วยงานรับมือภัยคุกคามไซเบอร์ของประเทศเกาหลีใต้ KrCERT (Korea Computer Emergency Response Team) ได้ประกาศแจ้งเตือนการค้นพบ Adobe Flash Player (หมายเลขช่องโหว่ CVE-2018-4878) ส่งผลให้ผู้ประสงค์ร้ายสามารถโจมตีเพื่อควบคุมเครื่องของเหยื่อได้ โดยช่องโหว่ดังกล่าวเป็นลักษณะประเภท 0-day นอกจากนี้พบว่าช่องโหว่ถูกใช้เพื่อโจมตีแล้วโดยมุ่งเป้าจำกัดเฉพาะกลุ่มเป้าหมาย

การโจมตีที่พบมาในรูปแบบไฟล์เอกสารแนบมากับอีเมล เช่น ไฟล์ประเภท Excel โดยในไฟล์เอกสารมีการฝังส่วนประกอบที่เรียกว่า ActiveX object ที่มีโค้ดอันตรายสำหรับโจมตีช่องโหว่ใน Adobe Flash Player แฝงอยู่ หากเหยื่อเปิดไฟล์เอกสารและกดอนุญาตเพื่อแสดงเนื้อหา ActiveX ก็อาจถูกโจมตีส่งผลให้เครื่องถูกควบคุมได้

ช่องโหว่นี้ส่งผลกระทบใน Adobe Flash Player ตั้งแต่รุ่น 28.0.0.137 และรุ่นก่อนหน้า ถึงแม้ยังพบการโจมตีจำกัดเฉพาะกลุ่ม แต่ผู้ประสงค์ร้ายรายอื่นก็อาจสามารถนำช่องโหว่ไปใช้โจมตีอย่างแพร่หลาย ทาง Adobe ได้เผยแพร่อัปเดตเป็นเวอร์ชัน 28.0.0.161 เพื่อปิดช่องโหว่ สำหรับแนวทางการป้องกันเพิ่มเติม หากไม่มีความจำเป็นต้องใช้ซอฟต์แวร์นี้ ผู้ใช้อาจพิจารณาถอนการติดตั้งซอฟต์แวร์ดังกล่าวเพื่อลดความเสี่ยงจากการถูกโจมตีในอนาคต

จะเห็นได้ว่าการส่งอีเมลแนบไฟล์อันตรายเป็นช่องทางหนึ่งที่ผู้ประสงค์ร้ายมักใช้เพื่อโจมตี ซึ่งจริงๆ แล้วการโจมตีมีหลายรูปแบบ ผู้ใช้สามารถศึกษาวิธีการรับมือเพิ่มเติมได้ที่

https://www.facebook.com/thaicert/videos/660657847415685/

Malwarebytes
http://thcert.co/cyf7WP
Fireeye
http://thcert.co/NpXxTW
Adobe
http://thcert.co/OGJDaK
9/2/2561

นักวิจัยพบช่องโหว่ในระบบปฏิบัติการ macOS ทำให้ได้สิทธิ root ยังไม่มีอัปเดตแก้ไข

เมื่อวันที่ 31 ธันวาคม 2560 นักวิจัยด้านความมั่นคงปลอดภัย ได้ประกาศการพบช่องโหว่ในระบบปฏิบัติการ macOS ประเภท Privilege Escalation ส่งผลให้ผู้ประสงค์ร้ายยกระดับสิทธิเป็น root ทำให้เพิ่มความสามารถในการโจมตี อย่างไรก็ตามช่องโหว่นี้ไม่สามารถใช้โจมตีจากระยะไกลได้ ผู้ประสงค์ร้ายจำเป็นต้องได้สิทธิเข้าถึงเครื่องก่อน

ช่องโหว่ดังกล่าวถูกพบใน IOHIDFamily macOS kernel driver ซึ่งเป็นส่วนเสริมของ macOS ที่ช่วยในการติดต่อสื่อสารระหว่างระบบปฏิบัติการและอุปกรณ์ที่เชื่อมต่อ เช่น ทัชสกรีน หรือคีย์บอร์ด เพื่อให้ระบบปฏิบัติการสามารถใช้งานอุปกรณ์เหล่านี้ได้

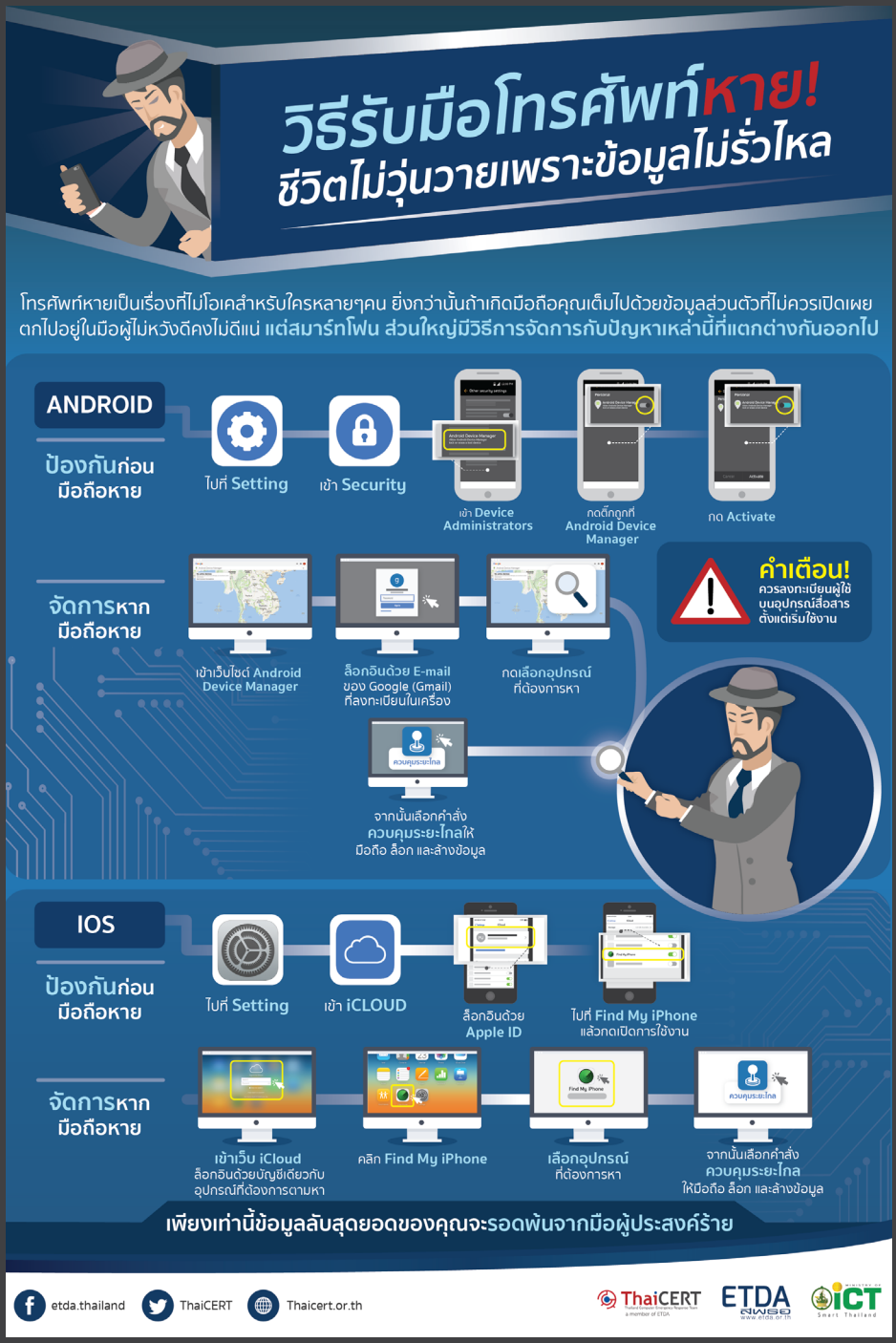
นักวิจัยระบุว่าช่องโหว่ดังกล่าวมีอยู่ในระบบปฏิบัติการหลายปีก่อนหน้า และได้เผยแพร่โค้ดตัวอย่างสาธิตการโจมตีโดยใช้ช่องโหว่ดังกล่าวสู่สาธารณะ นอกจากนี้ยังไม่มีอัปเดตปิดช่องโหว่ ผู้เชี่ยวชาญคาดว่าช่องโหว่จะได้รับการแก้ไขในเดือนนี้พร้อมกับช่องโหว่อื่นๆ ผู้ใช้สามารถติดตามข่าวจากเว็บไซต์ทางการของ Apple สำหรับอัปเดตเพื่อแก้ไขช่องโหว่

https://support.apple.com/en-ca/HT201222

Threatpost
http://thcert.co/7xU9o1
The Hacker News
http://thcert.co/h8LFVY
Bleeping Computer
http://thcert.co/Sb61FB
3/1/2561


01
02
03
04

อินโฟกราฟิก


วิธีรับมือโทรศัพท์หาย!
ชีวิตไม่วุ่นวายเพราะข้อมูลไม่รั่วไหล
โทรศัพท์หายเป็นเรื่องที่ไม่โอเคสำหรับใครหลายๆคน ยิ่งกว่านั้นถ้าเกิดมือถือคุณเต็มไปด้วยข้อมูลส่วนตัวที่ไม่ควรเปิดเผย
ตกไปอยู่ในมือผู้ไม่หวังดีคงไม่ดีแน่ แต่สมาร์ทโฟน ส่วนใหญ่มีวิธีการจัดการกับปัญหาเหล่านี้ที่แตกต่างกันออกไป
ANDROID
ป้องกันก่อน มือถือหาย
ไปที่ Setting
เข้า Security
เข้า Device Administrators
กดติ๊กถูกที่ Android Device Manager
กด Activate
จัดการหาก มือถือหาย
เข้าเว็บไซต์ Android Device Manager
ล็อกอินด้วย E-mail ของ Google (Gmail) ที่ลงทะเบียนในเครื่อง
กดเลือกอุปกรณ์ ที่ต้องการหา
ควบคุมระยะไกล
จากนั้นเลือกคำสั่ง ควบคุมระยะไกลให้ มือถือ ล็อก และล้างข้อมูล
คำเตือน!
ควรลงทะเบียนผู้ใช้ บนอุปกรณ์สื่อสาร ตั้งแต่เริ่มใช้งาน
IOS
ป้องกันก่อน มือถือหาย
ไปที่ Setting
เข้า iCLOUD
ล็อกอินด้วย Apple ID
ไปที่ Find My iPhone แล้วกดเปิดการใช้งาน
จัดการหาก มือถือหาย
เข้าเว็บ iCloud ล็อกอินด้วยบัญชีเดียวกับ อุปกรณ์ที่ต้องการตามหา
คลิก Find My iPhone
เลือกอุปกรณ์ ที่ต้องการหา
ควบคุมระยะไกล
จากนั้นเลือกคำสั่ง ควบคุมระยะไกล ให้มือถือ ล็อก และล้างข้อมูล
เพียงเท่านี้ข้อมูลลับสุดยอดของคุณจะรอดพ้นจากมือผู้ประสงค์ร้าย
etda.thailand
ThaiCERT
Thaicert.or.th
ThaiCERT
ETDA
ICT

เวอร์ชั่น 01
22 ม.ค.2561

แบ็กอัปข้อมูลไว้ก่อน
เพราะถ้าหายไป เสียเงินเท่าไร... ก็อาจไม่ได้คืนมา

รู้มั้ย? **34%**(1) ของคนทั่วโลกเคย**สูญเสียข้อมูล**

ในปี 2560
กว่าล้านคนถูกโจมตี ด้วยมัลแวร์เรียกค่าไถ่ (2)

ซึ่งจะล็อกข้อมูลในเครื่อง เช่น เอกสาร รูปภาพ ทำให้เปิดใช้งานไม่ได้เพื่อเรียกค่าไถ่
และแม้จ่ายค่าไถ่ไปแล้ว**ก็ไม่ได้รับประกัน**ว่าจะได้ข้อมูลนั้นคืนมา

แบ็กอัปแบบไหน...ถามใจเธอดู?

วิธีเก็บ	ข้อดี	ข้อเสีย
บริการ Cloud เช่น Google Drive, Dropbox, OneDrive	ใช้ง่าย ฟรี เข้าที่ไหนก็ได้ แบ็กอัปอัตโนมัติได้	ต้องมีอินเทอร์เน็ต มีความเสี่ยงปิดบริการ
อุปกรณ์เก็บข้อมูลแบบพกพา เช่น DVD, ฮาร์ดดิสก์, Flash Drive	ใช้ง่าย เก็บรักษาในที่ปลอดภัย พกติดตัวได้	มีโอกาสสูญหายหรือเสียหาย
พิมพ์เป็นกระดาษ	ไม่ขึ้นต่อฮาร์ดแวร์ ป้องกันการถูกเจาะข้อมูล	จัดการยาก ไม่ดีต่อสิ่งแวดล้อม
NAS (Network Attach Storage)	เก็บข้อมูลจากคอมพิวเตอร์หลายเครื่อง พร้อมกันได้ แบ็กอัปอัตโนมัติได้	ต้องติดตั้งและดูแลระบบ ราคาสูง มีโอกาสเสียหาย

(1) : https://www.acronis.com/en-us/blog/posts/acronis-world-backup-day-survey-results
(2) : https://kasperskycontenthub.com/securelist/files/2017/12/KSB_statistics_2017_EN_final.pdf

NAS (Network Attach Storage)
*คือ อุปกรณ์ที่ให้บริการเก็บและแชร์ข้อมูลแก่เครื่องของผู้ใช้งานในเครือข่ายเดียวกัน

ข้อมูลเพิ่มเติม ศึกษาได้ที่
www.thaicert.or.th / www.etda.or.th

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (ThaiCERT)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ThaiCERT
ETDA สพธอ www.etda.or.th
ThaiCERT ThaiCERT thaicert.or.th

PASSWORD
พาสเวิร์ด
รหัสผ่าน

ตั้งให้ยาก
จำให้ได้
ไม่แชร์กับใคร
อย่าใช้ซ้ำทุกบัญชี

อย่างน้อย
ควรมี **8 ตัวอักษร**

เดายาก
ไม่เป็นคำจากพจนานุกรม

ไม่เป็นตัวเลข
หรือตัวอักษร**เรียงกัน**
หรือซ้ำกัน เช่น abcd1111

ไม่ใช้พาสเวิร์ดหรือ
default password
ที่ตั้งค่ามาตั้งแต่แรก

ไม่ใช้ข้อมูลส่วนตัว
เช่น วันเดือนปีเกิด
เบอร์โทร.

ไม่ใช้ซ้ำกัน
ในบัญชีต่าง ๆ

ใช้การ**ยืนยัน 2 ขั้นตอน**
หรือหลายขั้นตอน

ระวังอีเมลฟิชชิง
หลอกให้เปลี่ยนพาสเวิร์ด
โดยให้คลิกลิงก์

พิจารณา**ใช้งาน**
ซอฟต์แวร์ช่วยจัดการ
พาสเวิร์ด

ThaiCERT a member of ETDA
ETDA
www.etda.or.th


01
02
03
04

บทความแจ้งเตือนที่สำคัญและข้อแนะนำสำหรับผู้ใช้ทั่วไป

ระวังภัย ช่องโหว่ Meltdown, Spectre อาจถูกขโมยข้อมูลในเครื่องได้ผ่านซีพียู กระทบระบบปฏิบัติการ Windows, Linux, Mac

วันที่ประกาศ: 5 มกราคม 2561

ปรับปรุงล่าสุด: 5 มกราคม 2561

ประเภทภัยคุกคาม: Information disclosure

ข้อมูลทั่วไป

เมื่อวันที่ 3 มกราคม 2561 National Cybersecurity and Communications Integration Center (NCCIC) ซึ่งเป็นศูนย์กลางการแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์ระหว่างภาครัฐกับภาคเอกชนของประเทศสหรัฐฯ ได้แจ้งเตือนช่องโหว่ 2 รายการที่ได้รับการเปิดเผยโดยทีมวิจัย Google Project Zero เรียกว่า Meltdown และ Spectre ซึ่งส่งผลกระทบกับการทำงานของ CPU ในระดับฮาร์ดแวร์ ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ อุปกรณ์มือถือ และเครื่องแม่ข่ายที่ให้บริการต่าง ๆ และระบบที่ให้บริการคลาวด์

ช่องโหว่ Spectre และ Meltdown สามารถดึงเอาข้อมูลที่สำคัญจากหน่วยความจำจากระดับโครงสร้างภายในการออกแบบของ CPU ผ่านการทำงาน Kernel ของระบบปฏิบัติการ ซึ่งโดยปกติระบบปฏิบัติการจะไม่อนุญาตให้โปรแกรมแอปพลิเคชันเข้าถึงข้อมูลในระดับโครงสร้างของ CPU ได้ ในกรณีนี้มีการทำการทดลองโดยอาศัยช่องว่างระหว่างการรอทำคำสั่งของ CPU เพื่อการเข้าถึง และสามารถทำสำเนาข้อมูลบางส่วนได้

กรณีที่มีผู้ประสงค์ร้ายนำเอาเทคนิคดังกล่าวไปใช้ ก็อาจสั่งงานให้มีการค้นข้อมูล และทำสำเนาข้อมูลสำคัญ เช่น รหัสผ่าน ออกไปจากระบบได้ ทั้งนี้ผู้ผลิต CPU รุ่นIntel AMD และ ARM (ชิปในอุปกรณ์มือถือ และ Tablet ส่วนใหญ่) ได้ร่วมมือกับผู้ผลิตระบบปฏิบัติการในการออกแพตช์เพื่อปิดช่องโหว่ดังกล่าว การอัปเดตแพตช์อาจทำให้ระบบทำงานช้าลงตั้งแต่ 5 - 30 % บริษัท Microsoft บริษัท Apple บริษัท Google (Android) และ Linux ได้ออกซอฟต์แวร์เพื่อแก้ไขปัญหาดังกล่าวแล้ว

Details	Meltdown	Spectre
Allows kernel memory read	Yes	No
Was patched with KAISER/KPTI	Yes	No
Leaks arbitary user memory	Yes	Yes
Could be executed remotely	Sometimes	Definitely
Most likely to impact	Kernel integrity	Browser memory
Practical attacks against	Intel	Intel, AMD, ARM
CVE	rogue data cache load (CVE-2017-5754)	branch target injection (CVE-2017-5715) bounds check bypass (CVE-2017-5)

ตารางเปรียบเทียบแสดงรายละเอียดช่องโหว่ Meltdown และ Spectre

ผลกระทบ

ผู้ประสงค์ร้ายสามารถเจาะผ่านระบบป้องกันความปลอดภัย และเข้าถึงข้อมูลสำคัญของเครื่องผู้ใช้ได้

โดยช่องโหว่ Spectre เปิดโอกาสผู้ประสงค์ร้ายสามารถเข้าถึงหน่วยความจำที่กำลังทำงานอยู่ ส่วนช่องโหว่ Meltdown เปิดโอกาสให้สามารถเข้าถึงหน่วยความจำได้ในระดับ Kernel ซึ่งหมายถึงข้อมูลบัญชีผู้ใช้ และรหัสผ่านที่ใช้ภายในระบบปฏิบัติการอาจถูกขโมยได้

ทั้งนี้นักวิจัยยังกล่าวว่าช่องโหว่ดังกล่าวอาจไม่ได้มีผลกระทบที่ทำให้สามารถเปลี่ยนแปลงหรือลบข้อมูลได้

และในการโจมตีผู้ประสงค์ร้ายต้องมีสิทธิเข้าถึงอุปกรณ์ที่ใช้งานซีพียูที่ได้รับผลกระทบก่อนจึงจะสามารถใช้ช่องโหว่โจมตีได้ เช่น หลอกเหยื่อติดตั้งมัลแวร์เพื่อควบคุมเครื่อง หรือหลอกให้เหยื่อเข้าถึงเว็บไซต์ที่มีโค้ดอันตราย เป็นต้น

ระบบที่ได้รับผลกระทบ

ช่องโหว่ Meltdown ส่งผลกระทบกับระบบปฏิบัติการที่ใช้งานซีพียู Intel และช่องโหว่ Spectre ส่งผลกระทบต่อระบบปฏิบัติการที่ใช้งานซีพียู Intel, AMD และ ARM

ข้อแนะนำในการป้องกันและแก้ไข

ทางผู้พัฒนาระบบปฏิบัติการและอุปกรณ์ที่ใช้งานซีพียูที่มีช่องโหว่ ได้เริ่มสร้างแพตช์เพื่อลดผลกระทบจากช่องโหว่ดังกล่าว โดยติดตามรายละเอียดของการพัฒนาแพตช์ของแต่ละผลิตภัณฑ์ตามตารางด้านล่าง อย่างไรก็ตามการติดตั้งแพตช์ดังกล่าวอาจไม่ได้แก้ไขช่องโหว่ได้ทุกกรณี เนื่องจากช่องโหว่กระทบต่อสถาปัตยกรรมของซีพียูโดยตรง และเมื่อติดตั้งแพตช์แล้วอาจส่งผลให้ประสิทธิภาพการทำงานของซีพียูลดลง ผู้ดูแลระบบควรตรวจสอบประสิทธิภาพการทำงานสำหรับแอปพลิเคชันและบริการที่สำคัญก่อนเพื่อลดผลกระทบที่อาจเกิดขึ้น

สำหรับช่องโหว่ Meltdown นั้นได้รับการแก้ไขแล้วสำหรับ บริการ Coud computing ของ Amazon, Google and Microsoft

อ้างอิง

1. https://meltdownattack.com/#meltdown-reported
2. https://meltdownattack.com/
3. https://spectreattack.com/
4. https://www.ncsc.gov.uk/guidance/meltdown-and-spectre-guidance
5. https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html
6. https://www.nytimes.com/2018/01/03/business/computer-flaws.html?hpw&rref=technology&action=click&pgtype=Homepage&module=well-region®ion=bottom-well&WT.nav=bottom-well
7. https://www.kb.cert.org/vuls/id/584653
8. https://www.sans.org/webcasts/meltdown-spectre-understanding-mitigating-threats-106815

แจ้งเตือน มัลแวร์ขุดเงินดิจิทัลระบาดผ่านลิงก์ย่อ ประเทศไทยดาวน์โหลดสูงสุด

วันที่ประกาศ: 2 กุมภาพันธ์ 2561

ปรับปรุงล่าสุด: 2 กุมภาพันธ์ 2561

ประเภทภัยคุกคาม: Malicious Code

สถานการณ์การแพร่ระบาด

เมื่อวันที่ 24 มกราคม 2561 ทีมนักวิจัยของ Palo Alto Networks เผยแพร่ข้อมูลพบว่ามีมัลแวร์ที่ใช้ขุดเงินดิจิทัล (Cryptocurrency) สกุลเงิน Monero ซึ่งเป็นเหรียญที่ใช้เทคโนโลยีของ Blockchain ในการรับส่ง และเหรียญดังกล่าวมีคุณสมบัติในการปกปิดข้อมูลที่อยู่บน Blockchain รวมถึงรองรับการขุดเครื่องคอมพิวเตอร์โดยทั่วไปที่ไม่ต้องการใช้ประมวลผลมาก เมื่อเทียบกับเหรียญอื่นๆ จึงอาจเป็นตัวเลือกที่ผู้ประสงค์ร้ายใช้เหรียญนี้

โดยในช่วงเดือนตุลาคมถึงธันวาคม 2560 พบว่ามัลแวร์ดังกล่าว มียอดดาวน์โหลดมากกว่า 15 ล้านครั้ง ที่น่ากังวลคือประเทศไทยมีการดาวน์โหลดสูงที่สุดกว่า 3.5 ล้านครั้ง

รูปที่ 1 จำนวนการดาวน์โหลดมัลแวร์ดังกล่าวทั่วโลก
(hxxps://researchcenter.paloaltonetworks.com/wp-content/uploads/2018/01/Monero_11.png)

มัลแวร์ดังกล่าวแพร่กระจายผ่านลิงก์อันตราย เมื่อคลิกติดตั้งแล้วจะส่งผลทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง เนื่องจาก CPU จะต้องสลับงานที่ทำปกติ ไปประมวลผลการถอดรหัสต้องไปประมวลผลถอดรหัสจากการขุดเหรียญ Monero ให้กับผู้ประสงค์ร้าย

การแฮกเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ (Internet of Things) เพื่อใช้ติดตั้งมัลแวร์ขุดเงินดิจิทัลนั้นเริ่มมีแนวโน้มสูงมากขึ้นในปัจจุบัน เนื่องจากความสามารถในการปกปิดข้อมูลเจ้าของบัญชีเงิน และสามารถนำเงินไปใช้ในตลาดมืดได้โดยตรวจสอบติดตามได้ยาก ผู้ใช้หรือผู้ดูแลระบบควรตรวจสอบความผิดปกติ เช่น โพรเซสที่ใช้ CPU สูง เพื่อป้องกันการถูกนำเครื่องคอมพิวเตอร์มาใช้โดยไม่ได้รับอนุญาติ

ช่องทางการแพร่กระจายของมัลแวร์

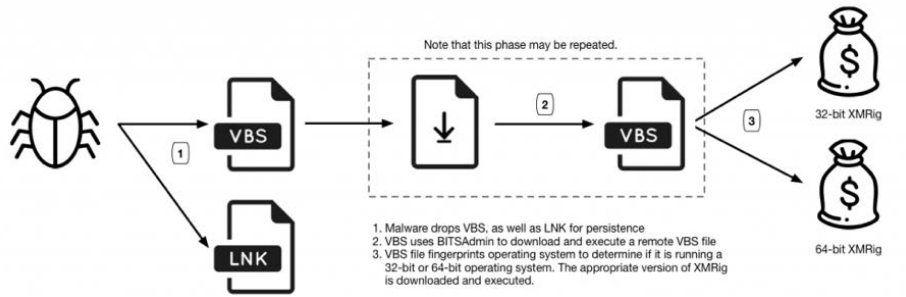
การแพร่กระจายที่พบเกิดจากผู้ประสงค์ร้ายนำมัลแวร์ไปฝากไว้บนบริการฝากไฟล์บนคลาวด์ตามที่ต่างๆ และมีการใช้งานบริการย่อลิงก์ให้สั้น เช่น bit.ly ในการสร้างลิงก์สำหรับเผยแพร่มัลแวร์ ซึ่งหากเหยื่อคลิกลิงก์จะส่งผลให้ไฟล์ที่เป็นมัลแวร์ถูกดาวน์โหลดลงในเครื่อง โดยรูปแบบการเผยแพร่ อาจเกิดจากมีการแจกไฟล์ต่างๆ ที่ดึงดูดให้ผู้ใช้งานทำการดาวน์โหลดและติดตั้ง เช่น แจกซอฟต์แวร์ฟรี ซอฟต์แวร์โกงเกมส์

การทำงานของมัลแวร์

ผู้ประสงค์ร้ายมีการทดลองเปลี่ยนแปลงรูปแบบการเผยแพร่มัลแวร์อยู่เป็นระยะ เริ่มจากผู้ใช้งานทำการคลิกลิงก์ของผู้ประสงค์ร้าย ส่งผลให้ทำการดาวน์โหลดมัลแวร์ไปยังเครื่องผู้ใช้งาน โดยขั้นตอนการดาวน์โหลดที่ทีมนักวิจัยของ Palo Alto Networks พบนั้นมีความแตกต่างกันไปตามรุ่นของมัลแวร์ ดังนี้

แบบที่ 1

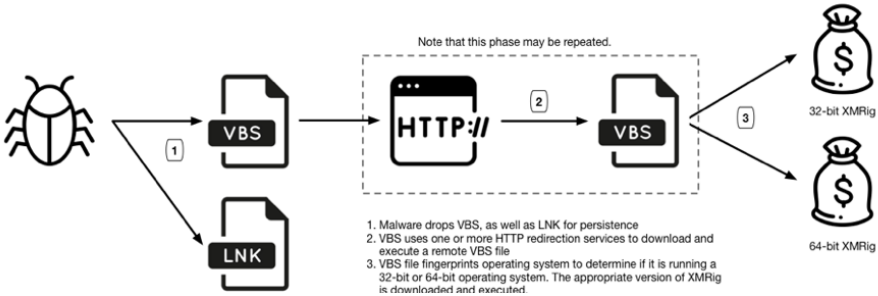
- เมื่อผู้ใช้งานคลิกลิงก์ bit.ly แล้วจะทำการดาวน์โหลดไฟล์สคริปต์ประเภท VBScript ไปยังเครื่องผู้ใช้งานทันที
- ไฟล์ดังกล่าวจะสั่งเครื่องมือ BITSAdmin บนระบบปฏิบัติการ Windows เพื่อดาวน์โหลดสคริปต์ที่สอง
- สคริปต์ที่สองจะตรวจสอบระบบปฏิบัติการว่าเป็นเวอร์ชัน 32 หรือ 64 บิต จากนั้นจะดาวน์โหลดและติดตั้งเวอร์ชันที่เหมาะสมของ XMRig ซึ่งเป็นเครื่องมือสำหรับขุดเงิน



รูปที่ 2 ขั้นตอนการดาวน์โหลดมัลแวร์โดยใช้เครื่องมือ BITSAdmin บนระบบปฏิบัติการ Windows (hxxps://researchcenter.paloaltonetworks.com/wp-content/uploads/2018/01/figure4-2.png)

แบบที่ 2

- คล้ายรูปแบบที่ 1 แต่เปลี่ยนรูปแบบการดาวน์โหลดสคริปต์ที่สองจากการใช้ BITSAdmin เป็นการดาวน์โหลดผ่าน HTTP



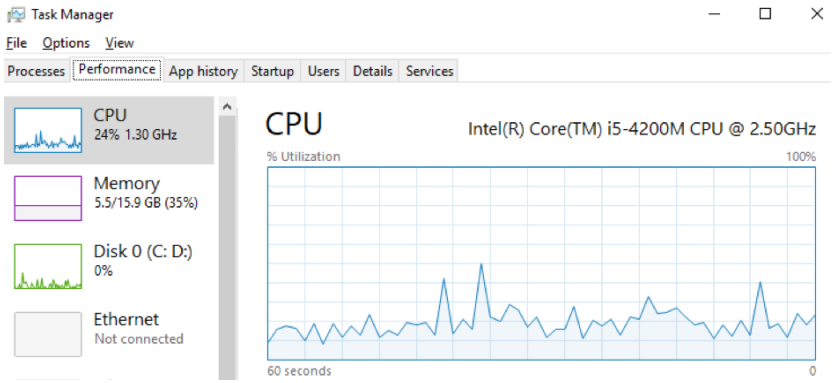
รูปที่ 3 ขั้นตอนการดาวน์โหลดมัลแวร์โดยอาศัยการเปลี่ยนเส้นทางไปยังเว็บไซต์ต่าง ๆ ก่อนพาไปยังเว็บไซต์ที่มีมัลแวร์จริงอยู่เพื่อดาวน์โลด
(hxxps://researchcenter.paloaltonetworks.com/wp-content/uploads/2018/01/Monero_6.png)

นอกจากนี้ภายหลังยังมีการเปลี่ยนแปลงรูปแบบการเผยแพร่อย่างต่อเนื่อง เช่น มีการใช้ .Net Framework เพื่อ Compile ไฟล์ที่ใช้สำหรับเผยแพร่ลงในเครื่องผู้ใช้ ซึ่งจะสร้างสคริปต์สำหรับดาวน์โหลดมัลแวร์ต่ออีกที รายละเอียดศึกษาได้จากรายงานอ้างอิง **[2]**

มัลแวร์สำหรับขุดเงินที่ถูกดาวน์โหลดแล้วนั้น โดยส่วนใหญ่พบว่ามีการติดตั้งไว้ภายใต้โฟลเดอร์ย่อยชื่อ msvc ซึ่งอยู่ในโฟลเดอร์ %APPDATA% และใช้ชื่อไฟล์ msvc.exe winmsvc.exe หรือ ondrive.exe เป็นต้น จากนั้นเมื่อมัลแวร์เริ่มทำงานจะเรียกใช้พร็อกซี่ (XMRig proxies) ในการเชื่อมต่อไปยังเซิร์ฟเวอร์ปลายทางที่รับข้อมูลในการประมวลผลขุดเหรียญ ซึ่งการใช้พร็อกซี่ดังกล่าวทำให้ไม่สามารถตรวจสอบที่อยู่กระเป๋าเงินดิจิทัลของผู้ประสงค์ร้ายที่รับเงินจากการขุด จึงยากที่จะระบุว่าผู้ประสงค์ร้ายได้เงินจากเผยแพร่มัลแวร์ดังกล่าวมากน้อยเพียงใด

ข้อแนะนำในการตรวจสอบ

เบื่องต้นให้ทำการตรวจสอบว่าคอมพิวเตอร์ที่ใช้งานมีการทำงาน CPU ผิดปกติหรือไม่ โดยการตรวจสอบผ่าน Task Manager หากพบการทำงานของ CPU ผิดปกติเช่น การทำงาน 100% อยู่ตลอดเวลาให้ต้องสงสัยว่าอาจจะติดมัลแวร์ดังกล่าวอยู่ โดยตรวจสอบได้จากโปรแกรม Task Manager ที่มาพร้อมกับระบบปฏิบัติการ Windows



รูปที่ 4 โปรแกรม Task Manager สำหรับตรวจสอบการใช้งาน CPU

ตรวจสอบเครือข่ายว่ามีการเชื่อมต่อไปยังเซิร์ฟเวอร์พร็อกซี่ (XMRig Proxy Connections) ที่ใช้ในการประมวลผลขุดเหรียญดังกล่าวหรือไม่ โดยมีข้อมูลของรายการเซิร์ฟเวอร์ดังนี้

หมายเลขไอพีปลายทาง	พอร์ตปลายทาง
5.101.122.228	8080
5.23.48.207	7777
144.76.201.175	80
144.76.201.175	8080
f.pooling.cf	80
b.pool.gq	80
a.pool.ml	8080
a.pool.ml	123
a.pool.ml	443
a.pool.ml	8443
a.pool.ml	80
a.pool.ml	1725

ตารางที่ 1 ข้อมูลเซิร์ฟเวอร์พร็อกซี่ (XMRig Proxy) ที่ใช้ในการประมวลผลขุดเหรียญ

ตรวจสอบประวัติการใช้งานอินเทอร์เน็ตว่ามีการเข้าลิงก์สำหรับเผยแพร่มัลแวร์หรือไม่ โดยมีรายการลิงก์ดังนี้

hxxp://bit[.]ly/2j3Yk8p
hxxp://bit[.]ly/2hxuusK
hxxp://bit[.]ly/2C7caP6
hxxp://bit[.]ly/HSGADGFDS
hxxp://bit[.]ly/2yV0JNa
hxxp://bit[.]ly/2Algzhc
hxxp://bit[.]ly/2zA08wz
hxxp://bit[.]ly/2hcsSUN
hxxp://bit[.]ly/2hr6KGb
hxxp://bit[.]ly/2xOVfPH
hxxp://bit[.]ly/2BoFNMr
hxxp://bit[.]ly/2xlWVQl
hxxp://bit[.]ly/2kEApR6
hxxp://bit[.]ly/2AkVK8t
hxxp://bit[.]ly/2yyUhLX
hxxp://bit[.]ly/2AkyUvs
hxxp://bit[.]ly/2zXRI6r
hxxp://bit[.]ly/2jjXmbJ
hxxp://bit[.]ly/2hzW6Rb
hxxp://bit[.]ly/2mkHzdP
hxxp://bit[.]ly/FSJKHJK
hxxp://bit[.]ly/2gB0ZW0
hxxp://bit[.]ly/2ixSCPu
hxxp://bit[.]ly/FSFSAASA
hxxp://bit[.]ly/2A5rxKB
hxxp://bit[.]ly/2xbUmjC
hxxp://bit[.]ly/2EHv415
hxxp://bit[.]ly/2Aq3gja
hxxp://bit[.]ly/2Bhr1tv
hxxp://bit[.]ly/2ynGl7o
hxxp://bit[.]ly/SOURCETXT
hxxp://bit[.]ly/2zGXAQx
hxxp://bit[.]ly/2hEhF3i
hxxp://bit[.]ly/2y3iGnG
hxxp://bit[.]ly/2ic2mvM
hxxp://bit[.]ly/2itoMrG
hxxp://bit[.]ly/2yvqOSU
hxxp://bit[.]ly/2zCj1n2
hxxp://bit[.]ly/2jEqYks

ตรวจสอบไฟล์ที่ต้องสงสัย จากค่า Hash ของไฟล์มัลแวร์ในรายงาน หรือตรวจสอบภายใต้โฟลเดอร์ %APPDATA% หากพบไฟล์ที่มีชื่อ msvc.exe winmsvc.exe หรือ ondrive.exe ให้ดำเนินการลบทิ้ง

ข้อแนะนำในการป้องกัน

1. เบื้องต้นอาจพิจารณาบล็อกการเชื่อมต่อไปยังเซิร์ฟเวอร์พร็อกซี่และลิงก์ที่ถูกใช้การโจมตีตามข้อมูลในส่วนของข้อแนะนำในการตรวจสอบ
2. ไม่ติดตั้งซอฟต์แวร์จากแหล่งที่ไม่น่าเชื่อถือ โดยอาจเลือกดาวน์โหลดจากเว็บไซต์ของผู้พัฒนาโดยตรง
3. ติดตั้งแอนติไวรัสและอัปเดตฐานข้อมูลอย่างสม่ำเสมอ
4. หากพบเหตุต้องสงสัยหรือต้องการคำแนะนำเพิ่มเติมในกรณีนี้ สามารประสานกับไทยเซิร์ตได้ทางอีเมล report@thaicert.or.th หรือโทรศัพท์ 0-2123-1212

อ้างอิง

1. http://monero.org
2. https://researchcenter.paloaltonetworks.com/2018/01/unit42-large-scale-monero-cryptocurrency-mining-operation-using-xmrig/
3. https://researchcenter.paloaltonetworks.com/wp-content/uploads/2018/01/figure2-2.png
4. https://researchcenter.paloaltonetworks.com/wp-content/uploads/2018/01/figure3-2.png

แจ้งเตือนการแพร่ระบาดมัลแวร์ VPNFilter กระจายไปยัง 54 ประเทศทั่วโลก

วันที่ประกาศ: 2 กุมภาพันธ์ 2561

ปรับปรุงล่าสุด: 2 กุมภาพันธ์ 2561

ประเภทภัยคุกคาม: Malicious Code

ข้อมูลทั่วไป

เมื่อวันที่ 23 พฤษภาคม 2561 ทีมนักวิจัยด้านความปลอดภัย Talos จากบริษัท Cisco รายงานการแพร่ระบาดของมัลแวร์ VPNFilter มุ่งเป้าไปที่อุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ (Internet of Things หรือ IoT) กว่า 5 แสนเครื่อง ใน 54 ประเทศ โดยพบการแพร่ระบาดตั้งแต่ปี 2559 อุปกรณ์ที่ได้รับผลกระทบส่วนใหญ่เป็นอุปกรณ์สำหรับสำนักงานขนาดเล็ก เช่น อุปกรณ์ยี่ห้อ Linksys, MikroTik, NETGEAR และ TP-Link เป็นต้น ขณะเดียวกันเจ้าหน้าที่ FBI เข้าควบคุมโดเมน toknowall.com ที่เป็นช่องทางสำรองในการเผยแพร่มัลแวร์

รายงานยังระบุว่ามัลแวร์ดังกล่าวถูกพัฒนาโดยกลุ่มแฮกเกอร์รัสเซีย ชื่อ Fancy Bear ที่แทรกแซงการเลือกตั้งของสหรัฐอเมริกาในปี 2559 และส่วนหนึ่งของโค้ดที่ใช้มัลแวร์ VPNFilter มีความคล้ายกับมัลแวร์ Black Energy ที่ใช้ในปฏิบัติการโจมตีระบบพลังงานไฟฟ้าของประเทศยูเครนในปี 2558

ผลกระทบ

มัลแวร์ดังกล่าวมีความสามารถหลายประการ และอาจทำให้เกิดผลกระทบอย่างรุนแรงต่อระบบเครือข่ายที่มีข้อมูลสำคัญ ซึ่งผลกระทบในเชิงต่างๆ สามารถสรุปได้ดังนี้

- สูญเสียข้อมูลสำคัญ/ข้อมูลความลับ
- สูญเสียความพร้อมใช้งาน ทำให้ระบบเครือข่ายไม่สามารถใช้งานได้ปกติ
- สูญเสียค่าใช้จ่ายที่เกิดขึ้นจากการกู้คืนระบบ

การแพร่ระบาดของมัลแวร์ VPNFilter ตรวจพบตั้งแต่ปี 2559 และได้ขยายขอบเขตการโจมตีไปทั่วโลก กว่า 5 แสนเครื่อง ใน 54 ประเทศ

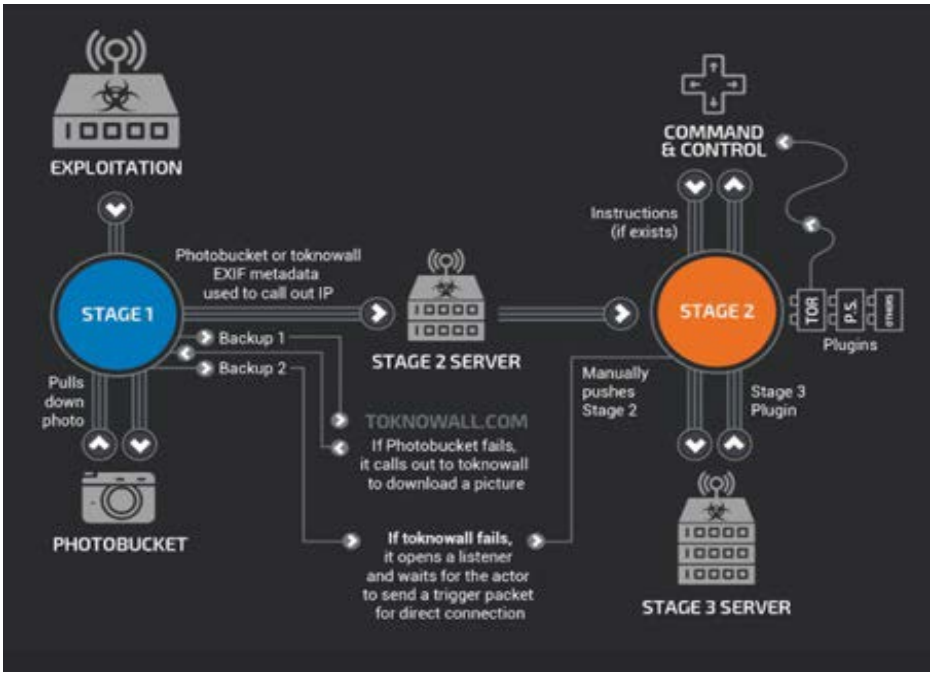
การทำงาน

มัลแวร์ VPNFilter อาศัยช่องโหว่เดิมแพร่กระจายไปยังอุปกรณ์ IoT ส่วนใหญ่เป็นอุปกรณ์เราเตอร์ทั่วไปที่ใช้งานในบ้านหรือสำนักงาน มัลแวร์สามารถทำงานได้บนหลายแพลตฟอร์ม และมีการทำงานที่ซับซ้อน โดยมีขั้นตอนการติดมัลแวร์เป็น 3 ระยะ ดังนี้

- มัลแวร์ ระยะที่ 1 แม้รีบูตเครื่องใหม่มัลแวร์ยังทำงานได้ปกติ ซึ่งเป็นจุดที่ทำให้ต่างจากมัลแวร์บางสายพันธุ์ที่โจมตีอุปกรณ์ IoT ที่ปกติมัลแวร์จะถูกกำจัดไปเมื่อรีบูตเครื่อง เป้าหมายหลักของการทำงานระยะนี้คือ แอบอาศัยอยู่ในเครื่องเพื่อดาวน์โหลดมัลแวร์ในระยะที่ 2

- มัลแวร์ ระยะที่ 2 มัลแวร์ในระยะนี้จะถูกติดตั้งในลักษณะ NON-PERSISTENT กล่าวคือ มัลแวร์จะหยุดทำงานเมื่อทำการรีบูตเครื่อง มัลแวร์ดังกล่าวสามารถขโมยไฟล์และข้อมูล รับคำสั่งต่างๆ จากผู้ประสงค์ร้าย บางเวอร์ชันสามารถทำให้อุปกรณ์ใช้งานไม่ได้โดยการเขียนข้อมูลทับส่วนสำคัญของเฟิร์มแวร์

- มัลแวร์ ระยะที่ 3 เป็นส่วนเสริม (plug-in) เพิ่มความสามารถให้มัลแวร์ระยะที่ 2 ได้แก่ โมดูลการดักรับข้อมูลที่วิ่งผ่านอุปกรณ์ ขโมยรหัสผ่านของบัญชีที่ใช้งานในเว็บไซต์ และการดักรับข้อมูลโปรโตคอลของ Modbus SCADA รวมถึงเพิ่มความสามารถให้รับส่งข้อมูลไปยังเครื่องผู้ประสงค์ร้ายผ่านเครือข่าย TOR ได้



รูปที่ 4 โปรแกรม Task Manager สำหรับตรวจสอบการใช้งาน CPU

อุปกรณ์ที่ได้รับผลกระทบ

อุปกรณ์ส่วนใหญ่ที่ได้รับผลกระทบจากมัลแวร์ VPNFilter ประกอบด้วยอุปกรณ์ยี่ห้อ Linksys, MikroTik, NETGEAR และ TP-Link รวมไปถึงอุปกรณ์จัดเก็บบันทึกข้อมูลในเครือข่าย NAS จากค่าย QNAP

Linksys	MikroTik	NETGEAR	TP-Link	QNAP
E1200	1016	DGN2200	R600VPN	TS251
E2500	1036	R6400	-	TS439P
WRVS4400N	1072	R7000	-	-
-	-	R8000	-	-
-	-	WNR1000	-	-
-	-	WNR2000	-	-

ข้อแนะนำในการตรวจสอบ

ตรวจสอบว่าอุปกรณ์ในระบบมีความเสี่ยงที่จะติดมัลแวร์หรือไม่ โดยใช้ข้อมูลสำหรับตรวจสอบ (IoC - Indicator of Compromise) จากข้อมูล การเชื่อมต่อไปยังเว็บไซต์ หมายเลขไอพี รวมถึง ค่า File Hashes ของมัลแวร์ต้องสงสัยภายในเครื่อง ดังต่อไปนี้

ระบบที่ถูกใช้งานเป็นฐาน C&C และหมายเลขไอพี

ข้อมูลที่เกี่ยวข้องกับระยะที่ 1

photobucket[.]com/user/nikkireed11/library

photobucket[.]com/user/kmila302/library

photobucket[.]com/user/lisabraun87/library

photobucket[.]com/user/eva_green1/library

photobucket[.]com/user/monicabelci4/library

photobucket[.]com/user/katyperry45/library

photobucket[.]com/user/saragray1/library

photobucket[.]com/user/millerfred/library

photobucket[.]com/user/jeniferaniston1/library

photobucket[.]com/user/amandaseyfried1/library

photobucket[.]com/user/suwe8/library

photobucket[.]com/user/bob7301/library

toknowall[.]com

ข้อมูลที่เกี่ยวข้องกับระยะที่ 2

91.121.109[.]209

217.12.202[.]40

94.242.222[.]68

82.118.242[.]124

46.151.209[.]33

217.79.179[.]14

91.214.203[.]144

95.211.198[.]231

195.154.180[.]60

5.149.250[.]54

91.200.13[.]76

94.185.80[.]82

62.210.180[.]229

zuh3vcyskd4gipkm[.]onion/bin32/update.php

มัลแวร์ ระยะที่ 1

50ac4fcd3fbc8abcaa766449841b3a0a684b3e217fc40935f1ac22c34c58a9ec
0e0094d9bd396a6594da8e21911a3982cd737b445f591581560d766755097d92

มัลแวร์ ระยะที่ 2

9683b04123d7e9fe4c8c26c69b09c2233f7e1440f828837422ce330040782d17
d6097e942dd0fdc1fb28ec1814780e6ecc169ec6d24f9954e71954eedbc4c70e
4b03288e9e44d214426a02327223b5e516b1ea29ce72fa25a2fcef9aa65c4b0b
9eb6c779dbad1b717caa462d8e040852759436ed79cc2172692339bc62432387
37e29b0ea7a9b97597385a12f525e13c3a7d02ba4161a6946f2a7d978cc045b4
776cb9a7a9f5afbaffdd4dbd052c6420030b2c7c3058c1455e0a79df0e6f7a1d
8a20dc9538d639623878a3d3d18d88da8b635ea52e5e2d0c2cce4a8c5a703db1
0649fda8888d701eb2f91e6e0a05a2e2be714f564497c44a3813082ef8ff250b

มัลแวร์ ระยะที่ 3

f8286e29faa67ec765ae0244862f6b7914fcdde10423f96595cb84ad5cc6b344
afd281639e26a717aead65b1886f98d6d6c258736016023b4e59de30b7348719

Self-Signed Certificate Fingerprints

d113ce61ab1e4bfcb32fb3c53bd3cdeee81108d02d3886f6e2286e0b6a006747
c52b3901a26df1680acbfb9e6184b321f0b22dd6c4bb107e5e071553d375c851
f372ebe8277b78d50c5600d0e2af3fe29b1e04b5435a7149f04edd165743c16d
be4715b029cbd3f8e2f37bc525005b2cb9cad977117a26fac94339a721e3f2a5
27af4b890db1a611d0054d5d4a7d9a36c9f52dffeb67a053be9ea03a495a9302
110da84f31e7868ad741bcb0d9f7771a0bb39c44785055e6da0ecc393598adc8
fb47ba27dceea486aab7a0f8ec5674332ca1f6af962a1724df89d658d470348f
b25336c2dd388459dec37fa8d0467cf2ac3c81a272176128338a2c1d7c083c78
cd75d3a70e3218688bdd23a0f618add964603736f7c899265b1d8386b9902526
110da84f31e7868ad741bcb0d9f7771a0bb39c44785055e6da0ecc393598adc8
909cf80d3ef4c52abc95d286df8d218462739889b6be4762a1d2fac1adb2ec2b
044bfa11ea91b5559f7502c3a504b19ee3c555e95907a98508825b4aa56294e4
c0f8bde03df3dec6e43b327378777ebc35d9ea8cfe39628f79f20b1c40c1b412
8f1d0cd5dd6585c3d5d478e18a85e7109c8a88489c46987621e01d21fab5095d
d5dec646c957305d91303a1d7931b30e7fb2f38d54a1102e14fd7a4b9f6e0806
c0f8bde03df3dec6e43b327378777ebc35d9ea8cfe39628f79f20b1c40c1b412

ข้อแนะนำในการรับมือและป้องกัน

ตรวจสอบว่าอุปกรณ์ในเครือข่ายติดมัลแวร์หรือไม่ โดยใช้ข้อมูลสำหรับตรวจสอบ (IoC - Indicator of Compromise) จากข้อมูลข้างต้น หรือเว็บไซต์ทางการของ Cisco

หากพบอุปกรณ์เน็ตเวิร์คเราเตอร์สำหรับสำนักงานขนาดเล็ก (SOHO) หรืออุปกรณ์สตอเรจ (NAS) ให้ทำการรีเซ็ตเป็นค่าเริ่มต้นจากโรงงาน (Factory reset)

ผู้ใช้งานสามารถตั้งค่าป้องกันการเข้าถึงหน้าเว็บบริหารจัดการเราเตอร์จากเครือข่ายอินเทอร์เน็ต ด้วยการเลือกใช้งานฟังก์ชัน ACL (Access Control List) ซึ่งเป็นฟังก์ชันที่ใช้ในการจำกัดการเข้าถึงบริการต่าง ๆ ตามเงื่อนไขที่สร้างขึ้น ที่มีอยู่ในเราเตอร์ เพื่อลดความเสี่ยงจากการถูกโจมตีช่องโหว่ดังกล่าวได้ อย่างไรก็ตามผู้ใช้ยังคงมีความเสี่ยงที่อาจถูกโจมตีจากผู้ไม่หวังดีที่เชื่อมต่ออยู่ในระบบเครือข่ายเดียวกันกับผู้ใช้ ดังนั้นสิ่งสำคัญที่สุดคือผู้ใช้งานควรหมั่นตรวจสอบค่าต่าง ๆ ที่ตั้งไว้ในเราเตอร์ระหว่างที่ผู้พัฒนากำลังแก้ไขปัญหาดังกล่าว และอัปเดตอุปกรณ์เป็นเวอร์ชันล่าสุดเพื่อป้องกันการติดมัลแวร์ รวมถึงตั้งรหัสผ่านในการเข้าถึงส่วนบริการจัดการระบบให้คาดเดาได้ยาก

ผู้ดูแลระบบภายในหน่วยงานอาจพิจารณาตั้งค่า เงื่อนไขในการตรวจจับพฤติกรรมต้องสงสัยบนอุปกรณ์เครือข่ายที่รองรับการตรวจจับ โดยใช้เงื่อนไขในรูปแบบ Snort Rule หมายเลข 45563 45564 46782 46783

ทั้งนี้ ไทยเซิร์ตได้ดำเนินการประสานขอข้อมูลรายการหมายเลขไอพีที่ได้รับผลกระทบในประเทศไทยจากหน่วยงานภายในเครือข่าย โดยเบื้องต้นพบจำนวนหมายเลขไอพีที่มีความเสี่ยงกว่า 50 รายการ และกำลังประสานข้อมูลไปยังผู้ให้บริการอินเทอร์เน็ตที่เกี่ยวข้อง สำหรับการดำเนินการแก้ไขต่อไป

อ้างอิง

1. https://blog.talosintelligence.com/2018/05/VPNFilter.html
2. https://www.thaicert.or.th/papers/general/2012/pa2012ge005.html


บทความแจ้งเตือนที่สำคัญและข้อแนะนำสำหรับผู้ดูแลระบบ

แจ้งเตือน ปฏิบัติการ GhostSecret ล้วงข้อมูลโครงสร้างพื้นฐานสำคัญและหน่วยงานอื่น ๆ กว่า 17 ประเทศ พบส่วนใหญ่เป็นเครื่องในประเทศไทย

วันที่ประกาศ: 25 เมษายน 2561

ปรับปรุงล่าสุด: 25 เมษายน 2561

ประเภทภัยคุกคาม: Intrusion

ข้อมูลทั่วไป

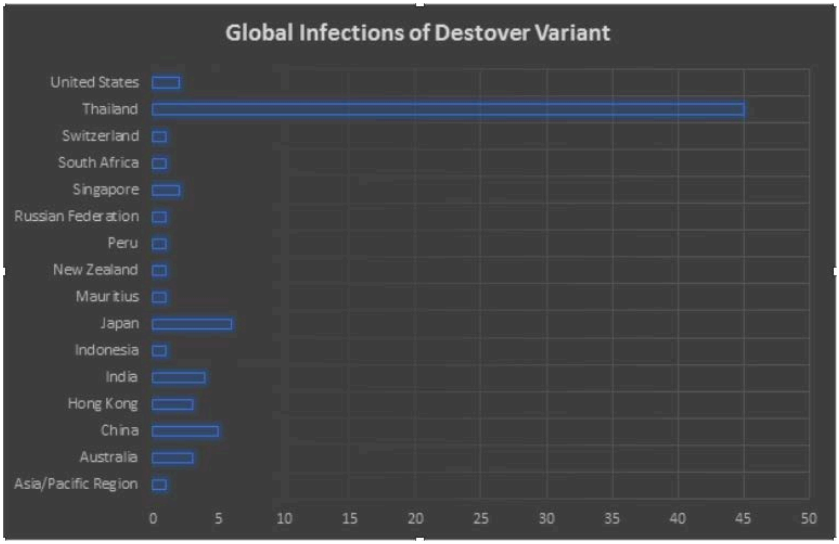
McAfee ได้เผยแพร่การค้นพบปฏิบัติการโจมตีขโมยข้อมูลด้วยมัลแวร์ ซึ่งมุ่งเป้าไปยังหน่วยงานโครงสร้างพื้นฐานสำคัญ หน่วยงานภาคอุตสาหกรรมบันเทิง ภาคการเงิน ภาคสาธารณสุข ในประเทศต่าง ๆ กว่า 17 ประเทศ รวมถึงประเทศไทย โดยเริ่มพบตั้งแต่เดือนกุมภาพันธ์ 2561 ปฏิบัติการดังกล่าวถูกตั้งชื่อว่า GhostSecret ซึ่งดำเนินการโดยกลุ่มแฮกเกอร์ที่ชื่อ Hidden Cobra ในรายงานของ McAfee ระบุพบการใช้เซิร์ฟเวอร์ในประเทศไทยในการโจมตี ซึ่งหมายเลขไอพีของระบบเป็นกลุ่มเดียวกับที่พบในการโจมตีบริษัท Sony Pictures นอกจากนี้ยังพบว่าลักษณะมัลแวร์ที่ใช้โจมตีคล้ายกับมัลแวร์ที่ใช้โจมตีบริษัท Sony Pictures ด้วย

ผลกระทบ

มัลแวร์ดังกล่าวมีความสามารถหลายประการ และอาจทำให้เกิดผลกระทบอย่างรุนแรงต่อระบบคอมพิวเตอร์ที่มีข้อมูลสำคัญ ซึ่งผลกระทบในเชิงต่าง ๆ สามารถสรุปได้ดังนี้

- สูญเสียข้อมูลสำคัญ/ข้อมูลความลับขององค์กร
- สูญเสียความพร้อมใช้งาน ทำให้ระบบคอมพิวเตอร์ไม่สามารถใช้งานได้ปกติ
- สูญเสียค่าใช้จ่ายที่เกิดขึ้นจากการกู้คืนระบบ

ปฏิบัติการ GhostSecret ได้เริ่มจากโจมตีหน่วยงานภาคการเงินของประเทศตุรกี ในเดือนกุมภาพันธ์ 2561 และในช่วงวันที่ 14 ถึง 18 มีนาคม 2561 ได้ขยายขอบเขตการโจมตีไปยังหน่วยงานต่าง ๆ กว่า 17 ประเทศ รวมถึงประเทศไทยที่พบ 45 ระบบติดมัลแวร์ดังกล่าว



รูปแสดง จำนวนระบบที่ติดมัลแวร์ แบ่งตามประเทศ ช่วงเดือนมีนาคม 2561

ลักษณะมัลแวร์และช่องทางการโจมตี

McAfee คาดการณ์ว่าในช่วงแรกมีการแพร่กระจายจากการโจมตีด้วยรูปแบบ Spear Phishing ซึ่งเป็นการโจมตีแบบมีเป้าหมายเฉพาะเจาะจง มัลแวร์นี้ถูกจัดอยู่ในประเภท Backdoor ซึ่งมีความสามารถหลบซ่อนตัวเพื่อติดต่อกับผู้ประสงค์ร้ายเป็นหลัก และสามารถรับคำสั่งต่าง ๆ เช่น ขโมยข้อมูลที่เกี่ยวกับระบบ ดาวน์โหลดและอัปโหลดไฟล์ ฯลฯ

โดยในช่วงเดือนกุมภาพันธ์ 2561 พบว่าผู้ประสงค์ร้ายได้ส่งอีเมลแนบไฟล์เอกสาร Microsoft Word ซึ่งมีโค้ดอันตรายฝังอยู่ ส่งไปยังหน่วยงานภาคการเงินในประเทศตุรกี โค้ดอันตรายดังกล่าวโจมตีอาศัยช่องโหว่ของ Adode Flash (หมายเลข CVE 2018-4878) เพื่อเผยแพร่มัลแวร์ที่ชื่อ Bankshot

ต่อมาในช่วงเดือนมีนาคม 2561 ผู้ประสงค์ร้ายได้โจมตีโดยหน่วยงานอื่น ๆ กว่า 17 ประเทศ โดยใช้มัลแวร์เพื่อขโมยข้อมูล รายงานไม่ได้ระบุช่องทางที่ใช้ในการเผยแพร่รวมถึงข้อมูลที่ถูกขโมย มัลแวร์บางตัวที่ใช้ในการโจมตี เช่น Bankshot2 มีลักษณะคล้ายกับ Bankshot ที่ใช้โจมตีเดือนกุมภาพันธ์ และบางตัวเหมือนกับมัลแวร์สายพันธุ์ Destover ที่ใช้ในการโจมตีบริษัท Sony Pictures โดยมัลแวร์ Bankshot2 มีความสามารถและพฤติกรรม ดังนี้

- ขโมยข้อมูลในเครื่องและส่งไปยังเครื่องเซิร์ฟเวอร์โดยอัตโนมัติ
- ติดต่อเครื่องเซิร์ฟเวอร์ผ่าน พอร์ต 443
- ติดต่อเครื่องเซิร์ฟเวอร์โดยใช้โปรโตคอลที่ผู้ประสงค์ร้ายสร้างเอง
- ลบไฟล์ต่าง ๆ ในเครื่อง
- ติดตั้ง Service อื่น ๆ ในเครื่อง
- เรียกดูรายการ Process ที่ทำงานในเครื่อง

AGREEMENT

Between

(Exchange Name)

With

[redacted]

This Agreement is made and entered into on the (month-day-year) by and between the undersigned parties below:

1. (EXCHANGE NAME), a company established under (Country Name) Law and having its address of business at (Address), in this matter represented by CEO name, in his capacity as Board of Director and therefore acting for and on behalf of (EXCHANGE NAME) hereinafter referred to as ---------- FIRST PARTY;

2. [redacted] individual whose holding France passport and having its address at [redacted] and therefore acting for and on behalf of himself/herself, hereinafter referred to as ----------SECOND PARTY;

Here in after FIRST PARTY and SECOND PARTY may sometimes individually be referred to as PARTY and collectively as THE PARTIES.

In consideration of the following underlying matters of the agreement, hereby declare as follows:

1. First Party is a company operating as a marketplace for trading the digital currencies especially Bitcoin, through its website exchange URL;

2. Second Party is a trader engaged in money service and cryptocurrency trading system and has a concern to cooperate with the First Party to conduct the trade of Bitcoin Trading;

3. The Parties agree to cooperate within the terms and conditions set forth herein, in order to allow the Second Party to operate Bitcoin Trading Activities and to distribute bitcoin on the Bitcoin Marketplace operated by the First Party, under the supervision of the First Party.

NOW, THEREFORE, The Parties are intending to be mutually bound under this Memorandum of Understanding and hereby agree as follows:

รูปแสดงตัวอย่างเอกสารที่ฝังโค้ดอันตราย

ข้อแนะนำในการตรวจสอบ

จากข้อมูลบทวิเคราะห์ของ Mcafee พบว่า โดยส่วนใหญ่มัลแวร์ดังกล่าวจะติดต่อไปยังเครื่อง C&C ผ่านพอร์ต 443 และใช้งาน SSL ในการส่งข้อมูล ซึ่งอาจทำให้การตรวจจับเป็นไปได้ยาก อย่างไรก็ตามให้พิจารณาความผิดปกติของเครื่องคอมพิวเตอร์ที่มีการเชื่อมต่อกับไอพีดังต่อไปนี้ ซึ่งคาดว่าจะมีส่วนเกี่ยวกับการทำงานของมัลแวร์ อ้างอิงจากผลการวิเคราะห์มัลแวร์ของ Mcafee IP addresses ของเครื่อง C&C

- 203.131.222.83
- 203.131.222.109
- 203.131.222.95
- 14.140.116.172

Hashes

- fe887fcab66d7d7f79f05e0266c0649f0114ba7c
- 8f2918c721511536d8c72144eabaf685ddc21a35
- 33ffbc8d6850794fa3b7bccb7b1aa1289e6eaa45
- 650b7d25f4ed87490f8467eb48e0443fb244a8c4
- 65e7d2338735ec04fd9692d020298e5a7953fd8d
- 166e8c643a4db0df6ffd6e3ab536b3de9edc9fb7
- a2e966edee45b30bb6bb5c978e55833eec169098

ข้อแนะนำในการรับมือและป้องกัน

- เบื้องต้นอาจพิจารณาบล็อกการเชื่อมต่อไปยังเซิร์ฟเวอร์ปลายทาง จากข้อมูลในส่วนข้อแนะนำในการตรวจสอบ

- ในกรณีที่พบว่าเครื่องคอมพิวเตอร์ติดมัลแวร์ ควรตัดการเชื่อมต่อจากเครือข่ายทันที เช่น การดึงสายแลนด์ออก

- ใช้เทคนิค Application whitelist เพื่อป้องกันมัลแวร์และโปรแกรมที่ไม่ได้รับการอนุญาตสามารถทำงานบนเครื่องคอมพิวเตอร์ได้ โดยจัดการให้มีเพียงโปรแกรมที่ระบุและตรวจสอบแล้วทำงานบนเครื่องคอมพิวเตอร์ ส่วนโปรแกรมอื่นๆ ซึ่งรวมถึงมัลแวร์จะไม่สามารถทำงานได้

- อัปเดตระบบปฏิบัติการและซอฟต์แวร์ให้เป็นปัจจุบันอยู่เสมอ โดยช่องโหว่ของโปรแกรมและระบบปฏิบัติการนั้นจะเป็นเป้าหมายในการการโจมตีอยู่บ่อยครั้ง การติดตั้งแพตช์ในเวอร์ชันล่าสุดจะถือได้ว่าเป็นการลดความเสี่ยงจากการถูกโจมตีได้เป็นอย่างดี

- หมั่นอัปเดตโปรแกรมป้องกันไวรัส และดาวน์โหลดซอฟต์แวร์จากเว็บไซต์ทางทางการหรือแหล่งที่น่าเชื่อถือ

- จำกัดสิทธิของผู้ใช้งาน (Permissions) ในการติดตั้งและรันโปรแกรมต่างๆ โดยยึดหลัก least privilege สำหรับทุกระบบและทุกบริการ การจำกัดสิทธิ์ดังกล่าวจะเป็นการป้องกันมัลแวร์ในการรัน และการแพร่กระจายในระบบเครือข่ายคอมพิวเตอร์

- หลีกเลี่ยงในเปิด Macro จากไฟล์เอกสารแนบที่มากับอีเมล เนื่องจากอาจมีการเรียกทำงานโค้ดที่ซ่อนตัวอยู่ในไฟล์ดังกล่าว ส่งผลให้ติดมัลแวร์บนเครื่องคอมพิวเตอร์ และก่อให้เกิดความเสียหายได้ กรณีหน่วยงานและองค์กรขนาดใหญ่ ควรบล็อกอีเมลที่มีไฟล์แนบจากแหล่งไม่น่าเชื่อถือ

- หากพบเหตุต้องสงสัยหรือต้องการคำแนะนำเพิ่มเติมในกรณีนี้ สามารถประสานกับไทยเซิร์ตได้ทางอีเมล report@thaicert.or.th หรือโทรศัพท์ 0-2123-1212

ปัจจุบันไทยเซิร์ตอยู่ในระหว่างการประสานไปยังหน่วยงานที่เกี่ยวข้องเพื่อเข้าถึงข้อมูลในเซิร์ฟเวอร์ที่ใช้ในการโจมตี เพื่อวิเคราะห์ร่วมกับ McAfee และหน่วยงานอื่นที่เกี่ยวข้อง และรวบรวมรายการผู้ตกเป็นเหยื่อในประเทศไทยเพื่อดำเนินการประสานแจ้งเหตุและให้ความช่วยเหลือต่อไป

อ้างอิง

1. https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide
2. https://www.thaicert.or.th/newsbite/2014-12-09-03.html
3. https://securingtomorrow.mcafee.com/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/


HACKER
INTERNET
CRIME
ATTACK
THIEF
CODING
CYBER
USERNAME
PASSWORD

THNIC แจ้งเตือน เว็บไซต์ที่ไม่รองรับมาตรฐาน EDNS อาจใช้งานไม่ได้หลัง 1 กุมภาพันธ์ 2562 ผู้ดูแลระบบโปรดตรวจสอบ

วันที่ประกาศ: 27 ธันวาคม 2561

ปรับปรุงล่าสุด: 27 ธันวาคม 2561

เรื่อง: THNIC แจ้งเตือน

ประเภทภัยคุกคาม: Availability

ที่มาและความสำคัญ

THNIC ประกาศแจ้งเตือนหน่วยงานเตรียมพร้อมรับมือเหตุการณ์ DNS Flag Day วันที่ 1 กุมภาพันธ์ 2562 เนื่องจากจะมีการเปลี่ยนแปลงกระบวนการทำงานของ DNS ระบบที่ยังไม่รองรับมาตรฐานใหม่อาจไม่สามารถใช้งานได้

DNS (Domain Name System) เป็นโพรโทคอลที่ใช้ในการติดต่อสื่อสารผ่านอินเทอร์เน็ต จุดประสงค์เพื่อให้สามารถเข้าใช้งานเว็บไซต์ อีเมล หรือบริการอื่นๆ ในอินเทอร์เน็ตได้โดยการพิมพ์ชื่อโดเมนแทนที่จะเป็นการพิมพ์ที่อยู่ไอพีโดยตรง มาตรฐาน DNS เกิดขึ้นในปี พ.ศ. 2525 และมีการปรับปรุงพัฒนาต่อมาเรื่อยๆ หนึ่งในการเปลี่ยนแปลงที่สำคัญคือมีการเพิ่มมาตรฐาน EDNS (Extension Mechanisms for DNS) ขึ้นมาในปี พ.ศ. 2542 โดยมีการปรับปรุงหลายอย่าง เช่น ขยายขนาดของข้อมูลที่รับส่งผ่าน DNS จากเดิมไม่เกิน 512 ไบต์เป็น 4096 ไบต์ ใช้ DNS Cookie เพื่อป้องกันการโจมตีแบบ DoS หรือใช้ DNSSEC ในการยืนยันตัวตนเซิร์ฟเวอร์ เป็นต้น

อย่างไรก็ตาม ถึงแม้มาตรฐาน EDNS จะมีการประกาศใช้งานมาเกือบ 20 ปีแล้ว แต่ซอฟต์แวร์ที่ใช้ให้บริการ DNS หรือการตั้งค่าเซิร์ฟเวอร์/ไฟร์วอลล์ ของบางระบบอาจยังไม่ได้รับการปรับปรุงให้รองรับมาตรฐานนี้ ที่ผ่านมาทั้งผู้พัฒนาซอฟต์แวร์และผู้ให้บริการ DNS ใช้วิธีแก้ปัญหาเฉพาะหน้า โดยยอมรับการเชื่อมต่อกับระบบที่ยังไม่รองรับมาตรฐาน EDNS ไปก่อน อย่างไรก็ตาม เนื่องจากการแก้ไขปัญหาแบบเฉพาะหน้านั้นมีผลกระทบหลายอย่าง เช่น ความล่าช้าในการทำงานเนื่องจากระบบต้องรองรับทั้งมาตรฐานเก่าและใหม่ไปพร้อมกัน หรือข้อจำกัดในการพัฒนาและใช้งานคุณสมบัติที่อยู่ในมาตรฐานใหม่ ที่สำคัญคือมีเซิร์ฟเวอร์อยู่จำนวนมากที่ยังไม่ได้รับการปรับปรุงระบบเพื่อให้รองรับมาตรฐานใหม่เนื่องจากยังคงใช้งานระบบเดิมต่อไปได้ ผู้พัฒนาซอฟต์แวร์ DNS และผู้ให้บริการ DNS รายหลักๆ จึงตกลงกันว่าตั้งแต่วันที่ 1 กุมภาพันธ์ 2562 จะบังคับให้บริการ DNS ในอินเทอร์เน็ตต้องรองรับมาตรฐาน EDNS เท่านั้น โดยบริการที่ยังไม่รองรับมาตรฐานใหม่จะถูกตัดออกจากระบบไป วันที่จะมีการปรับปรุงระบบครั้งใหญ่นี้ถูกเรียกว่า DNS Flag Day ผลกระทบที่จะตามมาคือระบบที่ยังไม่รองรับมาตรฐาน EDNS อาจไม่สามารถเข้าถึงได้

ผลกระทบที่อาจเกิดขึ้น

ตั้งแต่วันที่ 1 กุมภาพันธ์ 2562 ระบบให้บริการที่ไม่รองรับมาตรฐาน EDNS อาจไม่สามารถเข้าถึงได้

อ้างอิงข้อมูลจากมูลนิธิศูนย์สารสนเทศเครือข่ายไทย (THNIC Foundation) พบว่าโดเมนในประเทศไทยประมาณ 10,000 โดเมน หรือคิดเป็น 15% ของโดเมน .TH ทั้งหมด ยังไม่ได้รองรับมาตรฐาน EDNS ทำให้ระบบดังกล่าวอาจไม่สามารถเข้าถึงได้ตั้งแต่วันที่ 1 กุมภาพันธ์ 2562

ข้อแนะนำในการตรวจสอบและปรับปรุงระบบ

การตรวจสอบ

ผู้ดูแลระบบสามารถตรวจสอบว่าระบบของตนนั้นรองรับมาตรฐาน EDNS แล้วหรือไม่ โดยการใช้บริการสาธารณะ เช่น เว็บไซต์ DNS Flag Day (https://dnsflagday.net/) หรือเว็บไซต์ EDNS Complicance (https://ednscomp.isc.org/ednscomp)

การปรับปรุงระบบ

หากพบว่าระบบยังไม่รองรับมาตรฐาน EDNS อาจเกิดได้จาก 2 สาเหตุหลัก คือ ใช้งานซอฟต์แวร์รุ่นเก่าหรือยังไม่ได้ตั้งค่าให้รองรับ EDNS กับอีกสาเหตุคือมีการตั้งค่าไฟร์วอลล์ไม่ถูกต้อง

กระบวนการแก้ไขปัญหา

1. ตรวจสอบและปรับปรุงซอฟต์แวร์ DNS ให้เป็นรุ่นล่าสุด และตรวจสอบการตั้งค่าให้รองรับ EDNS

2. ตรวจสอบการตั้งค่าไฟร์วอลล์ให้รองรับ EDNS เช่น อนุญาตให้ UDP packet ขนาดเกิน 512 ไบต์สามารถผ่านเข้าออกได้

ทั้งนี้ ถึงแม้ทางหน่วยงานจะมีการแก้ไขปัญหาในระบบบริการ DNS ของตนเองแล้ว แต่หากหน่วยงานภายนอกไม่ได้มีการแก้ไขปัญหาดังกล่าว เมื่อถึงวันที่ 1 กุมภาพันธ์ 2562 ระบบปลายทางนั้นอาจไม่สามารถเข้าถึงได้ ทางหน่วยงานอาจจำเป็นต้องมีการประชาสัมพันธ์ให้กับบุคลากรภายในทราบ รวมถึงให้ความรู้และเตรียมคำตอบสำหรับเจ้าหน้าที่ Call Center, IT Support และ Help Desk ในกรณีที่มีผู้ใช้งานโทรศัพท์เข้ามาสอบถามปัญหาในวันที่มีการปรับระบบมาตรฐาน DNS

อ้างอิง

1. https://www.thnic.or.th/edns/
2. https://www.thaipr.net/it/909743


01
02
03
04

บทความให้ความรู้

แนวทางการจัดตั้งศูนย์ปฏิบัติการไซเบอร์เพื่อเฝ้าระวังภัยคุกคาม

ผู้เขียน: Martijn vander Heide และ ณัฐโชติ ดุสิตานนท์

วันที่เผยแพร่: 3 ตุลาคม 256๔1

ปรับปรุงล่าสุด: 3 ตุลาคม 2561

จากแนวโน้มภัยคุกคามไซเบอร์ที่สูงขึ้นอย่างต่อเนื่อง ในปัจจุบันองค์กรต่าง ๆ จึงให้ความสำคัญในด้านความมั่นคงปลอดภัยไซเบอร์มากขึ้น โดยหนึ่งในการดำเนินการหลักที่องค์กรควรพิจารณา คือ การจัดตั้งศูนย์ปฏิบัติการไซเบอร์ (Security Operations Center – SOC หรือ Cyber Security Operations Center – CSOC) เพื่อเป็นศูนย์กลางในการเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์ขององค์กร ซึ่งเป็นส่วนหนึ่งในหน้าที่ของทีม CSIRT (Computer Security Incident Response Team) โดย SOC ที่มีประสิทธิภาพ จะช่วยให้องค์กรสามารถรับรู้ถึงสถานการณ์ภัยคุกคามต่าง ๆ ในเครือข่ายของตนได้อย่างครอบคลุม และสามารถระบุถึงเหตุการณ์ผิดปกติได้อย่างรวดเร็วและแม่นยำ รวมถึงตอบสนองต่อเหตุการณ์นั้นได้ทันท่วงที นอกจากนี้ SOC ยังสามารถทำหน้าที่อื่น เช่น การวิเคราะห์ข้อมูลเชิงลึก การตรวจสอบหาช่องโหว่ในระบบ และการสร้างความตระหนักรู้ให้กับเจ้าหน้าที่ในองค์กร เป็นต้น เนื้อหาในบทความนี้เป็นการแนะนำองค์ประกอบที่สำคัญในการจัดตั้ง SOC อ้างอิงจากเอกสารโดยมีรายละเอียดดังนี้

ข้อแนะนำในการตรวจสอบและปรับปรุงระบบ

การกำหนดขอบเขตหน้าที่ของ SOC เป็นองค์ประกอบที่มีความสำคัญที่สุด เพื่อให้ทุกฝ่ายในองค์กรมีความเข้าใจอย่างชัดเจนว่า SOC คืออะไรและทำหน้าที่อะไร และสามารถวัดความก้าวหน้าและประสิทธิภาพการดำเนินงานของ SOC ได้ โดยเอกสารกำหนดขอบเขตหน้าที่ของ SOC ควรประกอบด้วย

- พันธกิจ
- บริการ
- เป้าหมาย
- หน้าที่ความรับผิดชอบ
- วัน-เวลาทำการ
- ข้อมูลสำหรับติดต่อ
- โครงสร้างตำแหน่งบุคลากรของ SOC

เข้าใจสภาพแวดล้อมของระบบสารสนเทศ

เจ้าหน้าที่ SOC ต้องมีความเข้าใจอย่างถ่องแท้ในโครงสร้างและสถาปัตยกรรมระบบ แผนผังโครงสร้างเครือข่าย (network diagram) และมาตรการด้านความมั่นคงปลอดภัย รวมถึงมีการจัดทำบัญชีทรัพย์สินสารสนเทศที่ต้องเฝ้าระวังทั้งหมด เพื่อให้สามารถวิเคราะห์และหาความสัมพันธ์ของเหตุการณ์โจมตีที่เกิดขึ้น รวมถึงตรวจสอบช่องโหว่ในระบบได้อย่างถูกต้อง นอกจากนี้ เจ้าหน้าที่ SOC ควรหมั่นตรวจสอบความถูกต้องของระบบ SIEM หรือระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่าย เพื่อให้มั่นใจได้ว่าล็อค (log) จากอุปกรณ์เครือข่ายต่าง ๆ ได้รับการบันทึกอย่างครบถ้วน

จัดเตรียมบุคลากร

ตำแหน่งและหน้าที่ของเจ้าหน้าที่ SOC โดยทั่วไปเป็นดังที่แสดงในตารางที่ 1 องค์กรสามารถเลือกที่จะปฏิบัติหน้าที่เหล่านี้โดยเจ้าหน้าที่ในองค์กร หรือว่าจ้างบริษัทที่มีความเชี่ยวชาญ (Outsourced) ในขั้นต้น องค์กรควรมีเจ้าหน้าที่ประจำอย่างน้อยหนึ่งคนในแต่ละระดับ อย่างไรก็ตาม ควรมีการเตรียมทีมเจ้าหน้าที่สำรอง เพื่อให้สามารถรับมือภัยคุกคามขนาดใหญ่ ซึ่งจำเป็นต้องใช้เจ้าหน้าที่จำนวนมากเพียงชั่วคราว

ตำแหน่ง	หน้าที่
ระดับ 1: เจ้าหน้าที่วิเคราะห์การแจ้งเตือนภัยคุกคาม (Alert Analyst)	เฝ้าระวังและแจ้งเตือนภัยคุกคามอย่างต่อเนื่อง ตรวจสอบความพร้อมของอุปกรณ์รักษาความมั่นคงปลอดภัยไซเบอร์ ได้แก่ sensors และendpointsตรวจสอบและรวบรวมข้อมูลภัยคุกคามในเบื้องต้นและประสานไปยังเจ้าหน้าที่ในระดับ 2 (เจ้าหน้าที่รับมือภัยคุกคาม)
ระดับ 2: เจ้าหน้าที่รับมือภัยคุกคาม (Incident Responder)	วิเคราะห์ภัยคุกคามเชิงลึก หาความสัมพันธ์ของข้อมูลที่เกี่ยวกับการโจมตีที่ได้รับจากแหล่งต่าง ๆ ประเมินผลกระทบของระบบและข้อมูลสำคัญ รวมถึงอัปเดตระบบอย่างต่อเนื่องเพื่อให้สามารถตรวจจับภัยคุกคามใหม่ได้อย่างมีประสิทธิภาพ
ระดับ 3: ผู้เชี่ยวชาญเฉพาะทาง (Subject Matter Expert)	มีความเชี่ยวชาญในด้านต่าง ๆ เช่น เครือข่าย การตรวจพิสูจน์พยานหลักฐานดิจิทัล การวิเคราะห์มัลแวร์ หรือเชี่ยวชาญเกี่ยวกับซอฟต์แวร์หรือระบบเฉพาะที่ใช้ในหน่วยงาน ผู้เชี่ยวชาญเฉพาะทางมีหน้าที่ปฏิบัติการเชิงรุก ค้นหาภัยคุกคามที่แอบแฝงในระบบ พัฒนา ปรับปรุงรูปแบบตรวจจับและวิเคราะห์ภัยคุกคาม

ตารางที่ 1 ประเภทเจ้าหน้าที่ SOC

องค์กรจำเป็นต้องเลือกตัวชี้วัดที่เหมาะสมซึ่งสามารถวัดประสิทธิภาพการปฏิบัติงานของเจ้าหน้าที่ เช่น ควรใช้ ระยะเวลาที่ใช้ในการตอบสนองต่อภัยคุกคาม (time to first response) แทนที่จะใช้ จำนวนการแจ้งเตือนภัยคุกคามที่ได้รับการจัดการ (number of alerts handled)

กระบวนการ

กระบวนการสำหรับ SOC มีหลากหลายขึ้นกับขอบเขตและบริการของ SOC ในแต่ละองค์กร ในเบื้องต้น SOC ควรมีกระบวนการหลักดังนี้

- กระบวนการตรวจจับภัยคุกคาม
- กระบวนการแจ้งเตือนภัยคุกคาม (ผ่านเว็บไซต์ โทรศัพท์ อีเมล)
- กระบวนการรายงานไปยังเจ้าหน้าที่ระดับสูง และยกระดับการดำเนินการ
- กระบวนการแจ้งข้อมูลที่จำเป็นให้ทีมที่เข้ากะใหม่รับทราบเมื่อเปลี่ยนกะ
- กระบวนการบันทึกงานที่เจ้าหน้าที่ได้ทำ
- กระบวนการบันทึกภัยคุกคามที่พบ
- กระบวนการตรวจสอบเพื่อให้มั่นใจว่าการดำเนินการได้มาตรฐาน
- กระบวนการสร้าง Dashboard เพื่อเฝ้าระวังและรายงานภัยคุกคาม
- กระบวนการวิเคราะห์ภัยคุกคามที่พบ

กระบวนการที่พูดถึงข้างต้นเป็นกระบวนการในการจัดการภัยคุกคาม ซึ่งหลายหน่วยงานได้สร้างมาตรฐานหรือแนวทางไว้ ตัวอย่าง เช่น NIST SP 800-61 ซึ่งเป็นมาตรฐานจัดการภัยคุกคามโดยหน่วยงาน NIST (National Institute of Standards and Technology) ประเทศสหรัฐฯ ได้ระบุ 4 ขั้นตอนหลักคือ

1. การเตรียมตัวเพื่อรับมือภัยคุกคาม (Preparation) เช่น มีการร่างขอบเขตการทำงานของศูนย์ฯ กระบวนการรับมือ กำหนดหน้าที่และบทบาทของเจ้าหน้าที่ตามที่ได้กล่าวข้างต้น

2. การตรวจจับและวิเคราะห์ (Detection & Analysis)

- ระบุปัญหา การเปลี่ยนแปลงแนวโน้มภัยคุกคาม และช่องว่างของนโยบายด้านความมั่นคงปลอดภัย
- ค้นหาภัยคุกคามแฝง และประเมินผลกระทบ
- เก็บข้อมูลเหตุการณ์และเวลาเกิดเหตุ เพื่อให้การวิเคราะห์ทำได้ง่ายขึ้น
- ระบุลักษณะรูปแบบของภัยคุกคามที่พบ
- ประเมินจุดเริ่มต้นของการโจมตี
- ประเมินเป้าหมายของการโจมตี
- หลีกเลี่ยงการดำเนินการที่ทำให้ผู้โจมตีรู้ตัวว่าองค์กรตรวจจับการโจมตีได้แล้ว
- วิเคราะห์ ทำความเข้าใจการโจมตี

3. การจำกัดความเสียหาย (Containment) กำจัดภัยคุกคามรวมถึงต้นตอปัญหาเพื่อไม่ให้เกิดซ้ำ และฟื้นฟูระบบให้สามารถใช้งานโดยเร็วที่สุด

4. การดำเนินการหลังการแก้ไขปัญหา (Post-incident Activity) ศึกษาบทเรียนจากเหตุการณ์ที่เกิด วิเคราะห์จุดที่ยังต้องปรับปรุงเพื่อเพิ่มประสิทธิภาพในการรับมือภัยคุกคามและลดความเสียหายที่อาจเกิดขึ้น รวมถึง

นำข้อเสนอแนะจากผู้บริหาร มาปรับปรุงนโยบาย กระบวนการรับมือภัยคุกคาม และติดตั้งปรับปรุงระบบด้านความมั่นคงปลอดภัยเพิ่มเติม

กระบวนการทั้งหมดนี้จะใช้งานได้ดี ควรมีการบันทึกและปรับปรุงอย่างต่อเนื่อง องค์กรอาจจัดเตรียมเท็มเพลตหรือฟอร์ม สำหรับใช้สื่อสารเมื่อเกิดภัยคุกคาม ซึ่งช่วยให้รับมือภัยคุกคามได้เร็วขึ้น

การเลือก ติดตั้ง และใช้งานเครื่องมือ

เครื่องมือที่สนับสนุนการปฏิบัติการของ SOC ได้แก่ เครื่องมือค้นหาทรัพย์สินสารสนเทศ (asset discovery) เครื่องมือบริหารจัดการช่องโหว่ (vulnerability management) เครื่องมือตรวจจับภัยคุกคาม (intrusion detection) และเครื่องมือการรวบรวมและวิเคราะห์ข้อมูลที่เกี่ยวกับภัยคุกคาม (threat Intelligence) เป็นต้น ในการเลือกเครื่องมือและแนวทางการติดตั้งที่เหมาะสม ให้พิจารณาจากสถานการณ์ที่องค์กรต้องการให้ SOC สามารถรับมือได้ และก่อนการปรับแต่งเครื่องมือในตรวจจับภัยคุกคามซึ่งเป็นส่วนที่ยากสุด ควรทดลองใช้งานเครื่องมือไปก่อน เพื่อศึกษาและสร้างข้อมูลบรรทัดฐาน (baseline) ให้สามารถแยกแยะรูปแบบข้อมูลที่รับส่งในเครือข่ายแบบปกติและแบบผิดปกติได้

นอกจากนี้ SOC ควรมีระบบ ticket ที่ใช้บันทึกการจัดการเหตุการณ์ภัยคุกคาม ซึ่งควรเป็นระบบที่แยกออกมาต่างหากจากระบบ ticket อื่น ๆ เนื่องจากอาจมีข้อมูลที่เป็นความลับ และเพื่อป้องกันไม่ให้มัลแวร์แพร่กระจายไปยังระบบอื่น และควรใช้ระบบอัตโนมัติ (automation) ในส่วนที่ต้องทำซ้ำให้มากที่สุด โดยพยายามสร้างระบบให้อยู่บนแพลตฟอร์มเดียวกันเพื่อให้บริหารจัดการได้ง่าย

ปฏิบัติการของ SOC

ในระยะแรกที่ระบบต่าง ๆ ยังไม่ได้รับการปรับแต่งนัก อาจส่งผลให้มีการแจ้งเตือนผิดพลาด (false positive) จำนวนมาก จึงจำเป็นต้องใช้เวลาในการปรับแต่ง ซึ่งถือเป็นการดำเนินการที่สำคัญของ SOC

ในบางกรณี SOC อาจต้องอาศัยบริการสนับสนุนอื่นเพิ่มเติม เช่น การพิสูจน์พยานหลักฐานดิจิทัลเพื่อรายงานผลในชั้นศาล การประสานกับฝ่ายกฎหมาย หรืองานที่ต้องใช้ความเชี่ยวชาญเฉพาะด้านซึ่งอยู่นอกเหนือขอบเขตของ SOC ในกรณีเช่นนี้ หากมีการจัดทำข้อตกลงความร่วมมือไว้ล่วงหน้าก็จะช่วยได้มากเมื่อเกิดภัยคุกคาม

ข้อมูลอื่น ๆ เพื่อศึกษา

เนื้อหาในบทความนี้เป็นการแนะนำข้อมูลเบื้องต้นในการจัดตั้ง SOC โดยผู้ที่สนใจสามารถศึกข้อมูลเพิ่มเติมได้จากเอกสารดังนี้

- ThaiCERT Handbook: Establishing a CSIRT
- NIST SP 800-61 rev 2
- McAfee (Intel Security) White Paper: Creating and Maintaining a SOC

อ้างอิง

1. https://www.thaicert.or.th/downloads/files/Establishing_a_CSIRT_th.pdf
2. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
3. https://community.mcafee.com/nysyc36988/attachments/nysyc36988/siem/7399/1/wp-creating-maintaining-soc.pdf

การตั้งค่ากำหนดสิทธิการเข้าถึงข้อมูล AWS S3 Bucket

วันที่เผยแพร่: 16 เมษายน 2561

ปรับปรุงล่าสุด: 16 เมษายน 2561

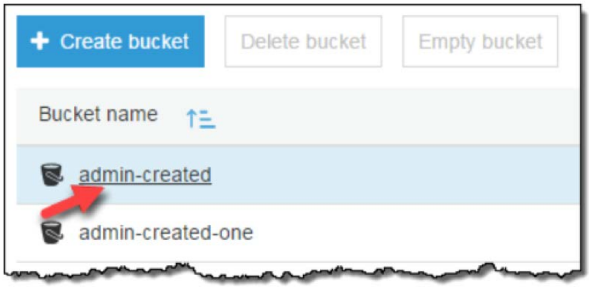
mazon Simple Storage Service หรือ Amazon S3 เป็นบริการสำหรับจัดเก็บข้อมูลบนอินเทอร์เน็ตของผู้ใช้บริการ AWS ซึ่งผู้ใช้สามารถกำหนดขนาดพื้นที่จัดเก็บได้ตามต้องการ รวมถึงการกำหนดสิทธิของข้อมูลแต่ละส่วน ให้เข้าถึงได้เฉพาะผู้ใช้ที่ต้องการได้

ในการตั้งค่าสิทธิของ Amazon S3 นั้น เบื้องต้น ผู้ใช้จะต้องกำหนด Buckets หรือ ถัง เพื่อใช้กำหนดขนาดพื้นที่ข้อมูล รวมถึง objects ต่าง ๆ โดยการตั้งค่าเริ่มต้นของระบบ (Default) จะมีการกำหนดสิทธิในการเข้าถึงข้อมูลแบบส่วนตัว ซึ่งจะเข้าถึงได้เฉพาะเจ้าของข้อมูลนั้น ๆ แต่อย่างไรก็ตาม ผู้พัฒนาสามารถตั้งค่าแบบสาธารณะได้ด้วย ซึ่งจะทำให้ผู้ใช้งานทั่วไปสามารถเข้าถึงข้อมูลได้ จึงไม่เหมาะกับกรณีที่เป็นข้อมูลสำคัญหรือเป็นความลับ และอาจเป็นช่องทางให้ผู้ประสงค์ร้ายเข้าถึงข้อมูลสำคัญหรือเป็นความลับดังกล่าวได้

สำหรับแนวทางในการตั้งค่าเพื่อกำหนดสิทธิไม่ให้ผู้ใช้งานทั่วไปสามารถเข้าถึงข้อมูลได้จากสาธารณะสามารถตั้งค่าได้ดังนี้

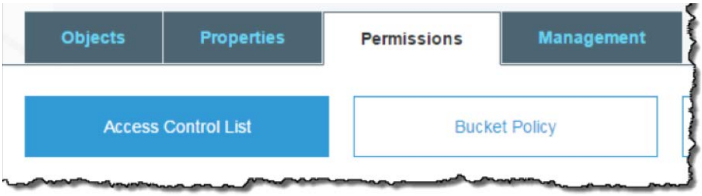
การกำหนดสิทธิการเข้าถึงข้อมูล ในแต่ละ Bucket

1. เข้าสู่ระบบ AWS Management Console https://s3.console.aws.amazon.com/s3/
2. เลือก Bucket ที่ต้องการกำหนดสิทธิการเข้าถึง



ตารางที่ 1 ประเภทเจ้าหน้าที่ SOC

3. เลือกแท็บ Permissions



รูปที่ 2 ภาพแสดงในส่วนกำหนด Permission

4. สามารถจัดการการกำหนดสิทธิการเข้าถึงได้ ดังต่อไปนี้:

Owner access: โดย Owner หมายถึงบัญชีผู้ใช้งาน root ของ AWS (root)

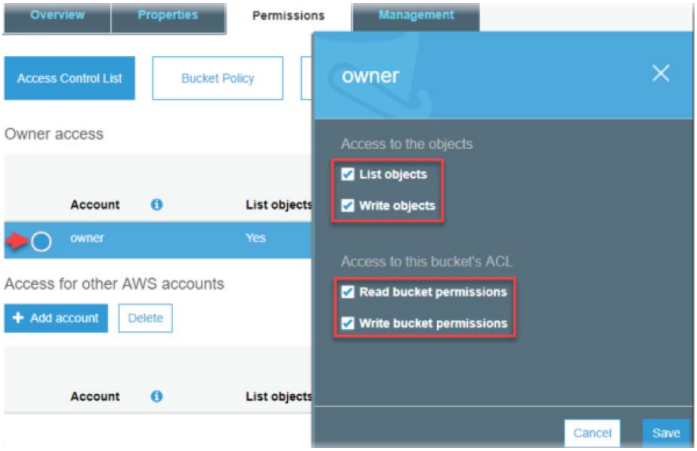
การกำหนดสิทธิให้กับ owner โดยมีขั้นตอน ดังนี้

1. เลือกบัญชีผู้ใช้ (root) โดยอยู่ในส่วน owner access
2. จากนั้นกำหนดค่า permission โดยมีรายละเอียด ดังนี้

   Access to the objects: คือ การเข้าถึงข้อมูลที่อยู่ใน Bucket

   List objects: สามารถเรียกข้อมูลที่อยู่ใน Bucket ได้

   Write objejects: สามารถเขียนข้อมูลใน Bucket ได้
3. เมื่อกำหนดค่าเสร็จแล้ว จากนั้นเลือก save เพื่อบันทึก

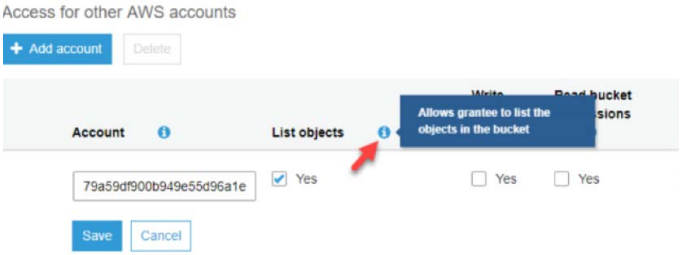


รูปที่ 3 การกำหนด Permission ให้กับ Owner

Access for other AWS accounts

การกำหนดสิทธิการเข้าถึงให้กับ AWS accounts อื่น โดยระบุ User ID ที่ต้องการให้เข้าถึงข้อมูล

ซึ่งการกำหนดให้ AWS accounts อื่นๆสามารถเข้าถึงข้อมูล จะทำให้ บัญชีสามารถกำหนดสิทธิให้กลับผู้ใช้ภายใต้บัญชีดังกล่าวได้ เพิ่มเติม **[4]**



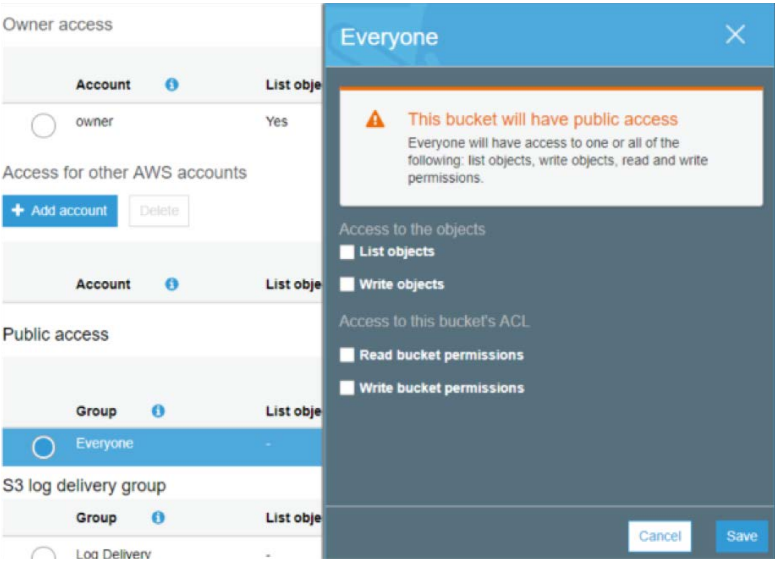
รูปที่ 4 การกำหนด Permission ให้กับบัญชีผู้ใช้อื่น

Public access:

เป็นการกำหนดสิทธิให้คนทั่วไปสามารถเข้าถึงข้อมูลใน Bucket นี้ได้ โดยหากเป็นข้อมูลที่เป็นความลับหรือมีความสำคัญ ไม่ควรกำหนดให้คนทั่วไปเข้าถึงได้

การกำหนดสิทธิไม่ให้ผู้คนทั่วไปสามารถเข้าถึงได้ มีขั้นตอนดังนี้

4. เลือก Everyone ในส่วนของ Public access
5. ทำการยกเลิก checkbox ทั้งหมด
6. เมื่อกำหนดค่าเสร็จแล้ว เลือก save เพื่อบันทึก



รูปที่ 5 การกำหนด Permission ให้กับ Public access

อ้างอิง

1. https://docs.aws.amazon.com/AmazonS3/latest/user-guide/set-permissions.html

2. https://docs.amazonaws.cn/en_us/AmazonS3/latest/user-guide/set-bucket-permissions.html

3. http://docs.amazonaws.cn/IAM/latest/UserGuide/id_root-user.html

4. http://docs.amazonaws.cn/en_us/IAM/latest/UserGuide/id_roles_create_for-user.html

ภาคผนวก

ประเภทข่าว	คำอธิบาย
Awareness	รวบรวมข่าวสาระน่ารู้ (ข้อแนะนำ, ความก้าวหน้าด้านเทคโนโลยี ฯลฯ) เช่น ข่าว MasterCard เปิดตัวฟีเจอร์ใหม่ ให้เซลฟีหรือใช้ลายนิ้วมือยืนยันตัวตน
Fraud	รวบรวมข่าวที่เกี่ยวกับการหลอกลวงทางออนไลน์ (การสร้างหน้าเว็บไซต์ปลอมเพื่อหลอกขโมยรหัสผ่าน, ข้อความหลอกลวงจากอีเมลหรือโซเชียลมีเดีย ฯลฯ) เช่น ข่าว การขโมยเงินจากธนาคารออนไลน์ด้วยการหลอกเปลี่ยนชิมมีแนวโน้มเพิ่มสูงขึ้น
Incident	รวบรวมข่าวที่เกี่ยวกับการโจมตีโดยทั่วไป (การเจาะระบบองค์กร, การโจมตีที่ส่งผลต่อการทำงานของระบบ ฯลฯ) เช่น ข่าว ธนาคารในเอกวาดอร์ถูกโจมตีระบบ SWIFT มูลค่าความเสียหายกว่า 12 ล้านดอลลาร์
Law & Policy	รวบรวมข่าวที่เกี่ยวกับกฎหมายและนโยบายทั้งในและต่างประเทศ ซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัยหรือสิทธิความเป็นส่วนตัวของประชาชน เช่น ข่าว ศาลลอสแองเจลิสสั่งให้ผู้ต้องสงสัยปลดล็อกโทรศัพท์มือถือโดยใช้ลายนิ้วมือ
Malware	รวบรวมข่าวที่เกี่ยวกับมัลแวร์ (การค้นพบมัลแวร์สายพันธุ์ใหม่, การแพร่ระบาดของมัลแวร์, ความสามารถใหม่ของมัลแวร์ ฯลฯ) เช่น ข่าว ระวังภัยมัลแวร์เรียกค่าไถ่ CTB-Locker เวอร์ชันใหม่ระบาด มุ่งโจมตีเว็บไซต์
Privacy	รวบรวมข่าวที่เกี่ยวกับเหตุการณ์ที่ส่งกระทบต่อสิทธิความเป็นส่วนตัวของประชาชน (การสอดแนม, การรั่วไหลข้อมูลส่วนบุคคล ฯลฯ) เช่น ข่าว นักวิจัยเตือน QQ Browser แอบขโมยข้อมูลผู้ใช้และมีช่องโหว่ด้านความมั่นคงปลอดภัย
Standard & Guideline	รวบรวมข่าวที่เกี่ยวข้องกับมาตรฐานและแนวปฏิบัติ เช่น OWASP ออกมาตรฐานการตรวจสอบความมั่นคงปลอดภัยของแอปพลิเคชันบนโทรศัพท์มือถือ
Statistics	รวบรวมข่าวที่เกี่ยวข้องกับสถิติ เช่น ข่าว FBI เผย บริษัทเอกชนสูญเสียเงิน 2.3 พันล้านดอลลาร์ใน 2 ปีครึ่ง ให้กับอีเมลหลอกลวง
Vulnerability	รวบรวมข่าวที่เกี่ยวกับช่องโหว่ในซอฟต์แวร์หรืออุปกรณ์ต่าง ๆ พร้อมคำแนะนำ เช่น ข่าว ระวัง กล้องวงจรปิดไร้สายของ D-Link มีช่องโหว่ถูกเจาะระบบได้

ศูนย์ประสานการรักษาความมั่นคงปลอดภัย
ระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

Thailand Computer Emergency Response Team (ThaiCERT)
Electronic Transactions Development Agency (ETDA)
Ministry of Digital Economy and Society

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี)
ชั้น 20 เลขที่ 33/4ถนนพระราม 9 แขวงห้วยขวาง
เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์: 0 2123 1212

ISBN
978-616-7956-45-9