รับมือกับภัยคุกคามทางคอมพิวเตอร์อย่างไรให้ปลอดภัย

2021

INFORMATION TECHNOLOGY

Agenda

HACKER / CRACKER

CYBER SECURITY

MALWARE / VIRUS

HACKER / CRACKER

Hacker & Cracker ต่างกันอย่างไร

HACKER / CRACKER

HACKER คือ ผู้ที่มีความสามารถเชี่ยวชาญเกี่ยวกับระบบคอมพิวเตอร์โปรแกรมต่างๆ สามารถเปลี่ยนแปลง หรือ แก้ไข และสร้างโปรแกรมต่างๆ มีความสามารถในการเข้าถึงโปรแกรม หรือ ระบบต่างๆ อย่างเช่น การเจาะรหัส หรือ ระบบรักษาความปลอดภัยในคอมพิวเตอร์เครื่องอื่นๆ ได้เป็นอย่างดี หรือ มีหน้าที่ปองกันระบบโปรแกรม และเครื่องคอมพิวเตอร์เครื่องอื่นๆ

HACKER / CRACKER

HACKER มีประเภท ผู้ที่นำความรู้ ที่มีมาใช้ให้เกิดประโยชน์ในด้านดี

ส่วนอีกประเภท ก็คือ นำความรู้ที่มีมาใช้ในทางผิด เพื่อประโยชน์ส่วนตน

แต่โดยส่วนใหญ่แล้วภาพลักษณ์ที่เราเห็นกัน หรือ ได้ยินมาจากแหล่งข่าวต่างๆ

จะออกมาในแนวทางที่ไม่ดีเท่าไหร่ และแต่ละประเภทก็จะมีดังนี้

- ไวต์แฮต (White Hat)
- เกรย์แฮต (Gray Hat)
- แบล็กแฮต (Black Hat)

HACKER / CRACKER

CRACKER กลุ่มบุคคลที่มีความสามารถเกี่ยวกับระบบของคอมพิวเตอร์เช่นเดียวกัน แต่การกระทำ หรือ วัตถุประสงค์นั้นแตกต่างกันโดยสิ้นเชิง

ในทางส่วนใหญ่แล้ว พวกนี้จะชอบเจาะข้อมูล หรือ โปรแกรมต่างๆ ของผู้ดูแลเพื่อประโยชน์ส่วนตนเท่านั้น

เปาหมาย ก็คือ ทำลายระบบ และนำไปใช้เป็นของตน

HACKER / CRACKER

CRACKER สิ่งที่พวก cracker ทำ เป็นสิ่งที่ผิดกฎหมาย อย่างเช่น การเจาะข้อมูล

เข้าระบบองค์กรที่มีผลกระทบต่อประเทศเพราะอาจจะทำลายข้อมูลเหล่านั้น

และอาจจะนำข้อมูลไปขายให้พวกก่อการร้าย

ซึ่งอาจจะทำให้ส่งผลเสียความมั่นคงให้ประเทศเลยก็ว่าได้ อีกมุมหนึ่ง

ถ้าเปรียบเทียบกันแล้วกลุ่มพวก cracker ก็คือพวก Black hat นั่นเอง

CRACKER

COMEX / JAILBRAKEME.COM

แค็กเกอร์หนุ่มรายนี้มีชื่อว่า **นิโคลาส อัลเลกร้า** (Nicholas Allegra) อายุ 19 ปี ซึ่งเป็นที่รู้จักกันอย่างดีในนามของ "โคเม็กซ์" (Comex) ได้รับข้อเสนอให้เข้าทำงานกับบริษัทแอปเปิ้ล ด้วยการเริ่มจากตำแหน่งพนักงานทดลองงาน เพื่อมาช่วยกันหาทางสร้างระบบป้องกันของไอโฟน (iPhone) ให้แน่นหนามากขึ้นกว่าเดิม

นายอัลเลกร้า เป็นผู้ก่อตั้งเว็บไซต์แนะนำและเผยแพร่การเจาะระบบไอโฟนชื่อดัง "เจลเบรกมีดอทคอม" (JailBreakMe.com) และยังเป็นแฮ็กเกอร์คนดังที่มีผลงานแฮ็กระบบข้อมูลสินค้าของแอปเปิ้ลมาแล้วหลายชิ้น โดยเฉพาะกับการเจาะระบบปฏิบัติการ "ไอโอเอส" (iOS) ซึ่งทำให้ผู้ใช้ไอโฟน ไอพอด (iPod) และไอแพด (iPad) ได้ลงโปรแกรมละเมิดลิขสิทธิ์ทั้งหลายลงบนผลิตภัณฑ์ของแอปเปิ้ลได้อย่างง่ายดาย


O2-UK
09:22
99%
JailbreakMe
by comex (et al.)
JailbreakMe
Jailbreak to get tweaks and apps Apple won't allow in the App Store. Free, legal, safe.
You should sync with iTunes before using this tool.
More Info »
slide to jailbreak
iPhone

CRACKER

นายทวีทรัพย์ หรือ ภูมิพัฒน์ หรือ โอ๋ อายุ 41 ปี เคยถูกตำรวจกองปราบปรามจับกุมเมื่อปี 2550 หลังจากเข้าไปเจาะข้อมูลระบบคอมพิวเตอร์ของบริษัทแอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน) หรือเอไอเอส โดยเข้าไปแก้ไขเพิ่มเติมข้อมูลในบัตรเติมเงินไปขายให้บุคคลอื่นผ่านทางอินเทอร์เน็ต มูลค่าความเสียหายกว่า 50 ล้านบาท ตำรวจจับแฮ็กเกอร์รายนี้ได้ที่ห้องพักเลขที่ 2918 ชั้น 9 อาคารวงศ์เจริญแมนชั่น หรือ แกรนด์แมนดาริน ซ.ลาดพร้าว 130 แขวงคลองจั่น เขตบางกะปิ กทม.

นายทวีทรัพย์ จบปริญญาตรี คณะรัฐศาสตร์ จากมหาวิทยาลัยแห่งหนึ่ง มีความสนใจในเรื่องคอมพิวเตอร์ และศึกษาเรียนรู้ด้วยตัวเองจนมีความรู้ความสามารถเข้าขั้นเทพสามารถเจาะระบบคอมพิวเตอร์ของบริษัทต่างๆ ได้ ปี 2548 เคยเจาะข้อมูลของบริษัททรูเข้าไปแก้ไขข้อมูลค่าบัตรเติมเงินยี่ห้อออเร้นจ์ สร้างความเสียหายกว่า 105 ล้านบาท นอกจากนี้ยังเคยเจาะระบบธนาคารพาณิชย์หลายแห่ง รวมทั้งเคยทดลองเจาะระบบองค์การบริหารการบินและอวกาศแห่งชาติสหรัฐอเมริกา (นาซา) มาแล้ว แต่ไม่มีการยืนยันว่าทำสำเร็จหรือไม่

CYBER SECURITY

CYBER SECURITY

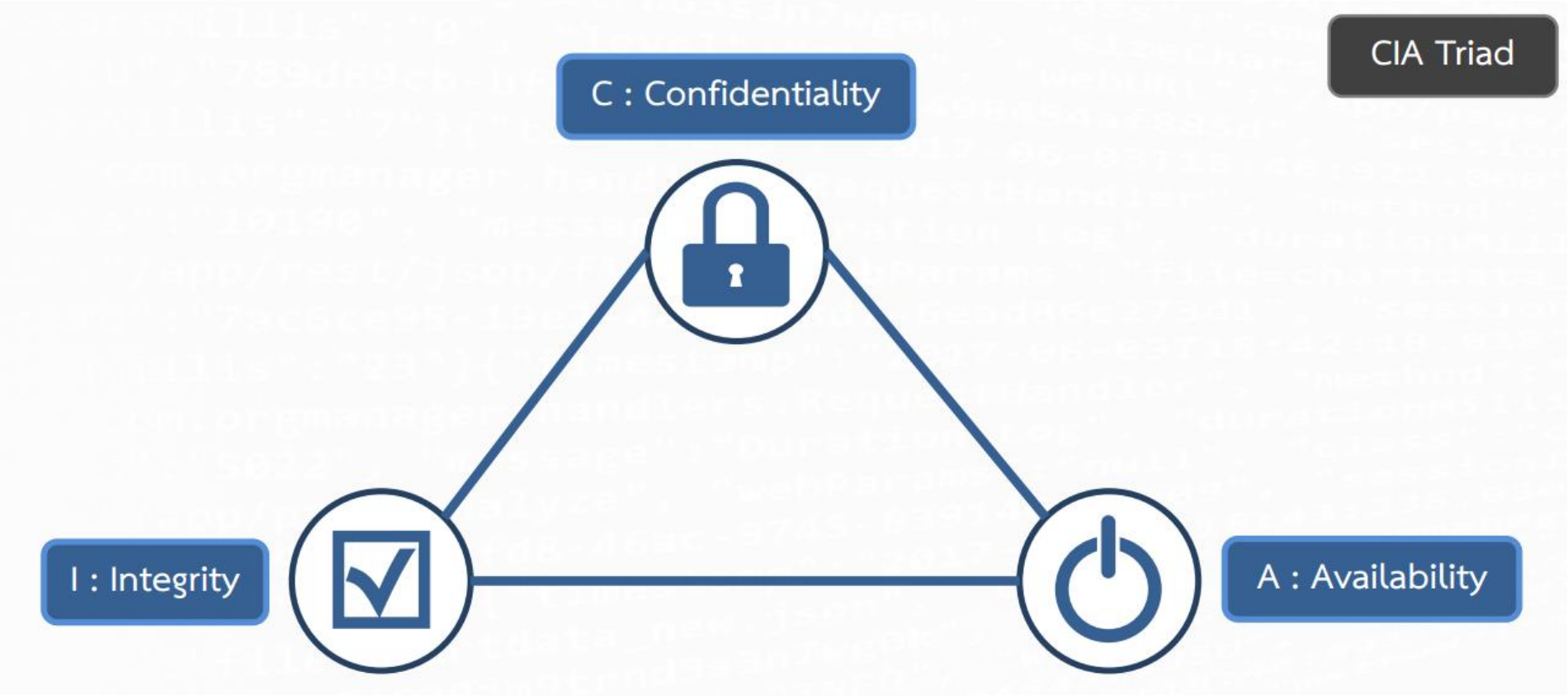
CYBER SECURITY

ความมั่นคงปลอดภัยทางไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้

เพื่อปองกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย, โครงสร้างพื้นฐานทางสารสนเทศ

CYBER SECURITY

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์



CYBER SECURITY

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์

Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้

Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง

Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล

CYBER SECURITY

LAW OF CYBER SECURITY

ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

- พ.ร.บ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
- พ.ร.บ คุ้มครองข้อมูลส่วนบุคคล PDPA
- มาตรฐานด้านความปลอดภัย ISO 27001 (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

MALWARE / VIRUS

MALWARE

มาจากคำว่า Malicious และ Software หมายถึง โปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมา เพื่อทำอันตรายกับข้อมูลในระบบ เช่น ทำให้เครื่องคอมพิวเตอร์ทำงานผิดปกติ ขโมยหรือทำลายข้อมูลหรืออาจจะเปิดช่องทางให้ผู้ไม่หวังดีเข้ามาควบคุมเครื่องของเราได้

1.VIRUS COMPUTER

ไวรัสคอมพิวเตอร์ (Computer Virus)

สามารถแพร่กระจายตัวเองไปยังเครื่องอื่น ๆ ผ่านไฟล์ที่ส่งต่อกันระหว่างเครื่อง เมื่อมันแอบเข้ามายังคอมพิวเตอร์ได้แล้ว มันก็จะเข้าไปก่อกวนการทำงาน จนทำให้เกิดผลเสียต่อเครื่องคอมพิวเตอร์ เหมือนเวลาที่เราป่วยเพราะไวรัส ร่างกายของเราก็จะทำงานได้ไม่เต็มที่เท่าเดิม คอมพิวเตอร์เองก็เช่นเดียวกัน

2. COMPUTER WORM

Computer Worm (หนอนคอมพิวเตอร์)

หนอนคอมพิวเตอร์จะมีความแตกต่างจากไวรัสคอมพิวเตอร์ตรงที่วิธีการทำงานโดยที่ Worm จะเป็นโปรแกรมที่สามารถแพร่ตัวเองได้ Worm ไม่ผ่านการใช้งานของผู้ใช้ และไม่จำเป็นต้องไปเกาะกับไฟล์ใดๆเลย โดยส่วนมากมันจะคัดลอกและกระจายตัวมันเองข้ามเครือข่าย เช่น ระบบเครือข่าย หรือ อินเทอร์เน็ต เช่น การส่งอีเมล การส่ง IM และการใช้ Network แบบ Peer-2-Peer นั่นเอง

2. COMPUTER WORM

วิธีป้องกัน WORM หนอนคอมพิวเตอร์

1. หลีกเลี่ยงที่จะไม่เปิดไฟล์ที่แนบมาที่มาจากอีเมล หากเรายังไม่แน่ใจว่าผู้ส่งเป็นคนที่เชื่อถือได้ หรือถ้าไม่แน่ใจว่าไฟล์ที่แนบมาเป็นอะไรกันแน่
2. บนเครื่องคอมพิวเตอร์ควรทำการติดตั้ง โปรแกรมป้องกันไวรัส อย่างน้อย 1 ตัว
3. ทำการ อัปเดตข้อมูลไวรัสของโปรแกรมป้องกันไวรัสให้เป็นปัจจุบันตลอด
4. ติดตั้งและเปิดใช้งาน ไฟร์วอลล์ (Fire wall)
5. หลีกเลี่ยงการดาวน์โหลดไฟล์หรือโปรแกรมที่ผิดลิขสิทธ์ เช่น โปรแกรม Crack เป็นต้น

3. TROJAN HORSE

ม้าโทรจัน คือ โปรแกรมที่ถูกโหลดเข้าไปใน
คอมพิวเตอร์ เพื่อ ปฏิบัติการ "ล้วงความลับ"เช่น
รหัสผ่าน, User Name และข้อมูลส่วนตัวเกี่ยวกับการ
Login ระบบ ที่ถูกพิมพ์ผ่านคีย์บอร์ดโดย
ผู้ใช้งาน โดยส่วนใหญ่แฮคเกอร์จะส่งโปรแกรมม้าโทร
จัน เข้าไปในคอมพิวเตอร์เพื่อดักจับข้อมูลดังกล่าว
แล้วนำไปใช้ในการเจาะระบบ หรือเพื่อโจมตี
คอมพิวเตอร์ เซิร์ฟเวอร์

4. ROOTKIT

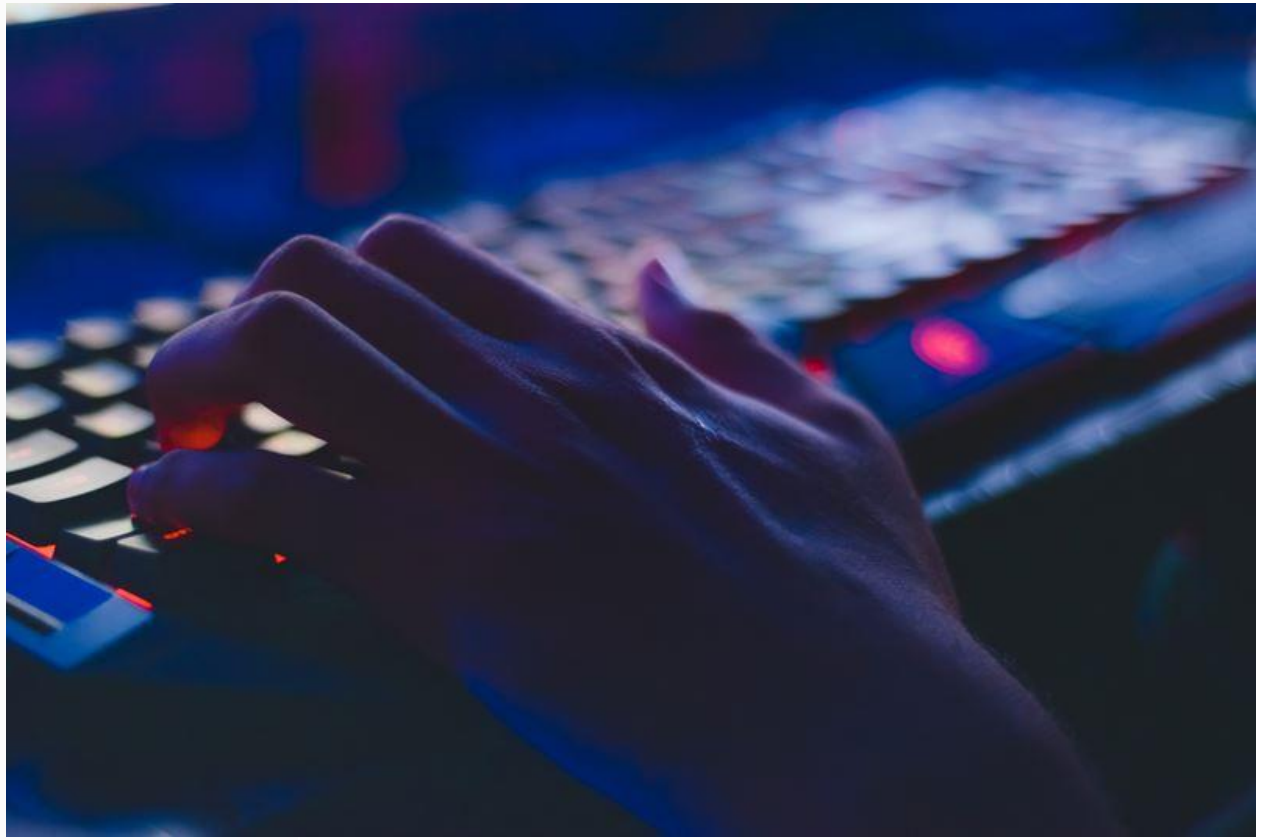
Rootkit (รูตคิต)

Rootkit คือ ชุดโปรแกรมที่สามารถซ่อนตัวอยู่ในคอมพิวเตอร์หรือนำมาใช้เพื่อซ่อนมัลแวร์* (Malware) ตัวอื่นๆ ให้ทำงานอยู่ในคอมพิวเตอร์ได้ยาวนานขึ้น เนื่องจาก **Rootkit** นั้นถูกออกแบบมาให้ฝังตัวอยู่ในชั้นของระบบคอมพิวเตอร์ที่โปรแกรมป้องกันไวรัสทั่วๆ ไปตรวจพบได้ยาก

5. KEY LOGGER

Key logger (เครื่องมือดักจับการพิมพ์บนคีย์บอร์ด)

Keylogger คือ เครื่องมือดักจับข้อมูล ที่สามารถเก็บ (หรือดักจับ) ตัวอักษรทุกตัวที่ผู้ใช้คอมพิวเตอร์ปอนเข้าสู่ระบบผ่านการกดแปนคีย์บอร์ด โดยอาศัยวิธีการต่างๆ เช่น อุปกรณ์ฮาร์ดแวร์หรือโปรแกรมพิเศษ ส่วนใหญ่แล้วผู้ใช้จะไม่ทราบว่าตนเองกำลังถูกเก็บข้อมูลอยู่



6. GRAY WARE

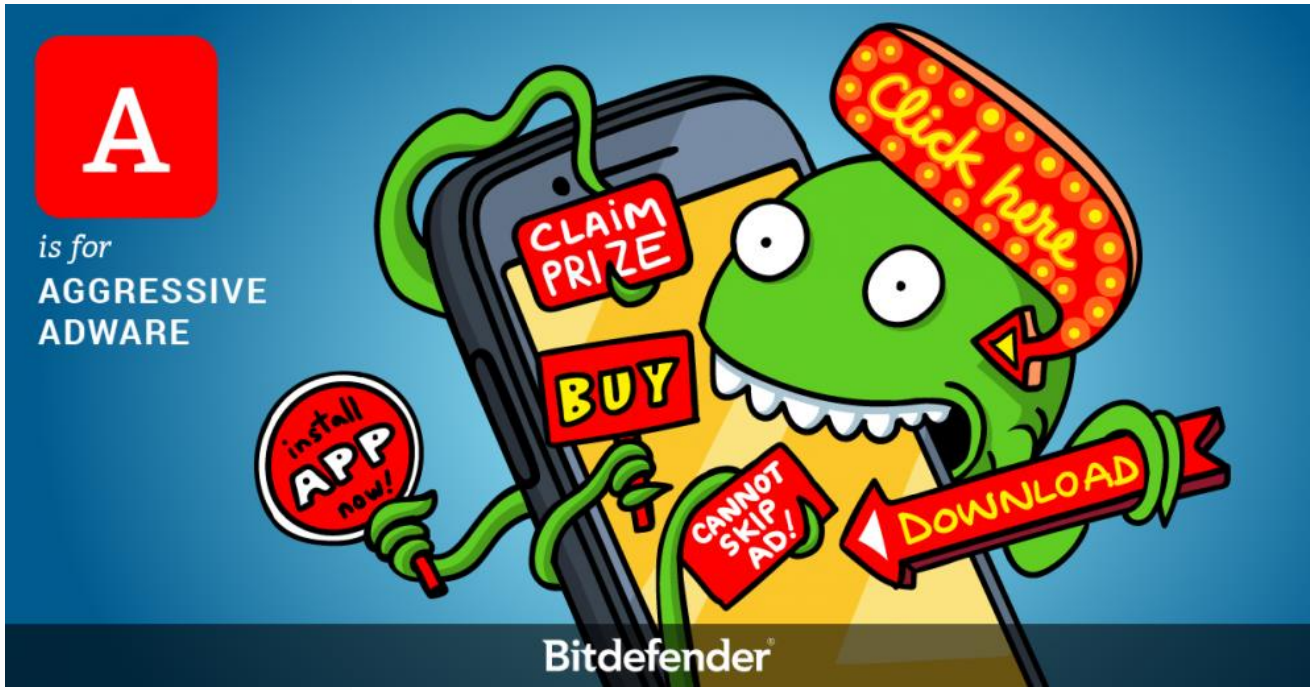
Gray ware (ซอฟต์แวร์สีเทา)

เป็นซอฟต์แวร์ปกติที่เราใช้งานอยู่เป็นประจำ แต่เมื่อมีการค้นพบช่องโหว่ แล้วผู้พัฒนาไม่อัปเดตปิดช่องโหว่ให้ เราก็สามารถเรียกว่า **Grayware** ได้เช่นกัน เช่น ระบบปฏิบัติการ Windows เวอร์ชันเก่าที่ Microsoft หยุดสนับสนุนไปแล้ว

7. ADWARE

Adware (ซอฟต์แวร์สนับสนุนโฆษณา)

Adware (แอดแวร์) มีชื่อย่อมาจาก Advertising Supported Software เป็นโปรแกรมที่มักติดตั้งมาโดยที่เราไม่ได้ตั้งใจ โดยที่มาของโปรแกรม Adware มักจะมาจากการที่เราไปดาวน์โหลดโปรแกรมฟรีตามเว็ปต่าง ๆ นั่นเอง



8. BACKDOOR VIRUS

Backdoor Virus

Backdoor Virus หรือ Remote Access **Trojan** (RAT) เป็น Malware ที่เมื่อถูกติดตั้งแล้ว โปรแกรมจะทำการลอบเข้าระบบอย่างลับๆ ทาง **Backdoor** (รูรั่วของระบบ) เพื่อให้แฮคเกอร์สามารถ Remote Control ระบบได้โดยไม่มีการแจ้งเตือนผู้ดูแลระบบ

9. SPY WARE

Spyware (สปายแวร์ หรือ ซอฟต์แวร์สายสืบ)

Spyware คือ โปรแกรมที่แฝงเข้ามาในคอมพิวเตอร์ขณะที่คุณท่องอินเตอร์เน็ต เป็นโปรแกรมที่ถูกเขียนขึ้นมาสอดส่อง (Spy) หรือดักจับข้อมูลการใช้งานเครื่องคอมพิวเตอร์ของคุณ

10. MALVERTISING

Malvertising (มัลแวร์ในรูปแบบโฆษณา)

Malvertising คือ การใช้โฆษณาบนโลกออนไลน์ เพื่อแพร่กระจายมัลแวร์ เมื่อเราคลิกดูโฆษณาดังกล่าว เราจะถูกพาไปยังเว็บไซต์อันตรายที่มีการฝังสคริปต์มัลแวร์เอาไว้ อันตรายที่น่ากลัว **คือ** แฮกเกอร์จะนำโฆษณานี้ไปลง กับระบบโฆษณาต่างๆ ที่เว็บไซต์ทั่วไปนิยมใช้งานกัน

11. CRYTO JACKING

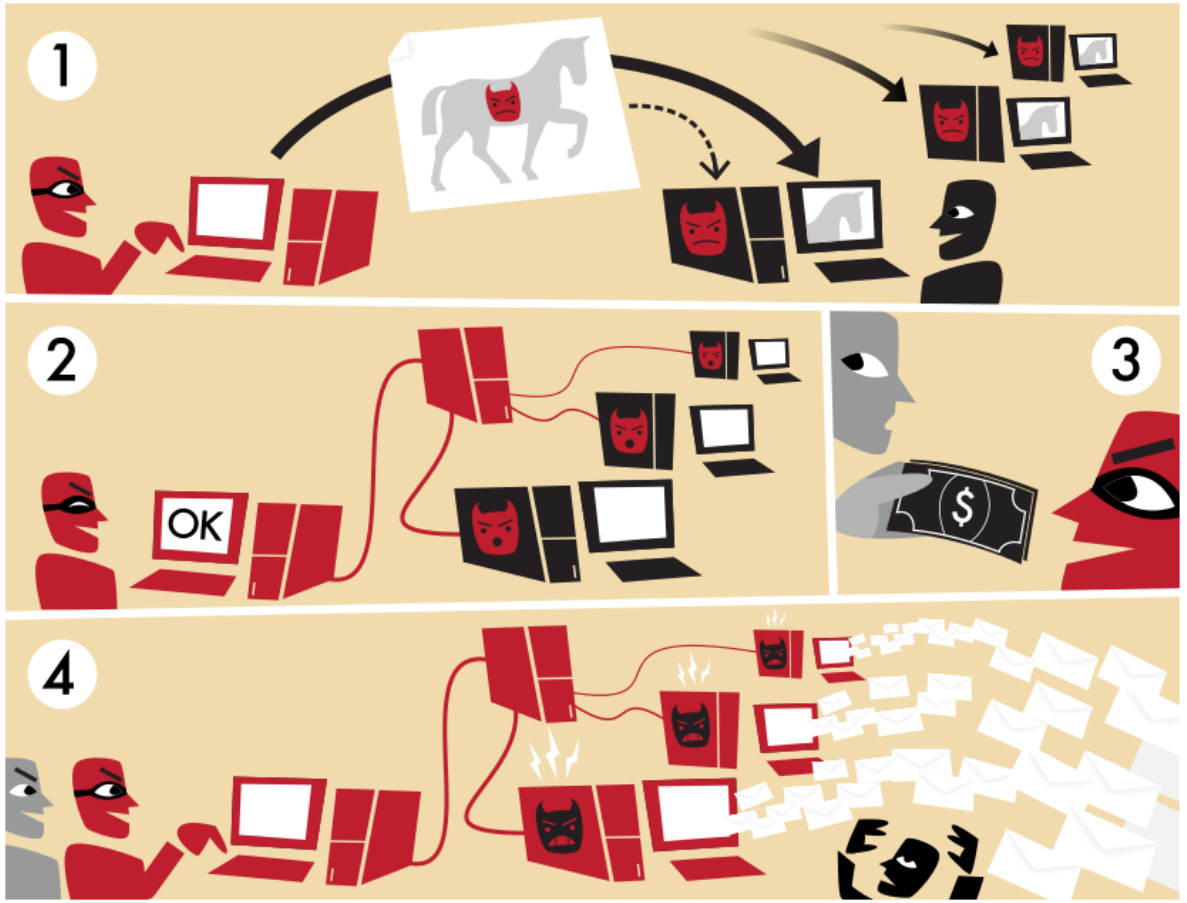
Crypto jacking (การขโมยทรัพยากรคอมพิวเตอร์)

Crypto jacking หรือ การขโมยทรัพยากรคอมพิวเตอร์ เป็นการหาเงินดิจิทัลจำเป็นต้องใช้ฮาร์ดแวร์ประสิทธิภาพสูงในการถอดสมการ หรือที่เรียกกันว่า "ขุดเหรียญ" ที่ต่อมามีคนพัฒนาระบบคลาวด์สำหรับขุดเหรียญขึ้นมา เพื่อดึงทรัพยากรจากคอมพิวเตอร์หลายๆ เครื่องมาช่วยกันขุดผ่านอินเทอร์เน็ต

12. BOTNETS

Bots (บอต) และ Botnets (บอตเน็ต)

BOTNET หรือ ro**BOT NET**work เป็นภัยคุกคามต่อผู้ใช้งานอินเทอร์เน็ตรูปแบบใหม่ ซึ่งมิจฉาชีพเขียนโปรแกรมบอตเน็ตนี้ถูกเขียนโดยมิจฉาชีพโดยใช้เทคนิคการโจมตีเครือข่ายด้วยโปรแกรมประสงค์ร้าย (Malware) ที่ซับซ้อนและมีรูปแบบที่หลากหลายกว่าไวรัสคอมพิวเตอร์หรือหนอนอินเทอร์เน็ตทั่วไป บอตเน็ตที่ถูกสร้างขึ้นนี้อาจจะเป็นเครื่องมือที่ใช้ส่ง Spam Mail และ Phishing

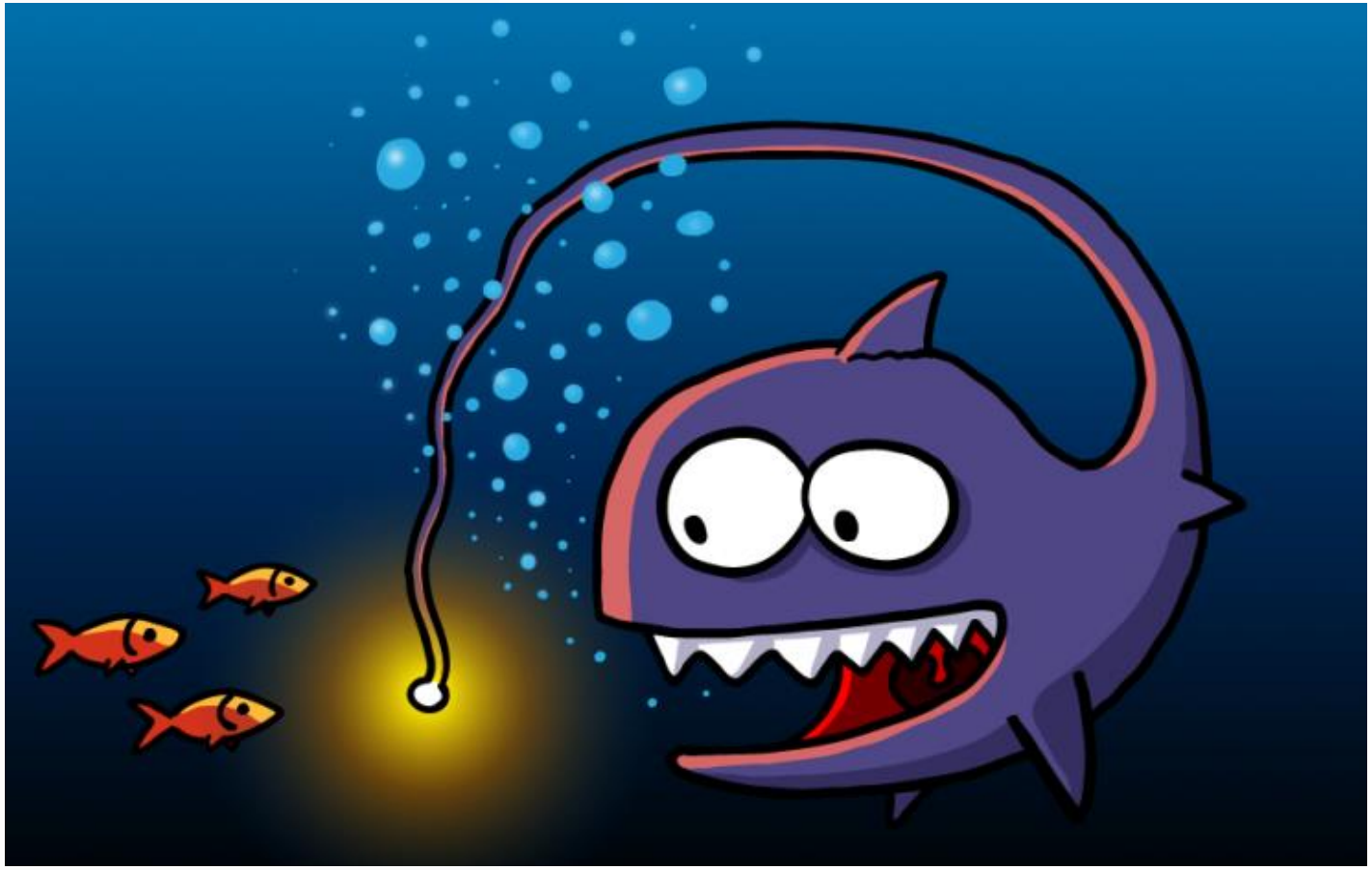


13. PHISHING AND SPEAR PHISHING

PHISHING

PHISHING AND SPEAR PHISHIN

Phishing (ฟิชชิง) ถ้าแผลงมาจากคำว่า "Fishing" ที่แปลว่าการ "ตกปลา" นั่นเองซึ่ง Phishing นั้นมีความหมายถึง การปล่อยให้ปลามากินเหยื่อที่ล่อไว้ เป็นหนึ่งในภัยร้ายบนโลกอินเทอร์เน็ตรูปแบบหนึ่ง ที่มีความอันตรายไม่แพ้การโจมตีจากมัลแวร์เลยแม้แต่น้อย



PHISHING

มารู้จักกับเทคนิค

Phishing

ทั้ง 8 รูปแบบ

1. Email Phishing
(การหลอกลวงแบบฟิชชิง ด้วยการหว่าน หรือปูพรม)

การสังเกต Email Phishing

หากสังเกตจะพบว่าผู้ส่งจะไม่มีระบุข้อมูลที่เป็นลักษณะเฉพาะบุคคล มักจะใช้คำว่า "เรียนเจ้าของบัญชี " หรือ " เรียนสมาชิกผู้มีอุปการคุณ" และบ่อยครั้งจะมีการใช้คำที่สามารถสร้างความหวาดวิตกให้แก่ผู้รับ อย่างเช่น ด่วนที่สุด, ลับเฉพาะ ฯลฯ เพื่อกดดันทางอ้อมให้ผู้ใช้ดาวน์โหลดไฟล์มัลแวร์ หรือกดลิงก์อันตรายที่แนบมากับอีเมล

(การหลอกลวงแบบฟิชชิง)

ตอบกลับ ตอบกลับทั้งหมด ส่งต่อ

Tue 14-May-19 7:39 AM

ธนาคารไทยพาณิชย์ จำกัด (มหาชน) <securityinfo@scb.com>

การแจ้งเตือนความปลอดภัย: บัญชีถูกแฮ็ก

ถึง undisclosed-recipients:

SCB ไทยพาณิชย์

เรียนลูกค้าทุกท่าน

เพื่อให้คุณทราบว่าการเข้าถึง SCB Easy Net ของคุณนั้นถูก จำกัด ชั่วคราวเนื่องจากธนาคารไทยพาณิชย์สงสัยว่าอาจถูกแฮ็ค สิ่งนี้อาจเกิดขึ้นเนื่องจากคุณป้อนรหัสผ่านของคุณในเว็บไซต์หลอกลวงหรือเนื่องจากคอมพิวเตอร์ของคุณติดไวรัส

โปรดยืนยันรายละเอียดการเข้าสู่ระบบของคุณ: https://www.scbeasy.com/secure/srv.asp
รหัสยืนยันจะถูกส่งท่าน SMS ฟรีเพื่อสร้างรหัสผ่านใหม่เมื่อคุณป้อนรายละเอียดที่ถูกต้อง บัญชีของคุณจะถูกปลดล็อคหลังจากเปลี่ยนรหัสผ่าน

นอกจากนี้โปรดตรวจสอบคำถามเพื่อความปลอดภัยข้อมูลส่วนบุคคลและที่อยู่อีเมลของคุณเพราะอาจมีการเปลี่ยนแปลง

เรายินดีที่จะทำงานร่วมกับคุณและรับรองการกู้คืนบัญชีของคุณอย่างเต็มที่และบริการของคุณจะได้รับการคืนค่าอย่างสมบูรณ์

เราขออภัยในความไม่สะดวกที่เกิดขึ้น

ความนับถือ,

SCB Easy Net

(การหลอกลวงแบบฟิชชิง)

B

BualuangiPayAlert <BualuangiPayAlert@bangkokbank.com>

7:30

To: @hotmail.com

Automatic Alert: เปลี่ยนหมายเลขโทรศัพท์มือถือสำหรับบริการบัวหลวงไอเพย์

May 10, 2019, 2:30 am (Thailand time)

ที่รัก @hotmail.com

หมายเลขโทรศัพท์มือถือที่ลงทะเบียนกับบริการบัวหลวงไอเพย์ได้รับการเปลี่ยนแปลงเรียบร้อยแล้ว นี่คือข้อความที่สร้างขึ้นโดยอัตโนมัติ

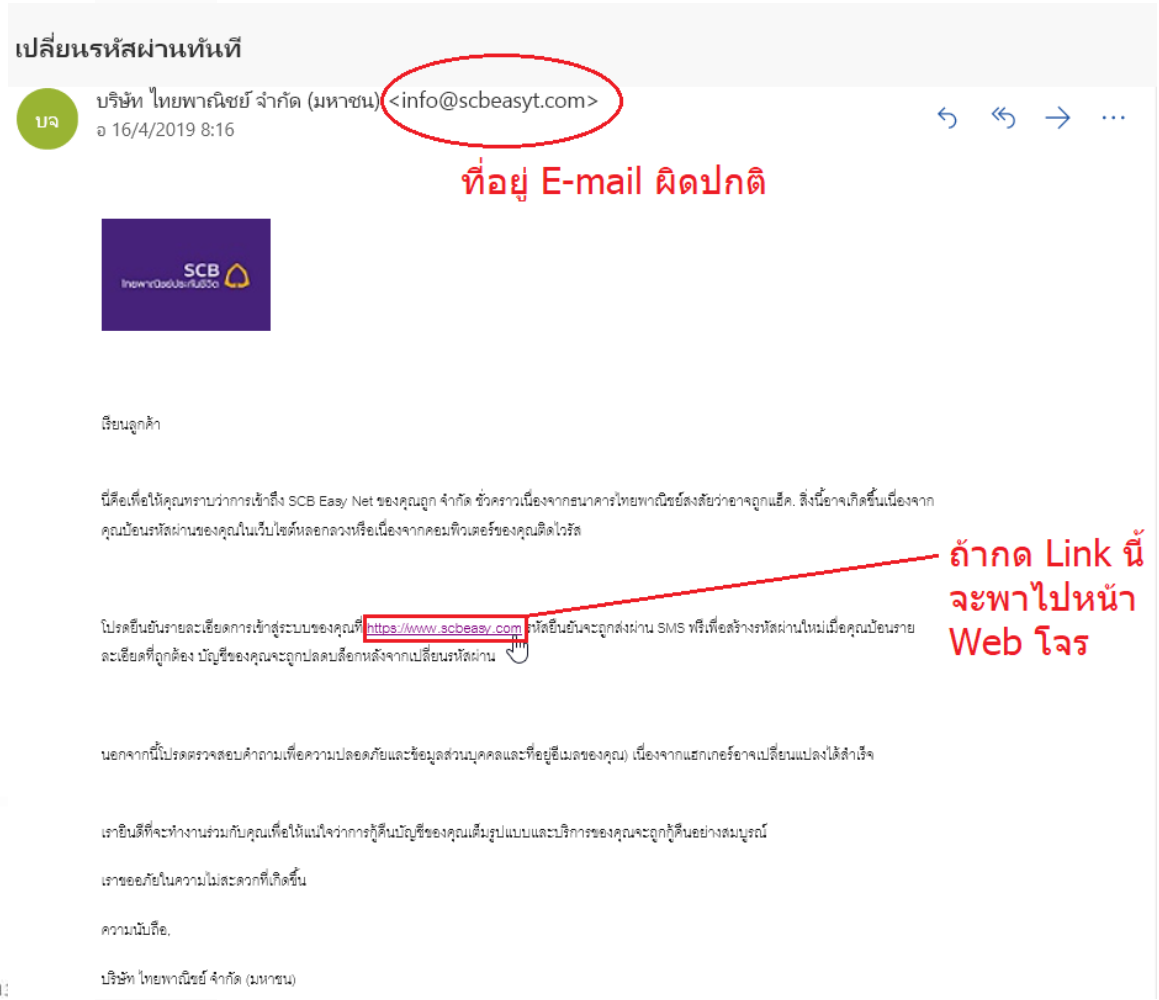
หากคุณไม่ได้เปลี่ยนหมายเลขโทรศัพท์มือถือของคุณโปรดยืนยันบัญชีของคุณและคลิกลิงก์ด้านล่าง

ตรวจสอบบัญชีของคุณ ←อย่าคลิก

ขอแสดงความนับถือ,
Bualuang iPay

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับหลักประกันโปรดไปที่โฮมเพจบัวหลวงไอเพย์ (เข้าสู่หน้า) ที่เว็บไซต์ของธนาคารกรุงเทพ

อีเมลฉบับนี้ไม่ใช่รูปแบบการติดต่อสื่อสารที่ปลอดภัย - โปรดอย่าตอบกลับอีเมลฉบับนี้ หากมีคำถามหรือต้องการความช่วยเหลือกรุณาโทรศัพท์บัวหลวงโฟน 1



เปลี่ยนรหัสผ่านทันที

บจ

บริษัท ไทยพาณิชย์ จำกัด (มหาชน) <info@scbeasyt.com>

อ 16/4/2019 8:16

ที่อยู่ E-mail ผิดปกติ

SCB

เรียนลูกค้า

นี่คือเพื่อให้คุณทราบว่าการเข้าถึง SCB Easy Net ของคุณถูก จำกัด ชั่วคราวเนื่องจากธนาคารไทยพาณิชย์สงสัยว่าอาจถูกแฮ็ค. สิ่งนี้อาจเกิดขึ้นเนื่องจากคุณบ้อนรหัสผ่านของคุณในเว็บไซต์หลอกลวงหรือเนื่องจากคอมพิวเตอร์ของคุณติดไวรัส

โปรดยืนยันรายละเอียดการเข้าสู่ระบบของคุณที่ https://www.scbeasy.com รหัสยืนยันจะถูกส่งผ่าน SMS ฟรีเพื่อสร้างรหัสผ่านใหม่เมื่อคุณป้อนรายละเอียดที่ถูกต้อง บัญชีของคุณจะถูกปลดบล็อกหลังจากเปลี่ยนรหัสผ่าน

ถ้ากด Link นี้ จะพาไปหน้า Web โจร

นอกจากนี้โปรดตรวจสอบคำถามเพื่อความปลอดภัยและข้อมูลส่วนบุคคลและที่อยู่อีเมลของคุณ) เนื่องจากแฮกเกอร์อาจเปลี่ยนแปลงได้สำเร็จ

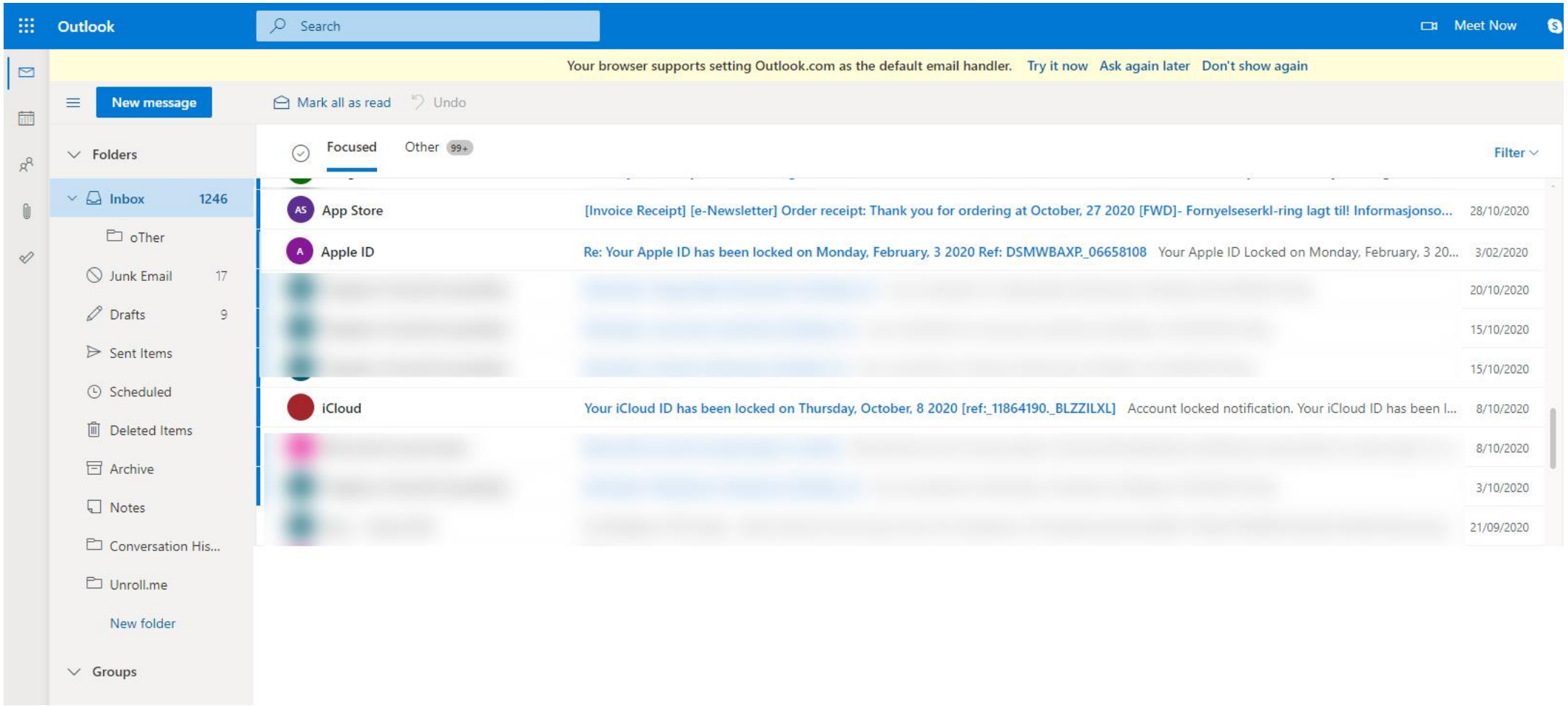
เรายินดีที่จะทำงานร่วมกับคุณเพื่อให้แน่ใจว่าการกู้คืนบัญชีของคุณเต็มรูปแบบและบริการของคุณจะถูกกู้คืนอย่างสมบูรณ์

เราขออภัยในความไม่สะดวกที่เกิดขึ้น

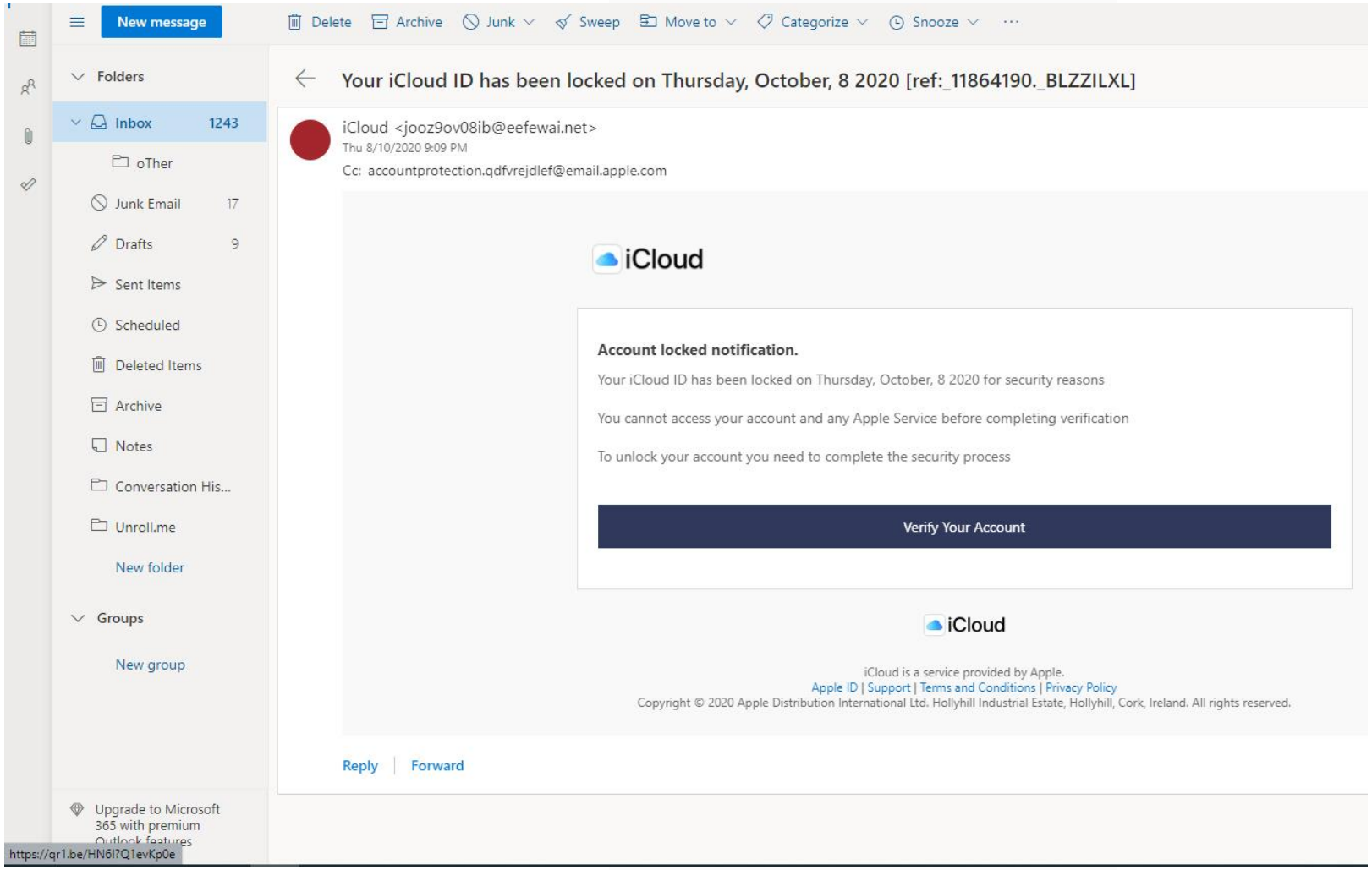
ความนับถือ,

บริษัท ไทยพาณิชย์ จำกัด (มหาชน)

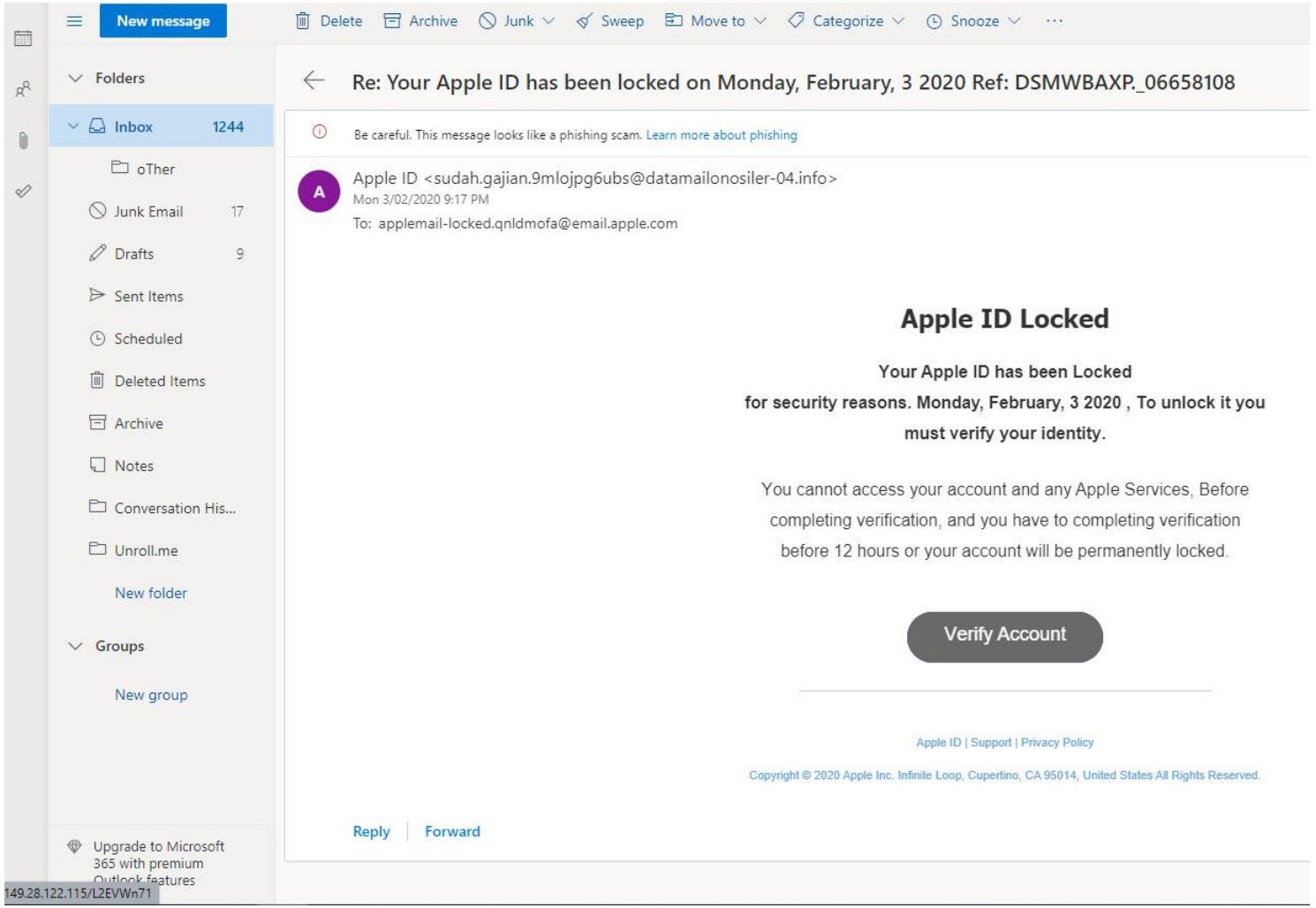
(การหลอกลวงแบบฟิชชิง)



(การหลอกลวงแบบฟิชชิง)



(การหลอกลวงแบบฟิชชิง)



(การหลอกลวงแบบฟิชชิง)

From: Bank of Ayudhya [mailto:updatebofa@optusnet.com.au] ①

To: undisclosed-recipients:

Subject: Bank of Ayudhya :- Account Verification Process ②

ธนาคารกรุงศรีอยุธยา
BANK OF AYUDHYA

Dear Customer,

As part of our commitment to satisfy our customers, we always update annually. To ensure you are always protected, we are introducing a new programmed on security called BankSecure-cfx-08 and you'll see a number of initiatives that will be put in place to enhance your Bank of Ayudhya experience.

Due to this, you are requested to follow the provided steps and confirm your Krungsri Online details for the safety of your accounts.

To initiate the verification process: Kindly Sign In below. ③
https://www.krungsrionline.com/cgi-bin/bvisapi.dll/krungsri_ib/login/login.jsp

เมื่อคลิกแล้ว จะเข้าสู่หน้าเว็บหลอกลวง เช่น
http://acc.stcosme.free.fr/components/com_expose/expose/img/thumbs/login.eng.html

Sincerely,

Copyright 2001 Bank of Ayudhya PCL. All right reserved

2. Spear Phishing
(การหลอกลวงแบบฟิชชิง ที่พุ่งเป้าเจาะจง)

การสังเกต Spear Phishing

หมั่นสังเกตอีเมล และรูปแบบตัวอักษรของผู้ส่งให้ละเอียดว่ามาจากบุคคลที่คุณรู้จัก และเชื่อใจได้จริงๆ ตัวอย่างเช่น เพื่อนคุณใช้อีเมล olay@gmail.com แต่เมลปลอมจากแฮกเกอร์อาจจะใช้ 0lay@gmail.com ส่งมาหา ก่อนที่จะดาวน์โหลดไฟล์ หรือคลิกลิงก์ที่อยู่ในอีเมล

3. Whaling Phishing
(การหลอกลวงแบบฟิชชิง ที่พุ่งเป้าเจาะจงไปที่บุคคลสำคัญ)

การสังเกต Whaling

แฮกเกอร์นิยมส่งลิงก์หน้าเว็บไซต์ปลอม ให้เหยื่อที่หลงเชื่อกรอกข้อมูลส่วนตัวที่สำคัญ อย่างพวก บัญชี และรหัสผ่าน บางครั้งแฮกเกอร์จะแนบไฟล์แฝงมัลแวร์มาพร้อมกับอีเมล แล้วร้องขอให้เหยื่อดาวน์โหลดไฟล์ไปเปิดดู เพื่อติดตั้งมัลแวร์ลงคอมพิวเตอร์

4. Vishing Phishing
(การหลอกลวงแบบฟิชชิง ผ่านทางเสียง หรือการสนทนา)

การสังเกต Vishing

ในการโน้มน้าวให้เหยื่อหลงเชื่อ อาชญากรมักจะเตรียมเทปบันทึกเสียงจากบริการต่างๆ ที่มีอยู่ในท้องถิ่นของเหยื่อมาเปิดให้เหยื่อฟังด้วย เพื่อหลอกให้เหยื่อเชื่อว่าเป็นสายที่โทรมาจากเจ้าของบริการจริงๆ

ในการระวังตัว ผู้เชี่ยวชาญได้เตือนว่าผู้ใช้ไม่ควรเปิดเผยข้อมูลส่วนตัวที่มีความสำคัญผ่านทางโทรศัพท์โดยเด็ดขาด (ซึ่งโดยปกติเจ้าหน้าที่ธนาคารก็จะไม่ขอข้อมูลส่วนตัวอยู่แล้ว) ทางที่ดีให้รีบวางสาย แล้วติดต่อไปยังธนาคารด้วยตนเองทันที

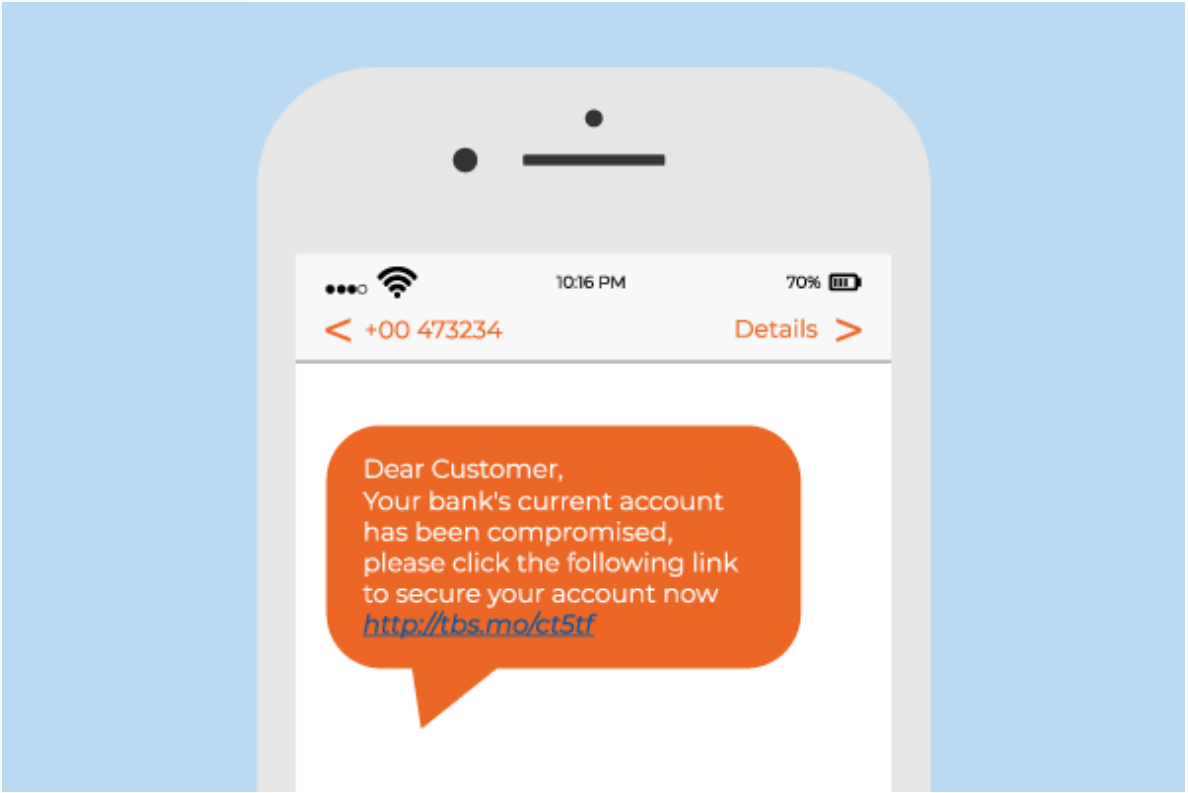
(การหลอกลวงแบบฟิชชิง)

(การหลอกลวงแบบฟิชชิง)

5. Smishing Phishing (การหลอกลวงแบบฟิชชิง ผ่านทางข้อความสั้น SMS)

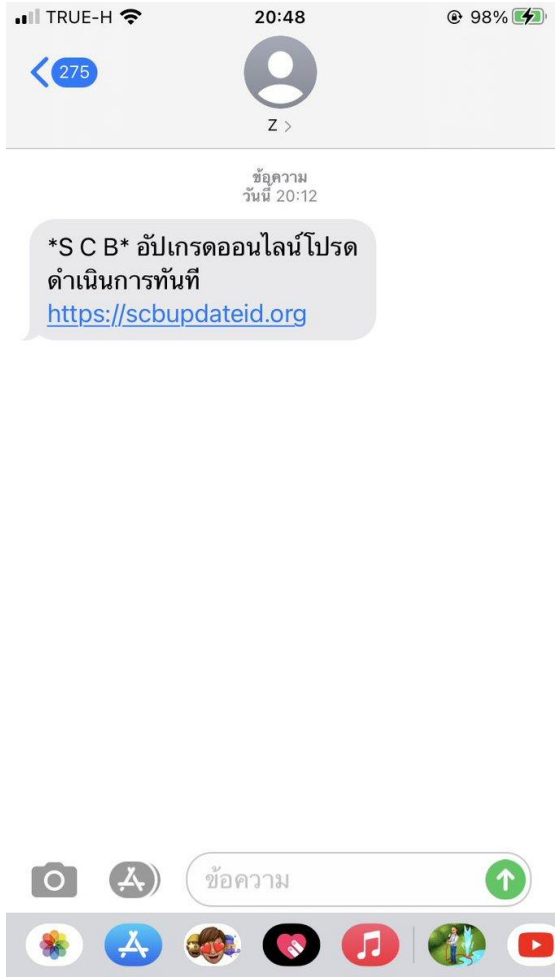
การสังเกต Smishing

เนื้อหาที่ใช้หลอกลวงของ Smishing มักจะเหมือนกับ Vishing แต่โดยส่วนใหญ่จะนิยมอ้างว่าคุณถูกรางวัล แล้วขอให้คุณกรอกข้อมูลเพื่อให้ได้สิทธิ์รับรางวัล สำหรับการป้องกันตัวก็ให้ยึดกฎสามัญ อย่างคลิก หรือตอบข้อความที่ส่งมาจากคนไม่รู้จัก โดยเฉพาะอย่างยิ่งเมื่อมีลิงก์แนบติดมาด้วย



(การหลอกลวงแบบฟิชชิง)

(การหลอกลวงแบบฟิชชิง)



6. Angler Phishing
(การหลอกลวงแบบฟิชชิง ชนิดสังเกตพฤติกรรมทางโซเชียล)

การสังเกต Angler Phishing

หลังจากสนทนากันสักพักแฮกเกอร์ก็จะส่งลิงก์ให้คุณกรอกข้อมูลโดยอ้างว่าเพื่อเป็นการ "ยืนยันตัวตน"

หากคุณหลงเชื่อ ทุกอย่างก็จบ

หากคุณเจอกับเหตุการณ์เช่นนั้น สิ่งที่คุณควรทำ คือ วางสายแล้วรีบติดต่อกับเจ้าหน้าที่ฝ่ายบริการของบริษัท หรือหน่วยงานที่คุณมีปัญหาอยู่ เพื่อตรวจสอบสถานการณ์จริงที่เกิดขึ้น

7. CEO Fraud Phishing
(การหลอกลวงแบบฟิชชิง ที่ใช้บุคคลสำคัญเป็นตัวล่อ)

การสังเกต CEO Fraud Phishing

แฮกเกอร์มักจะพุ่งเปาโจมตีไปยังคนที่มีอำนาจในการโอนเงิน หรือผู้ที่ครอบครองข้อมูลสำคัญ บ่อยครั้งที่ข้อความในอีเมลจะระบุว่าเป็นเรื่องด่วนที่ต้องดำเนินการในทันที เพื่อให้เหยื่อไม่มีเวลาคิด หรือตรวจสอบว่ามันเป็นเรื่องจริงหรือไม่

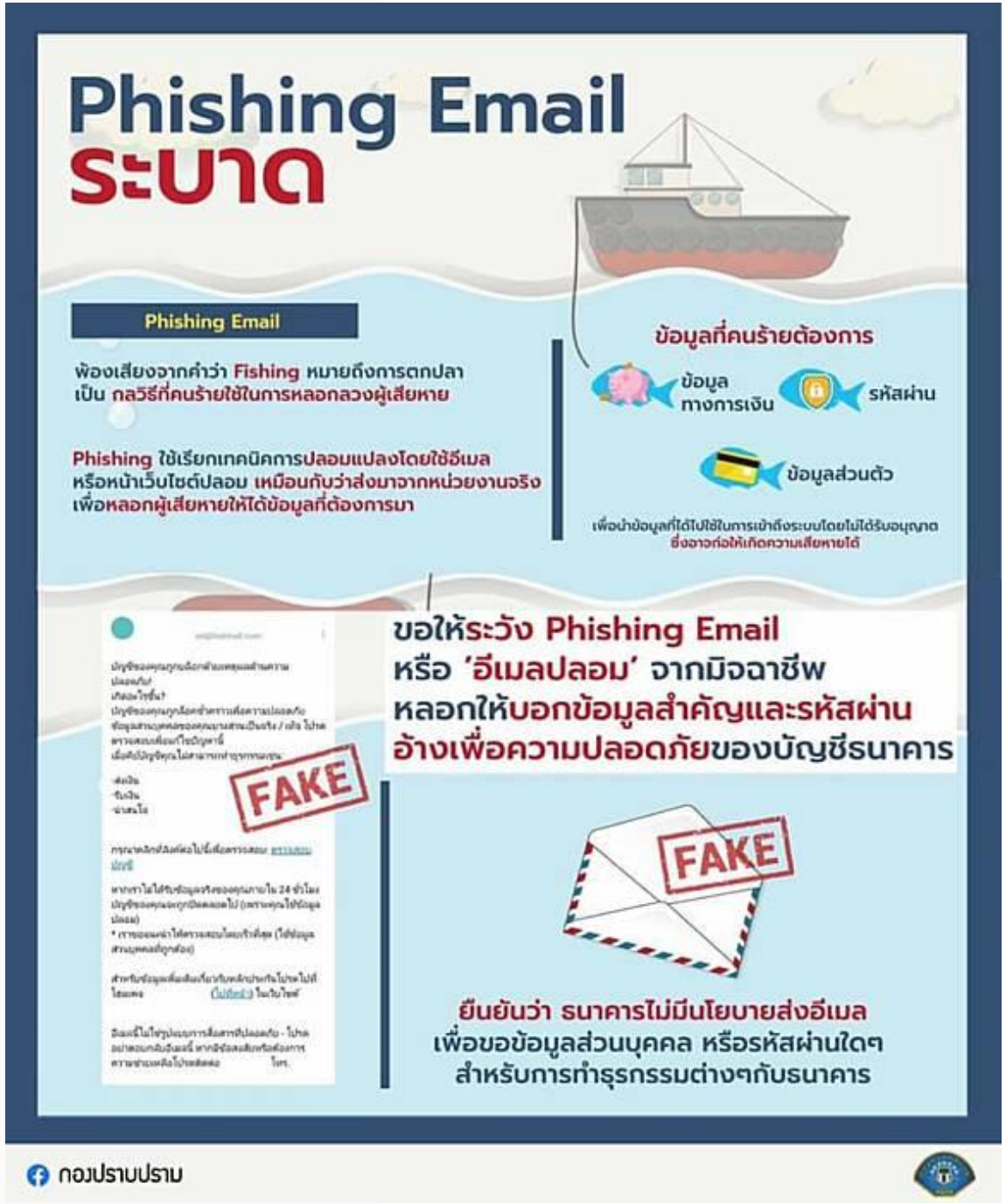
8. Search Engine Phishing
(การหลอกลวงแบบฟิชชิง ที่สร้างความน่าเชื่อถือจาก เครื่องมือค้นหา)

การสังเกต Search Engine Phishing

เมื่อเราค้นหาอะไรก็ตาม พึงระลึกไว้ว่าผลลัพธ์ที่แสดงอยู่อาจจะมีเว็บไซต์ปลอมถูกแสดงผลขึ้นมาด้วยก็ได้ ในเว็บเหล่านั้นมักจะมีข้อเสนอที่คุณกำลังมองหาอยู่ แต่ก่อนจะได้มา มันจะขอให้คุณกรอกข้อมูลส่วนตัวก่อน ซึ่งเว็บไซต์ที่ดีมักไม่ทำแบบนั้น เราไม่ควรหลงเชื่อกรอกข้อมูลให้ไป จนกว่าจะมั่นใจว่าเว็บไซต์นั้นมีการดำเนินการที่โปร่งใส

ตัวอย่างการแจ้งเตือน

(การหลอกลวงแบบฟิชชิง)



(การหลอกลวงแบบฟิชชิง)

Bangkok Bank
ธนาคารกรุงเทพ

แจ้งเตือน SMS และอีเมล หลอกลวง

ธนาคารไม่มีนโยบายส่ง SMS หรืออีเมล เพื่อให้ท่านกดลิงก์ เพื่อดาวน์โหลด หรือติดตั้งโปรแกรมใดๆ ลงบนสมาร์ทโฟน แท็บเล็ต หรือคอมพิวเตอร์ รวมทั้งการกรอกข้อมูลส่วนตัวของท่านแต่อย่างใด

ธนาคารขอแนะนำให้ท่านโปรดระวัง
โดยอย่ากดลิงก์และให้ข้อมูลใดๆ
เนื่องจากโปรแกรมไม่พึงประสงค์จะสามารถขโมยข้อมูลส่วนตัว หรือลักลอบโอนเงินออกจากบัญชีของท่านได้

(การหลอกลวงแบบฟิชชิง)

รับมืออย่างไรเมื่อโดนหลอก

(การหลอกลวงแบบฟิชชิง)

14. RANSOMWARE

RANSOMWARE

RANSOMWARE

Ransomware เป็นมัลแวร์ (Malware) ประเภทหนึ่ง ที่มีลักษณะการทำงานที่แตกต่างกับมัลแวร์ประเภทอื่น ๆ คือไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของผู้ใช้งานแต่อย่างใด แต่จะทำการเข้ารหัสหรือล็อกไฟล์ ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใด ๆ ได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” ที่ปรากฏ

RANSOMWARE

RANSOMWARE

RANSOMWARE

RANSOMWARE

RANSOMWARE

ต้นกำเนิด Ransomware มัลแวร์เรียกค่าไถ่

ช่วงปีปลายทศวรรษ 1980 PC Cyborg : หรือที่เรารู้จักกันดีในนาม AIDS Trojan

ปี 2004 GpCode

ปี 2007 WinLock

ปี 2012 Reveton

ปี 2013 Crypto Locker

ปี 2016 Locky

ปี 2017 WannaCry

ปี 2019 Sodinokibi

RANSOMWARE

RANSOMWARE

RANSOMWARE

Ransomware มีกี่ประเภท ?

Crypto malware

Lockers

Scareware

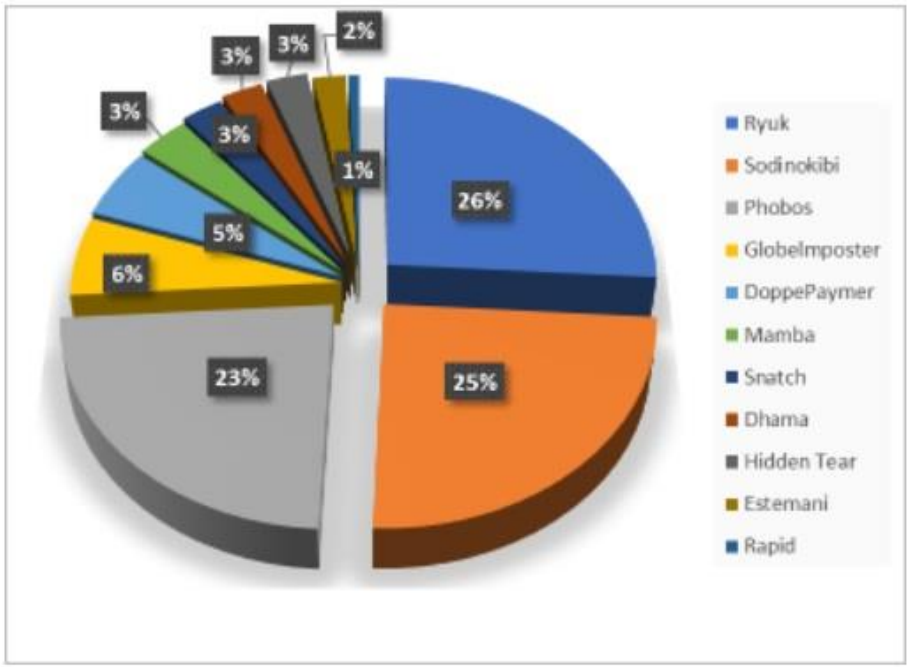
Doxware

RaaS

Mac ransomware

Ransomware บนมือถือ

ประเภทของมัลแวร์เรียกค่าไถ่



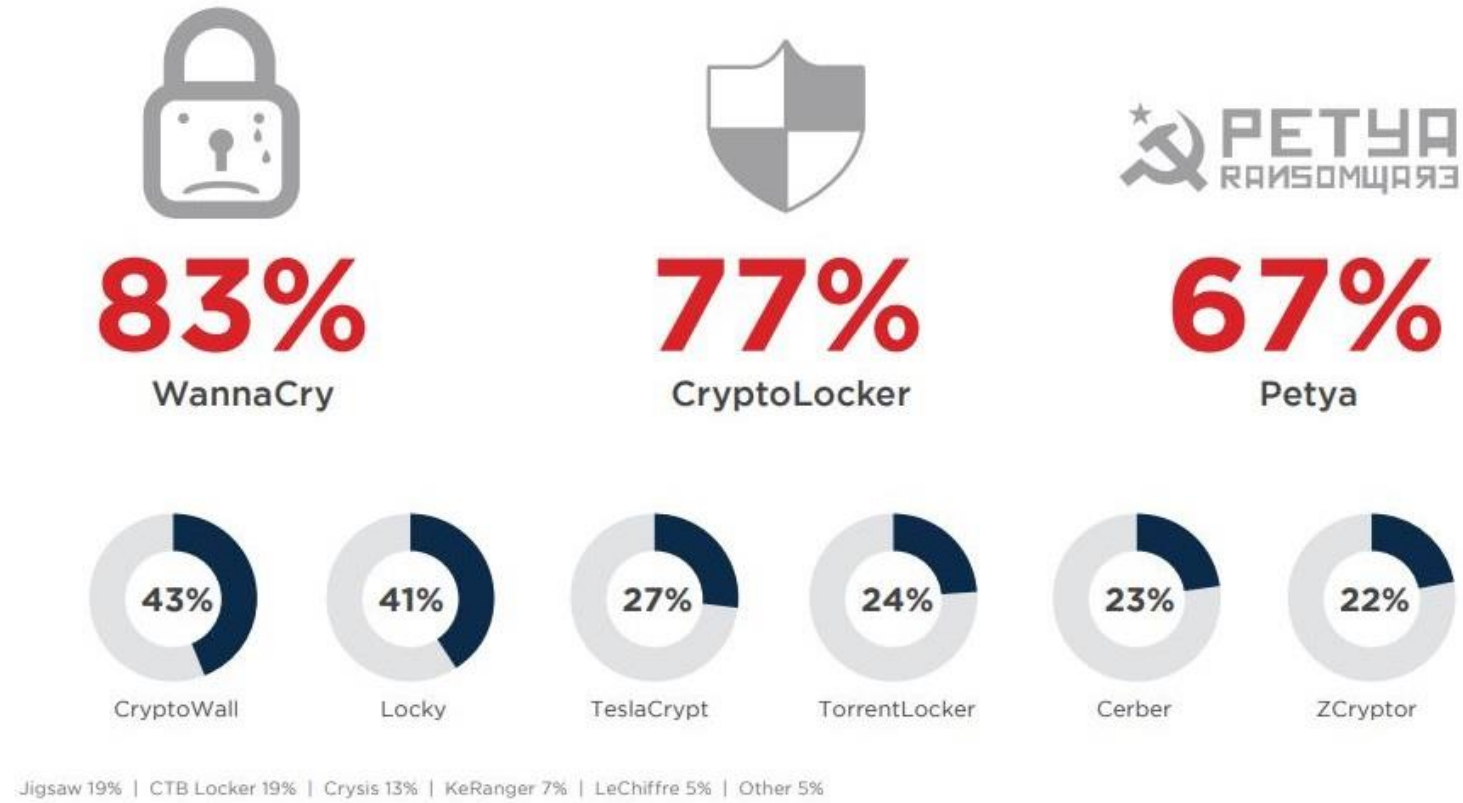
มัลแวร์เรียกค่าไถ่ หลักๆ แล้วมี 2 ประเภท คือ: มัลแวร์เรียกค่าไถ่แบบ Locker ซึ่งล็อคคอมพิวเตอร์ หรืออุปกรณ์ และมัลแวร์เรียกค่าไถ่แบบ Crypto ซึ่งจะทำการเข้ารหัส เพื่อป้องกันการเข้าถึงไฟล์ หรือข้อมูล โดยมักทำผ่านการเข้ารหัสเป็นหลัก

จากข้อมูลของกราฟทางด้านซ้ายมือ คุณสามารถดูประเภทของมัลแวร์เรียกค่าไถ่ล่าสุด โดยแบ่งตามชื่อและระดับของการโจมตี

- RYUK
- Sodinokibi
- Phobos
- GlobeImposter
- DoppelPaymer
- Mamba
- Snatch
- Dharma
- HiddenTear
- Estemani
- Rapid

RANSOMWARE

มัลแวร์เรียกค่าไถ่ที่ส่งผลกระทบมากที่สุด



CryptoLocker 2013

CryptoWall 2014

CTB-Locker 2014

TorrentLocker 2014

Bitcryptor and CoinVault 2015

TeslaCrypt 2015

Locky 2017

WannaCry 2017

WannaCry ได้แพร่กระจายไปยังคอมพิวเตอร์มากกว่า 100,000 เครื่อง ในเดือนพฤษภาคม 2017 ด้วยการใช้ประโยชน์จากช่องโหว่ของ Microsoft Windows ที่ออกมา (MS17-010)

WannaCry (หรือ WannaCrypt, WanaCrypt0r 2.0, Wanna Decryptor) จะทำการเข้ารหัสไฟล์ของคุณ และเก็บไว้เพื่อเรียกค่าไถ่ เป็นเวลาหลายวัน โดยเงินค่าไถ่จะอยู่ที่ประมาณ 0.17 BTC (ประมาณ 300 เหรียญสหรัฐ) ซึ่งเงินค่าไถ่จะเพิ่มขึ้นตามระยะเวลาที่ปล่อยเอาไว้ หลังจากนั้นหนึ่งสัปดาห์ไฟล์ที่ถูกเข้ารหัสจะถูกลบ ไฟล์ที่เข้ารหัสจะมีนามสกุล WCRY พบว่ามัลแวร์ได้อธิบาย "kill switch functionality" นอกจากนี้ยังมี Wannacry รุ่นใหม่กว่า ที่สามารถเห็นได้ทั่วไปในวันอาทิตย์ พร้อมโดเมน kill switch แบบใหม่

GandCrab 2018

RANSOMWARE

RANSOMWARE

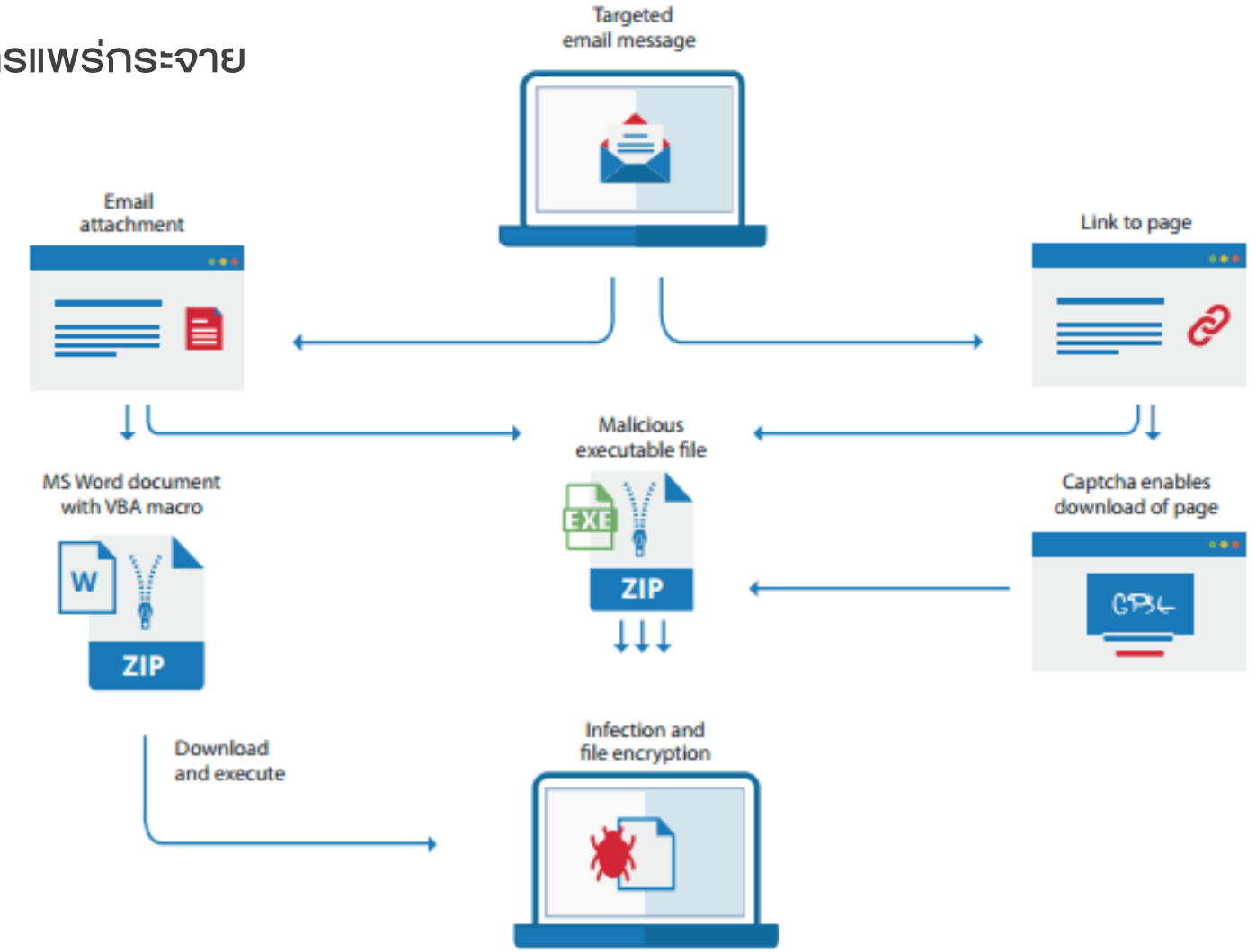
RANSOMWARE

คุณกำลังตกเป็นเปาหมาย Ransomware อยู่หรือเปล่า ?

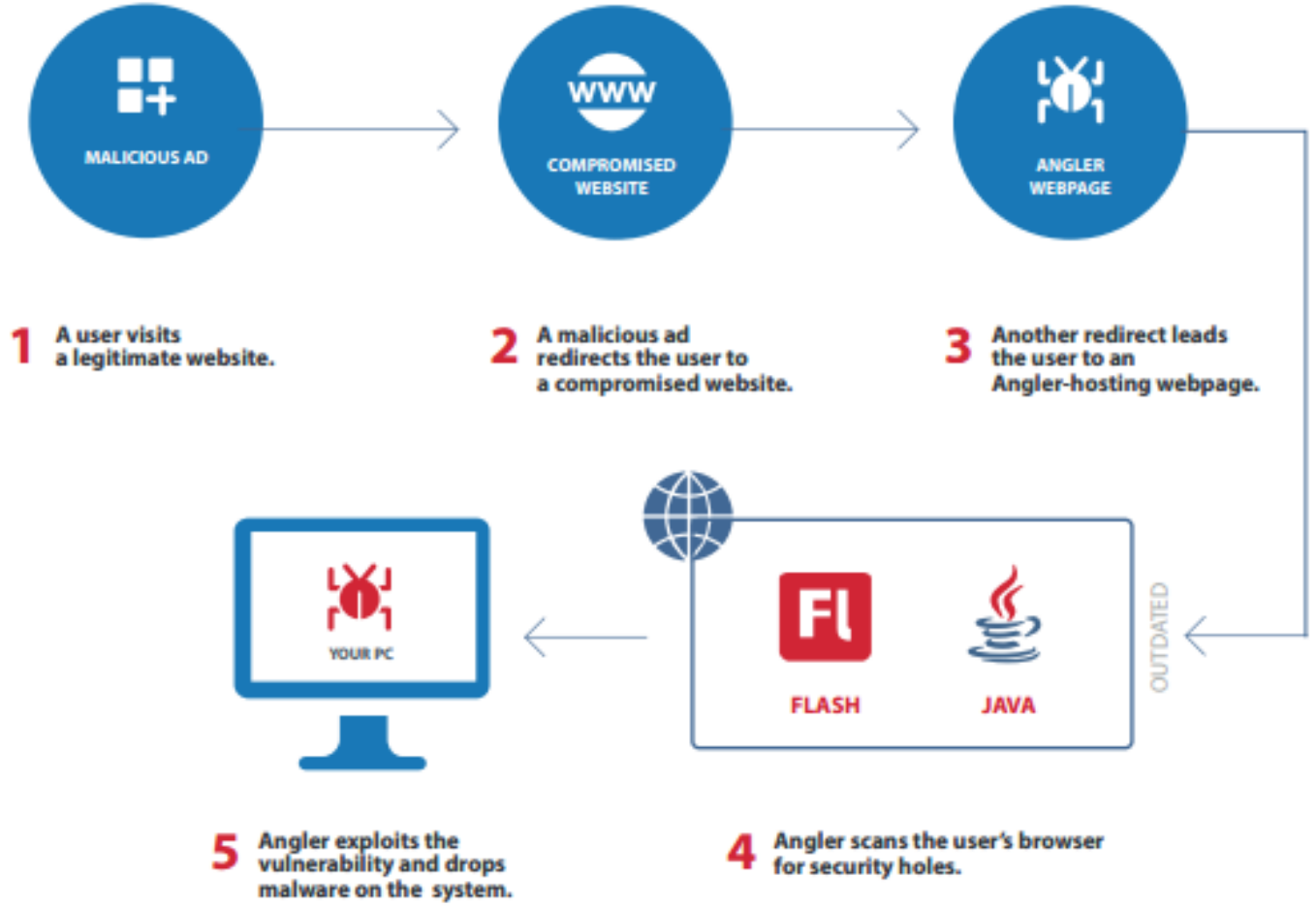
- กลุ่มคน ธุรกิจ หรือองค์กรที่ไม่มี หรือมีระบบรักษาความปลอดภัยทางไซเบอร์ขนาดเล็ก
- ธุรกิจ หรือองค์กรต่าง ๆ ที่มีโอกาสในการจ่ายเงินสูง
- ธุรกิจหรือองค์กรที่ถือข้อมูลสำคัญ

RANSOMWARE

ช่องทางการแพร่กระจาย



RANSOMWARE


MALICIOUS AD
COMPROMISED WEBSITE
ANGLER WEBPAGE
1 A user visits a legitimate website.
2 A malicious ad redirects the user to a compromised website.
3 Another redirect leads the user to an Angler-hosting webpage.
YOUR PC
FLASH
JAVA
OUTDATED
5 Angler exploits the vulnerability and drops malware on the system.
4 Angler scans the user's browser for security holes.

RANSOMWARE

วิธีป้องกันการติดมัลแวร์เรียกค่าไถ่

มัลแวร์เรียกค่าไถ่นั้นมีความร้ายกาจเป็นอย่างยิ่ง แม้ว่ามันแพร่กระจายผ่านทางผ่านอีเมล แต่ก็เป็นที่ทราบกันดีตัวของมันเอง ยังใช้ประโยชน์จากแบ็คดอร์หรือช่องโหว่ของระบบ นอกจากนี้เรายังได้เผยแพร่บทความเกี่ยวกับวิธีการใช้การรักษาความปลอดภัยไซเบอร์ สำหรับ**บริษัทที่มีขนาดเล็กไปจนถึงขนาดกลาง**

มัลแวร์เรียกค่าไถ่ลักลอบเข้าไปยังองค์กรของคุณได้อย่างไร?

สถิติข้างต้นแสดงให้เห็นถึงวิธีที่เป็นที่นิยมที่สุดในการแพร่กระจายเข้าไปยังระบบขององค์กรของคุณ
อ่านต่อเพื่อเรียนรู้วิธีที่คุณสามารถหลีกเลี่ยงการโจมตีสำหรับมัลแวร์เรียกค่าไถ่

RANSOMWARE

RANSOMWARE

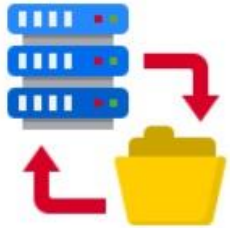
RANSOMWARE

1. ทำการแยก/ปิดเครือข่าย และระบบต่าง ๆ

ขั้นตอนแรกในการจัดการการระบาดของมัลแวร์เรียกค่าไถ่ คือการแยกระบบที่ติดมัลแวร์ออกจากส่วนที่เหลือของเครือข่าย ปิดระบบเหล่านั้น และดึงสายเคเบิลเครือข่ายออก ปิด WiFi ของระบบที่ติดมัลแวร์ โดยระบบดังกล่าวจะต้องถูกแยกออกจากคอมพิวเตอร์เครื่องอื่น และอุปกรณ์เก็บข้อมูลบนเครือข่ายอย่างสมบูรณ์

2. ระบุประเภทและกำจัดมัลแวร์เรียกค่าไถ่

จากนั้นให้ตรวจสอบว่ามัลแวร์ประเภทใดที่ติดเครื่องคอมพิวเตอร์ของคุณ ทีมรับมือเหตุการณ์องค์กรด้านไอที หรือที่ปรึกษาภายนอกนั้น จะสามารถกำหนดค่าของมัลแวร์เรียกค่าไถ่ และเริ่มวางแผนสำหรับวิธีที่ดีที่สุดในการจัดการกับการติดมัลแวร์ดังกล่าว



3. ล้างเครื่องที่ติดมัลแวร์ และกู้คืนจากข้อมูลสำรอง

เพื่อให้แน่ใจว่าไม่มีเศษซากของมัลแวร์เหลืออยู่ในระบบของคุณ เราขอแนะนำให้ทำการลบข้อมูลทั้งหมด แล้วเรียกคืนข้อมูลทุกอย่างจากการสำรองข้อมูลที่ปลอดภัย โดยสมมติว่ามีการสำรองข้อมูลที่ดี

4. การวิเคราะห์และติดตามการตรวจสอบภายหลัง

การเรียนรู้จากความผิดพลาด เป็นหนึ่งในวิธีที่ดีในการทำความเข้าใจกายวิภาคของการโจมตี และป้องกันการโจมตีที่คล้ายกันไม่ให้เกิดขึ้นอีกครั้ง

RANSOMWARE


7 วิธี ปลอดภัยจาก
“ RANSOMWARE ”
ฉบับเริ่มต้นได้ด้วยตัวเอง
openlandscape

RANSOMWARE

7 วิธีรับมือ และป้องกัน Ransomware ในปี 2021

1.อัปเดตระบบปฏิบัติการ (Operating System) และโปรแกรมอื่น ๆ บ่อย ๆ

2.ติดตั้งโปรแกรมแอนตี้ไวรัสที่มีการป้องกันแรนซัมแวร์

3.ไม่คลิกลิงก์แปลก ๆ หรือดาวน์โหลดไฟล์ที่ไม่มีแหล่งที่มา

ปลอดภัยมากขึ้นด้วยการสำรองข้อมูลแบบ Backup

5. ป้องกันไฟล์สำคัญด้วย Read-Only

6. ปิดการเข้าถึงข้อมูลจากระยะไกล RDP

7.ให้ Snapshot ทุกครั้งไม่มีพลาด

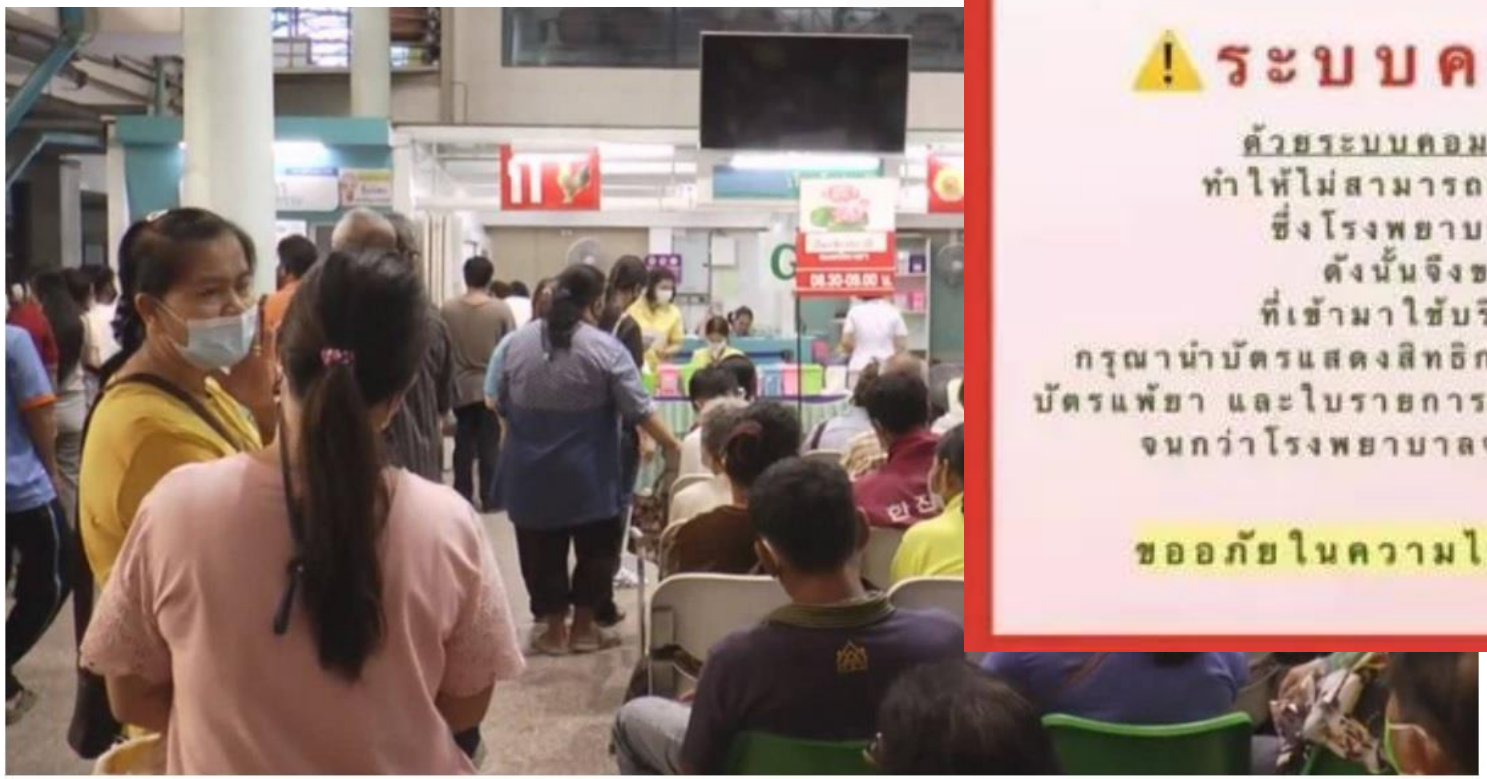
RANSOMWARE

วิธีป้องกัน Ransomware

- ทำการสำรองข้อมูล (Backup)
- อัปเดตซอฟต์แวร์ในเครื่องอย่างสม่ำเสมอ
- ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware)
- ตรวจสอบอีเมลที่เป็นอันตรายเบื้องต้น

ตัวอย่างบริษัท หรือ หน่วยงาน ในที่โดน RANSOMWARE

RANSOMWARE



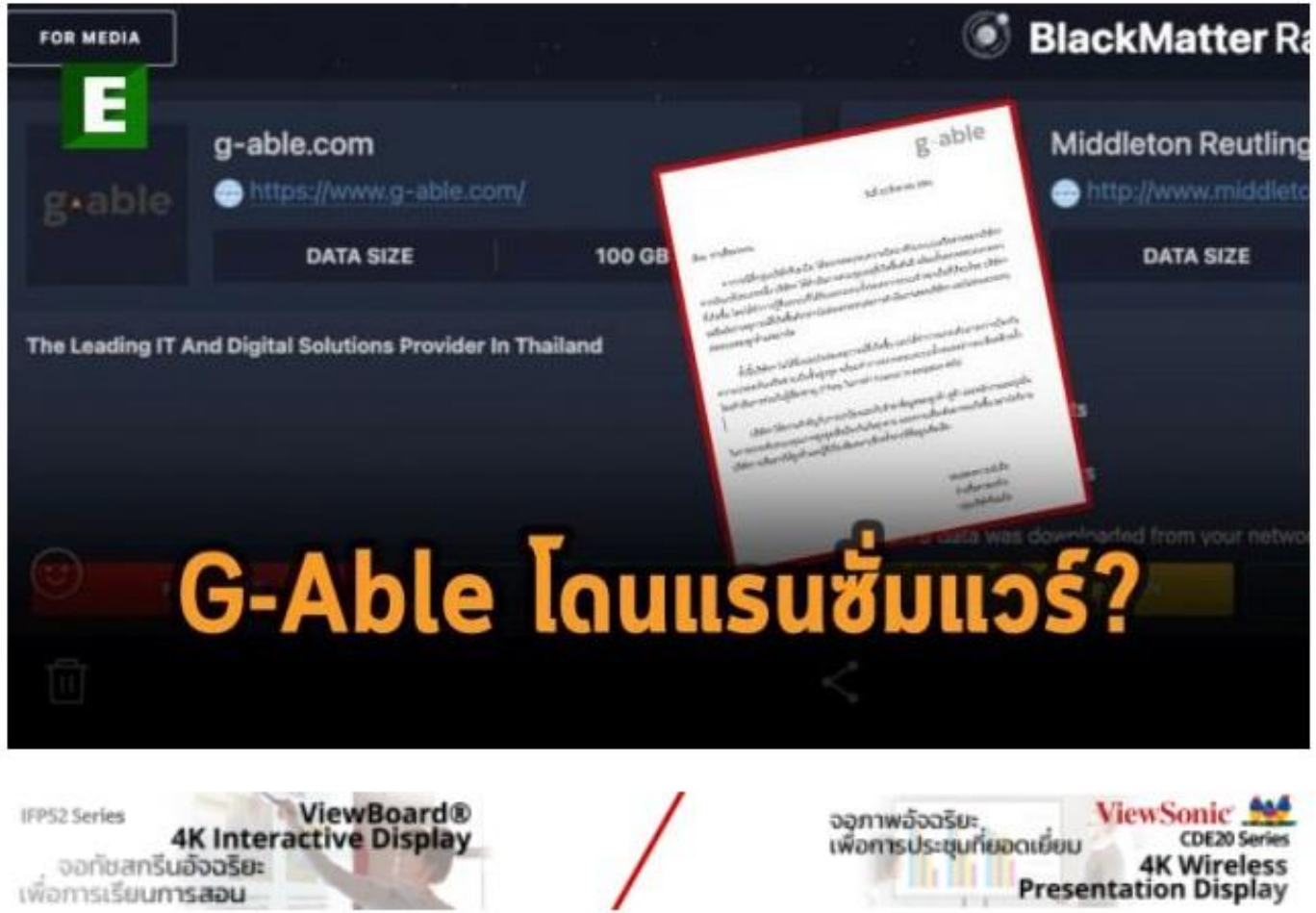
รพ.สระบุรีโดนมัลแวร์เรียกค่าไถ่ ระบบคอมฯ พัง ต้องซักประวัติใหม่ทำล่าช้า

RANSOMWARE

17 พฤษภาคม 2021 NT cyfence IT 360° โอกี ง่ายๆ รอบๆ ตัว

บริษัทประกันภัยรายใหญ่ในเอเชีย AXA ถูก Ransomware โจมตีจากกลุ่มแฮกเกอร์ Avaddon และยึดไฟล์สำคัญต่าง ๆ เช่น บัตรประชาชน ข้อมูลสุขภาพ รายงานการรักษา รวมไปถึงผลการพิจารณาการเบิกค่ารักษา จำนวนกว่า 3 TB เหตุดังกล่าวอาจกระทบต่อบริษัท AXA สาขาในประเทศไทย มาเลเซีย ฮ่องกงและฟิลิปปินส์

RANSOMWARE



วันนี้ (25 ส.ค. 2564) เราได้รับทราบข่าวเกี่ยวกับการที่บริษัท G-Able ซึ่งเป็นบริษัทด้านไอทีรายใหญ่ของเมืองไทย โดยมีแหล่งข่าวได้ส่งข้อมูลเกี่ยวกับการที่ G-Able โดนโจมตีจาก Ransomware จากกลุ่ม BlackMatter มาให้ที่กองบรรณาธิการ ให้ตรวจสอบ ซึ่งพบว่ามีข้อมูลจำนวนมากที่โดนโจมตีและถูกปล่อยออกให้ดาวน์โหลดทาง Internet กว่า 100 GB

RANSOMWARE

บริษัทประกันภัยรายใหญ่ในประเทศ ถูกโจมตีด้วย Ransomware - NT ...

บริษัทประกันภัยรายใหญ่ในเอเชีย AXA ถูกโจมตี **Ransomware** จากกลุ่มแฮกเกอร์ Avaddon โดยมีข้อมูลที่อาจกระทบต่อผู้ใช้บริการในประเทศไทยด้วย.

https://marketeeronline.co › archives · Translate this page

ป่วนไม่เลิก! แฮกเกอร์คุกคามหนักข้อ แบรนด์ใหญ่ทั่วโลกอ่วม

Feb 3, 2565 BE — ทว่ากลุ่มแฮกเกอร์ที่สหรัฐฯ คาดว่ามีฐานอยู่ในรัสเซีย ยังคงเหิมเกริม โจมตีบริษัทใหญ่ในธุรกิจอื่น ๆ อีกหลายครั้ง ทั้งยิง**Ransomware**ใส่ระบบ IT ...

https://marketeeronline.co › archives · Translate this page

โลกยุค Super Connect เสียหายมหาศาลจากภัย Ransomware

Oct 5, 2564 BE — Colonial Pipeline เป็นเหยื่อรายล่าสุดของ **Ransomware** ซึ่งเฉพาะปี 2020 ก็สร้างความเสียหายให้บริษัทใหญ่ ๆ มหาศาล ขณะที่หน่วยงานรัฐก็โดนโจมตีเช่นกัน ...

https://www.techhub.in.th › hacker-r... · Translate this page

โดนจัดหนัก แฮกเกอร์ปล่อย Ransomware เรียกค่าไถ่ โจมตีบริษัท ...

Jul 7, 2564 BE — เมื่อช่วงสุดสัปดาห์ที่ผ่านมา พบบริษัทด้านไอทีนับ 1000 แห่ง ถูก **Ransomware** หรือมัลแวร์เรียกค่าไถ่โจมตีกันทั่วหน้า.

https://www.thairath.co.th › tech · Translate this page

Nvidia ออกแถลงการณ์ยอมรับถูกแฮกเกอร์ขโมยข้อมูล หลังถูกโจมตี ...

Mar 2, 2565 BE — นอกจากนั้น พวกเขามีความพยายามที่จะโจมตีบริษัทสื่อชื่อดังของโปรตุเกสอย่าง Impresa และบริษัทโทรคมนาคม Claro และ Embratel ...

https://www.beartai.com › itnews · Translate this page

บริษัท GIGABYTE ถูกกลุ่ม RansomExx โจมตีด้วย ransomware ...

Aug 7, 2564 BE — ล่าสุด GIGABYTE ซึ่งเป็นที่รู้จักในด้านบริษัทผู้ผลิตฮาร์ดแวร์คอมพิวเตอร์ เช่น แล็บท็อป หน้าจอ การ์ดจอ หรือเมนบอร์ด ได้ให้สัมภาษณ์กับสำนักข่าว ...

https://droidsans.com › axa-asia-divis... · Translate this page

บริษัทเครือ AXA ในไทย โดน Ransomware ขโมยข้อมูลลูกค้าไปกว่า ...

May 17, 2564 BE — ย้อนกลับไปเมื่อวันที่ 9 พฤษภาคมที่ผ่านมา ทาง AXA ได้ออกมาเปลี่ยนนโยบาย ระบุว่า พวกเขาจะยุติการจ่ายค่าประกันที่เกี่ยวกับ **Ransomware** ทุกกรณี โดย ...

Thank you

QUESTIONS?

Game

1. Computer Worm คืออะไร

2. AXA โดน hacker กลุ่มไหน โจมตี และเป็น Malware อะไร

3. Malware คืออะไร

4. CRACKER คืออะไร

5. กฎหมายที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ มีอะไรบ้าง