คู่มือ

การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่

สำนักดิจิทัลเพื่อการศึกษา

CONTENTS

1. ระบบรักษาความปลอดภัยภาพรวมของมหาวิทยาลัยราชภัฏเชียงใหม่
   - เกี่ยวกับ Ransomware
   - Operating System ที่ Ransomware เลือกในการโจมตี
   - วิธีการโจมตีหลัก ๆ ของ Ransomware
   - เมื่อถูก Ransomware โจมตีแล้วจะเป็นอย่างไร ?
   - อาการที่บ่งบอกว่าเครื่องของคุณอาจจะติด Ransomware
   - ช่องทางการโจมตีของ Ransomware
   - กลุ่มเป้าหมายในการโจมตี
   - ถ้าติด Ransomware แล้วต้องทำอย่างไร ?
   - วิธีรับมือกับ Ransomware
2. ภัยคุกคามทางคอมพิวเตอร์ในปัจจุบันที่ควรระวัง
3. กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์
4. แนวปฏิบัติและแนวทางการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์

ระบบรักษาความปลอดภัยภาพรวมของมหาวิทยาลัยราชภัฏเชียงใหม่

Ransomware คืออะไร ?

Ransomware จัดว่าเป็น Malware ประเภทหนึ่งที่มีลักษณะการทำงานที่แตกต่างกับ Malware ประเภทอื่น ๆ คือไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของผู้ใช้งานแต่อย่างใด แต่จะทำการเข้ารหัส หรือล็อกไฟล์ทุกประเภท ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใด ๆ ได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” ที่ปรากฏ ส่วนมากจะต้องชำระด้วย Bitcoin แต่อย่างไรก็ตามการชำระเงินก็ไม่ได้หมายความว่าผู้ไม่หวังดีจะส่งคีย์ที่ใช้ในการปลดล็อคไฟล์ให้กับผู้ใช้งานเมื่อชำระแล้วจะได้รับ Key สำหรับการถอดรหัสไฟล์ ซึ่งก็ไม่สามารถการันตีได้ว่าจะกู้ได้จริงหรือไม่

วิธีการโจมตีหลัก ๆ ของ Ransomeware

- แฮกเกอร์ส่ง Spam Mail
- จาก Flash Drive ที่มี Malware
- จาก Website ที่เป็นอันตราย

→ ผ่านตัวกรอง Spam เข้ามาใน Inbox ของผู้ใช้คอมพิวเตอร์ → ผู้ใช้กดลิ้งค์ในเมลล์ที่แฮกเกอร์ส่งมา

แอนตี้ไวรัสตรวจจับไม่เจอไฟล์ Malware ฝังตัวลงในเครื่องของผู้ใช้

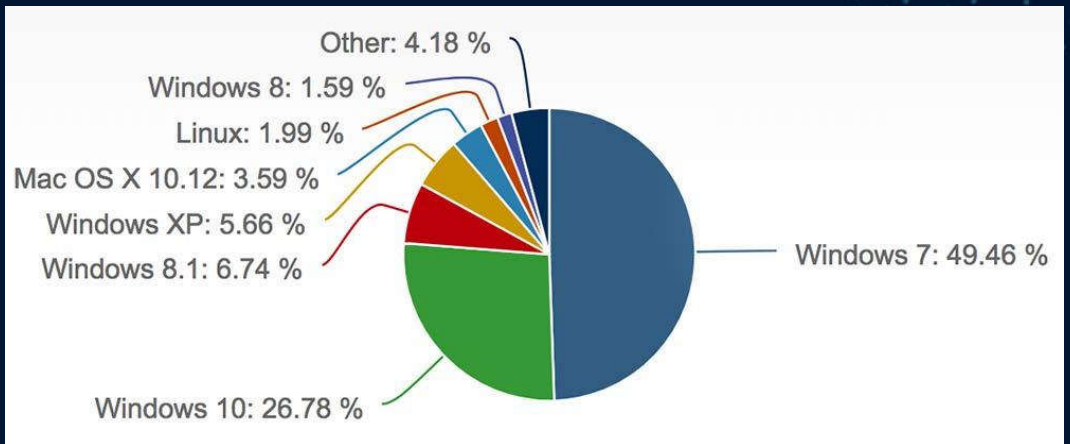
เข้ารหัสไฟล์ในเครื่องของผู้ใช้ หรือเข้าไปยังเซิฟเวอร์ส่วนกลางขององค์กร เพื่อเข้ารหัสข้อมูลสำคัญในเซิฟเวอร์

แฝงตัวเข้าไปยังคอมพิวเตอร์เครื่องอื่นๆ ที่มีการเชื่อมต่อกับเซิฟเวอร์ส่วนกลางขององค์กร

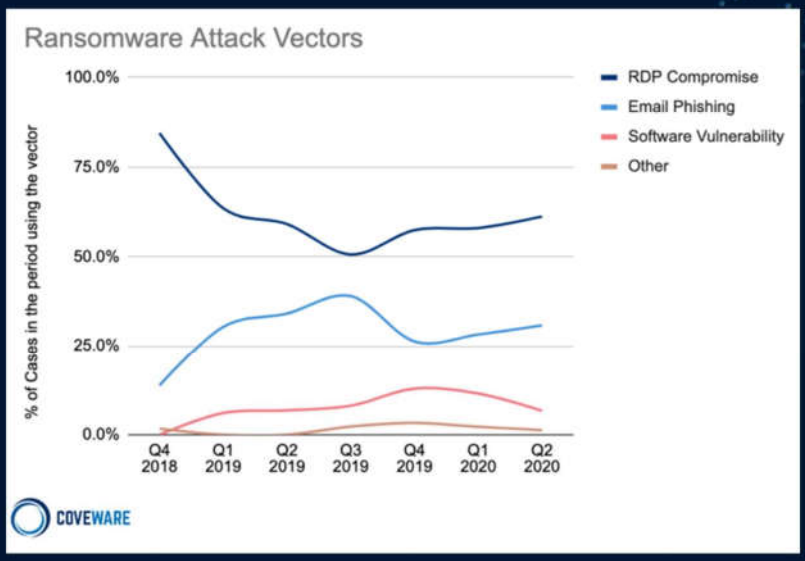
ส่งแจ้งเตือนเรียกค่าไถ่

แม้จะมีการจ่ายค่าไถ่ แต่ไฟล์ Malware ยังสามารถทิ้งซากไฟล์ที่ตรวจจับได้ยากไว้ในเครื่องหรือเซิฟเวอร์ เพื่อรอวันถูกกระตุ้นให้กลับมาทำงานอีกครั้ง

Operating System ที่ Ransomware เลือกโจมตี



การโจมตีผ่าน Service ต่าง ๆ



ตัวอย่าง Windows ขึ้นหน้าจอ Lock Screen

เมื่อ Ransomware เข้ารหัสไฟล์ของเครื่องเป้าหมายเป็นที่เรียบร้อยแล้วจะสร้างหน้าจอขึ้นมาเพื่อแจ้งรายละเอียดต่าง ๆ ตามที่ต้องการ บางกรณีจะไม่สามารถปิดหน้าจอนี้ได้เลย เนื่องจากถูกฝังลงไปใน Startup และแก้ไขค่า Registry ของ Windows ไปเป็นที่เรียบร้อยแล้ว

ตัวอย่าง Android Phone ขึ้น Pop Up ให้ชำระเงิน

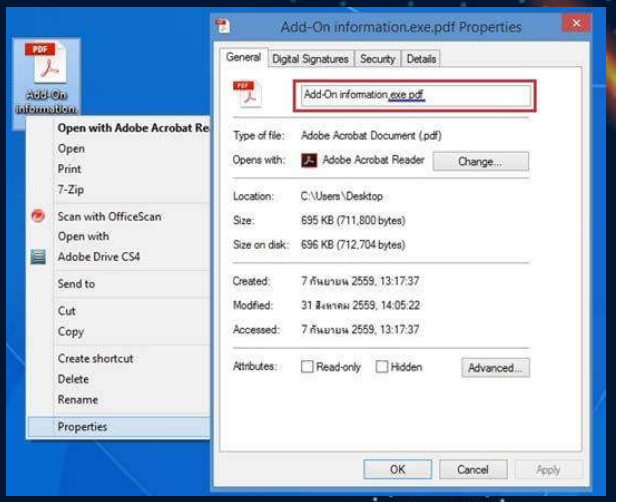
หน้าจอขึ้นมาเพื่อหลอกล่อเหยื่อ เพื่อให้ชำระเงิน หากต้องการได้ไฟล์กลับคืนมา บางกรณีเป็นแค่หน้าจอที่ทำมาหลอก ๆ เท่านั้น ซึ่งไฟล์นั้นอาจได้ถูกเข้ารหัสจริง ๆ ก็ได้

อาการที่บ่งบอกว่าคุณเครื่องของคุณอาจจะติด Ransomware

1. เครื่องทำงานช้าลงอย่างเห็นได้ชัด ทั้ง ๆ ที่ไม่ได้ใช้งานอะไรเลย
2. ไฟแสดงการทำงานของฮาร์ดดิสก์ กระพริบตลอดเวลา
3. การใช้อินเทอร์เน็ตช้าลง
4. มี Message ขึ้นหน้าจอ หรือ Popup แปลกๆ แจ้งเตือนเป็นจำนวนมาก
5. ใช้โปรแกรม Antivirus Scan ทั้งเครื่องก็ยังไม่หาย บางครั้งตรวจไม่พบ
6. มีไฟล์แปลก ๆ เพิ่มขึ้นมาใน Drive ต่าง ๆ โดยที่ไม่ได้มีการบันทึกอะไรลงไป
7. พื้นว่างที่ของฮาร์ดดิสก์ลดลง

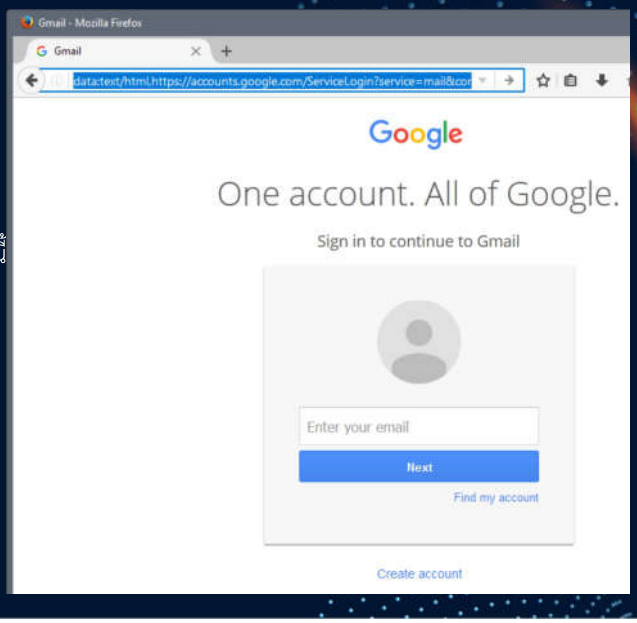
ช่องทางการโจมตีของ Ransomware

1. การโจมตีส่วนใหญ่จะมาทางอีเมล์หลอกลวงที่แนบไฟล์ Ransomware ไว้ โดยเนื้อหาในอีเมล์จะดึงดูดให้ผู้อ่านอยากคลิกเข้าไปอ่าน เช่น อีเมล์แจ้งเลขที่ใบสั่งซื้อสินค้า (OrderID) หากผู้ใช้ไม่คลิกไปเปิดไฟล์แนบ ก็อาจจะทำให้สูญเสียโอกาสทางการค้าได้ ซึ่งถ้าผู้ใช้คลิกเปิดไฟล์โดยไม่ระมัดระวังก็จะตกเป็นเหยื่อของ Ransomware ทันที ไฟล์แนบที่มากับอีเมล์จะเป็น zip file หากแตกไฟล์ออกมาก็จะพบไฟล์นามสกุล .doc, .xls หรือไฟล์อื่น ๆ ที่เราคุ้นเคย แต่ถ้าสังเกตดี ๆ จะพบว่านามสกุลของไฟล์จริง ๆ แล้วเป็น .exe เรียกเทคนิคการตั้งชื่อไฟล์แบบนี้ว่า Double Extensions



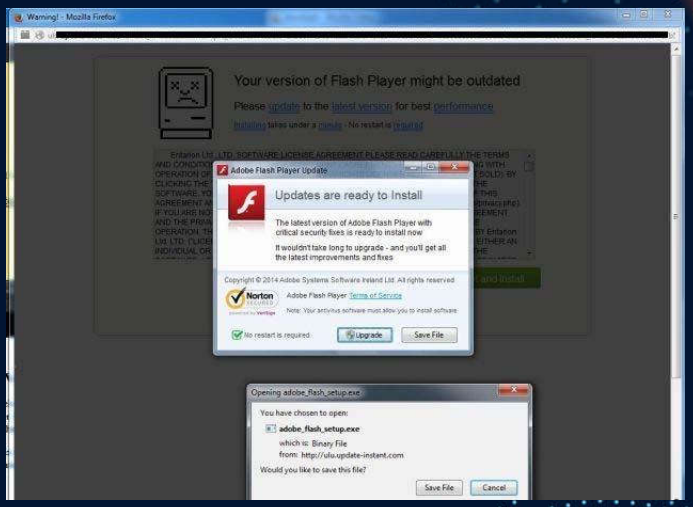
ช่องทางการโจมตีของ Ransomware

2. โจมตีด้วยวิธี Social Engineering เป็นการหลอกผู้ใช้งานให้ดาวน์โหลดโปรแกรมมาติดตั้งในเครื่อง เช่น ในขณะที่ใช้งานระบบลงทะเบียนเรียนออนไลน์ของมหาวิทยาลัย พบว่ามี Pop-up ขึ้นมาบอกว่า ให้ดาวน์โหลดโปรแกรมเสริมมาติดตั้งเพื่อให้สามารถลงทะเบียนได้สะดวก และรวดเร็วขึ้น ทั้ง ๆ ที่โปรแกรมนี้ไม่มีอยู่จริง หากผู้ใช้งานหลงเชื่อและทำการดาวน์โหลดมาติดตั้งไฟล์ต่าง ๆ ก็จะโดนจับเป็นตัวประกันทันที



ช่องทางการโจมตีของ Ransomware

3. โจมตีทางช่องโหว่ของ Browser รวมถึง Add-on, Plug-in ต่าง ๆ เช่น Java, Flash และ Acrobat Reader เป็นต้น



กลุ่มเป้าหมายของการโจมตี

1. กลุ่มคน ทั่วไปผู้ใช้งานตามบ้าน และในกลุ่มธุรกิจ หรือองค์กรที่ไม่มีหรือมีระบบรักษาความปลอดภัยทางไซเบอร์ โดยเฉพาะกลุ่มคนในแวดวงการศึกษา หรือมหาวิทยาลัย ที่มักตกเป็นเหยื่อบ่อยครั้ง เพราะจะต้องรับ –ส่ง ไฟล์หรือแชร์ไฟล์บ่อย ๆ โอกาสที่จะแพร่กระจายในระบบ Network เป็นไปได้ง่าย

2. ธุรกิจ หรือองค์กรต่าง ๆ ที่มีโอกาสในการจ่ายเงินสูง เช่น องค์กรภาครัฐ โรงพยาบาลธนาคาร องค์กรสาธารณสุข กองสลาก หรือองค์กรอื่น ๆ ที่มีความคล้ายคลึงกัน

3. ธุรกิจหรือองค์กรที่ถือข้อมูลสำคัญ เช่น องค์กรที่เกี่ยวกับกฎหมาย ข้อมูลประชากร กรมการขนส่ง ข้อมูลบัตรเครดิต สินเชื่อ

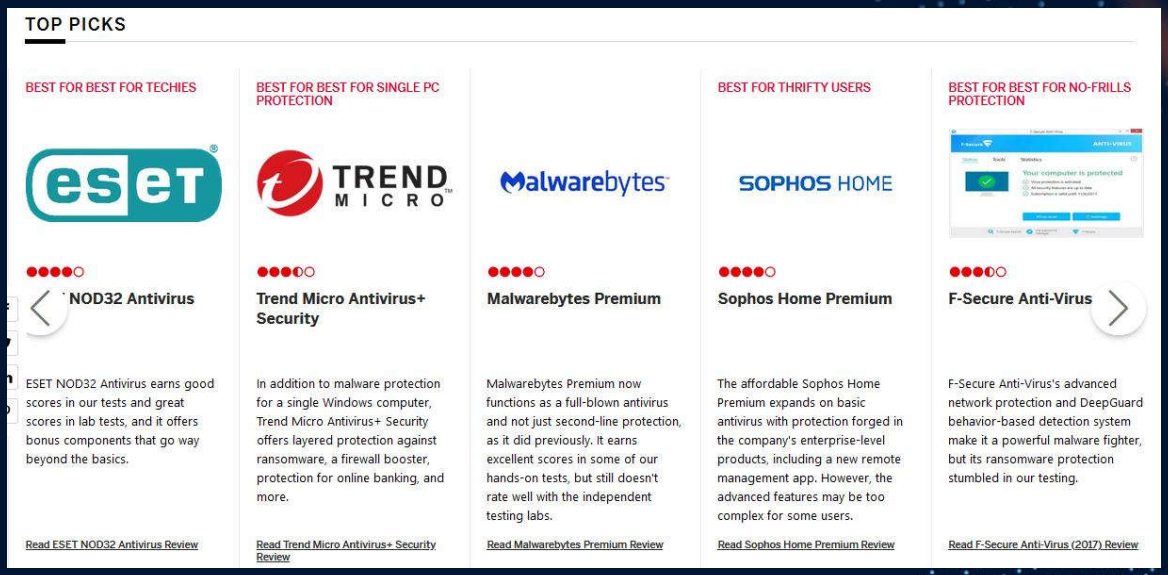
ถ้าติด Ransomware ต้องทำอย่างไร ?

1. ตัดการเชื่อมต่อเครือข่ายออกเพื่อป้องกันการลุกลามไปยังเครื่องอื่น
2. หาโปรแกรมที่สามารถยับยั้งการทำงานของ Ransomeware ได้ เช่น Malwarebyte, Kaspersky, Mcafee
3. ไม่ควรจ่ายเงินให้โจร เพราะโอกาสที่จะได้ไฟล์กลับคืนมานั้นน้อยมาก
4. ปรึกษาผู้เชี่ยวชาญเพื่อขอคำแนะนำเพิ่มเติม
5. เครื่องมือถอดรหัสออนไลน์อาจช่วยได้ : โดยมีเครื่องมือที่เรียกว่า “Crypto Sheriff” ที่ใช้ในการระบุว่า Malware หรือไวรัสที่ติดคอมพิวเตอร์ของคุณนั้นเป็นชนิดใด จากนั้นระบบจะค้นหาแหล่งทรัพยากรอย่าง No More Ransom เพื่อดูว่ามีคีย์ถอดรหัสสำหรับสายพันธุ์นั้น ๆ หรือไม่ หากเป็น Ransomware สายพันธุ์ธรรมดา ก็มีโอกาสสูงที่คุณอาจสามารถกู้ไฟล์คืนได้

วิธีรับมือกับ Ransomware

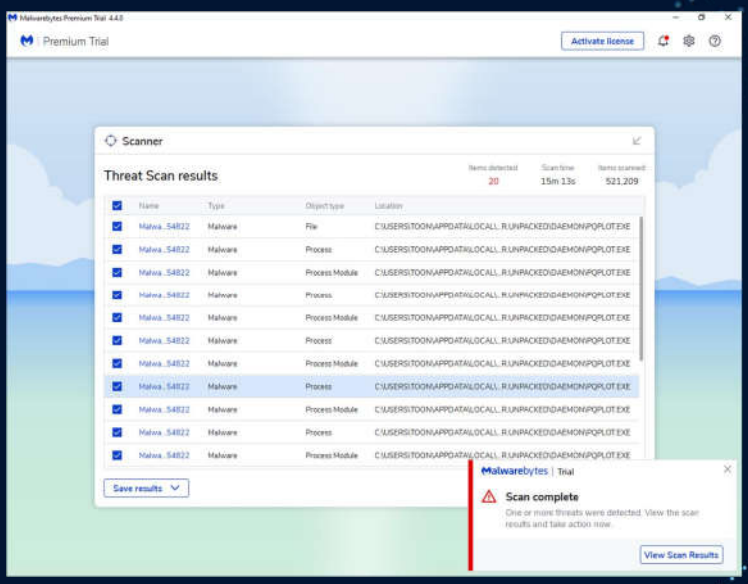
1. อัพเดตระบบปฏิบัติการ (Operating System) และโปรแกรมอื่น ๆ บ่อย ๆ
2. ติดตั้งโปรแกรมแอนตี้ไวรัสที่มีการป้องกัน Ransomware เช่น Malwarebyte
3. ไม่คลิกลิงก์แปลก ๆ หรือดาวน์โหลดไฟล์ที่ไม่มี Crack หรือนามสกุลแปลกๆ
4. สำรองข้อมูลไว้หลายที่ เช่น เก็บบน Cloud หรือ External Harddisk
5. กรณีที่ต้องแชร์ไฟล์กันในเครือข่าย ควรกำหนดสิทธิ์ในการเข้าถึง ป้องกันไฟล์สำคัญด้วย Read-Only
6. ปิดการเข้าถึงข้อมูลจากระยะไกล Remote Desktop และโปรแกรมรีโมทต่างๆ
7. กรณีที่ใช้ระบบ Virtual Machine ควรมีการสำรองข้อมูล ตรวจสอบไฟล์ Snap Shot
8. ใช้ซอฟต์แวร์ลิขสิทธิ์แท้

ตัวอย่างโปรแกรม Antivirus ที่นิยมใช้กันในปัจจุบัน



https://www.pcmag.com

ตัวอย่างโปรแกรม Malwarebyte



ภัยคุกคามทางคอมพิวเตอร์ในปัจจุบันที่ควรระวัง

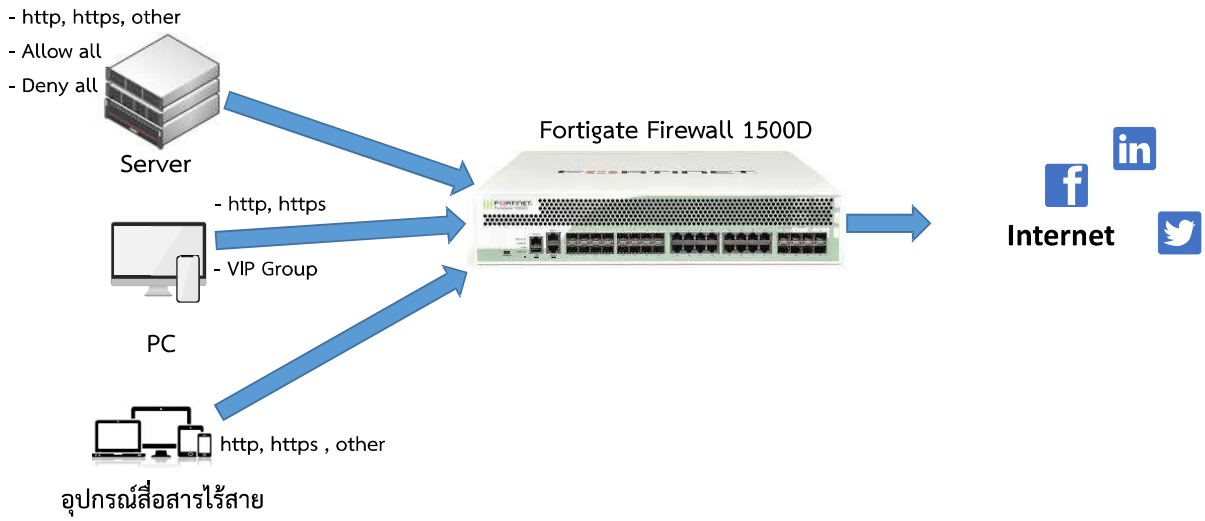
ภัยคุกคามทางคอมพิวเตอร์ในปัจจุบันที่ควรระวัง

1. ภัยคุกคามทางระบบฮาร์ดแวร์ (Physical)
   - กระแสไฟฟ้าดับ
   - ไฟไหม้
   - การถูกขโมยเครื่อง และอุปกรณ์คอมพิวเตอร์
   - อุปกรณ์ถูกทำลายเสียหาย

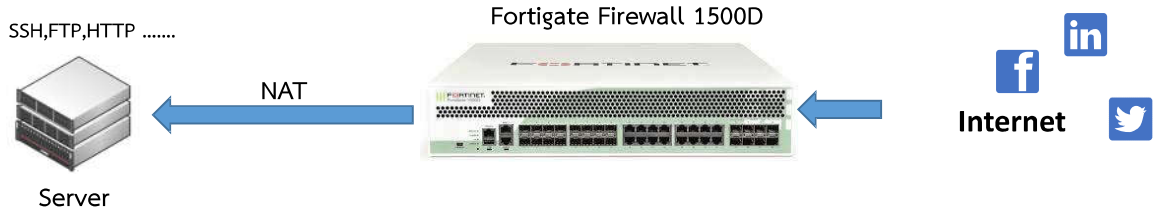
2. ภัยคุกคามทางซอฟต์แวร์ (Logical)
   - ถูก Hacker โจมตีด้วยวิธีการต่าง ๆ
   - ติดไวรัส Worm, Malware, Trojan, Spyware, Backdoor, DDOS .....
   - Phishing ขโมยข้อมูลสำคัญส่วนตัว โดยหลอกให้กรอกข้อมูลคล้ายกับเว็บไซต์ของจริง
   - Spam Mail ส่งข่าวสารเชิญชวน โฆษณาสินค้าและบริการ ทำให้เกิดความรำคาน
   - Sniffing การดักจับข้อมูล

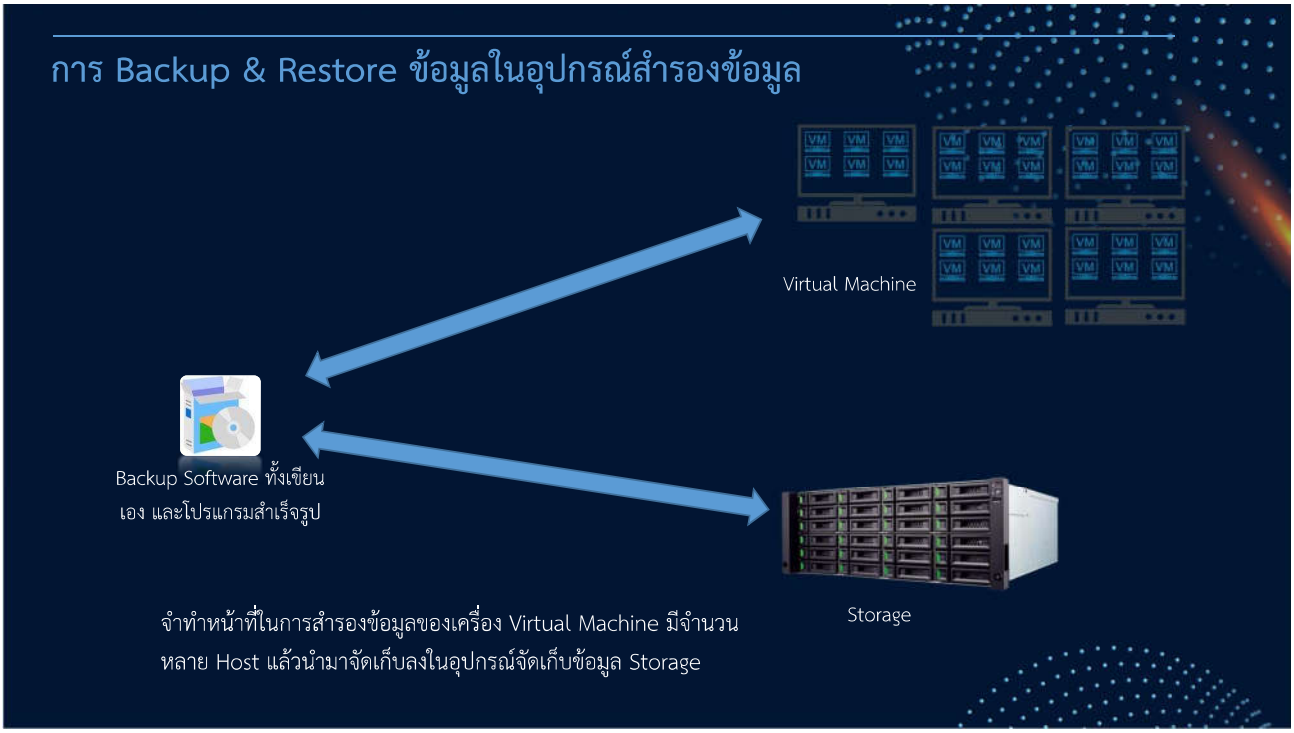
การเตรียมความพร้อมในการรับมือภัยคุกคามคอมพิวเตอร์
ของมหาวิทยาลัยราชภัฏเชียงใหม่

เข้มงวดการเข้าถึงอินเทอร์เน็ตของผู้ใช้งานภายในองค์กรด้วย Firewall Policy

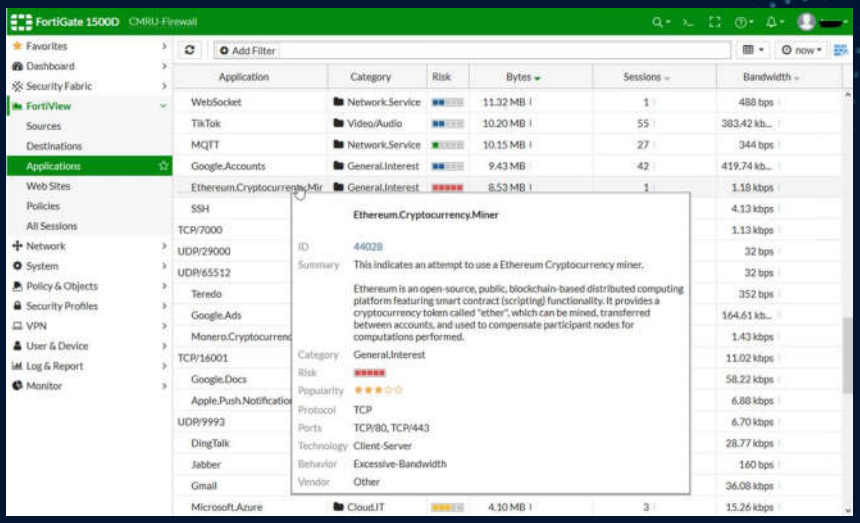


เข้มงวดการ Access เข้ามาจากภายนอก โดยจัดทำ Policy ให้เหมาะสมกับการใช้งาน

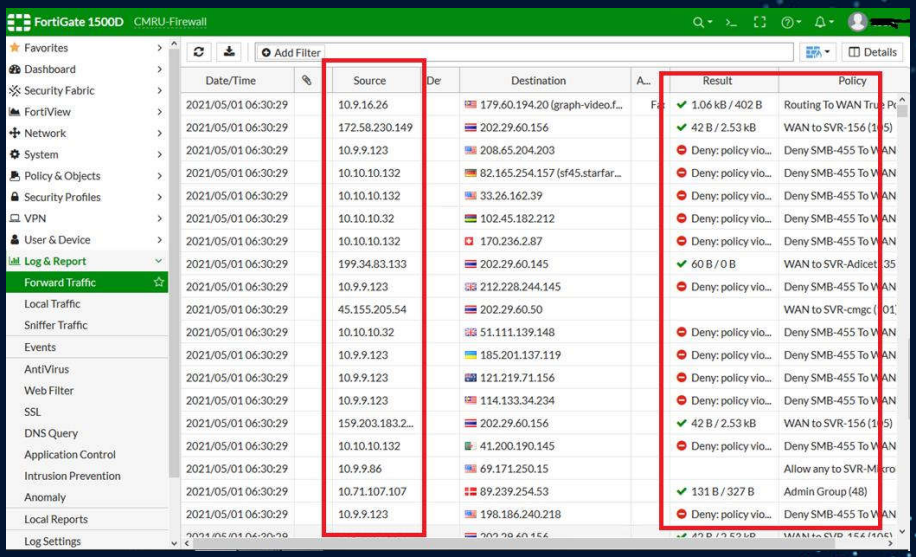




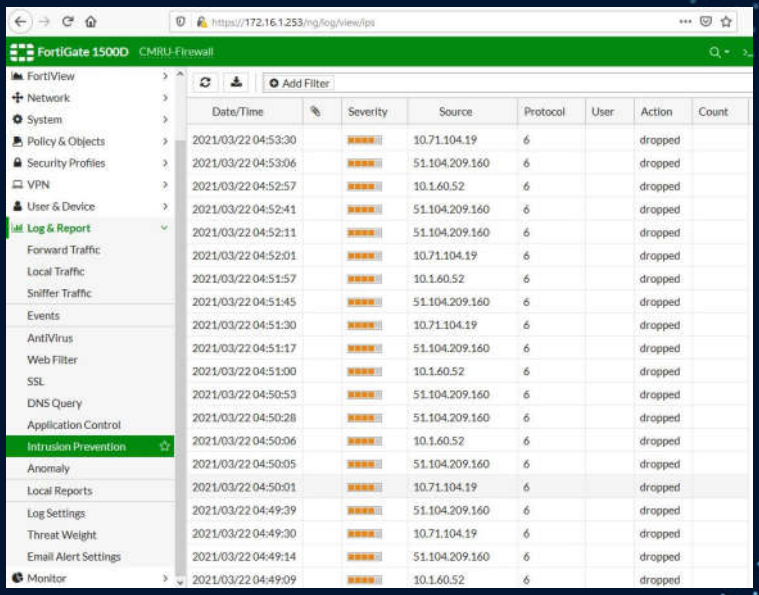
ตรวจสอบ Firewall Log เพื่อแก้ไขจุดบกพร่องต่าง ๆ



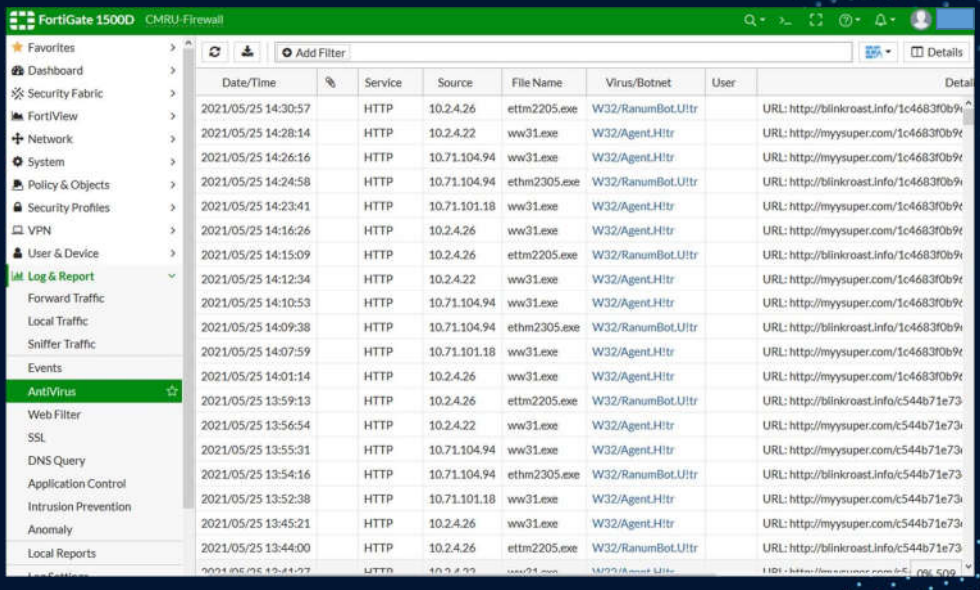
ตรวจสอบเครื่องที่ติด Ransomware



ตรวจสอบการทำงานของ IPS บน Firewall

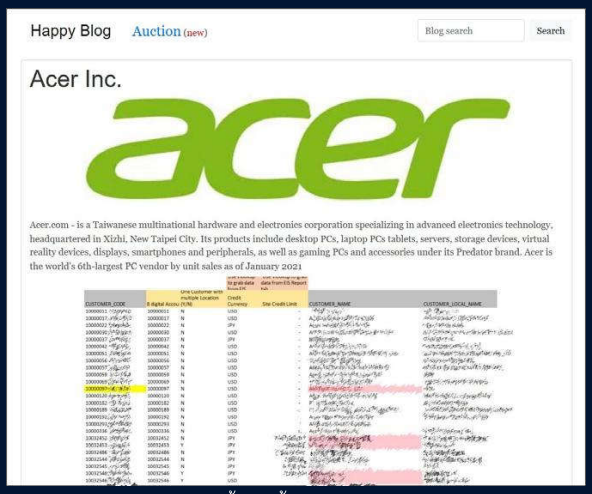


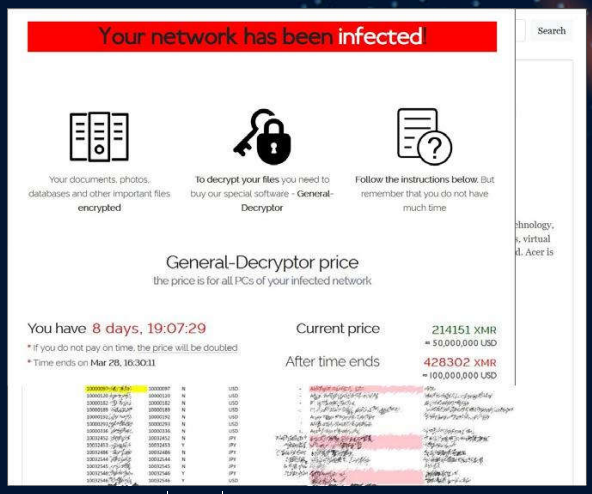
การตรวจสอบ Antivirus บนอุปกรณ์ Firewall



กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์ (หน่วยงานภาครัฐ และเอกชนภายนอก)

Acer บริษัทยักษ์ใหญ่แห่งวงการคอมพิวเตอร์ถูกโจมตีด้วย REvil ransomware โดยมีการเรียกค่าไถ่เป็นจำนวนสูงที่สุดเท่าที่เคยมีมา ที่ 50 ล้านดอลลาร์

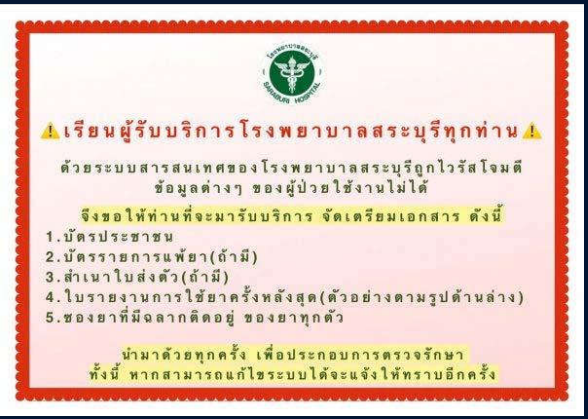




หลักฐานว่าการโจมตี Acer นั้นเกิดขึ้นจริง เช่น ข้อมูลทางการเงิน ยอดคงเหลือในธนาคาร และข้อมูลที่ติดต่อสื่อสารกับธนาคาร เป็นต้น ผู้โจมตีเสนอส่วนลดให้ 20% หากชำระเงินภายในวัน เวลา ที่กำหนด และจะจัดหาตัวถอดรหัส รายงานเรื่องช่องโหว่ และลบไฟล์ที่ขโมยมาทั้งหมดเป็นการตอบแทน

https://www.beartai.com/news/itnews/576375

แฮกเกอร์ส่ง'มัลแวร์'เรียกค่าไถ่ รพ.สระบุรี เป็นเงินทั้งสิ้น 200,000 Bitcoin หรือราว ๆ 63,000 ล้านบาท



เนื่องด้วย เมื่อวันที่ ๕ กันยายน ๒๕๖๓ โรงพยาบาลสระบุรี ได้รับการโจมตีจากไวรัสเรียกค่าไถ่ชื่อ Ransomware ทำให้ข้อมูลการบริการรวมถึงระบบสนับสนุนทั้งหมดได้รับความเสียหาย และโรงพยาบาลไม่สามารถเข้าถึงข้อมูลได้ ซึ่งส่งผลกระทบกับประชาชนทำให้ได้รับบริการล่าช้าและไม่มีข้อมูลการรักษาพยาบาลเดิม โรงพยาบาลสระบุรีได้ดำเนินการแก้ไขโดยเริ่มระบบการทำงานด้วยมือทั้งหมดโดยทันที และกู้คืนฐานข้อมูลจากแหล่งอื่น ๆ ทำให้กู้คืนข้อมูลบางส่วนกลับมาได้ได้แก่ ผล LAB ผล X-Ray และประวัติยาเดิมบางส่วน เหตุการณ์ดังกล่าว แม้ทางโรงพยาบาลสระบุรีจะมีการสำรองข้อมูลสม่ำเสมอทุกวันและเก็บสำรองไว้ ๓ วัน แต่เนื่องจากการโจมตีฐานข้อมูลได้กระทำอย่างรวดเร็วและการกระทำระหว่างสำรองข้อมูล จึงไม่สามารถป้องกันฐานข้อมูลไว้ได้ ฐานข้อมูลที่ยังรักษาไว้ได้มีเพียงฐานข้อมูลก่อน ๓๑ มกราคม ๒๕๖๐ โรงพยาบาดสระบุรีจะเร่งดำเนินการแก้ไขโดยการถอดรหัส และวางระบบปฏิบัติการทางคอมพิวเตอร์ใหม่

https://www.dailynews.co.th/regional/794273

กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์ (ของมหาวิทยาลัยราชภัฏเชียงใหม่)

กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์

เครื่อง Windows Server ถูก Ransomware โจมตีในปี 2020

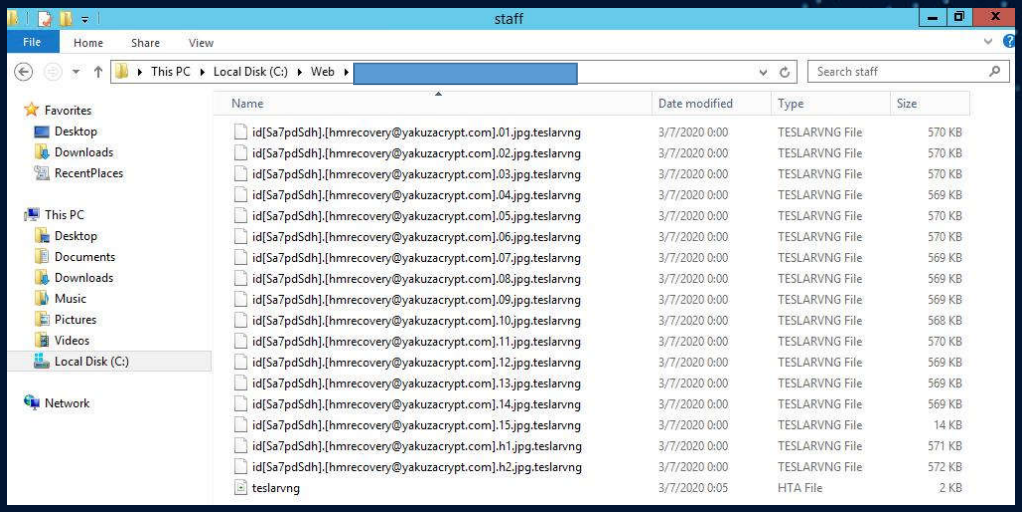
<u>สาเหตุเกิดจาก</u>

1. เครื่องไม่ได้ทำการ Update Patch
2. คาดว่าจะถูกเจาะผ่านทาง Remote Desktop
3. มีลักษณะของการ Share Drive คาดว่าใช้รหัสเดียวกันกับ Remote Desktop
4. โปรแกรม Antivirus หมดอายุ

<u>วิธีการแก้ไข</u>

1. Restore Backup วันล่าสุดก่อนที่จะถูกโจมตีขึ้นมาใช้งาน
2. Update Patch ของ Windows ให้เป็นปัจจุบัน
3. ติดตั้งโปรแกรม Antivirus, Malwarebyte
4. จัดทำ Firewall Policy ใหม่ให้รัดกุมมากขึ้น

กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์



กรณีเครื่อง Windows Server ถูก Ransomware โจมตีในปี 2020

กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์

กรณีเครื่อง Linux Server ถูกเจาะเข้ามาแล้วสร้างไฟล์ใน Server เป็นจำนวนมาก

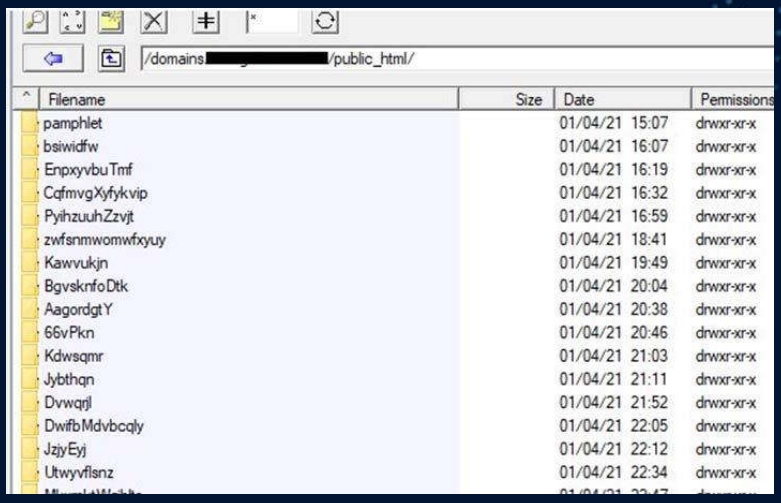
<u>สาเหตุเกิดจาก</u>

1. เครื่อง Server ไม่ได้ทำการ Update Patch
2. เจาะเข้ามาผ่านช่องโหว่ของ PHP Version เก่า และ Server มีการเปิดให้รัน CGI ผ่านทาง PHP Script
3. รหัสของเว็บไซต์สามารถคาดเดาได้ง่ายมากเกินไป เช่น “cmru1234”, “tak1234”, “aaaabbbb”
4. โปรแกรมภาษา PHP ยังคงเป็น Version เก่า 5.xx
5. เว็บไซต์ไม่มี SSL เนื่องจากไม่รองรับ

<u>วิธีการแก้ไข</u>

1. Update Patch ของ OS ให้ใหม่ล่าสุด
2. ลบไฟล์ที่น่าสงสัยทิ้ง
3. กำหนดสิทธิ์การเข้าถึงในแต่ละ Folder ให้เหมาะสม
4. เปลี่ยนรหัสผ่านทุกอย่าง รหัสผ่าน Root, MySQL, FTP โดยเพิ่มความยากของตัวอักษรเข้าไป
5. แนะนำให้ admin ที่ดูแลเว็บไซต์นั้นย้ายไปใช้บริการ Server ที่มี PHP Version ใหม่ และรองรับ SSL

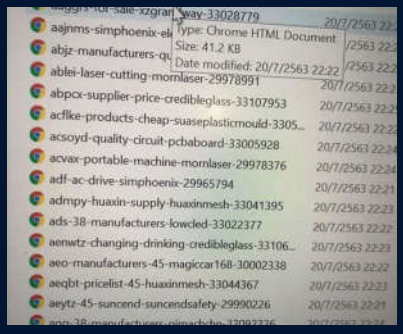
กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์



กรณีเครื่อง Linux Server ถูกเจาะเข้ามาแล้วสร้างไฟล์ใน Server เป็นจำนวนมาก

สั่ง Run Command เพื่อใช้เครื่อง Server ในการขุด Bitcoin

```
Apr28   0:00 sh -c ./xmrig -a cryptonight -o stratum+tcp://xmr.pool.minergate.com:45700 -u castorforelli42@gmail.com -p x 2>&1
Apr28 167726:32 ./xmrig -a cryptonight -o stratum+tcp://xmr.pool.minergate.com:45700 -u castorforelli42@gmail.com -p x
```



กรณีเครื่อง Linux Server ถูกเจาะเข้ามาเพื่อใช้เป็นเครื่องขุด Bitcoin

แนวปฏิบัติและแนวทางการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์

แนวปฏิบัติและแนวทางการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์

1. หมั่นตรวจสอบการ Update ของ OS รวมไปถึงโปรแกรม Antivirus, Spyware, Malware ต่าง ๆ
2. การตั้งรหัสผ่านจะต้องตั้งค่าให้มีความยากต่อการคาดเดา
3. มีการสำรองข้อมูลอย่างสม่ำเสมอ มีตารางการสำรองข้อมูลที่แน่นอน และจัดเก็บข้อมูลไว้มากกว่า 1 แหล่งเสมอ
4. ทดสอบการกู้คืนข้อมูล เพื่อให้แน่ใจว่าข้อมูลที่สำรองไว้นั้นสามารถนำมาใช้งานได้จริง
4. ควบคุมการเข้าถึงเครือข่าย และระบบสารสนเทศ จำกัดสิทธิ์ในการเข้าถึงทรัพยากรในระบบเครือข่ายให้สามารถเข้าถึงได้เฉพาะเครื่องที่จำเป็นเท่านั้น
5. ไม่ควรเปิดไฟล์ที่ถูกส่งมาทาง E-mail หรือ กด Link ที่ไม่รู้จัก
6. กรณีที่จำเป็นต้องทำการ Remote มายังเครื่อง Server จากภายนอกมหาวิทยาลัย ต้องใช้งานผ่าน VPN เท่านั้น

แนวปฏิบัติและแนวทางการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์ (ต่อ)

7. ใช้ Software ที่ถูกต้องตามลิขสิทธิ์เท่านั้น หลีกเลี่ยงการใช้ Software เถื่อนที่มี Crack
8. ผู้ดูละระบบต้องตรวจสอบความผิดปกติของเครื่อง Server และข้อมูลบันทึกกิจกรรม (log) อย่างสม่ำเสมอ
9. ตรวจสอบช่องโหว่ ของระบบสารสนเทศ หรือซอฟต์แวร์ที่ให้บริการ อย่างสม่ำเสมอ และให้รีบแก้ไขช่องโหว่ทันทีหากพบว่าเป็นความเสี่ยงที่รุนแรง
10. ประเมินความเสี่ยงทางด้านระบบสารสนเทศอย่างสม่ำเสมอ มีการประชุมเพื่อสรุปปัญหาที่ได้พบจากการปฏิบัติงาน
11. ลดการใช้ Flash Drive ในการโอนถ่ายข้อมูล เพราะปัจจุบัน Cloud Services อย่าง Google Drive, OneDrive
12. อย่าเปิดเผยข้อมูลส่วนตัวเช่น E-mail หรือเบอร์โทรศัพท์โดยไม่จำเป็น