

คู่มือ

การป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์
(Ransomware) ในบริบทของมหาวิทยาลัยราชภัฏเชียงใหม่

สำนักดิจิทัลเพื่อการศึกษา

DIGITAL EDUCATION | **DIGITAL** KM day 2021 | ขอเชิญเข้าร่วม กิจกรรมแลกเปลี่ยนเรียนรู้



การป้องกันการเรียกค่าไถ่ฐานข้อมูล จากอาชญากรไซเบอร์ (Ransomware)

หัวข้อ

ในระบบของมหาวิทยาลัยราชภัฏเชียงใหม่

วันจันทร์ที่ 31 พฤษภาคม 2564 เวลา 9.00 – 12.00 น. ผ่านระบบ **zoom meeting**

ลงทะเบียน



เรื่องที่จะ KM เกี่ยวกับ

- ระบบรักษาความปลอดภัยทางดิจิทัล ในภาพรวมมหาวิทยาลัย
- กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์
- ศึกษาศูนย์ควบคุมตัวละเมิดในปัจจุบัน ที่วสสจ-งวิ
- แนวปฏิบัติและแนวทางการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์

ติดต่อ สำนักส่งเสริมการศึกษา มหาวิทยาลัยราชภัฏเชียงใหม่ สอบถามรายละเอียดเพิ่มเติม โทร. 053-885-942

CONTENTS

- ระบบรักษาความปลอดภัยภาพรวมของมหาวิทยาลัยราชภัฏเชียงใหม่
 - เกี่ยวกับ Ransomware
 - Operating System ที่ Ransomware เลือกในการโจมตี
 - วิธีการโจมตีหลัก ๆ ของ Ransomware
 - เมื่อถูก Ransomware โจมตีแล้วจะเป็นอย่างไร ?
 - อาการที่บ่งบอกว่าเครื่องของคุณอาจจะติด Ransomware
 - ช่องทางการโจมตีของ Ransomware
 - กลุ่มเป้าหมายในการโจมตี
 - ถ้าติด Ransomware แล้วต้องทำอะไร ?
 - วิธีรับมือกับ Ransomware
- ภัยคุกคามทางคอมพิวเตอร์ในปัจจุบันที่ควรระวัง
- กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์
- แนวปฏิบัติและแนวทางการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรไซเบอร์

ระบบรักษาความปลอดภัยภาพรวมของมหาวิทยาลัยราชภัฏเชียงใหม่

Ransomware คืออะไร ?

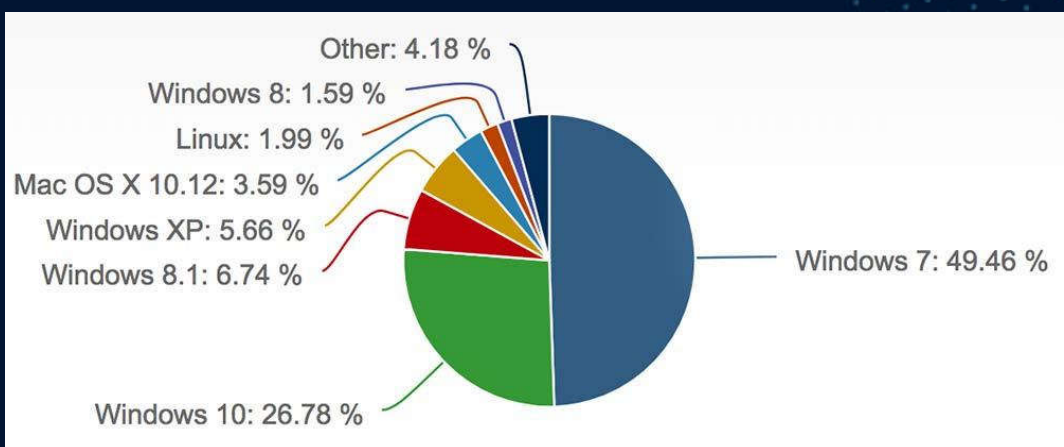
Ransomware จัดว่าเป็น Malware ประเภทหนึ่งที่มีลักษณะการทำงานที่แตกต่างกับ Malware ประเภทอื่น ๆ คือไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของผู้ใช้งานแต่อย่างใด แต่จะทำการเข้ารหัส หรือล็อกไฟล์ทุกประเภท ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใด ๆ ได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจำเป็นต้องใช้คีย์ในการปลดล็อกเพื่อกู้ข้อมูลคืนมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” ที่ปรากฏ ส่วนมากจะต้องชำระด้วย Bitcoin แต่อย่างไรก็ตามการชำระเงินก็ไม่ได้หมายความว่าผู้ไม่หวังดีจะส่งคีย์ที่ใช้ในการปลดล็อกไฟล์ให้กับผู้ใช้งานเมื่อชำระแล้วจะได้รับ Key สำหรับการถอดรหัสไฟล์ ซึ่งก็ไม่สามารถรับประกันได้ว่าจะกู้ได้จริงหรือไม่



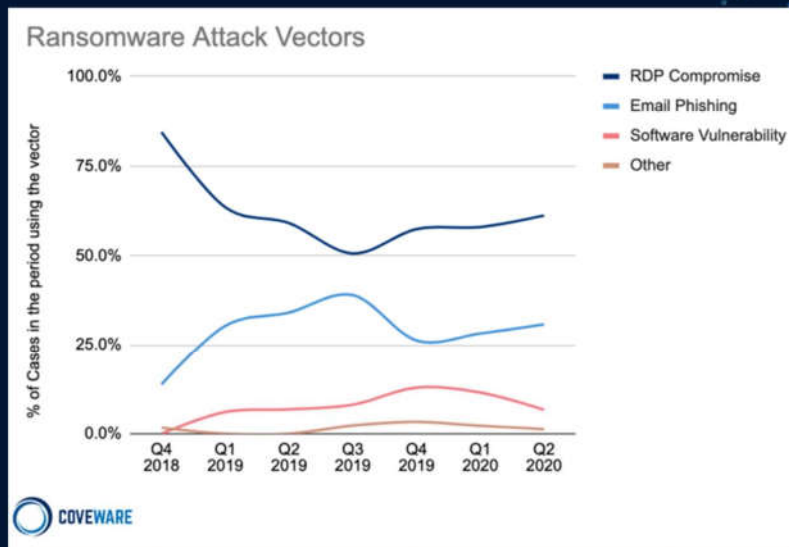
วิธีการโจมตีหลัก ๆ ของ Ransomware



Operating System ที่ Ransomware เลือกโจมตี



การโจมตีผ่าน Service ต่าง ๆ



ตัวอย่าง Windows ขึ้นหน้าจอ Lock Screen



เมื่อ Ransomware เข้ารหัสไฟล์ของเครื่อง เป้าหมายเป็นที่เรียบร้อยแล้วจะสร้างหน้าจอ ขึ้นมาเพื่อแจ้งรายละเอียดต่าง ๆ ตามที่ ต้องการ บางกรณีจะไม่สามารถปิดหน้าจอนี้ ได้เลย เนื่องจากถูกฝังลงไป ใน Startup และ แก้ไขค่า Registry ของ Windows ไปเป็นที่ เรียบร้อยแล้ว

ตัวอย่าง Android Phone ขึ้น Pop Up ให้ชำระเงิน



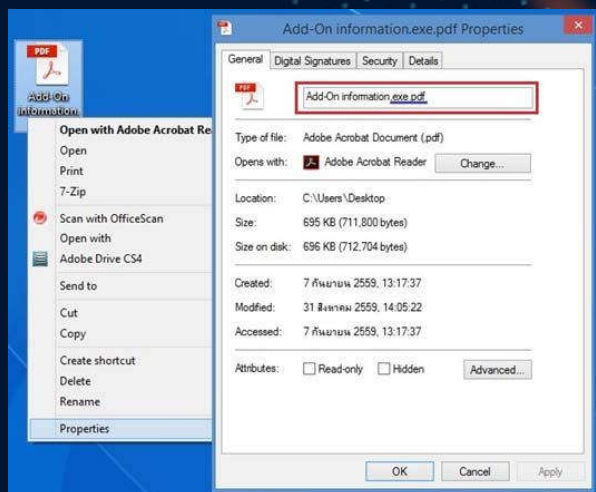
หน้าจอขึ้นมาเพื่อหลอกล่อเหยื่อ เพื่อให้ชำระเงิน หากต้องการได้ไฟล์กลับคืนมา บางกรณีเป็นแค่หน้าจอที่ทำมาหลอก ๆ เท่านั้น ซึ่งไฟล์นั้นอาจได้ถูกเข้ารหัสจริง ๆ ก็ได้

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 เพิ่มขึ้นใน Drive ต่าง ๆ โดยที่ไม่ได้มีการบันทึกอะไรลงไป
7. พื้นที่ว่างที่ของฮาร์ดดิสก์ลดลง

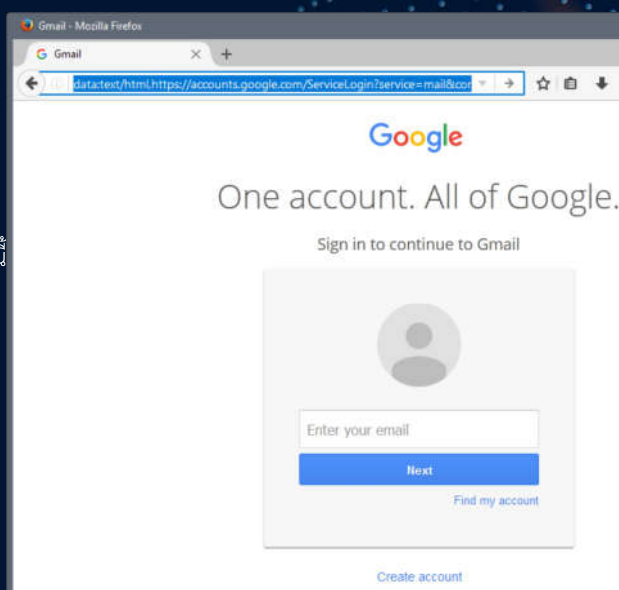
ช่องทางการโจมตีของ Ransomware

1. การโจมตีส่วนใหญ่จะมาทางอีเมลหลอกลวงที่แนบไฟล์ Ransomware ไว้ โดยเนื้อหาในอีเมลจะดึงดูดให้อ่านอยากคลิกเข้าไปอ่าน เช่น อีเมลแจ้งเลขที่ใบสั่งซื้อสินค้า (OrderID) หากผู้ใช้ไม่คลิกไปเปิดไฟล์แนบ ก็อาจจะทำให้สูญเสียโอกาสทางการค้าได้ ซึ่งถ้าผู้ใช้คลิกเปิดไฟล์โดยไม่ระมัดระวังก็จะตกเป็นเหยื่อของ Ransomware ทั้งนี้ ไฟล์แนบที่มากับอีเมลจะเป็น zip file หากแตกไฟล์ออกมา ก็จะพบไฟล์นามสกุล .doc, .xls หรือไฟล์อื่น ๆ ที่เรารู้จัก 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 ก็จะได้โดนจับเป็นตัวประกันทันที



ช่องทางการโจมตีของ Ransomware

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



กลุ่มเป้าหมายของการโจมตี

1. กลุ่มคนทั่วไปผู้ใช้งานตามบ้าน และในกลุ่มธุรกิจ หรือองค์กรที่ไม่มีหรือมีระบบรักษาความปลอดภัยทางไซเบอร์ โดยเฉพาะกลุ่มคนในแวดวงการศึกษา หรือมหาวิทยาลัย ที่มักตกเป็นเหยื่อบ่อยครั้ง เพราะจะต้องรับ - ส่ง ไฟล์ หรือแชร์ไฟล์บ่อย 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 ต้องทำอะไร ?

1. ตัดการเชื่อมต่อเครือข่ายออกเพื่อป้องกันการลุกลามไปยังเครื่องอื่น
2. หาโปรแกรมที่สามารถยับยั้งการทำงานของ Ransomware 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. อัปเดตระบบปฏิบัติการ (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. ใช้ซอฟต์แวร์ลิซิทซ์แท้

ตัวอย่างโปรแกรม Antivirus ที่นิยมใช้กันในปัจจุบัน

TOP PICKS

BEST FOR BEST FOR TECHIES



ESET NOD32 Antivirus

ESET NOD32 Antivirus earns good scores in our tests and great scores in lab tests, and it offers bonus components that go way beyond the basics.

[Read ESET NOD32 Antivirus Review](#)

BEST FOR BEST FOR SINGLE PC PROTECTION



Trend Micro Antivirus+ Security

In addition to malware protection for a single Windows computer, Trend Micro Antivirus+ Security offers layered protection against ransomware, a firewall booster, protection for online banking, and more.

[Read Trend Micro Antivirus+ Security Review](#)



Malwarebytes Premium

Malwarebytes Premium now functions as a full-blown antivirus and not just second-line protection, as it did previously. It earns excellent scores in some of our hands-on tests, but still doesn't rate well with the independent testing labs.

[Read Malwarebytes Premium Review](#)

BEST FOR THRIFTY USERS



Sophos Home Premium

The affordable Sophos Home Premium expands on basic antivirus with protection forged in the company's enterprise-level products, including a new remote management app. However, the advanced features may be too complex for some users.

[Read Sophos Home Premium Review](#)

BEST FOR BEST FOR NO-FRILLS PROTECTION



F-Secure Anti-Virus

F-Secure Anti-Virus's advanced network protection and DeepGuard behavior-based detection system make it a powerful malware fighter, but its ransomware protection stumbled in our testing.

[Read F-Secure Anti-Virus \(2017\) Review](#)

<https://www.pcmag.com>

ตัวอย่างโปรแกรม Malwarebyte

Malwarebytes Premium Trial 4.42

Scanner

Threat Scan results

Items detected: 20 | Scan time: 15m 13s | Items scanned: 521,209

Name	Type	Object type	Location
Malwa_54822	Malware	File	C:\USERS\TOON\APPROXDATALOCAL\RUN\PACKED\DAEMON\POPLOT.EXE
Malwa_54822	Malware	Process	C:\USERS\TOON\APPROXDATALOCAL\RUN\PACKED\DAEMON\POPLOT.EXE
Malwa_54822	Malware	Process Module	C:\USERS\TOON\APPROXDATALOCAL\RUN\PACKED\DAEMON\POPLOT.EXE
Malwa_54822	Malware	Process	C:\USERS\TOON\APPROXDATALOCAL\RUN\PACKED\DAEMON\POPLOT.EXE
Malwa_54822	Malware	Process Module	C:\USERS\TOON\APPROXDATALOCAL\RUN\PACKED\DAEMON\POPLOT.EXE
Malwa_54822	Malware	Process	C:\USERS\TOON\APPROXDATALOCAL\RUN\PACKED\DAEMON\POPLOT.EXE
Malwa_54822	Malware	Process Module	C:\USERS\TOON\APPROXDATALOCAL\RUN\PACKED\DAEMON\POPLOT.EXE
Malwa_54822	Malware	Process	C:\USERS\TOON\APPROXDATALOCAL\RUN\PACKED\DAEMON\POPLOT.EXE
Malwa_54822	Malware	Process Module	C:\USERS\TOON\APPROXDATALOCAL\RUN\PACKED\DAEMON\POPLOT.EXE
Malwa_54822	Malware	Process	C:\USERS\TOON\APPROXDATALOCAL\RUN\PACKED\DAEMON\POPLOT.EXE
Malwa_54822	Malware	Process Module	C:\USERS\TOON\APPROXDATALOCAL\RUN\PACKED\DAEMON\POPLOT.EXE

Save results

Malwarebytes | Trial

Scan complete

One or more threats were detected. View the scan results and take action now.

View Scan Results

ภัยคุกคามทางคอมพิวเตอร์ในปัจจุบันที่ควรระวัง

ภัยคุกคามทางคอมพิวเตอร์ในปัจจุบันที่ควรระวัง

1. ภัยคุกคามทางระบบฮาร์ดแวร์ (Physical)

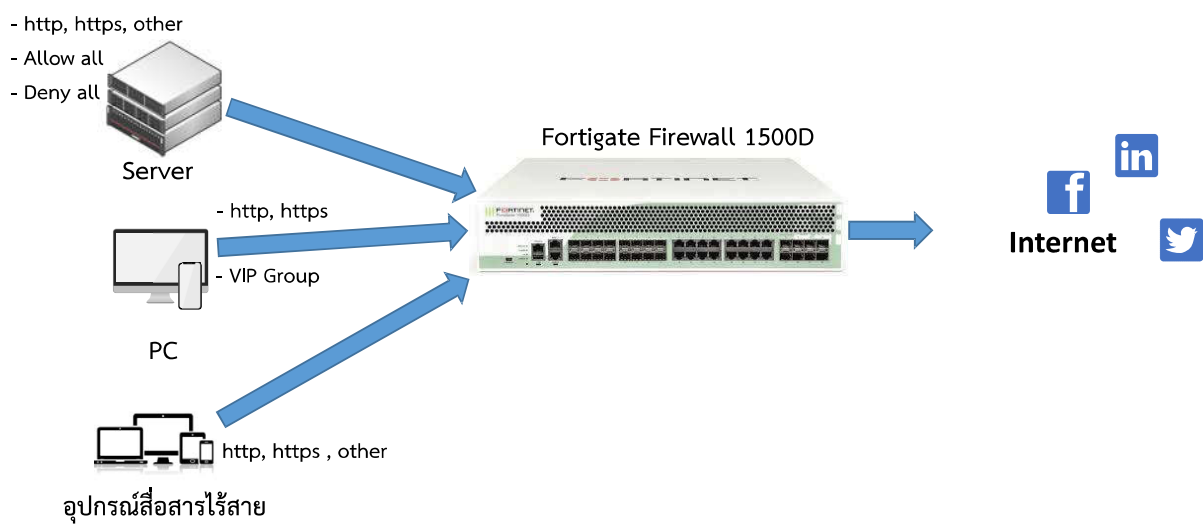
- กระแสไฟฟ้าดับ
- ไฟไหม้
- การถูกขโมยเครื่อง และอุปกรณ์คอมพิวเตอร์
- อุปกรณ์ถูกทำลายเสียหาย

2. ภัยคุกคามทางซอฟต์แวร์ (Logical)

- ถูก Hacker โจมตีด้วยวิธีการต่าง ๆ
- ติดไวรัส Worm, Malware, Trojan, Spyware, Backdoor, DDOS
- Phishing ขโมยข้อมูลสำคัญส่วนตัว โดยหลอกให้กรอกข้อมูลคล้ายกับเว็บไซต์ของจริง
- Spam Mail ส่งข่าวสารเชิญชวน โฆษณาสินค้าและบริการ ทำให้เกิดความรำคาญ
- Sniffing การดักจับข้อมูล

การเตรียมความพร้อมในการรับมือภัยคุกคามคอมพิวเตอร์ ของมหาวิทยาลัยราชภัฏเชียงใหม่

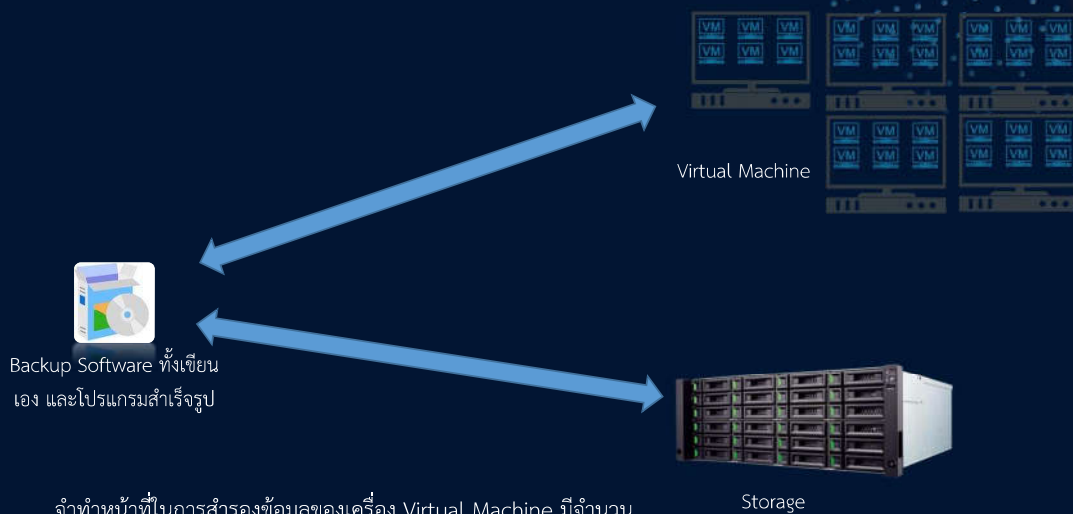
เข้มงวดการเข้าถึงอินเทอร์เน็ตของผู้ใช้งานภายในองค์กรด้วย Firewall Policy



เข้มงวดการ Access เข้ามาจากภายนอก โดยจัดทำ Policy ให้เหมาะสมกับการใช้งาน



การ Backup & Restore ข้อมูลในอุปกรณ์สำรองข้อมูล



จำทำหน้าทีในการสำรองข้อมูลของเครื่อง Virtual Machine มีจำนวนหลาย Host แล้วนำมาจัดเก็บลงในอุปกรณ์จัดเก็บข้อมูล Storage

ตรวจสอบ Firewall Log เพื่อแก้ไขจุดบกพร่องต่าง ๆ

Application	Category	Risk	Bytes	Sessions	Bandwidth
WebSocket	Network.Service	Low	11.32 MB	1	488 bps
TikTok	Video/Audio	Low	10.20 MB	55	383.42 kb/s
MQTT	Network.Service	Low	10.15 MB	27	344 bps
Google.Accounts	General.Interest	Low	9.43 MB	42	419.74 kb/s
Ethereum.Cryptocurrency.Miner	General.Interest	High	8.53 MB	1	1.18 kbps
SSH					4.13 kbps
TCP/7000					1.13 kbps
UDP/29000					32 bps
UDP/65512					32 bps
Teredo					352 bps
Google.Ads					164.61 kb/s
Monero.Cryptocurrency					1.43 kbps
TCP/16001	General.Interest	Low			11.02 kbps
Google.Docs		High			58.22 kbps
Apple.Push.Notification					6.88 kbps
UDP/9993	TCP/80, TCP/443				6.70 kbps
DingTalk	Technology	Client-Server			28.77 kbps
Jobber	Behavior	Excessive-Bandwidth			160 bps
Gmail	Vendor	Other			36.08 kbps
Microsoft.Azure	Cloud.IT	Low	4.10 MB	3	15.26 kbps

Ethereum.Cryptocurrency.Miner
 ID: 44028
 Summary: This indicates an attempt to use a Ethereum Cryptocurrency miner.
 Description: Ethereum is an open-source, public, blockchain-based distributed computing platform featuring smart contract (scripting) functionality. It provides a cryptocurrency token called "ether", which can be mined, transferred between accounts, and used to compensate participant nodes for computations performed.

ตรวจสอบเครื่องที่ติด Ransomware

Date/Time	Source	Dest	Destination	Result	Policy
2021/05/01 06:30:29	10.9.16.26		179.60.194.20 (graph-video.f...	✓ 1.06 kB / 402 B	Routing To WAN True Pr...
2021/05/01 06:30:29	172.58.230.149		202.29.60.156	✓ 42 B / 2.53 kB	WAN to SVR-156 (1-5)
2021/05/01 06:30:29	10.9.9.123		208.65.204.203	Deny: policy vio...	Deny SMB-455 To WAN
2021/05/01 06:30:29	10.10.10.132		82.165.254.157 (sf45.starfar...	Deny: policy vio...	Deny SMB-455 To WAN
2021/05/01 06:30:29	10.10.10.132		33.26.162.39	Deny: policy vio...	Deny SMB-455 To WAN
2021/05/01 06:30:29	10.10.10.32		102.45.182.212	Deny: policy vio...	Deny SMB-455 To WAN
2021/05/01 06:30:29	10.10.10.132		170.236.2.87	Deny: policy vio...	Deny SMB-455 To WAN
2021/05/01 06:30:29	199.34.83.133		202.29.60.145	✓ 60 B / 0 B	WAN to SVR-Adicet: 35
2021/05/01 06:30:29	10.9.9.123		212.228.244.145	Deny: policy vio...	Deny SMB-455 To WAN
2021/05/01 06:30:29	45.155.205.54		202.29.60.50		WAN to SVR-cmgc (01
2021/05/01 06:30:29	10.10.10.32		51.111.139.148	Deny: policy vio...	Deny SMB-455 To WAN
2021/05/01 06:30:29	10.9.9.123		185.201.137.119	Deny: policy vio...	Deny SMB-455 To WAN
2021/05/01 06:30:29	10.9.9.123		121.219.71.156	Deny: policy vio...	Deny SMB-455 To WAN
2021/05/01 06:30:29	10.9.9.123		114.133.34.234	Deny: policy vio...	Deny SMB-455 To WAN
2021/05/01 06:30:29	159.203.183.2...		202.29.60.156	✓ 42 B / 2.53 kB	WAN to SVR-156 (1-5)
2021/05/01 06:30:29	10.10.10.132		41.200.190.145	Deny: policy vio...	Deny SMB-455 To WAN
2021/05/01 06:30:29	10.9.9.86		69.171.250.15	Deny: policy vio...	Allow any to SVR-Micro
2021/05/01 06:30:29	10.71.107.107		89.239.254.53	✓ 131 B / 327 B	Admin Group (48)
2021/05/01 06:30:29	10.9.9.123		198.186.240.218	Deny: policy vio...	Deny SMB-455 To WAN

ตรวจสอบการทำงานของ IPS บน Firewall

Date/Time	Severity	Source	Protocol	User	Action	Count
2021/03/22 04:53:30	High	10.71.104.19	6		dropped	
2021/03/22 04:53:06	High	51.104.209.160	6		dropped	
2021/03/22 04:52:57	High	10.1.60.52	6		dropped	
2021/03/22 04:52:41	High	51.104.209.160	6		dropped	
2021/03/22 04:52:11	High	51.104.209.160	6		dropped	
2021/03/22 04:52:01	High	10.71.104.19	6		dropped	
2021/03/22 04:51:57	High	10.1.60.52	6		dropped	
2021/03/22 04:51:45	High	51.104.209.160	6		dropped	
2021/03/22 04:51:30	High	10.71.104.19	6		dropped	
2021/03/22 04:51:17	High	51.104.209.160	6		dropped	
2021/03/22 04:51:00	High	10.1.60.52	6		dropped	
2021/03/22 04:50:53	High	51.104.209.160	6		dropped	
2021/03/22 04:50:28	High	51.104.209.160	6		dropped	
2021/03/22 04:50:06	High	10.1.60.52	6		dropped	
2021/03/22 04:50:05	High	51.104.209.160	6		dropped	
2021/03/22 04:50:01	High	10.71.104.19	6		dropped	
2021/03/22 04:49:39	High	51.104.209.160	6		dropped	
2021/03/22 04:49:30	High	10.71.104.19	6		dropped	
2021/03/22 04:49:14	High	51.104.209.160	6		dropped	
2021/03/22 04:49:09	High	10.1.60.52	6		dropped	

การตรวจสอบ Antivirus บนอุปกรณ์ Firewall

Date/Time	Service	Source	File Name	Virus/Botnet	User	Detail
2021/05/25 14:30:57	HTTP	10.2.4.26	ettm2205.exe	W32/RanumBot.Ultr		URL: http://blinkroast.info/1c4683f0b9f...
2021/05/25 14:28:14	HTTP	10.2.4.22	ww31.exe	W32/Agent.Hltr		URL: http://mysuper.com/1c4683f0b9f...
2021/05/25 14:26:16	HTTP	10.71.104.94	ww31.exe	W32/Agent.Hltr		URL: http://mysuper.com/1c4683f0b9f...
2021/05/25 14:24:58	HTTP	10.71.104.94	ethm2305.exe	W32/RanumBot.Ultr		URL: http://blinkroast.info/1c4683f0b9f...
2021/05/25 14:23:41	HTTP	10.71.101.18	ww31.exe	W32/Agent.Hltr		URL: http://mysuper.com/1c4683f0b9f...
2021/05/25 14:16:26	HTTP	10.2.4.26	ww31.exe	W32/Agent.Hltr		URL: http://mysuper.com/1c4683f0b9f...
2021/05/25 14:15:09	HTTP	10.2.4.26	ettm2205.exe	W32/RanumBot.Ultr		URL: http://blinkroast.info/1c4683f0b9f...
2021/05/25 14:12:34	HTTP	10.2.4.22	ww31.exe	W32/Agent.Hltr		URL: http://mysuper.com/1c4683f0b9f...
2021/05/25 14:10:53	HTTP	10.71.104.94	ww31.exe	W32/Agent.Hltr		URL: http://mysuper.com/1c4683f0b9f...
2021/05/25 14:09:38	HTTP	10.71.104.94	ethm2305.exe	W32/RanumBot.Ultr		URL: http://blinkroast.info/1c4683f0b9f...
2021/05/25 14:07:59	HTTP	10.71.101.18	ww31.exe	W32/Agent.Hltr		URL: http://mysuper.com/1c4683f0b9f...
2021/05/25 14:01:14	HTTP	10.2.4.26	ww31.exe	W32/Agent.Hltr		URL: http://mysuper.com/1c4683f0b9f...
2021/05/25 13:59:13	HTTP	10.2.4.26	ettm2205.exe	W32/RanumBot.Ultr		URL: http://blinkroast.info/c544b71e73...
2021/05/25 13:56:54	HTTP	10.2.4.22	ww31.exe	W32/Agent.Hltr		URL: http://mysuper.com/c544b71e73...
2021/05/25 13:55:31	HTTP	10.71.104.94	ww31.exe	W32/Agent.Hltr		URL: http://mysuper.com/c544b71e73...
2021/05/25 13:54:16	HTTP	10.71.104.94	ethm2305.exe	W32/RanumBot.Ultr		URL: http://blinkroast.info/c544b71e73...
2021/05/25 13:52:38	HTTP	10.71.101.18	ww31.exe	W32/Agent.Hltr		URL: http://mysuper.com/c544b71e73...
2021/05/25 13:45:21	HTTP	10.2.4.26	ww31.exe	W32/Agent.Hltr		URL: http://mysuper.com/c544b71e73...
2021/05/25 13:44:00	HTTP	10.2.4.26	ettm2205.exe	W32/RanumBot.Ultr		URL: http://blinkroast.info/c544b71e73...
2021/05/25 13:41:27	HTTP	10.2.4.22	ww31.exe	W32/Agent.Hltr		URL: http://mysuper.com/c544b71e73...

กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์ (หน่วยงานภาครัฐ และเอกชนภายนอก)

Acer บริษัทยักษ์ใหญ่แห่งวงการคอมพิวเตอร์ถูกโจมตีด้วย REvil ransomware โดยมีกรเรียกค่าไถ่เป็นจำนวนสูงที่สุดเท่าที่เคยมีมา ที่ 50 ล้านดอลลาร์

Happy Blog Auction (new) Blog search Search

Acer Inc.

acer

Acer.com - is a Taiwanese multinational hardware and electronics corporation specializing in advanced electronics technology, headquartered in Xizhi, New Taipei City. Its products include desktop PCs, laptop PCs tablets, servers, storage devices, virtual reality devices, displays, smartphones and peripherals, as well as gaming PCs and accessories under its Predator brand. Acer is the world's 6th-largest PC vendor by unit sales as of January 2021

CUSTOMER_CODE	LINE Customer name	Customer	LINE Credit Limit	CUSTOMER_NAME	CUSTOMER_LOCAL_NAME
2000000000000000000
2000000000000000001
2000000000000000002

Your network has been infected

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - General-Decryptor

Follow the instructions below. But remember that you do not have much time

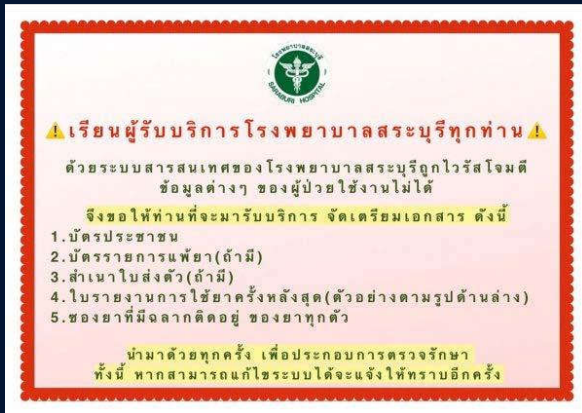
General-Decryptor price
The price is for all PCs of your infected network

You have **8 days, 19:07:29**
* If you do not pay on time, the price will be doubled
* Time ends on **Mar 28, 16:30:11**

Current price	214151 XMR	= 53000,000 USD
After time ends	428302 XMR	= 100,000,000 USD

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

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



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

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

กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์
(ของมหาวิทยาลัยราชภัฏเชียงใหม่)

กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์

เครื่อง Windows Server ถูก Ransomware โจมตีในปี 2020

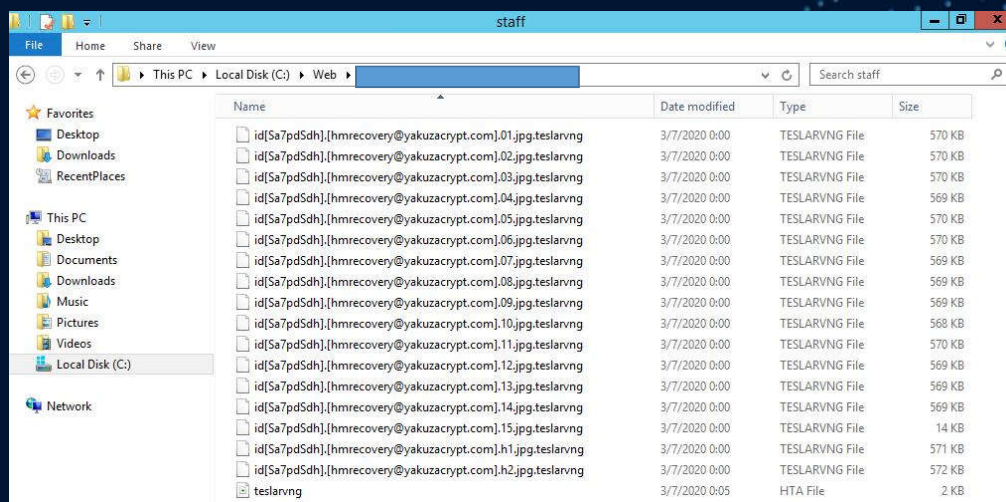
สาเหตุเกิดจาก

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

วิธีการแก้ไข

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

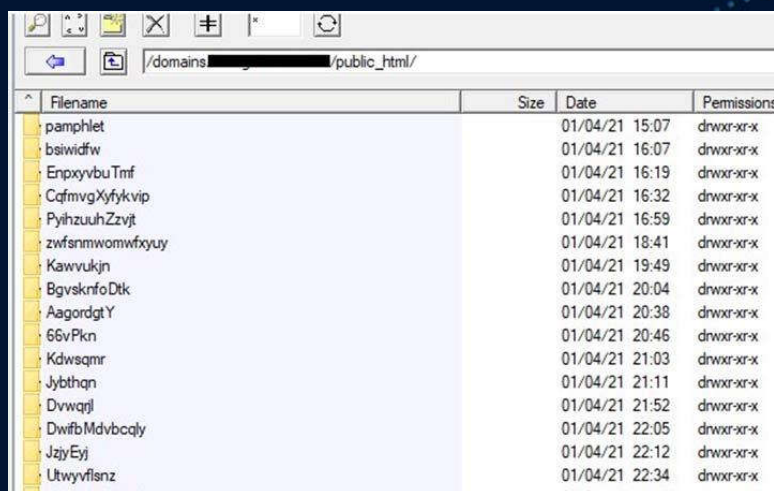
สาเหตุเกิดจาก

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

วิธีการแก้ไข

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

กรณีศึกษา เรื่องการป้องกันการเรียกค่าไถ่ฐานข้อมูลจากอาชญากรรมไซเบอร์

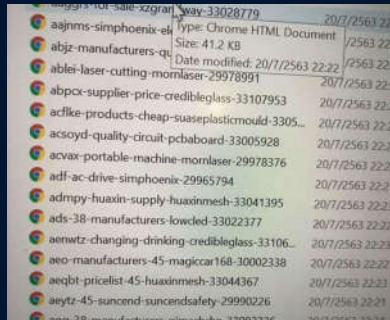


Filename	Size	Date	Permissions
pamphlet		01/04/21 15:07	drwxr-xr-x
bsiwidfw		01/04/21 16:07	drwxr-xr-x
EnpxyvbuTmf		01/04/21 16:19	drwxr-xr-x
CqfmvgXyfykvip		01/04/21 16:32	drwxr-xr-x
PyihzuuhZzvtj		01/04/21 16:59	drwxr-xr-x
zwfsmwomwfxuy		01/04/21 18:41	drwxr-xr-x
Kawvukjn		01/04/21 19:49	drwxr-xr-x
BgvskrfoDtk		01/04/21 20:04	drwxr-xr-x
AagordgtY		01/04/21 20:38	drwxr-xr-x
66vPkN		01/04/21 20:46	drwxr-xr-x
Kdwsqmr		01/04/21 21:03	drwxr-xr-x
Jybthqn		01/04/21 21:11	drwxr-xr-x
Dvwqrl		01/04/21 21:52	drwxr-xr-x
DwifbMdvbcqly		01/04/21 22:05	drwxr-xr-x
JzyEyj		01/04/21 22:12	drwxr-xr-x
Utwyvfisnz		01/04/21 22:34	drwxr-xr-x

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 16:7726:32 ./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 เลื่อนที่มี Crack
8. ผู้ดูแลระบบต้องตรวจสอบความผิดปกติของเครื่อง 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 หรือเบอร์โทรศัพท์ที่ไม่จำเป็น