แนวทางการป้องกันความเสี่ยงจากการบุกรุกโจมตีด้านไซเบอร์ของมหาวิทยาลัยเชียงใหม่

สำนักบริการเทคโนโลยีสารสนเทศ

มหาวิทยาลัยเชียงใหม่

WHAT IS CYBER SECURITY?

The Facts You Need to Know About This Fast-Growing Field

รูปแบบการโจมตี Cyber Security

1. Malware “มัลแวร์” หมายถึงการรูปแบบหนึ่งของซอฟต์แวร์ ที่เป็นอันตรายต่อผู้ที่ได้รับ เช่น ไวรัส และ ransomware “มัลแวร์” จะทำงานก็คือการแฝงตัวเข้ามาในรูปแบบต่างๆ
2. Phishing การปลอมหน้าเวปไซต์ (Phishing) เป็นการปลอมแปลงหรือเปลี่ยนแปลงข้อมูลบนหน้าเวปไซต์ เพื่อให้เกิดการเข้าใจ ผิด หรือเกิดความเสื่อมเสีย และอาจเชื่อมโยงไปสู่การขโมยข้อมูลสำคัญ
3. SQL Injection Attack การโจมตีจากช่องโหว่ของโปรแกรมภาษา SQL เนื่องจากภายในเซิร์ฟเวอร์ของแต่ละองค์กรมักจะรวบรวม “ข้อมูลของลูกค้า” “ข้อมูลส่วนบุคคล” “หมายเลขบัตรเครดิตและระบบการเงิน”
4. Cross-Site Scripting (XSS) การโจมตีแบบ XSS ซึ่งทำงานผ่านการเขียนสคริปต์ข้ามไซต์ โดยจะทำงานคล้ายคลึงกับการโจมตีแบบ SQL แต่จะแตกต่างกันที่ XSS จะไม่สร้างความเสียหายให้กับเว็บไซต์ที่เผยแพร่ข้อมูล
5. Denial of Service (DoS) หรือ Distributed Denial of Service Attack การโจมตีในลักษณะของการสร้างความหนาแน่น (Traffic) ให้กับเครื่องคอมพิวเตอร์ เสมือนมีการทำรายการ (Transaction) จำนวนมาก ทำให้เครื่องคอมพิวเตอร์เกิดความหน่วงช้าจนไม่สามารถทำงานได้
6. Session Hijacking and Man-in-the-Middle Attacks การดักจับข้อความสำคัญในระหว่างการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์กับเครื่องคอมพิวเตอร์แม่ข่ายระยะไกล ถือว่าเป็นการขโมยข้อมูลสำคัญในระหว่างที่มีผู้ใช้งานผ่านเครือข่ายอินเทอร์เน็ต
7. Credential Reuse การแฮกข้อมูลสำคัญเช่นชื่อผู้ใช้งานและรหัสผ่าน เพื่อใช้ตัวตนของเราเข้าสู่ระบบอื่นๆที่

Ransomware ไวรัสเรียกค่าไถ่

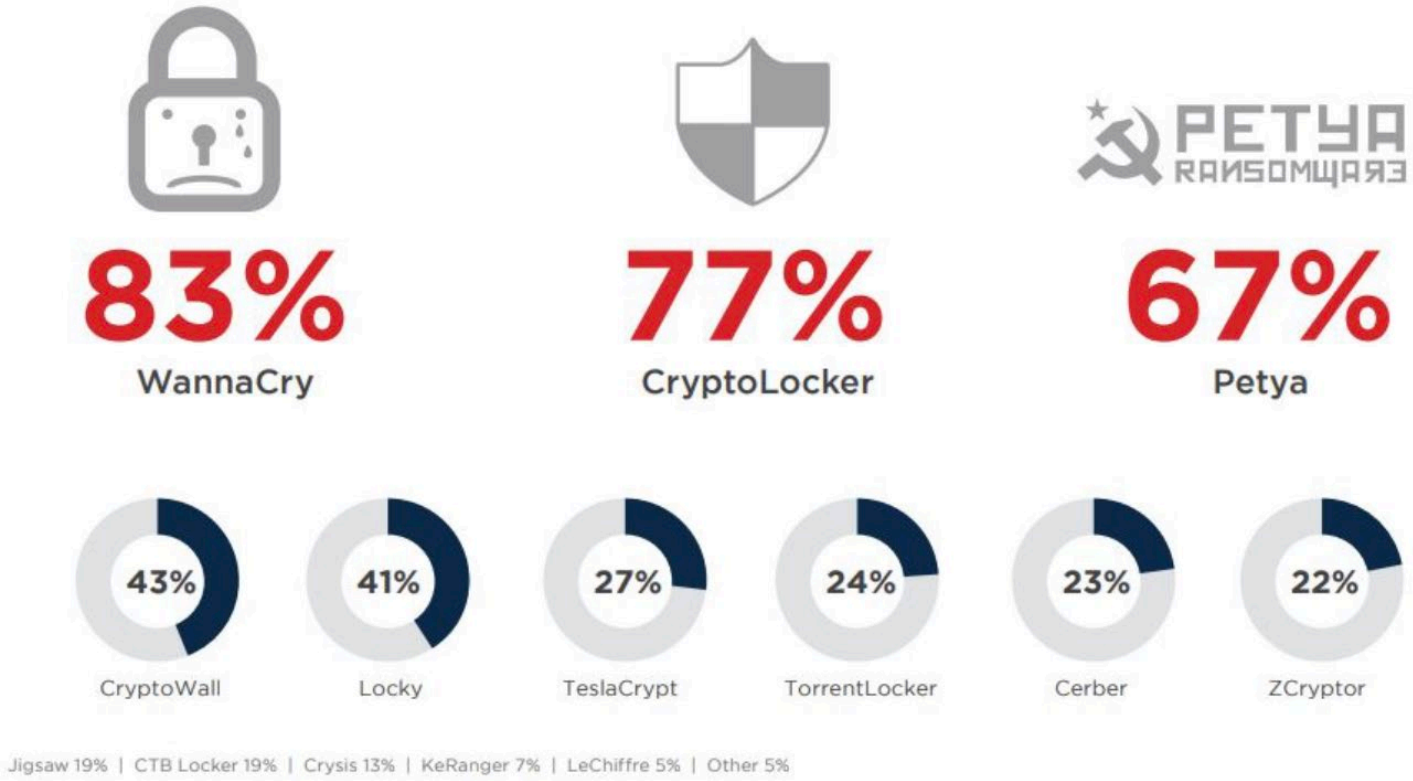
Ransomware หรือ มัลแวร์เรียกค่าไถ่ มีพฤติกรรมคือการ Lock file หรือ encryption file เพื่อไม่ให้เหยื่อเข้าใช้งานไฟล์ที่ถูก Lock ไว้ได้ จากนั้นจะมีข้อความเพื่อทำการเรียกค่าไถ่ข้อมูลที่ได้ Lock ไว้ หากเหยื่อยินยอมจ่ายค่าไถ่แฮกเกอร์ก็จะปลดล็อค และในระยะหลังเริ่มมีการขู่ว่าจะปล่อยข้อมูลสู่สาธารณะ

Ransomware จะแพร่กระจายผ่านทางสแปม หรือฟิชชิ่งอีเมล แต่ยังมีการค้นพบว่า สามารถแพร่กระจายผ่านทางเว็บไซต์ หรือการดาวน์โหลดโดยไดรฟ์เพื่อติดมัลแวร์ดังกล่าวผ่านอุปกรณ์ปลายทาง และการเจาะเครือข่าย เมื่อมัลแวร์เรียกค่าไถ่ได้เข้ามาแล้ว มันจะทำการล็อคไฟล์ทั้งหมดที่สามารถเข้าถึงได้ ปกติจะให้จ่ายเป็น Bitcoins

ประเภทของ Ransomware

Ransomeworm หนอนเรียกค่าไถ่ - มุ่งทำลายข้อมูลและแพร่กระจายตัวไปยังไฟล์คอมพิวเตอร์ในเครื่องของตัวเองและเครื่องคอมพิวเตอร์อื่นๆในระบบเครือข่าย

มัลแวร์เรียกค่าไถ่ที่ส่งผลกระทบมากที่สุด



Ransomware ที่มีอยู่ในปัจจุบัน

- CryptoLocker 2013
- CryptoWall 2014
- CTB-Locker 2014
- TorrenLocker 2014
- Bitcryptor and CoinVault 2015
- TeslaCrypt 2015
- Locky 2017
- WannaCry 2017
- GandCrab 2018
- Petya
- Bad Rabbit
- RYUK
- Sodinokibi
- Phobos
- Globelmposter
- DoppelPaymer
- Mamba
- Snatch
- Dharma
- HiddenTear
- Estemani
- Rapid

ที่มา https://www.bitdefender.co.th/post/ransomware/

ขั้นตอนการเรียกค่าไถ่ Ransomware

1. การติดเชื้อ

หลังจากที่ได้ทำการส่งอีเมลฟิชชิงไปยังระบบแล้ว มัลแวร์เรียกค่าไถ่จะทำการติดตั้งตัวเองบนอุปกรณ์ปลายทางและอุปกรณ์บนเครือข่ายใด ๆ ที่สามารถเข้าถึงได้

2. การแลกเปลี่ยนคีย์ที่ปลอดภัย

มัลแวร์เรียกค่าไถ่จะติดต่อกับคำสั่ง และเซิร์ฟเวอร์สำหรับควบคุม ซึ่งดำเนินการโดยอาชญากรไซเบอร์ ที่อยู่เบื้องหลังการโจมตีเพื่อสร้างคีย์การเข้ารหัส (Cryptographic)

3. ทำการเข้ารหัส

มัลแวร์เรียกค่าไถ่จะเริ่มทำการเข้ารหัสไฟล์ใด ๆ ที่สามารถค้นหาได้ในเครื่อง Local และบน Network

4. ทำการข่มขู่

เมื่อการเข้ารหัสเสร็จสิ้น มัลแวร์เรียกค่าไถ่จะแสดงคำแนะนำสำหรับการจ่ายเงิน โดยจะมีข้อความออกแนวกรรโชกและข่มขู่คุกคามสำหรับการทำลายข้อมูลที่สำคัญของคุณ หากไม่มีการชำระเงินค่าไถ่ (โดยทั่วไปจะให้เหยื่อชำระเป็น Bitcoins) **(1 BTC=333,900 Baht)**

5. ปลดล็อก

หลายองค์กรได้เลือกที่จะทำการจ่ายเงินค่าไถ่ และหวังว่าอาชญากรไซเบอร์นั้น จะทำการถอดรหัสไฟล์ที่ได้รับผลกระทบ (ซึ่งในหลายกรณีนั้นมักไม่เกิดขึ้นจริง) หรือพวกเขาสามารถพยายามกู้คืน โดยการลบไฟล์และระบบที่ติดมัลแวร์เรียกค่าไถ่จากเครือข่าย และกู้คืนข้อมูลจากการสำรองข้อมูล

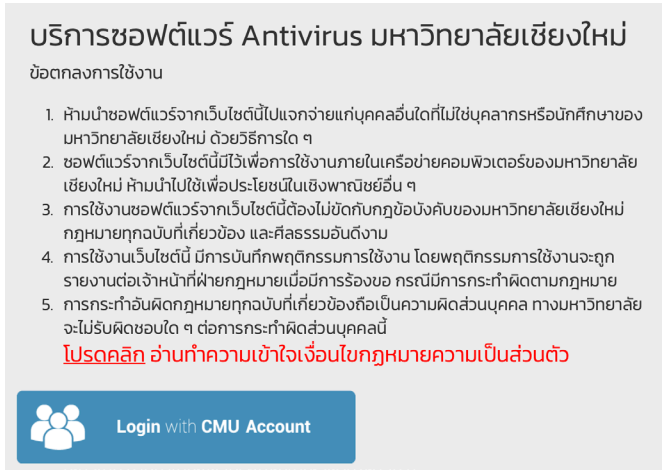
แนวทางการป้องกันและรับมือกับ Ransomware

1. ให้ผู้ดูแลระบบเครื่องแม่ข่ายของแต่ละส่วนงานสำรองข้อมูล (Data Backup) รวมทั้งการทดสอบการกู้คืน
2. ติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) และมัลแวร์ (Malware)
3. วิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามแนวทางการบริหารความมั่นคงปลอดภัย สารสนเทศ ISO/IEC 27001 วางแผนการจัดการที่เหมาะสม
4. สร้างความตระหนักให้บุคลากร และ นักศึกษา เรื่องความมั่นคงปลอดภัยสารสนเทศ ในชีวิตประจำวัน
5. การอัพเดท Patch ของระบบปฏิบัติการให้เป็นปัจจุบัน โดยเฉพาะอย่างยิ่งเครื่องแม่ข่าย และ อุปกรณ์ จัดเก็บข้อมูล
6. ติดตั้ง Firewall กลางของมหาวิทยาลัยหรือติดตั้ง Firewall ของส่วนงาน เพื่อป้องกันการโจมตีจากภายนอก
7. หลีกเลี่ยงการแชร์ข้อมูลแบบ File Sharing หากจำเป็นต้องใช้ File Sharing อัพเดท Patch อย่างสม่ำเสมอ
8. จัดทำแผนรับมือ (Incident Response) และ แผนบริหารความต่อเนื่อง (Business Continuity Plan : BCP) สำหรับการทำงานสำคัญอย่างต่อเนื่องเมื่อระบบขัดข้อง
9. จัดตั้ง Securities Operation Center ในระดับมหาวิทยาลัย เพื่อติดตามสถานการณ์ด้าน ความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย และให้คำแนะนำช่วยเหลือส่วนงานกรณีพบปัญหา การให้ความรู้ด้าน ความมั่นคงปลอดภัยสารสนเทศ จัดทาแนวนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ และตรวจประเมินความมั่นคงปลอดภัยสารสนเทศ

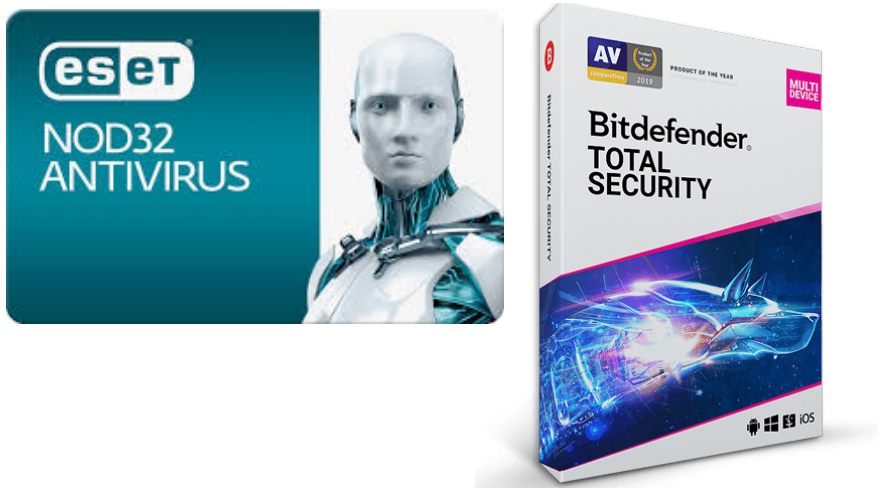
แนวทางการป้องกันและรับมือกับ Ransomware

1

https://antivirus.cmu.ac.th



2



3

Firewall

4

Backup and Recovery Site (DR Site)