RANSOMWARE

stolen everywhere everytime and everything

Ransomeware หรือ Crypto Locker
จอมโจรเรียกค่าไถ่ วายร้ายที่ทำให้เจ้า
ของเครื่องน่าตาไหล กับข้อมูลสำคัญ
ที่ถูกเข้ารหัสลับ
จนไม่มีวันได้กลับมา

ร.อ.จารุกฤษณ์ เรืองสุวรรณ
ศรค.ทสอ.ภท.
charukris.r@mod.go.th

เจ้าวายร้ายเข้ามาในเครื่องเราทางไหนได้บ้างนะ

วิธีการป้องกัน

ใช้ Antivirus และหมั่นอัปเดตอย่างสม่ำเสมอ

ตั้ง PASSWORD ให้มีจำนวนอย่างน้อย 15 ตัวอักษร

เข้าใช้เว็บไซต์ที่เป็น HTTPS เท่านั้น

BACKUP ไฟล์ที่สำคัญไว้ 2 ที่ อย่างน้อยเดือนละ 1 ครั้ง

Ransomware เป็นภัยคุกคามจากเครือข่ายอินเทอร์เน็ตที่กำลังคืบคลานเข้าสู่องค์กร ซึ่งผู้ใช้งานเครื่องคอมพิวเตอร์โดยเฉพาะ Windows สมควรที่จะเรียนรู้และหาทางป้องกัน คำว่า ransom บวกกับคำว่า ware ซึ่งเป็นคำย่อของ software แปลได้ว่า โปรแกรมเรียกค่าไถ่ ซึ่งเป็นมัลแวร์ชนิดหนึ่ง

Ransomware เริ่มเป็นที่รู้จักเมื่อเดือนพฤษภาคม 2548 ซึ่งมีการค้นพบ TROJ_PGPCODER.A โทรจันตัว แรกที่ใช้ประโยชน์การเข้ารหัสลับเพื่อขู่เอาเงินจากผู้ใช้โดยตรง มัลแวร์ชนิดนี้จะทำการเข้ารหัสลับไฟล์บางไฟล์ในคอมพิวเตอร์ ทำให้ผู้ใช้ไม่สามารถเปิดไฟล์นั้นได้จนกว่าจะได้รับตัวถอดรหัสจากเจ้าของมัลแวร์ หมายความว่าเจ้าของไฟล์จะต้องจ่ายเงินค่าไถ่เพื่อให้ไฟล์ที่โดนเข้ารหัสไว้สามารถกลับมาใช้ได้ดังเดิม

ปัจจุบัน CryptoLocker เป็น Ransomware บนระบบปฏิบัติการ Windows ตัวล่าสุดที่ถูกค้นพบเมื่อช่วงเดือนกันยายน 2556 ที่ผ่านมา โดยยังคงถูกเผยแพร่ผ่านทางไฟล์แนบในอีเมลหลอกลวง เช่น อีเมลแจ้งการติดตามพัสดุจาก FedEx, UHS หรือ UPS พร้อมกับแนบไฟล์ ZIP ซึ่งภายในมีไฟล์ EXE ที่ถูกปลอมแปลงว่า

เป็นไฟล์ PDF หรือผ่านทางมัลแวร์ประเภทบอตเน็ตซึ่งหลักการทำงานการไม่แตกต่างจากของอดีตคือ ทำการเข้ารหัสลับข้อมูลไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ และไฟล์ประเภทอื่นๆ ในเครื่องคอมพิวเตอร์ของเหยื่อ จากนั้นจะขึ้นข้อความข่มขู่ให้ผู้ใช้ทำการชำระเงินภายในเวลาที่กำหนด ก่อนที่ข้อมูลทั้งหมดจะไม่สามารถถูกถอดรหัสลับได้อีกตลอดไปทั้งนี้ไม่ใช่เฉพาะข้อมูลในคอมพิวเตอร์ของเหยื่อเท่านั้นที่ถูกเข้ารหัสลับ แต่ข้อมูลที่แชร์ร่วมกันในระบบ เครือข่ายก็ถูกเข้ารหัสลับด้วยเช่นกันในเรื่อง Key สำหรับเข้ารหัสลับ (Encrypt) นั้นได้ใช้ความสามารถของ Crypto API ของ Windows และใช้Encryption Algorithm แบบ RSA ความยาว Key ขนาด 2048 bits ซึ่งหากจะทำการถอดรหัส RSA-2048 ได้โดยไม่ต้องใช้ Key มันเป็นสิ่งที่ยากมากๆรูปแบบการเข้ารหัสนั้นเทียบเคียงกับการเข้ารหัสของธนาคารหรือหน่วยงานความมั่นคงของประเทศ

ขั้นตอนการเข้ารหัสเริ่มต้นจากการค้นหาไพล์ ที่เป็นเป้าหมาย จากนั้นก็ใส่ Encrypt file ในเครื่องเป้าหมาคือไฟล์เอกสารและรูปภาพ ขั้นตอนสุดท้ายคือ การทิ้งจดหมายเรียกค่าไถ่ไว้ให้เหยื่อ

โดยจ่ายเงินผ่านทาง Bitcoin เท่านั้นโดยจะระบุห้วงเวลาเพื่อเป็นการบังคับหากเลยห้วงเวลาดังกล่าวจะไม่สามารถถอดรหัสได้ นั้นหมายถึงไม่สามารถกู้ข้อมูลกลับมาได้เลย

วิธีป้องกัน

1. ควรทำการ Backup ข้อมูล หากจะใช้ External Harddisk ในการ Backup ควรถอดสายออกจากเครื่อง คอมพิวเตอร์โดยทันทีหลังจากการสิ้นสุดการ Backup

2. ในหน่วยงานที่มี NAS หรือ File sharing ต้องแยกที่เก็บ Files ออกจากกันในแต่ละ Users ไม่เช่นนั้น หากเกินมีการโดย RansomWare โจมตี จะโดนเข้ารหัส File ทั้งหมด ซึ่งจะก่อให้เกิดปัญหาต่อองค์กรเป็นอย่างมาก

3. ควรตรวจสอบ Files ที่จะทำการ Download ไม่ว่าจะมาจาก Website หรือ Email โดยเข้าไป website www.VirusTotal.com เพื่อนำ file ดังกล่าวมาทำการทดสอบเพื่อความปลอดภัย https://www.virustotal.com