สำนักส่งเสริมการเคารพสิทธิมนุษยชน
เลขรับ 1252
วันที่ 15 ก.ย. 2563
เวลา 14.49

บันทึกข้อความ

ส่วนราชการ สำนักดิจิทัลสิทธิมนุษยชน กลุ่มงานพัฒนาระบบสารสนเทศและฐานข้อมูล โทร. ๑๓๘๘๕

ที่ สม ๐๐๐๙/ว ๔๐๓ **วันที่** ๑๕ กันยายน ๒๕๖๓

เรื่อง แจ้งแนวทางการป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware)

เรียน
- ☐ เลขาธิการคณะกรรมการสิทธิมนุษยชนแห่งชาติ
- ☐ รองเลขาธิการฯ (นางสาวรตญา กอบศิริกาญจน์)
- ☐ รองเลขาธิการฯ (นางสาวอัจฉรา ฉายากุล)
- ☐ รองเลขาธิการฯ (นายอัญญะรัฐ เอ่งฉ้วน)
- ☐ ที่ปรึกษาสำนักงานฯ (นางหรรษา บุญรัตน์)
- ☐ ที่ปรึกษาสำนักงานฯ (นางสาวชุลีพร เดชขำ)
- ☐ ผู้ช่วยเลขาธิการฯ (นายคมสรรค์ เมธีกุล)
- ☐ ผู้อำนวยการสำนักบริหารกลาง
- ☐ ผู้อำนวยการสำนักกิจการ กสม.
- ☐ ผู้อำนวยการสำนักคุ้มครองสิทธิมนุษยชน
- ☑ ผู้อำนวยการสำนักส่งเสริมการเคารพสิทธิมนุษยชน
- ☐ ผู้อำนวยการสำนักเฝ้าระวังและประเมินสถานการณ์ฯ
- ☐ ผู้อำนวยการสำนักมาตรฐานและติดตามการคุ้มครองฯ
- ☐ ผู้อำนวยการสำนักสิทธิมนุษยชนระหว่างประเทศ
- ☐ ผู้อำนวยการสำนักกฎหมาย
- ☐ ผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชน
- ☐ ผู้อำนวยการหน่วยตรวจสอบภายใน

ด้วยขณะนี้ได้มีมัลแวร์เรียกค่าไถ่ (Ransomware) ได้แพร่ระบาดและสร้างความเสียหายอย่างร้ายแรงต่อข้อมูลอิเล็คทรอนิกส์ของหน่วยงานรัฐหลายแห่ง เช่น โรงพยาบาลของรัฐ โดยมัลแวร์ดังกล่าวจะมีลักษณะการทำงานที่จะเข้ารหัสหรือล็อคไฟล์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วีดีโอ ทำให้ผู้ใช้งานจะไม่สามารถเปิดหรือเข้าถึงไฟล์เหล่านั้นได้ เพื่อผู้ใช้จะต้องทำการจ่ายเงินเพื่อปลดล็อคกู้ข้อมูลคืนมา

ในการนี้ เพื่อเป็นการป้องกันปัญหาและผลกระทบจากมัลแวร์เรียกค่าไถ่ (Ransomware) สำนักดิจิทัลสิทธิมนุษยชนจึงได้จัดทำแนวทางการป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) และ Infographic เพื่อเป็นแนวทางให้ผู้บริหารและเจ้าหน้าที่สำนักงาน กสม. ปฏิบัติและระมัดระวังในการเปิดไฟล์จากอีเมลหรือโปรแกรมแปลกปลอม รวมถึงการสำรองข้อมูลที่สำคัญ หากมีข้อสงสัยหรือปัญหาเกี่ยวกับข้อมูลของมัลแวร์ดังกล่าว โปรดติดต่อนายวณัท รุจนันตกุล นักวิชาการคอมพิวเตอร์ชำนาญการ โทร. ๑๓๘๘๔ หรือนายนพดล คงสมฤทธิ์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ โทร. ๑๑๙๙๐

จึงเรียนมาเพื่อโปรดทราบ

(นางสาวอังคณา สังข์ทอง)
ผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชน

เรียน ผช.
- ☐ เพื่อทราบ ☐ ดำเนินการ
- ☑ อื่นๆ แจ้งเวียน

(นายนรอรรจน์ สุนทรพุกก์)
ผู้อำนวยการสำนักส่งเสริมการเคารพสิทธิมนุษยชน
15 ก.ย. 2563

แนวทางการป้องกัน
มัลแวร์เรียกค่าไถ่ (Ransomware)

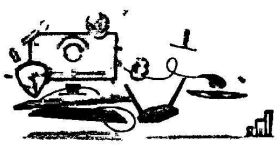
Ransomware

เป็นมัลแวร์ (Malware) ประเภทหนึ่งที่มีลักษณะการทำงานที่แตกต่างกับมัลแวร์ประเภทอื่น ๆ คือไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของผู้ใช้งานแต่อย่างใด แต่จะทำการเข้ารหัสหรือล็อกไฟล์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใด ๆ ได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อค เพื่อกู้ข้อมูลคืนมาผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ "เรียกค่าไถ่" ที่ปรากฏ โดยข้อมูลหรือข้อความ "เรียกค่าไถ่" จะแสดงขึ้นหลังไฟล์ถูกเข้ารหัสเรียบร้อยแล้ว จำนวนเงินค่าไถ่ก็จะแตกต่างกันไป และการชำระเงินจะต้องชำระผ่านระบบที่มีความยากต่อการตรวจสอบหรือติดตาม เช่น การโอนเงินผ่านทางอิเล็กทรอนิกส์, Paysafecard หรือ Bitcoin เป็นต้น แต่อย่างไรก็ตามการชำระเงินก็ไม่ได้หมายความว่าผู้ไม่หวังดีจะส่งคีย์ที่ใช้ในการปลดล็อคไฟล์ให้กับผู้ใช้งาน

วิธีป้องกัน Ransomware

สำรองข้อมูล (Backup) เป็นประจำ

หากผู้ใช้งานติด Ransomware อย่างน้อยถ้ามีการสำรองข้อมูล (Backup) ก็จะสามารถกู้คืนไฟล์ของคุณได้ และเพื่อป้องกันข้อมูลที่ Backup ถูกเข้ารหัสไปด้วย ผู้ใช้งานควรสำรองข้อมูลลงบนอุปกรณ์สำหรับจัดเก็บข้อมูลภายนอกเครื่องข่าย (Cloud Storage, External Hard Drive, USB Flash Drive)



อัปเดตซอฟต์แวร์ในเครื่องอย่างสม่ำเสมอ

การอัปเดตระบบปฏิบัติการและซอฟต์แวร์จะช่วยป้องกันการโจมตีที่ต้องอาศัยช่องโหว่ของซอฟต์แวร์ได้ โดยเฉพาะอย่างยิ่งใน Adobe Flash, Microsoft Silverlight และเว็บบราวเซอร์ ควรติดตามและอัปเดตให้เป็นเวอร์ชั่นปัจจุบัน

ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) ลงบนเครื่องคอมพิวเตอร์

SOPHOS

เพื่อป้องกันการเข้าถึงเว็บไซต์ที่เป็นอันตรายและตรวจสอบไฟล์ทั้งหมดที่ถูกดาวน์โหลด ควรมีการติดตั้งโปรแกรมป้องกันมัลแวร์ลงบนเครื่องคอมพิวเตอร์ไว้ด้วย สำหรับของสำนักงาน กสม. มีโปรแกรม Antivirus Sophons สามารถป้องกัน Ransomware โปรดตรวจสอบในเบื้องต้น ว่ามีการติดตั้งในเครื่องของท่านหรือไม่ และมีการอัพเดทข้อมูลเป็นปัจจุบันหรือไม่ หากไม่โปรดติดต่อเจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชนให้ดำเนินการได้

ตรวจสอบอีเมลที่เป็นอันตรายเบื้องต้น

SPAM

ผู้ไม่หวังดีมักใช้อีเมลเป็นช่องทางในการหลอกลวงผู้ใช้งานให้หลงเชื่อเปิดหรือดาวน์โหลดเอกสารแนบ ดังนั้นเมื่อเราได้รับอีเมลควรตรวจสอบอีเมลฉบับนั้นให้ดีเสียก่อน

หากเจ้าหน้าที่ท่านใดพบการติด Ransomware ให้ปิดเครื่องและแจ้งเจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชนโดยทันที เบอร์โทรติดต่อ 02-1413884 หรือ 02-1411990

แนวทางการป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware)

Ransomware **เป็นมัลแวร์** (Malware) ประเภทหนึ่งที่มีลักษณะการทำงานที่แตกต่างกับมัลแวร์ประเภทอื่นๆคือไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของผู้ใช้งานแต่อย่างใด แต่จะทำการเข้ารหัสหรือล็อกไฟล์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใดๆได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ "เรียกค่าไถ่" ที่ปรากฏ โดยข้อมูลหรือข้อความ "เรียกค่าไถ่" จะแสดงขึ้นหลังไฟล์ถูกเข้ารหัสเรียบร้อยแล้ว จำนวนเงินค่าไถ่ก็จะแตกต่างกันไป และการชำระเงินจะต้องชำระผ่านระบบที่มีความยากต่อการตรวจสอบหรือติดตาม เช่น การโอนเงินผ่านทางอิเล็กทรอนิกส์, Paysafecard หรือ Bitcoin เป็นต้น แต่อย่างไรก็ตามการชำระเงินก็ไม่ได้หมายความว่าผู้ไม่หวังดีจะส่งคีย์ที่ใช้ในการปลดล็อคไฟล์ให้กับผู้ใช้งาน

ช่องทางการแพร่กระจายของ Ransomware

1. แฝงมาในรูปแบบเอกสารแนบทางอีเมลในกรณีส่วนใหญ่ Ransomware จะมาในรูปแบบเอกสารแนบทางอีเมล โดยอีเมลผู้ส่งก็มักจะเป็นผู้ให้บริการที่เรารู้จักกันดี เช่น ธนาคาร และจะใช้หัวข้อหรือประโยคขึ้นต้นที่ดูน่าเชื่อถืออย่าง "Dear Valued Customer", "Undelivered Mail Returned to Sender", "Invitation to connect on LinkedIn." เป็นต้น ประเภทของไฟล์แนบที่เห็นก็จะเป็น ".doc" หรือ ".xls" ผู้ใช้อาจจะคิดว่าเป็นไฟล์เอกสาร Word หรือ Excel ธรรมดาแต่เมื่อตรวจสอบชื่อไฟล์เต็ม ๆ ก็จะเห็นนามสกุล .exe ซ่อนอยู่ เช่น "Paper.doc.exe" แต่ผู้ใช้จะเห็นเฉพาะ "Paper.doc" และทำให้เข้าใจผิดว่าเป็นไฟล์ที่ไม่เป็นอันตราย

2. แฝงตัวมาในรูปแบบของ Malvertising (โฆษณา) Ransomware นี้อาจจะมาในรูปแบบของโฆษณา ไม่ว่าจะเป็นโฆษณาที่ฝังมากับซอฟต์แวร์หรือตามหน้าเว็บไซต์ต่าง ๆ เชื่อมโยงไปยังเว็บไซต์อันตรายและอาศัยช่องโหว่ของซอฟต์แวร์ ผู้ใช้ยังสามารถกลายเป็นเหยื่อได้โดยไม่ได้ตั้งใจเพียงเข้าเยี่ยมชมหน้าเว็บที่ถูกผู้ไม่หวังดีเข้ามาควบคุม ตัวอย่างเช่น ถูกดาวน์โหลดโค้ด (Code) ที่เป็นอันตรายผ่านทางโฆษณาแบนเนอร์ใน Flash โดย Ransomware มักจะใช้ประโยชน์จากข้อบกพร่องหรือช่องโหว่ด้านความปลอดภัยอื่น ๆ ในเบราว์เซอร์, แอพลิเคชั่น หรือ ระบบปฏิบัติการ บ่อยครั้งก็มักจะเกิดจากช่องโหว่ในเว็บเบราว์เซอร์, Java และ PDF แต่ช่องโหว่ที่พบมากที่สุดก็คือใน Flash

วิธีป้องกัน Ransomware

1. ทำการสำรองข้อมูล (Backup) เป็นประจำ หากผู้ใช้งานติด Ransomware อย่างน้อยถ้ามีการสำรองข้อมูล (Backup) ก็จะสามารถกู้คืนไฟล์ของคุณได้ และเพื่อป้องกันข้อมูลที่ Backup ถูกเข้ารหัสไปด้วย ผู้ใช้งานควรสำรองข้อมูลลงบนอุปกรณ์สำหรับจัดเก็บข้อมูลภายนอกเครือข่าย (Cloud Storage, External Hard Drive, USB Flash Drive)

2. อัปเดตซอฟต์แวร์ในเครื่องอย่างสม่ำเสมอ การอัพเดทระบบปฏิบัติการและซอฟต์แวร์จะช่วยป้องกันการโจมตีที่ต้องอาศัยช่องโหว่ของซอฟต์แวร์ได้ โดยเฉพาะอย่างยิ่งใน Adobe Flash, Microsoft Silverlight และเว็บเบราว์เซอร์ ควรติดตามและอัปเดตให้เป็น Version ปัจจุบัน

3. ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) ลงบนเครื่องคอมพิวเตอร์ เพื่อป้องกันการเข้าถึงเว็บไซต์ที่เป็นอันตรายและตรวจสอบไฟล์ทั้งหมดที่ถูกดาวน์โหลด ควรมีการติดตั้งโปรแกรมป้องกันมัลแวร์ลงบนเครื่องคอมพิวเตอร์ไว้ด้วย สำหรับของสำนักงาน กสม. มีโปรแกรม Antivirus Sophons สามารถป้องกัน Ransomware ได้โปรดตรวจสอบในเบื้องต้นว่ามีการติดตั้งในเครื่องของท่านหรือไม่ และมีการอัพเดทข้อมูลเป็นปัจจุบันหรือไม่ หากไม่มีโปรดติดต่อเจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชน

4. ตรวจสอบอีเมลที่เป็นอันตรายเบื้องต้น ผู้ไม่หวังดีมักใช้อีเมลเป็นช่องทางในการหลอกลวงผู้ใช้งานให้หลงเชื่อเปิดหรือดาวน์โหลดเอกสารแนบ ดังนั้นเมื่อเราได้รับอีเมลควรตรวจสอบอีเมลฉบับนั้นให้ดีเสียก่อน

หากพบการติด Ransomware

<u>หากเจ้าหน้าที่ท่านใดพบการติด Ransomware ให้ปิดเครื่องและแจ้งเจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชนโดยทันที เบอร์โทรติดต่อ 02-1411384 หรือ 02-1411990</u>

ที่มา: Ransomware คืออะไร? : it.chula

Defending Against Crypto-Ransomware: Netwrix Corporation

Ransomware Definition: Trend Micro