ข้อปฏิบัติตัวเมื่อคิดว่าเครื่องคอมพิวเตอร์โดน Ransomware โจมตี

เราจะรู้ได้อย่างไรว่าเราโดนโจมตี

Ransomware ที่ระบาดอยู่ในปัจจุบันนั้นมีชื่อว่า WannaCry Version 2.0 ซึ่งพบว่า Ransomware ตัวนี้มีความอันตรายต่อระบบเครือข่ายในปัจจุบันมาก เนื่องจาก Ransomware ตัวก่อนหน้า จะแพร่กระจายลงสู่ระบบคอมพิวเตอร์ของเราก็ต่อเมื่อเราได้รับอีเมล์ Ransomware จากผู้โจมตี แล้วเราเผลอไปดับเบิ้ลคลิกเพื่อเปิดไฟล์มัน มันก็จะแพร่กระจายลงในระบบคอมพิวเตอร์ของเราในทันที

แต่!!!! Ransomware WannaCry Version 2.0 มีความร้ายกาจ และ อันตรายมากตรงที่ WannaCry Version 2.0 จะโจมตีได้ถึง 2 ช่องทาง คือ

1. โจมตีผ่านทางอีเมล์เช่น Ransomware ตัวเดิมๆ จะแพร่กระจายลงสู่ระบบคอมพิวเตอร์ของเราก็ต่อเมื่อเราได้รับอีเมล์ Ransomware จากผู้โจมตี แล้วเราเผลอไปดับเบิ้ลคลิกเพื่อเปิดไฟล์มัน มันก็จะแพร่กระจายลงในระบบคอมพิวเตอร์ของเราในทันที
2. โจมตีผ่านทางช่องโหว่ของระบบปฏิบัติการ Windows ผ่าน Port SMVb1 ผู้โจมตีจะทำการ Run Scan Port เครื่องเป้าหมาย หลังจากนั้นผู้โจมตีจะทำการฝัง Script ลงในเครื่องคอมพิวเตอร์ของเป้าหมาย หลังจากนั้นเจ้าตัว WannaCry Version 2.0 ก็จะทำการแพร่กระจายตัวเองโดยอัตโนมัติลงในระบบคอมพิวเตอร์ในทันที โดยที่ผู้ใช้งานยังไม่ทันรู้ตัวด้วยซ้ำ กว่าจะรู้ตัวอีกทีก็โดนเล่นงานไปหมดทั้งเครื่องแล้ว และ ที่สำคัญคือเจ้าตัว WannaCry Version 2.0 สามารถแพร่กระจายเข้าไปภายในระบบเครือข่ายภายในไปยังเครื่องคอมพิวเตอร์อื่นๆ ที่ต่อระบบเครือข่ายอยู่ในวงเดียวกันได้อีกด้วย

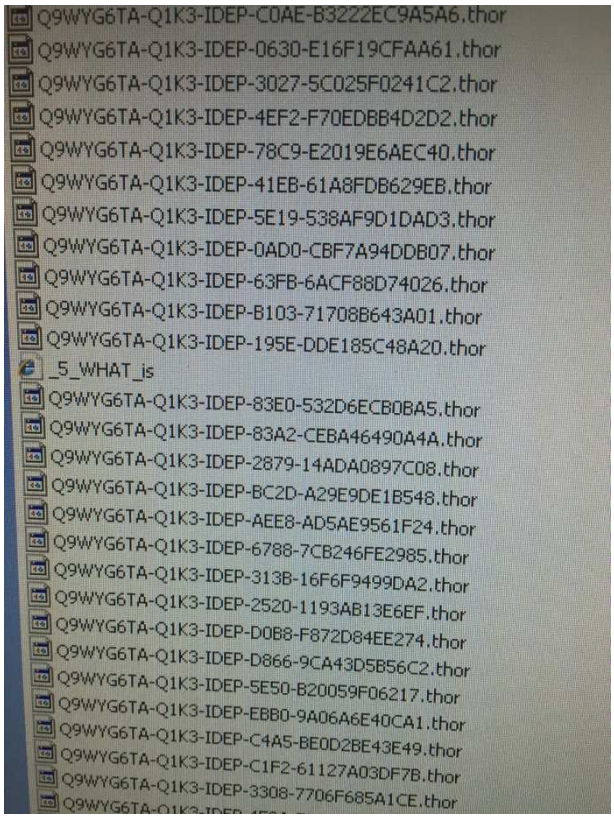
เป็นการยากที่จะล่วงรู้ถึงการโจมตีของ Malware ตัวนี้ เพราะทันทีที่เราทำการคลิกเพื่อเปิดไฟล์แนบที่มี Malware แฝงอยู่ เจ้าตัว Malware ตัวนี้ก็จะทำการโจมตีข้อมูลภายในเครื่องเราแบบเงียบๆ กว่าที่เราจะรู้ตัวก็อาจจะโดน Malware ตัวนี้โจมตีไฟล์เอกสารของเราจนครบทุกไฟล์แล้ว

ดังนั้นขอสรุปวิธีการสังเกตุเบื้องต้นไว้ 2 วิธี ดังนี้

1. หากเราพลาดไปเปิดไฟล์แปลกๆ ที่แฝงมากับ Email หรือ Website แล้วนั้น เราจะรู้สึกว่าเครื่องจะหน่วงๆ เข้าใช้งานโปแกรมต่างๆ ได้ค่อนข้างช้ามาก แต่วิธีนี้ก็ใช้ได้ไม่เสมอไป เพราะบางครั้งที่เครื่องช้าอาจจะเกิดจากสภาพเครื่องที่เก่า, Spec. เครื่องต่ำ หรือ อาจจะเกิดจากที่เราได้เปิดหลายๆ โปรแกรม พร้อมๆ กัน ก็จะทำให้เกิดอาการแบบนี้ได้ เช่นกัน

2. ไฟล์งานของเราเริ่มกลายร่าง เช่นพวกไฟล์งาน Word, Excel จากที่เป็นไอคอนปกติ

 ก็อาจจะกลายร่างมาเป็นไอคอนแปลกๆ ได้  และชื่อไฟล์งานก็จะเปลี่ยน และ มีนามสกุลไฟล์งานเปลี่ยนเป็น .THOR หรือนามสกุลอื่นๆ ที่มีไอคอนเปลี่ยนไป ก็แสดงว่าเครื่องของเราได้ถูก Ransomware โจมตีแล้ว



3. ที่หน้าจอของเราจะขึ้นหน้าต่างใหม่ขึ้นมา ดังรูปด้านล่าง

สิ่งที่เราต้องดำเนินการเมื่อรู้ตัวว่าถูกโจมตี

หากเรารู้ตัวว่าเครื่องของเราได้โดนเจ้า Ransomware โจมตี เราต้องรีบดำเนินการ ดังต่อไปนี้

1. รีบปิดเครื่องคอมพิวเตอร์ของเราในทันที โดยการปิดที่เครื่องสำรองไฟ (UPS) ได้เลย โดยที่ไม่ต้องรอทำการ Shutdown เครื่องตามระบบ

2. รีบถอดสาย เชื่อมต่อระบบเครือข่าย (LAN) ที่อยู่ด้านหลังเครื่อง โดยทันที เพราะ เจ้าตัว Ransomware อาจจะกระจายไปโจมตีที่ File Share Server ได้

3. โทรแจ้งไอทีเพื่อรับการตรวจสอบ เพราะหากเรารู้ตัวเร็ว และ ปิดเครื่องได้เร็ว ทางไอที จะสามารถถอดตัวเก็บข้อมูลที่อยู่ภายในเครื่อง มาต่อกับเครื่องอื่น แล้วทำการ Copy ไฟล์ที่ยังไม่โดน Ransomeware มาใช้งานได้

4. หากยังไม่ได้รับการตรวจสอบจากทางไอที ห้ามเปิดเครื่องคอมพิวเตอร์ที่โดนโจมตีเป็นอันขาด

วิธีป้องกันไม่ให้ติดมัลแวร์ Ransomware

1. หากเจอเมลที่เราไม่รู้จัก ไม่ควรคลิกเปิดอ่านและควรลบจดหมายทิ้งทันที

2. หากเจออีเมล์ต้องสงสัยให้ทำการฟอร์เวิร์ดอีเมล์มาที่ it@hansarsamui.com เพื่อทำการตรวจสอบก่อนที่จะคลิกใช้งาน

3. หากเจอเมลที่สงสัย ให้เอาเมาส์มาชี้ที่ปุ่ม แล้วสังเกต **url** ว่ามันลิงค์ไปที่ใด บริเวณด้านมุมซ้ายล่าง ถ้าไปเว็บแปลกๆ ไม่ควรคลิกซ้ายเพื่อเปิดไฟล์ และควรสแกนลิงค์ผ่านทางเว็บ www.virustotal.com เพื่อตรวจสอบว่าเป็นมัลแวร์หรือไม่

4. แนะนำให้พนักงานเก็บไฟล์งานไว้ที่ Share Drive เนื่องจากระบบ Share Drive ของเราได้ทำระบบสำรองข้อมูลไว้ 2 ชั้น (Online & Offline) จึงทำให้ค่อนข้างปลอดภัยกว่าการเก็บไว้ในเครื่องคอมพิวเตอร์ของตนเอง

นายทวินันท์ วิริยะนานนท์

IT Manager

29 พฤษภาคม 2562