9 ประเภทของวายร้ายมัลแวร์

มัลแวร์ (Malware) ย่อมาจากคำว่า Malicious Software โดยเราจะอธิบายคำว่ามัลแวร์ว่าคือโปรแกรมที่ถูกสร้างขึ้นมาเพื่อประสงค์ร้ายต่อเครื่องคอมพิวเตอร์และเพื่อขโมยข้อมูล หรือ หลบเลี่ยงการตรวจสอบในการเข้าถึงระบบ หรือพยายามทำให้เครื่องที่ติดตั้งซอฟต์แวร์เสียหาย ในเบื้องต้นสามารถแยกเป็นประเภท ได้ 9 ประเภทด้วยกัน คือ

1. **Adware (แอดแวร์)** เป็นศัพท์เทคนิคมาจากคำว่า Advertising Supported Software ซึ่งเป็นมัลแวร์ประเภทหนึ่งที่เมื่อติดตั้งแล้ว มักจะมีโฆษณาอยู่ในตัวโปรแกรมเลย หรือบางครั้งก็เรียกเปิดหน้าเว็บเพื่อป๊อปอัพขึ้นมาโดยอัตโนมัติ (ไม่ต้องคลิก) ตัวอย่างเช่น ถ้าเราลองไปดาวน์โหลดโปรแกรมฟรีตามเว็ปต่าง ๆ เราก็จะเห็นโฆษณาสินค้าปรากฏขึ้นมาบ่อย ๆ ถ้าเราอยากให้โฆษณานั้นหายไป ก็ต้องจ่ายตังค์ค่าลิขสิทธิ์ เพื่อไม่ให้มีโฆษณาขึ้นมากวนใจอีกต่อไป

   อาการของเครื่องที่ติด Adware

   1. หน้าหลักของเบราว์เซอร์เปลี่ยนไปเป็นเว็บที่เราไม่รู้จัก

   2. หน้าเว็บอาจมีป้ายโฆษณา pop-up เล็กๆ ปรากฏขึ้นมา

   3. ในคอมพิวเตอร์จะมีโปรแกรมแปลกๆโผล่มาโดยที่เราไม่รู้จัก

   4. มีแถบ Tool bar แปลกๆโผล่มาในเว็บเบราว์เซอร์

   วิธีป้องกัน Adware

   - ดาวน์โหลดโปรแกรมจากเว็บไซต์ของผู้พัฒนา หรือเว็บไซต์ที่น่าเชื่อถือได้
   - หลีกเลี่ยงการใช้โปรแกรมประเภท Crack ที่ละเมิดลิขสิทธิ์
   - อ่านรายละเอียดของโปรแกรมที่จะติดตั้งให้ละเอียดทั้งก่อนและขณะติดตั้ง เพราะมีบางกรณีที่เราสามารถกดเลือกไม่เอาโปรแกรม Adware ที่แถมมาได้

2. **Bot** เป็นคำที่ย่อมาจากคำว่า “Robot” ซึ่งเป็นโปรแกรมที่ทำงานในลักษณะที่เรียกว่า Agent โดยจะรอคำสั่งจากเครื่องหรือโปรแกรมอื่นที่สั่งหรือปลุกให้เครื่องที่มี Bot ติดตั้งอยู่ทำงาน ถ้าเครื่อง ของเราถูก Bot ติดเข้าไป เครื่องของเราก็จะถูกโปรแกรมหรือบุคคลอื่น ๆ สั่งงานให้ทำงานอย่างใด อย่างหนึ่งตามเจ้านายหรือบุคคลสั่ง

   การกำจัด Bot

   - Remove แบบ Manual โดยการลบและแก้ไขค่าต่าง ๆ ที่ Registry การใช้เครื่องมือ เข้ามาช่วยดักจับพวก Bot หรือ Malware ต่างๆ โดยเครื่องมือเหล่านี้จะเป็นส่วนที่เข้าเสริมการทำงาน ในการตรวจจับ

   * แต่วิธีป้องกันที่ดี เราไม่ควรไป Download โปรแกรมหรือเข้าเว็บไซต์ที่ไม่ปลอดภัย

3. **Bug** คำคุ้นหูของโปรแกรมเมอร์ ที่เกิดมาจากความผิดพลาดของโปรแกรมเมอร์ หรือแม้กระทั่งความผิดพลาดของผู้ใช้งานระบบ จนเป็นช่องโหว่ให้แฮกเกอร์เข้าไปโจมตีระบบได้ นอกจากปัญหาเกี่ยวกับโปรแกรมแล้ว อาจเป็นปัญหาเกี่ยวกับตัวเครื่องก็ได้ บางทีคนเขียนโปรแกรมอาจจงใจทำไว้ หรืออาจไม่ได้ตั้งใจก็ได้ เมื่อเกิด bug ในโปรแกรมขึ้นมาสร้างปัญหากวนใจ เราจะใช้การ debug หรือการตรวจสอบแก้ไขจุดบกพร่องของโปรแกรม การสั่งให้โปรแกรมทำการ Debug นั้นก็คือให้โปรมแกรมสามารถทำงานได้เป็นปกติเหมือนเดิม
4. **Ransomware** มัลแวร์ประเภทนี้จะทำการเข้ารหัสไฟล์ให้ไม่สามารถเปิดใช้งานได้ ซึ่งถ้าต้องการให้สามารถใช้งานได้อีกครั้งจำเป็นต้องจ่ายเงินค่าไถ่ให้กับเหล่าแฮกเกอร์เพื่อถอดรหัสไฟล์เหล่านั้น

   ขั้นตอนการทำงานของ Ransomware

   - พยายามแพร่กระจายผ่านเว็บไซด์ต่างๆ, แนบไฟล์ไปใน email
   - เมื่อผู้ใช้งานเปิดใช้งานจะสร้าง service และฝังการทำงานของ service ไปยัง Registry ของเครื่อง เพื่อให้ทำงานทุกครั้งเมื่อมีการเปิดเครื่อง

- Ransomware ติดต่อกลับไปยังเครื่อง C&C Server(Command and Control Server) ของแฮกเกอร์เพื่อ download key สำหรับการเข้ารหัสและ config ต่างๆของภายใน Ransomware พร้อมทั้งลงทะเบียนกับ C&C Server เพื่อระบุว่าเครื่องที่ติดอยู่ที่ใด
- นำ Key และ config ที่ได้รับจาก C&C Server มาเข้ารหัสเอกสารข้อมูลต่างๆภายในเครื่อง
- แสดงหน้าข่มขู่ผู้ใช้งานพร้อมกับบอก link สำหรับวิธีการโอน Bitcoin ไปให้กับแฮกเกอร์

วิธีการป้องกัน Ransomware

- ไม่ download file จาก email หรือเว็บไซด์ใดๆที่ไม่น่าเชื่อถือ
- Scan file ใดๆก็แล้วแต่ที่ถูกส่งมาใน email หรือที่ download จากเว็บไซด์ใดๆ ด้วย Antivirus ก่อนใช้งาน หรือหากไม่สะดวกในการใช้งาน Antivirus ให้ทำการ upload ไฟล์เหล่านั้นไปยังเว็บไซด์สำหรับการตรวจสอบ malware เช่น www.virustotal.com, analysis.avira.com เป็นต้น
- ปิดการเข้าใช้งานเว็บไซด์ต่างๆที่เป็นเว็บไซด์อันตรายหรือเว็บไซด์ที่เป็น C&C Server ของ Malware ต่างๆ เพื่อปิดการรับคำสั่งหรือหยุดการทำงานในช่วงเริ่มต้นของ Ransomware โดยลักษณะการใช้งานแบบนี้สามารถมักพบได้ใน Next Generation Firewall และเครื่องมือตรวจจับ Advance Persistence Threat(APT)
- คอยสอดส่องและปิดการใช้งาน Tor Network เพื่อป้องกันการเชื่อมต่อจากเครื่องที่ติด Malware ไปยัง C&C Server ของ Hacker ที่ให้บริการอยู่ใน Tor Network

วิธีการแก้ไขเมื่อติด Ransomware

- เราสามารถใช้ System Restore เพื่อ Restore ไปยังวันก่อนที่จะติด Ransomware ได้ เมื่อ Restore เรียบร้อยแล้วจะพบว่า Ransomware เหล่านั้นจะไม่ได้ถูกติดตั้งในเครื่องของเราแต่อย่างใด
- Boot เข้าแผ่น Rescue CD ของ Antivirus ต่างๆทำการลบ file ต่างๆที่เกี่ยวกับ Malware เหล่านั้นได้เช่น Kaspersky, MalwareBytes เป็นต้น
- หากเครื่องท่านติด Ransomware ที่มีชื่อว่า CryptoLocker สามารถนำไฟล์ที่ถูกเข้ารหัสเหล่านั้นไปถอดรหัสด้วยบริการในเว็บไซด์ที่ถูกสร้างขึ้นมาโดยเฉพาะ แน่นอนว่าเป็นบริการแบบใช้งานได้ฟรี โดย

เป็นการร่วมมือกันระหว่าง 2 บริษัทยักษ์ใหญ่ทางด้านต่อต้านภัยคุกคาม FireEye และ Fox-IT โดยเว็บไซต์สำหรับการถอดรหัสไฟลคือ decryptcryptolocker.com

5. **Rootkit** เป็นมัลแวร์ที่สามารถควบคุมเครื่อง หรือ เข้าใช้เครื่องที่ถูกติดตั้งได้จากระยะไกล และมีคุณสมบัติเด่นในด้านการหลบซ่อน ทำให้จะทำการลบ หรือ ตรวจจับเป็นไปได้ยาก
   การทำงานของ Rootkit โดยทั่วไปแล้วคือ การปกปิด User Login ที่ใช้ในการเข้าสู่ระบบ, โพรเซส, ไฟล์, Log, โปรแกรมที่ใช้ในการดักจับข้อมูล และการต่อเชื่อมกับระบบเน็ตเวิร์ก ซึ่งใน Rootkit หลายต่อหลายตัวนั้นถูกจัดให้อยู่ในพวกเดียวกับม้าโทรจันด้วย เนื่องด้วยการทำงานที่คล้ายกันมาก

6. **Spyware** ชื่อฟ้องไว้อย่างชัดเจนว่าเป็นสายลับ ซึ่งจะทำการเก็บข้อมูลการใช้งานต่างๆ ของเครื่องที่ถูกติดตั้งแล้วส่งไปยังแฮกเกอร์ และเนื่องจากโปรแกรมจำพวกนี้ไม่ใช่ไวรัสคอมพิวเตอร์ ถึงแม้เราจะติดตั้งโปรแกรมป้องกันไวรัสก็ไม่สามารถป้องกันได้ Spyware จะฝังตัวอยู่ในคอมพิวเตอร์แทบทุกเครื่องที่ต่ออินเทอร์เน็ต เพราะความรู้เท่าไม่ถึงการณ์ โดยผู้ใช้มักจะคิดว่าเพียงแต่ใช้โปรแกรมป้องกันไวรัสก็ปลอดภัยแล้ว แต่ถึงแม้จะติดตั้งโปรแกรม หากไม่มีการอัพเดทหรือดาวน์โหลดตัวสนับสนุนให้โปรแกรมสามารถตรวจพบไวรัสตัวใหม่ ๆ ที่ออกมาใหม่แทบทุกวัน ก็ไม่สามารถป้องกันคอมพิวเตอร์ให้ปลอดภัยได้
7. **Trojan Horse (ม้าโทรจัน)** คือโปรแกรมที่ถูกโหลดเข้าไปในคอมพิวเตอร์ เพื่อ ปฏิบัติการ "ล้วงความลับ" เช่น User ID, Password และข้อมูลส่วนตัวเกี่ยวกับการ Login ระบบ ที่ถูกพิมพ์ผ่านคีย์บอร์ดโดยผู้ใช้งาน โดยส่วนใหญ่แฮคเกอร์จะส่งโปรแกรมม้าโทรจัน เข้าไปในคอมพิวเตอร์เพื่อดักจับข้อมูลดังกล่าว แล้วนำไปใช้ในการเจาะระบบ หรือเพื่อโจมตีคอมพิวเตอร์ เซิร์ฟเวอร์
   การป้องกัน-กำจัดม้าโทรจัน
   - ใช้ Firewall เพื่อป้องกันการถูกโจมตีจากแฮคเกอร์
   - ใช้ซอฟต์แวร์สำหรับการตรวจจับและทำลายโทรจัน
8. **Virus (ไวรัส)** คือมัลแวร์ประเภทหนึ่งที่สามารถคัดลอกตัวเองกระจายไปยังเครื่องอื่นๆ โดยผ่านไฟล์ประเภทต่างๆ เช่น Script file , Document File เป็นต้น เมื่อติดไวรัสแล้วจะส่งผลหลายอย่างเช่น อาจจะถูกขโมยข้อมูล ทำเครื่องที่โดนไวรัสช้า หรือ หยุดทำงานตลอดเวลา

การที่คอมพิวเตอร์ใดติดไวรัส หมายถึงว่าไวรัสได้เข้าไปผังตัวอยู่ในหน่วยความจำ คอมพิวเตอร์เรียบร้อยแล้ว เนื่องจากไวรัสก็เป็นแค่โปรแกรม ๆ หนึ่งการที่ไวรัสจะเข้าไปอยู่ ในหน่วยความจำได้นั้นจะต้องมีการถูกเรียกให้ทำงานได้นั้นยังขึ้นอยู่กับประเภทของไวรัส แต่ละตัวปกติผู้ใช้มักจะไม่รู้ตัวว่าได้ทำการปลุกคอมพิวเตอร์ไวรัสขึ้นมาทำงานแล้ว จุดประสงค์ของการทำงานของไวรัสแต่ละตัวขึ้นอยู่กับตัวผู้เขียนโปรแกรมไวรัสนั้น เช่นอาจสร้างไวรัสให้ไปทำลายโปรแกรมหรือข้อมูลอื่นๆ ที่อยู่ในเครื่องคอมพิวเตอร์หรือแสดงข้อความวิ่งไปมาบน หน้าจอ เป็นต้น

9. **Worm (เวิร์ม)** หรือหนอนคอมพิวเตอร์ เป็นมัลแวร์ที่พบเจอได้ง่ายที่สุด ด้วยวิธีการแพร่กระจายผ่านระบบเน็ตเวิรค์หรืออินเทอร์เน็ต ผ่านทางช่องโหว่ของระบบปฏิบัติการ เพื่อเข้าสร้างความเสียหาย ลบไฟล์ สร้างไฟล์ หรือขโมยข้อมูล โดยส่วนใหญ่หนอนคอมพิวเตอร์จะแพร่กระจายผ่านการส่งอีเมลที่แนบไฟล์ที่มีหนอนคอมพิวเตอร์อยู่ไปยังชื่อผู้ติดต่อของเครื่องที่โดนติดตั้ง

ที่มา : https://www.catcyfence.com/it-security/article/9-type-of-malware/