Rootkit

Rootkits (รูทคิต) เป็นมัลแวร์ (Malware)ประเภทหนึ่ง

- แฮกเกอร์มักจะใช้เพื่อซ่อนมัลแวร์บนคอมพิวเตอร์ของเหยื่อ มัลแวร์ที่ถูกซ่อนด้วยรูทคิต มักจะเฝ้ามอง กรองข้อมูล ขโมยข้อมูล หรือใช้ทรัพยากรเครื่องคอมพิวเตอร์ของเหยื่อ เช่น การใช้เพื่อทำเหมือง Bitcoin (บิทคอยน์) ซึ่งนำมาใช้ในการซ่อนกิจกรรมที่เป็นอันตรายมากในปัจจุบัน ทำให้คอมพิวเตอร์เครื่องที่ติดมัลแวร์สามารถส่งสแปม (Spam) หรือทำการโจมตีเครื่องอื่นๆ โดยที่เหยื่อเจ้าของคอมพิวเตอร์อาจจะยังไม่รู้ตัวเลยด้วยซ้ำ

ลักษณะการแพร่กระจายของรูทคิต (Rootkits)

- รูทคิตเป็นชนิดของซอฟแวร์ที่เป็นอันตราย ที่ออกแบบมาเพื่อการเข้าถึงจากระยะไกล เช่น ไฟล์ที่แนบมาจากอีเมลล์ หรือการคลิกลิงก์ใดๆ และการเข้าไปยังหน้าเว็บไซต์ที่แปลกๆ โดยที่จะเข้าควบคุมคอมพิวเตอร์และไม่ถูกตรวจพบโดยโปรแกรมรักษาความปลอดภัยของผู้ใช้

การแก้ไขและกำจัดรูทคิตในคอมพิวเตอร์

- ในปัจจุบันมีเทคโนโลยีที่ออกแบบมาเพื่อกำจัดรูทคิตจำนวนมาก แต่โดยลักษณะทั่วไปของรูทคิตจะไม่สามารถตรวจจับได้จากโปรแกรมแอนตี้ไวรัส ในกรณีนี้ให้ใช้โปรแกรมแอนตี้ไวรัส เช่น "Windows Defender Offline" ทำการสแกนแบบออฟไลน์ ซึ่งมักจะถูกออกแบบมาเพื่อกำจัดมัลแวร์ที่ตรวจจับได้ยากโดยเฉพาะ

บอตเน็ต (BOTNET)
หรือ
roBOT NETwork คืออะไร

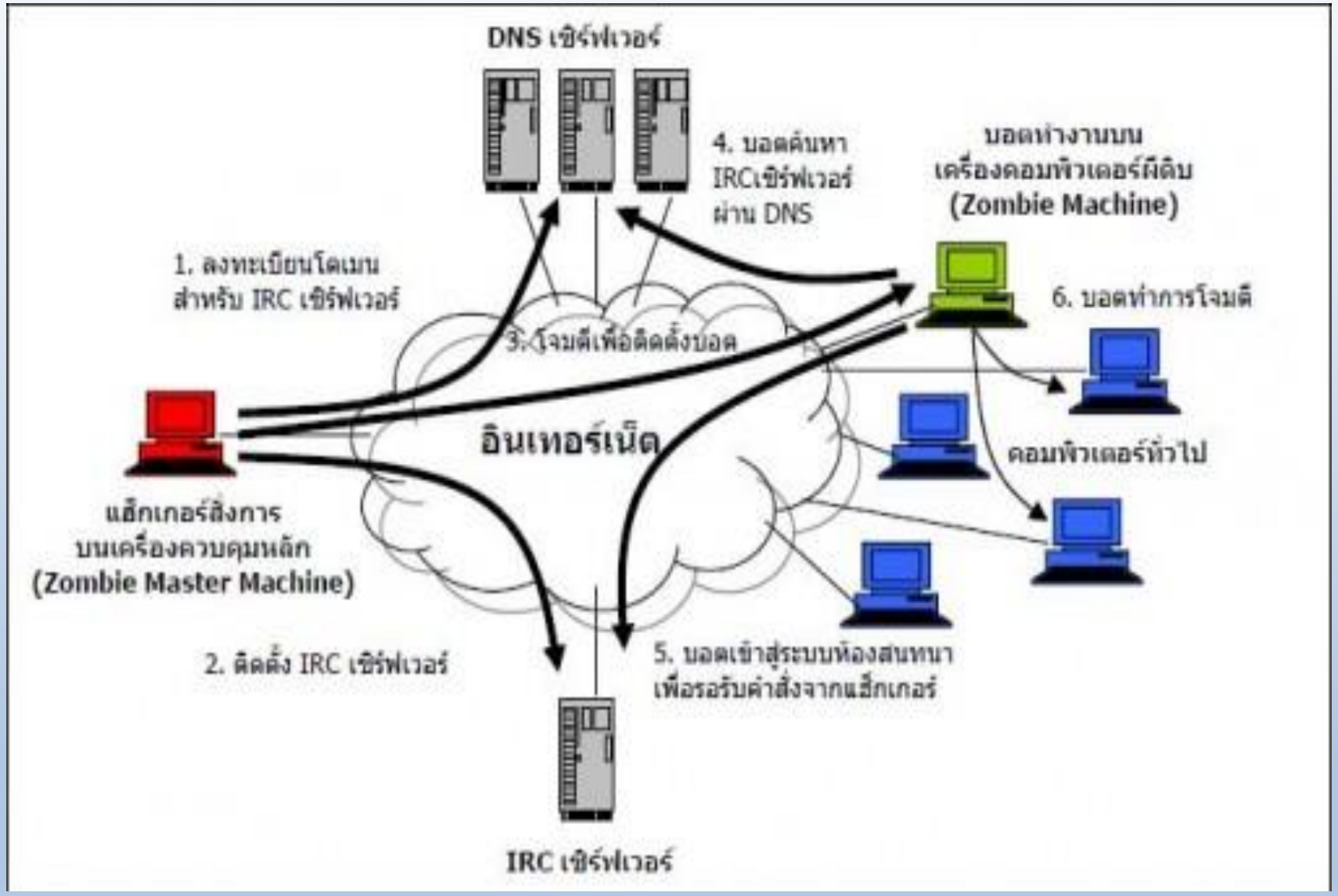
บอตเน็ต (BOTNET) หรือ roBOT NETwork

คือภัยคุกคามต่อผู้ใช้งานอินเทอร์เน็ตรูปแบบใหม่ ซึ่ง Hacker เขียนโปรแกรม BOTNET โดยใช้เทคนิคการโจมตีเครือข่ายอินเทอร์เน็ตด้วยโปรแกรมประสงค์ร้าย (Malware)ที่ซับซ้อน และมีรูปแบบที่หลากหลายกว่าไวรัสคอมพิวเตอร์หรือหนอนอินเทอร์เน็ตทั่วไป

BOTNET ที่ถูกสร้างขึ้นนี้ อาจเป็นเครื่องมือที่ใช้ส่งสแปมเมล์ (Spam Mail) และ Phishing เป็นวิธีการสร้างความเสียหายให้กับระบบเครือข่ายอินเทอร์เน็ตได้ หากผู้ใช้ทั่วไปขาดความเข้าใจถึงการป้องกันความปลอดภัยแก่เครื่องคอมพิวเตอร์ อาจจะทำให้ตกเป็นเครื่องมือ Hacker ผู้สร้าง BOTNET ได้โดยง่าย

การทำงานของ BOTNET

- ลักษณะที่สำคัญของ BOTNET ก็คือจะมีศูนย์กลางควบคุมและสั่งการโดย Hacker อยู่ที่ใดที่หนึ่งบนอินเทอร์เน็ต กลไกการทำงานของ BOT ถูกออกแบบให้มีการแพร่กระจายตัวเพื่อหาเครื่องใหม่ให้เข้ามาอยู่ในกลุ่มและมีความสามารถในการแก้ไขโปรแกรม ที่ฝังตัวอยู่บนเครื่องคอมพิวเตอร์ผีดิบเพื่อเปลี่ยนแปลงรูปแบบการบุกรุก ลักลอบใช้งานและสั่งการผ่านศูนย์ควบคุม ซึ่งองค์ประกอบหลักของ BOTNET ได้แก่ เครื่องคอมพิวเตอร์สั่งการระยะไกลของ Hacker เครื่องเซิร์ฟเวอร์ของห้องสนทนา IRC(Internet Relay Chat) ที่เป็นจุดนัดพบระหว่างกลุ่มของ BOT และ Hacker เพื่อรอรับคำสั่งกลุ่มของ DNS ซึ่งเป็นทางผ่านเพื่อทำให้ BOT สามารถหาเครื่องเซิร์ฟเวอร์ของห้องสนทนา IRC เจอได้
- นอกจากนี้ Hacker ยังสามารถที่จะสั่งการให้เกิดการแพร่กระจายและจู่โจมด้วยไวรัสคอมพิวเตอร์โดยอาศัยเครื่องคอมพิวเตอร์ผีดิบได้อีกด้วย ซึ่งจะส่งผลให้มีการติดตั้ง BOT เพิ่มขึ้นบนคอมพิวเตอร์อื่นๆอีกนับพันเครื่องในระบบเครือข่ายอินเทอร์เน็ต
- เทคนิคที่เครื่องคอมพิวเตอร์ผีดิบนิยมใช้โจมตีเครื่องคอมพิวเตอร์อื่น ๆ ก็คือการโจมตีโดยอาศัยโปรโตคอลปกติทั่วไป เช่นโปรโตคอลของเว็บ เป็นต้น ประกอบกับเทคนิคการปลอมแปลงหมายเลข IP ของผู้ส่ง ส่งผลให้การค้นหาต้นกำเนิดของ BOTNET ที่แท้จริงนั้นทำได้ยากมากยิ่งขึ้นเทคนิค IP Spoofing

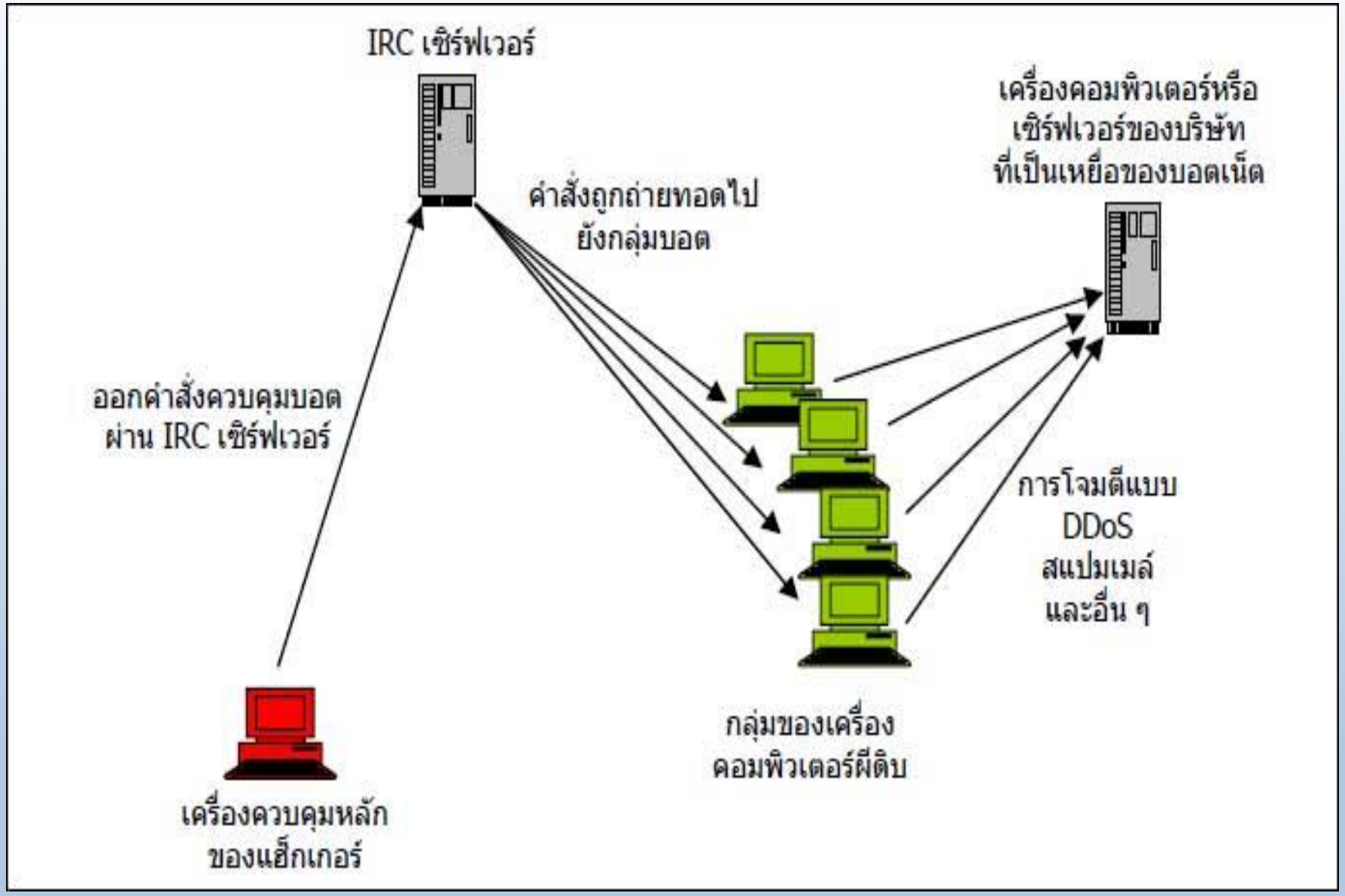


รูป แสดงขั้นตอนการทำงานของ BOTNET

ผลกระทบของภัยคุกคามจาก BOTNET

ผลกระทบของภัยคุกคามจาก BOTNET จากความซับซ้อนและรูปแบบของการโจมตีต่างๆ ของ BOTNET ดังที่อธิบายแล้วในข้างต้น จะเห็นได้ว่า BOTNET สามารถทำให้เกิดผลกระทบในวงกว้างต่อองค์กรและผู้ใช้อินเทอร์เน็ตทั่วไปได้ มีการคาดการณ์ว่า BOTNET อาจเป็นภัยรูปแบบใหม่ที่มีระดับความรุนแรงสูงสุดเท่าที่เคยมีมาบนเครือข่ายอินเทอร์เน็ต เห็นได้ว่าผลกระทบของภัยคุกคามจาก BOTNET มีลักษณะครอบคลุมตั้งแต่ *Distributed Denial of Service (*DDoS) การส่งสแปมเมล์ การขู่กรรโชกทรัพย์ การขโมยข้อมูลสำคัญ และอื่น ๆ เป็นต้น

ยิ่งถ้าจำนวนเครื่องคอมพิวเตอร์ผีดิบภายใต้กลุ่ม BOTNET มีจำนวนมากเท่าไรก็ยิ่งจะทำให้ความรุนแรงเพิ่มสูงขึ้นเท่านั้น ปัจจุบัน BOTNET สร้างความเดือดร้อนและมีผลกระทบต่อทุก ๆ ส่วนของอินเทอร์เน็ต โดยเฉพาะอย่างยิ่งบริษัทที่ทำการค้าขายบนอินเทอร์เน็ตไม่ว่าจะเป็นการทำธุรกรรมอิเล็กทรอนิกส์ เว็บไซต์เพื่อโฆษณาสินค้า หรือบริษัทที่ให้บริการเกี่ยวกับอินเทอร์เน็ตต่าง ๆ (จนเมื่อไม่นานมานี้ในบางประเทศถึงกับพยายามจัดให้การสร้าง BOTNET นั้นเป็นอาชญากรรมทางคอมพิวเตอร์ที่ร้ายแรงชนิดหนึ่งเลยทีเดียว)



รูป แสดงลักษณะของผลกระทบที่เกิดจาก BOTNET

วิธีการป้องกันและแก้ไข

- ห้ามรันไฟล์ที่แนบมากับอีเมล์ซึ่งมาจากบุคคลที่ไม่รู้จักหรือไม่มั่นใจว่าผู้ส่งเป็นใครและไม่ทราบว่าไฟล์ดังกล่าวนั้นเป็นไฟล์อะไร ตลอดจนไฟล์ที่ถูกส่งด้วยโปรแกรมสนทนา (Chat) ต่างๆ
- ติดตั้งโปรแกรมซ่อมแซมช่องโหว่ (patch) ของทุกซอฟต์แวร์อยู่เสมอ โดยเฉพาะโปรแกรม Internet Explorer และระบบปฏิบัติการ ให้เป็นเวอร์ชันใหม่ที่สุด
- ติดตั้งโปรแกรมป้องกันไวรัส และต้องทำการปรับปรุงฐานข้อมูลป้องกันไวรัสให้ทันสมัยอยู่เสมอ
- ติดตั้งโปรแกรมกำจัดสปายแวร์ ปรับปรุงฐานข้อมูล และสแกนหาสปายแวร์อยู่เสมอ
- ติดตั้งและใช้งานโปรแกรมกรองสแปมเมล์ ทั้งในเครื่องไคลเอ็นต์และที่เมล์เซิร์ฟเวอร์
- หากพบว่ามีการติดตั้งเซิร์ฟเวอร์ที่ให้บริการ IRC โดยมีจำนวนเครื่องที่เข้าสู่ระบบดังกล่าวสูงแต่ไม่มีการส่ง ข้อมูลคุยตามปกติระหว่างกัน เซิร์ฟเวอร์ดังกล่าวก็อาจกลายเป็นช่องทางในการควบคุม BOTNET ได้ ต้องดำเนินการหยุดการทำงานของเซิร์ฟเวอร์ดังกล่าวทันที

1. เปลี่ยนรหัสผ่านของอุปกรณ์ – อุปกรณ์ IoT ที่ใช้รหัสผ่านดั้งเดิมจากโรงงานมักถูกแฮกแล้วเปลี่ยนเป็น Botnet ได้ง่าย
2. อัปเดตซอฟต์แวร์สม่ำเสมอ – เพื่ออุดช่องโหว่ไม่ให้แฮกเกอร์ใช้โจมตีอุปกรณ์
3. ใช้ Firewall – Firewall ปัจจุบันช่วยตรวจจับทราฟฟิกไม่พึงประสงค์และป้องกันการโจมตีอุปกรณ์ในระบบเครือข่ายจากแฮกเกอร์
4. แยกวงอุปกรณ์ IoT ออกมา – แทนที่จะรวมอุปกรณ์ IoT ไว้ในเครือข่ายหลัก ให้สร้างเครือข่ายสำหรับอุปกรณ์ IoT โดยเฉพาะขึ้นมา และไม่มีการแชร์ข้อมูลข้ามเครือข่าย เมื่ออุปกรณ์ IoT ถูกโจมตี เครือข่ายหลักจะไม่ได้รับผลกระทบ
5. ควรระมัดระวังในการใช้งานอินเทอร์เน็ต – หลีกเลี่ยงการเข้าถึงเว็บโป๊หรือเว็บการพนัน ไม่กดโฆษณาที่ดูให้ผลตอบแทนเกินจริง รวมไปถึงติดตั้งโปรแกรม Antivirus และ Adblocker เพื่อป้องกันการลอบขุดเหรียญเงินดิจิทัล

Adware

- Adware แอดแวร์ เป็นศัพท์เทคนิคมาจากคำว่า Advertising Supported Software แปลเป็นไทยได้ว่า โปรแกรมสนับสนุนโฆษณา โดยทางบริษัทต่าง ๆ จะพยายามโฆษณาสินค้าของตนเอง เพื่อที่จะได้ขายสินค้านั้น ๆ ตัวอย่างเช่น ถ้าเราลองไปดาวน์โหลดโปรแกรมฟรีตามเว็ปต่าง ๆ เราก็จะเห็นโฆษณาสินค้าปรากฏขึ้นมาบ่อย ๆ ถ้าเราอยากให้โฆษณานั้นหายไป ก็ต้องจ่ายตังค์ค่าลิขสิทธิ์ เพื่อไม่ให้มีโฆษณาขึ้นมากวนใจอีกต่อไป xml namespace prefix o ns urn schemas-microsoft-com office offic

Adware

Adware (แอดแวร์) มีชื่อย่อมาจาก **Advertising Supported Software** เป็นโปรแกรมที่มักติดตั้งมาโดยที่เราไม่ได้ตั้งใจ โดยที่มาของโปรแกรม Adware มักจะมาจากการที่เราไปดาวน์โหลดโปรแกรมฟรีตามเว็ปต่าง ๆ นั่นเอง ซึ่งโปรแกรมฟรีเหล่านี้นี่เองที่ผู้สนับสนุนได้ทำการแฝงตัวโฆษณาหรือโปรแกรมอื่นๆมาไว้ในขั้นตอนการ Install ด้วย และหากเราไม่ได้สังเกตุหรืออ่านข้อมูลดีๆในขั้นตอนการติดตั้งเราก็อาจเผลอกด Next ยอมรับการติดตั้งโปรแกรมเหล่านั้นไปโดยปริยายนั่นเอง

อาการของเครื่องที่ติด Adware

1. หน้า Home Page (หน้าหลัก) ของเบราว์เซอร์เปลี่ยนไปกลายเป็นเว็บที่เราไม่รู้จัก
2. อาจมีป้ายโฆษณา pop-up เล็กๆ ปรากฏขึ้นมา
3. ในคอมพิวเตอร์มีโปรแกรมแปลกๆโผล่ขึ้นมาโดยที่เราไม่รู้จัก
4. มีแถบ Tool bar แปลกๆ โผล่ขึ้นมาในเว็บเบราว์เซอร์

นอกจากนั้น Adware บางตัวยังเป็นโปรแกรมที่อันตรายและไม่ได้คุณภาพจึงอาจส่งผลทำให้เครื่องคอมพิวเตอร์ของเราเกิดอาการผิดปกติ เครื่องช้า เนื่องจากโปรแกรมเหล่านั้นถูกเปิดอยู่ตลอดเวลาโดยที่เราไม่รู้และเข้าไปแย่งทรัพยากรของเครื่องอยู่เบื้องหลังนั่นเอง แถมบางโปรแกรมยังแอบส่งข้อมูลต่าง ๆ ของเราไปให้ทางบริษัท โดยที่เราไม่รู้ตัวอีกด้วยนับว่าเป็นอันตรายอย่างยิ่งเลยล่ะครับ

วิธีการป้องกัน Adware

1. ดาวน์โหลดโปรแกรมจากเว็บไซต์ของผู้พัฒนาโดยตรง หรือเว็บไซต์ที่น่าเชื่อถือไว้ใจได้
2. หลีกเลี่ยงการใช้โปรแกรมประเภท Crack ที่ละเมิดลิขสิทธิ์
3. อ่านรายละเอียดของโปรแกรมที่จะติดตั้งให้ละเอียดทั้งก่อนและขณะติดตั้ง เพราะมีบางกรณีที่เราสามารถกดติ๊กไม่เอาโปรแกรม Adware ที่เขาแถมมาให้ได้

ซึ่งหากเราปฏิบัติวิธีการป้องกัน Adware ที่ได้กล่าวไปอยู่เสมอๆ เชื่อได้เลยว่าจะสามารถป้องกัน Adware ได้อย่างแน่นอนครับ

Spyware

Spyware สไปแวร์ แปลตามตัวก็ โปรแกรมสายลับ โปรแกรมจำพวกนี้จะดึงข้อมูลต่าง ๆ ที่อยู่ในคอมพิวเตอร์ของเรา ส่งไปยังบริษัทแม่ ถึงแม้ว่าทางบริษัทจะมีนโยบายเกี่ยวกับสิทธิของบุคคล แต่ความเป็นจริงแล้ว ข้อมูลต่าง ๆ จะถูกส่งไปให้บริษัทแม่อย่างต่อเนื่อง อาทิเช่น ข้อมูลที่เกี่ยวกับเวลาที่เราใช้อินเทอร์เน็ท เว็ปไหนที่เราเข้าไปดูบ่อย ๆ เป็นต้น

และเนื่องจากโปรแกรมจำพวกนี้ ไม่ใช่ ไวรัส คอมพิวเตอร์ ถึงแม้เราจะติดตั้งโปรแกรมป้องกันไวรัส ก็ไม่สามารถป้องกันได้

Adware amp Spyware จะฝังตัวอยู่ในคอมพิวเตอร์แทบทุกเครื่องที่ต่ออินเทอร์เน็ต เพราะความรู้เท่าไม่ถึงการ โดยผู้ใช้มักจะคิดว่าเพียงแต่ใช้โปรแกรมป้องกันไวรัส ก็จะปลอดภัยแล้ว แต่เราจะบอกว่า แม้จะติดตั้งโปรแกรมแล้ว แต่ไม่มีการอับเดท หรือ ดาวน์โหลด ตัวสนับสนุนให้โปรแกรมสามารถตรวจพบไวรัสตัวใหม่ ๆ ที่ออกมาใหม่แทบทุกวัน เดือนละประมาณร้อยชนิด ก็ไม่สามารถป้องกันคอมพิวเตอร์ของเพื่อนๆให้ปลอดภัยได้

- Spyware ถูกเผยแพร่ไปยังผู้ใช้อินเทอร์เน็ตทั่วโลกอย่างรวดเร็ว ซึ่งรูปแบบของการเผยแพร่ก็แตกต่างกันไป ส่วนใหญ่มักเผยแพร่ผ่านหน้าเว็บไซต์ที่เราเข้าไปดูไปชม และเมื่อผู้ใช้งานเข้าไปในเว็บนั้นๆ ก็จะปรากฏ Pop up เชวนให้เราคลิก ด้วยความมือไวไม่ทันระวังพวกเราก็คลิก OK Yes Accept ฯลฯ โดยที่ไม่ได้อ่าน Spyware จึงถูกโหลดมายังเครื่องของเราโดยทันที จะเห็นได้ว่าเรามีทางเลือกที่จะเปิดโอกาสให้ Spyware เข้ามาในเครื่องของเราหรือไม่ก็ได้ เพียงแค่เราใส่ใจอ่านข้อความบน Pop up ดังกล่าว xml namespace prefix v ns urn schemas-microsoft-com vml

❑ โทษของ Adware amp Spyware

- ส่งข้อมูลต่าง ๆ ของเราไปให้ทางบริษัท โดยที่เราไม่รู้ตัว
- โปรแกรมถูกรันให้ทำงานในคอมพิวเตอร์ ทำให้เกิดอาการ แฮงค์ เปลืองแมมโมรี่ หรือ เปิดโปรแกมบางตัวไม่ได้ เพราะแมมโมรี่ไม่พอ หรือบางที่ เปิดคอมฯไม่ติดเลยก็มี
- บางครั้ง Adware amp Spyware จะตั้งค่าต่าง ๆ ในระบบ เช่น ค่าเว็ปไซต์แรกที่เราเปิดใน Internet Explorer หรือ Netscape Navigator
- บาง Adware amp Spyware ตั้งค่า โมเด็ม ให้หมุนหมายเลขโทรศัพท์ต่างประเทศ ทำให้เสียค่าโทรศัพท์ในอัตราสูง

❑ อาการของเครื่องคอมฯที่มี Spyware

- อาจมีป้ายโฆษณาเล็กๆ ปรากฏขึ้นมา Adware หรือที่เรียกว่า pop-up
- ขโมยข้อมูลส่วนตัวในเรื่องคอมฯ ของคุณ โดยเฉพาะ username password
- เก็บข้อมูลการเข้าเว็บไซต์ต่างๆ และเว็บที่คุณชื่นชอบ ส่งไปยังผู้ที่ต้องการ
- เว็บเริ่มต้นในการทำงาน ถูกเปลี่ยนไป
- มีโปรแกรมใหม่ๆ ถูกติดตั้งขึ้นมาโดยที่ไม่ได้มีการติดตั้ง
- ค้นหาข้อมูลใน Search Engine จะมีความแตกต่างออกไปจากเดิม

❑ การป้องกัน Spyware ในเบื้องต้น

- ระวังเรื่องการ download โปรแกรมจากเว็บไซต์ต่างๆ
- ระวังอีเมล์ ที่ให้คำแนะนำเกี่ยวกับการแจกโปรแกรมฟรี เกี่ยวกับกำจัด spyware
- ระหว่างการใช้งานอินเตอร์เน็ต ถ้ามีหน้าต่างบอกให้คลิกปุ่ม Yes ระวังสักนิด อ่านรายละเอียดให้ดี อาจมี spyware แฝงอยู่ แนะนำให้คลิก No ไว้ก่อน จะปลอดภัยกว่า
- หน้ามีหน้าต่าง pop-up ขึ้นมา แนะนำให้คลิกตัว X แทนการคลิกปุ่มใด ๆ และโดยเฉพาะบริเวณป้ายโฆษณา นั่นอาจหมายถึงคุณกำลังยืนยันให้มีการติดตั้ง spyware แล้ว
- ตรวจสอบ ด้วยโปรแกรมกำจัด spyware อย่างน้อยอาทิตย์ละครั้ง สำหรับองค์กร แนะนำให้ตรวจสอบทุกวัน โดยเฉพาะเวลาพักทานข้าว ซึ่งถือได้ว่าเป็นเวลาที่เหมาะสมมากที่สุด ไวร้ายตัวจริงของ Adware amp Spyware คือ บางโปรแกรม ถูกสร้างมาเพื่อ แฮกค์ระบบโดยเราโดยตรง เช่น โปรแกรมจะบันทึกทุกตัวอักษรที่เราคีย์เข้าไปในเครื่อง หรือทุกเว็ปไซต์ที่เราเข้าไปดู หรือ แม้แต่จับหน้าจอ ว่าเราทำงานอะไรบ้าง แล้วจะส่งข้อมูลไปให้แฮกเกอร์ นับว่าเป็นการกระทำที่ผิดกฎหมายอย่างแท้จริง

Key logger

- Keyloggers หรือที่รู้จักกันในชื่อ keystroke loggers นี่คือโปรแกรมที่ทำงานตลอดเวลาบนคอมพิวเตอร์ของคุณนับจากนาทีที่คุณเริ่มต้นทำงาน Keylogger จะบันทึกการกดแป้นพิมพ์ทุกครั้งที่คุณสร้างหรือเฉพาะที่ทำในฟิลด์เฉพาะบนเว็บไซต์.
- Keyloggers จะไม่ทำให้คอมพิวเตอร์ของคุณช้าลงและคุณจะไม่สังเกตเห็นแม้เมื่อมีการใช้งาน Windows 10 มี keylogger ในระบบปฏิบัติการด้วย แม้ว่าจะมีการใช้คีย์ล็อกเกอร์อย่างถูกกฎหมายเช่นในที่ทำงานหรือเพื่อติดตามกิจกรรมทางอินเทอร์เน็ตของเด็ก ๆ แต่คุณก็มีความเสี่ยงที่โปรแกรมเหล่านี้จะเปลี่ยนคอมพิวเตอร์ของคุณให้กลายเป็นสายลับให้แฮกเกอร์.

- Keyloggers สามารถฝังตัวเองลงในระบบปฏิบัติการของคอมพิวเตอร์ของคุณ. **มัลแวร์ประเภทนี้เรียกว่าไวรัส "รูทคิท"**. มีชนิดของ keyloggers ที่สามารถทำงานได้ในระดับต่ำกว่าระบบปฏิบัติการ สิ่งเหล่านี้เรียกว่า "มัลแวร์ไฮเปอร์ไวเซอร์" Keylogger อาจแนบตัวเองเข้ากับเบราว์เซอร์ของคุณเป็นส่วนขยายที่ซ่อนอยู่และเพียงรายงานการกดแป้นพิมพ์ทั้งหมดที่คุณทำผ่านแอปนั้น โปรแกรมล็อกเกอร์หลักอื่น ๆ สามารถติดเชื้อในหน้าเว็บได้ดังนั้นทุกคนที่เข้าชมหน้าเหล่านั้นจะถูกขโมยข้อมูล.

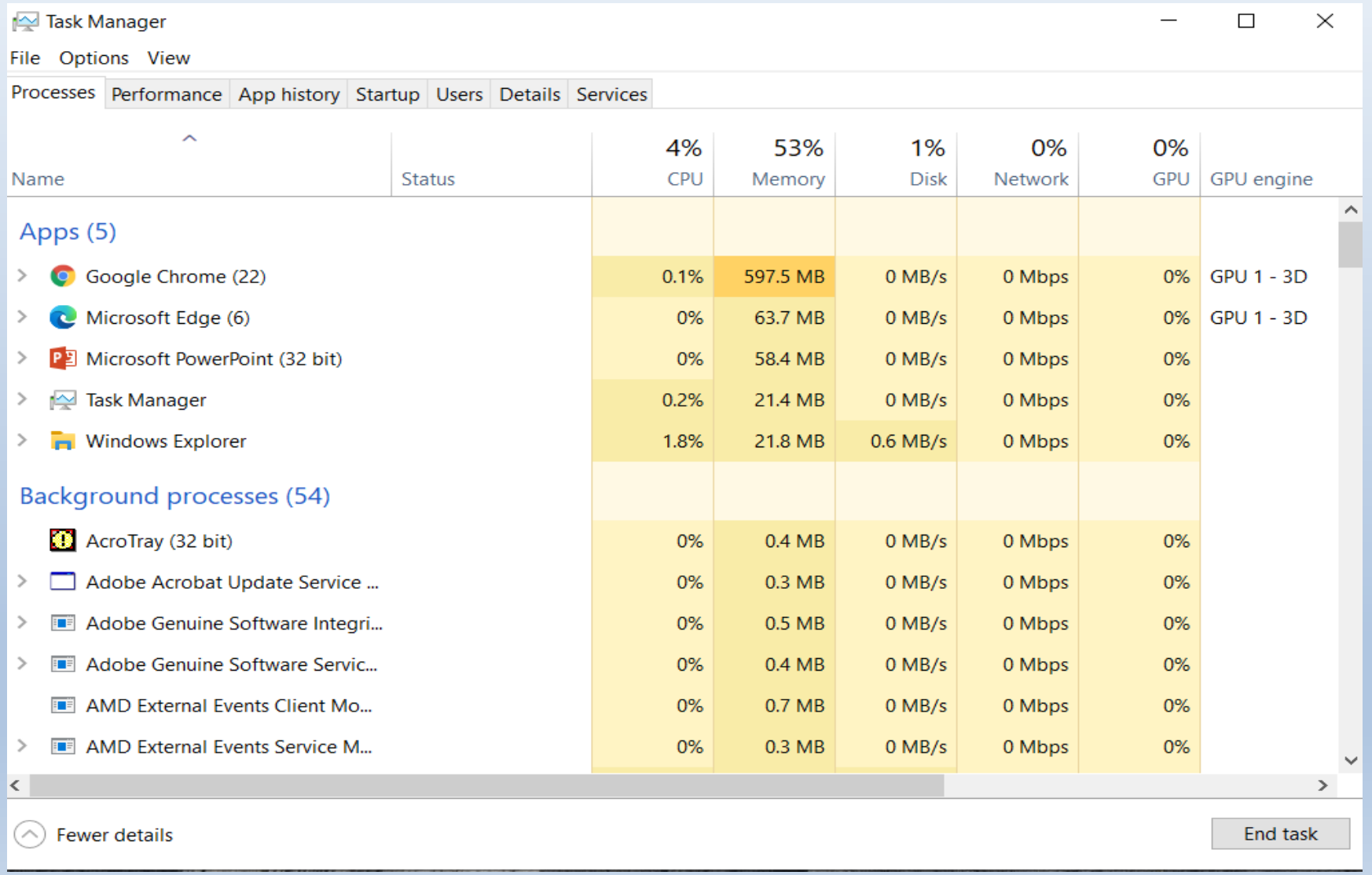
- Keyloggers สามารถเปลี่ยนกระบวนการเข้าถึงหน่วยความจำของเบราว์เซอร์ของคุณและขโมยข้อมูล ณ จุดนั้นหรือสามารถเรียกใช้งานได้โดยคลิกปุ่มส่งแบบฟอร์มบนเว็บ ในระยะสั้น, **มีสถานการณ์จำลองการทำงานหลายอย่างสำหรับ keyloggers** และตำแหน่งต่าง ๆ มากมายบนคอมพิวเตอร์ของคุณซึ่งโปรแกรมอาจทำงานอยู่ คีย์ล็อกเกอร์รูทคิทและไฮเปอร์ไวเซอร์นั้นยากเป็นพิเศษในการกำจัด โปรแกรมต่อต้านมัลแวร์มักจะไม่สามารถลงไปถึงระดับนั้นได้ดังนั้นโปรแกรมล็อกคีย์เหล่านี้จะยังคงทำงานต่อไปโดยไม่ได้รับอนุญาต Keyloggers ที่ปลอมตัวเป็นส่วนขยายเบราว์เซอร์มักจะหลบเลี่ยงการตรวจจับจากมัลแวร์.

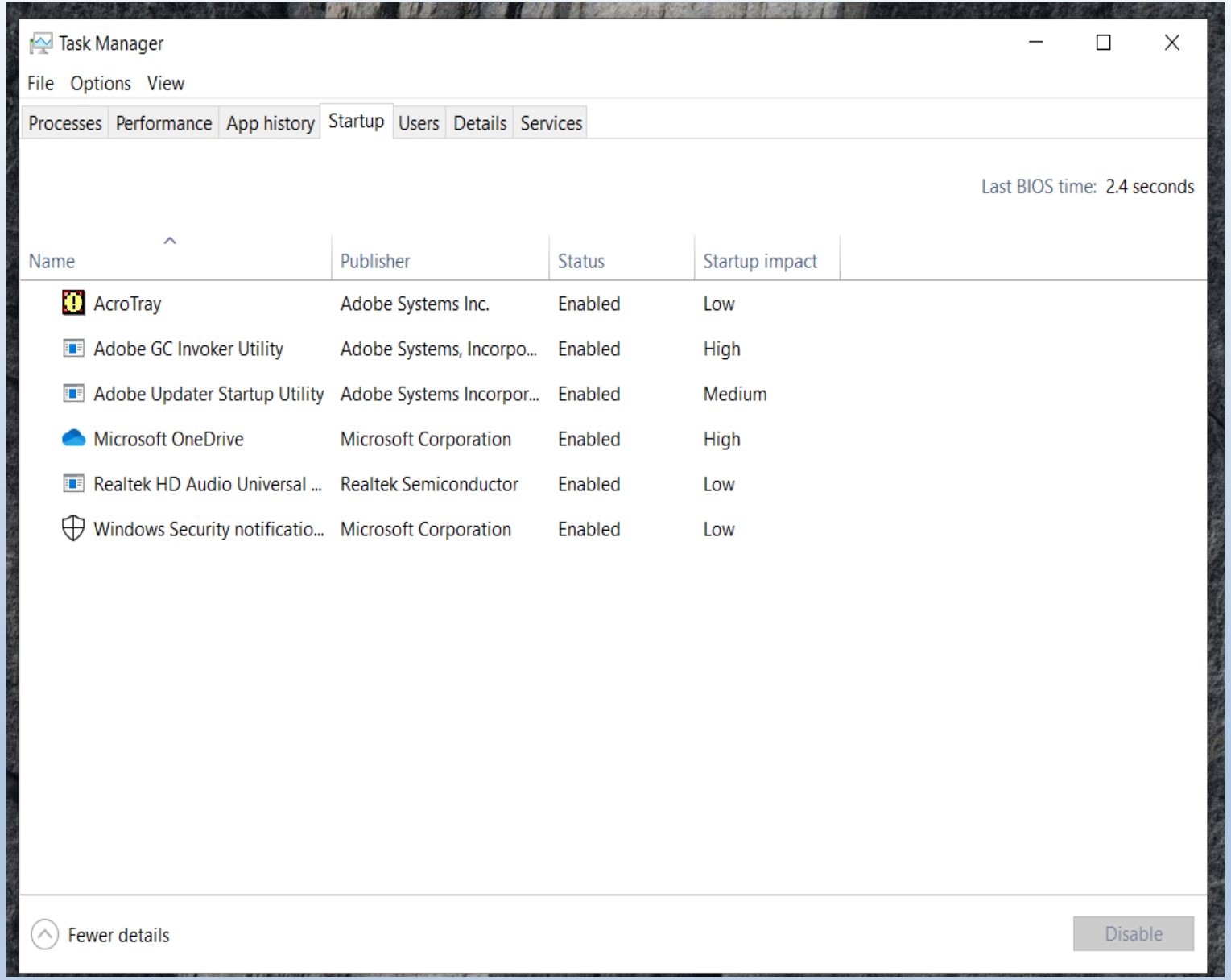
วิธีการที่ keyloggers เข้าสู่คอมพิวเตอร์ของคุณ

- โอกาสที่ดีที่สุดที่คุณจะป้องกันไม่ให้ keylogger ทำงานบนคอมพิวเตอร์ของคุณคือการบล็อกก่อนที่จะถูกติดตั้ง สำหรับสิ่งนี้คุณต้องมีซอฟต์แวร์ป้องกันมัลแวร์ที่ดีมากและยังมีความสงสัยในการดาวน์โหลดทุกสิ่งบนเว็บ
- **วิธีการทั่วไปในการเข้าใช้สำหรับ keylogger นั้นเป็นส่วนหนึ่งของโทรจัน**. โทรจันเป็นซอฟต์แวร์ชิ้นหนึ่งที่อ้างว่าเป็นประโยชน์อย่างยิ่ง เมื่อคุณดาวน์โหลดแอพฟรีและติดตั้งไม่ว่าจะใช้งานได้หรือแอปใช้งานได้จริงตามที่สัญญา แต่โปรแกรมติดตั้งจะส่งมัลแวร์ไปยังคอมพิวเตอร์ของคุณเช่นกัน.

- โทรจันมักใช้งานเป็นชุดซอฟต์แวร์โดยแต่ละองค์ประกอบมีความเชี่ยวชาญในงานที่แตกต่างกัน โทรจันเริ่มต้นอาจโหลดเป็นตัวดาวน์โหลดซึ่งช่วยให้แฮกเกอร์ได้รับมัลแวร์เพิ่มเติมรวมถึง keylogger ผ่านไฟร์วอลล์และบนคอมพิวเตอร์ของคุณ Keylogger จะบันทึกการกดแป้นของคุณในไฟล์บนคอมพิวเตอร์ของคุณจากนั้นโปรแกรมแยกต่างหากจะส่งข้อมูลนั้นออกไปทางอินเทอร์เน็ต

วิธีการตรวจสอบ keylogger




Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Last BIOS time: 2.4 seconds
Name Publisher Status Startup impact
AcroTray Adobe Systems Inc. Enabled Low
Adobe GC Invoker Utility Adobe Systems, Incorpo... Enabled High
Adobe Updater Startup Utility Adobe Systems Incorpor... Enabled Medium
Microsoft OneDrive Microsoft Corporation Enabled High
Realtek HD Audio Universal ... Realtek Semiconductor Enabled Low
Windows Security notificatio... Microsoft Corporation Enabled Low
Fewer details
Disable

วิธีกำจัด keylogger

- ซอฟต์แวร์ Antikeylogger เปิดโอกาสให้คุณกำจัด keyloggers ได้ดีกว่ามัลแวร์ทั่วไปหรือแม้แต่โปรแกรมป้องกันสปายแวร์ Antikeylogger ที่ครอบคลุมจำเป็นต้องตรวจสอบกระบวนการทั้งหมดที่ทำงานอยู่ในคอมพิวเตอร์ของคุณตั้งแต่ BIOS ไปจนถึงระบบปฏิบัติการไปจนถึงบริการพื้นหลังและแอพที่ทำงานบนคอมพิวเตอร์ของคุณตลอดจนการตั้งค่าเครือข่ายปลั๊กอินและการตั้งค่าเบราว์เซอร์.
- อาจต้องใช้เวลาสักครู่ก่อนที่คุณจะกำจัด keylogger และท้ายที่สุดคุณอาจต้องติดตั้งระบบปฏิบัติการใหม่เพื่อกำจัดมัน.
- คีย์ล็อกเกอร์จำนวนมากเป็นไวรัสรูทคิทดังนั้นนอกเหนือจากระบบป้องกันการบุกรุกพิเศษโปรแกรมต่อต้านรูทคิทสามารถกำจัดปัญหาของคุณได้ นี่คือรายการของซอฟต์แวร์ที่ดีที่สุดที่จะช่วยคุณลบ keyloggers

Rogue Application

- ในยุคสมัยที่คอมพิวเตอร์ใช้งานได้ง่ายขึ้น ใครๆก็สามารถใช้งานได้สะดวกมากยิ่งขึ้น แต่จะมีใครรู้บ้างว่ารูปแบบของ มัลแวร์ (Malware) ได้มีเพิ่มมากขึ้นเช่นกัน ไม่ใช่เป็นเพียงแค่ ไวรัส (Virus)ที่ทำลายไฟล์งาน หรือไฟล์รูปภาพของเราแล้ว แต่ในวันนี้มัลแวร์ (Malware) ได้มีการพัฒนาให้สามารถเข้ารหัสเพื่อล็อคไฟล์ต่างๆของเรา เพื่อนำไปเรียกค่าไถ่ หรือแม้กระทั่งหลอกขโมยข้อมูลของเรา โดยที่เราอาจจะยังไม่รู้ตัวด้วยซ้ำ

Rogue Security Malware

คือมัลแวร์ชนิดหนึ่งที่มักจะแฝงมาในรูปแบบของ โปรแกรมแอนตี้ไวรัส (AntiVirus Program) หรือ โปรแกรมแอนตี้สปายแวร์ (AntiSpyware) โดยวิธีการการทำงานของมันคือจะให้ผู้ใช้ทำการติดตั้งโปรแกรม หลังจากนั้น จะทำการตรวจค้นหาไวรัสบนเครื่องของเรา หลังจากนั้นจะรายงานผลการตรวจจับที่ไม่มีอยู่จริง และจะให้เหยื่อทำการโอนเงินไปให้เพื่อกำจัดไวรัสหรือมัลแวร์ที่โปรแกรมตรวจจับได้ แต่ที่จริงแล้วเป็นการหลอกลวงทั้งหมด

การทำงานของ Rogue Security Malware

จะเริ่มจากเมื่อเหยื่อเข้าชมเว็บไซต์ที่ร่วมมือกับโปรแกรมเหล่านี้ มันจะทำการแสดงป๊อปอัพพร้อมข้อความหลอกลวงในลักษณะต่างๆ ซึ่งทำให้เหยื่อข้าใจผิดว่าเครื่องของตนเองได้โดนไวรัส ตัวอย่างข้อความที่พบได้บ่อยๆ เช่น "YOUR COMPUTER IS INFECTED!

จากนั้น Rogue ก็จะเสนอความช่วยเหลือในการแก้ไขแบบ Step by Step ซึ่งจะรวมถึงการหลอกให้ซื้อโปรแกรม พร้อมทั้งใช้จิตวิทยากับเหยื่อ โดยการแสดงผลการสแกนแบบหลอกๆว่า พบมัลแวร์จำนวนมากบนเครื่อง หากเหยื่อหลงเชื่อและทำการติดตั้ง ก็จะนำมาซึ่งปัญหาต่างๆ เช่น ต้องเสียเงินโดยไม่จำเป็น หรือในกรณีที่ชำระผ่านบัตรเครดิต อาจจะถูกขโมยข้อมูลในบัตรเครดิต เป็นต้น

- วิธีการป้องกันหรือกำจัด

หากติดตั้งโปรแกรมไปแล้ว ให้ถอนการติดตั้ง หรือถ้าทราบว่าโปรแกรมที่ใช้อยู่ในเครื่องนั้นเป็น Rogue Security Malware จะมีการเรียกเก็บค่าใช้งานการกำจัดไวรัสก็ไม่ต้องไปชำระตามที่โปรแกรมเรียกขอ

?