เตือนภัยไวรัส ransomware

ณ ขณะนี้ได้มีไวรัสตระกูลมัลแวร์ที่มีชื่อว่า แรนซัมแวร์ (ransomware) กำลังระบาดอยู่ภายในโลกอินเตอร์เน็ต โดยผลของมันจะทำให้ไฟล์ข้อมูล เอกสาร รูปภาพต่าง ๆ ภายที่อยู่ในเครื่องคอมพิวเตอร์ถูกล็อกเปิดใช้งานไม่ได้ โดยขณะนี้ทางด้านสำนักเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ กรมสอบสวนคดีพิเศษ (ดีเอสไอ) ได้มีหนังสือแจ้งเตือนภัยแก่ประชาชน เกี่ยวกับไวรัสดังกล่าวแล้ว

แรนซัมแวร์คืออะไร? CBT-Locker ransomware หรือเรียกอีกอย่างหนึ่งว่า Cryptolocker นั้นเป็นโปรแกรมไวรัสประเภทมัลแวร์ ซึ่งจะเรียกกันในนามของ “โปรแกรมเรียกค่าไถ่” โดยเจ้าไวรัสตัวนี้จะทำการจับไฟล์ของคุณตัวประกันโดยการจับไฟล์เหล่านั้นเข้ารหัสเสียใหม่ จึงส่งผลส่งผลให้ไฟล์ของเรานั้นเปิดใช้งานไม่ได้ ซึ่งถ้าหากอยากจะได้ไฟล์มาต้องทำการจ่ายเงินค่าไถ่ให้กับ Hacker โดยเริ่มต้นที่ราคาราว ๆ 300$ ซึ่งเมื่อตีค่าเป็นเงินไทยก็ถือว่าแพงเอาเรื่อง ซึ่งเมื่อเราจ่ายเงินไปแล้วก็จะได้รับรหัส decrypt มาทำการปลดล็อกไฟล์ แต่ทั้งนี้ทั้งนั้นก็ไม่แปลว่าจะมี สัจจะในหมู่โจร หรือก็คือจ่ายเงินแล้วก็ใช่ว่าจะได้รับการแก้ไขนะครับ

แรนซัมแวร์เข้ามาในเครื่องเราได้อย่างไร? โดยส่วนมากแล้วเจ้ามัลแวร์พวกนี้มันมาจากไฟล์แนบใน e-mail โดยจะมาในรูปแบบของลิงค์ไฟล์ประเภท .zip หรือไม่ก็ .exe บางครั้งก็เป็นพวกเว็บลิงค์ต่าง ๆ ที่ส่งมาหลอกล่อทาง facebook ก็มีเช่นกัน บางครั้งก็แถมมากับพวก Crack โปรแกรมเถื่อน ๆ ที่หาโหลดกันมาทางอินเตอร์เน็ต ซึ่งถ้าผลอไปกดเข้าให้แล้วก็โดนไวรัสเข้าเต็ม ๆ แน่นอนครับ

จะรู้ได้อย่างไรว่าโดนเจ้าวายร้ายนี่เล่นงานเข้าไปแล้ว? โดยมากแล้วไฟล์ที่จะเป็นเป้าหมายเล่นงานของมัลแวร์ตัวนี้ก็คือไฟล์จำพวก .pdf, .xls, .ppt, .txt, .py, .wb2, .jpg, .odb, .dbf, .md, .js, .pl,

และ .doc เป็นต้น แต่ว่าพวกไฟล์มัลติมีเดียอย่าง รูปภาพ เพลง หรือ วีดีโอจะรอดพ้น พูดง่าย ๆ ก็คือโดนเรียบไม่ว่าไฟล์อะไรก็ตามแต่นั่นแหละ โดยไฟล์ที่โดนเล่นงานมักจะรหัสไฟล์ตามหลังนามสกุลดั่งเดิมว่า .ikjyiia ตัวอย่างเช่นไฟล์ word ชื่อว่า งานประจำ.docx แต่พอโดนไวรัสนี้เข้าไปก็จะเปลี่ยนเป็น งานประจำ.docx.ikjyiia แบบนี้เป็นต้น

ถ้าเราฆ่าไวรัสได้แล้วไฟล์เราจะกลับมาได้หรือเปล่า? คำตอบคือ NO ไม่ได้ครับแม้จะกำจัดไวรัสไปแล้ว แต่ไฟล์ที่ถูกแก้ไขรหัสไปแล้วก็จะไม่ได้กลับคืนมาแต่อย่างใด ซึ่งถ้าใครโดนไวรัสนี้เข้าให้แล้ว ก็บอกคำเดียวว่าต้องทำใจ fomat เครื่องใหม่เท่านั้นแหละเพราะไฟล์ในเครื่องคุณได้ตายไปแล้วนั่นเอง

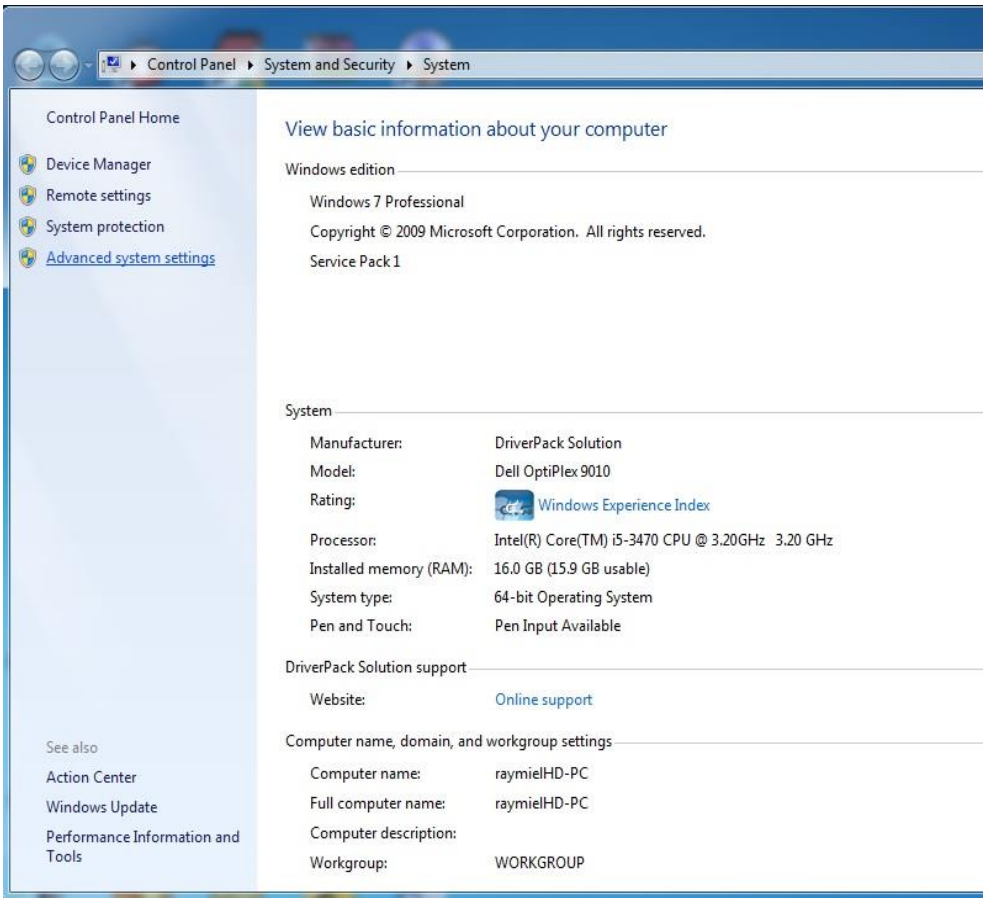
มี Anti-Virus อยู่ในเครื่องแล้วมันไม่ช่วยเลยหรือ? อันที่จริงแล้วมันก็ช่วยได้ในระดับหนึ่งเท่านั้นเองครับ แอนตี้ไวรัสที่ได้รับการอัพเดทจะมีความสามารถในการดักจับมัลแวร์ แต่มันก็ค่อนข้างไร้ความหมาย หากตัว User เองได้อนุญาตให้ไวรัสตัวนี้เข้ามาด้วยตนเองโดยการลดการป้องของโปรแกรมแอนตี้ไวรัสลงเอง โดยที่อาจจะไม่รู้ตัว เพราะหลายคนชอบตอบ Yes ไปโดยไม่ดูให้ดีก่อน และผลก็คือคุณได้เปิดประตูให้โจรเข้าบ้านแล้วนั่นเอง

เราจะป้องกันตัวจากแรนซัมแวร์ได้อย่างไร? อันที่จริงแล้วเจ้าไวรัสประเภทนี้ก็ไม่ใช่ของใหม่อะไรนักมันเคยระบาดมาก่อนในช่วงหนึ่งแล้ว ทางที่ดีที่สุดสำหรับข้อมูลสำคัญมาก ๆ แล้วควรทำ backup เก็บไว้ เช่นเซฟข้อมูลของเราเอาไว้หลาย ๆ ที่ เช่นในแฟลชไดร์ฟ คลาวด์ไดร์ฟ บน E-Mail ของเราเป็นต้น พยายามหลีกเลี่ยงการเปิดเมล์แปลก ๆ จากคนที่เราไม่รู้จัก ไม่เปิดเว็บลิงค์ที่ไม่มีที่มาที่ไป เพียงเท่านี้มันก็จะช่วยให้เรารอดพ้นจากมัลแวร์ตัวนี้ได้บ้างแล้ว

Trick สำหรับรับมือเผื่อโดนเล่นงาน

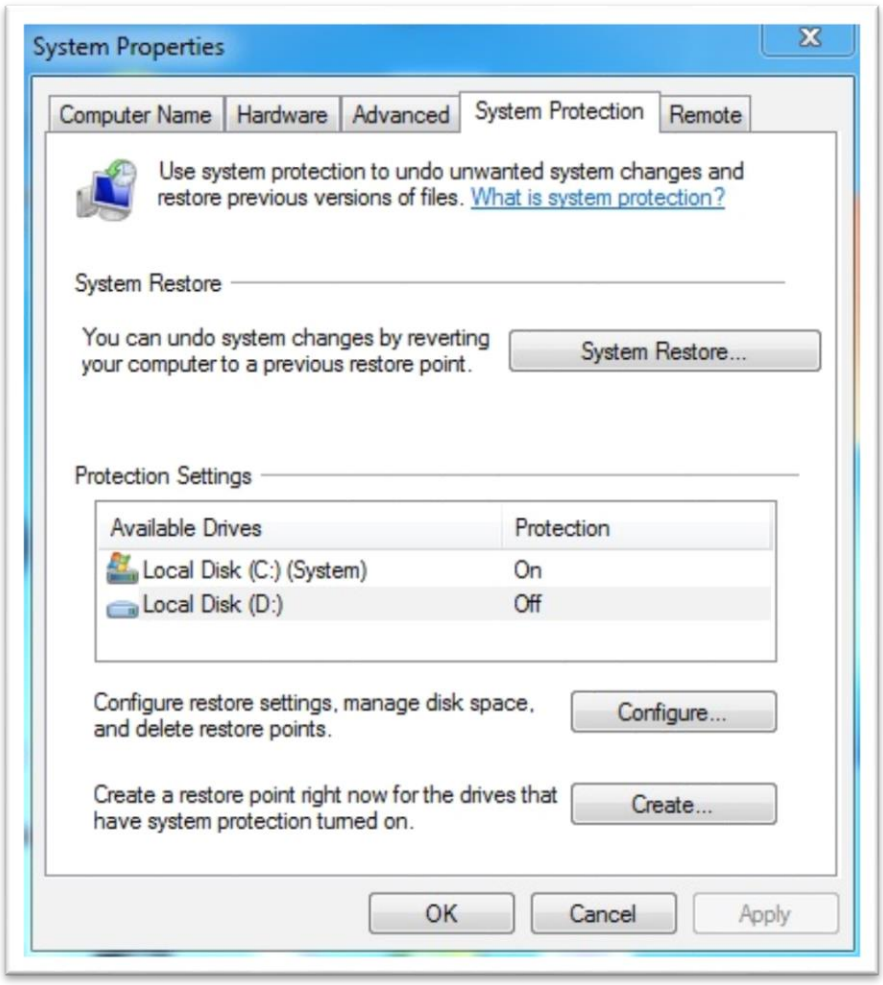
จริง ๆ แล้วมันก็พอจะเทคนิคที่พอจะเป็นการเตรียมรับมือไวรัสตัวนี้ได้อยู่เหมือนกัน หากแต่ว่าเราจะต้องกระทำการเซ็ตค่าตัวเครื่องคอมพิวเตอร์ของเราให้มีความพร้อมก่อนโดนเล่นงาน ซึ่งการเซ็ตค่านี้จะกระทำโดยใช้ฟังก์ชั่นตัวหนึ่งของระบบปฏิบัติการ Windows และโปรแกรมตัวหนึ่งเพื่อใช้เรียกไฟล์กลับมาได้ แม้ไม่การันตี 100% แต่วิธีนี้ผมก็เคยใช้ได้ผลมาแล้วกับเครื่องที่โดนไวรัสนี้เล่นงานซึ่งสามารถเรียกไฟล์กลับมาได้ โดยทำดังนี้

1. เซ็ต System Restore ให้กับทุกไดร์ฟที่มีอยู่ภายในเครื่องคอมพิวเตอร์ โดยให้เราไปทำการคลิ๊กขวาที่ My Computer –> Properties จะปรากฏหน้าต่างดังภาพ



จากนั้นเลือกไปที่ Advanced system setting

2. เมื่อเลือก Advanced system setting แล้วจะมีหน้าต่างอีกอันหนึ่งปรากฏขึ้นให้เลือกไปที่คำว่า System Protection จะพบกับหน้าต่างดังภาพ

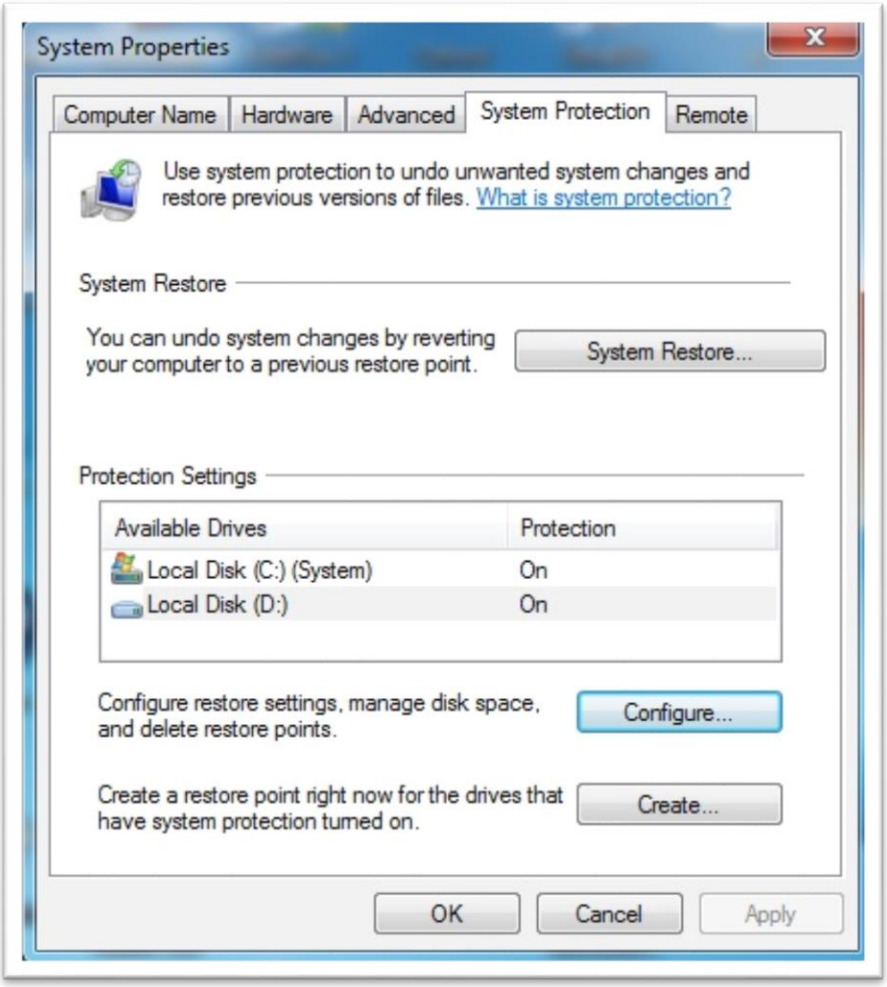


สังเกตในช่อง Protection Setting ที่อยู่ตรงกลางจะพบรายชื่อไดร์ฟทั้งหมดในเครื่องคอมพิวเตอร์ของเรา ในภาพตัวอย่างนี้มีแค่ 2 ไดร์ฟ โดยปกติแล้ววินโดว์จะเปิด System Restore เอาไว้ที่ไดร์ฟ C: อยู่แล้ว โดยสังเกตคำว่า On ที่อยู่ทางด้านขวาของไดร์ฟนั้น ๆ ถ้าหากเป็น Off แปลว่า System Restore ยังไม่ได้ถูกเปิด เราจะทำการเปิดระบบนี้ให้กับไดร์ฟที่เราต้องการได้ โดยคลิ๊กเลือกไปที่ไดร์ฟที่เราต้องการ ในตัวอย่างคือไดร์ฟ D: คลิ๊กให้แถบสีฟ้าปรากฏขึ้นมา จากนั้นเลือกไปที่ Configure……

3. เมื่อกดเลือกแล้วจะพบกับหน้าต่างสำหรับตั้งค่า Restore Setting โดยจะมีตัวเลือกให้เราเลือกอยู่ทั้งหมด 3 ข้อคือ

    - Restore system and previous verion of files
    - Only restore previous verion of files
    - Turn off system protection

    ให้เราเลือกการตั้งค่าใหม่ไปที่ Only restore previous verion of files จากนั้นกด Apply ตามด้วย OK เมื่อทำเสร็จแล้วก็จะได้เป็นดังภาพ กด OK อีกครั้งเพื่อออกจากหน้าต่าง



เมื่อทำการตั้งค่าเครื่องของเราเอาไว้เช่นนี้แล้วตั้งเครื่องก็จะทำการแบ็คอัพไฟล์ไว้ให้เป็นช่วงเวลาโดยอัตโนมัติ โดยแลกกับพื้นที่บางส่วนบน Harddisk ของไดร์ฟนั้น ๆ ซึ่งถ้าหากถูกไวรัสเข้าเล่นงานทำเอาไฟล์เปิดไม่ได้แล้วล่ะก็ ให้ทำการฆ่าไวรัสให้หมดด้วยโปรแกรมกำจัดมัลแวร์ เช่น malwarebyte จากนั้นให้ทำการติดตั้งโปรแกรมสำหรับเรียกคืนข้อมูลจาก Restore Point ที่ชื่อว่า shadow explorer มาติดตั้งในเครื่องซะ ซึ่งโปรแกรมตัวนี้เป็นฟรีแวร์นะครับ ไม่เสียค่าใช้จ่ายใด ๆ สามารถโหลดได้ที่ http://www.shadowexplorer.com/ ครับ

ในส่วนของวิธีการใช้งาน shadow explorer นั้นได้มีผู้จัดทำเป็นไฟล์วีดีโอและเผยแพร่บนเว็บไซต์ youtube เป็นที่เรียบร้อยแล้วนะครับ สามารถเข้าไปดูได้ที่ลิงค์ด้านล่างนี้

https://www.youtube.com/watch?v=5LHdqxvdXGU

อนึ่งวิธีนี้ขอย้ำว่านี่ไม่ใช่วิธีป้องกันไวรัสชนิดนี้ที่ดีที่สุด และไฟล์ที่ได้กลับมาก็อาจไม่ใช่ไฟล์ที่เป็นปัจจุบัน ฉะนั้นแล้วทางที่ดีที่สุดก็คือทำแบ็คอัพเอาไว้หลาย ๆ ที่จะดีกว่า และที่ดีที่สุดก็คืออย่าไปโดนเข้าเลยนั่นแหละครับ

By raymiel02