Matichon Online
วันที่ 4 เมษายน พ.ศ. 2552
http://www.matichon.co.th/

เตือนภัยคุกคามเวิร์มตัวใหม่

บริษัท เทรนด์ ไมโคร ผู้นำระดับโลกด้านการจัดการและรักษาความปลอดภัยข้อมูลบนอินเตอร์เน็ต ตรวจพบหนอน WORM_DOWNAD.A เมื่อเดือนพฤศจิกายน 2551 และเมื่อต้นปี 2552 ตรวจพบ WORM_DOWNAD.AD และ WORM_DOWNAD.KK โดยหนอน DOWNAD เริ่มใช้ประโยชน์จากระบบปฏิบัติการไมโครซอฟท์ ซึ่งไมโครซอฟท์มีการออกแพทช์อัพเดต MS08-067 เมื่อเดือนตุลาคม

ทั้งนี้ หนอน DOWNAD.AD เพิ่มความสามารถในการแพร่กระจายผ่านทางระบบเครือข่าย และผ่านทางอุปกรณ์จัดเก็บข้อมูล (เช่น ยูเอสบี ไดรฟ์) ด้วยการใช้ฟังก์ชั่นการทำงานแบบอัตโนมัติในวินโดวส์

ส่วนหนอน DOWNAD.KK จะทำการปิดกั้นบริการรักษาความปลอดภัย, ปิดกั้นการติดเชื้อในเครื่องคอมพิวเตอร์ขณะที่เชื่อมต่อไปยังเว็บไซต์รักษาความปลอดภัย จากนั้นจะทำการดาวน์โหลดโทรจันเข้าสู่เครื่อง นอกจากนี้ยังแพร่กระจายการติดเชื้อคอมพิวเตอร์ผ่านทางบริการติดต่อสื่อสารแบบเพียร์ทูเพียร์ ซึ่งรวมถึงขั้นตอนวิธีการอัพเดตเครื่องคอมพิวเตอร์ที่ติดเชื้อ

สำหรับเป้าหมายของหนอนร้าย คือการสร้างเครือข่ายบ็อตเน็ต เพื่อทำให้เครื่องคอมพิวเตอร์ติดเชื้อ และสร้างจุดส่งอี-เมลขยะ เพื่อขโมยข้อมูลส่วนบุคคล (เช่น ข้อมูลผู้ใช้, รหัสผ่าน, ข้อมูลบัตรเครดิต ฯลฯ) และชี้นำผู้ใช้งานคอมพิวเตอร์ไปยังเว็บไซต์ที่เป็นอันตรายเพื่อหลอกให้ดาวน์โหลดมัลแวร์เพิ่มเติม

โดยในวันที่ 1 เมษายน 2552 คาดว่าหนอนร้ายสายพันธุ์ใหม่ที่ชื่อว่า WORM_DOWNAD.KK จะเริ่มปรับเปลี่ยนวิธีในการสื่อสารกับเครื่องคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่ติดเชื้อบ็อตเน็ต และจะเพิ่มจำนวนเครื่องโดยการติดต่อกับเครื่องคอมพิวเตอร์อื่นเพื่อแพร่กระจายเชื้อร้าย ไม่มีหลักฐานระบุว่าหนอนจะทำอะไรที่นอกเหนือจากการปรับเปลี่ยนวิธีการสื่อสาร

สำหรับวิธีที่จะป้องกันได้ดีคือ หมั่นอัพเดตโปรแกรมต่อต้านไวรัสและอัพเดตการอุดช่องโหว่ของไมโครซอฟท์ โดยสามารถสแกนไวรัสออนไลน์เพื่อตรวจสอบได้ ที่ http://housecall.trendmicro.com/ เพื่อตรวจสอบว่าเครื่องคอมพิวเตอร์ของคุณติดเชื้อหรือไม่ และหากพบว่าเครื่องคอมพิวเตอร์ของคุณได้รับการติดเชื้อ สามารถคลิกไปดูคำแนะนำเพิ่มเติมได้ดังนี้ :

สำหรับผู้บริโภคทั่วไป คลิกไปดูคำแนะนำได้ที่ http://esupport.trendmicro.com/Pages/How-do-I-protect-my-system-from-the-new-variant-of-the-WORM_Downad_KK%20infection.aspx

สำหรับองค์กรธุรกิจขนาดเล็ก คลิกไปดูคำแนะนำได้ที่ http://esupport.trendmicro.com/Pages/How-to-clean-the-WORM_DOWNAD-and-WORM_DOWNADAD-malware-For-Small-and-M.aspx

สำหรับองค์กรธุรกิจขนาดกลาง และขนาดใหญ่ คลิกไปดูคำแนะนำได้ที่

http://esupport.trendmicro.com/Pages/How-to-clean-Worm_Downad-malware.aspx

มติชนรายวัน วันที่ 04 เมษายน พ.ศ. 2552 ปีที่ 32 ฉบับที่ 11347 หน้า 18

ที่มา :
http://www.matichon.co.th/matichon/view_news.php?newsid=01tec06040452&sectionid=0143&day=2009-04-04