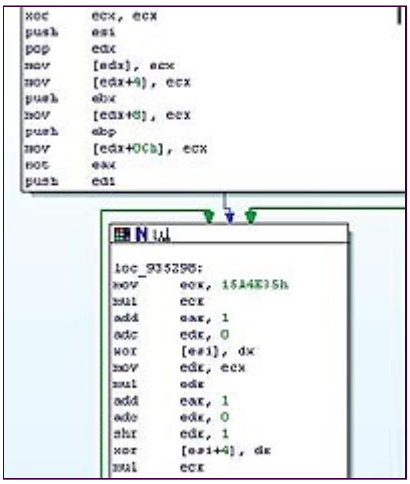
Matichon Online
วันที่ 15 เมษายน พ.ศ. 2552
http://www.matichon.co.th/

เผยวิธีการทำงานของเจ้าหนอนร้าย



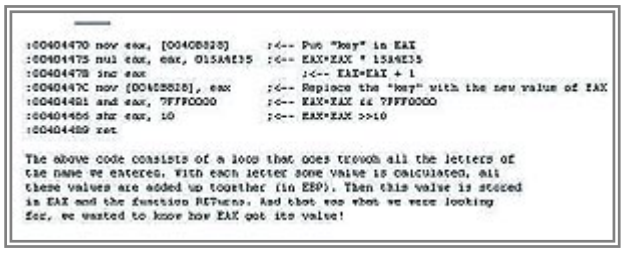
นายพอล เฟอร์กูสัน นักวิจัยภัยคุกคามชั้นสูง จาก เทรนด์ ไมโคร อิงค์ เปิดเผยว่า จากเหตุการณ์หนอนอันตรายระบาดช่วงวันเมษาหน้าโง่ หรือ April Fool"s Day จากการวิเคราะห์ขั้นตอนการตรวจสอบการติดต่อสื่อสารที่ใช้โปรโตคอลเพียร์ทูเพียร์ (P2P) ของหนอนร้าย WORM_DOWNAD.KK พบว่าการกระทำดังกล่าวได้รับการสนับสนุนจากแหล่งที่มาบางแห่ง และค้นพบการทำงานของโค้ดบางอย่างที่สำคัญซึ่งถูกนำมาใช้จากเอกสารที่มีอยู่ย้อนหลังไปเมื่อ พ.ศ.2540

หน่วยงานที่ดูแลด้านการรักษาความปลอดภัยระบบคอมพิวเตอร์ ประเทศฝรั่งเศส และความช่วยเหลือด้านการวิเคราะห์จากหน่วยงานระดับชาติ SRI International เกี่ยวกับวิธีการทำงานของ WORM_DOWNAD.KK p2p ให้ความสนใจไปที่โค้ดเฉพาะในพอร์ตชุดคำสั่งประจำ (โปรแกรมคอมพิวเตอร์ซึ่งถูกเรียกใช้บ่อย) เพื่อแพร่กระจายหนอนร้าย WORM_ DOWNAD.KK p2p

รูปที่ 1 - พอร์ตชุดคำสั่งประจำเพื่อแพร่กระจายหนอนร้าย WORM_ DOWNAD.KK p2p

โดยเฉพาะค่า "15A4E35h" - ซึ่งเป็น "hard-coded" ต้นกำเนิดสำหรับสุ่ม-หมายเลขชุดคำสั่งประจำ (โปรแกรมคอมพิวเตอร์ซึ่งถูกเรียกใช้บ่อย) เพื่อแพร่กระจายหนอนร้าย WORM_DOWNAD.KK นอกจากนี้ ยังพบอีกว่าสิ่งที่สำคัญที่สุด คือโค้ดนี้ไม่ใช่ของใหม่ แต่มันเคยเกิดขึ้นเมื่อปี พ.ศ.2540 ในชื่อ "raZZia" ที่พบในการแพร่กระจายชุดคำสั่งประจำ (โปรแกรมคอมพิวเตอร์ซึ่งถูกเรียกใช้บ่อย)

ความจริงโค้ดดังกล่าวเกือบจะแพร่กระจายเชื้อร้าย WORM_DOWNAD.KK เพื่อใช้เป็นตัวแพร่กระจายชุดคำสั่งประจำ (โปรแกรมคอมพิวเตอร์ซึ่งถูกเรียกใช้บ่อย) โดยกำหนดว่าพอร์ตไหนจะใช้เพื่อการติดต่อสื่อสารแบบเพียร์ทูเพียร์ (P2P) กับเครื่องคอมพิวเตอร์ในเครือข่าย อีกทั้งผู้สร้างหนอนร้าย WORM_DOWNAD.KK ยังเปลี่ยนความต้องการใหม่ แทนที่จะใช้มันเพื่อพุ่งเป้าไปที่ชุดคำสั่งประจำหลัก เปลี่ยนเป็นการสุ่มตัวอย่างหาพอร์ตชุดคำสั่งเพื่อแพร่กระจายเชื้อร้ายต่อไป



รูปที่ 2 - โค้ด "1997 raZZia"

เช่นเดียวกันกับชุดคำสั่งด้านบน โดยเฉพาะค่าความสำคัญของ "15a4e35h" เป็น hard-coded ในหนอนร้าย WORM_DOWNAD.KK ซึ่งเป็นตัวแปรสำคัญในการแพร่พันธุ์ ทั้งการเลือก key-gen code และ WORM_DOWNAD.KK จะใช้หลักตรรกวิทยาที่ใกล้เคียงกันมากที่สุด โค้ด WORM_DOWNAD.KK จะมีข้อแตกต่างเพิ่มขึ้นมาเล็กน้อย แต่ว่าคุณสามารถที่จะดูได้จากตารางด้านล่าง

รูปที่ 3 – ภาพแสดงตัวอย่างว่าโค้ดนี้เคยถูกใช้โดยอาชญากรใต้ดิน

รูปที่ 4 – ตัวอักษรจีนที่ไม่ชัดเจน

เป็นตัวอักษรจีนที่แปลความหมายได้ว่า "บริเวณทุ่งหญ้าที่หนาแน่น" หรือ "ต้นหญ้า, วัชพืชที่หนาแน่น" ซึ่งเป็นคำเหน็บแนมที่หมายถึงโฮสต์ที่ติดเชื้อร้ายเป็นจำนวนมาก ตัวอย่างเช่น เครือข่ายบ็อตเน็ตขนาดใหญ่

ความจริงแล้ว 15A4E35h คือรูปแบบเลขทศนิยม 22695477 และ 15A4E35 ไม่ได้มีความหมายพิเศษสำหรับ raZZia - เพียงแต่พวกเขาเคยใช้โค้ดดังกล่าว และขณะนี้วิธีการดังกล่าวถูกนำกลับมาใช้อีกครั้งโดยผู้สร้างโค้ด Conficker

ต่อด้านหลัง

นักวิจัยภัยคุกคามสรุปข้อมูลได้ว่า กลุ่มคนบางพวกซึ่งอาจจะเป็นอาชญกรไซเบอร์ หรืออีกคำหนึ่งที่เรามักจะพบ คือ Russkrainians (อาชญกรไซเบอร์ชาวรัสเซียและยูเครน) เลือกใช้ลักษณะบางอย่างของวัฒนธรรมจีน เพื่อก่อให้เกิดผลกระทบ และเกิดความเสียหายแก่ชาวจีน ขณะนี้อาชญกรไซเบอร์ชาว Russkrainians มีแนวโน้มที่จะสร้างความปั่นป่วนเพิ่มขึ้นโดยใช้สินทรัพย์ของชาวจีน (เช่น ในการจดทะเบียนโดเมน. .CN ฯลฯ) เพื่อหลอกลวงกลุ่มคนที่ไม่รู้เรื่องให้ตกเป็นเหยื่อของอาชญกรไซเบอร์ดังกล่าวด้วย

พวกเรายังคงวิเคราะห์โค้ดร้ายนี้ และคิดว่าน่าจะมีประโยชน์ในแง่ของการพยายามตรวจสอบหาข้อเท็จจริงให้แน่ชัด หรือถ้าหากเกิดเหตุการณ์ใดๆ ที่แสดงให้เห็นว่าโค้ดนี้ถูกนำกลับมาใช้โดยเหล่าอาชญากรไซเบอร์ใต้ดิน และถูกพบในสถานที่ที่ไม่ควรจะเกิด

เทรนด์ ไมโคร มีแนวทางการป้องกันข้อมูลเบื้องต้นสำหรับผู้ใช้งานออนไลน์ว่า ป้องกันโดยตรวจสอบชื่อเสียง และประวัติเว็บไซต์ (Web Reputation) สามารถวัดระดับความปลอดภัย และความน่าเชื่อถือของเว็บไซต์ก่อนเข้าชมได้ และต้องมั่นใจว่าอัพเดทหรือติดตั้งซอฟต์แวร์ป้องกันไวรัสใหม่ ทั้งควรหมั่นอัพเดท วินโดว์ส (Update Windows) ทุกครั้งที่มีการเตือน โอกาสที่จะมีปัญหากับเวิร์มหรือไวรัสเข้ามาแทรกแซงการทำงานของเครื่องคอมพิวเตอร์ก็จะมีน้อยลง

มติชนรายวัน วันที่ 15 เมษายน พ.ศ. 2552 ปีที่ 32 ฉบับที่ 11358 หน้า 26

ที่มา :
http://www.matichon.co.th/matichon/view_news.php?newsid=01epe02150452&sectionid=0147&day=2009-04-15