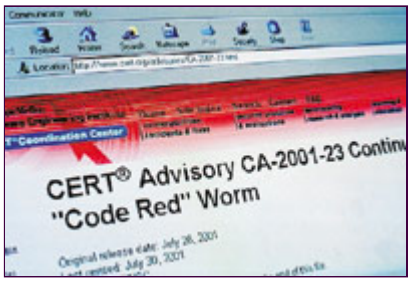
ข่าวประชาสัมพันธ์
มหาวิทยาลัยศรีนครินทรวิโรฒ
114 สุขุมวิท 23 แขวงคลองเตยเหนือ เขตวัฒนา กรุงเทพฯ 10110 โทรศัพท์ 0-2649-5005 ภายใน 5666
โทรศัพท์/โทรสาร 0-2258-0311
ข่าวจากหนังสือพิมพ์มติชน ฉบับประจำวันที่ 2 เดือนมีนาคม พ.ศ.2552 หน้า 26
ศูนย์สารสนเทศและการประชาสัมพันธ์ ได้จัดระบบข่าวสื่อสิ่งพิมพ์ สนใจดูที่ได้ http://news.swu.ac.th/newsclips/

20 ไวรัสที่ถูกบันทึกไว้ในประวัติศาสตร์



ในโอกาสครบ 20 ปี เทรนด์ ไมโคร อิงค์ ธุรกิจจัดการและรักษาความปลอดภัยข้อมูลบนอินเตอร์เน็ต จัดทำรายงานสรุป 20 อันดับไวรัสที่ถูกบันทึกไว้ในประวัติศาสตร์ พร้อมเสนอแนะแนวทางการป้องกันภัยคุกคามข้อมูลไว้

20 อันดับไวรัสที่ถูกบันทึกไว้ในประวัติศาสตร์

1.CREEPER (1971) โปรแกรมหนอนอินเตอร์เน็ตตัวแรกเกิดขึ้นเมื่อวันที่ 10 ธันวาคม ในคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ TOPS TEN

2.ELK CLONER (1985) ไวรัสคอมพิวเตอร์ส่วนบุคคลตัวแรกที่เกิดกับ Apple IIe เป็นผลงานของเด็กนักเรียนระดับมัธยมศึกษา (เกรด 9)

3.THE INTERNET WORM (1985) เขียนโดยบุคลากรในมหาวิทยาลัยคอร์เนลล์ซึ่งมีผลต่อการใช้งานอินเตอร์เน็ต

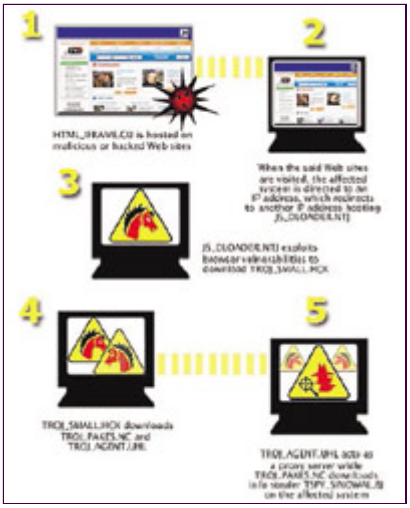
4.PAKISTANI BRAIN (1988) ไวรัสตัวแรกที่ติดกับคอมพิวเตอร์พีซีไอบีเอ็ม เขียนโดยสองพี่น้องจากปากีสถาน ถือเป็นไวรัสตัวแรกที่สื่อให้ความสนใจอย่างแพร่หลาย

5.JERUSALEM FAMILY (1990) มีสายพันธุ์ที่แตกต่างกันประมาณ 50 สายพันธุ์ เชื่อกันว่ามีต้นกำเนิดมาจากมหาวิทยาลัยเยรูซาเล็ม

6.STONED (1989) ไวรัสที่แพร่ระบาดหนักที่สุดช่วงสิบปีแรก ติดเชื้อในส่วนบูตระบบ /.mbr ส่งผลให้รีบูตระบบหลายครั้งและยังแสดงข้อความว่า "your computer is now stoned"

7.DARK AVENGER MUTATION ENGINE (1990) เขียนเมื่อปี 1988 แต่นำไปใช้ครั้งแรกต้นปี 1990 เช่นเดียวกับไวรัส POGUE และ COFFEESHOP กลไกการกลายพันธุ์ได้หลากหลายรูปแบบของไวรัสตัวนี้ทำให้ไวรัสสามารถทำงานได้ตลอดเวลา

8.MICHEANGELO (1992) สายพันธุ์หนึ่งของ STONED ความสามารถทำลายล้างสูง โดยวันที่ 6 มีนาคม ไวรัสตัวนี้จะลบ 100 เซ็คเตอร์แรกของฮาร์ดไดรฟ์ให้ใช้งานไม่ได้



9.WORLD CONCEPT (1995) ไวรัส Microsoft Word Macro ตัวแรกที่แพร่กระจายสู่โลกภายนอก โดยมีการแอบใส่ข้อความไว้ว่า "That"s enough to prove my point" ถือเป็นการเปิดศักราชใหม่ในยุคที่สองของไวรัสคอมพิวเตอร์ และที่สำคัญเป็นไวรัสคอมพิวเตอร์ที่เกิดจากแฮกเกอร์ซึ่งมีทักษะน้อยมาก

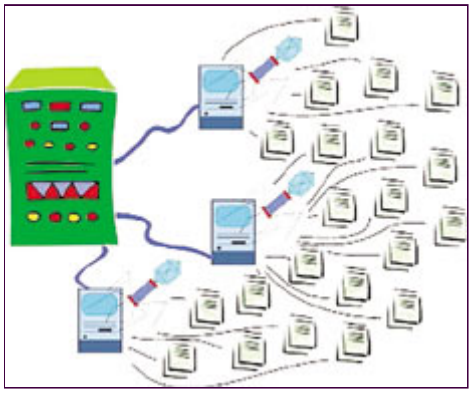
10.CIH/CHERNOBYL (1998) ไวรัส Chernobyl เป็นไวรัสทำลายล้างมากที่สุดเท่าที่เคยพบ เริ่มปฏิบัติการทำลายล้างโดยอาศัยเงื่อนไข คือ เมื่อปฏิทินในเครื่องคอมพิวเตอร์ตรงกับวันที่ 26 ในทุกๆ เดือน สามารถทำลายข้อมูลในฮาร์ดดิสก์ และทำลายข้อมูลการบูตที่เก็บอยู่ในไบออส โดยแฟลชไบออสด้วยข้อมูลขยะส่งผลให้ข้อมูลต่างๆ ที่เคยแสดงตอนบูตเครื่องกลายเป็นหน้าว่างๆ และไม่สามารถเรียกขึ้นมาใช้งานได้อีกต่อไป

11.MELISSA (1999) ไวรัสสำคัญตัวแรกที่แพร่ระบาดผ่านอี-เมล และเป็นการเริ่มต้นของยุคไวรัสอินเตอร์เน็ตอย่างแท้จริง แม้ Melissa ไม่ได้มีวัตถุประสงค์เพื่อการทำลาย แต่ก่อให้เกิดความรำคาญแก่ผู้ใช้เนื่องจากจะทำให้กล่องรับอี-เมลเต็มในทุกที่ที่เกิดการติดเชื้อ

12.LOVEBUG (2001) หนอนอี-เมลที่ได้รับความนิยมสูงสุด เป็นรูปแบบของการใช้ชุมชนเครือข่ายสังคมออนไลน์ให้เป็นประโยชน์

13.Code RED (2001) ตั้งชื่อตามเครื่องดื่มที่มีคาเฟอีนสูงที่ได้รับความนิยม ไวรัสเครือข่ายตัวนี้จะอาศัยอยู่ในคอมพิวเตอร์ที่มีช่องโหว่ความปลอดภัย และทำการแพร่ระบาดด้วยตัวเอง

14.NIMDA (2001) เรียกกันว่า "Swiss Army Knife" หรือมีดอเนกประสงค์ของไวรัส ซึ่งจะใช้หลายวิธีในการเข้าสู่เครือข่าย ไม่ว่าจะเป็นหน่วยความจำล้นอี-เมล การใช้เครือข่ายร่วมกัน และวิธีการอื่นๆ อีกเป็นสิบวิธี



15.BAGEL/NETSKY (2004) เป็นไวรัสที่ออกแบบมาโดยมีความสามารถเทียบเคียงกัน และต่อสู้กันเอง แต่ละตัวสร้างสายพันธุ์ออกมาอีกนับร้อยสายพันธุ์ และใช้เทคโนโลยีใหม่ๆ ซึ่งประสบความสำเร็จในการแพร่ระบาดอย่างมาก หนอนทั้งสองตัวนี้ติดอยู่ในกระแสข่าวตลอดทั้งปี

16.BOTNETS (2004) นักรบซอมบี้ในโลกอินเตอร์เน็ตเหล่านี้ช่วยงานอาชญากรไซเบอร์ด้วยการสะสมกำลังพลคอมพิวเตอร์ที่ติดเชื้ออย่างไม่มีวันสิ้นสุด โดยอาชญากรไซเบอร์จะสามารถกำหนดค่าใหม่ให้กับคอมพิวเตอร์ในเครือข่ายได้ เพื่อให้ส่งต่อสแปม เพิ่มเหยื่อติดเชื้อ และขโมยข้อมูล

17.ZOTOB (2005) หนอนตัวนี้มีผลเฉพาะกับระบบ Windows 2000 ที่ไม่ได้ติดตั้งโปรแกรมซ่อมแซม แต่ความสามารถที่โดดเด่น เข้าควบคุมไซต์ของสื่อรายใหญ่หลายแห่ง รวมทั้งซีเอ็นเอ็น และนิวยอร์กไทม์ส ด้วย

18.ROOTKITS (2005) หนึ่งในเครื่องมือที่ได้รับความนิยมสูงสุดในโลกของโค้ดที่เป็นอันตราย ซึ่งถูกใช้เพื่อทำให้มัลแวร์อื่นสามารถซ่อนตัวอยู่ในคอมพิวเตอร์ได้ โดยมัลแวร์ที่ซ่อนตัวอยู่จะทำงานที่เป็นอันตรายอย่างลับๆ

19.STORM WORM (2007) ไวรัสลวงที่ที่เกิดขึ้นซ้ำนับพันๆ ครั้ง และในท้ายที่สุดก็จะสร้างบ็อตเน็ตที่มี

ขนาดใหญ่ที่สุดในโลก โดยเชื่อว่ามีคอมพิวเตอร์ที่ติดเชื้อในเวลาเดียวกันมากกว่า 15 ล้านเครื่อง และอยู่ภายใต้การควบคุมของอาชญกรใต้ดิน

20.ITALIAN JOB (2007) ไม่ใช่มัลแวร์ที่ใช้เครื่องมือเดี่ยวๆ แต่เป็นการโจมตีร่วมกันโดยใช้ชุดเครื่องมือที่จัดเตรียมไว้ล่วงหน้าหรือรู้จักว่า MPACK เพื่อสร้างมัลแวร์รุ่นใหม่เพื่อการขโมยข้อมูลขึ้นมา และมีเว็บไซต์กว่าหมื่นแห่งตกเป็นเหยื่อ

วิธีป้องกันภัยคุกคามข้อมูล

⊙ เปิดใช้งานและปรับปรุงซอฟต์แวร์รักษาความปลอดภัยให้ทันสมัยเสมอ โดยเฉพาะถ้าใช้งานแล็ปท็อปที่ต้องเชื่อมต่อกับเครือข่ายที่ไม่มีการป้องกันใดๆ ในบริเวณสนามบิน ร้านกาแฟ และสถานที่ต่างๆ

⊙ ตรวจสอบให้แน่ใจว่าซอฟต์แวร์ป้องกันภัยบนเว็บครอบคลุมการป้องกันอี-เมล และแอพพลิเคชั่นการประมวลผลที่ใช้ทั้งหมด และสามารถแจ้งเตือนเกี่ยวกับปริมาณการส่งผ่านข้อมูลทั้งเข้าและออกจากคอมพิวเตอร์ของผู้ใช้งานในเวลาจริง

⊙ ปรับใช้เทคโนโลยีล่าสุด เช่น การป้องกันโดยเทคโนโลยีการตรวจสอบชื่อเสียง และประวัติเว็บไซต์ (Web Reputation) ซึ่งสามารถวัดระดับความปลอดภัย และความน่าเชื่อถือของเว็บไซต์ก่อนที่คุณจะเข้าเยี่ยมชมได้ ควรใช้เทคโนโลยีการตรวจสอบประวัติเว็บร่วมกับเทคโนโลยีการกรองยูอาร์แอล และการสแกนเนื้อหา

⊙ ถ้าผู้ใช้งานใช้ระบบปฏิบัติการ Microsoft Windows ให้เปิดใช้งาน Automatic Update และติดตั้งโปรแกรมปรับปรุงใหม่ๆ ทันทีที่พร้อมใช้งาน

สำหรับผู้ใช้งานคอมพิวเตอร์-อินเตอร์เน็ตที่ต้องการทราบข้อมูลเกี่ยวกับภัยคุกคามข้อมูลรูปแบบใหม่ๆ ที่เกิดขึ้น คลิกไปได้ที่ http://blog.trendmicro.com หรือต้องการหาเครื่องมือป้องกันภัยคุกคามข้อมูลบนเว็บโดยไม่ต้องเสียค่าใช้จ่ายใดๆ คลิกที่ http://us.trendmicro.com/us/products/personal/ free-tools-and services/index.html