Matichon Online
วันที่ 20 มกราคม พ.ศ. 2552
http://www.matichon.co.th/

8 ภัยคุกคามข้อมูลที่พบมาก

ศูนย์วิจัยเทรนด์แล็ปส์ บริษัท เทรนด์ ไมโคร อิงค์ จัดทำรายงานสรุปภัยคุกคามข้อมูลที่พบมากที่สุด 8 ประเภทในปี 2551 พบว่า

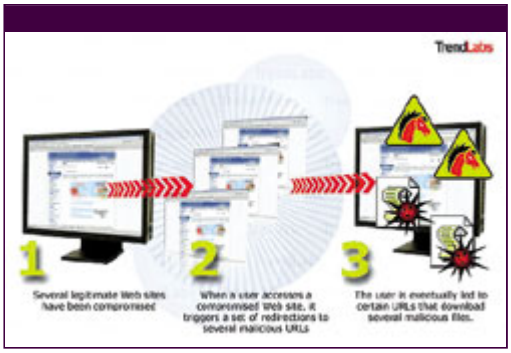
@ แพร่ระบาดสูงสุด : สร้างอันตรายในวงกว้าง

การโจมตีที่มีเป้าหมายไปยังกลุ่มผู้ใช้เฉพาะและเว็บไซต์ยอดนิยม มีเว็บไซต์หลายประเภท ทั้งบันเทิง การเมือง ช็อปปิ้งออนไลน์ เครือข่ายทางสังคมถูกใช้แพร่ระบาดมัลแวร์ ภาวะอันตรายนี้เกิดสูงสุดในเดือนพฤษภาคม มีเว็บไซต์ทั่วโลกที่ติดโค้ดร้าย ส่งไปถึงผู้ใช้อินเตอร์เน็ต ดูเหมือนว่าแนวโน้มนี้ยังคงเกิดต่อเนื่องเกินกว่าที่คาดหมายไว้

@ ฝังแน่นที่สุด : บ็อตเน็ต

บ็อตเน็ตเปรียบเสมือนสิ่งชั่วร้ายที่มีอยู่ในทุกที่ โดยตัวอันตรายสำคัญอย่าง Storm, Kraken, Mega-D/Odzok, MayDay และ ASProx ปรากฏขึ้นเป็นระลอกๆ ตลอดปี 2551 และมีอยู่อย่างต่อเนื่อง เมื่อนักวิจัยบ็อตเน็ตดำเนินการตรวจสอบ แม้มีการปิดเว็บไซต์ McColo ผู้สนับสนุนอาชญากรรมไซเบอร์รายใหญ่ไปแล้วแต่ก็แค่หยุดกลุ่มผู้เชี่ยวชาญด้านบ็อตชั่วคราว ที่พวกเขาจะค้นหาเครื่องมืออื่นๆ มาใช้ในการแพร่ระบาดอีกครั้ง

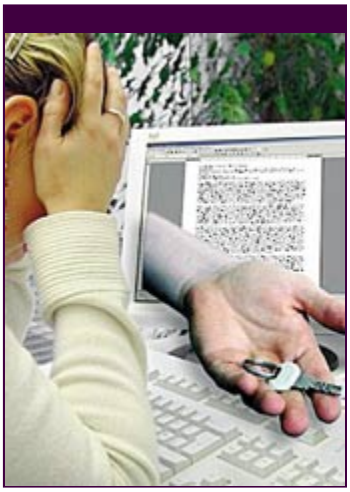
@ แคมเปญจัดจำหน่ายใหญ่ที่สุด : โปรแกรมป้องกันไวรัส (ของปลอม)



ซอฟต์แวร์ป้องกันไวรัสลวง แบ่งทำงานเป็น 2 ขั้น ขั้นแรกจะหลอกผู้ใช้ว่าระบบของพวกเขาติดมัลแวร์แล้วด้วยการสร้างอาการติดเชื้อหลอกๆ ขึ้นมา ขั้นต่อมาจะชักชวนให้ผู้ใช้ซื้อโปรแกรมป้องกันไวรัสปลอม เพื่อล้างการติดเชื้อลวงนั้นภัยคุกคามนี้ใช้ช่องทางติดเชื้อและมาในหลายรูปแบบ ตั้งแต่สแปมไปจนถึงการวางอันดับเว็บของตนให้ติดในเว็บไซต์ค้นหายอดนิยม (SEO) เพื่อให้เหยื่อหลงเชื่อซึ่งยังรวมถึงการฝังตัวอยู่ในเว็บไซต์ที่เป็นอันตรายหลายแห่งด้วย

@ ติดตามได้ยากที่สุด : ตัวเปลี่ยน DNS

เทรนด์ ไมโคร ตรวจพบมัลแวร์สองตัวที่เปลี่ยน DNS ได้แก่ TROJ_AGENT.NDT และ BKDR_AGENT.CAHZ ถือเป็นอันตรายต่อโฮสต์ต่างๆ ในเครือข่ายย่อยภายในองค์กร โดยจะติดตั้ง Dynamic Host Configuration Protocol (DHCP) Server ปลอมบนเครือข่ายมัลแวร์เหล่านี้จะตรวจสอบการรับส่งข้อมูลและดักจับ แพคเก็ตที่ร้องขอจากคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย จากนั้นตอบกลับการร้องขอที่ดักจับได้นั้นด้วยแพคเก็ตที่มี DNS server เป็นอันตรายให้ผู้ได้รับแพคเก็ตถูกเปลี่ยนทิศทางไปยังเว็บไซต์อันตรายโดยไม่ได้รับอนุญาต



@ อัตโนมัติที่สุด : ช่องโหว่

หนอน .DLL ชื่อ WORM_DOWNAD.A ได้ใช้ช่องโหว่ MS08-067 แสดงชุดคำสั่งที่ทำให้นักวิเคราะห์ด้านความปลอดภัยเชื่อว่าจะเป็นส่วนประกอบสำคัญในการพัฒนาบ็อตเน็ตใหม่ขึ้นมาโดยมีโฮสต์ที่ไม่ซ้ำกันกว่า 500,000 แห่งที่แพร่ระบาดหนอนตัวนี้ไปยังในประเทศต่างๆ แล้ว และมีข้อบกพร่องซีโร่เดย์ใน Internet Explorer นำไปสู่ภัยคุกคามข้อมูลออนไลน์ขนาดใหญ่ 2 อย่างด้วยได้แก่ การขโมยข้อมูลและโจมตีแบบ SQL Injection (ใช้คำสั่ง SQL เพื่อช่วยในการแฮกระบบ) ซึ่งเกิดกับเว็บไซต์ 6,000 แห่ง อาชญากรไซเบอร์ใช้ประโยชน์ข้อบกพร่องเหล่านี้โดยที่ผู้ใช้ไม่รู้ตัวแม้แต่น้อย

@ ใช้เทคโนโลยีขั้นสูงสุด : รูตคิตส์

รูตคิตส์ MBR (Master Boot Record) เริ่มแพร่ระบาดช่วงต้นปี 2551 ตรวจพบรูตคิตส์ที่ชื่อว่า TROJ_SINOWAL.AD ซึ่งจะค้นหาพาร์ติชันที่สามารถบู๊ตได้ของระบบที่ติดเชื้อ จากนั้นจะสร้าง MBR อันตรายใหม่ขึ้นมาเพื่อโหลดส่วนประกอบของรูตคิตส์ที่ชื่อว่า RTKT_AGENT.CAV ลงไว้ในระบบ แล้วทำการบันทึกไว้ในเซกเตอร์ภายในพาร์ติชันที่บู๊ตได้

ต่อด้านหลัง

@ อันตรายสูงสุด : มัลแวร์เรียกค่าไถ่ (Ransomware)

มัลแวร์เรียกค่าไถ่ GPcode รุ่นใหม่ที่ เทรนด์ ไมโครตรวจพบชื่อว่า TROJ_RANDSOM.A พบในเดือนพฤศจิกายน มัลแวร์ตัวนี้จะค้นหาและเข้ารหัสไฟล์ที่พบในไดรฟ์ที่อ่านและเขียนได้ของระบบจากนั้นก็จะแสดงให้ผู้ใช้เห็นว่าไม่สามารถเข้าถึงไฟล์ดังกล่าวได้ถ้าไม่มีคีย์เข้ารหัสลับเหยื่อจะได้รับแจ้งว่าต้องซื้อเครื่องมือถอดรหัสลับซึ่งจะมีการทิ้งไฟล์ข้อความไว้ในแต่ละโฟลเดอร์ที่มีไฟล์ที่ถูกเข้ารหัสลับไว้

@ น่ารำคาญที่สุด : มัลแวร์แบบรันอัตโนมัติ (AUTORUN)

ไดรฟ์แบบถอดได้และไดรฟ์ที่ใช้งานจริงถือเป็นแหล่งติดเชื้อสูงสุดอันดับ 4 ของโลก โดย 15% ของการติดเชื้อทั้งหมดในเอเชียและออสเตรเลียมาจากมัลแวร์ที่เกิดจากไดรฟ์แบบถอดได้ประเทศในเอเชียส่วนใหญ่จะมีมัลแวร์แบบรันอัตโนมัติเป็นตัวติดเชื้อสูงสุดและเป็นมัลแวร์ที่ติดเชื้อมากที่สุดในพีซีของประเทศในภูมิภาคยุโรป ตะวันออกกลางและแอฟริกา (EMEA) ด้วย นอกจากนี้มัลแวร์ดังกล่าวยังสามารถผ่านเข้าไปยังเครือข่ายของนาซาและกระทรวงกลาโหมสหรัฐได้สำเร็จแล้วด้วย

มติชนรายวัน วันที่ 20 มกราคม พ.ศ. 2552 ปีที่ 32 ฉบับที่ 11273 หน้า 26

ที่มา : http://www.matichon.co.th/matichon/view_news.php?newsid=01epe01200152&sectionid=0147&day=2009-01-20