ก4889

เดลินิวส์

ฉบับที่ 19941, 4 มกราคม 2546 : หน้า 12

เจาะลึกพฤติกรรมไวรัสร้าย

จากการศึกษาของศูนย์ TrendLabs ของบริษัทเทรนด์ ไมโคร อิงค์ ซึ่งเป็นศูนย์สนับสนุนและวิจัยเครือข่ายป้องกันไวรัส ทำหน้าที่ในการตรวจหาภัยคุกคามต่อระบบรักษาความปลอดภัยที่อาจเกิดขึ้นได้ทั่วโลกรวมถึงพัฒนาการให้นิยามคำศัพท์ใหม่สำหรับไวรัส การตรวจหาไวรัสสายพันธุ์ใหม่และกำจัดไวรัสเหล่านั้น

ทั้งนี้จากการศึกษาในระยะ 3 ปีที่ผ่านมา (พ.ศ. 2543-2545) โดยเฉพาะในช่วงเดือนพฤษภาคม-ตุลาคม ซึ่งถือว่าเป็นช่วงที่เหล่าโปรแกรมร้ายออกอาละวาดมากที่สุด ปรากฏว่าปี พ.ศ. 2544 มีการแพร่ระบาดทั่วโลกเพิ่มขึ้นถึง 175% เมื่อเปรียบเทียบกับปีพ.ศ. 2543

โดยก่อนช่วง 3 ปีดังกล่าว การระบาดของโปรแกรมร้ายจะแพร่ผ่านแผ่นฟลือปปี้ดิสก์ หรือไฟล์ที่ติดไวรัสส่งไปยังคนที่เราติดต่อ หรือการใช้ไดร์ฟร่วมกัน ซึ่งการแจ้งเตือนของบริษัทต่าง ๆ ไปยังแผนกต่าง ๆ ให้อัพเกรดโปรแกรมป้องกันไวรัส จะเกิดขึ้นก็ต่อเมื่อได้รับผลกระทบจากไฟล์ที่ติดไวรัสแล้ว

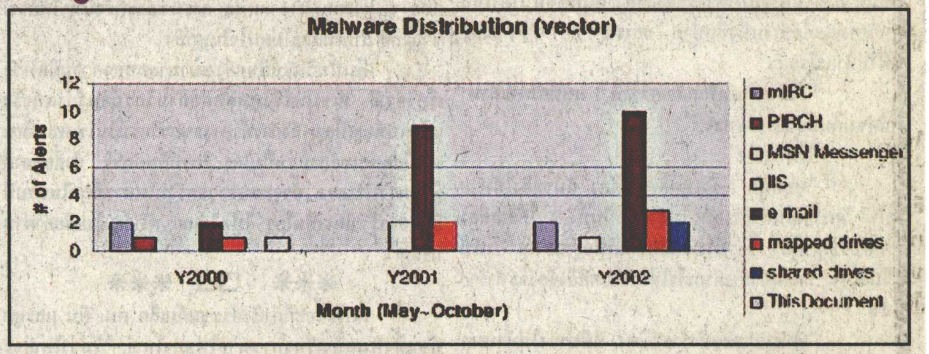
สำหรับในช่วง 3 ปีที่ศึกษาพบว่าผู้เขียนไวรัสได้มีการพัฒนาเทคโนโลยีของหนอนไวรัสคอมพิวเตอร์อย่างรวดเร็ว 4 ใน 5 ส่วนของการระบาด เป็นหนอนไวรัสคอมพิวเตอร์ และปัจจุบันการแพร่กระจายเป็นหนอนไวรัสคอมพิวเตอร์ถึง 100%

จากการสำรวจพบว่าปัจจุบันการแพร่ระบาดของแมคโคร ไวรัส และไวรัส สคริปต์มีการแพร่ระบาดน้อยลงมาก เห็นได้ชัดในปี 2545

หากพิจารณาถึงการเปลี่ยนแปลงของช่องทางในการแพร่ระบาดไวรัสทางคอมพิวเตอร์ ในปี พ.ศ. 2545 พบว่าเกิดจากการใช้ Internet relay chat (IRC) ซึ่งเป็นระบบการติดต่อสนทนาเป็นกลุ่มบนอินเทอร์เน็ต และการมุ่งโจมตีบนเว็บ เซิร์ฟเวอร์ อาทิ ไมโครซอฟท์ อินเทอร์เน็ต อินฟอร์เมชั่น เซอร์วิส (IIS) และอาพาเช่ (Apache) และการแพร่ไวรัสผ่าน mass-mailing (การส่งเมล์), mapped drive (การใช้ไดร์ฟของผู้อื่น) และ shared driyes (การให้ผู้อื่นมาร่วมใช้ไดร์ฟ) รวมทั้งการส่งข้อความ Instant Messaging ซึ่งถือว่าไวรัสใช้ช่องทางที่หลากหลายยิ่งขึ้น

ส่วนหนอนไวรัสคอมพิวเตอร์ส่วนใหญ่จะใช้อีเมลเป็นช่องทางแพร่มากที่สุด และลวงให้ผู้ใช้คลิกและเปิดไฟล์แนบ นอกจากนั้นยังสามารถบีบตัวเอง (self compression) และการเข้ารหัส encryption ซึ่งมีความซับซ้อน และยากต่อนักวิเคราะห์ในการติดตามพฤติกรรมพวกโปรแกรมร้ายว่ากำลังทำอะไรอยู่

มิหนำซ้ำยังกลายเป็นเครื่องมือของแฮคเกอร์ทำให้แฮคเกอร์สามารถเจาะและล้วงข้อมูลที่สำคัญได้จากทางประตูหลังของระบบ



กราฟแสดงช่องทางของโปรแกรมร้ายแบ่งตามการใช้งาน

ความร้ายแรงที่เกิดกับโปรแกรมอีเมลไม่ได้จำกัดวงแค่โปรแกรมไมโครซอฟท์ เอาต์ลุค เพราะคนเขียนไวรัสทุกวันนี้ไม่ได้มุ่งเป้าหมายที่ระบบโปรแกรมไมโครซอฟท์ เอาต์ลุค และเอาต์ลุค เอ็กซเพรสเท่านั้น แต่รวมถึงโปรแกรมอีเมลที่ใช้โปรโตคอล SMTP (Simple Mail Transfer Protocol) อื่นๆ อีกด้วย

จากข้อมูลดังกล่าวข้างต้น ทำให้สามารถคาดการณ์และวางกลยุทธ์ในการป้องกันไวรัสปี 2546 ดังนี้

คือไวรัสยังคงใช้วิธีแพร่กระจายภัยคุกคามหลายวิธีผนวกเข้าด้วยกัน เช่น แพร่กระจายผ่านทางอีเมลและทางไดร์ฟที่แชร์การใช้งาน หรืออาจจะเป็นช่องทางอื่นโจมตีไปพร้อม ๆ กัน

โปรแกรมร้ายในปัจจุบัน และในอนาคต จะยังคงพยายามต่อไปในการทำให้โปรแกรมป้องกันไวรัสไฟร์วอลล์ และโปรแกรมป้องกันไวรัสม้า โทรจัน ไม่สามารถทำงานได้ องค์กรขนาดใหญ่ควรออกนโยบายในการใช้อินเทอร์เน็ต หรือติดตั้งซอฟต์แวร์กรองเว็บไซต์ทั้งนี้เพื่อป้องกันไม่ให้ผู้ใช้งานท่องไปยังเว็บที่มีโปรแกรมร้ายอยู่โดยไม่ได้ตั้งใจ องค์กรควรติดตั้งซอฟต์แวร์ในการสแกนไวรัสไฟล์แนบที่มากับอีเมล ถึงแม้ว่าซอฟต์แวร์ป้องกันไวรัสสำหรับเกตเวย์จะมีประสิทธิภาพในการตรวจสอบไฟล์ที่เข้ามาในเครือข่ายแล้วก็ตาม

ช่องทางของข้อความอย่าง IRC และการเชื่อมเครือข่ายแบบ P2P มีการเติบโตอย่างมหาศาล เพราะความต้องการในการสื่อสารข้อมูลที่รวดเร็ว เช่นเดียวกับการใช้งานอีเมลที่มีการใช้งานตลอดเวลา

รายงานที่เผยแพร่สู่สาธารณชนฉบับต่างๆ รายงานตรงกันว่าอีกไม่เกิน 5 ปีนับจากนี้ อีเมล 25% จะเป็นอีเมลขยะ (spam mail) แปลว่าอีเมลที่ได้รับมา 10 ฉบับ จะเป็นอีเมลขยะถึง 2 ฉบับทีเดียว ไมโครซอฟท์กำลังผลักดันโครงสร้าง .NET ซึ่งสามารถทำงานได้กับระบบคอมพิวเตอร์ทุกแพลตฟอร์ม ดังนั้น ถ้าไมโครซอฟท์ทำโครงการนี้สำเร็จแล้วละก็ ไวรัสจะใช้ช่องทางนี้ในการแพร่กระจายซึ่งจะสามารถแพร่กระจายได้ทุกแพลตฟอร์มเลยทีเดียว

ผู้บริหารระบบต้องใช้ความระมัดระวังในการประเมินซอฟต์แวร์ที่จำเป็นใช้งานสำหรับองค์กร และเป็นซอฟต์แวร์ที่นักพัฒนาสามารถแก้ไขจุดอ่อนของระบบได้.

เล่นหวยผ่านเว็บระวัง! เจอดี

ผู้เชี่ยวชาญหวั่นเล่นหวยผ่านเว็บ ข้อมูลอาจโดนขโมย ด้านเว็บดังโต้มีการป้องกันแน่นหนา หมดสิทธิที่ข้อมูลจะอันตรธานหรือขายให้กับบริษัทอื่น

สำนักข่าวเอพีรายงานว่า ผู้เชี่ยวชาญระบบรักษาความปลอดภัยคอมพิวเตอร์ของนิวเจอร์ซีย์เตือนผู้ที่ชอบเล่นลอตเตอรี่ทางเว็บไซต์ว่า ระวังข้อมูลต่าง ๆ ที่ใช้ในการสมัครเพื่อเป็นสมาชิกเข้าเล่นลอตเตอรี่ถูกขโมย เนื่องจากข้อมูลเหล่านั้นเป็นข้อมูลส่วนตัวที่สามารถไขความลับเข้าสู่รหัสอื่น ๆ ได้ อาทิ วันเดือนปีเกิด ชื่อ อายุ และอีเมล พร้อมแนะราคาจากส่วนลดและข้อมูลที่ได้ผ่านทางอีเมลไม่คุ้มค่าเมื่อเทียบกับการที่ข้อมูลส่วนตัวถูกขโมย

ด้านตัวแทนขาย ลอตเตอรี่ วีไอพี คลับ เปิดเผยว่า สมาชิกประมาณ 77,000 คน ที่ลงทะเบียนสมัครเพื่อใช้บริการข้อมูลมาเกือบปี ยังไม่เคยพบว่าข้อมูลต่าง ๆ โดนขโมยเพื่อนำไปใช้ในทางไม่ดี ที่สำคัญการสมัครเพื่อเข้าเป็นสมาชิกได้มีการตรวจสอบอย่างละเอียดว่าอายุเกิน 18 ปีหรือไม่ รวมทั้งมีการใส่รหัสผ่านเพื่อเข้าสู่เว็บไซต์ไว้ป้องกันด้วย นอกจากนี้ข้อมูลประวัติทั้งหมดจะไม่มีการเก็บรวบรวมเพื่อนำไปขายให้กับบริษัทที่ทำการขายตรงอื่น ๆ ด้วย.