เดลินิวส์
ฉบับที่ 20,585 วันอังคารที่ 21 กุมภาพันธ์ พ.ศ. 2549 หน้า 16

ก16703

# แนวโน้มภัยคุกคามทางคอมพิวเตอร์ 2549

**ในรอบปีที่ผ่านมาอุตสาหกรรมด้านความปลอดภัยและป้องกันไวรัสมีความเปลี่ยนแปลงไม่มากนัก แต่มีแนวโน้มว่าภัยคุกคามรูปแบบใหม่กำลังเริ่มปรากฏขึ้น ด้วยเหตุที่อินเทอร์เน็ตกลายเป็นเครื่องมือสำคัญด้านการทำตลาด, สื่อสาร และการค้าทั่วโลก แต่โชคร้ายที่มีกลุ่มคนผู้ไม่ประสงค์ดีจำนวนมากกำลังพยายามใช้อินเทอร์เน็ตแสวงหาประโยชน์เข้าตัว ไม่ว่าจะใช้เป็นช่องทางการโฆษณาสินค้าไปจนถึงการก่ออาชญากรรมชโมยหมายเลขบัญชีธนาคารของผู้บริโภค ส่งผลให้ชีวิตในโลกไซเบอร์ดูจะอันตรายไม่น้อย และไม่แปลกที่จะมีบางคนเรียกโลกแห่งนี้เป็น "บ้านป่าเมืองเถื่อน" หรือ wild wild west แห่งสุดท้าย**

จากรายงานสรุปของเทรนด์ ไมโคร ซึ่งวิเคราะห์ภาวะภัยคุกคามคอมพิวเตอร์และเครือข่ายที่เกิดขึ้นในปี 2548 และยังทำนายสิ่งที่จะเกิดขึ้นในปี 2549 และปีต่อ ๆ ไปด้วย บอกว่า ภัยคุกคามที่เกี่ยวกับโปรแกรม IRC และ P2P ได้มีจำนวนมากขึ้นถึง 16% ส่วนสแปมและฟิชชิ่งก็ยังคงเป็นปัญหาใหญ่ที่ผู้ใช้ทั้งองค์กรและผู้ใช้ตามบ้านต้องเผชิญในรอบปีที่ผ่านมา ที่สำคัญสแปมไปได้มาในรูปของภาษาอังกฤษอีกต่อไป มีหลากหลายภาษาทยอยออกมาโจมตีผู้ใช้ตามภูมิภาคมากขึ้นเรื่อย ๆ หรือจะเป็นการขโมยรหัสผ่าน และหนอนบ็อตที่ออกอาละวาด ขณะที่สปายแวร์และแอดแวร์ก็ยังคงซุกซ่อนตัวเองอยู่หลังหน้าเว็บต้องสงสัยทั่วไปบนโลกอินเทอร์เน็ต

รายงานดังกล่าวสรุปด้วยว่าปีที่ผ่านมาถือเป็น "ปีแห่งเกรย์แวร์" ไปโดยปริยาย เนื่องจากครองสัดส่วนของภัยคุกคาม 15 อันดับแรกสูงสุดถึง 65% ซึ่งมีรายงานแจ้งความเสียหายมากถึง 11 ล้านฉบับ

ส่วนวิธีการลวงด้วยแอดเดรสบาร์ครองอันดับหนึ่งด้วยจำนวน 81% ซึ่งฟิชชิ่งรูปแบบนี้จะเลือกผู้โจมผู้ใช้เบราเซอร์อินเทอร์เน็ตเอ็กซ์พลอเรอร์ หรือไออี ที่มีจำนวนมากเกือบ 90% ของผู้ใช้ที่ติดตั้งระบบปฏิบัติการ วินโดว์สไว้ในคอมพิวเตอร์ ทั้งนี้วินโดว์สถือเป็นระบบปฏิบัติการยอดนิยมที่มีผู้ใช้มากถึง 95% ของจำนวนคอมพิวเตอร์ตั้งโต๊ะทั่วโลก ขณะที่การลวงด้วยยูอาร์แอลลดลงเหลือ 13% ในช่วงปลายปีที่ผ่านมาเมื่อเทียบกับต้นปีที่มีจำนวนมากถึง 76%

**รูทคิตส์ (rootkits)**

ด้านไวรัสมือถือ หนอนมือถือตัวแรกถูกค้นพบในเดือนสิงหาคม 2547 ใช้ชื่อว่า SYMBOS_CABIR แพร่ระบาดตัวเองไปยังมือถือเครื่องอื่น ๆ ที่ใช้ระบบปฏิบัติการซิมเบียน 60 ผ่านทางเทคโนโลยีบลูทูธ ซึ่งผู้ใช้งานในเครือข่ายจีเอสเอ็มกว่า 80% ล้วนประสบพบเจอกับหนอนร้ายตัวนี้มาแล้ว

หลังจากหนอนมือถือตัวแรกแพร่ระบาด เทรนด์ไมโครก็ได้คอยบันทึกจำนวนภัยร้ายทางมือถือนี้ตลอดมา และพบว่ากำลังทวีจำนวนเพิ่มมากขึ้น และยังมีความสามารถในการใช้เทคโนโลยีมือถืออื่น ๆ มาเป็นตัวกลางในการแพร่ระบาดด้วย ไม่ว่าจะเป็นเอ็มเอ็มเอส และคุณสมบัติด้านการท่องอินเทอร์เน็ต และการดาวน์โหลดไฟล์แนบท้ายอีเมล์

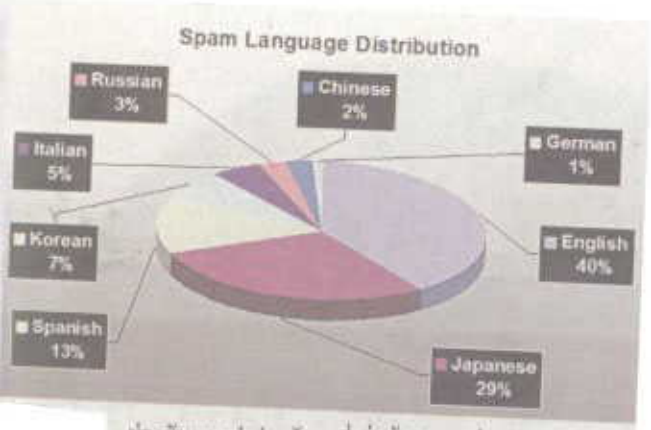
อย่างไรก็ตามเทคโนโลยีมือถือใหม่ ๆ โดยเฉพาะ

**ภัยคุกคาม 15 อันดับแรกของปี2548**
**วัดจำนวนคอมพิวเตอร์ที่ติดเชื้อ**

| Threat Name | Machine Count | Threat Type |
|---|---|---|
| WORM_NETSKY . P | 1,602,069 | Worm |
| JAVA_ BYTEVER . A | 667,448 | Java Applet |
| PE_PARITE . A | 320,924 | File Infector |
| TSPY_ SMALL . SN | 268,171 | Grayware |
| WORM_NETSKY. D | 242,243 | Worm |
| SPYW_GATOR . B | 163,495 | Grayware |
| PE_FUNLOVE .4099 | 147,416 | File Infector |
| VBS_REDLOF . A | 145,701 | VBScript |
| HKTL_RADMIN . A | 63,557 | Grayware |
| PE_ZAFI . B | 62,708 | File Infector |
| ADW_SOLU180. A | 61,959 | Grayware |
| PE_TENGA . A | 44,036 | File Infector |
| PE_JEEFO . A | 27,831 | File Infector |
| PE_LOVGATE . AC | 25,595 | File Infector |
| PE_NIMDA . A | 16,824 | Worm |

ที่มา : เทรนด์ ไมโคร

[ต่อด้านหลัง]

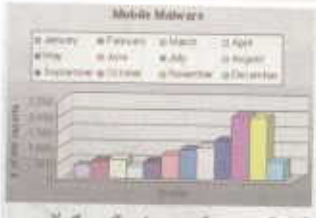



ช่องสัญญาณส่งผ่านข้อมูลที่เพิ่มขึ้นในการเชื่อมต่ออินเทอร์เน็ต เช่น ไว-ไฟ, เอจ/จีพีอาร์เอส, 3จี/ยูเอ็มทีเอส และแม้แต่ไวแมกซ์ที่กำลังจะเกิดขึ้นก็เป็นเป้าหมายที่ต้องคอยระมัดระวังเช่นกัน

ทั้งนี้แนวโน้มภัยตลอดทั้งปี 2549 เทรนด์ ไมโครคาดว่าสิ่งที่พบเจอในรอบปีที่ผ่านมาจะยังคงเกิดขึ้นต่อเนื่องในปี 2549 นั่นก็คือ สปาย-ฟิชชิ่ง จะยังคงเพิ่มขึ้นอย่างต่อเนื่อง บ็อตส์จะใช้ทุกศักยภาพในการเพิ่มความสามารถให้กับตัวเองสเปียร์-ฟิชชิ่ง (Spear-phishing) จะสร้างความกังวลใจให้กับองค์กรธุรกิจต่าง ๆ ไม่น้อย สแปมจะมาในรูปภาษาท้องถิ่นมากขึ้น มัลแวร์จะมาในรูปของการเข้ารหัสและแบ่งย่อยตัวเองมากขึ้น เพื่อหลบเลี่ยงการตรวจจับโปรแกรมสแกนไวรัสออนไลน์อย่าง IRC, IM และ P2P จะยังคงเป็นช่องทางแพร่ไวรัสอยู่

ช่องโหว่ของระบบปฏิบัติการวินโดว์สยังคงเป็นเป้าหมายไม่หยุดหย่อน เกรย์แวร์และมัลแวร์เริ่มแยกกันไม่ออก แต่ที่ส่งผลดีต่อผู้ค้าผลิตภัณฑ์รักษาความปลอดภัยที่จะสามารถกำจัดภัยร้ายนี้ได้ง่ายขึ้น บ็อตส์และบ็อตเน็ตส์เพิ่มจำนวนขึ้น และแอดแวร์และสปายแวร์ยังคงแพร่ระบาดอยู่

ข้อแนะนำสำหรับผู้ใช้รับมือมัลแวร์ ปี 2549




สำหรับผู้ใช้องค์กรแล้ว ควรหมั่นใช้ระบบสแกนหาไวรัสทางอินเทอร์เน็ตให้เหมือนกับระบบสแกนอีเมล์ที่ใช้กันมานานแล้วปิดกั้นการเข้าถึงเครือข่ายองค์กรของโปรโตคอลที่ไม่จำเป็น โดยเฉพาะโปรแกรมสนทนาออนไลน์ทั้งหลาย ใช้ซอฟต์แวร์สแกนช่องโหว่ในเครือข่าย ใช้ระบบสแกนสปายแวร์องค์กร ให้ความรู้กับผู้ใช้ และกำหนดนโยบายการใช้งานเครือข่ายองค์กรอย่างเข้มงวด

สำหรับผู้ใช้ตามบ้าน ให้ระวังเว็บไซต์ที่มีช่องแม้ให้คุณต้องติดตั้งซอฟต์แวร์ลงในคอมพิวเตอร์ และอย่าติดตั้งซอฟต์แวร์ใหม่จากเว็บไซต์แปลกหน้านอกจากคุณจะมั่นใจว่าเว็บไซต์หรือเจ้าของซอฟต์แวร์นั้นน่าเชื่อถือจริง สแกนโปรแกรมที่ดาวน์โหลดทางอินเทอร์เน็ตด้วยซอฟต์แวร์ป้องกันสปายแวร์และไวรัสที่ได้รับการอัพเดตแล้ว ไม่ว่าจะดาวน์โหลดจากเครือข่าย P2P ผ่านเว็บไซต์ หรือแหล่งอื่นใดก็ตาม

ระวังอีเมล์หน้าตาแปลก ๆ อย่าเปิดไฟล์แนบท้ายหรือคลิกลิงค์ที่มาพร้อมกับอีเมลไม่น่าไว้ใจ

ตั้งค่า "Automatic Update" ในระบบปฏิบัติการวินโดว์สของคุณไว้ และอัพเดตใหม่ทันทีที่มีการประกาศให้เข้าไปอัพเดต

**และควรใช้บริการสแกนไวรัสแบบเรียลไทม์ เพื่อช่วยให้การท่องโลกออนไลน์ปลอดภัยไร้กังวล**