

# เทรนด์ไมโครเผย 10 สิ่งอันตราย

## ● ความเสี่ยงข้อมูลมากที่สุดในปี 2553

มาร์ติน รอสเลอร์ ผู้อำนวยการด้านการวิจัยภัยคุกคาม ศูนย์วิจัยเทรนด์ไมโครของ บริษัท เทรนด์ ไมโคร อิงค์ เปิดเผยรายงานสรุป 10 รายชื่อสิ่งที่เป็นอันตรายและเสี่ยงกับการเกิดภัยคุกคามข้อมูลมากที่สุดในปี 2553 ดังนี้

1. ฮาร์ดแวร์ : อุปกรณ์ฮาร์ดแวร์ที่มีความเสี่ยงสูงที่สุดที่มีการใช้งานในปี 2553 คือเครื่องอ่านบัตรประจำตัวของชาวเยอรมันบัตรประจำตัวดังกล่าวจะมีข้อมูลส่วนตัวที่ได้รับการเข้ารหัสไว้ เช่น ลายพิมพ์นิ้วมือ แต่โชคไม่ดีที่ข้อมูลดังกล่าวถูกขโมยได้โดยง่ายผ่านทางเครื่องอ่านบัตรบางเครื่อง

2. ซอฟต์แวร์สำหรับเว็บไซต์ : ซอฟต์แวร์ที่มีความเสี่ยงที่สุดสำหรับการใช้งานบนเว็บไซต์ในปี 2553 คือ WordPress ซึ่งเป็นแพลตฟอร์มยอดนิยมสำหรับการสร้างบล็อก โดยบล็อก WordPress นับพันรายการที่ยังไม่ได้รับการแก้ไขช่องโหว่จะถูกอาชญากรไซเบอร์ใช้ประโยชน์ในรูปแบบที่หลากหลาย ซึ่งรวมถึงการเป็นส่วนหนึ่งของการปรับเปลี่ยนทิศทางการเว็บไซต์ที่อาจนำไปสู่มัลแวร์อันตรายหรือรูปแบบที่เกี่ยวข้องกับการเพิ่มประสิทธิภาพเครื่องมือค้นหา (Search Engine Optimization : SEO) ได้

3. ไอพี (IP) : ไอพีที่อันตรายที่สุดที่มีการใช้งานในปี 2553 คือ Internet Relay Chat (IRC) จะเห็นได้ว่า 30% ของบ็อตเน็ตทั้งหมดใช้ IRC ในการสื่อสารกับเครื่องที่ติดมัลแวร์และเซิร์ฟเวอร์ในการส่งการและควบคุม (C&C) ของบ็อตเน็ต แต่โชคดีที่การบล็อกการใช้ IRC ในเครือข่ายสามารถหยุด

บ็อตเน็ตได้อย่างดีเยี่ยม

4. ระบบปฏิบัติการ (โอเอส) : โอเอสที่มีความเสี่ยงสูงสุดคือ Mac OS X ของ Apple โดยเมื่อเดือนพฤศจิกายนที่ผ่านมา Apple ได้ส่งรุ่นโอเอสที่ได้รับการแก้ไขหลายอย่างให้แก่ผู้ใช้และเป็นรุ่นที่มีขนาดใหญ่มาก โดยล่าสุดมีขนาดที่ 644.48 เมกะไบต์ ถือเป็นการอัปเดตครั้งใหญ่ที่รวมการแก้ไขช่องโหว่ด้านความปลอดภัยจำนวนมากนับตั้งแต่บริษัทได้ทำการอัปเดตก่อนหน้านี้เมื่อกลางเดือนมิถุนายน จะเห็นได้ว่าด้วยแนวโน้มในด้านการรักษาความลับและรอบการแก้ไขที่ยาวนานของ Apple เนื่องจากยังคงเพิ่มความเสถียรต่อผู้ใช้ได้

5. เว็บไซต์ : เว็บไซต์ที่อันตรายที่สุดในโลกคือ Google ด้วยความนิยมอย่างมหาศาลของเว็บไซต์แห่งนี้ทำให้อาชญากรไซเบอร์ใช้เป็นเครื่องมือในลักษณะที่เกี่ยวข้องกับ SEO (BlackhatSEO : การทำให้ลิงก์ของตนอยู่สูงกว่าผลการค้นหาทั่วไป) อีกทั้งยังนำผู้ใช้งานเข้าสู่ความเสี่ยงด้านภัยคุกคามของมัลแวร์ที่สำคัญด้วย โดยเฉพาะโปรแกรมแอนตี้ไวรัสของปลอม (FAKEAV) นอกจากนี้ เครือข่ายโฆษณาของ Google ยังมักจะตกเป็นเหยื่อจากโฆษณาอันตราย (Malvertisements) อยู่บ่อยครั้งอีกด้วย

6. เครือข่ายสังคม : ในอีกกรณีี่แสดงให้เห็นว่าความนิยมอาจนำไปสู่อันตรายได้ นั่นคือ Facebook ที่ได้รับการพิจารณาว่าไซต์เครือข่ายสังคมที่เป็นอันตรายสูงสุด โดยการสำรวจทุกสิ่งผ่านทาง Facebook อาจลวงไปสู่การแพร่กระจายของมัลแวร์ KOOFACE ได้ ทั้งนี้อาชญากรไซเบอร์มักจะแฝงตัวเข้าไป

อยู่ในทุกๆ ที่ที่ผู้คนอยู่รวมกัน และสถานที่แห่งนั้นก็คือ Facebook นั่นเอง

7. โดเมนระดับบนสุด : โดเมนระดับบนสุดที่เป็นอันตรายที่สุดในโลกคือ CO.CC ซึ่งเปิดโอกาสให้อาชญากรไซเบอร์สามารถจดทะเบียนโดเมนได้นับพันโดเมนบนอินเทอร์เน็ตโดยที่ผ่านขั้นตอนการตรวจสอบน้อยมาก และการที่ผู้ให้บริการอินเทอร์เน็ตในรัสเซียปฏิเสธการปิดการทำงานของไซต์ที่เป็นอันตรายก็ได้อีกทำให้เกิดการผสมรวมของสิ่งที่เป็นอันตรายอย่างมากขึ้นในปัจจุบัน

8. รูปแบบไฟล์ : PDF เป็นรูปแบบไฟล์ที่มีความเสี่ยงที่สุดในปี 2553 เนื่องจาก ช่องโหว่ต่างๆ ของ Adobe Acrobat และ Reader ได้กลายเป็นส่วนหนึ่งของชุดเครื่องมือในการใช้หาประโยชน์ในทางที่ผิดๆ

9. สภาพแวดล้อม : สภาพแวดล้อมขณะทำงานที่อันตรายสูงสุดสำหรับผู้ใช้งานในปี 2553 คือ Internet Explorer (IE) ที่สามารถเปิดใช้งานสคริปต์ได้ ในปัจจุบันยังคงมีการใช้ประโยชน์จากราวเซอร์อยู่เป็นจำนวนมากโดยพุ่งเป้าเป็นพิเศษไปที่ IE อย่างไรก็ตาม Java ก็กำลังตกเป็นเป้าหมายด้วยเช่นกันและอาจกลายเป็นเป้าหมายหลักในปี 2554 ก็ได้

10. ช่องทางการติดต่อ : ช่องทางการติดต่อที่เป็นไปได้สูงสุดยังคงเป็นบราวเซอร์ จะเห็นได้ว่ามากกว่า 2 ใน 3 ของการติดต่อทั้งหมดใช้บราวเซอร์เป็นพาหนะในการติดต่อ ส่วนช่องทางการติดต่อก่อนหน้านี้ เช่น แฟลชดิสก์ และข้อความสแปม ยังคงมีอยู่ในปัจจุบัน แต่ก็ได้รับความนิยมลดลงเมื่อเทียบกับช่วงเวลาก่อนหน้านี้