สรุปภัยคุกคามด้านไอทีปี 2552 และแนวโน้มปี 2553

โดย บริษัท โกลบอลเทคโนโลยี อินทิเกรเทด จำกัด

เมื่อปีเก่ากำลังจะผ่านพ้นไป ปีใหม่เคลื่อนเข้ามา หลายคนอาจกำลังทบทวนสิ่งที่เกิดขึ้นเพื่อนำมาเป็นบทเรียนแก้ไขข้อผิดพลาดต่าง ๆ ทั้งในการดำเนินชีวิตและการทำงาน สำหรับแวดวงด้านความปลอดภัยข้อมูลสารสนเทศนั้น การทบทวนคงไม่มีอะไรดีไปกว่าศึกษาเหตุการณ์ภัยคุกคามในอดีตและคาดหมายอนาคต เพื่อจะได้เตรียมพร้อมรับมือกับภัยคุกคามเหล่านั้นได้อย่างรู้เท่าทัน โกลบอลเทคฯ จึงขอสรุปเหตุการณ์ด้านภัยคุกคามในแวดวงไอทีที่เกิดขึ้นในปี 2552 พร้อมคาดการณ์แนวโน้มในปี 2553 ดังต่อไปนี้

สรุปภัยคุกคามในแวดวงไอทีปี 2552

1. หนอนคอมพิวเตอร์ “คอนฟิกเกอร์”

“คอนฟิกเกอร์” คือหนอนคอมพิวเตอร์ที่ตั้งเป้าโจมตีระบบปฏิบัติการวินโดวส์ และผู้สร้างสามารถสั่งการได้จากระยะไกล ปัจจุบันหนอนชนิดนี้ควบคุมเครื่องคอมพิวเตอร์กว่าเจ็ดล้านเครื่อง ทั้งภาครัฐ, เอกชน และเครื่องคอมพิวเตอร์ส่วนตัว ในกว่า 200 ประเทศทั่วโลก[1]

คอนฟิกเกอร์จะโจมตีช่องโหว่ในส่วนของวินโดวส์เซิร์ฟเวอร์เซอร์วิส (Windows Server service) (ซึ่งไมโครซอฟต์ได้ออกซอฟต์แวร์แก้ไข (MS08-067) ในเดือนตุลาคม 2552) โดยอาศัยเทคนิคออโต้รันเพื่อการแพร่กระจายผ่านทาง Thumb Drive แบบยูเอสบี เมื่อเข้าถึงคอมพิวเตอร์เครื่องหนึ่งแล้ว มันจะพยายามเข้าถึงเน็ตเวิร์กแชร์ (Network Shares) และพยายามแคร็กรหัสผ่านของแอคเคานต์ในเครื่อง หากแคร็กรหัสผ่านของผู้ดูแลระบบได้ ก็จะใช้เซอร์วิสที่ชื่อ Windows Task Scheduler Service เพื่อแพร่กระจายตัวเองไปยังคอมพิวเตอร์เครื่องอื่นต่อไป

เนื่องจากคอนฟิกเกอร์จำเป็นต้องใช้ช่องโหว่เฉพาะ (MS08-067) เพื่อการแพร่กระจาย จึงจำเป็นต้องรู้ว่าคอมพิวเตอร์ที่มันโจมตีใช้ภาษาอะไร โดยคอนฟิกเกอร์เวอร์ชั่นก่อนๆ จะมีความสามารถจำกัด ต้องรับข้อมูลทางอินเทอร์เน็ตก่อนจึงจะแปลง IP Address ให้เป็น Physical Address ได้ ทั้งนี้เมื่อโจมตีคอมพิวเตอร์ในอเมริกา หนอนชนิดนี้จะพยายามโจมตีวินโดวส์เวอร์ชั่นภาษาอังกฤษ แต่ถ้า IP Address ที่ถูกโจมตีอยู่ในจีน มันจะพยายามโจมตีวินโดวส์เวอร์ชั่นภาษาจีนแทน การโจมตีวินโดวส์เวอร์ชั่นภาษาอื่นๆ ก็เป็นลักษณะเดียวกัน

ด้วยความที่หนอนคอมพิวเตอร์ชนิดนี้สร้างด้วยเทคนิคชั้นสูง ทำให้ตรวจจับได้ยากและแพร่กระจายอย่างรวดเร็วสู่เครื่องคอมพิวเตอร์ทั่วโลก ซึ่งส่วนใหญ่ยังใช้ระบบปฏิบัติการวินโดวส์เป็นหลัก จึงเป็นหนอนที่เชื่อกันว่าแพร่เชื้อขยายวงกว้างที่สุดนับแต่ปี พ.ศ. 2546

2. เครือข่ายสังคม ภัยร้ายใกล้ตัว

บริการเครือข่ายสังคม หรือ Social Network ที่เปิดโอกาสให้ผู้ใช้งานอินเทอร์เน็ตสร้างบัญชีผู้ใช้ส่วนตัวเพื่อสื่อสารกับบุคคลอื่นในเครือข่าย และสามารถเขียนข้อความ, แช็ต, แบ่งปันรูปภาพ / เพลง / วิดีโอ และสร้าง

[1] ข้อมูลจาก *The New York Times*

บล็อกส่วนตัวนั้น มีผู้ใช้งานอย่างแพร่หลายมากเป็นจำนวนหลายร้อยล้านแอคเคานต์ จึงตกเป็นเป้าหมายหลักของอาชญากรออนไลน์ที่อาศัยความเชื่อถือระดับสูงในกลุ่มเพื่อน นำไปสู่ภัยคุกคามรูปแบบต่างๆ เช่น

<u>กรณีเฟซบุ๊ค</u>

- แอคเคานต์ผู้ใช้งานถูกบุกรุก ซึ่งอาจเกิดการขโมยรหัสผ่านจากฟิชชิงหรือมัลแวร์ แล้วใช้บัญชีนั้นเพื่อขอความช่วยเหลือทางการเงินจากกลุ่มเพื่อนในเครือข่ายของเหยื่อ จนมีผู้หลงเชื่อส่งเงินไปให้
- ผู้ใช้งานถูกขโมยรหัสผ่านและเปลี่ยนหน้าเว็บโดยมิชอบ
- ผู้พัฒนาแอพพลิเคชั่นที่มีเจตนามุ่งร้าย ใช้เอพีไอ (API) หรือแอพพลิเคชั่นโปรแกรมของเฟซบุ๊ค เพื่อหลอกล่อผู้ใช้ให้ติดตั้งแอพพลิเคชั่นของผู้พัฒนา
- การเผยแพร่ลิงค์เว็บไซต์มุ่งร้าย เพราะผู้ใช้งานมีแนวโน้มที่จะเชื่อถือและคลิกลิงค์ที่มาจากเพื่อนหรือญาติ มากกว่าไฟล์หรือลิงค์ในอีเมลจากคนไม่รู้จัก

<u>กรณีทวิตเตอร์</u>

- แอคเคานต์ของทวิตเตอร์ถูกใช้เป็นเครื่องมือของบอทเน็ต โดยใช้หน้าทวิตเตอร์ของผู้ใช้รายหนึ่งที่แสดงข้อความที่เข้ารหัสไว้ เพื่อสั่งการให้คอมพิวเตอร์ที่ติดมัลแวร์เข้าไปยังเว็บไซต์อื่นๆ เพื่อรับคำสั่งจากผู้ควบคุมบอทเน็ต เช่น ดาวน์โหลดและเปิดใช้มัลแวร์เพื่อขโมยข้อมูลในระบบของผู้ใช้
- แอคเคานต์ของทวิตเตอร์ถูกใช้ในการส่งผู้ใช้งานไปยังผลิตภัณฑ์ที่ลวงว่าเป็นซอฟต์แวร์แอนตี้ไวรัส (Rogue Antivirus Products) โดยข้อความทวีตที่ส่งจากแอคเคานต์เหล่านี้ถูกสร้างขึ้นโดยอัตโนมัติ ไม่ว่าจะเลือกจากคำค้นของทวิตเตอร์เอง หรือการ re-tweet ที่ส่งโดยคนจริงๆ ซึ่งลิงค์เหล่านี้จะนำผู้ใช้ไปยังเว็บไซต์ปลอม ที่ใช้วิธีต่างๆ หลอกล่อให้ผู้ใช้งานกลัว และหลงเชื่อ ซื้อผลิตภัณฑ์ที่ไม่จำเป็นต้องใช้
- หนอนทวิตเตอร์ (Twitter Worm) อาศัยช่องโหว่ชนิด cross-site scripting ที่มักพบในเว็บแอพพลิเคชั่นแล้วส่งข้อความสแปม เช่น "I love www.StalkDaily.com!" ซึ่งสร้างความรำคาญให้ผู้ใช้งานทวิตเตอร์จำนวนมากที่คลิกไปที่ลิงค์นั้น ด้วยหลงเชื่อว่าเป็นข้อความทวีตจากเพื่อนของตน และมีการทวีตข้อความแบบเดียวกันต่อไปอีกหลายทอด การโจมตีเหล่านี้อาศัยจาวาสคริปต์ จึงควรปิดการทำงานของจาวาสคริปต์ หรือจำกัดการทำงานของจาวาสคริปต์ให้ทำงานกับเว็บไซต์ที่น่าเชื่อถือเท่านั้น เพื่อป้องกันภัยจากหนอนอินเทอร์เน็ตในลักษณะนี้

3. การโจมตีการเพิ่มประสิทธิภาพเครื่องมือค้นหา (Search Engine Optimization; SEO)

การโจมตีรูปแบบนี้ ผู้โจมตีจะส่งหัวข้อยอดนิยมเข้าไปในเว็บค้นหา หรือ Search Engine เช่น ชื่อดาราดังที่ตกเป็นข่าว, ไข้หวัดใหญ่ 2009 เป็นต้น เมื่อมีผู้คลิกเปิดดูเว็บไซต์ ไซต์นั้นกลับกลายเป็นเว็บไซต์มุ่งร้าย ส่งผลให้คอมพิวเตอร์ที่ใช้งานถูกควบคุม หรือนำผู้ใช้ไปยังผลิตภัณฑ์ที่ลวงว่าเป็นซอฟต์แวร์แอนตี้ไวรัส (rogue antivirus products) ด้วยเหตุนี้จึงควรคำนึงถึงชื่อเสียงและความน่าเชื่อถือของเว็บไซต์ที่แสดงผลโดยเว็บค้นหา ก่อนเข้าเยี่ยมชม

ผลิตภัณฑ์ประเภท “Rogue Security Product” เป็นมัลแวร์ที่ล่อลวงให้ผู้ใช้งาน จ่ายเงินซื้อผลิตภัณฑ์ปลอม

ตัวอย่างเช่น “File Fix Professional” ที่ผู้เขียนซอฟต์แวร์นี้ไม่ได้ผลักดันซอฟท์แวร์เอง แต่ทำโดยผู้เป็นเจ้าของบอทเน็ต โดย "File Fix Pro" จะ “เข้ารหัส” ไฟล์บางไฟล์ในโฟลเดอร์ "My Documents" แล้วแสดงข้อความบ่งบอกความผิดพลาดที่ดูสมจริง บอกว่าระบบวินโดวส์แนะนำให้ดาวน์โหลดเครื่องมือพิเศษเพื่อแก้ไขไฟล์ โดยให้ผู้ใช้คลิกดาวน์โหลด "File Fix Pro" เพื่อ “ซ่อม” ไฟล์ดังกล่าว แต่แท้จริงแล้วเป็นเพียงการ “ถอดรหัส” ให้สามารถใช้งานได้ตามปกติ หากผู้ใช้ยอมจ่ายเงินจำนวนหนึ่งสำหรับผลิตภัณฑ์นี้

วิธีนี้เป็นกลยุทธ์ที่แยบยลในการหลอกผู้ใช้ ซึ่งไม่รู้ว่าไฟล์ของตน “ถูกจับเป็นตัวประกัน” และการซื้อซอฟต์แวร์นี้เป็นเพียงการจ่ายค่าประกันตัวในการกู้คืนไฟล์เท่านั้น ซึ่งผู้ขายซอฟต์แวร์ดังกล่าวไม่ได้ทำสิ่งผิดกฎหมายแต่อย่างใด

4. แม็ค โอเอส เอ็กซ์ (MAC OS X)

เดือนมกราคม 2552 ได้มีการเผยแพร่ก็อปปี้ของซอฟต์แวร์ไอเวิร์ค 2009 (iWork 2009) ในเว็บไซต์แชร์ไฟล์ยอดนิยมแห่งหนึ่ง ซึ่งผู้ดาวน์โหลดเวอร์ชั่นฟรีนี้ ได้รับของแถมที่น่าประหลาดใจในซอฟท์แวร์ติดตั้ง คือแบ็คดอร์ชื่อไอเวิร์คเซิร์ฟดอทเอ (iWorkServ.A) โดยกลุ่มผู้เผยแพร่มัลแวร์รายเดียวกันนี้ยังได้เผยแพร่โปรแกรมโฟโต้ชอปเวอร์ชั่นสำหรับ MAC ที่แถมแบ็คดอว์ด้วยเช่นกัน

ซอฟต์แวร์มุ่งร้ายทุกชนิด จะอาศัยการหลอกล่อให้ผู้ใช้ป้อนรหัสผ่าน ซอฟต์แวร์นี้ก็เช่นกัน การติดตั้งซอฟต์แวร์ในแม็ค โอเอส เอ็กซ์ จะบังคับให้ผู้ใช้ใส่รหัสผ่านของผู้ดูแลระบบ เมื่อผู้ใช้ใส่รหัสผ่านเพื่อติดตั้งซอฟต์แวร์ผิดกฎหมายนี้เข้าไปแล้ว นอกจากจะได้ซอฟท์แวร์ที่ทำงานได้จริงแล้ว ยังทำให้ระบบของเขาถูกบุกรุกไปด้วย

5. การโจมตีแอพพลิเคชั่นเป้าหมาย

แอพพลิเคชั่นที่ถูกโจมตีมากที่สุด ในปี 2551 นั้น คือไมโครซอฟต์เวิร์ด (.doc) แต่ช่วงปี 2552 ตำแหน่งไฟล์ยอดนิยมที่ถูกโจมตีสูงสุดตกเป็นของ ไฟล์พีดีเอฟ (.pdf) ของค่าย Adobe อันเนื่องจากช่องโหว่ในโปรแกรม Adobe Acrobat และ Adobe Reader

6. หนอนอินเทอร์เน็ตไอโฟน (iPhone Worm)

ปี 2552 สมาร์ทโฟนเข้ามามีบทบาทและได้รับความนิยมเพิ่มมากขึ้น มีการใช้งานอินเทอร์เน็ตผ่านสมาร์ทโฟนอย่างกว้างขวาง รวมไปถึงเว็บเครือข่ายสังคม โดยไอโฟนมีส่วนแบ่งตลาดในระดับต้นๆ จึงดึงดูดความสนใจจากผู้เขียนมัลแวร์จำนวนมาก

ไอโฟนส่วนหนึ่งผ่านการทำเจลเบรก (Jailbreak) ซึ่งเป็นขั้นตอนที่ทำให้ไอโฟนและไอพอด ทัช สามารถใช้คำสั่งที่ไม่เป็นทางการในอุปกรณ์ โดยไม่ต้องผ่านระบบป้องกันของบริษัทแอปเปิล ทำให้ผู้ใช้ไอโฟนสามารถติดตั้งแอพพลิคชั่นต่าง ๆ ที่ละเมิดลิขสิทธิ์ได้ และเครื่องที่ทำเจลเบรก ได้กลายเป็นเป้าหมายของมัลแวร์ที่ผู้สร้างต้องการทำเงิน เช่น โจมตีช่องโหว่ในไอโฟนที่ผ่านการทำเจลเบรก, หนอนคอมพิวเตอร์ “ไอคี” (Ikee) ที่เจาะระบบของผู้ใช้ที่ไม่เปลี่ยนรหัสผ่านของซีเคียวเชลล์ (SSH) ที่กำหนดมาพร้อมกับการติดตั้ง โดยเปลี่ยนภาพวอลล์เปเปอร์ของไอโฟนให้เป็นรูปอื่น

นอกจากนี้ยังมีหนอนคอมพิวเตอร์ที่เจาะระบบไอโฟน โดยพยายามเปลี่ยนเส้นทางเว็บของผู้ใช้ จากธนาคารแห่งหนึ่งไปยังไซต์ฟิชชิ่ง เมื่อผู้ใช้งานพยายามเข้าถึงบริการธนาคารออนไลน์จากไอโฟน จึงควรที่ผู้ใช้งานสมาร์ทโฟนจะได้หันมาให้ความสนใจกับความปลอดภัยของเครื่องมือสื่อสารของตนให้มากยิ่งขึ้น

7. การโจมตีเครือข่ายแบบ DDoS มีแนวโน้มเพิ่มสูงขึ้น

การโจมตีเครือข่ายเพื่อให้เครื่องคอมพิวเตอร์ปลายทางหยุดทำงาน ซึ่งมีผู้โจมตีพร้อมกันจำนวนมาก หรือที่เรียกว่า Distributed Denial of Service (DDoS) นั้น เกิดขึ้นมากมายทั่วโลกในปี 2552 ด้วยหลายเหตุปัจจัย และมีแนวโน้มทวีความรุนแรงขึ้น สรุปได้ดังนี้

- เหตุการณ์ความขัดแย้งในการเลือกตั้งประธานาธิบดีของอิหร่านเมื่อกลางปี 2552 นำไปสู่การประท้วงครั้งใหญ่ และเกิดกระแสการใช้สื่อเครือข่ายสังคม ทั้งทวิตเตอร์, เฟซบุ๊ค, ยูทูบ และไซต์อื่นๆ เพื่อกระจายข้อมูลข่าวสารและหลีกเลี่ยงการตรวจจับของรัฐบาล อีกมุมหนึ่งของเทคโนโลยีคือการโจมตีเครือข่ายแบบ DDoS ซึ่งถูกนำมาใช้โจมตีเครื่องแม่ข่ายของรัฐบาลอิหร่าน รวมทั้งโจมตีแอคเคานต์ ของผู้ใช้งานทวิตเตอร์และเฟซบุ๊คนับล้านคน ซึ่งผู้อยู่เบื้องหลังการโจมตีนี้จะต้องมีแบนด์วิธมหาศาลเพื่อการโจมตีครั้งนี้โดยเฉพาะ
- การโจมตี DDoS ในวันที่ 31 สิงหาคม 2552 ซึ่งเป็นวันชาติของมาเลเซีย โดยเป้าหมายคือเว็บไซต์ในมาเลเซียที่ถูกบุกรุกและเปลี่ยนเนื้อหาไปกว่าร้อยเว็บไซต์ รวมถึงเว็บไซต์ที่เกี่ยวข้องกับสถาบันแห่งชาติ สื่อมวลชน และภาคธุรกิจของมาเลเซีย
- เว็บไซต์รัฐบาลสหรัฐและเกาหลีใต้ ถูกโจมตีแบบ DDoS จนทำให้เครือข่ายใช้งานไม่ได้เป็นเวลาหลายชั่วโมง

การโจมตีเครือข่ายแบบ DDoS นี้ มีแนวโน้มเกิดขึ้นได้กับทุกประเทศในโลก โดยเฉพาะอย่างยิ่งเมื่อมีการใช้สมาร์ทโฟน และเว็บไซต์ประเภทเครือข่ายสังคม อย่างแพร่หลาย ซึ่งหากผู้ใช้งานไม่ป้องกันตนเองอย่างเหมาะสมแล้ว ก็อาจตกเป็นเหยื่อของผู้ไม่ประสงค์ดีที่ใช้เราเป็นเครื่องมือโจมตีผู้อื่นได้โดยที่เราไม่รู้ตัว

แนวโน้มภัยคุกคามข้อมูลสารสนเทศ ปี 2553

1. แอนตี้ไวรัสไม่เพียงพอสำหรับการป้องกัน

การกำเนิดขึ้นของมัลแวร์แบบโพลีมอร์ฟิค (polymorphic code) ซึ่งเป็นโค้ดที่สามารถเปลี่ยนรูปแบบได้ทุกครั้งที่มันทำงาน แต่ยังคงรักษาอัลกอรึทึมเดิมไว้ โดยเชลล์โค้ดและหนอนคอมพิวเตอร์ หรือมัลแวร์ชนิดใหม่ๆ จะใช้เทคนิคในการซ่อนตัวตนของมัน ดังนั้นแอนตี้ไวรัสที่ใช้วิธีการเดิมๆ ที่อาศัยการวิเคราะห์มัลแวร์เพียงอย่างเดียวจึงไม่เพียงพอต่อการป้องกันภัยคุกคามอีกต่อไป จึงต้องอาศัยวิธีการใหม่ๆ ในการตรวจจับมัลแวร์มาใช้ด้วย

2. **โซเชียล เอนจิเนียริ่งเป็นวิธีหลักในการโจมตี (Social Engineering Attack)**

การโจมตีในลักษณะนี้ ผู้โจมตีจะมุ่งเป้าไปที่ผู้ใช้ปลายทางและพยายามขโมยข้อมูลความลับจากผู้ใช้ หรือหลอกล่อให้ผู้ใช้ดาวน์โหลดมัลแวร์ เช่น ผู้โจมตีส่งอีเมล์ให้บุคคลอื่นโดยหลอกว่าเป็นผู้ดูแลระบบ และถาม

รหัสผ่านหรือชักจูงให้เหยื่อเปิดไวรัสที่แนบมาพร้อมกับอีเมล์ เป็นต้น ซึ่งเป็นวิธีการที่ได้รับความนิยมมากขึ้น เนื่องจากไม่เกี่ยวข้องกับช่องโหว่ในระบบปฏิบัติการและเว็บบราวเซอร์ของเครื่องคอมพิวเตอร์เหยื่อ แต่มุ่งเป้าไปที่ผู้ใช้งานโดยตรง ด้วยเหตุนี้โซเชียล เอ็นจิเนียริ่ง จึงเป็นวิธีการเบื้องต้นที่แพร่หลายในปัจจุบัน และคาดว่าจะมีเทคนิคการโจมตีที่สลับซับซ้อนยิ่งขึ้นในปี 2553

3. ผู้ขายซอฟท์แวร์ประเภท "Rogue Security Software" จะเพิ่มความพยายามมากขึ้น

คาดว่าการแพร่กระจาย Rogue Security Software หรือมัลแวร์ที่พยายามลวงให้ผู้ใช้จ่ายเงินซื้อผลิตภัณฑ์ปลอม จะเพิ่มจำนวนขึ้น โดยการโจมตีคอมพิวเตอร์ของผู้ใช้งาน เพื่อทำให้เครื่องนั้นใช้การไม่ได้ หรือการ "เข้ารหัส" ไฟล์แล้วเรียกเงินค่าไถ่จากเจ้าของเครื่องนั้น ซึ่งผู้ขายซอฟต์แวร์จะเปลี่ยนชื่อซอฟท์แวร์แอนตี้ไวรัสแจกฟรีที่สามารถดาวน์โหลดได้ทั่วไป มาใช้เป็น "สินค้า" เพื่อเสนอขายให้กับผู้ใช้ที่ไม่รู้ข้อเท็จจริง และเข้าใจว่าต้องจ่ายเงินซื้อซอฟต์แวร์ดังกล่าว

4. การโจมตีผลการค้นหาเสิร์ชเอนจิ้น (SEO Poisoning attack)

การโจมตีในลักษณะนี้เกิดขึ้นเมื่อแฮกเกอร์โจมตีผลการค้นหาจากเสิร์ชเอนจิ้น เพื่อส่งลิงค์ของตนให้อยู่สูงกว่าผลการค้นหาทั่วไป เมื่อผู้ใช้ค้นหาคำค้นที่เกี่ยวข้อง ลิงค์ที่มีมัลแวร์จะปรากฏใกล้กับตำแหน่งสูงสุดของผลการค้นหา ทำให้เกิดจำนวนคลิกไปยังเว็บมุ่งร้ายที่มากยิ่งกว่าเดิมหลายเท่า เมื่อมีการรณรงค์ตรวจจับและลบลิงค์ดังกล่าวออกจากผลการค้นหา ผู้โจมตีก็จะเปลี่ยนเส้นทางของบอทเน็ตไปยังคำค้นใหม่ที่เหมาะกับเวลาและสถานการณ์ และอาจก่อให้เกิดปัญหาที่ผู้ใช้บริการไม่ให้ความเชื่อถือในผลการค้นหา ตราบใดที่ผู้ให้บริการยังไม่เปลี่ยนวิธีการบันทึกและแสดงผลลิงค์

5. โปรแกรมเสริมสำหรับเครือข่ายสังคมจะถูกใช้เพื่อการหลอกลวง

ด้วยความนิยมของเว็บไซต์เครือข่ายสังคมที่มีการเติบโตอย่างสูง ประกอบกับเว็บไซต์ดังกล่าวยอมให้นักพัฒนาโปรแกรมสามารถเข้าถึงเอพีไอ (API) และพัฒนาแอพพลิเคชั่นเสริมสำหรับผู้ใช้เครือข่ายสังคมได้ ด้วยเหตุนี้จึงมีผู้โจมตีที่พยายามบุกรุกช่องโหว่ในแอพพลิเคชั่นเสริมดังกล่าว จึงคาดว่าจะมีความพยายามในการหลอกลวงผู้ใช้เพิ่มขึ้น เช่นเดียวกับเจ้าของเว็บไซต์ที่พยายามสร้างมาตรการในการแก้ไขภัยคุกคามเหล่านี้เพื่อสร้างความปลอดภัยให้กับผู้ใช้งาน

6. บริการ Short URL จะกลายเป็นเครื่องมือสำหรับฟิชชิ่ง (Short URL Phishing)

บริการ Short URL หรือการย่อลิงค์ URL ให้สั้นลง ที่นิยมทำกันเวลาโพสต์ลิงค์ที่อยากเผยแพร่บนเว็บบอร์ดหรือเว็บไซต์ประเภทเครือข่ายสังคมนั้น เนื่องจากผู้ใช้มักไม่ทราบว่าลิงค์ URL ที่ย่อให้สั้นแล้วนั้นจะพาไปที่ไหน ผู้โจมตีฟิชชิ่ง (phishing) จึงสามารถซ่อนลิงค์เพื่อล่อลวงผู้ใช้งานที่ไม่ระแวดระวัง และไม่คิดก่อนคลิกได้ โดย Short URL นี้จะเป็นภัยคุกคามที่ผสมผสานกับหลายเรื่อง ไม่ว่าจะเป็นการค้นหาบน Search Engine, การทำลิงค์บน SEO หรือแม้แต่การสนทนาออนไลน์ผ่านระบบคอมพิวเตอร์หรืออุปกรณ์มือถือ ก็สามารถซ่อนลิงค์ URL มุ่งร้ายไปกับผู้ให้บริการ short URL ได้เช่นกัน

ด้วยเหตุนี้จึงมีแนวโน้มที่จะนำ Short URL มาใช้ในการแพร่กระจายแอพพลิเคชั่นหลอกลวง เพิ่มมากขึ้น

ทั้งยังมีความพยายามหลีกเลี่ยงระบบกลั่นกรองสแปม โดยคาดว่าผู้ส่งสแปมจะใช้บริการย่อลิงค์ให้สั้นเพื่อใช้กระทำการที่มุ่งร้าย ดังนั้น จึงควรใช้บริการ short URL ที่สามารถตรวจสอบภัยคุกคามได้ เช่น SRAN short URL (http://sran.org) ที่มีบริการตรวจหาฟิชชิ่ง (phishing) และภัยคุกคามจาก URL ต้นฉบับได้ เป็นต้น

7. มัลแวร์ในระบบปฏิบัติการแม็คและอุปกรณ์พกพาจะเพิ่มมากขึ้น

รูปแบบและจำนวนการโจมตีที่ออกแบบมาเพื่อระบบปฏิบัติการหรือแพลตฟอร์มหนึ่งๆ เช่น วินโดวส์, แม็ค, สมาร์ทโฟน นั้น มีความสัมพันธ์โดยตรงกับส่วนแบ่งทางการตลาดของแพลตฟอร์มนั้น ๆ เนื่องจากผู้สร้างมัลแวร์ต้องการรายได้สูงสุด ช่วงหลายปีที่ผ่านจึงเห็นภาพการโจมตีระบบปฏิบัติการวินโดวส์เป็นหลัก แต่ในปี 2552 จะเห็นได้ชัดว่าระบบปฏิบัติการแม็คและสมาร์ทโฟน ตกเป็นเป้าหมายการโจมตีมากขึ้น เช่น บอทเน็ต "Sexy Space" ที่โจมตีระบบปฏิบัติการซิมเบียน และโทรจัน "OSX.lservice" ที่โจมตีระบบแม็ค

เนื่องจากแม็คและสมาร์ทโฟน มีความนิยมเพิ่มสูงขึ้นอย่างต่อเนื่อง และคาดว่าจะมีส่วนแบ่งตลาดเพิ่มมากขึ้นในปี 2553 จึงคาดว่าจะมีผู้โจมตีที่อุทิศเวลาเพื่อสร้างมัลแวร์ที่โจมตีอุปกรณ์เหล่านี้มากขึ้นเช่นกัน

8. ผู้ส่งสแปมปรับตัว ทำให้จำนวนสแปมผันผวน

นับตั้งแต่ปี 2550 สแปมมีจำนวนเพิ่มขึ้นเฉลี่ยร้อยละ 15 ถึงแม้ว่าจำนวนสแปมเมล์จะไม่เพิ่มขึ้นในระยะยาว แต่ก็เป็นที่แน่ชัดว่าผู้ส่งสแปมยังไม่ยอมเลิกราง่าย ๆ ตราบใดที่ยังมีเหตุจูงใจทางการเงินอยู่ ในขณะเดียวกันผู้ส่งสแปมยังต้องปรับตัวให้เข้ากับความซับซ้อนของซอฟต์แวร์รักษาความปลอดภัย, การแทรกแซงของผู้ให้บริการอินเทอร์เน็ต ตลอดจนรัฐบาลในหลายประเทศที่หันมาให้ความสำคัญกับภัยคุกคามเครือข่ายสารสนเทศมากขึ้น

ทั้งนี้คาดว่าผู้ส่งสแปมจะปรับตัวและหาวิธีส่งสแปมผ่าน IM หรือ Instant Messaging มากขึ้น เนื่องจากเหล่าสแปมเมอร์ (Spammer) ค้นพบวิธีใหม่ในการเอาชนะเทคโนโลยี CAPTCHA (การกรอกรหัสก่อนส่งข้อความ) การโจมตีโปรแกรมประเภท IM นี้จึงน่าจะมีแนวโน้มเพิ่มมากขึ้น ด้วยการส่งข้อความสแปมที่ผู้รับไม่ต้องการและมีลิงค์มุ่งร้าย โดยเฉพาะการโจมตีที่มุ่งเป้าไปที่การขโมยแอคเคานต์ IM เพื่อนำไปกระทำการไม่เหมาะสม

9. เกิดมัลแวร์ที่ออกแบบมาเพื่องานเฉพาะด้าน

ในปี 2552 ได้มีการค้นพบมัลแวร์ที่ออกแบบมาเพื่อทำงานเฉพาะด้าน ซึ่งมีเป้าหมายโจมตีระบบเอทีเอ็ม ชี้ให้เห็นว่ามีการล่วงรู้กระบวนการทำงานภายในตลอดจนช่องโหว่ที่สามารถโจมตีได้ คาดว่าแนวโน้มนี้จะยังดำเนินต่อไป รวมถึงความเป็นไปได้ของมัลแวร์ที่สามารถโจมตีระบบเฉพาะทางอื่นๆ อีก เช่น ระบบการโหวตผ่านเครือข่ายโทรศัพท์ที่เชื่อมต่อกับรายเรียลลิตี้โชว์หรือการแข่งขันรูปแบบต่าง เป็นต้น

10. วินโดวส์ 7 จะตกเป็นเป้าโจมตี

วินโดวส์ 7 เป็นระบบปฏิบัติการใหม่ที่เพิ่งเปิดตัวไปไม่นาน จึงคาดว่าจะมีผู้ใช้งานเพิ่มมากขึ้นทั้งบนเครื่องคอมพิวเตอร์และสมาร์ทโฟน เป็นช่องทางใหม่ให้ผู้โจมตีระบบคิดค้นไวรัสสายพันธุ์ใหม่ รวมทั้งมัลแวร์รูปแบบอื่นเพื่อเจาะและทำลายระบบปฏิบัติการนี้ในระยะเวลาอันใกล้อย่างแน่นอน ไม่ว่าไมโครซอฟต์จะทดสอบระบบก่อนวางตลาดอย่างละเอียดเพียงใด แต่หากโค้ดมีความซับซ้อนมาก ก็ยิ่งมีโอกาสสูงที่จะมีช่องโหว่ที่ยังค้นไม่พบเช่นกัน

บทสรุป

หลังจากที่ได้ทราบถึงภัยคุกคามที่เกิดขึ้นในปี 2552 และแนวโน้มที่จะเกิดขึ้นในปี 2553 แล้ว ผู้อ่านไม่จำเป็นต้องตื่นตระหนกแต่อย่างใด ธุรกิจด้านการรักษาความปลอดภัยยังคงมีความแข็งแกร่งในการรับมือกับภัยคุกคามเหล่านี้ เนื่องจากการสร้างสรรค์สิ่งใหม่ ๆ, การตระหนักถึงภัยคุกคามที่มีเพิ่มขึ้น ตลอดจนการแข่งขันกันระหว่างผู้ขายเอง ทำให้ภาพในอนาคตไม่น่าจะเลวร้ายมากนัก อย่างไรก็ตาม การสร้าง “Security Awareness” ทั้งในแง่ส่วนบุคคลและองค์กร ก็ยังเป็นส่วนสำคัญที่ไม่ควรมองข้าม ซึ่งสามารถศึกษารายละเอียดเพิ่มเติมเกี่ยวกับวิธีการป้องกันภัยคุกคามรูปแบบต่างๆ ได้ในหนังสือ “SRAN เปิดโลก IT Security”