มติชน

วันจันทร์ที่ 21 ธันวาคม พุทธศักราช 2552 ปีที่ 32 ฉบับที่ 11517 หน้า 26

ก 10150

# แนวโน้มความปลอดภัย บนเครือข่าย 'อินเตอร์เน็ต'

มติชน วิทยาการ ePeople

เมื่อเดือนธันวาคม 2551 ไซแมนเทค คาดการณ์ทิศทางความปลอดภัยในปี 2552 ไว้นี้ พร้อมด้วยแนวโน้มน่าสนใจที่เด่นชัดในช่วงครึ่งแรกของปี 2552

## การเพิ่มขึ้นของมัลแวร์หลากหลายสายพันธุ์

นักวิจัยด้านความปลอดภัยของไซแมนเทค ตรวจพบและป้องกันการโจมตีจากโค้ดอันตรายกว่า 245 ล้านครั้งทั่วโลกในแต่ละเดือน ส่วนใหญ่เป็นภัยคุกคามที่ไม่เคยพบมาก่อนและแพร่ระบาดบนเว็บเป็นหลัก ผู้โจมตีระบบได้ปรับเปลี่ยนจากเป้าหมายในวงกว้างที่ใช้โค้ดอันตรายจำนวนไม่มาก มาเป็นการโจมตีแบบจำกัดกลุ่มแต่ใช้โค้ดอันตรายที่แตกต่างกันนับล้าน

มัลแวร์หลากหลายประเภทชนิดใหม่นั้นประกอบไปด้วยภัยคุกคามหลายพันรูปแบบซึ่งแพร่ระบาดผ่านทั้งระบบไฟล์แชริ่ง (file sharing) อีเมลและสื่อเก็บข้อมูลแบบพกพา ผสมผสานทำให้เกิดจำนวนมัลแวร์ที่มีลักษณะจำเพาะแบบนับไม่ถ้วน เป็นการประกาศเตือนถึงความจำเป็นในการค้นหาวิธีใหม่ในการตรวจสอบภัยคุกคาม ทั้งแบบที่สามารถตรวจจับได้ตามลักษณะสถานการณ์แวดล้อม (heuristics) การป้องกันแบบอิงตามพฤติกรรม และโมเดลด้านความปลอดภัยแบบอิงตามข้อมูลความปลอดภัยจากผู้ใช้ทั่วโลก

## วิกฤตเศรษฐกิจ

การโจมตีรูปแบบใหม่ในปี 2552 อาศัยวิกฤตเศรษฐกิจโลกเป็นช่องทางในการโจมตีผ่านทั้งฟิชชิ่ง (phishing) และอี-เมลขยะ (spam) เป้าหมายคือบรรดาผู้คนที่ตกงานเป็นจำนวนมากนอกจากรูปแบบที่คุ้นเคยแล้ว ยังพบรูปแบบอื่นๆ ด้วย ผ่านเว็บบอร์ดโฆษณาและประกาศสมัครงานต่างๆ โดยเห็นการหลอกลวงรูปแบบต่างๆ ที่ฟุ้งเป้าไปยังผู้คนซึ่งจำนองบ้านหรือกำลังมองหาช่องทางในการจำนองบ้านและรีไฟแนนซ์ และยังมีการหลอกลวงอีกจำนวนหนึ่งที่แอบอ้างถึงนโยบายการกระตุ้นเศรษฐกิจของภาครัฐในสหรัฐด้วย

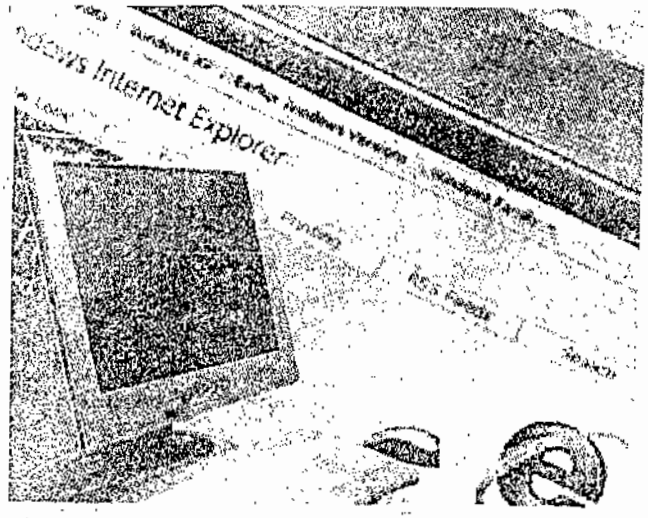
## เว็บเครือข่ายเชิงสังคม (social networks)

เว็บเครือข่ายเชิงสังคมยังคงเป็นเป้าหมายที่ได้รับความนิยมจากบรรดาผู้ไม่หวังดีที่ล่อลวงผ่านทางฟิชชิ่ง เพราะการโจมตีแต่ละครั้งนั้นได้ผลตอบรับกลับอย่างมากมาย ตัวอย่างเช่น การโจมตีเว็บเครือข่ายเชิงสังคมชื่อดังผ่านรูปแบบต่างๆ ซึ่งฟิชเชอร์ได้เข้าควบคุมบัญชีผู้ใช้ของผู้อื่น และใช้เป็นทางผ่านในการโจมตีเพื่อนของผู้ใช้ดังกล่าวอีกต่อหนึ่ง หรือบางอย่างก็มาในรูปของเกมที่ประกฏบนเว็บบล็อกที่ชื่อดัง โดยที่ผู้เล่นจะถูกสอบถามและเยี่ยมส่วนบุคคล ทั้งชื่อเล่นเพื่อนที่ดู และเกมตลกๆ ต่างๆ โดยที่ผู้เล่นไม่มีโอกาสได้รู้ตัวเลยว่า เกมปลอมๆ ดังกล่าวได้แอบเก็บรวบรวมข้อมูลสำคัญเกี่ยวกับผู้ใช้ไปเรียบร้อยแล้ว

## อี-เมลขยะที่มีจำนวนเพิ่มสูงขึ้น

ปี 2551 ไซแมนเทคพบว่า อี-เมลขยะนั้นได้ลดลงไปเหลือ 65% ในช่วง

(ต่อด้านหลัง)



ระยะเวลา 24 ชั่วโมงก่อนที่ McColo (หนึ่งในแหล่งต้นตอของปัญหาอี-เมลขยะทั่วโลก) จะถูกปิดตัวลง และในยุก 24 ชั่วโมงหลังจากนั้น เรายังได้คาดการณ์ด้วยว่า ปัญหาอี-เมลขยะจะกลับมาอีกครั้งในระดับ 75-80% ซึ่งเมื่อต้นเดือนมิถุนายนที่ผ่านมา

ไซแมนเทคได้รายงานว่า ทางหน่วยงานที่รับผิดชอบให้ร่วมมือกันเพื่อสั่งปิดผู้ให้บริการอินเตอร์เน็ตอย่าง Pricewert LLC ที่เป็นอีกหนึ่งแหล่งต้นตอของอี-เมลขยะทั่วโลก ซึ่งถือเป็นตัวอย่างอันดีในการร่วมมือกันระหว่างผู้เชี่ยวชาญด้านความปลอดภัยที่ต่อสู้ร่วมกันเพื่อจัดการกับอาชญากรรมออนไลน์ อย่างไรก็ดี ปัญหาอี-เมลขยะนั้นยังคงอยู่ในระดับสูงตลอดเดือนมิถุนายน คิดเฉลี่ยเป็นจำนวน 90% ของอี-เมลทั้งหมด นอกจากนี้ สแปมเมอร์ยังได้ฉวยเหตุการณ์สำคัญที่เกิดขึ้น อาทิ การเสียชีวิตของไมเคิล แจ็กสัน และปัญหาไข้หวัดใหญ่สายพันธุ์ใหม่ 2009 รวมไปถึงเหตุการณ์แผ่นดินไหวในอิตาลีเพื่อหลอกล่อผู้ใช้ผ่านอี-เมลขยะด้วย

## ความก้าวหน้าของภัยคุกคามทางเว็บ

ภัยคุกคามยังคงเกิดขึ้นอย่างต่อเนื่องโดยเฉพาะบนเว็บ ซึ่งมีเป้าหมายหลักก็คือ ผู้ใช้ที่เข้ามาเยี่ยมชมเว็บไซต์ต่างๆ ที่ถูกลอบควบคุมสั่งการและส่งผู้ใช้ไปยังเว็บไซต์ที่เต็มไปด้วยโค้ดอันตรายหนึ่งรูปแบบที่ใช้บ่อยก็คือการสั่งให้เกิดการดาวน์โหลดโค้ดอันตรายโดยที่ผู้ใช้ไม่รู้ตัวและเราก็ได้ตรวจพบการโจมตีผ่านเว็บไปยังโดเมนชื่อดังต่างๆ ผ่านสภาพแวดล้อมแบบเครือข่ายเชิงสังคม หนึ่งกรณีที่เพิ่งเกิดขึ้นไม่นานและกลายเป็นข่าวดังก็คือ คำเชิญแบบปลอมๆ ให้เข้าร่วมเป็นสมาชิกบนเว็บเครือข่ายเชิงสังคมแห่งหนึ่งที่มาพร้อมกับไฟล์แนบและเวิร์ม (worm) สำหรับส่งอี-เมลขยะแบบอัตโนมัติ

นอกจากนี้ ยังพบการโจมตีแบบอื่นๆ ด้วย เช่น การเจาะแอพพลิเคชั่นผ่านโปรแกรมเสริมประเภทปลั๊กอิน หรือช่องโหว่ cross-site scripting ได้รับความนิยมเพิ่มขึ้นเหนือการโจมตีรูปแบบเดิมที่ผ่านจาวาสคริปต์และบราวเซอร์รุ่นที่ไม่ปลอดภัย

ขณะที่เราได้คาดการณ์แนวโน้มใหม่ในปี 2552 ก็ยังมีแนวโน้มอื่นๆ เพิ่มเติมและน่าจับตาในช่วงครึ่งแรกของปีนี้ด้วยเช่นกัน

**การกลับมาของภัยคุกคามเดิมๆ ในปี 2552 : ช่วงครึ่งแรกของปี** ภัยคุกคามแบบเดิมได้กลับมาสร้างปัญหาให้กับผู้ใช้อีกครั้ง การปล่อยภัยคุกคามจำนวนไม่มากแต่ส่งผลกระทบในวงกว้างดังเช่น CodeRed และ Nimda กลายเป็นส่วนหนึ่งในเทคนิคการโจมตีที่ถูกใช้โดยเวิร์ม Koobface ที่แพร่ระบาดผ่านเว็บเครือข่ายเชิงสังคมและเวิร์ม Conficker ซึ่งเป็นหนึ่งในภัยคุกคามที่มีความซับซ้อนและระบาดอย่างหนักบนอินเตอร์เน็ตในช่วงหลายปีที่ผ่านมา

การระบาดของภัยคุกคามก่อนหน้านี้มักมีแรงจูงใจมาจากด้านการเงินเป็นหลัก (เช่น ขโมยข้อมูลส่วนบุคคล การปล่อยโปรแกรมแอนตี้ไวรัสปลอม หรือการแพร่กระจายอี-เมลขยะ) เช่นเดียวกับไทรจัน Dozer ที่แพร่กระจายโดยการโจมตีแบบ DDoS (distributed denial of service) ทั้งนี้ เห็นได้ว่าเทคนิคในการโจมตีต่างๆ ที่เกิดขึ้นก่อนหน้านี้ ยังคงถูกใช้ในภัยคุกคามในปัจจุบัน และเชื่อว่ามาตรการป้องกันแบบหลายชั้นที่รวมวิธีการปกป้องแบบดั้งเดิมเข้ากับปรการเสริมรูปแบบใหม่ เช่น การใช้โมเดลด้านความปลอดภัยแบบอิงตามข้อมูลความปลอดภัยจากผู้ใช้ทั่วโลกถือเป็นเรื่องที่สำคัญยิ่ง

**ความร่วมมือในวงกว้างเพื่อจัดการกับปัญหาความปลอดภัยบนโลกไซเบอร์ :** เมื่อรูปแบบการโจมตีเริ่มมีความซับซ้อนมากยิ่งขึ้น ความร่วมมือกันระหว่างหน่วยงานต่างๆ ในระดับที่เข้มข้นถือเป็นสิ่งจำเป็นในการจัดการกับการแพร่ระบาดของภัยคุกคามเหล่านั้น ในเดือนกุมภาพันธ์ 2552 ที่ผ่านมาได้มีการก่อตั้งคณะทำงานเกี่ยวกับเวิร์ม Conficker ขึ้นมาเฉพาะ ซึ่งเป็นความร่วมมือระหว่างบริษัทชั้นนำในอุตสาหกรรมและด้านการศึกษา เพื่อจัดการกับการแพร่ระบาดของ Conficker ทั่วโลก

โดยมีทั้งนักวิจัยด้านความปลอดภัย หน่วยงานด้านการจัดสรรชื่อโดเมนอย่าง ICANN (Internet Corporation for Assigned Names and Numbers) และผู้ให้บริการอีกจำนวนมากมาเชื่อมโยงรวมไปถึงบริษัทชั้นนำต่างๆ ที่ร่วมมือกันสกัดกั้นโดเมนที่เป็นเป้าหมายของ Conficker ซึ่งเราต่างได้เห็นความร่วมมือลักษณะนี้เพิ่มมากขึ้นในอุตสาหกรรม วงการการศึกษา และหน่วยงานภาครัฐเพื่อจัดการกับภัยคุกคามอื่นๆ ที่กำลังเกิดขึ้นอยู่ในขณะนี้

โปรแกรมหลอกและสร้างความเข้าใจผิด ยังคงมีให้เห็นอย่างต่อเนื่อง ทุกวันนี้ผู้ไม่หวังดีระบบนั้นได้เพิ่มความซับซ้อนและวางแผนเพื่อปิดบังได้ดีขึ้น และยังคงใช้แนวทางการเลียนแบบธุรกิจต่างๆ ที่มีชื่อเสียงเพื่อหลอกลวงเหยื่อ อาทิ โฆษณาอันตรายหรือ malvertisements ที่มาในรูปของโฆษณาแบบแฟลช ที่ส่งผู้ใช้ไปยังหน้าเว็บปลอม โดยเลียนแบบเว็บไซต์ชื่อดังหลายแห่ง หรือที่มาในรูปของแอพพลิเคชั่นปลอมที่เรียกว่า scareware ที่เลียนแบบซอฟต์แวร์แอนตี้ไวรัสและโฆษณาชิ้นคุณสมบัติในการกำจัดภัยคุกคาม แต่เมื่อติดตั้งลงบนระบบคอมพิวเตอร์ กลับพยายามแจ้งเตือนผู้ใช้อย่างไม่ถูกต้องให้เชื่อว่าบนคอมพิวเตอร์ดังกล่าวมีภัยคุกคามอยู่มากมาย ผ่านการแจ้งเตือนด้วยหน้าต่างป๊อปอัพ ไอคอนแถบแถบเครื่องมือ ฯลฯ โดยหลอกล่อด้วยการสแกนหาภัยคุกคามทั้งที่ไม่ได้เกิดขึ้นจริง และแสดงรายงานที่ผิดๆ ให้แก่ผู้ใช้ โดยมีเป้าหมายเพื่อให้ผู้ใช้หันเงินซื้อผลิตภัณฑ์ปลอมที่โฆษณาเกินคุณสมบัติในการจัดการกับภัยคุกคามที่เกิดขึ้นทั้งที่ทำไม่ได้จริง

โดยผู้ที่ตกเป็นเหยื่อมักถูกชักนำไปสู่หน้าเว็บสำหรับสั่งซื้อสินค้าและถูกหลอกล่อให้จ่ายเงินผ่านระบบออนไลน์เป็นที่สุด