กรุงเทพธุรกิจ
ปีที่ 20 ฉบับที่ 6747 วันพุธที่ 14 มีนาคม พ.ศ. 2550 หน้า 2

ก 7467

มัลแวร์แอบอยู่ในคอมพิวเตอร์

● เอกรัตน์ สาธุธรรม

มีรายงานที่น่าสนใจ จากบริษัทไซแมนเทค ผู้ผลิตซอฟต์แวร์ป้องกันไวรัส ระบุว่า อาชญากรรมออนไลน์มีแนวโน้มมุ่งโจมตีผู้ใช้ตามบ้านเพิ่มขึ้นเพื่อหวังผลทางการเงินเป็นหลัก

คุณอาจจะไม่รู้ว่าแอพพลิเคชั่นที่ใช้งานอยู่ทุกค่ำคืน พรุนไปด้วยช่องโหว่มากมาย ขณะเดียวกันจำนวนเทคนิคในการพรางตัวเองของเจ้าหนอนอันตรายพวกนี้ก็มีอัตราเพิ่มสูงขึ้นเช่นกัน

รายงานภัยร้ายบนอินเทอร์เน็ตฉบับล่าสุด (Symantec Internet Security Threat Report) ย้ำกับผู้ใช้ตามบ้านว่าหากยังประมาท เลินเล่อ อาจต้องเสียใจภายหลัง ดีไม่ดี อาจตกเป็นเหยื่อของการถูกขโมยตัวตน (identity theft - ถูกปลอมสถานะบุคคล แอบอ้างชื่อ) ไปแบบไม่รู้อีโหน่อีเหน่

เพราะยุคนี้ เจ้าวายร้ายออนไลน์มีเทคนิคอันแพรวพราว เพื่อหลบหนีการตรวจจับ ทำให้สามารถอำพรางตัวบนระบบคอมพิวเตอร์เป้าหมายได้นานขึ้นเพื่อขโมยข้อมูลสำคัญ ยึดข้อมูลในเครื่องคอมพิวเตอร์เป็นประกันเพื่อหวังผลทางการค้า ตลอดจนเข้าควบคุมเครื่องคอมพิวเตอร์เป้าหมายจากทางไกลและการส่งต่อ หรือขายข้อมูลลับ เป็นต้น

ที่สำคัญ รายงานฉบับเดียวกันนี้ยังเผยข้อมูลที่น่าตกใจด้วยว่า 'ผู้ใช้ตามบ้าน' คือเป้าหมายหลักของวายร้ายออนไลน์ คิดเป็น 86 เปอร์เซ็นต์ของการโจมตีทั้งหมด ตามมาด้วยสถาบันการเงินเป็นอันดับที่สอง เจ้าหนอนไซเบอร์มักอาศัยช่องโหว่ในแอพพลิเคชั่นบนเครื่องคอมพิวเตอร์ปลายทางเป็นหลัก และใช้เทคนิคอันแพรวพราวในการพรางตัวเพื่อเลี่ยงกับดักที่มนุษย์คิดค้นขึ้น

องค์กรธุรกิจเอง ก็เตรียมการรับมือกับภัยคุกคามทางคอมพิวเตอร์ที่มีประสิทธิภาพยิ่งขึ้นโดยมีกลยุทธ์ป้องกันระบบอย่างเป็นรูปธรรม แต่เจ้าวายร้ายพวกนี้ก็ยังสามารถหลบหลีก และยังเปลี่ยนเป้าโจมตีไปได้เรื่อยๆ อย่างไม่สะทกสะท้าน

โดยเฉพาะในแอพพลิเคชั่นใช้งานที่ถูกเจ้าวายร้ายไซเบอร์นี้ตามโจมตีสูงถึง 69 เปอร์เซ็นต์

ที่สำคัญ ยังพบโค้ดอันตรายอีกกว่า 18 เปอร์เซ็นต์ที่ไม่เคยพบเห็นมาก่อนหน้านี้ ซึ่งชี้ให้เห็นว่าวายร้ายต่างๆ กำลังพยายามสรรหาเทคนิคและวิธีการใหม่ในการหลบซ่อนตัวเองจากซอฟต์แวร์แอนตี้ไวรัสและซอฟต์แวร์ปกป้องระบบจากผู้รุกราน

นอกจากนี้ เจ้าวายร้ายที่ชื่อ 'ฟิชเชอร์' (Phishers - อาชญากรที่ส่งอีเมลหลอกลวงเป้าหมายและแอบอ้างว่ามาจากบริษัทหรือสถาบันการเงินต่างๆ เพื่อหลอกขโมยรหัสผ่านหรือข้อมูลทางการเงิน) ยังคิดค้นการส่งข้อความรูปแบบใหม่เพื่อให้หลุดพ้นจากระบบคัดกรอง และเข้าถึงเหยื่อได้อย่างมีประสิทธิภาพมากขึ้น

เมื่อปีที่แล้วมีข้อความที่เข้าข่ายการหลอกลวงลักษณะดังกล่าวสูงถึง 157,477 ข้อความที่ไม่ซ้ำกัน เพิ่มขึ้นกว่า 81 เปอร์เซ็นต์ ขณะเดียวกันปัญหาจากอีเมลขยะก็เพิ่มขึ้นเป็น 54 เปอร์เซ็นต์ของปริมาณอีเมลทั้งหมดในระบบ

อีเมลอันตรายส่วนใหญ่เปลี่ยนรูปแบบการเข้าถึงผู้ใช้ด้วยวิธีใหม่ จากเดิมที่เคยแนบไฟล์อันตรายติดมากับอีเมล ก็

ต่อด้านหลัง

เปลี่ยนเป็นการใส่ลิงค์เพื่ออ้างอิงผู้ใช้เยี่ยงเว็บไซต์อันตรายปลายทางแทน เพื่อหลบหลีกการตรวจจับอีเมลอันตรายจากระบบคัดกรองอีเมลของซอฟต์แวร์ปกป้องระบบต่างๆ จนสามารถหลุดลอดไปยังเมลบ็อกซ์ของผู้ใช้ทั่วไปได้สะดวกขึ้น

ว่ากันว่า 'เม็ดเงิน' ที่ได้รับยังคงเป็นแรงจูงใจหลักในการก่ออาชญากรรมออนไลน์ ดังจะเห็นได้จากเครือข่ายของเครื่องที่ตกเป็นเหยื่อ (bot network) ได้ถูกใช้เพื่อก่ออาชญากรรมในหลายรูปแบบมากขึ้น ทั้งการแพร่ระบาดโค้ดอันตราย การส่งอีเมลขยะและข้อความหลอกหลวง ดาวน์โหลดแอดแวร์และสปายแวร์ โจมตีเว็บไซต์ของบริษัทต่างๆ และแอบเก็บบันทึกข้อมูลลับ ฯลฯ

ที่ผ่านมา ได้ตรวจพบเครื่องคอมพิวเตอร์บน bot network รวมกว่า 4.6 ล้านเครื่องที่ยังคงถูกใช้เพื่อก่ออาชญากรรม เฉลี่ยแล้วในแต่ละวันจะมีคอมพิวเตอร์กว่า 57,717 เครื่องที่ถูกใช้เพื่อก่อการดังกล่าว

บ่อยครั้งที่เครือข่ายของคอมพิวเตอร์เหล่านี้ถูกใช้เพื่อโจมตีเว็บไซต์ปลายทางด้วยวิธี 'ดีโอเอส (DoS - Denial-of-Service)' ซึ่งถือเป็นภัยร้ายแรงต่อเว็บไซต์ของหลายบริษัท ทำให้ระบบสื่อสารข้อมูลของบริษัทเหล่านี้มีปัญหา สูญเสียรายได้ ส่งผลกระทบต่อความเชื่อมั่นของลูกค้า และเสี่ยงต่อการถูกข่มขู่โดยอาชญากรเพื่อเรียกเงินตอบแทน

'สถาบันการเงิน' ถือเป็นเป้าหมายที่ถูกแอบอ้างชื่อเพื่อหลอกขโมยข้อมูลจากผู้ใช้มากที่สุด นับได้กว่า 84 เปอร์เซ็นต์ของจำนวนเว็บไซต์ปลอมทั้งหมดที่ตรวจจับได้

ปัจจุบัน 3 ใน 10 ของภัยคุกคามใหม่ที่ตรวจพบ คือ แอพพลิเคชั่นหลอกลวง ที่แจ้งเตือนหรือสร้างรายงานเท็จเพื่อหลอกให้ผู้ใช้คอมพิวเตอร์เสียเงินเพื่ออัพเกรดซอฟต์แวร์ที่ติดตั้งอยู่ให้คุณสมบัติครอบคลุมยิ่งขึ้น แล้วก็หลอกว่าซอฟต์แวร์นี้จะจัดการภัยคุกคามออกไปจากคอมพิวเตอร์ได้อย่างสมบูรณ์ ขณะที่ความเป็นจริงคอมพิวเตอร์ดังกล่าวอาจไม่ได้มีปัญหาใดๆ เกิดขึ้นก็ได้

เพื่อป้องกันไม่ให้โจรแปลกหน้าเที่ยวมาบุก ล้วง ค้นคอมพิวเตอร์คุณ ปัจจุบันมีองค์กรเอกชนชื่อ 'ไซแมนเทค' ซึ่งเปิด 'ศูนย์มาตรวัดภัยอินเทอร์เน็ต' ที่เว็บไซต์ www.symantec.com/home-home-office ขึ้นมา เพื่ออัพเดทข้อมูลเกี่ยวกับเหล่าวายร้ายไซเบอร์เหล่านี้ ผู้ใช้จะได้รู้ทางหนีทีไล่เอาไว้ก่อน

นพชัย ตั้งไตรธรรม ที่ปรึกษาทางเทคนิค บริษัท ไซแมนเทค คอร์ปอเรชั่น เล่าว่า เวบนี้จะมีข้อมูลอัพเดทภัยต่างๆ สำหรับผู้ใช้อินเทอร์เน็ตทุกแขนง ไม่ว่าจะเป็นอีเมล เวบ การส่งข้อความด่วน หรือบริการแลกเปลี่ยนไฟล์ออนไลน์ต่างๆ

"ผู้บริโภคควรจะได้ใช้ชีวิตออนไลน์ได้อย่างมั่นใจ ไม่ว่าพวกเขาจะกำลังสื่อสารกันด้วยอีเมล ใช้จ่ายซื้อสินค้าผ่านอินเทอร์เน็ต พูดคุยกับเพื่อนผ่านการส่งข้อความด่วน หรือใช้งานบริการแลกเปลี่ยนไฟล์ต่างๆ โดยศูนย์นี้จะคอยอัพเดทข้อมูลข่าวสารล่าสุดให้ เหมือนกับบุคคลที่เดินทางบ่อยๆ ต้องตรวจสอบสภาพอากาศในจุดหมายปลายทางให้รอบคอบ ผู้ใช้คอมพ์เองก็ควรมีบริการที่ช่วยให้เขาสามารถเตรียมป้องกันตัวเองเพื่อให้การใช้งานอินเทอร์เน็ตเป็นไปอย่างราบรื่นที่สุดด้วย"

อย่างน้อยๆ มี 'ยาม' เป็นด่านแรกคอยสอดส่องดูแล พวกตื่นแมงจะได้ไม่สะดวกโยธินเหมือนที่ผ่านๆ มา

12 ข้อควรจำ ตัดกำลังหนอนร้าย

1.เลือกใช้โซลูชั่นระบบรักษาความปลอดภัยบนอินเทอร์เน็ตที่รวมประสิทธิภาพของการต่อต้านไวรัส ระบบไฟร์วอลล์ ระบบตรวจจับผู้บุกรุกและการบริหารจัดการช่องโหว่ เพื่อให้การปกป้องสูงสุดในการรับมือภัยคุกคามรูปแบบผสม

2.คอยหมั่นลงแพทช์ที่อัพเดทล่าสุดอยู่เสมอ

3.ควรกำหนดรหัสผ่านที่ประกอบด้วยการผสมกันระหว่างสัญลักษณ์ ตัวอักษร และตัวเลข ไม่ควรตั้งรหัสผ่านโดยใช้คำศัพท์ต่างๆ ในพจนานุกรม และควรเปลี่ยนรหัสผ่านบ่อยๆ

4.ไม่ควรเรียกดู เปิดไฟล์ หรือเปิดใช้งานไฟล์ที่แนบมาในอีเมล ยกเว้นว่าเราจะทราบถึงที่มาของไฟล์นั้นๆ

5.หมั่นอัพเดทข้อมูลไวรัสล่าสุด (virus definition) อยู่เสมอๆ ซึ่งจะช่วยให้ผู้ใช้ทั่วไปและผู้ใช้ระดับองค์กรได้รับการปกป้องจากไวรัสใหม่ๆ ที่แพร่ระบาดในขณะที่ยังไม่ได้รับการตรวจพบ

6.ผู้ใช้ทั่วไปควรตรวจสอบอยู่เป็นประจำว่าเครื่องพีซีหรือเครื่องแมคอินทอชของเรามีช่องโหว่ในระบบที่เสี่ยงต่อการถูกโจมตีหรือไม่ โดยสามารถเข้าไปใช้บริการของ Symantec Security Check ได้ที่ www.symantec.com/securitycheck

7.ผู้ใช้คอมพิวเตอร์ทุกคนควรทราบและประเมินได้ว่าอันไหนคืออีเมลหลอกเล่น (Hoax) หรืออีเมลหลอกลวงประเภทฟิชชิ่ง (Phishing) อีเมลหลอกเล่นมักมีข้อความเช่น "โปรดส่งอีเมลฉบับนี้ไปยังทุกคนที่คุณรู้จัก" และการใช้ถ้อยคำต่างๆ ที่สร้างความตื่นตระหนกให้แก่ผู้อ่าน หรือชี้นำไปในทางที่ไม่ถูก-ไม่ควร ส่วนฟิชชิ่งนั้นมักมาในรูปแบบที่แยบยลกว่า และมักจะมาในรูปแบบอีเมลที่เหมือนมาจากองค์กรที่เชื่อถือได้ โดยใช้วิธีสารพัดเพื่อชักจูงให้ผู้อ่านกรอกข้อมูลเกี่ยวกับบัตรเครดิต หรือข้อมูลส่วนตัวอื่นๆ ลงในฟอร์มที่ระบุอยู่บนเวบไซต์ซึ่งถูกสร้างลอกเลียนแบบให้ดูคล้ายกับเวบไซต์จริงขององค์กรนั้นๆ ดังนั้นผู้ใช้จึงควรพิจารณาอย่างรอบคอบว่าข้อมูลเหล่านี้ถูกส่งมาจากแหล่งใด และดูให้ถี่ถ้วนว่ามาจากแหล่งที่เชื่อถือได้หรือไม่ วิธีจัดการที่ดีที่สุดคือลบอีเมลประเภทนี้ทิ้งไป

8.ผู้ใช้ทั่วไปสามารถมีส่วนร่วมในการต่อกรกับอาชญากรรมในโลกไซเบอร์ได้ด้วยการติดตามและรายงานการบุกรุกที่เกิดขึ้น โดยใช้บริการการติดตามของ Symantec Security Check ซึ่งผู้ใช้สามารถระบุสถานที่ตั้งของแฮคเกอร์ได้อย่างรวดเร็วและส่งต่อข้อมูลไปยัง ISP ที่แฮคเกอร์ใช้ หรือแจ้งตำรวจท้องที่ได้

9.ผู้ใช้ควรรู้ถึงข้อแตกต่างระหว่างสปายแวร์และแอดแวร์ สปายแวร์ถูกใช้เป็นเครื่องมือในการจู่โจมแบบประสงค์ร้ายไปจนถึงการจารกรรมความเป็นตัวตนของผู้ใช้ ในขณะที่แอดแวร์มักจะถูกใช้เพื่อวัตถุประสงค์ในการรวบรวมข้อมูลเพื่อทำการวางแผนด้านการตลาด

10.ทั้งสปายแวร์และแอดแวร์สามารถทำการติดตั้งตัวเองโดยอัตโนมัติบนระบบของเราผ่านทางโปรแกรมแชร์ไฟล์ ฟรีดาวน์โหลด ฟรีแวร์และแชร์แวร์ต่างๆ หรือผ่านการคลิกไปที่ลิงค์หรือไฟล์ที่แนบมาในอีเมล และ instant message ดังนั้นเราควรจะคัดเลือกโปรแกรมที่ต้องการติดตั้งบนเครื่องคอมพิวเตอร์อย่างรอบคอบ

11.ไม่ควรคลิกปุ่ม 'ตอบตกลง' ในข้อตกลงการใช้ผลิตภัณฑ์สำหรับผู้ใช้ปลายทาง (End User License Agreement) แอพพลิเคชั่น สปายแวร์และแอดแวร์บางประเภทสามารถทำการติดตั้งตัวเองโดยอัตโนมัติหลังจากที่เรากดปุ่มยอมรับในเงื่อนไขดังกล่าว ดังนั้นเราจึงควรอ่านข้อความโดยละเอียดเพื่อตรวจสอบดูเงื่อนไขของ 'สิทธิส่วนบุคคล' ข้อตกลงควรจะระบุอย่างชัดเจนว่า ผลิตภัณฑ์นั้นทำอะไรบ้างและควรมีทางเลือกสำหรับการ 'ยกเลิกการติดตั้ง' ด้วย

12.ระวังโปรแกรมซึ่งกะพริบโฆษณาบนยูสเซอร์อินเตอร์เฟซ ทั้งนี้โปรแกรมสปายแวร์หลายชนิดสามารถติดตามพฤติกรรมที่คุณตอบรับโฆษณาเหล่านี้ เมื่อใดก็ตามที่คุณมองดูโฆษณาในยูสเซอร์อินเตอร์เฟซโปรแกรม เมื่อนั้นอาจหมายความว่า คุณกำลังจ้องดูสปายแวร์อยู่นั่นเอง