วารสารวิชาชีพบัญชี

มุมไอที

มนวิกา ผดุงสิทธิ์*

Spyware

มุม IT สำหรับนักบัญชีฉบับนี้ ผู้เขียนขอนำเสนอเรื่องของสปายแวร์ (Spyware) หรือซอฟต์แวร์สอดแนมที่ถูกออกแบบมาเพื่อสังเกตการณ์หรือดักจับข้อมูล หรือที่ร้ายแรงมากไปกว่านั้นคือเข้าควบคุมเครื่องคอมพิวเตอร์โดยที่เจ้าของเครื่องไม่ทราบ เจ้าโปรแกรมตัวร้ายนี้จะก่อความเสียหายให้เราและเครื่องคอมพิวเตอร์ของเราอย่างไรบ้าง ผู้เขียนได้รวบรวมข้อมูลเกี่ยวกับสปายแวร์มาจากเว็บไซต์ของ Lavasoft ซึ่งเป็นบริษัทที่จำหน่ายผลิตภัณฑ์เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ มานำเสนอในมุมไอทีฉบับนี้ (โดยที่ไม่ได้รับค่าโฆษณาแต่อย่างใด)

สปายแวร์เป็นโปรแกรมคอมพิวเตอร์ที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ ซึ่งส่วนใหญ่แล้วเจ้าของเครื่องคอมพิวเตอร์นั้นไม่ได้รับทราบเกี่ยวกับการติดตั้งโปรแกรมดังกล่าวเลย สปายแวร์เป็นที่รู้จักกันในชื่อต่างๆ เช่น Adware, Malware, Trackware หรือ Thiefware ซึ่ง Lavasoft ให้ความเห็นว่าสปายแวร์เป็นโปรแกรมที่ก่อให้เกิดความเสี่ยงมากที่สุดในโลกไซเบอร์ โดยเครื่องคอมพิวเตอร์เกือบ 90% จะมีสปายแวร์ฝังตัวอยู่ พูดง่ายๆ ก็คือคอมพิวเตอร์ทุกเครื่องที่เชื่อมต่อกับอินเทอร์เน็ตจะมีสปายแวร์ซุกซ่อนอยู่

* Ph.D (Accounting) ผู้ช่วยศาสตราจารย์ประจำ ภาควิชาการบัญชี ผู้อำนวยการโครงการปริญญาโททางการบัญชี คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
คณะกรรมการวิชาชีพด้านการศึกษาและเทคโนโลยีการบัญชี สภาวิชาชีพบัญชีฯ

ปีที่ 4 ฉบับที่ 10
มีนาคม 2551
หน้า 19-22

เมื่อสปายแวร์ถูกติดตั้งลงในเครื่องคอมพิวเตอร์ โปรแกรมดังกล่าวอาจจะเปลี่ยนการกำหนดค่าของระบบ (System Configurations) รวบรวมข้อมูลและสถิติการใช้งานรวมถึงบันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์ และส่งข้อมูลดังกล่าวผ่านอินเทอร์เน็ตกลับไปยังบุคคลหรือหน่วยงานภายนอก ซึ่งส่วนใหญ่มักจะเป็นบริษัทโฆษณาซึ่งจะนำข้อมูลส่วนบุคคลของผู้ใช้ไปใช้ประโยชน์ เช่น ใช้ในการส่งสแปมเมล์ สปายแวร์บางตัวอาจไม่ได้ก่อให้เกิดความเสียหายอย่างรุนแรง เพียงแต่ทำให้เกิดความรำคาญเนื่องจากจะส่งหน้าต่างโฆษณาเล็กๆ (Popup) ปรากฏขึ้นมาเรื่อยๆ ซึ่งสปายแวร์แบบนี้เป็นที่รู้จักกันในนามของแอดแวร์ (Adware) แต่สปายแวร์บางตัวอาจจะมีโปรแกรมประสงค์ร้ายที่เรียกว่ามัลแวร์ (Malware) ซึ่งเมื่อเข้ามาติดตั้งในเครื่องคอมพิวเตอร์แล้ว จะพยายามทำงานบางอย่างซึ่งมีผลทำให้เครื่องคอมพิวเตอร์ทำงานได้ช้าลง โดยเฉพาะอย่างยิ่งเมื่อเปิดโปรแกรมหลายโปรแกรม อาจจะมีข้อความที่แสดงถึงความผิดพลาดของซอฟต์แวร์วินโดวส์ปรากฏบ่อยครั้งขึ้น หรืออาจทำให้เข้าเว็บไซต์ต่างๆ ได้ช้า หรือทำให้เข้าเว็บไซต์ที่ต้องการไม่ได้เลย

สปายแวร์ในรูปแบบใหม่ที่ทำความเสียหายได้ร้ายแรงที่สุดจะทำการค้นหาคีย์หรือรหัสผ่านที่ผู้ใช้พิมพ์เมื่อ Login เข้าไปใน Accounts ต่างๆ รวมทั้งขโมยข้อมูลส่วนบุคคล เช่น เลขที่บัตรเครดิต เลขที่บัญชีธนาคารและรหัสผ่าน เป็นต้น ซึ่งผู้ใช้จะไม่ทราบเลยว่าข้อมูลใดของตนได้ถูกขโมยไปบ้าง ใครเป็นผู้นำข้อมูลส่วนบุคคลดังกล่าวไปใช้ และเอาไปใช้ทำอะไรบ้าง

เรามักเข้าใจว่าสปายแวร์ก็คือไวรัสคอมพิวเตอร์ แต่โดยแท้จริงแล้วสปายแวร์ต่างจากไวรัสคอมพิวเตอร์ตรงที่เมื่อถูกติดตั้งในเครื่องคอมพิวเตอร์แล้ว สปายแวร์จะไม่คัดลอกหรือสำเนาตัวเอง (Duplicate) ขึ้นมาเหมือนกับไวรัส ดังนั้น โปรแกรมป้องกันไวรัสจึงไม่สามารถตรวจจับสปายแวร์ได้ Lavasoft เสนอว่าวิธีที่ดีที่สุดคือการใช้การป้องกัน 3 ขั้นตอน นั่นคือ (1) ใช้โปรแกรมป้องกันสปายแวร์สำหรับดักจับสปายแวร์โดยเฉพาะ (2) ใช้โปรแกรมป้องกันไวรัสซึ่งจะทำงานโดยสแกนเนื้อหาของไฟล์และอีเมลที่เข้ามา รวมทั้งไฟล์ที่มีอยู่ในคอมพิวเตอร์เพื่อตรวจจับข้อมูลไวรัส และหากพบไวรัส ก็จะลบหรือกักไวรัสนั้นไว้ และ (3) ใช้ไฟร์วอลล์ (Firewall) ซึ่งเป็นอุปกรณ์หรือโปรแกรมที่ทำหน้าที่กลั่นกรองข้อมูลเข้าออก โดยไฟร์วอลล์จะปฏิบัติตามนโยบายการรักษาความปลอดภัยที่กำหนดไว้ เช่น สามารถป้องกันแฮกเกอร์ไม่ให้เจาะระบบ (Hacker) เข้ามาในระบบเครือข่ายได้ และยังช่วยหยุดไม่ให้คอมพิวเตอร์ของเราส่งซอฟต์แวร์ที่เป็นอันตรายไปยังคอมพิวเตอร์เครื่องอื่นอีกด้วย ไฟร์วอลล์สามารถทำหน้าที่บันทึกการติดต่อและการตรวจสอบ ซึ่งจะให้ข้อมูลสรุปเกี่ยวกับการติดต่อสื่อสารที่ผ่านไปมา (Traffic) และความพยายามที่จะเจาะระบบเข้ามาแก่ผู้ดูแลระบบ แต่ไฟร์วอลล์จะไม่สามารถป้องกันการโจมตีที่ไม่ผ่านไฟร์วอลล์ รวมทั้งอาจจะไม่สามารถป้องกันไวรัสได้ ดังนั้น การป้องกันแบบ 3 ขั้นตอนควบคู่กันไปจะทำให้มั่นใจได้ว่าระบบและเครื่องคอมพิวเตอร์ของเรามีความปลอดภัยในระดับหนึ่ง

ผู้เขียนใช้คำว่า เราจะสามารถมั่นใจได้ว่าเครื่องคอมพิวเตอร์ของเรามีความปลอดภัย “ในระดับหนึ่ง” เนื่องจากความก้าวหน้าอย่างต่อเนื่องของเทคโนโลยีส่งผลให้แฮกเกอร์และผู้ไม่ประสงค์ดีพัฒนาเทคนิควิธีการใหม่ๆ ในการเจาะระบบอย่างต่อเนื่องด้วยเช่นกัน ดังนั้น เราจึงไม่สามารถวางใจได้อย่าง 100% ว่าเครื่องคอมพิวเตอร์ของเราจะ Hacker-free ในอดีตเรามักจะได้รับการตักเตือนว่าเวลาที่จะดาวน์โหลดโปรแกรมจากเว็บไซต์ต่างๆ เราควรจะมีความระมัดระวัง เพราะโปรแกรมที่เราดาวน์โหลดมานั้นอาจจะมีมัลแวร์หรือไวรัสแฝงอยู่ แต่ในปัจจุบันเพียงแค่เราเข้าไปที่เว็บไซต์บางเว็บไซต์โดยที่ยังไม่ได้ดาวน์โหลดโปรแกรมอะไรเลย เว็บไซต์ดังกล่าวอาจติดตั้งสปายแวร์ในเครื่องคอมพิวเตอร์ของเราโดยที่เราไม่รู้ตัว หรือแม้แต่เมื่อจะดาวน์โหลดโปรแกรมจากเว็บไซต์ซึ่งเป็นที่น่าเชื่อถือและเป็นที่เผยแพร่โปรแกรมฟรีแวร์ (Freeware) และแชร์แวร์ (Shareware) ต่างๆ สปายแวร์อาจจะถูกซุกซ่อนอยู่ในฟรีแวร์และแชร์แวร์เหล่านั้น ซึ่งข้อความเกี่ยวกับสปายแวร์ก็จะแสดงไว้ในส่วนท้าย

สุดของข้อตกลงการอนุญาตให้ใช้ซอฟต์แวร์ (License Agreement) หรือนโยบายการรักษาความปลอดภัย (Privacy Statement) ซึ่งผู้เขียนยอมรับว่าเป็นคนหนึ่งที่ไม่เคยอ่าน License Agreement อย่างละเอียดเมื่อจะติดตั้งโปรแกรมใดๆ เพราะคิดว่าเมื่อตรวจสอบโดยโปรแกรมป้องกันไวรัสแล้วว่าโปรแกรมที่ดาวน์โหลดมาไม่มีไวรัส ก็ไม่น่าจะมีปัญหาอะไร และคิดว่าคงจะมีหลายๆ คนที่คิดเช่นเดียวกัน จึงเป็นโอกาสให้สปายแวร์เข้าไปฝังตัวอยู่ในเครื่องคอมพิวเตอร์ของเรา ตรวจจับกิจกรรมการใช้อินเทอร์เน็ตของเราและส่งข้อมูลดังกล่าวไปให้กับเจ้าของสปายแวร์ แล้วเหตุใดเจ้าของฟรีแวร์หรือแชร์แวร์จึงยอมให้มีสปายแวร์มาฝังตัวอยู่ในโปรแกรมของตน Lavasoft เปิดเผยว่าเจ้าของสปายแวร์จะจ่ายเงินให้กับเจ้าของฟรีแวร์หรือแชร์แวร์เป็นการแลกเปลี่ยน

เมื่อเทคโนโลยีคอมพิวเตอร์มีการพัฒนามากขึ้น สปายแวร์ก็ได้รับการพัฒนาให้มีความซับซ้อนมากขึ้น สปายแวร์บางประเภทสามารถกระจายตัวเองแอบซ่อนอยู่ในที่ต่างๆ ของเครื่องคอมพิวเตอร์ ทำให้การตรวจจับรวมทั้งการกำจัดสปายแวร์ให้หมดไปเป็นไปได้ยากยิ่งขึ้น แล้วเราจะป้องกันข้อมูลส่วนตัวและการโจมตีเครื่องคอมพิวเตอร์ของเราอย่างไร บางท่านอาจจะคิดว่าการป้องกัน 3 ขั้นตอนเป็นเรื่องที่ยุ่งยาก จริงๆ แล้วการป้องกันไม่เป็นเรื่องที่ยุ่งยากแต่อย่างใด โปรแกรมป้องกันไวรัสที่ติดตั้งในเครื่องคอมพิวเตอร์ของเราควรจะมีการ Update อย่างสม่ำเสมอ ส่วนโปรแกรมป้องกันสปายแวร์นั้น เราสามารถดาวน์โหลดโปรแกรม Ad-Aware 2008 ได้ฟรีที่เว็บไซต์ของ Lavasoft (แต่อย่าลืมอ่าน License Agreement อย่างละเอียดว่ามีสปายแวร์ซุกซ่อนไว้หรือไม่) เพียงแต่เวอร์ชั่นฟรีโปรแกรมจะไม่ Update โดยอัตโนมัติ ผู้ใช้จึงควร Update โปรแกรมอยู่เสมอ อย่างไรก็ตามในการดาวน์โหลดโปรแกรมป้องกันสปายแวร์นั้นควรจะดาวน์โหลดจากเว็บไซต์ที่เชื่อถือได้ เนื่องจากในปัจจุบันมีโปรแกรมจำนวนมากที่อ้างว่าเป็นโปรแกรมป้องกันสปายแวร์ทั้งๆ ที่โปรแกรมดังกล่าวนั้นเป็นสปายแวร์เสียเอง เช่น โปรแกรม Privacy Defender โปรแกรม

> “Lavasoft เสนอว่าวิธีที่ดีที่สุดในการป้องกันสปายแวร์ (Spyware) คือการใช้การป้องกัน 3 ขั้นตอน นั่นคือ (1) ใช้โปรแกรมป้องกันสปายแวร์สำหรับดักจับสปายแวร์โดยเฉพาะ (2) ใช้โปรแกรมป้องกันไวรัส และ (3) ใช้ไฟร์วอลล์ (Firewall) ซึ่งเป็นอุปกรณ์หรือโปรแกรมที่ทำหน้าที่กลั่นกรองข้อมูลเข้าออก”

SpyWiper หรือโปรแกรม PAL Spyware Remover เป็นต้น สำหรับโปรแกรมไฟร์วอลล์นั้นไม่จำเป็นต้องซื้อหา เราสามารถใช้ไฟร์วอลล์ของวินโดวส์ โดยสามารถศึกษาวิธีการตั้งค่าไฟร์วอลล์ได้จากเว็บไซต์ของ Microsoft

นอกจากนี้ สำหรับโปรแกรมทั่วๆ ไปนั้น เมื่อบริษัทที่เป็นเจ้าของโปรแกรมตรวจพบช่องโหว่ในซอฟต์แวร์ของตน บริษัทก็จะจัดทำโปรแกรมปรับปรุง (Patch) ซึ่งผู้ใช้โปรแกรมดังกล่าวสามารถดาวน์โหลดได้จากเว็บไซต์ของบริษัทเจ้าของโปรแกรม โปรแกรมปรับปรุงจะทำหน้าที่ “อุด” ช่องโหว่เพื่อป้องกันไม่ให้แฮกเกอร์ใช้สร้างปัญหา ดังนั้น ผู้ใช้โปรแกรมจึงควรดาวน์โหลดและติดตั้ง Patch ทันทีที่มีการให้บริการ

นอกจากการป้องกันสปายแวร์และโปรแกรมที่ไม่ประสงค์ดีโดยใช้การป้องกัน 3 ขั้นตอนแล้ว Lavasoft ยังได้แนะนำแนวทางเพิ่มเติมในป้องกันข้อมูลส่วนบุคคลและการใช้อินเทอร์เน็ตอย่างปลอดภัยดังนี้

1. ระมัดระวังในการดาวน์โหลดโปรแกรมและข้อมูล ควรจะดาวน์โหลดเฉพาะจากเว็บไซต์ที่เชื่อถือได้เท่านั้น และก่อนติดตั้งฟรีแวร์หรือแชร์แวร์ ควรจะอ่าน License Agreements หรือ Privacy Statement อย่างถี่ถ้วน

2. เมื่อมีหน้าต่างโฆษณา Pop up ขึ้นมา อย่าคลิก “OK” หรือ “Agree” เพราะอาจจะเป็นการไปกระตุ้นให้สปายแวร์ดำเนินการใดๆ ควรจะคลิกที่เครื่องหมาย “X” ที่มุมหน้าต่างหรือกด “Alt + F4” เพื่อปิดหน้าต่างดังกล่าว อย่างไรก็ตาม ในการคลิกปิดหน้าต่างโฆษณาก็ควรจะระมัดระวังเพราะหน้าต่างโฆษณาบางตัวจะมีเครื่องหมาย “Close” ให้คลิก แต่เมื่อกดที่เครื่องหมายดังกล่าว กลับทำให้มีหน้าต่าง Pop up เพิ่มขึ้น

3. Update โปรแกรมที่ใช้อย่างสม่ำเสมอ ไม่ว่าจะเป็นโปรแกรมป้องกันไวรัส โปรแกรมป้องกันสปายแวร์ หรือโปรแกรมที่ใช้งาน เช่น ไมโครซอฟต์เวิร์ด ในกรณีที่บริษัทเจ้าของโปรแกรมได้ออก Patch เพื่ออุดช่องโหว่

4. ใช้เว็บเบราเซอร์ที่ Update เนื่องจากมีระบบการรักษาความปลอดภัยที่เข้มงวดมากขึ้น ปรับระดับความปลอดภัยของเบราเซอร์ให้อยู่ที่ Medium หรือ Higher (ไม่ควรตั้งค่าระดับความปลอดภัยต่ำสุด)

5. ก่อนดาวน์โหลดไฟล์จากอีเมลหรือ Instant Message ควรจะตรวจสอบก่อนทุกครั้งว่าส่งมาจากผู้ส่งที่เชื่อถือได้หรือไม่

6. ข้อมูลส่วนบุคคลหรือข้อมูลที่สำคัญควรจัดเก็บแยกไว้ต่างหาก มีการกำหนดรหัสผ่านสำหรับเปิดโฟลเดอร์และไฟล์ข้อมูล และถ้าต้องมีการส่งข้อมูลผ่านเครือข่าย ควรใช้โปรแกรมเข้ารหัสข้อมูล เลือกใช้รหัสผ่านที่คาดเดาได้ยาก

7. ไม่ควรทำรายการทางการเงินโดยใช้คอมพิวเตอร์สาธารณะ หรือทำรายการโดยผ่านเครือข่ายไร้สาย (Wireless Networks) ซึ่งข้อมูลที่ใช้ในการ Login อาจจะถูกขโมยได้โดยง่าย

8. ติดตามข่าวเกี่ยวกับความเสี่ยงและการรักษาความปลอดภัยของคอมพิวเตอร์เพื่อให้รู้จักและรู้เท่าทันเทคนิคและวิธีการใหม่ๆ ที่ผู้ไม่ประสงค์ดีสามารถนำมาใช้ได้

สุดท้ายนี้ พึงสังวรไว้ว่า วิธีการที่มีประสิทธิภาพที่สุดในการป้องกันข้อมูลส่วนบุคคลและรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ของเราไม่ใช่อยู่ที่โปรแกรมต่างๆ แต่อยู่ที่ความระมัดระวังของเรานั่นเอง

JAP