วารสารวิชาชีพบัญชี

มุมไอที

มนวิกา ผดุงสิทธิ์*

SOPHOS's Security Threat Report: 2009

มุม IT สำหรับนักบัญชีฉบับนี้จะนำเสนอภัยคุกคามที่ผู้ใช้คอมพิวเตอร์ควรจะระมัดระวังในปี 2009 นี้ โดยเฉพาะภัยคุกคามในรูปแบบใหม่ จากรายงานเรื่อง “Security Threat Report: 2009” ซึ่งเป็นรายงานที่ออกโดยบริษัทโซโฟส (Sophos) บริษัทผู้เชี่ยวชาญทางด้านระบบรักษาความปลอดภัย

ภัยประการแรกคือ ภัยคุกคามบนเว็บไซต์ Sophos รายงานว่าในช่วง 2-3 ปีที่ผ่านมา แฮกเกอร์ได้มุ่งการโจมตีมาที่เว็บไซต์มากขึ้น แทนที่จะไปโจมตีเฉพาะระบบอีเมลเพียงอย่างเดียว เว็บไซต์ที่มีระบบการรักษาความปลอดภัยที่ไม่ดีเท่าที่ควร ก็จะถูกแฮกเกอร์ติดตั้งมัลแวร์ไว้ ผู้ที่เข้าไปเยี่ยมชมเว็บไซต์ดังกล่าวก็จะมีมัลแวร์ติดไปด้วยเป็นของแถม แฮกเกอร์มักจะมุ่งไปที่เว็บไซต์ที่เป็นที่นิยม เช่น เว็บไซต์ที่ขายบัตรเข้าชมฟุตบอล Euro 2008 เว็บไซต์ของบริษัทชั้นนำ และเว็บไซต์ของ Adobe เป็นต้น วิธีการหนึ่งที่แฮกเกอร์ใช้เรียกว่า “SQL Injection Attack” โดยการแทรกโค้ดอันตราย (Malicious Code) ไว้ในฐานข้อมูลที่ประมวลผลหรือทำงานตามคำสั่งของโปรแกรมในเว็บไซต์นั้นๆ เมื่อมีข้อมูลเข้า (เช่น ผู้ใช้กรอกข้อมูลในแบบฟอร์มบนเว็บ) ที่ไม่ได้รับการตรวจสอบอย่างถูกต้อง โค้ดอันตรายก็จะขัดขวางการทำงานของฐานข้อมูลตามคำสั่งที่ใส่ไว้ในโค้ด

ปีที่ 4 ฉบับที่ 11
พฤศจิกายน 2551
หน้า 19-22

* Ph.D (Accounting) ผู้ช่วยศาสตราจารย์ประจำ ภาควิชาการบัญชี
คณะกรรมการวิชาชีพด้านการศึกษาและเทคโนโลยีการบัญชี สภาวิชาชีพบัญชีฯ

นอกจากนี้ แฮกเกอร์อาจจะสร้างเว็บไซต์ที่มีโค้ดอันตรายขึ้นมาเองโดยใช้บริการของ Web-Hosting ที่ไม่ได้มีกระบวนการตรวจสอบการสมัครเข้าใช้เว็บไซต์มากนัก จากนั้นจึงส่งลิงค์ไปที่เว็บต่างๆ เสนอว่ามีโปรแกรมหรือวิดีโอคลิปแจกฟรีเพื่อหลอกให้คนเข้ามาที่เว็บไซต์ที่มีโค้ดอันตราย ประเทศที่เป็นแหล่งแพร่มัลแวร์ในเว็บไซต์มากที่สุด 3 อันดับแรก คือ สหรัฐอเมริกา จีน และรัสเซีย รายงานของ Sophos อ้างว่าประเทศไทยเป็นแหล่งแพร่มัลแวร์ในเว็บไซต์เป็นอันดับที่ 10 ร้อยละ 85 ของมัลแวร์จะซ่อนตัวอยู่ในเว็บไซต์ทั่วๆ ไปที่เป็นเว็บไซต์ที่ถูกต้องแต่ถูกโจมตีโดยแฮกเกอร์

เชื่อหรือไม่ว่า ปัจจัยสำคัญที่ทำให้ภัยคุกคามประเภทนี้แพร่หลายคือ คน ไม่ใช่จุดอ่อนของเว็บไซต์ เพราะเว็บไซต์ส่วนใหญ่มักจะถูกออกแบบมาเพื่อป้องกันมัลแวร์และภัยคุกคามในรูปแบบต่างๆ อยู่ในระดับหนึ่ง แต่ผู้ใช้ระบบมักจะหลีกเลี่ยงขั้นตอนการปฏิบัติบางประการทำให้ระบบการป้องกันทำงานได้ไม่เต็มที่ ตัวอย่างเช่น หน่วยงานอาจจะมีโปรแกรม Firewall เพื่อจำกัดการเข้าถึงเว็บไซต์บางเว็บ แต่ผู้ใช้งานจะใช้โปรแกรมที่สร้าง Proxy ปลอม (Anonymous Proxy) ซึ่งจะปกปิดเลขที่ประจำเครื่อง (IP Address) และข้อมูลบางอย่าง เช่น ข้อมูลของเครื่องต้นทาง รวมทั้งปกปิดลักษณะที่แท้จริงของเว็บไซต์ที่จะเข้าไป ทำให้โปรแกรม Firewall ของหน่วยงานยอมให้ผู้ใช้งานเข้าไปในเว็บไซต์ที่ถูกจำกัดการเข้าถึงได้ ดังนั้น โอกาสที่เครื่องคอมพิวเตอร์และระบบเครือข่ายของผู้ใช้คอมพิวเตอร์จะได้รับมัลแวร์จึงเพิ่มขึ้น ซึ่งโปรแกรมที่ใช้ทำ IP Address ปลอมหรือ Proxy ปลอมนั้น สามารถหา Download ได้ไม่ยากและที่สำคัญคือ มักจะแจกฟรี แต่ของฟรีและดีมักจะไม่มี จึงควรระวังว่าโปรแกรมดังกล่าวอาจจะมีโค้ดอันตรายซ่อนอยู่

ภัยประการที่สองคือภัยคุกคามทางอีเมล นับจากปี 2005 ภัยคุกคามที่แพร่หลายทางอีเมลในรูปแบบของไฟล์ที่แนบมากับอีเมลได้ลดลง อย่างไรก็ตาม ในช่วงครึ่งปีหลังของปี 2008 ภัยคุกคามดังกล่าวกลับเพิ่มขึ้น ซึ่ง Sophos ระบุว่าสาเหตุหนึ่งที่ทำให้ภัยคุกคามทางอีเมลเพิ่มขึ้นเกิดจากสแปมเมลซึ่งอาจจะมีไฟล์มัลแวร์แนบอยู่ เช่น เจ้าของอีเมลอาจจะได้รับอีเมล (ที่ดูเสมือนว่าส่งมาจาก FedEx หรือ UPS แจ้งว่าไม่สามารถส่งพัสดุได้ ซึ่งในอีเมลนั้นจะมีมัลแวร์ชื่อ Invo-Zip Trojan Horse แนบมาด้วย หรือบางรายได้รับอีเมล (ที่ดูเสมือนว่าส่งมาจากไมโครซอฟต์เพื่อให้ดาวน์โหลดโปรแกรมปรับปรุง (Patch) เพื่อ “อุด” ช่องโหว่ของซอฟต์แวร์โดยที่จริงๆ แล้ว Patch ดังกล่าวเป็นมัลแวร์ประเภท EncPk-CZ Trojan หรือมัลแวร์ที่ชื่อ Pushdo Trojan ที่แนบมากับอีเมลที่ส่งมาเพื่อชักชวนให้เข้าไปดูภาพเปลือยของนิโคล คิดแมนและแองเจลิน่า โจลี่ เมื่อเจ้าของอีเมลเปิดไฟล์ที่แนบมากับอีเมล ก็จะเป็นการรับให้มัลแวร์เข้ามาในเครื่องคอมพิวเตอร์

นอกจากการแนบโค้ดอันตรายมากับอีเมลแล้ว ยังมีการโจมตีโดยฝังลิงค์ของโค้ดอันตรายไว้ในอีเมลด้วย เพื่อหลอกให้ผู้ที่รับอีเมลคลิกที่ลิงค์ดังกล่าว เช่น ในเดือนสิงหาคม 2008 มีสแปมเมลที่ส่งข้อความอ้างว่าเป็นข่าวด่วนจาก MSNBC และ CNN ซึ่งในอีเมลนั้น จะให้ผู้ที่ได้รับอีเมลคลิกที่ลิงค์เพื่ออ่านข่าว แต่เมื่อคลิกที่ลิงค์ดังกล่าวแทนที่จะได้อ่านข่าว กลับถูกนำไปที่เว็บไซต์ที่มีโค้ดอันตรายที่ชื่อ Mal/EncPk-DA Trojan ฝังอยู่ ทำให้ระบบปฏิบัติการ Windows เสียหาย หรือในวันที่บารัค โอบามาชนะการเลือกตั้งประธานาธิบดีของสหรัฐอเมริกา ก็มีสแปมเมลส่งมาโดยมีลิงค์ให้คลิกเพื่อชมวิดีโอของโอบามา แต่เมื่อเข้าไปที่เว็บไซต์นั้นแล้ว ข้อมูลจากคอมพิวเตอร์ของผู้ใช้งานก็จะถูกขโมยและส่งออกไปให้กับเครื่อง Server ซึ่งอยู่ในประเทศยูเครน

ภัยคุมคามประเภทที่สามคือ มัลแวร์ วิธีการที่สำคัญอีกวิธีหนึ่งที่อาชญากรคอมพิวเตอร์ใช้เพื่อหลอกเอาเงินของเหยื่อไปคือ การใช้โปรแกรมป้องกันไวรัสปลอมที่เรียกกันว่า “Scareware” หรือ “Rogueware” ซึ่งการโจมตีดังกล่าวจะทำให้เหยื่อคิดว่าเครื่องคอมพิวเตอร์ของตนมีปัญหา โปรแกรม Scareware มักจะซ่อนตัวอยู่ในเว็บไซต์ในรูปของหน้าต่างโฆษณาเล็กๆ (Popup) หรือไฟล์ที่จะให้ดาวน์โหลด นอกจากนี้ แฮกเกอร์อาจจะส่ง

สแปมเมลที่มี Scareware แนบอยู่ หรืออาจใช้เทคนิคที่เรียกว่า Social Engineering ที่ล่อหลอกให้พนักงานในองค์กรคลิกไปที่ไฟล์ที่แนบหรือลิงค์เพื่อเข้าไปที่เว็บไซต์ที่มี Scareware ซึ่งเว็บไซต์ดังกล่าวจะมีโปรแกรมรักษาความปลอดภัย (ปลอม) พร้อมกับรีวิว (ปลอมๆ อีกเช่นกัน) ของโปรแกรมดังกล่าวว่ามีประสิทธิภาพมากในการกำจัดไวรัส บางเว็บไซต์ก็จะขโมยรายละเอียดเกี่ยวกับบัตรเครดิตของเหยื่อ Sophos ระบุว่าโดยเฉลี่ยแล้ว มีเว็บไซต์ที่มี Scareware เกิดขึ้นใหม่ 5 เว็บไซต์ทุกวัน บางวันอาจจะเพิ่มเป็น 20 เว็บไซต์ แม้แต่โปรแกรมรักษาความปลอดภัยที่มีชื่อเสียงอย่าง Norton Antivirus และ AVG ก็ตกเป็นเป้าหมายของการโจมตีด้วย

ที่น่าตกใจคือ Sophos เปิดเผยว่า บริษัทผู้ผลิตซอฟต์แวร์ที่ถูกต้องตามกฎหมายบางแห่งกลับใช้ Scareware เป็นเครื่องมือในการเพิ่มยอดขาย เช่น ลี ชินจา อดีตผู้บริหารของบริษัทผู้ผลิตโปรแกรมป้องกันไวรัสของเกาหลี ได้รับเงินมากกว่า 9.8 ล้านเหรียญในปี 2005 จากการหลอกให้ผู้ใช้อินเทอร์เน็ตมากกว่า 1 ล้านรายใช้โปรแกรมป้องกันสปายแวร์ฟรี โดยโปรแกรมดังกล่าวจะแสดงข้อความ (หลอก) ว่าเครื่องคอมพิวเตอร์ของผู้ใช้มีปัญหาด้านระบบการรักษาความปลอดภัย และแนะนำให้ผู้ใช้ซื้อโปรแกรมป้องกันไวรัสจากบริษัทของเขา

ในปัจจุบัน มัลแวร์ได้เพิ่มจำนวนขึ้นอย่างรวดเร็วผ่านทางอุปกรณ์เก็บข้อมูล เช่น Thumb Drive หรือการ์ดหน่วยความจำ การใช้เว็บไซต์ประเภทเครือข่ายสังคมออนไลน์ (Social Network) เช่น Hi5 หรือ Facebook ก็เป็นอีกทางหนึ่งที่ทำให้มัลแวร์เพิ่มหลาย แฮกเกอร์มักจะโจมตีเว็บไซต์ดังกล่าวเพื่อขโมยชื่อผู้ใช้และรหัสผ่าน และใช้ข้อมูลส่วนตัวดังกล่าวในการส่งมัลแวร์และสแปมออกไปตามเครือข่ายเป็นจำนวนมาก นอกจากนี้ แทนที่แฮกเกอร์จะจ้องโจมตีแพาะจุดอ่อนของระบบปฏิบัติการและเว็บเบราเซอร์ ปัจจุบันแฮกเกอร์มุ่งโจมตีไปที่จุดอ่อนของโปรแกรมที่มีการใช้งานกันอย่างแพร่หลายมากขึ้น เช่น PDF

ภัยคุกคามลำดับถัดมาคือ สแปม ซึ่งยังคงเป็นปัญหาสำคัญของธุรกิจ Sophos เปิดเผยว่า ร้อยละ 9[illegible] อีเมลธุรกิจเป็นสแปมเมล เมื่อพิจารณาเป็นรายประเทศพบว่า ในปี 2008 ประเทศสหรัฐอเมริกามีสแปมเมลมากที่สุด แต่เมื่อพิจารณาเป็นรายภูมิภาคพบว่า 1 ใน 3 ของสแปมทั้งหมดมาจากภูมิภาคเอเชีย สแปมส่วนใหญ่มาจากคอมพิวเตอร์ตามบ้านที่มีบอทเน็ต (BOTNET) นั่นคือการที่คอมพิวเตอร์จำนวนมากถูกควบคุมโดยแฮกเกอร์ถูกสั่งการให้ส่งข้อความหรือไวรัสผ่านเครือข่ายโดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่รู้ตัว นอกจากนี้ สแปมยังแพร่หลายผ่านทางเครือข่ายสังคมออนไลน์ (Social Network) และจดหมายข่าว (Newsletter) เช่นเดียวกับมัลแวร์

นอกจากผู้ใช้ระบบปฏิบัติการ Windows จะเป็นเป้าหมายหลักของการโจมตีจากภัยคุกคามในรูปแบบต่างๆ แล้ว Sophos ยังเตือนว่า ผู้ที่ใช้ระบบปฏิบัติการของ Apple Mac ก็ไม่ควรนิ่งนอนใจ เนื่องจากพบว่าในปี 2008 มีมัลแวร์ และ Scareware ที่โจมตีผู้ที่ใช้คอมพิวเตอร์ของ Mac มากขึ้น ซึ่งสาเหตุมาจากการที่มีผู้ใช้คอมพิวเตอร์ Mac มากขึ้น เพราะไม่ชอบ Windows Vista ทำให้ยอดขายของ Apple Mac เพิ่มขึ้น นอกจากนี้ ผู้ใช้ Mac มักจะคิดว่าระบบปฏิบัติการของตนไม่ใช่เป้าหมายในการโจมตี จึงไม่ได้มีความระมัดระวังเท่าที่ควร

นอกจากนี้ Sophos ยังได้เตือนถึงกระแสความนิยมในการใช้โทรศัพท์ไอโฟนของ Apple ซึ่งทำให้เข้าเว็บไซต์ได้เร็วขึ้นและราคาถูกลง แม้ว่าโทรศัพท์ไอโฟนจะยังไม่ใช่เป้าหมายหลักของการโจมตี แต่อีเมลมือถือของ Apple ก็มีจุดอ่อนและบริษัทก็ยังไม่ได้สร้าง Patch ขึ้นมาเพื่อแก้จุดอ่อนดังกล่าว ดังนั้น ผู้ที่ใช้โทรศัพท์ไอโฟนจึงควรระวังว่าอาจจะถูกโจมตีโดยเทคนิคที่เรียกว่า Phishing มากกว่าการถูกโจมตีเมื่อใช้คอมพิวเตอร์เสียอีก เนื่องจากเบราเซอร์ของไอโฟนจะแสดง URL (ที่อยู่ของไฟล์หรือเว็บไซต์) เพียงบางส่วนใน Address Bar (ตำแหน่งที่ใช้ในการพิมพ์ที่อยู่ของเว็บไซต์) ทำให้แฮกเกอร์หลอกผู้ใช้ไอโฟนได้ง่าย

ยิ่งขึ้นว่าเว็บดังกล่าวเป็นเว็บที่ถูกต้อง นอกจากนี้ ผู้ใช้ไอโฟนจะต้องคีย์ URL เองโดยใช้จอสัมผัส ซึ่งอาจจะคีย์ได้ยากกว่าคอมพิวเตอร์ ดังนั้น การคลิกที่ลิงค์ก็จะง่ายกว่า

การรั่วไหลของข้อมูล (Data Leakage) ก็เป็นภัยคุกคามอีกประเภทหนึ่งที่ควรระวัง เนื่องจากการทำงานในรูปแบบปัจจุบัน พนักงานจะสามารถเข้าถึงข้อมูลของบริษัทได้ทั้งจากภายในและภายนอกสำนักงาน รวมทั้งบริษัทอาจจะมีเปิดระบบบางส่วนให้ผู้ใช้ภายนอกบางรายเข้าถึงข้อมูลได้ เช่น กิจการคู่ค้าและลูกค้า ซึ่งการทำงานในรูปแบบดังกล่าวไม่ได้เป็นเรื่องใหม่ ผู้ใช้งานมักจะรู้สึกว่าเป็นงานประจำที่ทำอยู่เป็นปกติ จึงมักจะไม่ค่อยระมัดระวัง Sophos เปิดเผยว่า เกือบร้อยละ 30 ของผู้ใช้คอมพิวเตอร์เก็บข้อมูลทางการเงิน ข้อมูลลูกค้า รวมทั้งข้อมูลส่วนตัวในอุปกรณ์เก็บข้อมูลประเภท Removable เพราะสะดวกต่อการใช้งาน แต่จะทำให้ข้อมูลรั่วไหลได้มากกว่าการโดนโจมตีด้วยโค้ดอันตราย นอกจากนี้ ยังพบว่ามีความต้องการซื้อ Hard Disk เก่าทางเว็บไซต์ของ eBay มากขึ้น เนื่องจากบางบริษัทเมื่อเลิกใช้คอมพิวเตอร์แล้วจะนำคอมพิวเตอร์เก่าไปประมูลขายทาง eBay ผู้ที่ซื้อฮาร์ดดิสก์เก่าอาจจะกู้ข้อมูลในฮาร์ดดิสก์ขึ้นมาได้ถ้าบริษัทไม่ได้ลบข้อมูลที่อยู่ในฮาร์ดดิสก์ด้วยวิธีละเอียดถี่ถ้วน

วิธีการป้องกันการรั่วไหลของข้อมูลที่สำคัญคือ ควรจะเข้ารหัสข้อมูลที่สำคัญ รวมทั้งจำกัดการเข้าถึงระบบคอมพิวเตอร์ สื่อที่ใช้ในการเก็บข้อมูล อุปกรณ์ต่างๆ และอีเมล แม้แต่ระบบเครือข่ายแบบไร้สายก็ควรจะมีการป้องกันการเข้าถึงด้วย เนื่องจากแฮกเกอร์อาจจะใช้เทคนิคที่เรียกว่า Wardriving ในการเสาะหาหน่วยงานที่ใช้ระบบเครือข่ายแบบไร้สายแต่มีจุดอ่อนด้านการรักษาความปลอดภัย เพื่อเข้าไปในระบบคอมพิวเตอร์ของบริษัท ติดตั้งมัลแวร์และขโมยข้อมูลสำคัญไปขาย นอกจากนี้ Sophos ยังระบุว่าอีกสาเหตุหนึ่งที่ทำให้ภัยคุกคามทางอินเตอร์เน็ตเพิ่มขึ้นมาจากการที่บางประเทศมีการใช้ข้อมูลมาเพื่อใช้ประโยชน์ทางด้านการเมือง การค้าและการทหาร

Sophos สรุปว่าในปี 2009 นี้ ผู้ใช้คอมพิวเตอร์ยังคงต้องพบกับความท้าทายในการป้องกันและควบคุมความปลอดภัยของคอมพิวเตอร์ของตน เนื่องจากอาชญากรคอมพิวเตอร์ได้ใช้ประโยชน์ความก้าวหน้าของเทคโนโลยีเพื่อกระทำการทุจริตมากขึ้น การโจมตีจะเพิ่มรูปแบบที่หลากหลายมากขึ้น การใช้โทรศัพท์มือถือโดยเพิ่มความสามารถด้านการสื่อสารคล้ายกับคอมพิวเตอร์เปิดโอกาสให้แฮกเกอร์ก่อการทุจริตมากขึ้น นอกจากนี้ ภัยคุกคามประเภทการขโมยข้อมูลส่วนตัวและการทุจริตด้านคอมพิวเตอร์จะยังคงมีอยู่ต่อไปเนื่องจากความผิดพลาดและความไม่ระมัดระวังของผู้ใช้คอมพิวเตอร์ อย่างไรก็ตาม ปัญหาเหล่านี้จะเบาบางลงถ้าผู้ใช้คอมพิวเตอร์เตรียมพร้อมด้านการป้องกัน ปฏิบัติตามขั้นตอนในการรักษาความปลอดภัยอย่างเคร่งครัด และเรียนรู้เพื่อเตรียมรับมือกับภัยคุกคามในรูปแบบต่างๆ

JAP