เตรียมรับมือภัยคุกคามบนโลกไซเบอร์ปี 2554

ผศ.สุพล พรหมมาพันธุ์
คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

ลงตีพิมม์ในหนังสือพิมพ์ไทยโพสต์ ปีที่ 15 ฉบับที่ 5179 วันศุกร์ที่ 7 มกราคม พ.ศ. 2554 หน้า 4

จากปรากฏการณ์ของเว็บไซต์วิกิลีกส์ที่เปิดโปงแฉความลับทางการทูตและการทหาร ในช่วงส่งท้ายปีเก่า พ.ศ. 2553 ที่ผ่านมา ทำให้ประเทศมหาอำนาจอย่างสหรัฐอเมริกา และประเทศอื่นๆ ทั่วโลก ต่างหวั่นวิตกกันถ้วนหน้าว่า **"ความลับ จะยังคงเป็นความลับไปได้อีกนานเท่าใด ในเมื่อทุกประเทศก็มีศัตรู ทุกองค์กรธุรกิจก็มีคู่แข่งขัน"** ดังนั้น ความมั่นคงและความปลอดภัยของข้อมูลสารสนเทศ จึงเป็นหัวใจสำคัญที่จะไม่ให้ผู้ใดล่วงรู้ได้ง่ายๆ ในรอบปีที่ผ่านมา นายบารัค โอบามา ประธานาธิบดีของสหรัฐอเมริกา ได้ทุ่มงบประมาณรับมือกับการรักษาความปลอดภัย การปราบปรามอาชญากรรมคอมพิวเตอร์ รวมถึงความมั่นคงของชาติมากกว่า 250,000 ล้านดอลลาร์สหรัฐฯ ในแต่ละปี และมีรายงานจากห้องปฏิบัติการคอมพิวเตอร์ของ McAfee Lab บริษัทผู้ผลิตซอฟต์แวร์ทางด้านระบบรักษาความปลอดภัย ทำนายว่าภัยคุกคามร้ายแรงในโลกไซเบอร์ปี 2554 คือ :

(1). **ภัยจาก Social Media และบริการย่อ URL** การใช้งาน Social Media กลายเป็นเรื่องธรรมดาในชีวิตผู้ใช้งานทั่วๆ ไปเป็นที่เรียบร้อยแล้วในปัจจุบัน และเนื่องจากผู้ใช้งาน Social Media ส่วนใหญ่นั้นต้องการให้ข้อความของตนเองสั้นๆ (โดยเฉพาะใน Twitter ที่ใส่ได้เพียง 140 ตัวอักษรต่อข้อความ) บริการย่อ URL เช่น bit.ly จึงได้รับความนิยมเป็นอย่างมาก ซึ่งเป็นที่มาของการโจมตีในอนาคตที่อาจหลอกลวงให้เหยื่อ Click URL เหล่านี้เพื่อนำเหยื่อไปยัง Web Site หลอกลวง (เช่น Web Site ที่ออกแบบมาให้เหมือนกับธนาคารเพื่อหลอกถาม username/password) หรือ website ที่มี malware ต่างๆเป็นต้น, (2).**ภัยจาก Social Media และ Location-based service** การใช้งาน location-based service เช่น Facebook place หรือ foursquare เริ่มได้รับความนิยมมากขึ้นเรื่อยๆ ซึ่งนอกจากบริการเหล่านี้จะเป็นประโยชน์สำหรับครอบครัวและเพื่อนๆ ในการติดต่อสื่อสาร หรือเชื่อมความสัมพันธ์ระหว่างกันแล้ว ยังเป็นประโยชน์สำหรับผู้ไม่หวังดีในการติดตามเหยื่อด้วย ซึ่งมีกรณีศึกษาหลายกรณีแล้วในต่างประเทศ เช่นโจรในอังกฤษที่ใช้ location-based service เพื่อตรวจสอบว่าเหยื่อไม่อยู่บ้าน แล้วจึงเข้าไปโจรกรรมภายในบ้าน หรือ stalker ในสหรัฐอเมริกาที่ใช้ location-based service เพื่อตามหาที่อยู่ของผู้หญิงที่เป็นเหยื่อ พอให้เหยื่อ check-in เข้าบ้าน แล้วจึงบุกเข้าไปข่มขืนเป็นต้น ภัยเหล่านี้อาจดูไกลตัว แต่ในปี พ.ศ. 2554 สิ่งเหล่านี้คงไม่ใช่เรื่องไกลตัวอีกต่อไป, (3). **ภัยจากโทรศัพท์มือถือ** ในอดีตนั้นโทรศัพท์มือถือเป็น Platform ที่มีภัยคุกคามต่างๆ เช่น Virus, Trojan, Worm ไม่มากนัก เช่น ช่องโหว่บน iPhone ที่ทำให้นักพัฒนาสามารถทำ Jailbreak ได้ หรือ Trojan เต็มรูปแบบบน Android เป็นต้น แต่ในปี 2554 นี้ ภัยคุกคามต่างๆ จะเริ่มหันมาหาโทรศัพท์มือถือมากขึ้น เนื่องจากโทรศัพท์มือถือนั้นเป็นแหล่งข้อมูลชั้นดีไม่ว่าจะเป็นข้อมูลส่วนบุคคล ข้อมูลทางการเงิน ซึ่งกลายมาเป็นเป้าหมายสำคัญของการโจมตีในปัจจุบัน, (4). **ภัยจากระบบปฏิบัติการของ Apple** ในอดีตนั้นระบบปฏิบัติการ Apple ได้ชื่อว่าเป็นระบบปฏิบัติการที่ปลอดภัยมาก เนื่องจาก Run บน CPU ประเภท RISC ทำให้ Malicious Code ต่างๆ ที่ทำงานได้บน Platform อื่นๆ ไม่สามารถมาทำงานบนระบบปฏิบัติการของ Apple ได้ แต่การเปลี่ยนแปลงไปใช้ CPU ของ Intel ซึ่งเป็น CPU ประเภท CISC เช่นเดียวกับ Platform อื่นๆ และการเติบโตอย่างก้าวกระโดดของ Apple โดยเฉพาะการดึงดูดผู้ใช้ซึ่งมีลักษณะเป็น End User คือใช้งานเป็นอย่างเดียวเข้ามาเป็นจำนวนมากนั้น ย่อมหนีไม่พ้นที่จะดึงดูดเหล่ามิจฉาชีพเข้ามาเป็นจำนวนมากด้วย ดังนั้นผู้ใช้งานระบบปฏิบัติการต่างๆ ของ Apple ไม่ว่าจะเป็น Desktop, Notebook หรือแม้กระทั่ง iPhone จึงไม่ควรละเลยที่จะติดตามข่าวสาร และฟังคำแนะนำต่างๆ ในด้านการรักษาความปลอดภัยอย่างสม่ำเสมอ, (5). **ภัยจาก Application บน TV** ภัยคุกคามนี้ค่อนข้างจะไกลตัวพวกเรา

ซักเล็กน้อย เนื่องจาก Platform อย่าง Google TV ที่ได้รับความนิยมมากในสหรัฐอเมริกานั้น ไม่ค่อยได้รับความนิยมในบ้านเรานัก (อาจจะเนื่องมาจากบ้านเรายังมี Infrastructure ที่สนับสนุน เทคโนโลยีนี้ได้ไม่ดีเท่าไหร่ด้วย) การที่ Platform เหล่านี้อยู่ใกล้ตัวผู้ใช้งาน และมีจุดเด่นที่การให้บริการด้านความบันเทิง ทำให้ผู้ใช้งานทั่วไปอาจจะไม่ได้ใส่ใจในด้านความปลอดภัยของอุปกรณ์เหล่านี้นัก ทำให้มีโอกาสที่ Application ที่ไม่หวังดีจะเข้าไปขโมยข้อมูลส่วนตัวจากอุปกรณ์เหล่านี้ หรือแม้กระทั่งสร้างเครือข่าย Botnet ของตัวเองขึ้นมาได้, (6). **ภัยจากคนใกล้ชิดหรือคนรู้จัก** หมดสมัยแล้วครับที่ virus หรือ spam จะมาจากใครก็ไม่รู้ ภัยคุกคามในปี 2554 นั้นมีแนวโน้มที่จะมาจากเพื่อนหรือคนรู้จัก ที่ติดเชื้อแล้วส่งข้อความต่อไปโดยไม่รู้ตัวมากกว่า (ตัวอย่างที่เห็นได้ชัดก็คือ virus MSN ตัวใหม่นั้นมีแม้กระทั่งภาษาไทย) ดังนั้นต่อไปนี้จะ Click Link ใน Instant Messaging หรือ Social Network หรือ e-Mail จากเพื่อนหรือคนรู้จักนั้นก็ต้องพิจารณาให้ดีด้วย, (7).**ภัยจาก Botnet:** จากกรณีของ Wiikileaks ทำให้วงการ Network Security เริ่มหันมาสนใจการโจมตีด้วย Botnet อีกครั้ง เนื่องจากการโจมตีแบบนี้นั้นทำได้ไม่ยากนัก, ใช้ทรัพยากรไม่มาก (เนื่องจากใช้ CPU และ Network Resource จากเหยื่อเป็นหลัก), ตรวจจับได้ยาก (เนื่องจากเหยื่อกระจายอยู่ตามที่ต่างๆ ทั่วโลก) ดังนั้นการโจมตีในลักษณะนี้จึงมีแนวโน้มจะเพิ่มสูงขึ้นเรื่อยๆ และจะเริ่มเปลี่ยนจากการใช้ Botnet เพื่อโจมตีผู้อื่นแบบ DDoS (Distributed Denial of Service) หรือ Spam มาเป็นใช้เพื่อเก็บรวบรวมข้อมูล หรือทำลายข้อมูลเฉพาะบางอย่างเป็นหลัก (8). **ภัยจากการรวมกลุ่มกันของ Hacker** การรวมกลุ่มกันภายใต้ชื่อ Anonymous เพื่อโจมตีผู้ที่ไม่ให้ความสนับสนุน WikiLeaks เช่น Master Card หรือ Paypal ทำให้แนวโน้มของการโจมตีระดับใหญ่ๆ ในอนาคตของบรรดา Hacker มีแนวโน้มที่จะรวมกลุ่มกันมากกว่าที่จะแยกกันโจมตีแบบตัวใครตัวมันเหมือนในอดีต (9). Advanced Persistent Threat (APT) **ภัยคุกคามในรูปแบบใหม่** ภัยคุกคามรูปแบบนี้คือการโจมตีที่มุ่งเน้นเป้าหมายที่มี Scale ใหญ่ๆ เช่นองค์กรในองค์กรหนึ่ง หรือรัฐบาลประเทศใดประเทศหนึ่ง ซึ่งเกิดจากการให้ความสนับสนุน (ทั้งแบบเปิดเผยหรือแบบลับๆ) จากองค์กรขนาดใหญ่ หรือระดับรัฐบาลของอีกประเทศหนึ่ง ทำให้การโจมตีนั้นส่งผลอย่างรุนแรง และรับมือได้ยาก (www.blogkore.com)

นอกจากนี้ยังมี **ภัยจากการใช้** Windows 7 เนื่องจาก Windows 7 เป็นระบบปฏิบัติการที่เพิ่งเปิดตัวใหม่ คาดว่าจะมีปริมาณจำนวนผู้ใช้งานเพิ่มมากขึ้นทั้งบนเครื่องคอมพิวเตอร์และสมาร์ทโฟน เป็นช่องทางใหม่ให้ผู้โจมตีระบบคิดค้นไวรัสสายพันธุ์ใหม่ รวมทั้งมัลแวร์รูปแบบอื่นๆ เพื่อเจาะและทำลายระบบปฏิบัติการชนิดนี้ ในส่วนของประเทศไทยเองได้เตรียมรับมือภัยคุกคามบนโลกไซเบอร์เอาไว้บ้างแล้ว จะเห็นได้จากเมื่อวันที่ 13 พฤษภาคม พ.ศ. 2553 กระทรวงเทคโนโลยีสารสนเทศ และการสื่อสาร ได้ทุ่มงบประมาณเพื่อจ้างผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และคอมพิวเตอร์ โดยใช้งบประมาณจำนวน 28 ล้านบาท และมีกำหนดระยะเวลาปฏิบัติงานให้แล้วเสร็จภายใน 12 เดือน แต่ว่าจะได้ผลมากน้อยเพียงใดต้องติดตามดูกันต่อไป ส่วนภาคองค์กรธุรกิจก็ควรหันมาให้ความสำคัญกับเรื่องนี้กันให้มากขึ้นด้วย เพราะหากเกิดความเสียหายขึ้นแล้ว ย่อมส่งผลกระทบโดยรวมต่อระบบเศรษฐกิจของประเทศ.