ไทยรัฐ
วันที่ 4 สิงหาคม พ.ศ. 2551
http://www.thairath.co.th/

ภัยคุกคามครึ่งแรกปี 2551 ระบบไอที ถูกอะไรจู่โจมบ้าง

ผ่านพ้นไปแล้วกับช่วง 6 เดือนแรกของปี 2551 ในแวดวงการไอที ก็มักจะมีการสรุปภาพรวมของธุรกิจ และอุตสาหกรรม เช่นเดียวกับวงการซิเคียวริตี้ ก็จะมีการสรุปภาพรวมของภัยคุกคาม และเหตุการณ์ต่างๆ ที่เกิดขึ้นจากกลุ่มผู้ไม่ประสงค์ดีเพื่อหวังในทรัพย์สินจากการล่อลวง หรือ ทำเว็บไซต์หลอกเก็บข้อมูลส่วนบุคคล หรือ การจู่โจมระบบคอมพิวเตอร์ด้วยมัลแวร์ชั้นสูง เพื่อสร้างเครือข่ายบ็อตเน็ต หรือ กองทัพคอมพิวเตอร์ซอมบี้ เพื่อแฮกเกอร์จะได้นำไปใช้เป็นเครื่องมือโจมตีเว็บไซต์อื่นๆ เป็นต้น ดังนั้น เราทุกคนจึงควรรู้ว่าที่ผ่านมา เกิดอะไรขึ้น อันจะช่วยให้ผู้ใช้คอมพิวเตอร์สามารถรับมือกับภัยคุกคามต่างๆ ได้

นายคงศักดิ์ ก่อตระกูล ที่ปรึกษาด้านเทคนิค บริษัท เทรนด์ ไมโคร (ประเทศไทย) จำกัด เล่าถึงรายงานสรุปภัยคุกคามข้อมูลช่วง 6 เดือนแรก และการคาดการณ์ภัยคุกคามช่วงครึ่งหลังของปี 2551 ว่า ขณะนี้ บรรดาอาชญากรไซเบอร์ไม่เพียงแต่ใช้เทคโนโลยีใหม่ต่างๆ ในการเพิ่มประสิทธิภาพในการก่ออาชญากรรมมากขึ้นเท่านั้น แต่ยังสร้างรูปแบบใหม่ของเทคนิควิศวกรรมทางด้านสังคมเพื่อหลอกล่อให้ผู้บริโภค และองค์กรธุรกิจเข้ามาติดกับได้อย่างชาญฉลาด โดยจากการตรวจสอบในช่วง 6 เดือนที่ผ่านมา พบการเพิ่มขึ้นของภัยคุกคามบนเว็บ ในขณะที่แอดแวร์ และสปายแวร์ที่สร้างโดยใช้เทคนิคที่ล้าสมัย และไม่สามารถหลุดรอดการตรวจจับของโซลูชันรักษาความปลอดภัยระดับสูงได้นั้นกลับมีจำนวนลดลงอย่างต่อเนื่อง

BEIJING 2008 OLYMPIC LOTTERY PROMOTION

LOTTERY WINNING NOTIFICATION

Dear Sir / Madam,

Country: Beijing, China.

VERIFICATION FORM TO AUTHENTICATE YOUR EMAIL

Full Name
Delivery Address
Sex Age
Occupation

ที่ปรึกษาด้านเทคนิค บริษัท เทรนด์ ไมโครฯ อธิบายว่า ขณะที่เทคนิควิศวกรรมด้านสังคม เช่น **ฟิชชิงลวงของไนจีเรีย (Nigerian scam)** ที่ในเนื้อหาของอีเมล์กล่าวถึงเจ้าชายแห่งประเทศไนจีเรียกำลังเดือดร้อนให้คนที่ได้รับอี-เมล์นี้โอนเงินไปให้ และถ้าได้ขึ้นครองราชย์เมื่อใดจะมีการตอบแทนด้วยเงินจำนวนมหาศาล และการหลอกลวงของนักโทษชาวสเปน มีการใช้งานในลักษณะนี้มาหลายสิบปีแล้ว และอาชญากรต่างๆ ยังคงฟื้นฟูและปรับรูปแบบมาตรฐานของกลโกงนี้ให้ทันสมัยอยู่เสมอ ไม่ว่าแนวโน้มที่ปรากฏจะเป็นเช่นไร แต่เครื่องมือและเทคโนโลยีที่ใช้สร้างระบบโต้ตอบ ของไซต์เครือข่ายทางสังคมยอดนิยม กำลังจะกลายเป็นกับดักสำคัญของการก่ออาชญากรรม

นายคงศักดิ์ อธิบายต่อว่า ในช่วงเดือนมี.ค.ที่ผ่านมา บริษัท เทรนด์ ไมโครพบว่าชุดเครื่องมือฟิชชิงกว่า 400 ชุด ถูกออกแบบมาเพื่อสร้างไซต์ฟิชชิงที่มีเป้าหมายไปยังไซต์ Web 2.0 ชั้นนำ หรือเครือข่ายทางสังคม บริการแชร์วิดีโอ และ VoIP ผู้ให้บริการอีเมล์ฟรี เว็บไซต์ธนาคาร และอีคอมเมิร์ซยอดนิยม โดยเมื่อไม่นานมานี้ รูปแบบใหม่ของฟิชชิง นำเสนอในรูปการเตือนให้เหยื่อระวังเกี่ยวกับอีเมล์ฟิชชิง ที่เป็นวิธีที่ทำให้อีเมล์ฉบับนั้นดูน่าเชื่อถือ จากนั้นก็จะหลอกล่อให้เหยื่อคลิกลิงค์ ที่จะนำไปสู่ไซต์อันตรายต่อไป

ที่ปรึกษาด้านเทคนิค บงเทรนด์ ไมโครฯ เล่าเสริมว่า ขณะที่ เหล่าบรรดาสแปมเมอร์ยังนำเทคนิคเก่าๆ มาใช้ซ้ำ เมื่อเดือน ก.พ.ปีนี้ ได้ตรวจสอบพบฟิชชิงเสียง (หรือเรียกว่า "วิชชิง" (vishing)) ข้อความที่ปรากฏเชิญชวนจะมีลิงค์ที่นำไปสู่เพจเป้าหมายที่ดูไม่ผิดปกติ และในเพจนั้นได้แอบใส่หมายเลขโทรศัพท์ลวงเอาไว้ เพื่อให้ผู้รับทำการโทรไปเปิดใช้งานบัญชีของตนเองอีกครั้ง เมื่อหลงเชื่ออีเมล์ที่แจ้งไปว่าบัญชีของเหยื่อ "ใช้การไม่ได้" และหลังจากที่เหยื่อโทรไปยังหมายเลขโทรศัพท์นั้นแล้ว ก็จะถูกถามหมายเลขบัญชีธนาคาร และรหัสผ่าน (PIN) โดยจะเป็นการเปิดเผยข้อมูลบัญชีธนาคารของตัวเอง ให้กับเหล่าฟิชเชอร์โดยไม่รู้ตัว

นายคงศักดิ์ อธิบายอีกว่า ทั่วไปสายพันธุ์ต่างๆ ของมัลแวร์จะเป็นภัยคุกคามในรูปแบบที่แยกกันต่างหาก แต่ขณะนี้ ภัยคุกคามบนเว็บได้ผสมส่วนประกอบซอฟต์แวร์ร้ายกาจ อันหลากหลายรวมมาเป็นโมเดลทางธุรกิจของภัยคุกคามทางเว็บในรูปแบบเดียว เช่น อาชญากรไซเบอร์ส่งสแปม ที่มีลิงค์ฝังมาในอีเมล์ (URL ลวง) หรือมีข้อความด่วนมาให้เหยื่อ เมื่อเหยื่อคลิกก็จะถูกส่งไปยังเว็บไซต์ ที่จะดาวน์โหลดโทรจัน ลงในคอมพิวเตอร์ของเหยื่อโดยอัตโนมัติ จากนั้น โทรจันจะดาวน์โหลดสปายแวร์ เพื่อตรวจจับข้อมูลสำคัญ เช่น หมายเลขบัญชีธนาคาร แม้ว่าจะดูเหมือนว่าเป็นแค่เหตุการณ์เดียว แต่ภัยคุกคามลูกผสมในลักษณะนี้กำลังสร้างความยุ่งยาก และเป็นอันตรายต่อผู้ใช้มากขึ้นด้วยการใช้เทคโนโลยีใหม่ๆ

ที่ปรึกษาด้านเทคนิค บริษัท เทรนด์ ไมโครฯ กล่าวเพิ่มเติมว่า **เทคนิค Fast-flux** เป็นอีกหนึ่งตัวอย่างของอาชญากรที่ใช้การพัฒนาเทคโนโลยีไปในทางที่ผิด โดยเทคนิค Fast-flux เป็นกลไกสลับ DNS (domain-name-server) ที่รวมเครือข่ายเพียร์ทูเพียร์ การใช้คำสั่งและการควบคุมแบบกระจาย การใช้ โหลด บาลานซ์ซิง บนเว็บไซต์ และการเปลี่ยนเส้นทางพร็อกซี เพื่อทำให้ไซต์ที่แจกจ่ายฟิชชิงยากต่อการถูกตรวจพบ โดย Fast-flux จะช่วยให้ไซต์ฟิชชิงสามารถมีอายุที่ยาวนานขึ้น เพื่อว่าจะได้หลอกล่อเหยื่อได้มากขึ้น เช่น นักวิจัยมัลแวร์ต้องประสบปัญหาในการระบุโดเมนของ Storm วายร้าย เพราะอาชญากรใช้เทคนิค Fast-flux ที่สามารถหลบเลี่ยงการตรวจจับได้

นายคงศักดิ์ กล่าวถึงรายงานฯ ว่า เทรนด์ ไมโครพบการเพิ่มอย่างมาก ของภัยคุกคามบนเว็บในช่วงครึ่งแรกของปีนี้ โดยภัยคุกคามบนเว็บเกิดขึ้นสูงสุดในเดือน มี.ค.ที่ผ่านมาที่ระดับ 50 ล้านครั้งจากที่มีอยู่ประมาณ 15 ล้านครั้ง เมื่อเดือน ธ.ค. 2550 ขณะที่แอดแวร์ แทรกแวร์ คีย์ล็อกเกอร์ และฟรีโหลดเดอร์กลับมีจำนวนลดลง โดยเมื่อเดือน มี.ค.ปีที่แล้วพบว่าพีซีประมาณ 45% ติดแอดแวร์ เมื่อเทียบกับเดือน เม.ย.2551 มีพีซีเพียง 35% เท่านั้นที่มีการติดเชื้อ

ต่อด้านหลัง

ขณะที่รายงานเมื่อเดือน พ.ค.ปีก่อนพบว่า พีซีประมาณ 20% ติดเชื้อแทร็กแวร์ และจำนวนดังกล่าวลดลงเหลือไม่ถึง 5% ในเดือน เม.ย.ปีนี้ นอกจากนี้คีย์ล็อกเกอร์ก็มีจำนวนน้อยลงด้วย และยังคงลดลงอย่างต่อเนื่องโดยมีจำนวนไม่ถึง 5% ของพีซีที่ติดเชื้อ (จากเดิมมีมากกว่า 5% เมื่อเดือนกันยายน 2550) นี่เป็นตัวอย่างที่ดีที่จะได้ทราบว่าอาชญากรไซเบอร์กำลังพัฒนาไปในทิศทางใด คนกลุ่มนี้กำลังก้าวจากภัยคุกคามที่ใช้เทคโนโลยีเก่าหรือไม่มีประสิทธิภาพหันไปใช้ภัยคุกคามที่สร้างผลกำไรที่นำมาซึ่งรายได้ที่มากขึ้น

ด้าน **นายนพชัย ตั้งไตรธรรม** ที่ปรึกษาทางเทคนิค บริษัท ไซแมนเทค คอร์ปอเรชั่น กล่าวว่า จำนวนสแปมเมล์ในเดือน ก.ค.2551 ยังขยับตัวอยู่ระดับ 80% ที่ถือว่าคงที่ แต่ถ้าย้อนกลับไปดูเมื่อปี 2549 ที่ผ่านมาจำนวนอีเมล์ขยะขยับตัวสูงขึ้นเรื่อยๆ โดยเหล่าบรรดาสแปมเมอร์เปลี่ยนรูปแบบการโจมตี และวิธีล่อลวงแบบใหม่ จากผลสำรวจของไซแมนเทคพบว่า สแปมเมล์ประเภทการขโมยอีเมล์ส่วนตัว เพื่อส่งอีเมล์หลอกลวง และ อีเมล์ขยะประเภทภัยพิบัติจากแผ่นดินไหวในประเทศจีน หรือ สแปมบอทเพื่อล่าอีเมล์แอดเดรส และส่งสแปมเมล์สู่ผู้อื่นนั้นมีจำนวนมากในช่วงเดือนที่ผ่านมา ถ้าเหยื่อหลงเชื่อและตกหลุมพราง เว็บหลอกเหล่านี้ก็จะเก็บข้อมูลส่วนตัว และนำไปใช้ประโยชน์เพื่อการฉ้อฉลต่อไป

การขโมยอีเมล์ส่วนตัวเพื่อส่งอีเมลล่อลวง ที่เหล่าบรรดาสแปมเมอร์สร้างกลลวงโดยการขโมยบัญชีรายชื่ออีเมล์ส่วนตัว และข้อความหลอกลวงสู่บัญชีรายชื่อผู้ที่เราติดต่อ ที่อาจเป็นเพื่อน หรือเพื่อนร่วมงาน โดยข้อความในจดหมายนั้นส่วนมาก จะเป็นข้อความขอช่วยเหลือเรื่องการเงิน เจ้าของอีเมล์จะไม่สามารถล่วงรู้ถึงกลลวงนี้ หากเหยื่อตกหลุมพรางก็จะเก็บข้อมูลส่วนตัว และข้อมูลทางการเงิน และนำไปใช้ประโยชน์เพื่อการฉ้อฉลต่อไป

เหล่าบรรดาสแปมเมอร์ใช้เทคนิคที่เรียบง่ายในการเก็บเกี่ยวจากอีเมล์ เหล่าสแปมเมอร์ใช้กลยุทธ์หลากหลาย ในการเก็บรายชื่ออีเมล์เพื่อล่อลวงผู้รับ เช่น การใช้สแปมบอทเพื่อเก็บเกี่ยวรายชื่ออีเมล์ของบุคคลตามเว็บไซต์ต่างๆ หรือ การโจมตีอีเมล์เซิร์ฟเวอร์ที่เก็บอีเมล์แอดเดรส และเหล่าสแปมเมอร์จะเก็บอีเมล์ที่ไม่ตีกลับ หรือ การซื้ออีเมลแอดเดรสจากเหล่าบรรดาสแปมเมอร์รายอื่นๆ โดยจะนำอีเมล์แอดเดรสนำไปใช้ประโยชน์ในการฉ้อฉลต่อไป

อีเมล์ขยะประเภทการออกเดทสำหรับผู้ใหญ่ สแปมเมล์ประเภทการออกเดทสำหรับผู้ใหญ่ ที่ในอดีตจะส่งยูอาร์แอล เพื่อมาประชาสัมพันธ์เว็บไซต์ของการออกเดทสำหรับผู้ใหญ่ แต่เมื่อเร็วๆนี้ ไซแมนเทคได้สำรวจพบว่าอีเมล์ขยะประเภทการออกเดทสำหรับผู้ใหญ่ จะส่งข้อความเชิญชวนมา เพื่อให้ผู้รับค้นหาเว็บไซต์ในอินเทอร์เน็ตแทนการส่งยูอาร์แอลไปให้

อีเมล์ขยะประเภทภัยพิบัติจากแผ่นดินไหวในประเทศจีนถูกใช้เพื่อแพร่ไวรัส จากรายงานของไซแมนเทคพบการโจมตีจากสแปมเมล์ ประเภทภัยพิบัติจากแผ่นดินไหวในประเทศจีน ใช้เพื่อแพร่ไวรัส โดยหัวข้อที่ใช้ในการแพร่กระจายของอีเมล์คล้ายกับพาดหัวข่าว โดยหัวข้อในอีเมล์จะบอกเกี่ยวกับภัยคุกคามของมหกรรมกีฬาโอลิมปิค เนื่องจากภัยพิบัติแผ่นดินไหว หากเหยื่อสนใจและเปิดอ่านก็จะแพร่โทรจัน ที่มีชื่อว่า Trojan.Peacomm.D

กลโกงล็อตเตอรี่โอลิมปิกปรากฏเพื่อการฉ้อฉล จากรายงานสถานการณ์ของอีเมลขยะประจำเดือน มิ.ย.2551 ที่ผ่านมาไซแมนเทคสำรวจพบสแปมเมล์ประเภทล่อลวงการถูกรางวัลล็อตเตอรี่ จากมหกรรมกีฬาโอลิมปิกที่ปักกิ่ง ที่เหยื่อจะได้รับอีเมล์ถูกรางวัลจากล็อตเตอรี่ ของมหกรรมกีฬาโอลิมปิค ที่ปักกิ่ง และมีข้อปฏิบัติในการรับรางวัล โดยหากเหยื่อตกหลุมพรางก็จะเก็บข้อมูลส่วนตัว และข้อมูลทางการเงิน และนำไปใช้ประโยชน์เพื่อการฉ้อฉลต่อไป

อีเมล์ขยะมุ่งโจมตีตลาดมือถือในญี่ปุ่น สแปมเมล์ที่มุ่งโจมตีในมือถือไม่ใช้เรื่องที่ใหม่ แต่การส่งอีเมล์ผ่านมือถือเป็นสิ่งที่นิยมในหลายประเทศ โดยเฉพาะประเทศญี่ปุ่น โดยคงไม่แปลกที่ผู้ใช้มือถือจะตกเป็นกลุ่มเป้าหมายของการโจมตีจากเหล่าบรรดาสแปมเมอร์ โดยสแปมประเภทเสนอขายผลิตภัณฑ์โป๊เปลือย หรือเสนอบริการออกเดทสำหรับผู้ใหญ่ โดยประเภทของการโจมตีสแปมบนมือถือก็คล้ายกับสแปมเมล์ประเภทอื่นๆ และมีแนวโน้มสูงขึ้นเรื่อยๆ

อีเมล์ขยะประเภทรายงานข่าวกิจกรรมปลอมเพื่อล่อใจเหยื่อ อุปกรณ์ตรวจจับสแปมเมล์มีความซับซ้อนมากขึ้น แต่เหล่าบรรดาสแปมเมอร์ก็พัฒนาฝีมือในการโจมตีมากขึ้นเช่นกัน และเหล่าสแปมเมอร์ก็หันกลับมาใช้การโจมตีแบบเก่า โดยการส่งสแปมเมล์ที่มีการพาดหัวหลอกลวงเพื่อดึงดูดเหยื่อ และเชิญชวนให้เปิดอ่านสแปมเมล์ เช่น พาดหัวข่าวเรื่อง "ล่าสุด! โอบามาประกาศยุติการลงแข่งขันตำแหน่งประธานาธิบดีฯ" เหยื่อที่หลงกลก็จะเข้าไปดูตามลิงค์ที่ปรากฏในอีเมล์ จากนั้นแฮคเกอร์ก็จะเก็บข้อมูลส่วนตัว และนำไปใช้ประโยชน์เพื่อการฉ้อฉลต่อไป

ทั้งหมดที่นำเสนอมานี้ แม้จะดูเหมือนภัยคุกคามมีการพัฒนาเทคโนโลยี หรือกระบวนการต่างๆ และเจาะกลุ่มเป้าหมายที่หลากหลายมากขึ้น แต่สุดท้ายแล้วแนวคิด หรือ หลักในการโจมตีล่อลวง ก็ยังคงเป็นมุขโบราณที่มีมานานแล้ว และมุ่งหวังไปที่ข้อมูล และทรัพย์สินของเหยื่อเป็นสำคัญ ไม่ต่างจากการก่ออาชญากรรม ฉกชิงวิ่งราว หรือ ลักขโมยแต่อย่างใด สิ่งที่สำคัญ คือ เมื่อเกิดเหตุการณ์ขึ้นมา หรือ มีการแจ้งเตือนผู้ใช้งานตื่นตัว และสนใจมากแค่ไหน เพราะสิ่งที่จะช่วยได้มากที่สุด คือ การรู้เท่าทัน และมีความระมัดระวังไม่ตกเป็นเหยื่อ เพราะโจรย่อมเปลี่ยนวิธีการทำงานเสมอ แต่สิ่งที่ไม่เคยเปลี่ยนเลยนั่นคือ การมุ่งหวังทรัพย์สิน และข้อมูลจากเหยื่อนั่นเอง...

จุลดิส รัตนคำแปง

ที่มา : http://www.thairath.co.th/news.php?section=technology03a&content=99393