เทรนด์ ไมโครเผยรายงานด้านความปลอดภัยช่วงไตรมาสแรกปีนี้ พบสแปม, มือถือ, APT เป็นการโจมตีที่ได้รับนิยมสูงสุดในภูมิภาคเอเชียแปซิฟิก

บริษัท เทรนด์ ไมโคร อินคอร์ปอเรท (TYO: 4704; TSE: 4704) ผู้นำระดับโลกด้านการรักษาความปลอดภัย เปิดเผยรายงานด้านความปลอดภัยในภูมิภาคเอเชียแปซิฟิกประจำไตรมาสที่ 1 ปี 2555 พบว่า สแปม มือถือ และภัยคุกคามแบบต่อเนื่องขั้นสูง (Advanced Persistent Threats: APT) ถือเป็นความเสี่ยงด้านความปลอดภัยอันดับสูงสุด ขณะที่สื่อสังคมออนไลน์และช่องโหว่ต่างๆ ยังคงเป็นแหล่งสำคัญของการเกิดช่องโหว่และมัลแวร์อย่างไม่เปลี่ยนแปลง รายงานดังกล่าวได้ตั้งข้อสังเกตถึงการเปลี่ยนผ่านที่สำคัญจากการโจมตีในรูปแบบ “ลองผิดลองถูก” ที่อาชญากรไซเบอร์มักนำมาใช้งานกลายไปเป็นการโจมตีแบบมีเป้าหมายต่อเนื่องที่มีระยะเวลายาวนานมากขึ้นโดยอาศัยเทคนิควิศวกรรมสังคมและมัลแวร์เป็นเครื่องมือสำคัญ

ไมลา ปิลาโอ ผู้อำนวยการฝ่ายสื่อสารการตลาด ศูนย์วิจัยเทรนด์แล็บส์ กล่าวว่า “เอเชียเป็นแหล่งสแปมที่ใหญ่ที่สุดในโลก ทำให้เสี่ยงอย่างมากที่จะนำไปสู่ภัยคุกคามต่างๆ ในไตรมาสนี้เราพบหลักฐานสำคัญของการโจมตีที่เรียกว่าช่องโหว่หลุมดำ (lack hole exploit) ซึ่งใช้สแปมเป็นนกต่อ เราได้ตรวจสอบสแปมที่ดำเนินการโดยแอบอ้างชื่อของ Facebook, US Airways, USPS, CareerBuilder และอื่นๆ เพื่อล่อลวงผู้ใช้ให้เผลอคลิก จากนั้นก็จะเปลี่ยนเส้นทางนำเหยื่อไปยังหน้าเริ่มต้นที่มีชุดเครื่องมือช่องโหว่หลุมดำ (black hole exploit kits) ที่เป็นอันตรายซ่อนอยู่ สำหรับช่องโหว่ทั่วไปของ Adobe, Java, Windows และซอฟต์แวร์อื่นๆ นั้นยังคงถูกใช้ประโยชน์ในการปล่อยมัลแวร์และขโมยข้อมูลส่วนบุคคลเป็นหลัก”

“ขณะเดียวกันแนวโน้มภัยคุกคามระบบมือถือของภูมิภาคเอเชียก็ได้เปลี่ยนแปลงไปในลักษณะเดียวกับ สแปมเช่นกัน เฉพาะในไตรมาสนี้ เราสามารถระบุโปรแกรมที่เป็นอันตรายใหม่ๆ ของ *Android* ได้เกือบ 5,000 รายการ การพุ่งเป้าโจมตีระบบมือถือของอาชญากรไซเบอร์ได้เริ่มพัฒนาจากแนวทางลองผิดลองถูก (hit-and-miss) ไปเป็นแนวทางที่แข็งกร้าวยิ่งขึ้นโดยมีวัตถุประสงค์เพื่อดึงข้อมูลออกมาจากเหยื่อให้ได้” ปิลาโอกล่าวเพิ่มเติม

ความนิยมของสมาร์ทโฟนในการเชื่อมต่ออินเทอร์เน็ตและฐานผู้ใช้ *Android* ที่มีขนาดใหญ่ ทำให้การโจมตีแบบมีเป้าหมายที่มุ่งไปที่ Android OS เพิ่มจำนวนขึ้นอย่างไม่ต้องสงสัย มีการตรวจพบช่องโหว่ความปลอดภัยมากขึ้นในโปรแกรมมือถือที่ใช้งานปกติทั่วไป และโปรแกรมที่เป็นเครื่องมือสอดแนมยอดนิยมดังกล่าวติดอันดับในกลุ่มโปรแกรมที่เป็นอันตราย 17 โปรแกรมใน *Google Play* ที่มีผู้ดาวน์โหลดไปแล้วกว่า 700,000 ครั้งในขณะนี้

นอกจากนี้ การขยายตัวของปรากฏการณ์ที่เรียกว่า Bring Your Own Device (BYOD) หรือการนำอุปกรณ์ส่วนตัวของพนักงานเข้ามาใช้ในการทำงานยังส่งผลให้เกิดแนวโน้มที่ระบบมือถือจะเสี่ยงต่อความปลอดภัยมากขึ้นด้วย

ขณะที่ APT ยังคงเป็นแนวโน้มภัยคุกคามที่จะเกิดขึ้นอย่างต่อเนื่องในภูมิภาคเอเชียแปซิฟิก เช่นเดียวกับในส่วนอื่นๆ ของโลก “ตามที่คาดการณ์ไว้ การโจมตีแบบ APT จะยังคงเกิดขึ้นอย่างต่อเนื่องโดยมีเป้าหมายเป็นองค์กรธุรกิจต่างๆ ในเอเชีย สิ่งที่เราพบในขณะนี้คือการเปลี่ยนแปลงของเซิร์ฟเวอร์สั่งการและควบคุม (C&C) ที่โฮสต์จากผู้ให้บริการอินเทอร์เน็ตไปเป็นเครื่องทั่วไปที่ติดเชื้อมัลแวร์และมีความเกี่ยวข้องกับเป้าหมายดังกล่าว” ปิลาโอ กล่าวต่อว่า “เทคนิคนี้ทำให้การโจมตีแบบ APT ยากที่จะกรองและตรวจพบได้”

ภัยคุกคามในสื่อสังคมออนไลน์และช่องโหว่ต่างๆ จะยังคงเกิดขึ้นอย่างต่อเนื่อง แม้ว่าอาจยังไม่ได้พัฒนาจนทำให้เกิดความกังวลมากนัก อย่างไรก็ตาม จุดสำคัญที่สุดคือเทคนิควิศวกรรมสังคม ตัวอย่างเช่น การเสียชีวิตของวิทนีย์ ฮุสตัน และกรณีเหตุการณ์วุ่นวายทางสังคมและการเมืองต่างๆ ทำให้อาชญากรไซเบอร์มีข้อมูลในการแพร่กระจายเทคนิควิศวกรรมสังคมใหม่ๆ อยู่ตลอดเวลา จะเห็นได้ว่าการโจมตีและเผยแพร่ที่ทราบกันดีอยู่แล้วนี้เกิดขึ้นอย่างต่อเนื่องและใช้เวลายาวนานขึ้น และผู้ที่อยู่เบื้องหลังการโจมตีเหล่านี้จะใช้มัลแวร์ตัวเดียวกันแต่ในหลากหลายลักษณะและใช้การโจมตีใหม่ๆ ที่มุ่งไปยังเป้าหมายอย่างต่อเนื่องโดยใช้ประโยชน์จากเหตุการณ์ที่กำลังเป็นข่าวที่ได้รับความสนใจเพื่อล่อลวงเหยื่อให้เข้ามาติดกับ

โดยภาพรวมแล้ว ภัยคุกคามในภูมิภาคเอเชียแปซิฟิกที่ตรวจพบในไตรมาสที่หนึ่งไม่ได้แตกต่างจากไตรมาสก่อนหน้านี้มากนัก และจากภัยคุกคามทั้งสี่รูปแบบที่ตรวจพบในไตรมาสนี้ พบว่าการใช้งานมือถือที่แพร่หลายมากขึ้นทำให้ผู้ใช้ส่วนใหญ่ในเอเชียแปซิฟิกอาจพบกับความเสี่ยงด้านความปลอดภัยได้อย่างสูงสุด แม้ว่าองค์กรหลายแห่งก็ยังคงรู้สึกไม่สบายใจนักกับการนำเทคโนโลยีเข้ามาใช้ในธุรกิจ แต่ประเด็นด้านความปลอดภัยและการละเมิดข้อมูลในปี 2555 จะบังคับให้พวกเขาต้องพบกับปัญหาที่เกี่ยวข้องกับ BYOD โดยตรง

ในช่วงไตรมาสแรก เทรนด์ ไมโคร สมาร์ท โพรเท็คชั่น เน็ตเวิร์ค ซึ่งเป็นโครงสร้างการประมวลผลแบบคลาวด์ ได้ให้การปกป้องลูกค้าของบริษัท เทรนด์ ไมโคร ต่อสแปมไปแล้วทั้งสิ้น 15.3 พันล้านรายการ มัลแวร์ 338,400 รายการ และ URL ที่เป็นอันตรายอีก 1.3 พันล้านรายการ “มีแนวโน้มที่จะเกิดกรณีข้อมูลสูญหายมากขึ้นเรื่อยๆ ผ่านการติดมัลแวร์และการเจาะระบบในปี 2555 และอาชญากรไซเบอร์ยังพบวิธีหลบหลีกข้อกฎหมายต่างๆ ได้อีกด้วย แต่เทรนด์ ไมโคร ดีพ ซิเคียวริตี้ และเทรนด์ ไมโคร ดีพ ดิสคัฟเวอรี่ พร้อมให้การปกป้องเครือข่ายเสมือนและจัดการกับการโจมตีแบบ APT และด้วยสมาร์ท โพรเท็คชั่น เน็ตเวิร์ค ทำให้เราสามารถนำเสนอการรักษาความปลอดภัยรุ่นใหม่เพื่อป้องกันข้อมูลดิจิทัลได้โดยอัตโนมัติ ไม่ว่าผู้ใช้จะทำการเชื่อมต่อจากที่ใดก็ตาม” ปิลาโอกล่าวสรุป