เทรนด์ไมโครเผยรายงานความปลอดภัยไตรมาสที่ 2 ปี 2558 พบภัยคุกคามใหม่ๆ ต่อภาครัฐ

เทรนด์ไมโครเผยรายงานความปลอดภัยไตรมาสที่ 2 ปี 2558
พบภัยคุกคามใหม่ๆ ต่อภาครัฐ
– พบการโจมตีหน่วยงานภาครัฐ ระบบสาธารณูปโภคและภัยคุกคามแบบเจาะจงเป้าหมายอย่างกว้างขวาง –

กรุงเทพฯ, 05 ตุลาคม 2558 – ไตรมาสที่สองของปี 2558 เต็มไปด้วยปัญหาเรื่องช่องโหว่และการโจมตีระบบที่ซับซ้อน อาชญากรไซเบอร์ใช้วิธีโจมตีรูปแบบใหม่ๆ เพื่อแทรกซึมเข้าสู่เครือข่าย และใช้เทคโนโลยีที่มีอยู่ซึ่งมักจะถูกมองข้าม พัฒนาการเหล่านี้ได้รับการวิเคราะห์ในรายงานสรุปสถานการณ์ความปลอดภัยประจำไตรมาสที่ 2 ของ บริษัท เทรนด์ไมโคร (TYO: 4704; TSE: 4704) ที่ได้รับการตีพิมพ์เผยแพร่ภายใต้หัวข้อ “กระแสขาขึ้น: การเจาะระบบรูปแบบใหม่ๆ คุกคามเทคโนโลยีภาครัฐ” (“A Rising Tide: New Hacks Threaten Public Technologies”) รายงานดังกล่าวระบุรายละเอียดเกี่ยวกับวิวัฒนาการของเครื่องมือและวิธีการที่ผู้โจมตีใช้เพื่อให้ได้รับผลตอบแทนสูงสุดจากการลงทุนด้านอาชญากรรมไซเบอร์ในแต่ละครั้ง

“ในช่วงไตรมาสที่สอง เราพบการเปลี่ยนแปลงของสถานการณ์ภัยคุกคาม กล่าวคือ อาชญากรไซเบอร์มีความก้าวหน้ามากขึ้น มีการเปลี่ยนแปลงวิธีการโจมตี และใช้วิธีการโจมตีในรูปแบบใหม่ๆ ” ไรมันด์ จีนส์ ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยีของเทรนด์ไมโคร กล่าว “เราควรจะตื่นตัวเรื่องภัยคุกคามของอาชญากรรมไซเบอร์ให้มากขึ้น เพราะสถานการณ์ในช่วงไตรมาสที่ผ่านมาแสดงให้เห็นว่าความเสียหายที่อาจเกิดจากการโจมตีทางไซเบอร์ขยายวงกว้างเกินกว่าแค่การพบซอฟต์แวร์บั๊กทั่วไปที่สามารถ เข้าถึงการแฮ็กระบบเครื่องบิน ระบบรถยนต์อัจฉริยะ และสถานีโทรทัศน์”

แฮ็กเกอร์ใช้แนวทางเชิงกลยุทธ์มากขึ้น มีการปรับปรุงรูปแบบและเจาะกลุ่มเป้าหมายอย่างเฉพาะเจาะจง เพื่อปรับปรุงอัตราการแพร่กระจายของไวรัส ทั้งนี้มีการใช้วิธีการโจมตีหลายๆ วิธีเพิ่มมากขึ้น รวมถึงการใช้ชุดเครื่องมือ Angler สำหรับการเจาะระบบเพิ่มขึ้น 50% และการเติบโต 67% ในส่วนของภัยคุกคามที่เกี่ยวข้องกับชุดเครื่องมือการเจาะระบบโดยรวม ขณะที่มัลแวร์เรียกค่าไถ่ CryptoWall ransomware มีการเจาะจงเป้าหมายมากขึ้นโดยเกิดขึ้นในสหรัฐฯ 79%

นอกจากนี้ หน่วยงานภาครัฐตระหนักถึงผลกระทบของการโจมตีทางไซเบอร์ในช่วงไตรมาสที่สอง ที่เกิดปัญหาข้อมูลรั่วไหลอย่างกว้างขวางบนระบบของหน่วยงานสรรพากร (Internal Revenue Service – IRS) ในช่วงเดือน

พฤษภาคม และระบบของสำนักงานบริหารงานบุคคลสหรัฐอเมริกา (U.S. Office of Personnel Management – OPM) เมื่อเดือนมิถุนายน ปัญหาข้อมูลรั่วไหลของ OPM ส่งผลให้มีการเปิดเผยข้อมูลที่ระบุตัวบุคคลของประชาชนราว 21 ล้านคน หน่วยงานภาครัฐอื่นๆ ได้รับผลกระทบจากการโจมตีแบบเจาะจงเป้าหมาย โดยใช้มัลแวร์ที่เป็นมาโคร เซิร์ฟเวอร์ใหม่ๆ สำหรับการสั่งการและควบคุม (Command and Control – C&C) และการใช้งานอย่างต่อเนื่องสำหรับช่องโหว่และ Pawn Storm ใหม่ๆ

เมื่อตรวจสอบสถานการณ์ภัยคุกคามในช่วงไตรมาสที่ 2 สหรัฐฯ มีบทบาทสำคัญทั้งในแง่ของการปรับใช้และการถูกโจมตีด้วยลิงค์อันตราย สแปม เซิร์ฟเวอร์ C&C และมัลแวร์เรียกค่าไถ่ โดยทั้งหมดนี้ปรากฏให้เห็นอย่างกว้างขวาง

ประเด็นสำคัญที่ระบุในรายงานมีดังนี้:

 การแฮ็กระบบที่อาจส่งผลให้ระบบสาธารณูปโภคหยุดชะงัก

เครือข่ายสถานีโทรทัศน์ เครื่องบิน ระบบรถยนต์อัตโนมัติ และเราเตอร์ภายในบ้าน เสี่ยงต่อการแพร่กระจายของมัลแวร์ รวมถึงภัยคุกคาม และการทำงานหยุดชะงัก

 อาชญากรไซเบอร์ที่ทำงานคนเดียวจะประสบความสำเร็จในการใช้มัลแวร์เรียกค่าไถ่และการโจมตี PoS FighterPoS และ MalumPoS ซึ่งถูกใช้งานโดยแฮ็กเกอร์ที่ทำงานเพียงคนเดียว เช่น “Lordfenix” และ “Frapstar” รวมถึงการโจมตีด้วยโปรแกรมดักจับข้อมูลการกดคีย์บอร์ด Hawkeye keylogger ทั้งหมดนี้แสดงให้เห็นว่าแฮ็กเกอร์เพียงคนเดียวก็สามารถสร้างความวุ่นวายให้กับตลาดได้เป็นอย่างมาก

 หน่วยงานภาครัฐต่อสู้กับอาชญากรรมไซเบอร์

หน่วยงานตำรวจสากล (Interpol), ตำรวจยุโรป (Europol), กระทรวงความมั่นคงแห่งมาตุภูมิ และหน่วยงาน FBI ของสหรัฐฯ ทั้งหมดนี้มีบทบาทสำคัญในการปราบปรามการใช้บ็อตเน็ตที่มีมาอย่างยาวนาน นอกจากนี้ การที่รอส อุลบริคท์ ผู้ก่อตั้งตลาดมืด Silk Road ถูกตัดสินว่ามีความผิด แสดงให้เห็นถึงความคลุมเครือและอันตรายของมุมมืดบนอินเทอร์เน็ต หรือ Dark Web

 การโจมตีหน่วยงานภาครัฐก่อให้เกิดผลกระทบต่อประเทศและการเมือง

การโจมตีหน่วยงาน OPM นับเป็นเหตุการณ์ที่น่าตกใจ เพราะทำให้เรารู้ว่าไม่มีข้อมูลส่วนตัวของใครเลยที่จะปลอดภัย มัลแวร์ที่ใช้มาโคร การโจมตีทางอ้อมผ่านองค์กรอื่น (island-hopping) และเซิร์ฟเวอร์ C&C เป็นส่วนหนึ่งของยุทธวิธีที่ใช้เพื่อโจรกรรมข้อมูลจากภาครัฐ

 เว็บไซต์ที่ให้บริการแก่ประชาชนและอุปกรณ์พกพาถูกคุกคามในรูปแบบใหม่ๆ

ขณะที่ภัยคุกคามต่อซอฟต์แวร์ยังคงมีอยู่ ช่องโหว่ในเว็บแอพจึงมีอันตรายไม่ยิ่งหย่อนไปกว่ากัน โดยผู้โจมตีจะใช้ช่องโหว่ที่มีอยู่ และดังนั้นจึงจำเป็นที่จะต้องตรวจสอบความปลอดภัยของแอพพลิเคชั่นแบบกำหนดเอง เพื่อให้แน่ใจว่าช่องโหว่เหล่านั้นได้ถูกกำจัด

รายงานฉบับเต็มมีอยู่ที่:
http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/a-rising-tide-new-hacks-threaten-public-technologies

บล็อกโพสต์เกี่ยวกับรายงานนี้มีอยู่ที่นี่:
http://blog.trendmicro.com/a-rising-tide-new-hacks-threaten-public-technologies/

เกี่ยวกับเทรนด์ ไมโคร

บริษัท เทรนด์ ไมโคร ผู้นำระดับโลกในด้านซอฟต์แวร์ความปลอดภัย มุ่งมั่นที่จะสร้างโลกที่ปลอดภัยสำหรับการแลกเปลี่ยนข้อมูลดิจิตอล จากประสบการณ์มากกว่า 25 ปีของเรา โซลูชั่นของเราได้ให้บริการทั้งสำหรับผู้ใช้ทั่วไป องค์กรธุรกิจ และหน่วยงานภาครัฐ โดยนำเสนอระบบรักษาความปลอดภัยในการปกป้องข้อมูลแบบแบ่งระดับชั้น [Layered content security] ในอุปกรณ์พกพา อุปกรณ์ลูกข่าย เกตเวย์ เซิร์ฟเวอร์ และระบบคลาวด์ โซลูชั่นทั้งหมดของเราขับเคลื่อนด้วย Trend Micro™ Smart Protection Network™ ซึ่งเป็นเครือข่ายข้อมูลเกี่ยวกับภัยคุกคามทั่วโลกบนระบบคลาวด์ พร้อมการสนับสนุนจากผู้เชี่ยวชาญด้านภัยคุกคามกว่า 1,200 คนทั่วโลก ดูข้อมูลเพิ่มเติมได้ที่ www.trendmicro.co.th
##############################

ติดต่อข้อมูลประชาสัมพันธ์

จารุวรรณ ฤกษ์พิชญโยธิน

บริษัท เทรนด์ไมโคร (ประเทศไทย) จำกัด
+662 646 1968,
jaruwan_r@trendmicro.com

วราวอง จงรักษ์

ดุษฎี เย็นสุดใจ

บริษัท เอฟเอคิว จำกัด: +662 971 3700
Trendmicrothpr@faq.co.th