เทรนด์ไมโครเผยรายงานความปลอดภัยครึ่งปีแรก แสดงวิวัฒนาการของมัลแวร์เรียกค่าไถ่

เทรนด์ไมโครเผยรายงานความปลอดภัยครึ่งปีแรก
แสดงวิวัฒนาการของมัลแวร์เรียกค่าไถ่และอีเมลหลอกโอนเงิน

กรุงเทพฯ, 16 กันยายน 2559 – ตามที่เทรนด์ไมโครได้คาดการณ์ไว้ว่า ในช่วงปี 2559 จะมีการขู่กรรโชกทางออนไลน์เกิดขึ้นมากมายผ่านวิธีการโจมตีที่หลากหลาย ล่าสุด บริษัท เทรนด์ไมโคร (TYO: 4704; TSE: 4704) ผู้นำระดับโลกด้านซอฟต์แวร์และโซลูชั่นการรักษาความปลอดภัย ได้เผยแพร่รายงานสรุปสถานการณ์ความปลอดภัยที่มีชื่อว่า “ยุคมัลแวร์เรียกค่าไถ่ครองเมือง” (“The Reign of Ransomware”) ซึ่งวิเคราะห์แนวโน้มการโจมตีและช่องโหว่ที่ตรวจพบในช่วงครึ่งแรกของปีนี้ ในรายงานได้ให้ข้อมูลโดยละเอียดเกี่ยวกับการเพิ่มขึ้นและผลกระทบของการโจมตี เช่น การเพิ่มขึ้น 172% ของมัลแวร์เรียกค่าไถ่ และความเสียหายมูลค่า 3 พันล้านดอลลาร์จากอีเมลหลอกให้โอนเงินที่ส่งถึงฝ่ายการเงินของบริษัทต่างๆ (Business Email Compromise – BEC) ในช่วงครึ่งแรกของปี 2559 รวมถึงช่องโหว่ที่ตรวจพบเกือบ 500 ช่องโหว่ในผลิตภัณฑ์ต่างๆ

“มัลแวร์เรียกค่าไถ่ (Ransomware) ทำให้องค์กรที่ตกเป็นเหยื่อประสบปัญหาการดำเนินงานหยุดชะงัก และอาชญากรไซเบอร์ที่ใช้วิธีการโจมตีแบบนี้ก็กำลังดำเนินการพัฒนาอย่างต่อเนื่องเพื่อหลบหลีกการตรวจจับขององค์กรต่างๆ” นายไรมันด์ จีนส์ ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยีของเทรนด์ไมโคร กล่าว “ในช่วงครึ่งแรกของปี 2559 มัลแวร์เรียกค่าไถ่มีบทบาทมากที่สุดในสถานการณ์ภัยคุกคาม โดยก่อให้เกิดความเสียหายมูลค่ามหาศาลต่อองค์กรธุรกิจในหลากหลายกลุ่มอุตสาหกรรม องค์กรจะต้องปรับใช้โซลูชั่นการรักษาความปลอดภัยแบบหลายเลเยอร์ (multi-layered security solutions) เพื่อต่อสู้กับภัยคุกคามเหล่านี้ ซึ่งอาจพยายามแทรกซึมเข้าสู่เครือข่ายขององค์กรได้ทุกเมื่อ”

ข้อมูลในรายงานเน้นย้ำถึงปัญหาสำคัญด้านความปลอดภัยในช่วงครึ่งแรกของปี 2559:

 มัลแวร์เรียกค่าไถ่ครอบงำสถานการณ์ภัยคุกคาม: มัลแวร์เรียกค่าไถ่มีจำนวนเพิ่มขึ้นถึง 172% ในช่วงครึ่งแรกของปี 2559 เมื่อเทียบกับปี 2558 ส่งผลให้มัลแวร์เรียกค่าไถ่กลายเป็นภัยคุกคามที่แพร่หลาย โดยมัลแวร์เรียกค่าไถ่ชนิดต่างๆ ได้รับการออกแบบมาเพื่อโจมตีเครือข่ายทุกระดับ

 อีเมลหลอกลวง BEC แพร่กระจายทั่วโลก: หน่วยงานเอฟบีไอระบุว่า ตั้งแต่ต้นปี 2559 จนถึงปัจจุบัน มีเหยื่อ

มากกว่า 22,000 ราย และมูลค่าความเสียหายมากกว่า 3 พันล้านดอลลาร์ เทรนด์ไมโครพบว่า สหรัฐฯ เป็นประเทศที่ตกเป็นเป้าหมายมากที่สุดสำหรับการโจมตีเหล่านี้

 ช่องโหว่และมัลแวร์เรียกค่าไถ่ใหม่ๆ โจมตีผ่านชุดเครื่องมือเจาะระบบ: จำนวนการใช้งานชุดเครื่องมือเจาะระบบ Angler ลดลงหลังจากมีการจับกุมอาชญากรไซเบอร์ 50 ราย อย่างไรก็ดี ภายหลังการจับกุม มีการเปลี่ยนไปใช้ชุดเครื่องมืออื่นๆ เช่น Rig และ Sundown

 จำนวนช่องโหว่ที่พบในแพลตฟอร์ม Adobe Flash และ IoT เพิ่มขึ้นอย่างต่อเนื่อง: เทรนด์ไมโคร และ ZDI รายงานเกี่ยวกับช่องโหว่สำคัญๆ ในเบราว์เซอร์และช่องโหว่เคอร์เนล ซึ่งถูกระบุระหว่างการแข่งขัน Pwn2Own

 ปัญหาข้อมูลรั่วไหลสร้างความเสียหายต่อหลายกลุ่มอุตสาหกรรม: ทั้งภาครัฐและภาคเอกชนตกเป็นเหยื่อของการเจาะข้อมูลในช่วงครึ่งแรกของปีนี้ รวมถึง Myspace และ Verizon โรงพยาบาลและหน่วยงานภาครัฐหลายแห่ง

 มัลแวร์เครื่องคิดเงินรุ่นอัพเดต (Point-of-Sale malware) ก่อให้เกิดการโจมตีใหม่ๆ: FastPoS สามารถโจรกรรมข้อมูลบัตรเครดิตได้อย่างมีประสิทธิภาพ ส่งผลกระทบต่อองค์กรธุรกิจขนาดกลางและขนาดเล็กทั่วโลก รวมไปถึงองค์กรในสหรัฐฯ นอกจากนี้ FighterPoS ได้ทำการเปิดตัวซึ่งแสดงให้เห็นถึงคุณสมบัติคล้ายกับเวิร์ม จึงสามารถติดเชื้อข้ามเครือข่ายได้

 มัลแวร์หันมาใช้ช่องโหว่เก่าในการโจมตี: การโจมตีช่องโหว่ Shellshock มีจำนวนเพิ่มขึ้นในช่วงครึ่งแรกของปีนี้ แม้ว่าจะมีการเผยแพร่แพตช์สำหรับแก้ไขจุดบกพร่องของระบบแล้วก็ตาม โดยมีการตรวจพบช่องโหว่ใหม่ๆ หลายพันช่องโหว่ในแต่ละเดือน นี่เป็นอีกหนึ่งตัวอย่างที่แสดงให้เห็นถึงประโยชน์ของการติดตั้งแพตช์แบบเสมือน (Virtual Patching) ซึ่งช่วยเพิ่มความรวดเร็วในการปกป้องเครือข่ายขององค์กรเมื่อตรวจพบช่องโหว่
 อาชญากรไซเบอร์ทำลายขีดจำกัดด้วยโทรจันสำหรับโจมตีระบบธนาคารโดยเฉพาะ:
โทรจันอย่างเช่น QAKBOT เพิ่มการโจมตีภายหลังการจับกุมผู้สร้าง DYRE โทรจันดังกล่าวมีเป้าหมายที่จะโจรกรรมข้อมูลสำคัญๆ เช่น ข้อมูลธนาคาร พฤติกรรมการท่องเว็บ และข้อมูลสำคัญอื่นๆ ของผู้ใช้

โดยรวมแล้ว มีการตรวจพบมัลแวร์เรียกค่าไถ่ชนิดใหม่ 79 ชนิดในช่วง 6 เดือนแรกของปีนี้ แซงหน้าจำนวนมัลแวร์เรียกค่าไถ่ชนิดใหม่ที่ตรวจพบตลอดปี 2558 มัลแวร์ทั้งชนิดใหม่และชนิดเก่าได้สร้างความเสียหายต่อองค์กรต่างๆ รวมเป็นมูลค่า 209 ล้านดอลลาร์ การโจมตีด้วยมัลแวร์เรียกค่าไถ่ที่พบในช่วงครึ่งแรกของปี 2559 รวมถึงการหลอกลวงแบบ BEC ใช้อีเมลเป็นช่องทางมากถึง 58 เปอร์เซ็นต์

ผลการศึกษาชี้ให้เห็นว่าช่องโหว่และชุดเครื่องมือเจาะระบบมีจำนวนเพิ่มขึ้นและมีการพัฒนาอย่างต่อเนื่อง ทั้งนี้พบว่า Angler ถูกใช้งานลดลงอย่างต่อเนื่อง ขณะที่ชุดเครื่องมือเจาะระบบอื่นๆ เช่น Neutrino ได้รับความนิยมเพิ่มมากขึ้น และมีการเพิ่มเติมช่องโหว่และมัลแวร์เรียกค่าไถ่ใหม่ๆ เพื่อให้ชุดเครื่องมือเจาะระบบมีความทันสมัยและเปี่ยมประสิทธิภาพ ซอฟต์แวร์ที่ไม่ได้ติดตั้งแพตช์ยังคงเปิดโอกาสให้ผู้โจมตีส่งมัลแวร์เข้าสู่เครือข่ายผ่านทางชุด

เครื่องมือเจาะระบบ

ในช่วงครึ่งแรกของปี 2559 เทรนด์ไมโครตรวจพบช่องโหว่ 473 ช่องโหว่ในผลิตภัณฑ์ที่หลากหลาย โดย 28 ช่องโหว่มาจาก Adobe Flash และ 108 ช่องโหว่มาจาก Web Access ของ Advantech ซึ่งแสดงให้เห็นถึงศักยภาพที่เต็มเปี่ยมของทีมงานฝ่ายวิจัยของบริษัทฯ

“อาชญากรไซเบอร์มีความตื่นตัวและยืดหยุ่นในเรื่องของการปรับเปลี่ยนวิธีการโจมตีในแต่ละครั้งที่เราค้นพบวิธีแก้ปัญหาหรือติดตั้งแพตช์สำหรับแก้ไขจุดบกพร่องของระบบ” นายเอ็ด คาเบรร่า ประธานเจ้าหน้าที่ฝ่ายไซเบอร์ซีเคียวริตี้ของเทรนด์ไมโคร กล่าว “สถานการณ์เช่นนี้ก่อให้เกิดปัญหามากมายต่อองค์กรและผู้ใช้ทั่วไป เพราะภัยคุกคามมีการเปลี่ยนแปลงบ่อยครั้งจนยากที่จะแก้ไขปัญหาได้อย่างทันท่วงที ด้วยเหตุนี้ องค์กรธุรกิจจึงจำเป็นที่จะต้องเตรียมพร้อมล่วงหน้าเพื่อรับมือกับการโจมตีที่อาจเกิดขึ้นไม่ช้าก็เร็ว โดยจะต้องติดตั้งโซลูชั่นการรักษาความปลอดภัยรุ่นใหม่ล่าสุด ดำเนินการติดตั้งแพตช์แบบเสมือน และให้ความรู้แก่พนักงานเพื่อป้องกันความเสี่ยงอย่างรอบด้าน”

สำหรับรายงานฉบับสมบูรณ์ โปรดดูที่:
http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/the-reign-of-ransomware

เกี่ยวกับเทรนด์ไมโคร
เทรนด์ไมโคร อินคอร์ปอเรทเต็ด ผู้นำระดับโลกด้านโซลูชั่นความปลอดภัยไซเบอร์ มุ่งมั่นที่จะช่วยให้การแลกเปลี่ยนข้อมูลดิจิทัลในโลกของเราเป็นไปอย่างปลอดภัย เทรนด์ไมโครมีโซลูชั่นที่ให้บริการผู้ใช้ทั่วไป องค์กรธุรกิจ และหน่วยงานภาครัฐ โดยนำเสนอระบบรักษาความปลอดภัยหลายระดับให้กับดาต้าเซ็นเตอร์, คลาวด์, เน็ตเวิร์ค และเครื่องลูกข่าย ผลิตภัณฑ์และโซลูชั่นทั้งหมดของเทรนด์ไมโครผสานการทำงานร่วมกันเพื่อให้ข้อมูลเชิงลึกเกี่ยวกับการป้องกันภัยคุกคามอย่างชาญฉลาด และสร้างการป้องกันภัยคุกคามที่เกี่ยวโยงกันหลายส่วน ด้วยการควบคุมและแสดงผลแบบรวมศูนย์ ซึ่งช่วยให้สามารถป้องกันภัยคุกคามได้อย่างรวดเร็วและมีประสิทธิภาพมากขึ้น

เทรนด์ไมโครมีพนักงานมากกว่า 5,000 คนในกว่า 50 ประเทศ มีผลิตภัณฑ์ โซลูชั่น และความเชี่ยวชาญในการป้องกันภัยคุกคามที่ทันสมัยที่สุดในโลก เราช่วยให้องค์กรต่างๆ เดินทางสู่การใช้งานระบบคลาวด์ได้อย่างปลอดภัย ดูข้อมูลเพิ่มเติมได้ที่ www.trendmicro.co.th , www.trendmicro.com

###

ติดต่อข้อมูลประชาสัมพันธ์
จารุวรรณ ฤกษ์พิชญโยธิน
บริษัท เทรนด์ไมโคร (ประเทศไทย) จำกัด
+662 646 1968
jaruwan_r@trendmicro.com

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