NTT Security เผยรายงานวิเคราะห์แนวโน้มภัยคุกคามทางไซเบอร์ทั่วโลกประจำปี 2560

รายงานระบุว่า 77% ของแรนซัมแวร์ทั้งหมดพบใน 4 ภาคส่วนสำคัญ ได้แก่ บริการธุรกิจและวิชาชีพ รัฐบาล บริการสุขภาพ และการค้าปลีก ขณะที่สามในสี่ของมัลแวร์ทั้งหมดมาจากการโจมตีแบบฟิชชิง

NTT Security บริษัทซึ่งเชี่ยวชาญด้านความปลอดภัยในเครือ NTT Group ได้เผยแพร่รายงาน Global Threat Intelligence Report (GTIR) ประจำปี 2560 ซึ่งวิเคราะห์แนวโน้มของภัยคุกคามทางไซเบอร์ทั่วโลก โดยพิจารณาจากข้อมูลล็อก กิจกรรม การโจมตี เหตุการณ์ และช่องโหว่ (ระหว่างวันที่ 1 ตุลาคม 2558 ถึง 31 กันยายน 2559) ทั้งนี้ ข้อมูลวิเคราะห์จากบริษัทในเครือ NTT Group อันประกอบด้วย NTT Security, Dimension Data, NTT Communications และ NTT Data รวมถึงข้อมูลจาก Global Threat Intelligence Center (GTIC) หรือเดิมรู้จักในชื่อ SERT จะช่วยตีแผ่แนวโน้มล่าสุดของการโจมตีด้วยแรนซัมแวร์ ฟิชชิง และ DDoS ตลอดจนเผยผลกระทบของภัยคุกคามเหล่านี้ที่มีต่อองค์กรทั่วโลก

ปัจจุบัน ฟิชชิงถูกใช้เป็นเครื่องมือหลักในการแพร่กระจายแรนซัมแวร์ ซึ่งเป็นมัลแวร์ที่สามารถยึดข้อมูลหรืออุปกรณ์เป็นตัวประกัน รายงานฉบับนี้เผยให้เห็นว่า 77% ของแรนซัมแวร์ที่พบทั่วโลกกระจายอยู่ใน 4 ภาคส่วนสำคัญ ได้แก่ บริการธุรกิจและวิชาชีพ (28%) รัฐบาล (19%) บริการสุขภาพ (15%) และการค้าปลีก (15%)

แม้สื่อจะให้ความสนใจกับการโจมตีช่องโหว่ใหม่ๆ โดยใช้วิธีทางเทคนิค แต่แท้จริงแล้วการโจมตีจำนวนมากกลับอาศัยเทคนิคน้อยลง โดยรายงานระบุว่า เกือบสามในสี่ (73%) ของมัลแวร์ทั้งหมดที่พบในองค์กร มาจากการโจมตีแบบฟิชชิง ขณะที่หน่วยงานรัฐบาล (65%) รวมถึงบริการธุรกิจและวิชาชีพ (25%) เป็นภาคส่วนที่มีแนวโน้มถูกโจมตีมากที่สุดในภาพรวมทั่วโลก ส่วนประเทศที่เป็นต้นทางการโจมตีแบบฟิชชิงที่ใหญ่ที่สุดประกอบด้วยสหรัฐอเมริกา (41%) เนเธอร์แลนด์ (38%) และฝรั่งเศส (5%)

รายงานยังเผยด้วยว่า รหัสผ่าน 25 ชุด คิดเป็นสัดส่วนเกือบ 33% ของความพยายามยืนยันตัวตนเพื่อเข้าระบบเซิร์ฟเวอร์ลวง (ฮันนีพ็อต) ของ NTT Security ในปีที่แล้ว ขณะเดียวกัน กว่า 76% ของความพยายามในการเข้าระบบ มีการใช้รหัสผ่านที่ใช้ใน Mirai Botnet ซึ่งเป็นบ็อทเน็ตที่พุ่งเป้าไปยังอุปกรณ์ IoT และในอดีตเคยถูกนำมาใช้ในการโจมตี DDoS ครั้งใหญ่ที่สุด ณ ขณะนั้น

การโจมตีแบบ DDoS มีสัดส่วนไม่ถึง 6% ของการโจมตีทั่วโลก ทว่าคิดเป็นสัดส่วนกว่า 16% ของการโจมตีทั้งหมดจากเอเชีย และ 23% ของการโจมตีทั้งหมดจากออสเตรเลีย

ภาคการเงินถือเป็นภาคส่วนที่ถูกโจมตีบ่อยครั้งที่สุดทั่วโลก คิดเป็น 14% ของการโจมตีทั้งหมด และเป็นภาคส่วนเดียวที่ติด 3 อันดับแรกในทุกภูมิภาคที่มีการวิเคราะห์ ส่วนภาคการผลิตติด 3 อันดับแรกใน 5 ภูมิภาค จากทั้งหมด 6 ภูมิภาค ทั้งนี้ เมื่อพิจารณาในภาพรวม ภาคการเงิน (14%) รัฐบาล (14%) และภาคการผลิต (13%) ถือเป็น 3 ภาคส่วนที่ถูกโจมตีบ่อยที่สุด

สตีเวน บูลลิตต์ รองประธานฝ่าย Threat Intelligence & Incident Response ของศูนย์ GTIC ในเครือ NTT Security กล่าวว่า “GTIR ถือเป็นรายงานที่ครอบคลุมมากที่สุดในบรรดารายงานประเภทเดียวกัน เพราะมีการวิเคราะห์ข้อมูลล็อกรักษาความปลอดภัยนับล้านล้านล็อกตลอดปีที่ผ่านมา เราตรวจพบความพยายามในการโจมตีมากกว่า 6 พันล้านครั้งภายในระยะเวลา 12 เดือน หรือราว 16 ล้านครั้งต่อวัน และตรวจพบการโจมตีแทบทุกรูปแบบ นอกจากนี้ เรายังช่วยเหลือองค์กรต่างๆ ในการตรวจสอบการล้วงข้อมูล รวบรวมและวิเคราะห์ข้อมูลเชิงลึกเกี่ยวกับภัยคุกคามทั่วโลก ตลอดจนทำการวิจัยด้านความปลอดภัยด้วยตัวเอง สิ่งที่เราได้จากความพยายามทั้งหมดนี้ได้ถูกสะท้อนผ่านข้อเสนอแนะต่างๆ ในรายงานฉบับนี้”

“เราไม่ได้มีเจตนาที่จะสร้างความหวาดกลัว ความไม่แน่นอน และความกังขา หรือทำให้สถานการณ์ยุ่งยากขึ้นไปอีก เราเพียงต้องการสร้างระบบรักษาความปลอดภัยทางไซเบอร์ที่มีความน่าสนใจและครอบคลุมสำหรับทุกคนที่ต้องเผชิญกับความท้าทายจากภัยคุกคาม ไม่ใช่แค่ผู้เชี่ยวชาญด้านการรักษาความปลอดภัยเพียงกลุ่มเดียว เราต้องการให้ทุกคนได้รับความรู้เกี่ยวกับปัญหาเหล่านี้ และตระหนักว่าแต่ละคนมีความรับผิดชอบในการร่วมกันป้องกันองค์กรของตน ขณะที่องค์กรก็มีหน้าที่สนับสนุนบุคลากรในการดำเนินการดังกล่าวเช่นกัน”

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับภัยคุกคามสำคัญๆ รวมถึงวิธีที่ผู้บริหาร เจ้าหน้าที่เทคนิค และยูสเซอร์สามารถยกระดับความปลอดภัยภายในองค์กร สามารถดูได้ในรายงาน GTIR ประจำปี 2560 ของ NTT Security ที่ http://www.nttsecurity.com/GTIR2017

สรุปผลการค้นพบที่สำคัญ

– ประเทศที่เป็นต้นทางของภัยคุกคามทางไซเบอร์มากที่สุด ได้แก่ สหรัฐอเมริกา (63%) สหราชอาณาจักร (4%) จีน (3%)
– องค์กรที่มีแผนการรับมือกับการโจมตีทางไซเบอร์เพิ่มขึ้นจากเฉลี่ย 23% ในปีที่แล้ว เป็น 32% ในปีนี้
– 59% ของการโจมตีทั้งหมดเกิดขึ้นใน 4 ภาคส่วน ได้แก่ บริการสุขภาพ (17%) การเงิน (16%) บริการธุรกิจและวิชาชีพ (14%) และการค้าปลีก (12%)
– กว่า 60% ของการโจมตีทางไซเบอร์เป็นการโจมตีแบบฟิชชิง
– การโจมตีจากแรนซัมแวร์เป็นการโจมตีที่เกิดขึ้นบ่อยที่สุด (22%)
– 56% ของภัยคุกคามที่เกิดขึ้นในองค์กรการเงินเป็นการโจมตีจากมัลแวร์
– 50% ของภัยคุกคามที่เกิดขึ้นในองค์กรด้านสุขภาพเป็นการโจมตีจากแรนซัมแวร์

NTT Security เข้าถึงข้อมูลการใช้งานอินเทอร์เน็ตราว 40% ของทั้งหมดทั่วโลก จึงสามารถสรุปข้อมูลจากล็อกกว่า 3.5 ล้านล้านล็อก และการโจมตี 6.2 พันล้านครั้ง ไว้ในรายงาน Global Threat Intelligence Report (GTIR) ประจำปี 2560 โดยอาศัยการวิเคราะห์ข้อมูลล็อก กิจกรรม การโจมตี เหตุการณ์ และช่องโหว่ ร่วมกับรายละเอียดจากแหล่งข้อมูลวิจัยของ NTT Security ซึ่งรวมถึงฮันนีพ็อตและแซนด์บ็อกซ์ที่กระจายอยู่ในกว่า 100 ประเทศ ในสภาพที่เป็นอิสระจากโครงสร้างพื้นฐานสถาบัน

NTT Security เป็นบริษัทซึ่งเชี่ยวชาญด้านความปลอดภัยในเครือ NTT Group ระบบรักษาความปลอดภัยแบบฝังของเราช่วยให้กลุ่มบริษัทในเครือ (Dimension Data, NTT Communications และ NTT Data) สามารถนำเสนอโซลูชั่นทางธุรกิจที่ยืดหยุ่นเพื่อตอบสนองความต้องการของลูกค้าในการเปลี่ยนผ่านสู่ระบบดิจิทัล NTT Security มีศูนย์ SOC จำนวน 10 แห่ง ศูนย์วิจัยและพัฒนา 7 แห่ง รวมถึงผู้เชี่ยวชาญอีกกว่า 1,500 คน ที่คอยรับมือกับเหตุการณ์ด้านความปลอดภัยหลายแสนครั้งในแต่ละปีในทั่วทั้ง 6 ทวีป

NTT Security ใช้ทรัพยากรที่มีอย่างเต็มประสิทธิภาพ ด้วยการผสานบริการให้คำปรึกษาและบริการด้านการจัดการอย่างลงตัว โดยใช้ทรัพยากรในท้องถิ่นและศักยภาพระดับโลกให้เกิดประโยชน์สูงสุด ทั้งนี้ NTT Security เป็นส่วนหนึ่งของ NTT Group (Nippon Telegraph and Telephone Corporation) หนึ่งในบริษัทเทคโนโลยีสารสนเทศและการสื่อสาร (ไอซีที) รายใหญ่ที่สุดในโลก สามารถรับชมข้อมูลเพิ่มเติมได้ที่ nttsecurity.com

ติดต่อ: Paula Averley, paula@origincomms.com , +44(0)7766-257776

ที่มา: NTT Security