ซิสโก้เผยรายงานกลางปีไซเบอร์ซีเคียวริตี้ 2559 คาด “มัลแวร์เรียกค่าไถ่รุ่นอนาคต” (Next-Gen Ransomware)

ซิสโก้เผยรายงานกลางปีไซเบอร์ซีเคียวริตี้ 2559 คาด “มัลแวร์เรียกค่าไถ่รุ่นอนาคต” (Next-Gen Ransomware) จะใช้วิธีการใหม่ๆ สร้างรายได้มากขึ้น

ซิสโก้ขึ้นแท่นผู้นำการตรวจจับภัยคุกคามได้เร็วที่สุดด้วยสถิติใหม่โดยใช้เวลาเพียง 13 ชั่วโมง แนะองค์กรปิดโอกาสในการถูกโจมตีทุกทาง

กรุงเทพฯ, 16 สิงหาคม 2559 – ซิสโก้ (NASDAQ: CSCO) เปิดเผยรายงานความปลอดภัยกลางปีทางไซเบอร์ (The Cisco 2016 Midyear Cybersecurity Report – MCR) ระบุองค์กรต่างๆ ไม่มีความพร้อมสำหรับการเตรียมรับปัญหาในอนาคตที่เกิดจากมัลแวร์เรียกค่าไถ่ (Ransomware) ซึ่งจะมีความซับซ้อนมากขึ้น ด้วยโครงสร้างพื้นฐานที่เปราะบาง เครือข่ายที่มีสิ่งแปลกปลอม และการตรวจจับที่ล่าช้าเปิดโอกาสให้คนร้ายมีเวลาและพื้นที่เหลือเฟือในการดำเนินการ รายงานดังกล่าวชี้ให้เห็นว่าความพยายามในการจำกัดพื้นที่ดำเนินการของผู้โจมตีเป็นปัญหาท้าทายและสำคัญที่สุดซึ่งองค์กรธุรกิจต้องเผชิญ ทั้งยังคุกคามต่อโครงสร้างพื้นฐานที่จำเป็นสำหรับการปฏิรูประบบดิจิตอล (Digital Transformation) ข้อมูลสำคัญอื่นๆ ที่พบในรายงาน MCR ได้แก่ คนร้ายกำลังขยายไปสู่การโจมตีทางฝั่งเซิร์ฟเวอร์ โดยพัฒนาวิธีการโจมตีใหม่ๆ และใช้การเข้ารหัสเพิ่มมากขึ้นเพื่อปกปิดการโจมตี

จนกระทั่งปีนี้ “มัลแวร์เรียกค่าไถ่” ได้กลายเป็นมัลแวร์ประเภทที่สร้างกำไรให้แก่คนร้ายมากที่สุดในประวัติศาสตร์ ซิสโก้คาดว่าแนวโน้มนี้จะยังคงดำเนินไปอย่างต่อเนื่อง โดยมัลแวร์เรียกค่าไถ่จะมีอำนาจทำลายล้างเพิ่มมากขึ้น สามารถแพร่กระจายด้วยตัวเอง เข้ายึดเครือข่ายทั้งหมด และจับบริษัทไว้เป็นตัวประกัน มัลแวร์เรียกค่าไถ่สายพันธุ์ใหม่จะสามารถปรับเปลี่ยนกลวิธีได้อย่างรวดเร็วเพื่อให้เกิดประสิทธิภาพสูงสุด ตัวอย่างเช่น การโจมตีด้วยมัลแวร์เรียกค่าไถ่ในอนาคตจะเล็ดลอดการตรวจจับ โดยจะสามารถจำกัดการใช้ซีพียู และยกเลิกการดำเนินการควบคุมและสั่งการ มัลแวร์เรียกค่าไถ่ชนิดใหม่นี้จะแพร่กระจายได้รวดเร็วกว่า และสามารถคัดลอกตัวเอง (Self-replicate) ภายในเครือข่ายขององค์กร ก่อนที่จะทำงานร่วมกันเพื่อดำเนินกิจกรรมเรียกค่าไถ่ต่อไป

ความสามารถในการตรวจสอบเครือข่ายและอุปกรณ์ลูกข่ายอย่างทั่วถึงถือเป็นความท้าทายที่สำคัญ โดยเฉลี่ยแล้วองค์กรจะต้องใช้เวลามากถึง 200 วันในการระบุภัยคุกคามใหม่ๆ อย่างไรก็ตาม เวลาเฉลี่ยในการตรวจจับของซิสโก้

(Time to detection: TTD) ยังคงแซงหน้าค่าเฉลี่ยของอุตสาหกรรม โดยใช้เวลาเพียงแค่ 13 ชั่วโมงในการตรวจภัยคุกคามที่ไม่เคยรู้จักมาก่อนในรอบ 6 เดือนจนถึงเดือนเมษายน 2559 โดยลดลงจาก 17.5 ชั่วโมงสำหรับรอบระยะเวลาที่สิ้นสุดในเดือนตุลาคม 2558 เวลาในการตรวจจับภัยคุกคามที่รวดเร็วกว่านี้นับว่าจำเป็นอย่างยิ่งต่อการจำกัดพื้นที่ปฏิบัติการของผู้โจมตี และลดความเสียหายที่เกิดจากการบุกรุก ตัวเลขนี้อ้างอิงจากข้อมูลการตรวจวัดด้านความปลอดภัยที่เก็บรวบรวมจากผลิตภัณฑ์ด้านการรักษาความปลอดภัยของซิสโก้ที่ติดตั้งและใช้งานในองค์กรต่างๆ ทั่วโลก

ขณะที่ผู้โจมตีสร้างสรรค์นวัตกรรมใหม่ๆ ฝ่ายที่ทำหน้าที่ป้องกันก็พยายามที่จะรักษาความปลอดภัยให้กับอุปกรณ์และระบบต่างๆ ระบบที่ไม่ได้รับการสนับสนุนและไม่ได้ติดตั้งแพตช์จะเพิ่มโอกาสให้แก่ผู้โจมตีในการเจาะเข้าสู่ระบบอย่างง่ายดายโดยไม่ถูกตรวจจับ และสร้างความเสียหายต่อระบบเพื่อทำกำไรสูงสุด รายงานความปลอดภัยไซเบอร์ฉบับกลางปี 2559 ของซิสโก้แสดงให้เห็นว่าปัญหาท้าทายนี้ยังคงมีอยู่ทั่วโลก ขณะที่องค์กรต่างๆ ในอุตสาหกรรมสำคัญๆ อย่างเช่นสถานพยาบาล ประสบปัญหาการโจมตีที่เพิ่มขึ้นอย่างมากในหลายเดือนที่ผ่านมา รายงานฉบับนี้ยังระบุอีกด้วยว่าตลาดที่เฉพาะเจาะจงทั้งหมดและภูมิภาคต่างๆ ทั่วโลกล้วนตกเป็นเป้าหมายเช่นเดียวกัน สมาคม หน่วยงาน องค์กรการกุศล องค์กรเอกชน และธุรกิจอิเล็กทรอนิกส์ล้วนประสบปัญหาการโจมตีที่เพิ่มมากขึ้นในครึ่งแรกของปี 2559 ส่วนในระดับโลกนั้น มีปัญหาทางด้านการเมืองภูมิศาสตร์ เช่น กฎระเบียบที่ซับซ้อน นโยบายไซเบอร์ซีเคียวริตี้ที่ขัดแย้งกันในแต่ละประเทศ ความต้องการที่จะควบคุมหรือเข้าถึงข้อมูลอาจจำกัดและขัดแย้งกับการดำเนินการค้าระหว่างประเทศท่ามกลางสถานการณ์ภัยคุกคามที่ซับซ้อน

ผู้โจมตีดำเนินการอย่างไม่มีข้อจำกัด
สำหรับผู้โจมตี เวลาที่มากขึ้นในการดำเนินการโดยไม่ถูกตรวจจับย่อมหมายถึงผลกำไรที่เพิ่มมากขึ้น ทั้งนี้ในช่วงครึ่งแรกของปี 2559 ซิสโก้รายงานว่าผู้โจมตีได้รับผลกำไรเพิ่มสูงขึ้นอย่างมากเนื่องจากเหตุผลดังต่อไปนี้:

1). การขยายขอบเขตเป้าหมาย: ผู้โจมตีขยายขอบเขตจากการโจมตีทางฝั่งลูกข่าย (client-side) ไปสู่ฝั่งเซิร์ฟเวอร์ (server-side) เพื่อหลีกเลี่ยงการตรวจจับ เพิ่มความเสียหาย และสร้างผลกำไรเพิ่มมากขึ้น

• ช่องโหว่ใน Adobe Flash ยังคงเป็นหนึ่งในเป้าหมายหลักสำหรับโฆษณาอันตรายและการเจาะระบบ โดยในการเจาะระบบด้วยชุดเครื่องมือ Nuclear พบว่า Flash มีสัดส่วนถึง 80 เปอร์เซ็นต์ของการเจาะระบบที่ประสบความสำเร็จ

• นอกจากนี้ ซิสโก้ยังพบแนวโน้มใหม่ในการโจมตีด้วยมัลแวร์เรียกค่าไถ่ (Ransomware) ซึ่งอาศัยช่องโหว่ของเซิร์ฟเวอร์ โดยเฉพาะอย่างยิ่งภายในเซิร์ฟเวอร์ JBoss โดย 10 เปอร์เซ็นต์ของเซิร์ฟเวอร์ JBoss ที่เชื่อมต่ออินเทอร์เน็ตทั่วโลกพบว่ามีช่องโหว่ ทั้งนี้ช่องโหว่ JBoss จำนวนมากที่ใช้ในการเจาะระบบเหล่านี้ได้ถูกตรวจพบเมื่อ 5 ปีที่แล้ว นั่นหมายความว่าการติดตั้งแพตช์พื้นฐานและโปรแกรมอัพเดตจากเวนเดอร์สามารถช่วยป้องกันการโจมตีดังกล่าวได้อย่างง่ายดาย

2). การพัฒนาวิธีการโจมตี: ในครึ่งแรกของปี 2559 คนร้ายยังคงพัฒนาวิธีการโจมตีอย่างต่อเนื่อง เพื่อใช้ประโยชน์จากความบกพร่องของฝ่ายป้องกันในการตรวจสอบระบบเครือข่าย

• การใช้ช่องโหว่ของ Windows Binary กลายเป็นวิธีการโจมตีทางเว็บที่แพร่หลายที่สุดในช่วง 6 เดือนที่ผ่านมา วิธีการนี้ช่วยให้สามารถเจาะเข้าสู่โครงสร้างพื้นฐานเครือข่ายได้อย่างแน่นอนมากขึ้น และเพิ่มความยากลำบากในการระบุและกำจัดการโจมตีเหล่านี้

• ภายในระยะเวลาเดียวกันนี้ การหลอกลวงแบบ Social Engineering ผ่านทางเฟซบุ๊กลดลง จากเดิมที่เคยครองอันดับ 1 แต่ตอนนี้ร่วงลงไปอยู่ที่อันดับ 2

3). การปกปิดร่องรอย: คนร้ายหันมาใช้การเข้ารหัสเพิ่มมากขึ้นเพื่อปิดบังการดำเนินการในส่วนต่างๆ ซึ่งทำให้ฝ่ายป้องกันทำการตรวจสอบได้ยากยิ่งขึ้น

• ซิสโก้พบว่ามีการใช้เงินดิจิตอล การเข้ารหัสด้วย Transport Layer Security และ Tor ซึ่งรองรับการติดต่อสื่อสารบนเว็บโดยไม่เปิดเผยชื่อ

• สิ่งสำคัญก็คือ มัลแวร์ที่เข้ารหัส HTTPS ซึ่งใช้ในแคมเปญโฆษณาอันตราย เพิ่มขึ้น 300 เปอร์เซ็นต์ในเดือนธันวาคม 2558 ถึงมีนาคม 2559 มัลแวร์ที่เข้ารหัสนี้ยังช่วยให้คนร้ายสามารถปิดบังกิจกรรมบนเว็บและเพิ่มเวลาในการดำเนินการอีกด้วย

ฝ่ายป้องกันพยายามที่จะลดช่องโหว่และปิดช่องว่างที่นำไปสู่ภัยคุกคาม
ขณะที่ต้องเผชิญกับการโจมตีที่ซับซ้อน ทรัพยากรที่จำกัด และโครงสร้างพื้นฐานที่ล้าสมัย ฝ่ายป้องกันพยายามที่จะก้าวให้ทันกับคนร้าย ข้อมูลที่พบระบุว่า ฝ่ายป้องกันไม่สามารถตรวจสอบดูแลเครือข่ายได้อย่างเพียงพอ เช่น การติดตั้งแพตช์ โดยเฉพาะอย่างยิ่งในส่วนของเทคโนโลยีที่มีความสำคัญอย่างมากต่อการดำเนินธุรกิจ ตัวอย่างเช่น:

• ในส่วนของเบราว์เซอร์ Google Chrome ซึ่งใช้การอัพเดตอัตโนมัติ มีผู้ใช้ราว 75 ถึง 80 เปอร์เซ็นต์ที่ใช้เบราว์เซอร์เวอร์ชั่นล่าสุด หรือล้าสมัยกว่าที่มีอยู่หนึ่งเวอร์ชั่น

• เมื่อเราหันไปพิจารณาในส่วนของซอฟต์แวร์ ก็จะพบว่า Java มีการโยกย้ายที่ล่าช้า โดยหนึ่งในสามของระบบที่ถูกตรวจสอบยังคงรัน Java SE 6 ซึ่ง Oracle ยกเลิกการสนับสนุนแล้ว (เวอร์ชั่นปัจจุบันคือ SE 10)

• ใน Microsoft Office 2013 เวอร์ชั่น 15x พบว่ามีไม่เกิน 10 เปอร์เซ็นต์ที่ใช้เซอร์วิสแพ็ครุ่นล่าสุด

นอกจากนี้ ซิสโก้ยังพบว่าโครงสร้างพื้นฐานจำนวนมากไม่ได้รับการสนับสนุน หรือยังคงถูกใช้งานอยู่โดยที่มีช่องโหว่ที่รู้จัก ปัญหานี้เกิดขึ้นกับระบบของผู้ผลิตหลายราย รวมไปถึงอุปกรณ์ลูกข่าย ทั้งนี้ คณะนักวิจัยของซิสโก้ได้ตรวจสอบอุปกรณ์ของซิสโก้จำนวน 103,121 เครื่องที่เชื่อมต่อกับอินเทอร์เน็ต และพบว่า:

- โดยเฉลี่ยแล้ว อุปกรณ์แต่ละเครื่องมีช่องโหว่ที่รู้จัก 28 ช่องโหว่
- อุปกรณ์ถูกใช้งานมานานโดยเฉลี่ย 5.64 ปีทั้งๆ ที่มีช่องโหว่ที่รู้จัก
- กว่า 9 เปอร์เซ็นต์มีช่องโหว่ที่ตรวจพบมานานกว่า 10 ปี

นอกจากนี้ ซิสโก้ยังได้ตรวจสอบโครงสร้างพื้นฐานซอฟต์แวร์จากกลุ่มตัวอย่างกว่า 3 ล้านระบบที่ติดตั้ง โดยส่วนใหญ่เป็นระบบ Apache และ OpenSSH ที่มีช่องโหว่ที่รู้จักโดยเฉลี่ย 16 ช่องโหว่ และถูกใช้งานโดยเฉลี่ยมานานราว 5.05 ปี

อัพเดตของเบราว์เซอร์เป็นอัพเดตขนาดเล็กที่สุดสำหรับอุปกรณ์ลูกข่าย ขณะที่แอพพลิเคชั่นระดับองค์กรและโครงสร้างพื้นฐานทางฝั่งเซิร์ฟเวอร์ดำเนินการอัพเดตได้ยากกว่า และอาจก่อให้เกิดปัญหาต่อการดำเนินธุรกิจอย่างต่อเนื่อง โดยสาระสำคัญก็คือ ยิ่งแอพพลิเคชั่นมีความสำคัญต่อการดำเนินธุรกิจมากเท่าใด ก็จะยิ่งมีการอัพเดตน้อยลงเท่านั้น จึงก่อให้เกิดช่องว่างและโอกาสสำหรับผู้โจมตีเพิ่มมากขึ้น

ซิสโก้แนะนำขั้นตอนง่ายๆ ในการปกป้องสภาพแวดล้อมทางด้านธุรกิจ
คณะนักวิจัย Talos ของซิสโก้พบว่า องค์กรที่ดำเนินขั้นตอนที่เรียบง่ายแต่เป็นขั้นตอนที่สำคัญ 2-3 ขั้นตอน สามารถปรับปรุงการดำเนินงานด้านความปลอดภัยได้เป็นอย่างมาก เช่น:
- ปรับปรุงความเป็นระเบียบเรียบร้อยของเครือข่าย ด้วยการตรวจสอบดูแลเครือข่าย การติดตั้งแพตช์และการอัพเกรดตามกำหนดเวลา การแบ่งเครือข่ายเป็นส่วนๆ การปรับใช้ระบบป้องกันที่ส่วนรอบนอกของเครือข่าย รวมถึงการปกป้องอีเมลและเว็บ ไฟร์วอลล์รุ่นอนาคต (Next-Generation Firewall) และระบบป้องกันการบุกรุกรุ่นอนาคต (Next-Generation IPS)ฆ

- ผนวกรวมระบบป้องกันเข้าด้วยกัน โดยใช้แนวทางเชิงสถาปัตยกรรมสำหรับการรักษาความปลอดภัย แทนที่จะติดตั้งเฉพาะจุด

- ตรวจวัดเวลาในการตรวจจับ โดยเฉพาะอย่างยิ่งเวลาที่เร็วที่สุดในการตรวจพบภัยคุกคาม แล้วแก้ไขปัญหาอย่างทันท่วงที ทำให้การตรวจวัดเวลาในการตรวจจับ กลายเป็นส่วนหนึ่งของนโยบายการรักษาความปลอดภัยขององค์กรอย่างต่อเนื่อง

- ปกป้องผู้ใช้ของคุณทุกที่ทุกเวลา ไม่ว่าผู้ใช้จะอยู่หรือทำงานที่ใดก็ตาม ไม่ใช่ปกป้องเพียงแค่ระบบที่ผู้ใช้ใช้งานหรือขณะที่ผู้ใช้ใช้งานอยู่บนเครือข่ายของบริษัทเท่านั้น

- แบ็คอัพข้อมูลสำคัญ และทดสอบประสิทธิภาพอย่างสม่ำเสมอ พร้อมทั้งตรวจสอบว่าข้อมูลแบ็คอัพไม่มีความเสี่ยงที่จะได้รับความเสียหาย

คำกล่าวสนับสนุน

“ขณะที่องค์กรต่างๆ ใช้ประโยชน์จากรูปแบบธุรกิจใหม่ๆ ที่เป็นผลมาจากการปฏิรูประบบดิจิตอล (Digital Transformation) ความปลอดภัยถือเป็นรากฐานที่สำคัญอย่างยิ่ง ปัจจุบันผู้โจมตีระบบสามารถหลบหลีกการตรวจจับ และมีเวลาเพิ่มมากขึ้นในการดำเนินการ ในการปิดช่องว่างและลดโอกาสสำหรับการโจมตี ลูกค้าจำเป็นที่จะต้องยกระดับความสามารถในการตรวจสอบเครือข่ายอย่างทั่วถึง และจะต้องปรับปรุงกิจกรรมต่างๆ เช่น การติดตั้งแพตช์ และการยกเลิกการใช้งานโครงสร้างพื้นฐานที่ล้าสมัย ซึ่งขาดความสามารถด้านการรักษาความปลอดภัยขั้นสูง”

“คนร้ายยังคงสร้างรายได้จากการโจมตีอย่างต่อเนื่อง และคิดค้นรูปแบบธุรกิจที่สร้างรายได้เป็นจำนวนมาก ด้วยเหตุนี้ซิสโก้จึงทำงานร่วมกับลูกค้าของเรา เพื่อช่วยให้ลูกค้ายกระดับความก้าวหน้า ความสามารถในการตรวจสอบและควบคุมให้ใกล้เคียงหรือเหนือกว่าคนร้าย” มาร์ตี้ โรช รองประธานและหัวหน้าสถาปนิก กลุ่มธุรกิจการรักษาความปลอดภัยของซิสโก้ กล่าว

เกี่ยวกับรายงาน
รายงานความปลอดภัยทางไซเบอร์ของซิสโก้กลางปี 2559 ตรวจสอบข้อมูลข่าวกรองเกี่ยวกับภัยคุกคามล่าสุดที่เก็บรวบรวมโดยหน่วยงานข่าวกรองด้านความปลอดภัย Cisco Collective Security Intelligence รายงานดังกล่าวให้ข้อมูลเชิงลึกเกี่ยวกับอุตสาหกรรมที่ขับเคลื่อนด้วยข้อมูล รวมถึงแนวโน้มด้านความปลอดภัยทางไซเบอร์ในช่วงครึ่งแรกของปีนี้ พร้อมด้วยคำแนะนำในการปรับปรุงสถานะความปลอดภัย รายงานฉบับนี้อ้างอิงข้อมูลจากแหล่งต่างๆ มากมาย รวมถึงข้อมูลรายวันจากระบบตรวจวัดและระบบส่งข้อมูลทางไกลกว่า 4 หมื่นล้านแห่ง นักวิจัยของซิสโก้ได้ทำการเปลี่ยนข้อมูล (Intelligence) ให้เป็นมาตรการป้องกันแบบเรียลไทม์ (real-time protection) สำหรับผลิตภัณฑ์และบริการของซิสโก้ให้กับลูกค้าของซิสโก้ในประเทศต่างๆ ทั่วโลกในทันที

ทรัพยากรสนับสนุน
วิดีโอของซิสโก้ เดวิด เกอเคเลอร์, สตีฟ มาร์ติโน่: รายงานความปลอดภัยทางไซเบอร์ของซิสโก้ประจำกลางปี 2559
รายงานความปลอดภัยทางไซเบอร์ของซิสโก้ประจำกลางปี 2559
บล็อกของซิสโก้: เวลาคือสิ่งสำคัญ: เปิดเผยรายงานความปลอดภัยทางไซเบอร์ของซิสโก้ประจำกลางปี 2559
ภาพอินโฟกราฟิกของซิสโก้
กราฟิกในรายงานความปลอดภัยทางไซเบอร์ของซิสโก้ประจำกลางปี 2559
ติดตามซิสโก้บน Twitter @CiscoSecurity
ถูกใจ Cisco Security บน Facebook

เกี่ยวกับ ซิสโก้
ซิสโก้ (NASDAQ: CSCO) เป็นผู้นำระดับโลกด้านเทคโนโลยีที่ทำงานกับอินเทอร์เน็ตตั้งแต่ปี ค.ศ. 1984 บุคลากรของเรา ผลิตภัณฑ์ และ พันธมิตรช่วยเหลือสังคมเชื่อมต่อโอกาสทางดิจิตอลอย่างปลอดภัย ดูข่าวและข้อมูลเพิ่มเติมเกี่ยวกับซิสโก้ได้ที่ newsroom.cisco.com และติดตามข่าวสารของซิสโก้บนทวิตเตอร์ที่ @Cisco

###

ประชาสัมพันธ์ข่าวโดย:

วราวอง จงรักษ์

โทรศัพท์: 02-971-3711

อีเมล์: warawong@pc-a.co.th