เดลล์เผยรายงานภัยคุกคามประจำปี ชี้ อาชญากรไซเบอร์ ใช้ชั้นเชิงแข็งแกร่ง เร่งการเข้ารหัสทราฟฟิกให้เร็วขึ้น 50% กระทบผู้ใช้นับหลายล้านคนในปี 2558

เดลล์ เผยผลรายงานภัยคุกคามประจำปีของ Dell Security Annual Threat Report ปี 2558 สรุปผลการรวบรวมข้อมูลตลอดปีจากเครือข่ายการป้องกันระดับโลก Dell SonicWALL Global Response Intelligence Defense (GRID) พร้อมฟีดข้อมูลรายวันที่ได้จากไฟร์วอลล์จำนวนกว่าล้านตัว และอุปกรณ์ปลายทาง (เอ็นด์พอยท์) ที่เชื่อมต่อกันจำนวนนับหลายสิบล้านจุด เพื่อช่วยองค์กรธุรกิจได้รับข้อแนะนำที่มาจากเหตุการณ์ที่เกิดขึ้นจริง เพื่อเตรียมความพร้อมในการป้องกัน และรับมือกับภัยคุกคามได้อย่างมีประสิทธิผล

นายฮาน ชอน ผู้อำนวยการ การจัดการระบบปลายทาง และการรักษาความปลอดภัย ภูมิภาคเอเชีย แปซิฟิค และประเทศญี่ปุ่น กล่าวว่า ในปี 2558 มีการเจาะช่องโหว่มากมายและประสบความสำเร็จ เพราะอาชญากรไซเบอร์สามารถค้นพบจุดอ่อนในโปรแกรมรักษาความปลอดภัยของเหยื่อ ซึ่งมาจากการที่โซลูชันเฉพาะทาง ไม่มีการอัพเดทและไม่มีการเชื่อมต่อจึงไม่สามารถจับสิ่งผิดปกติในระบบนิเวศได้

จากรายงาน Dell SonicWALL ระบุว่ามีการใช้ Exploit Kits เพิ่มมากขึ้น โดยในปีที่ผ่านมา อาชญากรไซเบอร์ ได้นำยุทธวิธีการโจมตีใหม่ๆ เข้ามาใช้ เพื่อซ่อน exploit kit ไม่ให้ระบบรักษาความปลอดภัยจับได้ รวมถึงการใช้กลไกที่ต่อต้านการพิสูจน์ด้านนิติเวชศาสตร์ (Anti-forensic) การเปลี่ยนรูปแบบ URL และวิทยาการในการอำพรางข้อมูล ซึ่งก็คือการปกปิดไฟล์ ข้อความ รูปภาพ หรือ วิดีโอที่อยู่ในไฟล์อื่น ข้อความ รูปภาพ หรือวิดีโอ รวมถึงการใช้เทคนิคเพื่อปรับแก้หน้า Landing page

นอกจากนี้ การเติบโตของการเข้ารหัสอินเตอร์เน็ตแบบ SSL/TLS แบบผสมผสานยังเป็นช่องทางการคุกคามแบบใหม่ที่ล่อตาล่อใจแฮกเกอร์เช่นกัน การใช้วิธีเข้ารหัสแบบ SSL หรือ TSL ผู้โจมตีที่มีทักษะสามารถเข้าไปลบคำสั่งพร้อมควบคุมการสื่อสารและวางโค๊ดประสงค์ร้ายเพื่อหลีกเลี่ยงการตรวจจับของระบบป้องกันการบุกรุก IPS (Intrusion Prevention Systems) และระบบตรวจสอบแอนตี้มัลแวร์ (Anti-malware Inspection Systems) ซึ่งยุทธวิธีนี้ถูกใช้ในแคมเปญโฆษณาของมัลแวร์เพื่อหลอกลวง (Malvertising Campaign) ในเดือนสิงหาคม 2558 เพื่อเปิดเผยข้อมูลผู้ใช้ยาฮู จำนวนมากถึง 900 ล้านรายให้กับมัลแวร์ โดยจะเปลี่ยนเส้นทางไปที่เว็บไซต์ที่ติดมัลแวร์ Angler Exploit Kit

ทีมงาน Dell SonicWALL ยังชี้ให้เห็นว่าตลอดปี 2558 มีการใช้ HTTPS สูงขึ้นอย่างรวดเร็ว โดยไตรมาสที่ 4 ของ

ปีปฏิทิน 2558 มีการเชื่อมต่อด้วย HTTPS (SSL/TLS) เฉลี่ยอยู่ที่ 64.6 เปอร์เซ็นต์ ของการเชื่อมต่อเว็บทั้งหมด ซึ่งแซงหน้าการเติบโตของ HTTP เกือบตลอดทั้งปี เฉพาะในเดือนมกราคมของปี 2558 อัตราการเชื่อมต่อด้วย HTTPS สูงกว่าเดือนมกราคมของปีที่ผ่านมาถึง 109% และมีอัตราการเพิ่มขึ้นเฉลี่ยอยู่ที่ 53% ต่อเดือน เมื่อเทียบกับช่วงเดียวกันในปี 2557

นายชอน กล่าวว่า นอกจากนี้ มัลแวร์สำหรับแอนดรอยด์ยังคงเพิ่มขึ้นต่อเนื่อง ทำให้สมาร์ทโฟนจำนวน 81% ตกอยู่ในความเสี่ยง โดยในปี 2558 Dell SonicWALL สามารถค้นพบแนวโน้มใหม่ๆ เกิดขึ้น 2-3 รูปแบบ จากการโจมตีอุปกรณ์ที่ใช้แอนดรอยด์ ในปี 2558 ได้แก่ มัลแวร์เรียกค่าไถ่ (Ransomware) ซึ่งเจาะจงที่ระบบแอนดรอยด์ เพิ่มขึ้นอย่างรวดเร็วตลอดทั้งปี และยังมีการเพิ่มขึ้นของมัลแวร์แอนดรอยด์ใหม่ที่ฝังตัวอยู่ในคอนเท้นท์ประสงค์ร้าย บนไฟล์ Unix Library มากกว่า classes.dex file ที่ระบบรักษาความปลอดภัยมักจะสแกนเป็นปกติ ที่สำคัญ ภาคการเงินยังคงเป็นเป้าหมายหลักของมัลแวร์แอนดรอยด์ โดยภัยคุกคามจะมุ่งเป้าไปที่แอพพลิเคชันของธนาคารที่อยู่บนอุปกรณ์ที่ติดมัลแวร์

“แม้ว่าจะมีการออกระบบปฏิบัติการ Android 6.0 Marshmallow มาในเดือนตุลาคม 2558 ซึ่งรวมฟีเจอร์รักษาความปลอดภัยแบบใหม่มาด้วย เราคาดว่าอาชญากรไซเบอร์ก็จะยังคงพยายามหาทางหลบหลีกการป้องกันที่ว่าได้” ชอน กล่าว “ผู้ใช้ระบบแอนดรอยด์ควรระมัดระวังด้วยการติดตั้งแอพพลิเคชันจากแอพฯ สโตร์ที่น่าเชื่อถือ เช่น Google Play และคอยดูว่ามีการอนุญาติอะไรไปตามที่แอพฯ ขอมาบ้าง พร้อมทั้งหลีกเลี่ยงการ root โทรศัพท์อีกด้วย”

ทั้งนี้ การโจมตีของมัลแวร์ เพิ่มเกือบสองเท่าตัว จาก 4.2 ล้านครั้งจนแตะ 8.19 พันล้านครั้ง และสร้างความเสียหายอย่างคาดไม่ถึงให้กับหน่วยงานภาครัฐบาล องค์กรธุรกิจ บริษัทต่างๆ ไปจนถึงบุคคลทั่วไป จากการสำรวจด้านการโจมตี ทีมงานของ Dell SonicWALL ได้รับตัวอย่างมัลแวร์ที่โดดเด่นถึง 64 ล้านตัวอย่าง เทียบกับปี 2557 ซึ่งมีอยู่แค่ 37 ล้านตัวอย่าง และเป็นอัตราการเพิ่มที่สูงถึง 73 เปอร์เซ็นต์ ชี้ให้เห็นว่าผู้โจมตีใช้ความพยายามมากขึ้นในแต่ละปี ด้วยการใช้โค๊ดประสงค์ร้ายเจาะเข้าไปที่ระบบงานขององค์กร

นอกจากนี้ ยังมีการรวมตัวกันของทั้ง Dyre Wolf และ Parite อยู่บนในทราฟฟิกเครือข่ายตลอดปี 2558 ตลอดจนมัลแวร์อื่นๆ ที่อยู่ยงคงกระพันได้แก่ TongJi ที่ใช้ JavaScript อย่างแพร่หลายในการขับเคลื่อนแคมเปญหลากหลาย (เป็นมัลแวร์ที่ดาวน์โหลดตัวเองแบบอัตโนมัติอย่างเงียบๆ เวลาที่ผู้ใช้เข้าไปที่เว็บไซต์ที่ติดมัลแวร์ดังกล่าว) Virut บ็อตเน็ตที่ก่ออาชญากรรมไซเบอร์ทั่วไป มีมาตั้งแต่ปี 2549 เป็นอย่างต่ำ และการคืนชีพของ Conficker ไวรัสหนอนคอมพิวเตอร์ที่โด่งดัง โดยพุ่งเป้าไปที่ ระบบปฏิบัติการ Windows มาตั้งแต่ปี 2551

“การกระจายของมัลแวร์ แทบจะไม่จำกัดรูปแบบในการคุกคาม ไม่ว่าจะเป็นยุทธวิธีที่คลาสสิก เช่นอีเมลขยะ ตลอดจนเทคโนโลยีที่ใหม่ขึ้นไปอีก ทั้งกล้องถ่ายรูปที่สวมใส่ได้ รถยนต์ไฟฟ้า และอุปกรณ์ทุกประเภทที่เชื่อมต่ออินเตอร์เน็ตได้ (IoT Devices)” นายชอน กล่าว “ในโลกที่เชื่อมโยงถึงกัน ณ ปัจจุบัน สิ่งสำคัญคือการระวังภัยรอบตัวแบบ

360 องศา ทั้งระบบงานและซอฟต์แวร์ของตัวเอง ไปจนถึงการฝึกอบรมและการเข้าถึงระบบของพนักงาน รวมไปถึงทุกคนที่เข้ามาติดต่อกับคุณทั้งทางเครือข่ายและข้อมูล”

นอกจากนี้ รายงานภัยคุกคามประจำปีของ Dell Security ยังได้ระบุถึงแนวโน้ม และการคาดการณ์ที่มีการถกประเด็นกันต่อในรายละเอียด อาทิ การต่อสู้ระหว่างการเข้ารหัส HTTPS และการสแกนภัยคุกคามจะยังคงแข่งเดือดกันต่อ เนื่องจากบริษัทกลัวว่าจะต้องแลกกับประสิทธิภาพที่ลดลง การที่ไวรัส zero-day Adobe Flash จะลดลงในที่สุดเนื่องจากเบราเซอร์รายหลักๆ จะไม่รองรับ Adobe Flash อีกต่อไป ภัยคุกคามประสงค์ร้ายจะมุ่งเป้าไปที่ Android Pay ทางช่องโหว่ของ NFC (Near Field Communication) การโจมตีที่ว่าอาจสบช่องจากแอพฯ Android และ POS ซึ่งเป็นเครื่องมือที่แฮกเกอร์ใช้และควบคุมได้ง่าย รวมถึง ความเป็นไปได้ที่จะเกิดภัยคุกคามที่มุ่งเน้นไปที่รถยนต์ที่ใช้ Android Auto ที่จะผ่านมาทางมัลแวร์เรียกค่าไถ่ (ransomware) ที่ทำให้ผู้ซึ่งตกเป็นเหยื่อต้องจ่ายเงินเพื่อให้ออกจากรถได้ หรืออาจจะใช้ยุทธวิธีที่อันตรายกว่านั้นก็เป็นได้

รายงานภัยคุกคามระบบรักษาความปลอดภัยประจำปีของเดลล์ รวบรวมข้อมูลโดยเครือข่าย Dell Global Response Intelligence Defense (GRID) ซึ่งจัดหาข้อมูลโดยรวบรวมมาจากแหล่งข้อมูลและอุปกรณ์จำนวนมาก ทั้งจาก เซ็นเซอร์ระบบรักษาความปลอดภัยกว่าหนึ่งล้านตัวในเกือบ 200 ประเทศ และจากพื้นที่ต่างๆ ไปจนถึงข้อมูลเกี่ยวกับการคุกคามที่มีการแบ่งปันกันระหว่างระบบรักษาความปลอดภัย ไม่ว่าจะเป็นจากอุปกรณ์ไฟร์วอลล์ ระบบรักษาความปลอดภัยอีเมล ระบบรักษาความปลอดภัยจุดปลายทาง กับดักที่ติดตั้งเพื่อดักจับแฮกเกอร์ (honeypots) และระบบกรองเนื้อหา รวมถึงเทคโนโลยีแซนด์บ็อกซ์ในศูนย์ภัยคุกคามของเดลล์ โครงข่ายด้านการวิเคราะห์มัลแวร์ในแบบอัตโนมัติเฉพาะของ Dell SonicWALL และอื่นๆ