WannaCry ยังไม่ตาย! แคสเปอร์สกี้ แลป เผยแรนซัมแวร์ร้ายโจมตีผู้ใช้เกือบ 75,000 ราย ในไตรมาส 3

กว่าหนึ่งปีครึ่งแล้วที่เกิดเหตุแรนซัมแวร์วอนนาคราย (WannaCry) ระบาด ทำให้วอนนาครายขึ้นแท่นติดอันดับภัยแรนซัมแวร์ที่แพร่กระจายสร้างความเสียหายไปทั่วโลก โดยล่าสุดจากรายงาน Q3 IT threat evolution ของแคสเปอร์สกี้ แลป พบว่า ในไตรมาส 3 ปี 2018 นี้ วอนนาครายโจมตีผู้ใช้จำนวน 74,621 ราย คิดเป็น 28.72% ของเหยื่อคริปเตอร์ทั้งหมด อัตราส่วนการโจมตีเพิ่มขึ้นจากปีที่แล้วมากกว่าเศษสองส่วนสามเท่าจากไตรมาส 3 ปี 2017 ซึ่งมีเหยื่อวอนนาคราย 16.78%

ปรากฏการณ์การโจมตีทางไซเบอร์ของคริปเตอร์วอนนาครายเกิดขึ้นเมื่อเดือนพฤษภาคม 2017 และยังนับว่าเป็นการแพร่ระบาดแรนซัมแวร์ครั้งใหญ่ที่สุด แม้ว่าก่อนการโจมตี 2 เดือน วินโดวส์จะออกแพทช์เพื่อปิดช่องโหว่ EternalBlue แล้วก็ตาม แต่วอนนาครายก็ยังสามารถแพร่กระจายไปยังดีไวซ์หลายแสนเครื่องทั่วโลก คริปเตอร์ดำเนินการยึดการเข้าใช้งานเครื่อง เข้ารหัสไฟล์ในเครื่องของเหยื่อและเรียกค่าไถ่แลกกับกุญแจถอดรหัสไฟล์

เฟเดอร์ ซินิตซิน นักวิจัยด้านความปลอดภัยของแคสเปอร์สกี้ แลป กล่าวว่า “สัดส่วนการโจมตีของวอนนาครายที่เพิ่มสูงขึ้น เป็นการย้ำเตือนว่า การแพร่ระบาดนี้ยังไม่จบง่ายๆ การโจมตีอาจก่อความเสียหายรุนแรง จึงควรมีมาตรการป้องกันและแพทช์ดีไวซ์อย่างสม่ำเสมอ ซึ่งเป็นวิธีป้องกันที่ดีกว่าการแก้ปัญหาไฟล์เข้ารหัสแน่นอน”

สถิติภัยคุกคามออนไลน์อื่นๆ ในไตรมาส 3 ปี 2018

- โซลูชั่นของแคสเปอร์สกี้ แลป สามารถตรวจจับและสกัดกั้นการโจมตีจำนวน 947,027,517 ครั้ง จากแหล่งออนไลน์ที่กระจายอยู่ 200 ประเทศทั่วโลก (ลดลง 1.7% จากไตรมาสเดียวกันเมื่อปีที่แล้ว)
- เว็บแอนตี้ไวรัสคอมโพเน้นตรวจพบ URL มุ่งร้าย 246,695,333 รายการ (ลดลง 29.9% จากไตรมาสเดียวกันเมื่อปีที่แล้ว)
- พบการพยายามแพร่เชื้อมัลแวร์ที่มุ่งขโมยเงินจากช่องทางออนไลน์ของบัญชีธนาคาร จากคอมพิวเตอร์ 305,315 เครื่อง (เพิ่มขึ้น 41.5% จากไตรมาสเดียวกันเมื่อปีที่แล้ว)
- ไฟล์แอนตี้ไวรัสของแคสเปอร์สกี้ แลป ตรวจพบอ็อบเจ็คมุ่งร้ายและไม่พึงประสงค์จำนวน 239,177,356 รายการ (เพิ่มขึ้น 24.5% จากไตรมาสเดียวกันเมื่อปีที่แล้ว)

• ผลิตภัณฑ์ป้องกันความปลอดภัยโมบายของแคสเปอร์สกี้ แลป ตรวจจับแพ็คเกจติดตั้ง 1,305,015 รายการ (ลดลง 25.2% จากไตรมาสเดียวกันเมื่อปีที่แล้ว)

แคสเปอร์สกี้ แลป ขอแนะนำให้ผู้ใช้ลดความเสี่ยงจากภัยวอนนาครายและคริปเตอร์อื่นๆ ดังนี้

• อัพเดทระบบปฏิบัติการอย่างสม่ำเสมอเพื่อลดช่องโหว่ และใช้โซลูชั่นเพื่อความปลอดภัยที่มีการอัพเดทฐานข้อมูลสม่ำเสมอ การใช้โซลูชั่นเพื่อความปลอดภัยที่มีเทคโนโลยีการป้องกันแรนซัมแวร์โดยเฉพาะนั้นเป็นเรื่องสำคัญ อย่างเช่นเทคโนโลยี System Watcher ของแคสเปอร์สกี้ แลป สามารถบล็อกและกู้คืนการเปลี่ยนแปลงแก้ไขต่างๆ รวมถึงการถอดรหัสไฟล์ด้วย

• หากโชคร้ายไฟล์ถูกเข้ารหัสด้วยคริปโตมัลแวร์แล้ว ขอแนะนำไม่ให้จ่ายเงินค่าไถ่ให้โจรไซเบอร์ เพราะจะเป็นการกระตุ้นให้โจรไซเบอร์ดำเนินแผนการร้ายต่อไป ผู้ใช้ควรค้นหาตัวถอดรหัสหรือดีคริปเตอร์จากอินเทอร์เน็ต ซึ่งเปิดให้บริการฟรี เช่น เว็บ https://noransom.kaspersky.com/

• ควรทำการสำรองหรือแบ็คอัพไฟล์เวอร์ชั่นล่าสุดอย่างสม่ำเสมอ และจัดเก็บทั้งในฮาร์ดดิสก์และบนคลาวด์ เพื่อเรียกใช้งานได้ในกรณีไฟล์สูญหายจากมัลแวร์หรือดีไวซ์พัง และต้องไม่ลืมตั้งค่าปกป้องคลาวด์ด้วยรหัสที่แฮ็กยาก

• สำหรับองค์กรธุรกิจ ขอแนะนำให้ใช้โซลูชั่นเพื่อความปลอดภัยที่สามารถใช้ทูลฟรีของแคสเปอร์สกี้ แลป Kaspersky Anti-Ransomware Tool ร่วมกันได้

• เพื่อสร้างการป้องกันระดับองค์กร ควรให้ความรู้และจัดอบรมพนักงานและทีมไอที แยกจัดเก็บข้อมูลละเอียดอ่อน ควบคุมการเข้าใช้งาน และแบ็คอัพข้อมูลทุกอย่าง

• ใช้โซลูชั่นที่ครอบคลุม เช่น Kaspersky Endpoint Security for Business ที่สามารถตรวจจับและย้อนกระบวนการร้ายได้ โซลูชั่นที่ดีควรมีฟีเจอร์การจัดการช่องโหว่และแพทช์ที่จะสามารถกำจัดช่องโหว่และอัพเดทได้อัตโนมัติ ซึ่งจะช่วยลดช่องโหว่ที่โจรไซเบอร์มักใช้งานได้

• สุดท้าย ตระหนักเสมอว่าแรนซัมแวร์เป็นอาชญากรรม จึงไม่ควรจ่ายเงินค่าไถ่เด็ดขาด และหากตกเป็นเหยื่อก็ต้องแจ้งตำรวจด้วย

สามารถอ่านรายงาน Q3 IT threat evolution ของแคสเปอร์สกี้ แลป ฉบับเต็ม ได้ที่

IT threat evolution Q3 2018. Statistics