ด่วน! WannaCry แรง ร้าย กระจายทั่วโลก
แคสเปอร์สกี้ แลป เตือนถ้าไม่อยากร้องไห้ ต้องรีบหยุดมัน!

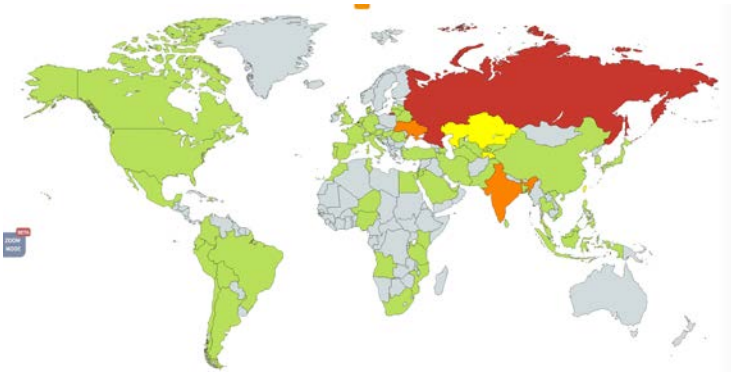
เพียงไม่กี่วันที่ผ่านมา โทรจันเอ็นคริปเตอร์ที่ชื่อ WannaCry ได้เริ่มระบาดและแพร่กระจายไปทั่วโลก **คอสติน ไรอู ผู้อำนวยการทีมวิเคราะห์และวิจัยของแคสเปอร์สกี้ แลป (ทีม GReAT)** ระบุว่า ผู้เชี่ยวชาญตรวจพบเหตุการณ์โจมตีมากกว่า 45,000 รายการ ซึ่งจริงๆ แล้ว มีจำนวนมากกกว่านั้นแน่นอน

เกิดอะไรขึ้นกันแน่?

องค์กรขนาดใหญ่จำนวนมากต่างก็แจ้งการติดเชื้อเข้ามาอย่างต่อเนื่อง หนึ่งในนั้นคือโรงพยาบาลในอังกฤษที่ต้องหยุดการดำเนินงานทั้งหมด พบว่ามีเครื่องคอมพิวเตอร์ที่ติดเชื้อ Wannacry แล้วมากกว่าหนึ่งแสนเครื่องทั่วโลก

การโจมตีส่วนมากเกิดขึ้นในรัสเซีย แต่ที่ยูเครน อินเดีย และไต้หวัน ก็เสียหายมหาศาลเช่นเดียวกัน ในวันแรกของการโจมตี พบว่า มีประเทศที่ได้รับความเสียหายมากถึง 74 ประเทศ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ของสเปน (CCN-CERT) ออกประกาศแจ้งเตือนพร้อมระบุว่า การโจมตีแรนซัมแวร์ครั้งใหญ่นี้ส่งผลกระทบต่อองค์กรมากมายหลายแห่งในสเปน สำนักงาน การบริการด้านสุขภาพแห่งชาติ ของสหราชอาณาจักร รออกประกาศยอมรับว่า สถาบันสุขภาพ 16 แห่งติดเชื้อแรนซัมแวร์ตัวนี้แล้วเช่นกัน



WannaCry คืออะไร

WannaCry แบ่งเป็น 2 ส่วน ส่วนแรก คือเป็นเอ็กพลอต์ที่มีจุดประสงค์เพื่อการติดเชื้อและแพร่กระจาย ส่วนที่สองคือส่วนที่เป็นเอ็นคริปเตอร์ที่ถูกดาวน์โหลดลงคอมพิวเตอร์หลังจากที่ติดเชื้อแล้ว ซึ่งนับเป็นลักษณะที่แตกต่างชัดเจนระหว่าง WannaCry กับเอ็นคริปเตอร์ตัวอื่นๆ ในการทำให้คอมพิวเตอร์ติดเชื้อด้วยเอ็นคริปเตอร์ธรรมดานั้น ยูสเซอร์จะต้องทำพลาด เช่น กด link น่าสงสัย ปล่อยในไมโครซอฟท์เวิร์ดรันมาโครแปลกปลอม หรือดาวน์โหลดไฟล์แนบน่าสงสัยจากอีเมล แต่สำหรับ WannaCry แล้ว ระบบคอมพิวเตอร์สามารถติดเชื้อได้ โดยไม่ต้องทำอะไรเลย

WannaCry เอ็กพลอต์และการแพร่กระจาย

ผู้คิดคัร WannaCry ได้ใช้ประโยชน์จากวินโดวส์เอ็กพลอต์ที่ชื่อว่า “EternalBlue” ซึ่งมีช่องโหว่ที่ไมโครซอฟท์ได้แพทช์ไว้ในซีเคียวริตี้อัพเดท MS17-010 วันที่ 14 มีนาคม 2017 การใช้เอ็กพลอต์นี้ จะสามารถรีโมทแอคเซสเข้าคอมพิวเตอร์และติดตั้งเอ็นคริปเตอร์ได้ทันที

ถ้ายูสเซอร์อัพเดทแล้ว ช่องโหว่นี้ก็จะหายไป ไม่สามารถโดนรีโมทแอคเซสเข้ามาได้ แต่ผู้เชี่ยวชาญของ GReAT ระบุว่า การแพทช์ช่องโหว่ไม่สามารถขัดขวางวิธีการอื่นๆ ของเอ็นคริปเตอร์ได้ ถ้ายูสเซอร์ทำพลาดอย่างที่กล่าวไว้ข้างต้น แพทช์ก็จะไม่ช่วยอะไร

เมื่อแฮกเข้าเครื่องได้สำเร็จ WannaCry จะพยายามแพร่กระจายตัวเองไปยังคอมพิวเตอร์เครื่องอื่นทั่วเน็ตเวิร์กในแบบเวิร์ม ตัวเอ็นคริปเตอร์จะสแกนหาคอมพิวเตอร์ที่มีช่องโหว่เดียวกันเพื่อเอ็กพลอต์โดยอาศัย “EternalBlue” และโจมตีด้วยการเอ็นคริปต์ไฟล์ในเครื่อง

ผู้เชี่ยวชาญพบว่า ตอนที่ WannaCry ทำให้เครื่องคอมพิวเตอร์ติดเชื้อ อาจจะแพร่ไปถึงเน็ตเวิร์กแลนทั้งระบบ และเอ็นคริปต์คอมพิวเตอร์ทุกเครื่องในเน็ตเวิร์กได้ ยิ่งเหยื่อเป็นบริษัทขนาดใหญ่มากเท่าใด มีคอมพิวเตอร์จำนวนมากแค่ไหน ก็จะยิ่งเสียหายมากขึ้นเท่านั้น

WannaCry ตัวเอ็นคริปเตอร์

ตัวเอ็นคริปเตอร์ของ WannaCry มีชื่อเรียกว่า WCrypt or WannaCry Decryptor (ชื่อหลอกว่าดีคริปเตอร์ แต่จริงๆ คือเป็นตัวเอ็นคริปเตอร์) ทำงานเหมือนเอ็นคริปเตอร์ตัวอื่นๆ คือการเข้ารหัสไฟล์ในคอมพิวเตอร์และเรียกร้องให้จ่ายเงินค่าไถ่เพื่อถอดรหัสคืนให้

WannaCry เข้ารหัสไฟล์ได้หลายประเภท รวมถึงไฟล์เอกสารไมโครซอฟท์ออฟฟิศ รูปภาพ วิดีโอ และไฟล์อื่นๆ ที่เก็บข้อมูลสำคัญของยูสเซอร์ เมื่อเข้ารหัสแล้วจะเปลี่ยนนามสกุลไฟล์เป็น .WCRY และยูสเซอร์ไม่สามารถเปิดไฟล์นั้นได้อีก จากนั้น ตัวโทรจันก็จะเปลี่ยนภาพบนหน้าจอเดสท็อปเป็นข้อมูลการติดเชื้อและขั้นตอนให้ยูสเซอร์ทำตามหากต้องการได้ไฟล์คืน นอกจากนี้ ยังส่งไฟล์ข้อความระบุคำเตือนเดียวกันนี้ไปยังโฟลเดอร์ต่างๆ เพื่อให้มั่นใจว่ายูสเซอร์จะต้องเห็นข้อความเรียกค่าไถ่นี้แน่นอน

โดยทั่วไปโจรไซเบอร์จะเรียกเงินค่าไถ่เป็นเงินบิตคอยน์ ค่าไถ่เริ่มต้นจะกำหนดไว้ที่ $300 แต่มักจะเพิ่มเงินค่าไถ่ขึ้นอีกเรื่อยๆ ล่าสุด WannaCry เรียกค่าไถ่สูงถึง $600 หรือประมาณ 20,000 บาท นอกจากนี้ยังขู่ว่าต้องจ่ายเงินค่าไถ่ภายใน 3 วัน และจะถอดรหัสไฟล์ให้ใน 7 วัน แคสเปอร์สกี้ แลป ไม่แนะนำให้ยูสเซอร์จ่ายค่าไถ่เป็นอันขาด เนื่องจากไม่มีอะไรรับประกันได้เลยว่า โจรไซเบอร์จะถอดรหัสไฟล์ให้ตามที่บอก และยังพบเหตุการณ์ที่โจรไซเบอร์ลบข้อมูลยูสเซอร์ทิ้งทำให้ไม่สามารถถอดรหัสไฟล์ได้เลย