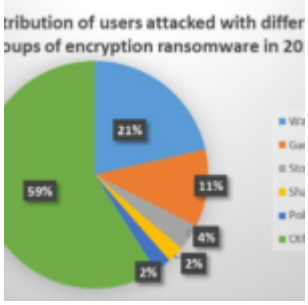
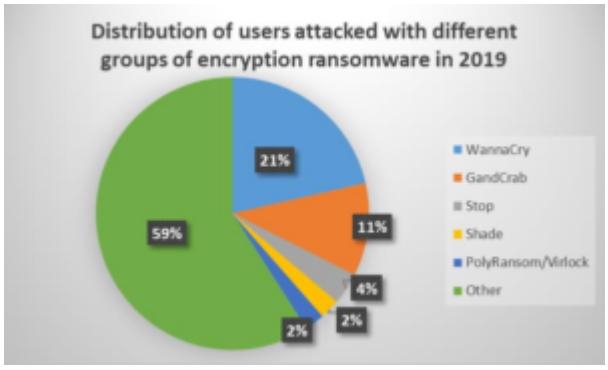
Kaspersky จับมือ INTERPOL กระตุ้นเตือนองค์กรธุรกิจให้ป้องกันภัยคุกคามแรนซัมแวร์





ย้อนอดีตวันที่ 12 พฤษภาคม 2017 เกิดภัยคุกคาม WannaCry ซึ่งเป็นแรนซัมแวร์ระบาดครั้งใหญ่ที่สุดในประวัติศาสตร์ สามปีต่อมา Wannacry และแรนซัมแวร์อื่นๆ ยังคงส่งผลกระทบต่อผู้ใช้และบริษัท การวิจัยล่าสุดของแคสเปอร์สกี้ได้เปิดเผยว่าในปี 2019 WannaCry ยังคงครองตำแหน่งสูงสุดของตระกูลแรนซัมแวร์ที่แพร่หลายที่สุด มีเป้าหมายเกือบหนึ่งในสาม (30%) ของผู้ใช้แรนซัมแวร์เป็นผู้ใช้ระดับองค์กร ในวันที่ 12 พฤษภาคม 2020 แคสเปอร์สกี้และตำรวจสากล หรือ INTERPOL ได้กระตุ้นให้องค์กรพิจารณาเรื่องการสำรองข้อมูลและใช้การป้องกันเพื่อหลีกเลี่ยงการโจมตีด้วยแรนซัมแวร์และไม่ให้ภัยพิบัติที่คล้ายกับ WannaCry ไม่เกิดขึ้นอีก

แรนซัมแวร์เป็นประเด็นความท้าทายที่ยิ่งใหญ่สำหรับหลายๆ องค์กร แม้ว่านี่จะไม่ใช่ภัยคุกคามขั้นสูงสุดจากมุมมองทางเทคนิค แต่อาชญากรไซเบอร์ก็สามารถสกัดกั้นการดำเนินธุรกิจและรีดไถเงินได้ ผลมาจากเหตุการณ์แรนซัมแวร์ในปี 2019 องค์กรต่างๆ เสียหายโดยเฉลี่ย 1.46 ล้านเหรียญสหรัฐ ซึ่งรวมถึงค่าใช้จ่ายสำหรับการหยุดทำงาน ค่าปรับและการเสียชื่อเสียง การโจมตีของ WannaCry นั้นเป็นสิ่งที่เห็นได้ชัดเจนมากที่สุด และแพร่กระจายด้วยความช่วยเหลือของอาวุธไซเบอร์ขั้นสูงคือ EternalBlue ซึ่งเป็นช่องโหว่ที่ซับซ้อนและมีประสิทธิภาพ เป็นผลให้ WannaCry ทำให้เกิดการแพร่ระบาดทางไซเบอร์ทั่วโลกอย่างแท้จริง

จากการวิจัยของแคสเปอร์สกี้ พบว่ามีผู้ใช้งานรวม 767,907 คนถูกจู่โจมโดยเอ็นคริปเตอร์ในปี 2019 โดยเกือบหนึ่งในสาม (30%) เป็นองค์กรธุรกิจ โดยในบรรดาเอ็นคริปเตอร์ทุกตระกูลพบ WannaCry มากที่สุด ในปี 2019

WannaCry โจมตีผู้ใช้ 164,433 รายคิดเป็น 21% ของการโจมตีที่ตรวจพบทั้งหมด ตามมาด้วยแรนซัมแวร์อื่น ๆ เช่น GandCrab (11%) และ Stop (4%) แรนซัมแวร์ GandCrab เป็น ransomware-as-a-service ที่รู้จักกันดีที่พัฒนาโดยทีมอาชญากรทำงานมานานหลายปี ส่วนแรนซัมแวร์ Stop เป็นภัยคุกคามที่รู้จักกันดีผ่านซอฟต์แวร์ เว็บไซต์ และแอดแวร์ที่ถูกบุกรุก

นายเซอร์เจย์ มาร์ตซินค์แยน หัวหน้าฝ่ายการตลาดผลิตภัณฑ์ B2B ของแคสเปอร์สกี้ กล่าวว่า “การแพร่ระบาดของ WannaCry ทำให้บริษัทต่างๆ สูญเสียเงินหลายล้านอันเนื่องมาจากการหยุดทำงานหรือค่าใช้จ่ายที่เกี่ยวข้องกับความเสียหายด้านชื่อเสียง ซึ่งเป็นตัวอย่างที่แสดงให้เห็นถึงสิ่งที่สามารถเกิดขึ้นได้หากแรนซัมแวร์เกิดขึ้นในวงกว้าง ภัยคุกคามยังคงอยู่ในปัจจุบัน เนื่องจากจะมีผู้ใช้งานซึ่งอาจยังไม่ทราบถึงภัยร้ายมากนักและอาจตกเป็นเหยื่อได้ ข่าวดีก็คือว่าวิธีการรักษาความปลอดภัยที่ถูกต้องและมาตรการป้องกันสามารถทำให้แรนซัมแวร์กลายเป็นภัยคุกคามที่ไม่วิกฤตอีกต่อไป และเราต้องการให้ ‘Anti-Ransomware Day’ ในวันที่ 12 พฤษภาคมเป็นวันที่องค์กรธุรกิจและผู้ใช้ทั่วโลกไม่ต้องเผชิญกับปัญหาแรนซัมแวร์อีกต่อไป”

มาตรการแนะนำจากผู้เชี่ยวชาญเพื่อช่วยให้องค์กรธุรกิจปลอดภัยจากแรนซัมแวร์ ดังนี้

• อธิบายให้พนักงานฟังว่าการปฏิบัติตามกฎง่ายๆ สามารถช่วยให้บริษัทหลีกเลี่ยงเหตุการณ์ที่เกิดจากการเรียกค่าไถ่ได้อย่างไร หลักสูตรการฝึกอบรมเฉพาะทางสามารถช่วยได้ เช่น แพลตฟอร์ม Kaspersky Automated Security Awareness Platform
• ทำสำเนาสำรองไฟล์ใหม่อยู่เสมอเพื่อใช้แทนที่ไฟล์กรณีที่ไฟล์สูญหาย (จากมัลแวร์หรืออุปกรณ์ที่เสียหาย) และจัดเก็บไฟล์ทั้งในอุปกรณ์จัดเก็บและบนคลาวด์ ตรวจสอบให้แน่ใจว่าคุณสามารถเข้าถึงได้อย่างรวดเร็วในกรณีฉุกเฉินเมื่อจำเป็น
• จำเป็นต้องติดตั้งการปรับปรุงความปลอดภัยทั้งหมดทันทีที่พร้อมใช้งาน อัปเดตระบบปฏิบัติการและซอฟต์แวร์เพื่อกำจัดช่องโหว่ล่าสุด
• ลองใช้เครื่องมือฟรี Kaspersky Anti-Ransomware Tool for Business ป้องกันแรนซัมแวร์และภัยคุกคามอื่นๆ จากการโจมตีช่องโหว่ในซอฟต์แวร์และแอปพลิเคชัน
• หากอุปกรณ์ขององค์กรถูกเข้ารหัส โปรดจำไว้ว่าแรนซัมแวร์เป็นความผิดทางอาญา คุณไม่ควรจ่ายค่าไถ่ตามความต้องการของผู้โจมตี หากคุณตกเป็นเหยื่อการโจมตีให้รายงานต่อหน่วยงานบังคับใช้กฎหมายในท้องที่ของคุณ และลองค้นหาตัวถอดรหัสบนอินเทอร์เน็ตก่อน บางตัวมีให้ใช้งานฟรีที่เว็บ
https://www.nomoreransom.org/en/index.html
ข้อมูลเพิ่มเติม
• รายงานการสรุปเรื่องแรนซัมแวร์โดยผู้เชี่ยวชาญของแคสเปอร์สกี้:
https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2020/05/12075747/KSN-article_Ransomware-in-2018-2020-1.pdf

• แคสเปอร์สกี้จัดทำวิดีโอเกี่ยวกับ WannaCry การค้นพบ การสกัดกั้น รวมถึงบทสัมภาษณ์พิเศษของผู้เชี่ยวชาญที่

ค้นพบ killswitch ในซอร์สโค้ด: