แคสเปอร์สกี้เผย พบกลุ่มแรนซัมแวร์จ้องโจมตีองค์กรในอาเซียน

หากจะมีเรื่องดีอย่างหนึ่งที่เกิดจากสถานการณ์ COVID-19 ในภูมิภาคเอเชียตะวันออกเฉียงใต้ นั่นก็คือการพิสูจน์ว่าภูมิภาคนี้มีความสามารถในการรองรับดิจิทัล งานวิจัยในปี 2020 ที่จัดทำโดยแคสเปอร์สกี้ที่สำรวจผู้ตอบแบบสอบถาม 760 คนในภูมิภาคนี้ พบว่าเกือบ 8 ใน 10 คนกำลังทำงานจากที่บ้าน

การเพิ่มเวลาอีกสองถึงห้าชั่วโมงจากค่าเฉลี่ยการท่องเว็บ 8 ชั่วโมงต่อวันของผู้บริโภคในภูมิภาคนี้ ในด้านการเงิน พบว่าผู้ตอบแบบสอบถาม 47% ได้เปลี่ยนไปชำระเงินและการทำธุรกรรมทางธนาคารทางออนไลน์เนื่องจากการล็อกดาวน์และการระวังด้านความปลอดภัยในแต่ละประเทศ

เทคโนโลยีและเวิลด์ไวด์เว็บกำลังก้าวขึ้นเป็นเครื่องมือที่มีประสิทธิภาพซึ่งทุกคนสามารถใช้ประโยชน์ได้เพื่อความอยู่รอดในช่วงเวลานี้ อย่างไรก็ตามการพึ่งพาอินเทอร์เน็ตที่เพิ่มขึ้นยังเปิดช่องโหว่ที่อาชญากรไซเบอร์สามารถใช้ประโยชน์ได้มากขึ้น ด้วยผลพวงจากการแพร่ระบาดทางดิจิทัลและสถานการณ์ทางภูมิรัฐศาสตร์ในภูมิภาคนี้ แคสเปอร์สกี้เปิดเผยว่าปัจจัยทั้งสองนี้ได้เปลี่ยนแปลงภูมิทัศน์ของภัยคุกคามในภูมิภาคไปอย่างไร

นายวิทาลี คัมลัก ผู้อำนวยการทีมวิเคราะห์และวิจัยของแคสเปอร์สกี้ ภูมิภาคเอเชียแปซิฟิก กล่าวว่า “ปี 2020 ไม่เหมือนปีอื่นๆ เป็นเวลาแห่งการเปลี่ยนแปลง และยังเป็นการเปลี่ยนแปลงเวลาอีกด้วย วิธีการเดินทาง วิธีที่เราซื้อสินค้า วิธีที่เรามีปฏิสัมพันธ์ซึ่งกันและกันนั้นเปลี่ยนไป รูปแบบภัยคุกคามทางคอมพิวเตอร์ก็มีการพัฒนาตั้งแต่เริ่มมี COVID-19”

“ก่อนหน้านี้เราระมัดระวังในการปรับปรุงระบบให้ทันสมัยเพื่อไม่ให้ตกเป็นเหยื่อของการแพร่ระบาดของ

คอมพิวเตอร์เวิร์มอย่าง WannaCry ในปี 2017 ซึ่งส่งผลกระทบต่อคอมพิวเตอร์หลายแสนเครื่องใน 150 ประเทศ เป็นอย่างน้อย ในช่วงเดือนกุมภาพันธ์ – มีนาคม 2020 เราได้เห็นแคมเปญฟิชชิ่งที่เกี่ยวข้องกับการแพร่ระบาดของโรคระบาด ซึ่งก่อนหน้านี้ทางแคสเปอร์สกี้ได้พูดถึงไปแล้ว แต่รูปแบบภัยคุกคามบางครั้งก็พัฒนาในรูปแบบที่คาดเดาไม่ได้” นายวิทาลีกล่าวเสริม

การเพิ่มขึ้นของแรนซัมแวร์แบบพุ่งเป้าโจมตี

นายวิทาลีเปิดเผยว่า อาชญากรไซเบอร์ได้เพิ่มการแบล็กเมล์ เพื่อให้แน่ใจว่าเหยื่อการโจมตีจะจ่ายค่าไถ่อย่างแน่นอน และยืนยันว่ากลุ่มแรนซัมแวร์ตัวสำคัญในภูมิภาคนี้ได้พุ่งเป้าโจมตีอุตสาหกรรมดังต่อไปนี้

- รัฐวิสาหกิจ
- การบินอวกาศและวิศวกรรม
- การผลิตและค้าเหล็กแผ่น
- บริษัทเครื่องดื่ม
- ผลิตภัณฑ์จากปาล์ม
- บริการโรงแรมและที่พัก
- บริการไอที

ในบรรดาตระกูลแรนซัมแวร์ที่โด่งดังและเป็นหนึ่งในกลุ่มแรกที่ดำเนินการดังกล่าวคือตระกูล Maze กลุ่มที่อยู่เบื้องหลังแรนซัมแวร์ Maze ได้ปล่อยข้อมูลของเหยื่อที่ไม่ยอมจ่ายค่าไถ่มากกว่าหนึ่งครั้ง ผู้ก่อภายคุกคามนี้ได้ปล่อยข้อมูลภายในจำนวน 700MB ทางออนไลน์ในเดือนพฤศจิกายน 2019 พร้อมคำเตือนเพิ่มเติมว่าเอกสารที่เผยแพร่เป็นเพียง 10% ของข้อมูลที่ขโมยมาได้

ยิ่งไปกว่านั้น ผู้ก่อภัยคุกคามนี้ยังได้สร้างเว็บไซต์ที่เปิดเผยตัวตนของเหยื่อ ตลอดจนรายละเอียดของการโจมตี เช่น วันที่ติดไวรัส จำนวนข้อมูลที่ถูกขโมย ชื่อเซิร์ฟเวอร์ และอื่นๆ ย้อนกลับไปในเดือนมกราคม กลุ่มนี้มีส่วนเกี่ยวข้องกับคดีความกับบริษัทผู้ผลิตสายเคเบิล ซึ่งส่งผลให้เว็บไซต์ต้องปิดตัวลง

กระบวนการโจมตีที่กลุ่มนี้ใช้นั้นง่ายมาก โดยจะแทรกซึมเข้าไปในระบบและมองหาข้อมูลที่ละเอียดอ่อนที่สุด จากนั้นอัปโหลดไปยังที่เก็บข้อมูลบนคลาวด์ หลังจากนั้น ข้อมูลเหล่านี้จะถูกเข้ารหัสด้วย RSA จะมีการเรียกค่าไถ่ตามขนาดของบริษัทและปริมาณข้อมูลที่ขโมยไป จากนั้นกลุ่มนี้จะเผยแพร่รายละเอียดในบล็อก และแนะนำวิธีการแก่นักข่าว

นายวิทาลีกล่าวว่า “เรากำลังตรวจสอบการตรวจจับแรนซัมแวร์ Maze ทั่วโลก รวมถึงบริษัทจำนวนหนึ่งในเอเชียตะวันออกเฉียงใต้ การโจมตีที่สร้างความอับอายในวงกว้างเพิ่มแรงกดดันในการยอมทำตามข้อเรียกร้องของอาชญากรไซเบอร์ ผมขอแนะนำบริษัทและองค์กรต่างๆ ว่าอย่าจ่ายค่าไถ่ และให้แจ้งข้อมูลแก่หน่วยงานบังคับใช้

กฎหมายและผู้เชี่ยวชาญในสถานการณ์ดังกล่าว โปรดจำไว้ว่าการสำรองข้อมูลสามารถป้องกันความปลอดภัยในโลกไซเบอร์ของคุณได้ เพื่อหลีกเลี่ยงการตกเป็นเหยื่อของผู้กระทำร้ายเหล่านี้”

เพื่อเสริมเกราะป้องกันองค์กรและเอ็นเทอร์ไพรซ์ นายวิทาลีขอแนะนำดังต่อไปนี้

- ก้าวนำหน้าศัตรู: ด้วยการสำรองข้อมูล จำลองการโจมตี เตรียมแผนปฏิบัติการสำหรับการกู้คืนจากภัยพิบัติ
- ปรับใช้เซ็นเซอร์ทุกที่: ตรวจสอบกิจกรรมของซอฟต์แวร์บนเครื่องเอ็นด์พอยต์ บันทึกการใช้งาน ตรวจสอบความสมบูรณ์ของฮาร์ดแวร์
- อย่าทำตามความต้องการของอาชญากร อย่าต่อสู้เพียงลำพัง: ติดต่อหน่วยงานบังคับใช้กฎหมาย หน่วยงาน CERT และผู้ให้บริการโซลูชั่นความปลอดภัย เช่น แคสเปอร์สกี้
- ฝึกอบรมพนักงานเมื่อต้องทำงานจากระยะไกล: นิติดิจิทัล การวิเคราะห์มัลแวร์ขั้นพื้นฐาน การประชาสัมพันธ์เพื่อจัดการวิกฤต
- ติดตามแนวโน้มล่าสุด โดยการสมัครรับข้อมูลภัยคุกคามระดับพรีเมียม เช่น Kaspersky APT Intelligence Service
- รู้จักศัตรู: ระบุมัลแวร์ใหม่ที่ยังตรวจไม่พบด้วย Kaspersky Threat Attribution Engine