วันที่ 5 พฤษภาคม 2569

VECT 2.0 Ransomware ทำลายไฟล์ที่มีขนาดเกิน 131KB แบบถาวรบน Windows, Linux และ ESXi

นักล่าภัยคุกคาม (Threat hunters) ออกมาเตือนว่า ปฏิบัติการอาชญากรรมไซเบอร์ที่ชื่อว่า VECT 2.0 มีพฤติกรรมคล้ายกับมัลแวร์ล้างข้อมูล (wiper) มากกว่า ransomware เนื่องจากมีข้อผิดพลาดร้ายแรงในกระบวนการเข้ารหัส ที่ส่งผลให้ไม่สามารถกู้คืนไฟล์ได้เลย ทั้งในเวอร์ชัน Windows, Linux และ ESXi

ประเด็นสำคัญคือ ตัวล็อกไฟล์ของ VECT ไม่ได้แค่เข้ารหัสไฟล์ แต่กลับ “ทำลายไฟล์ขนาดใหญ่แบบถาวร” ซึ่งหมายความว่า แม้เหยื่อจะยอมจ่ายค่าไถ่ ก็ไม่สามารถกู้ข้อมูลกลับมาได้ เพราะกุญแจถอดรหัสถูกทิ้งไปตั้งแต่ตอนที่มัลแวร์ทำงานแล้ว โดย VECT ถูกนำเสนอว่าเป็น ransomware แต่สำหรับไฟล์ที่มีขนาดเกิน 131KB ซึ่งเป็นไฟล์ส่วนใหญ่ที่องค์กรให้ความสำคัญ มันทำงานเหมือนเครื่องมือทำลายข้อมูลมากกว่า Eli Smadja ผู้จัดการกลุ่มจาก Check Point Research กล่าว

คำแนะนำสำหรับผู้บริหารและองค์กร

CISO ต้องเข้าใจว่า ในกรณีที่เจอ VECT การจ่ายเงินไม่ใช่ทางออกในการกู้ข้อมูล เพราะไม่มีเครื่องมือถอดรหัสให้ใช้งาน ไม่ใช่เพราะคนร้ายไม่ยอมให้ แต่เพราะข้อมูลที่ใช้สร้างตัวถอดรหัสถูกทำลายไปแล้วตั้งแต่ต้น

สิ่งที่ควรโฟกัสคือการเตรียมความพร้อม เช่น การมีแบ็กอัพแบบออฟไลน์ การทดสอบแผนกู้คืน และการควบคุมเหตุการณ์ให้เร็วที่สุด ไม่ใช่การเจรจา

โมเดลธุรกิจของ VECT 2.0 และความเชื่อมโยงกับ Dark Web

VECT (ซึ่งตอนนี้รีแบรนด์เป็น VECT 2.0) เป็นรูปแบบ ransomware-as-a-service (RaaS) ที่เริ่มเปิดโปรแกรม affiliate ตั้งแต่เดือนธันวาคม 2025 บนเว็บไซต์มืดของกลุ่ม มีข้อความว่า “Exfiltration / Encryption / Extortion” ซึ่งแสดงถึงโมเดลโจมตีแบบครบวงจรทั้งขโมยข้อมูล เข้ารหัส และเรียกค่าไถ่

จากการวิเคราะห์ของ Data Security Council of India (DSCI) พบว่า ผู้ที่ต้องการเข้าร่วมต้องจ่ายค่าสมัคร 250 ดอลลาร์ ด้วย Monero (XMR) แต่จะยกเว้นค่าธรรมเนียมสำหรับผู้สมัครจากประเทศในกลุ่ม CIS ซึ่งบ่งบอกว่ากลุ่มนี้พยายามดึงคนจากภูมิภาคนั้นเข้ามาร่วม

ในช่วงไม่กี่สัปดาห์ที่ผ่านมา กลุ่มนี้ยังได้ร่วมมือกับฟอรั่มอาชญากรรมไซเบอร์ BreachForums และกลุ่มแฮ็กเกอร์ TeamPCP เพื่อทำให้การโจมตีทำได้ง่ายขึ้น และกระตุ้นให้ affiliate นำข้อมูลที่ขโมยมาแล้วไปใช้โจมตีต่อ

การรวมกันของการขโมยข้อมูล credentials ในระดับซัพพลายเชน การเติบโตของ RaaS และการระดมคนจาก dark web ถือเป็นโมเดลใหม่ของ ransomware ที่ถูกทำให้เป็นอุตสาหกรรมอย่างเต็มรูปแบบ Dataminr กล่าว แม้จะมีความร่วมมือและภาพลักษณ์ที่ดูใหญ่โต แต่เว็บไซต์เปิดเผยข้อมูลเหยื่อ (data leak site) ของกลุ่มนี้ยังมีเพียง 2 ราย และทั้งคู่ถูกโจมตีผ่านช่องทาง supply chain ของ TeamPCP

เจาะลึกข้อผิดพลาดทางเทคนิค (Technical Flaws)

นอกจากนี้ ยังพบว่าระบบเข้ารหัสไม่ได้ใช้ ChaCha20-Poly1305 ตามที่อ้าง แต่ใช้วิธีที่อ่อนแอกว่าและไม่มีการตรวจสอบความถูกต้องของข้อมูล (integrity protection)

ปัญหาใหญ่ที่สุดคือ โค้ด C++ ของตัวมัลแวร์ในทุกแพลตฟอร์มมีข้อผิดพลาดพื้นฐาน ที่ทำให้ไฟล์ที่มีขนาดเกิน 131,072 ไบต์ถูกทำลายแบบถาวร แทนที่จะถูกเข้ารหัส Check Point อธิบายว่า มัลแวร์จะเข้ารหัสไฟล์ขนาดใหญ่โดยแบ่งเป็น 4 ส่วน และใช้ nonce (ค่าตัวเลขสุ่ม) 4 ค่า แต่จะบันทึกไว้เพียงค่าเดียวในไฟล์ ส่วนอีก 3 ค่าที่จำเป็นต่อการถอดรหัส ถูกสร้างขึ้น ใช้งานแล้วทิ้งทันที ไม่ได้เก็บไว้ที่ไหนเลย

เนื่องจากการถอดรหัสต้องใช้ทั้งกุญแจ 32 ไบต์ และ nonce ที่ตรงกัน ไฟล์ส่วนใหญ่ (3 ใน 4) จึงไม่สามารถกู้คืนได้ ไม่ว่าใครก็ตาม รวมถึงตัวคนร้ายเองด้วย ดังนั้นในทางปฏิบัติ VECT 2.0 จึงเป็นมัลแวร์ทำลายข้อมูล ที่แค่ปลอมตัวเป็น ransomware เท่านั้น

พฤติกรรมของมัลแวร์บนแต่ละแพลตฟอร์ม

เวอร์ชัน Windows: มัลแวร์สามารถเข้ารหัสไฟล์ในเครื่อง, อุปกรณ์ภายนอก และเครือข่ายได้ พร้อมทั้งมีระบบป้องกันการวิเคราะห์ (anti-analysis) ที่ตรวจจับเครื่องมือด้านความปลอดภัยและดีบักกว่า 44 รายการ อีกทั้งยังมีการตั้งค่าให้รันใน Safe Mode และมีสคริปต์สำหรับกระจายตัวในเครือข่าย

เมื่อใช้โหมด “--force-safemode” มัลแวร์จะตั้งค่าให้เครื่องบูตเข้า Safe Mode และเพิ่มตัวเองลงใน Registry เพื่อให้รันอัตโนมัติในโหมดนั้น ซึ่งเป็นสภาพแวดล้อมที่มีการป้องกันน้อยลง อย่างไรก็ตาม ฟีเจอร์ตรวจจับสภาพแวดล้อม (environment detection) ที่มีอยู่ในโค้ด กลับไม่ได้ถูกเรียกใช้งานจริง ทำให้นักวิเคราะห์สามารถรันตัวอย่างมัลแวร์ได้โดยไม่ถูกหลบเลี่ยง

เวอร์ชัน ESXi และ Linux: ในฝั่ง ESXi จะมีการตรวจสอบภูมิภาค (geofencing) และระบบป้องกันการดีบักก่อนเริ่มทำงาน และยังพยายามเคลื่อนที่ในเครือข่ายผ่าน SSH ส่วนเวอร์ชัน Linux ใช้โค้ดเดียวกับ ESXi แต่มีฟังก์ชันน้อยกว่า

ระบบ geofencing จะตรวจสอบว่าระบบอยู่ในประเทศกลุ่ม CIS หรือไม่ หากใช่ จะหยุดการทำงานทันที ซึ่งถือว่าแปลก เพราะ ransomware รุ่นใหม่ส่วนใหญ่มักเลิกใช้วิธีนี้ไปแล้ว Check Point ให้ความเห็นว่า อาจมี 2 สาเหตุ:

1. โค้ดบางส่วนถูกสร้างด้วย AI ที่ใช้ข้อมูลเก่า
2. หรือใช้โค้ด ransomware รุ่นเก่ามาปรับใช้

โดยรวมแล้ว เชื่อว่าผู้พัฒนา VECT เป็นกลุ่มมือใหม่ ไม่ใช่กลุ่มที่มีประสบการณ์สูง และอาจใช้ AI ช่วยเขียนโค้ดบางส่วน VECT 2.0 ดูเหมือนภัยคุกคามที่มีศักยภาพสูง ทั้งรองรับหลายแพลตฟอร์ม มีระบบ affiliate และมีพันธมิตรด้านการโจมตี แต่ในความเป็นจริง การพัฒนายังห่างไกลจากสิ่งที่นำเสนออย่างมาก

ข้อมูลอ้างอิง

Apr 28, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/04/vect-20-ransomware-irreversibly.html