26 มีนาคม 2568

แรนซัมแวร์ VanHelsing ตัวใหม่ ปรากฏตัว โจมตีคอมพิวเตอร์หลากหลายระบบทั่วโลก

Executive Summary

ภัยคุกคามทางไซเบอร์ตัวใหม่ชื่อ VanHelsing ถูกค้นพบเมื่อเร็วๆ นี้ โดยมันถูกออกแบบมาเพื่อโจมตีคอมพิวเตอร์หลายประเภท ไม่ว่าจะเป็นคอมพิวเตอร์ทั่วไป (Windows), เซิร์ฟเวอร์คลาวด์ (Linux, ESXi) และอุปกรณ์ที่ใช้ชิป ARM ซึ่งพบได้ในแท็บเล็ตและเซิร์ฟเวอร์ขนาดเล็ก VanHelsing ปรากฏตัวครั้งแรกในต้นเดือนมีนาคม 2025 และตอนนี้กำลังถูกใช้โจมตีเหยื่อจริงแล้ว

VanHelsing เป็นส่วนหนึ่งของกระแสที่เรียกว่า “Ransomware-as-a-Service” (RaaS) หรือแรนซัมแวร์แบบให้บริการ หมายความว่า ผู้พัฒนามัลแวร์นี้จะให้ผู้อื่นหรือที่เรียกว่า “พันธมิตร” เช่าเครื่องมือนี้ไปใช้โจมตีองค์กรต่างๆ โดยรายได้จากค่าไถ่จะถูกแบ่งกัน—ผู้พัฒนาได้รับ 20% และพันธมิตรได้ 80% หากผู้ใช้งานเป็นมือใหม่จะต้องวางเงินมัดจำ 5,000 ดอลลาร์ แต่ถ้าเป็นแฮกเกอร์ที่มีประสบการณ์จะสามารถเข้าร่วมได้ฟรี

กลุ่มผู้อยู่เบื้องหลัง VanHelsing เชื่อว่ามีถิ่นฐานในประเทศ รัสเซีย และมีการตั้งกฎห้ามโจมตีประเทศในกลุ่มเครือรัฐเอกราช (CIS) จนถึงขณะนี้ มีเหยื่อที่ปรากฏในเว็บไซต์ของกลุ่มแล้ว 3 ราย ได้แก่ หน่วยงานท้องถิ่นในรัฐ เท็กซัส สหรัฐอเมริกา และบริษัทด้านเทคโนโลยีอีกสองแห่งใน สหรัฐฯ และฝรั่งเศส ซึ่งแต่ละรายถูกเรียกค่าไถ่สูงถึง 500,000 ดอลลาร์ โดยผู้โจมตีขู่ว่าจะเผยแพร่ข้อมูลหากไม่จ่าย

สิ่งที่ทำให้ VanHelsing น่ากลัวคือ ความสามารถในการซ่อนตัวจากระบบรักษาความปลอดภัย ปกติแรนซัมแวร์จะเปลี่ยนชื่อไฟล์หลังจากเข้ารหัส แต่ VanHelsing สามารถทำงานแบบที่เรียกว่า โหมดลับ ได้ โดยแยกขั้นตอนการเข้ารหัสออกจากการเปลี่ยนชื่อไฟล์ ทำให้ยากต่อการตรวจจับโดยซอฟต์แวร์ป้องกันไวรัส

แม้ว่าจะยังมีข้อผิดพลาดบางอย่างในการเขียนโค้ด แต่ผู้เชี่ยวชาญด้านความปลอดภัยเตือนว่า VanHelsing เป็น ภัยคุกคามที่มีความซับซ้อนและพัฒนาอย่างรวดเร็ว มีแนวโน้มสูงว่าจะถูกนำไปใช้ในวงกว้างมากขึ้นในอนาคต

Preventative Measures & Takeaways

1. อัปเดตระบบอย่างสม่ำเสมอ ทั้งคอมพิวเตอร์และเซิร์ฟเวอร์ ควรติดตั้งแพตช์ความปลอดภัยทันทีเมื่อมีออกมา
2. สำรองข้อมูลอย่างสม่ำเสมอ โดยควรเก็บไว้แบบออฟไลน์หรือในคลาวด์ที่ปลอดภัย
3. อบรมพนักงาน ให้รู้จักหลีกเลี่ยงอีเมลหลอกลวงหรือไฟล์แนบที่น่าสงสัย เพราะเป็นจุดเริ่มต้นของการโจมตีหลายครั้ง
4. ใช้ซอฟต์แวร์ความปลอดภัย เช่น โปรแกรมแอนตี้ไวรัส ระบบตรวจจับภัยคุกคาม และไฟร์วอลล์

Reference information

1. https://www.bleepingcomputer.com/news/security/new-vanhelsing-ransomware-targets-windows-arm-esxi-systems/