แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

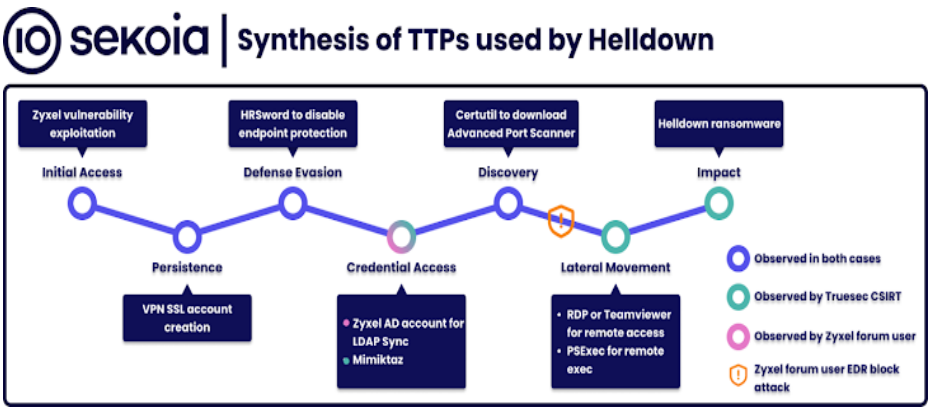
ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน การเฝ้าระวัง Ransomware “Helldown” ที่ใช้ประโยชน์จากช่องโหว่ Zyxel VPN (CVE-2024-42057) โจมตี VMware และ Linux

วันที่แจ้งเตือน 28 พฤศจิกายน 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้เผยแพร่รายงานกรณี Ransomware ใหม่ “Helldown” ที่ใช้ประโยชน์จากช่องโหว่ ของ IPSec VPN บนอุปกรณ์ Zyxel VPN (CVE-2024-42057) เพื่อโจมตีระบบ Vmware และ Linux โดยเว็บไซต์ Halcyon.ai ผู้ให้บริการด้าน anti-ransomware platform รายงานถึงกลุ่มผู้ไม่หวังดี Helldown ที่ active ในช่วงกลางปี 2567 ซึ่งพัฒนาโดยอาศัยโค้ดจาก LockBit 3.0 ซึ่งเน้นโจมตีไปยังระบบ Windows และปัจจุบันกำลังขยายการโจมตีไปที่ระบบ VMware virtual machines (VMs) และ Linux โดยอาศัยช่องโหว่บนอุปกรณ์ Zyxel VPN ข้างต้น ส่งผลให้ผู้ไม่หวังดีสามารถยกระดับสิทธิ ปิดระบบความปลอดภัย และส่งคำสั่งไปยังระบบปฏิบัติการณ์ด้วยบัญชีผู้ใช้งาน (username) ที่สร้างขึ้นใหม่



ภาพ Tactic, Technique & Procedure ที่ Helldown นำมาใช้โจมตี (อ้างอิง 2)

องค์กรจึงควรเฝ้าระวังและดำเนินการรักษาความมั่นคงปลอดภัยให้ยังคงมีประสิทธิภาพ และพิจารณาปิดช่องโหว่บนอุปกรณ์ดังกล่าว เพื่อลดความเสี่ยงที่อาจกระทบทำให้การบริการหยุดชะงักและกระทบต่อผู้ใช้บริการ

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 26 ก.พ. 2567
2) https://thehackernews.com/2024/11/new-helldown-ransomware-expands-attacks.html
3) https://nvd.nist.gov/vuln/detail/cve-2024-42057
4) https://www.halcyon.ai/attacks-news/ransomware-on-the-move-bianlian-helldown-meow-and-ransomhub