แจ้งเตือน : ช่องโหว่

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 กรณีการโจมตีจากกลุ่ม UAC-0125 ผ่านการใช้ Cloudflare Workers เพื่อเผยแพร่มัลแวร์

วันที่แจ้งเตือน 26 ธันวาคม 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้แจ้งเตือนเกี่ยวกับกรณีการโจมตีจากกลุ่ม UAC-0125 ที่ใช้บริการ Cloudflare Workers เพื่อแพร่กระจายมัลแวร์ โดยปลอมแปลงเป็นแอปพลิเคชัน Army+ ซึ่งเป็นแอปพลิเคชันที่พัฒนาโดยกระทรวงกลาโหมยูเครน

ทีม Computer Emergency Response Team of Ukraine (CERT-UA) ได้รายงานว่า การโจมตีนี้มีความซับซ้อน เนื่องจากผู้โจมตีสร้างเว็บไซต์ปลอมบน Cloudflare Workers ที่มีลักษณะเหมือนเว็บไซต์ทางการ เพื่อหลอกให้ผู้ใช้ดาวน์โหลดไฟล์ที่มีชื่อคล้ายแอปพลิเคชันจริง เมื่อเปิดไฟล์ดังกล่าว มัลแวร์จะติดตั้ง OpenSSH และสร้างช่องที่ทำให้ผู้โจมตีสามารถเข้าถึงเครื่องคอมพิวเตอร์ของเหยื่อได้จากระยะไกล ทำให้สามารถเข้าถึงข้อมูลสำคัญ ควบคุมระบบ และใช้เครื่องคอมพิวเตอร์ของเหยื่อเป็นฐานในการโจมตีต่อไปได้

ผู้ดูแลระบบอาจสามารถสแกนหา Indicators of Compromise (IOC) ที่เกี่ยวข้องกับการโจมตีจาก ช่องโหว่ดังกล่าว

Type of IOC	IOC
File	Filename: ArmyPlusInstaller-v.0.10.23672.exe MD5: 0799756f104a70cb6ce0cfc422de25db SHA-256: d2049157980b7ee0a54948d4def4ab62303ca51cadaada06fb5 1c583ecbce1a2 Filename: ArmyPlusInstaller-v.0.10.23722.exe MD5: a27a90a685dad9fc7f1c5962f278f197 SHA-256: 4dca04f1e16cbe88776a3187031cff64981155cb3b992031250c 6fed40496318 Filename: init.ps1 MD5: 52853b39922251a4166a5b032e577e7a SHA-256: 86039bc8b1a6bb823f5cbf27d1a4a3b319b83d242f09ffcd96f38bbdbbaaa78f Filename: guid.txt MD5: ed0c7c1925ac23bd8b4d09e77aabb0ee SHA-256: 8ba4c3ede1ed05a3ad7075fee503215648ec078a13523492e2e91a59fa40c8da Filename: ArmyPlus.exe (bait) MD5: a2f355057ade20d32afc5c4192ce3986 SHA-256: b663e08cc267cdb7a02d5131cb04b8b05cb6ad13ac1d571c6aaFe69e06bf8f80
Network (for workers [.]dev subdomains are not given)	desktopapluscom.workers[.]dev desktopaplus.workers[.]dev armyplus-desktop.workers[.]dev aplusdesktop.workers[.]dev armylpus.workers[.]dev aplusmodgovua.workers[.]dev wvtmsouaa2gt6jmcuxj5hkfrqdss5lhecoqijt5dl7gfruueu3i5mkad[.]onion

แจ้งเตือน : ช่องโหว่

Alert

ผลกระทบทางธุรกิจ
- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ
- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน กรณีการโจมตีจากกลุ่ม UAC-0125 ผ่านการใช้ Cloudflare Workers เพื่อเผยแพร่มัลแวร์ (ต่อ)

วันที่แจ้งเตือน 26 ธันวาคม 2567

องค์กรควรพิจารณาดำเนินการ ด้วยการตรวจสอบความน่าเชื่อถือของแหล่งที่มาแอปพลิเคชัน ก่อนดำเนินการดาวน์โหลด ควบคู่ไปกับการอัปเดตระบบปฏิบัติการและโปรแกรมป้องกันไวรัสให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ การเสริมสร้างความตระหนักรู้ให้แก่บุคลากรในการเปิดไฟล์หรือลิงก์จากแห่งที่เชื่อถือได้ และหลีกเลี่ยงการรันสคริปต์ หรือโปรแกรมที่ไม่ได้รับการยืนยัน นอกจากนี้ การใช้ระบบยืนยันตัวตนแบบ MFA ในการเข้าถึงระบบ ยังเป็นกลไกที่มีประสิทธิภาพในการเพิ่มระดับการป้องกันความมั่นคงปลอดภัย

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

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 20 ธ.ค. 2567
2) https://thehackernews.com/2024/12/uac-0125-abuses-cloudflare-workers-to.html
3) https://cert.gov.ua/article/6281701