เอกสารการแจ้งเตือนกรณีการโจมตีจากกลุ่ม UAC-0125 ผ่านการใช้ Cloudflare Workers เพื่อเผยแพร่มัลแวร์

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณีการโจมตีจากกลุ่ม UAC-0125 ผ่านการใช้ Cloudflare Workers เพื่อเผยแพร่มัลแวร์

ทีม Computer Emergency Response Team of Ukraine (CERT-UA) ได้เปิดเผยกรณีการโจมตีทางไซเบอร์ที่ดำเนินการโดยกลุ่ม UAC-0125 ซึ่งได้ใช้บริการ Cloudflare Workers เป็นเครื่องมือในการเผยแพร่มัลแวร์ โดยมีเป้าไปที่บุคลากรทางทหารในยูเครน การโจมตีในครั้งนี้เกี่ยวข้องกับการล่อลวงให้เหยื่อดาวน์โหลดมัลแวร์ที่ปลอมเป็นแอปพลิเคชันชื่อ Army+ ซึ่งเดิมพัฒนาโดยกระทรวงกลาโหมยูเครนเพื่อสนับสนุนการทำงานในกองทัพแบบ paperless [1]

CERT-UA ระบุว่า UAC-0125 มีความเชื่อมโยงกับกลุ่ม UAC-0002 ซึ่งเป็นที่รู้จักในชื่อ APT, APT44, FROZENBARENTS, Sandworm, Seashell Blizzard Voodoo Bear โดยมีรายละเอียดการโจมตีดังต่อไปนี้

- การกระจายมัลแวร์: ผู้โจมตีสร้างเว็บไซต์ปลอมที่มีลักษณะคล้ายคลึงกับหน้าเว็บไซต์ทางการของแอปพลิเคชัน "Army+" และโฮสต์ผ่านบริการ Cloudflare Workers เพื่อหลอกลวงให้ผู้ใช้ดาวน์โหลดไฟล์ปฏิบัติการที่เป็นอันตราย

- ไฟล์ที่เป็นอันตราย: ไฟล์ปฏิบัติการที่ดาวน์โหลดมีชื่อว่า "ArmyPlusInstaller-v.0.10.23722.exe" (ชื่อไฟล์อาจแตกต่างกัน) สร้างขึ้นด้วย Nullsoft Scriptable Install System (NSIS) และประกอบด้วยไฟล์.NET ที่เป็น decoy file ชื่อ "ArmyPlus.exe" ไฟล์ตัวแปลภาษา Python ไฟล์โปรแกรม Tor และสคริปต์ PowerShell ชื่อ "init.ps1" [2]

- การดำเนินการของมัลแวร์: เมื่อเปิดไฟล์ดังกล่าวจะมีการรัน decoy file และสคริปต์ PowerShell ที่ติดตั้ง OpenSSH บนเครื่องของผู้ใช้ สร้างคู่กุญแจ RSA เพิ่มกุญแจสาธารณะลงในไฟล์ "authorized_keys" ส่งกุญแจส่วนตัวไปยังเซิร์ฟเวอร์ของผู้โจมตีผ่านคำสั่ง "curl" และเปิดบริการ SSH ที่ซ่อนอยู่ผ่าน Tor ทำให้ผู้โจมตีสามารถเข้าถึงเครื่องของเหยื่อจากระยะไกลได้

ผู้ดูแลระบบอาจสามารถสแกนหา Indicators of Compromise (IOC) ที่เกี่ยวข้องกับการโจมตีจากช่องโหว่ดังกล่าว

Type of IOC	IOC
File	Filename: ArmyPlusInstaller-v.0.10.23672.exe MD5: 0799756f104a70cb6ce0cfc422de25db SHA-256: d2049157980b7ee0a54948d4def4ab62303ca51cadaada06fb51c583ecbce1a2 Filename: ArmyPlusInstaller-v.0.10.23722.exe MD5: a27a90a685dad9fc7f1c5962f278f197 SHA-256: 4dca04f1e16cbe88776a3187031cff64981155cb3b992031250c6fed40496318 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

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้งานใช้หลีกเลี่ยงการดาวน์โหลด และติดตั้งซอฟต์แวร์ที่ไม่ทราบแหล่งที่มา ตรวจสอบความถูกต้องของเว็บไซต์ก่อนทำการดาวน์โหลดแอปพลิเคชัน อัปเดตระบบปฏิบัติการ และซอฟต์แวร์ป้องกันไวรัสให้เป็นเวอร์ชันปัจจุบัน ระมัดระวังการเปิดไฟล์ที่ไม่ทราบแหล่งที่มา และหลีกเลี่ยงการรันสคริปต์ หรือโปรแกรมที่ไม่ได้รับการยืนยัน และสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://thehackernews.com/2024/12/uac-0125-abuses-cloudflare-workers-to.html
2. https://cert.gov.ua/article/6281701