Mphasis
The Next Applied

SPECTR Malware Targets Ukraine Defense Forces in SickSync Campaign

Date: June 9th, 2024 | Severity: High

Summary

SPECTR serves as an information stealer by grabbing screenshots every 10 seconds, harvesting files, gathering data from removable USB drives, and stealing credentials and from web browsers and applications like Element, Signal, Skype, and Telegram.

Attack Vectors

- Attack chains commence with spear-phishing emails containing a RAR self-extracting archive file containing a decoy PDF file, a trojanized version of the SyncThing application that incorporates the SPECTR payload, and a batch script that activates the infection by launching the executable.
- SPECTR serves as an information stealer by grabbing screenshots every 10 seconds, harvesting files, gathering data from removable USB drives, and stealing credentials and from web browsers and applications like Element, Signal, Skype, and Telegram.
- Vermin is also the name assigned to a .NET remote access trojan that has been used to target various Ukrainian government institutions for eight years. It was first publicly reported by Palo Alto Networks Unit 42 in January 2018, with a subsequent analysis from ESET tracing the attacker activity back to October 2015.
- "Upon execution of the Excel document, which contains an embedded VBA Macro, it drops an LNK and a DLL loader file," Broadcom-owned Symantec said. "Subsequently, running the LNK file initiates the DLL loader, potentially leading to a suspected final payload including Agent Tesla, Cobalt Strike beacons, and njRAT."

Indicator of compromise

INDICATOR TYPE	INDICATORS
IPs	• 176[.]119.2.212 • 176[.]119.2.214 • 176[.]119.5.194 • 176[.]119.5.195

URLs	• hxxp://176[.]119.2.212/web/t/data.out • hxxp://getmod[.]host/DSGb3Y3X	• hxxp://getmod[.]host/ThlAHy3S • hxxp://getmod[.]host/OcthdaLm
Domains	• getmod[.]host • syncapp[.]host • netbin[.]host	• stormpredictor[.]host • meteolink[.]host
Hashes	• baf502b4b823b6806cc91e2c1dd07613 • 993415425b61183dd3f900d9b81ac57f • 1c2c41a5a5f89eccafea6e34183d5db9 • d34dbbd28775b2c3a0b55d86d418f293 • 67274bdd5c9537affbd51567f4ba8d5f • 75e1ce42e0892ed04a43e3b68afdbc07 • e08d7c4daa45beca5079870251e50236 • adebdc32ef35209fb142d44050928083 • 3ed8263abe009c19c4af8706d52060f8 • f0197bbb56465b5e2f1f17876c0da5ba • d0632ef34514bbb0f675c59e6ecca717 • 00a54a6496734d87dab6685aa90588f8 • 5db4313b8dbb9204f8f98f2c129fd734 • 32343f2a6b8ac9b6587e2e07989362ab • ecc7bb2e4672b958bd82fe9ec9cfab14	

Recommendation

- Block all threat indicators at your respective controls.
- Maintain cyber hygiene by updating your anti-virus software and implementing a patch management lifecycle.
- Along with network and system hardening, code hardening should be implemented within the organization so that their websites and software are secure. Use testing tools to detect any vulnerabilities in the deployed codes.
- Enable two-factor authentication.
- Emails from unknown senders should always be treated with caution.

Reference Links

- https://thehackernews.com/2024/06/spectr-malware-targets-ukraine-defense.html
- https://securityaffairs.com/164250/intelligence/spectr-malware-used-in-sicksync-campaign.html