Mphasis
The Next Applied

The WineLoader Malware

Date: 27th April 2024 | Severity: Medium

Summary

WineLoader is distributed through malicious documents, often attached to phishing email messages, meticulously crafted to appear as legitimate invitation PDF files with diplomatic-related lures. These documents entice victims into downloading and opening them, facilitating the malware's infiltration of targeted systems. Upon execution, WineLoader compromises the infected system, likely establishing persistence and exfiltrating sensitive data. The malware also employs evasion techniques, such as encryption of strings and command and control (C2) communication.

Attack Vectors

- Researchers are warning that a notorious hacking group linked to Russia's Foreign Intelligence Service (SVR) is targeting political parties in Germany for the first time, shifting their focus away from the typical targeting of diplomatic missions. The phishing attacks are designed to deploy a backdoor malware named WineLoader, which allows threat actors to gain remote access to compromised devices and networks.
- APT29 (also known as Midnight Blizzard, NOBELIUM, Cozy Bear) is a Russian espionage hacking group believed to be part of the Russian Foreign Intelligence Service (SVR). When executed, the Rootsaw malware downloads and executes a backdoor named 'WineLoader' on the victim's computer.
- The WineLoader malware was previously discovered by Zscaler in February, who saw it deployed in phishing attacks pretending to be invites to diplomats for a wine-tasting event. The WineLoader backdoor features several similarities with other malware variants deployed in past APT29 attacks, such as 'burnbatter', 'myskybeat', and 'beatdrop,' suggesting a common developer. However, the malware is modular and more customized than previous variants, does not use off-the-shelf loaders, and establishes an encrypted communication channel for data exchange with the command and control (C2) server.
- Mandiant's analysts first saw WineLoader in late January 2024 in an operation targeting the Czech Republic, Germany, India, Italy, Latvia, and Peru diplomats. Thus, the particular variant appears to have been the malware of choice for APT29 lately. To evade detection, WineLoader is decrypted using RC4 and loaded directly into memory via DLL side-loading, abusing a legitimate Windows executable (sqldumper.exe).

- Wineloader sends the victim's username, device name, process name, and other information to the C2 to help profile the system. The C2 can order the execution of modules that can be dynamically loaded to perform specific tasks, such as establishing persistence. Though Mandiant does not delve into any modules, it is assumed that WineLoader's modular nature allows it to execute a wide range of espionage activities in line with APT29's mission.
- APT29 continues demonstrating its advanced technical proficiency and ongoing efforts to develop tools to infiltrate and spy on targeted entities. The shift to political parties suggests an intent to influence or monitor political processes, possibly reflecting broader geopolitical objectives.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 4866d6994c2f8b4dadfaabc2e2b81bd86c12f68fdf0da13d41d7b0e30bea0801 • 8bd528d2b828c9289d9063eba2dc6aa0 • 7a465344a58a6c67d5a733a815ef4cb7 • 44ce4b785d1795b71cee9f77db6ffe1b • efafcd00b9157b4146506bd381326f39 • 5928907c41368d6e87dc3e4e4be30e42 • e017bfc36e387e8c3e7a338782805dde • fb6323c19d3399ba94ecd391f7e35a9c • 72b92683052e0c813890caf7b4f8bfd331a8b2afc324dd545d46138f677178c4 • ad43bbb21e2524a71bad5312a7b74af223090a8375f586d65ff239410bbd81a7 • b014cdff3ac877bdd329ca0c02bdd604817e7af36ad82f912132c50355af0920 • c1223aa67a72e6c4a9a61bf3733b68bfbe08add41b73ad133a7c640ba265a19e • 3739b2eae11c8367b576869b68d502b97676fb68d18cc0045f661fbe354afcb9 • e477f52a5f67830d81cf417434991fe088bfec21984514a5ee22c1bcffe1f2bc
URLs	• https://siestakeying[.]com/auth[.]php • https://waterforvoiceless[.]org/invite[.]php • https://seeceafcleaners[.]co[.]uk/wine[.]php • https://waterforvoiceless[.]org/util[.]php • https://seeceafcleaners[.]co[.]uk/cert[.]php • https://passatempobasico[.]com[.]br/wine[.]php • https://castechtools[.]com/api[.]php • http://waterforvoiceless[.]org/invite[.]xn--php-9o0a • http://waterforvoiceless[.]org/util[.]xn--php-9o0a[.] • https://waterforvoiceless[.]org/invite[.]xn--php-9o0a[.]
Domains	• siestakeying[.]com • waterforvoiceless[.]org • 0x3bd487[.]open

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Submit the IPs to Network team to block in the firewall.
- Block the Domain in the Proxy.
- Make regular backups of important and critical files.

- Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security software's up to date with latest patches.
- Install anti-virus software on all devices

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://www.bleepingcomputer.com/news/security/russian-hackers-target-german-political-parties-with-wineloader-malware/
- https://www.zscaler.com/blogs/security-research/european-diplomats-targeted-spikedwine-wineloader