Mphasis
The Next Applied

Threats Actors Delivering Remcos RAT Distributed as UUE (Uuencoding) File

Date: 3rd May 2024 | Severity: Medium

Summary

AhnLab Security Intelligence Center (ASEC) has confirmed the accuracy of the Remcos RAT malware being distributed through UUE (UUEncoding) files compressed with Power Archiver. This sophisticated method of malware distribution has been observed in phishing emails disguised as export/import shipment-related emails or quotations, making it crucial for recipients to exercise caution.

Attack Vectors

- Researchers identified a campaign distributing Remcos RAT, a Remote Access Trojan, where the attack uses phishing emails disguised as legitimate business communication, such as import/export or quotations.
- The emails contain a UUEncoded (UUE) file compressed with Power Archiver, which likely contains the Remcos RAT downloader, which once executed would allow attackers remote access to the victim's machine.
- An attacker is distributing a malicious VBS script hidden within an attachment. The script is encoded using Unix-to-Unix Encoding (UUE), a method for converting binary data into readable text format.
- The UUE-encoded attachment has a header, an encoded data section, and an end Marke. Decoding the attachment reveals an obfuscated VBS script, further complicating the analysis.
- VBScript acts as a downloader, fetching a malicious PowerShell script (Talehmmedes.txt) and saving it in the victim's temporary directory, which in turn downloads Haartoppens.Eft, another malicious script, from a remote server and stores it in the user's AppData folder.
- Haartoppens.Eft is obfuscated, making it difficult to analyze its functionality. However, it can be identified as another PowerShell script and its primary function is to inject shellcode into the wab.exe process, a legitimate Windows process associated with address book contacts.
- The shellcode establishes persistence by modifying the registry, ensuring the attacker maintains access to the compromised system even after a reboot.
- It retrieves further malicious data (mtzDpHLetMLypaaA173.bin) from another remote server, which is likely another PowerShell script or a component used by the malware for malicious purposes.
- Ultimately, this entire chain of events leads to the execution of the Remcos Remote Access Trojan (RAT), granting the attacker unauthorized control over the victim's machine.

- Remcos RAT, a sophisticated remote access trojan, extracts system information via hxxp://geoplugin[.]net/json.gp, likely for geolocation purposes.
- The malware then logs keystrokes and stores them as mifvghs.dat within the user's application data directory (AppData), which is then exfiltrated to the attacker's command and control (C&C) server, granting the attacker comprehensive information about the victim's machine and their keystrokes.
- Downloader: The Path to Infection The VBS script is executed by saving a PowerShell script in the %Temp% path with the file name Talehmmedes.txt.
- This PowerShell script accesses a malicious URL and downloads a file named Haartoppens.Eft to the %AppData% path, and additional PowerShell scripts run.
- The additional PowerShell script is also obfuscated to interfere with analysis. Its main function is to load shellcode into the wab.exe process.
- The shellcode registers a registry to maintain persistence and loads additional data by accessing another malicious URL. The final malicious code executed is Remcos RAT.

Indicator of compromise

INDICATOR TYPE	INDICATORS
URLS	• frabyst44habvous1.duckdns[.]org:2980:0 • frabyst44habvous1.duckdns[.]org:2981:1 • frabyst44habvous2.duckdns[.]org:2980:0 • hxxp://geoplugin[.]net/json.gp

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- 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.

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://gbhackers.com/remcos-rat-uuencoding-theft/
- https://cybersecuritynews.com/threats-delivering-remcos/
- https://malware.news/t/remcos-rat-distributed-as-uuencoding-uue-file/82875/1