AL2022_37 SVCReady Malware Loads from Word doc Properties (8th June 2022)

Description

SVCReady, a previously unknown malware loader that uses an innovative method of loading malware from Word documents onto victim devices, has been detected in phishing attempts.

Summary

The malware has been in use since April 2022, with multiple updates released by the developers around May 2022. This suggests that it is still in the early stages and is currently under heavy development. However, it already supports information exfiltration, persistence, anti-analysis features, and encrypted C2 communications.

How it Works

A phishing email with a malicious .doc attachment starts the infection chain. In contrast to the normal technique of downloading payloads from remote locations using PowerShell or MSHTA via malicious macros, this campaign leverages VBA to run shellcode hidden in the file properties which is then extracted and executed by macros. By separating the macros from the malicious shell code, the threat actors hope to avoid detection by security tools.

Next, the shellcode from the document properties is imported into a variable. Depending on whether the system is 32-bit or 64-bit, different shellcode is loaded.

The required shell code is loaded into memory, from which it will acquire executable access permissions using the Windows API method "Virtual Protect." The SetTimer API then transmits the shellcode's address and executes it. A DLL (malware payload) is dropped into the percent TEMP% directory as a result of this activity. Under a different name, a copy of "rundll32.exe," a legal Windows file, is also stored in the same directory and is eventually utilized to run SVCReady.

The updated malware

The updated SVCReady malware profiles the machine using Registry queries and Windows API calls before sending the data to the C2 server via an HTTP POST request. An RC4 key is used to encrypt communication with the C2.

The malware also does two WMI queries on the host to see if it's running in a virtualized environment, and if it is, it goes into sleep mode for 30 minutes to avoid detection.

The virus's persistence method now relies on the creation of a scheduled task and a new registry key, but the malware will not run after a reboot owing to implementation issues.

The second phase of data collection begins, which entails taking screenshots, extracting "osinfo," and transmitting everything to C2. Every five minutes, SVCReady communicates to the C2 to report its status, receive new tasks, send stolen data, and validate the domain.

Finally, the malware can also fetch additional payloads. Security Analysts have observed one case where SVCReady dropped a Readline stealer payload on the infected host.

Remediation

The SVCReady malware is detected differently by different Anti-Virus Software, a list of the detection names can be found at the following URL:

https://www.virustotal.com/gui/file/08e427c92010a8a282c894cf5a77a874e09c08e283a66f1905c131871cc4d273/detection

It is advised to have a prestigious anti-virus software installed on your device to detect and remove this malware.

The Guyana National CIRT recommends that users and administrations review this alert and apply it where necessary.

References

- Toulas, Bill. (7th June 2022). *New SVCReady malware loads from Word doc properties.* Retrieved from Bleeping computer. https://www.bleepingcomputer.com/news/security/new-svcready-malware-loads-from-word-doc-properties/

- Lakshmanan, Ravie. (7th June 2022). *Researchers Warn of Spam Campaign Targeting Victims with SVCReady Malware.* Retrieved from The Hacker News. https://thehackernews.com/2022/06/researchers-warn-of-spam-campaign.html