Agent Tesla

Article URL
malware.php?mal_id=1256204997605352e6d0c968.15183613

Author
SecurityHome.eu

Published: 18 March 2021

Aliases :

There are no other names known for **Agent Tesla**

.

Explanation :

Agent Tesla remote access trojan (RAT) that target the Windows anti-malware interface used by security vendors to protect PCs from attacks.

Agent Tesla first came into the scene in 2014, specializing in keylogging (designed to record keystrokes made by a user in order to exfiltrate data like credentials and more) and data-stealing. Agent Tesla has historically arrived in a malicious spam email as an attachment.

The first stage of the malware's newer version includes a .NET-based downloader. The downloader collects obfuscated code from websites like Pastebin and Hastebin (which touts itself as an "open source alternative to Pastebin"). This is not a new tactic, with Agent Tesla previously turning to a legitimate Pastebin-like web service for downloading malware.

Then, Agent Tesla's installer attempts to overwrite code in Microsoft's AMSI. First, the downloader attempts to get the memory address of AmsiScanBuffer (Microsoft's function, also known as amsi.h, that scans a buffer-full of content for malware).

It does so by calling Windows' amsi.dll, using the Windows LoadLibraryA function, to get the DLL's base address. Then it uses the GetProcAddress function to retrieve the base address and the "AmsiScanBuffer" procedure name to get the address of the function.

Once Agent Tesla gets the address of AmsiScanBuffer, it patches the first 8 bytes of the function in memory. This forces AMSI to return an error (code 0x80070057), making all the AMSI scans of memory appear to be invalid, according to researchers.

This kneecaps AMSI-enabled endpoint protection software, by essentially making them skip further AMSI

scans for dynamically loaded assemblies within the Agent Tesla process, said researchers. Since this happens early in the first stage downloader's execution, it renders any AMSI protection against the subsequent components of the downloader, the second-stage loader, and the Agent Tesla payload itself.

The new version of Agent Tesla also has the added capabilities of deploying a Tor client. This free, open-source software enables anonymous communication - serving as a tool for Agent Tesla to conceal its communications, said researchers.

n the new Agent Telsa version, the developers can now capture data from the Windows clipboard. The Windows clipboard is a storage area for items the have been cut or copied; this data could include anything from sensitive copied data from emails or documents, to passwords. This data is then sent back to the command-and-control (C2) server.

Another difference is that in the new version of Agent Tesla, the number of applications targeted for credential harvesting has been expanded considerably.

Agent Tesla previously targeted credentials from applications like Apple Safari, Chromium, Google Chrome, Iridium, Microsoft IE and Edge, Mozilla Firefox, Mozilla Thunderbird, OpenVPN, Opera, Opera Mail, Qualcomm Eudora, Tencent QQBrowser and Yandex. The malware also now targets FTPNavigator (Windows-based Internet application that facilitates FTP transfer), WinVNC4 (a remote desktop control allowing users to control computers remotely), WinSCP (which provides secure file transfer between a local and a remote computer) and SmartFTP (network file transfer program for Microsoft).

The credential-stealing function also includes code which launches a separate thread to exfiltrate browser cookies. While this code is present in all the samples of Agent Tesla from both v2 and v3, it isn't always used,â€• said researchers. Also, this feature is not set from the configuration fileâ€”so, perhaps, it's a premium feature attackers must buy from Agent Tesla's developer.

While Agent Tesla has previously communicated with the C2 server over HTTP, SMTP (simple mail transfer protocol) and FTP (file transfer protocol), the new version also uses Telegram to exfiltrate data, by sending the stolen data to a private Telegram chat room.

Last update 18 March 2021