Malware Analysis — AgentTesla

medium.com/@b.magnezi/malware-analysis-agenttesla-2af3d73a7825

0xMrMagnezi February 15, 2024

0xMrMagnezi

--

Agent Tesla is a widely-used remote access Trojan (RAT) known for its keylogging and data exfiltration capabilities, often used in cyber espionage and information theft.

In this report I will Analyze an AgentTesla Sample that was uploaded to MalwareBazaar.

MalwareBazaar — Initial Sample

Stage 1-

As usual I downloaded the file and extracted it using the password “infected”.

.BAT file

Just from looking at it I noticed that I'm dealing with JS and PowerShell code. I assumed that trying to deobfuscate this .BAT file would be a waste of time. So I ran it in order to capture the PowerShell script that was being executed.

Capture of the PowerShell code

As I suspected the PS was starting under the cmd.exe (.BAT) , so I extracted it from the command line. Also its important to note that the original BAT file was deleted after execution.

Stage 2-

Obfuscated PowerShell code that was extracted from the command line

After a little bit of dirty work I managed to Deobfuscate the PS code.

Deobfuscated PowerShell code

In summary this script downloads a new file (.JPG) and executes it.

Stage 3-

I decided to get that file on my own terms without executing it , so I curled to this path and saved the output as "out".

Curl to the attacker JPG path

This out file contained another obfuscated PowerShell , so I had to do more deobfuscation.

Obfuscated PowerShell

The first Var — "u8yee" was going through manipulation in which at the end it swapped "A" with "00".

Using CyberChef to decode

After some cleaning and deobfuscation of the code

In summary the first function is decompressing any byte array that its getting as an argument.

The next 2 Vars — "y74gh00rffd" and "eSQy" are also going through manipulation just like before , just a bit different. The letters "EV" are being replace by "0x" which is representation of Hex. In addition to this replacement the output of this byte array is being passed to the Decoding functions.

First Byte Array Decode

Second Byte Array Decode

I knew this process was a success as soon as I saw the “MZ” in the beginning of the file — Indication of DOS Executable. I saved those 2 new files as .BIN files.

Stage 4-

Finding out that One file is EXE and the other is DLL — Both written in .NET

While Debugging this executable in DNSPY I noticed that I'm dealing with Info Stealer / Key Logger with more features and capabilities.
The Data is being sent using SMTP.

Finding SMTP Password to the attacker

Finding The Information about the computer that is being sent to the attacker

The Mail Addresses that were found.

IOC’s:

- DOC20241.bat — 380c9e85f6960add801843076c33ec3b
- out.jpg — 11d8ddcb74dd3c1c10dcf8e6df8e5af9
- stage4.dll –416c046fdcf4625c189ec37230052b62
- stage4.exe–2e8ecadb887cb758c0b0dcb79442d616
- hxxps://didaktik-labor[.]de/mx1[.]jpg
- hxxps://account.dyn[.]com
- hxxp://knoow[.]net/
- mx1@knoow[.]net
- mx2@knoow[.]net