**AGENT TESLA**

Agent Tesla is spyware that collects information about the actions of its victims by recording keystrokes and user interactions. It is falsely marketed as a legitimate software on the dedicated website where this malware is sold.

Most commonly delivered via phishing campaigns, Agent Tesla has been deployed in several iterations since it first appeared around 2014. According to recent research, Agent Tesla is being delivered within email attachments. When a user clicks to download the file, the malware can execute within the impacted device without additional user interaction. Specifically, Agent Tesla is a remote access trojan (RAT) written in .Net. If an attacker is able to fully deliver this RAT onto your device, they will have achieved full computer and network access. The tool specializes in stealing credentials, sensitive information, and keystrokes.

Agent Tesla an advanced RAT functioning as a keylogger and information stealer, which is capable of monitoring and collecting the victim’s keyboard input, system keyboard, taking screenshots, and exfiltrating credentials belonging to a variety of software installed on a victim’s machine (including Google Chrome, Mozilla Firefox and the Microsoft Outlook email client).

MD5: 059bb09924b0d8cb7a8cffb72fd0bb03

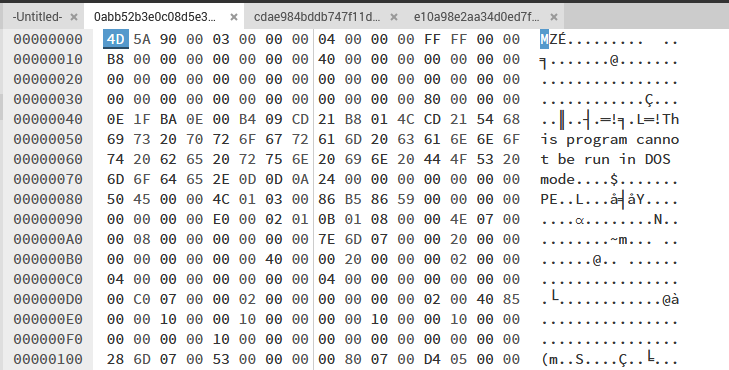
SHA-1: 87a02be494bc914211d91a45a9ccbf4d47238566

SHA-256: 0abb52b3e0c08d5e3713747746b019692a05c5ab8783fd99b1300f11ea59b1c9

Authentihash: 4801bcaf30c33f75847d6fd15b1984bc05ee7cc87621d68a328493825362d1a8

File type Win32 EXE

Magic PE32 executable for MS Windows (GUI) Intel 80386 32-bit Mono/.Net assembly



MD5: 32b2668174be406d98bde8c055e809d6

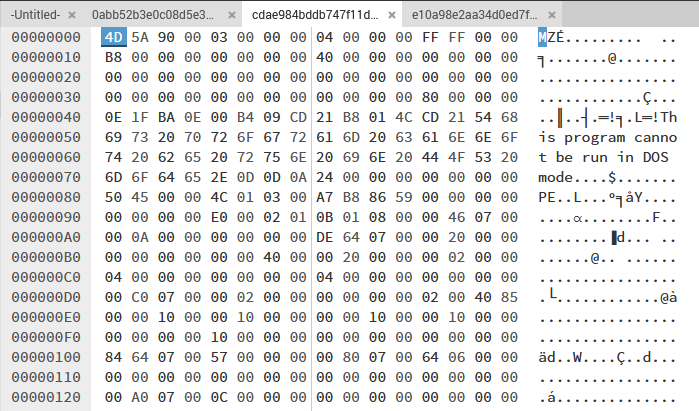
SHA-1: 62470fb3bec370be380172d6162674dda8d70f17

SHA-256: cdae984bddb747f11d7d3a8708fd7e3bcaa4c295d3441899a33b4ae9f6db5aba

Authentihash: e2102e931d422ca0705d7a98ad18de26509fffbf9d590c116b180ed9c7f9c703

File type: Win32 EXE

Magic: PE32 executable for MS Windows (GUI) Intel 80386 32-bit Mono/.Net assembly



SHA-256: e10a98e2aa34d0ed7f5cf78717efdc809d3084bd7ca29f3a5905a3c1a22ae118

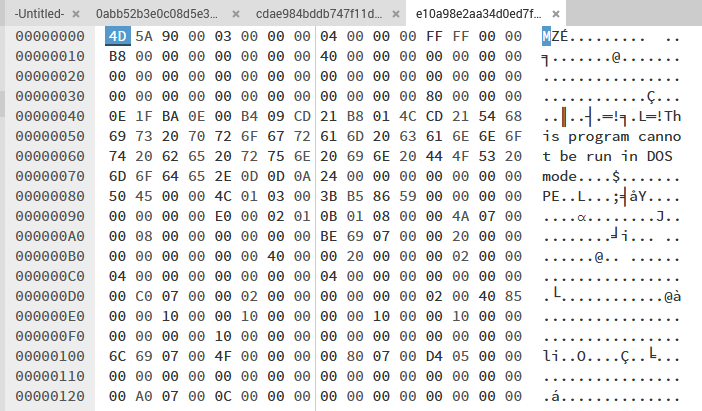
MD5: 732ad6e95c86b3be894fe6ffa27eb683

SHA-1: e126335f8c59c50dffa83ba5a42f9aff76c1752a

Authentihash: cc50cf74964b4e712f012518c6ae803c62d4976057c935cd00322afae96ec624

File type: Win32 EXE

Magic: PE32 executable for MS Windows (GUI) Intel 80386 32-bit Mono/.Net assembly



**a4attempt4:**

It is found to be a malware executable

Source –

1. <http://www.softpanorama.org/Malware/Bulletin/malware2009.shtml>
2. <https://infosec.cert-pa.it/analyze/059bb09924b0d8cb7a8cffb72fd0bb03.html>

**mscoree.dll:**

You can tell if the .NET Framework has been installed by looking for the MSCorEE.dll file in the %windir%\system32 directory. The existence of this file tells you that the .NET Framework is installed.

The mscoree.dll file is a part of the Microsoft.NET framework. It provides the possibility to connect information, systems, people and devices through software. The mscoree.dll file is a Microsoft Runtime Execution Engine; in other words, it contains the fundamental functions of the Microsoft.NET framework.

Imports are the functions that a piece of software calls from other files (typically various DLLs that provide functionality to the Windows operating system)

Source:

1. <https://www.dll-files.com/mscoree.dll.html>
2. <https://www.joesandbox.com/analysis/211650/0/html>

**Public Key token: b77a5c561934e089**

Register key created is -

HKLM\SOFTWARE\Microsoft\.NETFramework\v2.0.50727\NGenService\Roots\System.Data.Services.Design, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089\0

Source:

1. <https://otx.alienvault.com/indicator/file/bf9e237262ac1674f7c0e56f00db6dd64986e37f01cc59558b95b0c63afb903e/>
2. <https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~BHO-SO/detailed-analysis.aspx>

**Public Key token: b03f5f7f11d50a3a**

Register key created is –

HKLM\SOFTWARE\Microsoft\.NETFramework\v2.0.50727\NGenService\Roots\Microsoft.VisualBasic, Version=8.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a\0

Source:

1. <https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~PWS-BQP/detailed-analysis.aspx>
2. <https://otx.alienvault.com/indicator/file/bf9e237262ac1674f7c0e56f00db6dd64986e37f01cc59558b95b0c63afb903e/>

**YARA RULE:**

rule AgentTesla

{

meta:

Author = "Vigneswaran"

Date = "31.08.2021"

Description = "Sample rule written for Agent Tesla Open Directory"

strings:

$exe = "a4attempt.exe"

$dll = "mscoree.dll"

$Token1 = "b77a5c561934e089"

$Token2 = "b03f5f7f11d50a3a"

condition:

uint16(0) == 0x5A4D

and $exe and $dll and $Token1 and $Token2

}

**REFERENCES:**

1. <https://attack.mitre.org/software/S0331/>
2. <https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla>
3. <https://www.fortinet.com/blog/threat-research/analysis-of-new-agent-tesla-spyware-variant>
4. <https://blog.morphisec.com/agent-tesla-a-day-in-a-life-of-ir>
5. <https://any.run/malware-trends/agenttesla>