AgentVX and Taurus

aon.com/cyber-solutions/aon_cyber_labs/agentvx-and-taurus/

In an investigation occurring in 2021, Stroz Friedberg Incident Response Services team (Stroz Friedberg) encountered a new payload associated with the Taurus loader. Typically, the information security community sees this loader associated with the Taurus Stealer malware. The Taurus Stealer has the ability to collect information from various web browsers, including passwords, cookies, autofill forms and history. However, in this instance, Stroz Friedberg identified a new payload named "AgentVX". This payload contains several functions outlined below. On September 19th, 2022, NSFOCUS Security Labs released an article attributing AgentVX to the group "Evilnum." Since 2021, Stroz Friedberg has not seen publicly available information relating this loader and payload. We are releasing this blog post to provide additional threat intelligence on the AgentVX payload and release a script to assist with the automated decoding of the Taurus loader.

Taurus Loader

In this investigation, the Taurus loader matched publicly available analysis and Minerva Labs posted analysis on it earlier in 2021. The execution chain begins with a self-extracting archive. This archive drops the following files to "%AppData%\BueedgFYHdzEt\":

File	Description
Andate.xlm	Corrupt PE, used to build "Sapro.exe.com"
Calpestare.pptm	Unused
Poi.xltx	Obfuscated AutoIT loader is renamed to "x" and executed
Sapro.exe.com	AutoIT executable used for injection of payload
Seguente.mpg	Obfuscated batch file used to control the execution flow
Sta.xll	Encrypted "AgentVX" payload that is injected into "Sapro.exe.com"

Upon execution, the malware executes "Seguente.mpg", which conducts multiple kill-switch checks that are consistent with the Taurus loader including:

- Attempts to connect to the non-existent domain "QYLBUtMSCcIS.QYLBUtMSCcIS"
- Checks for the existence of a file called "C:\aaa_TouchMeNot_.txt"
- Checks to see if the system name is "DESKTOP-QO5QU33". The information security community has written about the name of this system multiple times.

When the checks pass, the malware continues execution to execute the obfuscated AutoIT script, "Poi.xlxt". The AutoIT script conducts additional checks like the above, including checking for the same system name of "DESKTOP-QO5QU33". If these checks pass, the malware injects a decrypted version of "Sta.xll" (AgentVX) into the newly created "Sapro.exe.com" process.

The Taurus AutoIT loader, "Poi.xlxt", obfuscates its strings by using an algorithm which takes an integer and an offset, then converts the integer and offset to its ASCII value. Below is an example of an encoded string that uses an offset value of 2:

Encoded String	Decoded String
"74>89>112>102>42>51>56>56>43",2	HWnd(166)

Performing the decoding manually for a sample is a very lengthy and cumbersome process. Stroz Friedberg has released code to assist with automatic extraction and decoding of the Taurus AutoIT loader strings. Decoding of the strings allows for quicker analysis of the Taurus loader, allowing an analyst to see de-obfuscated function calls to kernel32 and commands to be run by the script. The Python function described below will de-obfuscate AutoIT strings manually:

```
def decodeTaurus(string, integer, delim):
    res = ''
    tab = string.split(delim)
    for character in tab:
            res = res + chr(int(character)-int(integer))
    return res
```

The execution chain of the self-extracting archive to AgentVX is described in the below figure, followed by a short description of each step in the chain:

- C:\Update.exe[A]
    - "C:\Windows\System32\cmd.exe" /c echo iomMUgap[B]
    - "C:\Windows\System32\cmd.exe" /c C:\WINDOWS\system32\cmd.exe < Seguente.mpg[C]
        - findstr /V /R "^OgfZwjLcFcTXy...[snip]" Andate.xlm [D]
        - Sapro.exe.com x[E]
            - C:\Users\User\AppData\Roaming\BueedgFYHdzEt\Sapro.exe.com[F]

Figure 1: Execution chain of self-extracting archive to final AgentVX payload.
[A] Execution of self-extracting archive
[B] Start of execution of extracting routine
[C] Execution of obfuscated batch script
[D] Identification of start of encrypted payload
[E] Execution of Taurus AutoIT loader which is renamed from “Poi.xlxt” to “x”
[F] Execution of AgentVX via injection into “Sapro.exe.com”

AgentVX

Once the loading steps complete, the malware attempts to establish a connection to the Command and Control (C2) server with the following details:

Type	IOC
Domain	cdn.nvbcloud[.]com
URI	/timeout/voip.aspx
User-Agent	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36

AgentVX begins by dynamically resolving functions. The malware will gather fingerprint information to send to the C2 server, including:

- Java Runtime Environment (JRE) version
- .NET version
- Directory listing for “Program Files” and “Program Files (x86)” directories
- Drive letters
- OS version

Once the malware establishes C2 connectivity, it beacons out to the C2 every 6 seconds using the same details above. It waits to receive a “task list” from the server. The task list contains one or multiple tasks to complete and options for those tasks. The tasks within the task list can be any of the following:

Download and execute – this receives a payload from a server provided in the task options. The options allow for the operator to save the payload to disk and execute it, or to inject it into another process memory using calls to: NtMapViewOfSection, VirtualProtectEx, WriteProccessMemory, and ResumeThread. If the operator chooses process injection, they can specify if they wish the payload to be injected into one of the following:

– %SystemRoot%\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
– %SystemRoot%\Syswow64\nslookup.exe

If this task fails, the malware prints a debug string of “Download and execute failed.”

Execute – this receives a base64 encoded payload from the task options. If the payload is an executable, it writes the executable to disk and names it a random number from 6 to 12 and appends a “.exe” on the end. If the payload is a DLL, it allows the operator to choose one of the following to inject the payload into:

– %SystemRoot%\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
– %SystemRoot%\Syswow64\nslookup.exe
– %SystemRoot%\System32\nslookup.exe

Execute and setup persistence – this allows the operator to provide three base64 encoded payloads, at least one of which must be an executable. The malware downloads and writes the executable to disk. The executable is named with a random number between 6 and 12 and is given the “.exe” extension (i.e., 6.exe). It will set this executable up with persistence by adding the following registry key:

– HKCU\Software\Microsoft\Windows\CurrentVersion\Run

<random_string> = <XXX_PATH_TO_EXECUTE_XYZ>

The other two payloads use hardcoded file names:

– Dbghelp.dll
– Pic.png

- Cleanup Persistence – this option removes the registry run key persistence set by the “Execute and setup persistence” option.
- Setup new module – This function receives a base64 encoded DLL which the malware parses for the following exports:

– AgentVXModuleInitializer
– OnLoad
– OnUnLoad
– IsPersistent
– GetModuleName
– GetMinimumVersion
– ReadCommunication

The malware checks its version and if the version is less than “1.6d.1”, it prints the debug string: “Bot version is too low to install.”

- Get running modules – this gets the list of running modules specific to the malware.

- Execute Function – This allows the operator to specify another function of the malware to execute. In total, there are 156 functions that the malware can execute. Below are examples of the capabilities that four of these functions provide:
    - Manipulation of clipboard data
    - Collection of browser data from Firefox or Chrome. Only one of the browsers is targeted at a time. Stroz Friedberg suspects this is a bug in the malware. During this process, the malware creates the folder: %AppData%\XProfiles
    - File and directory upload and download
    - Collection of screenshots

Threat Intelligence

Stroz Friedberg captured an image of the threat actor's malware administration panel for AgentVX. The panel shows the title of "AgentVX from Cerberus" in the top left corner. Additionally, Stroz Friedberg observed the following similarities during our analysis of the malware:

> The BotID length and alphanumeric pattern matches what we observed in the threat actor's control panel.
>
> The malware shows the error message "Download and Execute failed" while the threat actor's control panel displays a task named "Download and Execute".
>
> The malware can execute various procedures which it refers to as "tasks". The threat actor's control panel shows that "tasks" for bots can be updated.
>
> In the malware, one particular task can have options such as EXE, MEMORY and NATIVE associated with it while the threat actor's control panel shows that a task has options of EXE, MEMORY and DISK.

Indicators of Compromise

Stroz Friedberg recommends alerting and blacklisting (where possible) the following indicators to help prevent and detect the AgentVX malware:

Type	IOC	Indicates	Notes
Domain	cdn.nvbcloud[.]com	Malware successfully initiated communications with C2	
Domain	QYLBUtMSCcIS.QYLBUtMSCcIS	The malware attempted an anti-sandbox check	
URI	/timeout/voip.aspx	Malware successfully initiated communications with C2	
User-Agent	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36	Malware successfully initiated communications with C2	Ensure to combine this with other IOCs to make this a higher fidelity indicator

File	Update.exe	The initial dropped may exist on the system	Ensure to combine this with other IOCs to make this a higher fidelity indicator
File	Andate.xlm	The initial dropper has executed	
File	Calpestare.pptm	The initial dropper has executed	
File	Poi.xltx	The initial dropper has executed	
File	Sapro.exe.com	The initial dropper has executed	
File	Seguente.mpg	The initial dropper has executed	
File	Sta.xll	The initial dropper has executed	This file is deleted once it is injected into memory and decrypted
Folder	%AppData%\XProfiles	The malware started collecting browser information	
Folder	%AppData%\BueedgFYHdzEt\	The initial dropper has executed	
File	%TEMP%\\[0-9]\.png	The malware has loaded an additional module	Regex IOC
File	Dbghelp.dll	The malware has loaded an additional module	
File	Pic.png	The malware has loaded an additional module	
SHA256	e437a05b660338b5bf068d8cd17c08a9dbf6499cac7f709ccfbf2dcce0fc759b	Hash of update.exe	

SHA256	7477aa86458346df14d8f7315391a28190c01a2caa5f3891eef0ffdb86072116	Hash of Andate.xlm
SHA256	0f34cbd62be0b3024e6a630763e5952e1445f74e96d23f862f7845067b1a76f5	Hash of Calpestare.pptm
SHA256	9c3d15cb8795e1d7e47d702c6530b960919c2de7bfe191a37b3ac2a2f5259d55	Hash of Poi.xltx
SHA256	05d8cf394190f3a707abfb25fb44d7da9d5f533d7d2063b23c00cc11253c8be7	Hash of Sapro.exe.com
SHA256	e0f90d7c68e0aeff8b2932b0e7e2b04c6d44728b383b34d810e3b127ff9f91e3	Hash of Seguente.mpg
SHA256	918a5954dc12b16b85900fd72fee1d76cef624b903d78f3ecc6d57a2a3840bb1	Hash of Sta.xll

Author: Zachary Reichert
February 3, 2023

Cyber security services offered by Stroz Friedberg Inc. and its affiliates. Insurance products and services offered by Aon Risk Insurance Services West, Inc., Aon Risk Services Central, Inc., Aon Risk Services Northeast, Inc., Aon Risk Services Southwest, Inc., and Aon Risk Services, Inc. of Florida and their licensed affiliates. Aon UK Limited is authorised and regulated by the Financial Conduct Authority in respect of insurance distribution services. FP.AGRC.238.JJ The following products or services are not regulated by the Financial Conduct Authority:
• Cyber risk services provided by Aon UK Limited and its affiliates
• Cyber security services provided by Stroz Friedberg Limited and its affiliates.