Malware Sample: https://malshare.com/sample.php?action=detail&hash=6095f96dd5eca96a3fb9338eec4ab574921c0febb36f6a6db60aae1aeb9ffcab

**Introduction**

According to Sophos, Squirrelwaffle is a malware loader that is distributed as a malicious Office document in spam campaigns. It provides attackers with an initial foothold in a victim's environment and a channel to deliver and infect systems with other malware. When a recipient opens a Squirrelwaffle-infected document and enables macros, a visual basic script typically downloads and executes malicious files and scripts, giving further control of the computer to an attacker. Squirrelwaffle operators also use DocuSign to try and trick the user into enabling macros in Office documents.

**Debugging**

Clicking the malware sample link will bring you to this page. You can make an account and

download the sample here:

Download

**Hashes**

MD5: dd6257665f634b5566e15bc62e90c809

SHA1: 54ded03f7b82c8aa4de10e673b556d0ba778177d

SHA256: 6095f96dd5eca96a3fb9338eec4ab574921c0febb36f6a6db60aae1aeb9ffcab

SSDEEP: 1536:CZYCKkPkDwBycMjIBbzreg/+UgOiALGr05:CZYCKkPkc7bHpdpin05

**Observed File Names**

squirrel.bin

**Yara Hits**

YRP/Microsoft_Visual_Cpp_v50v60_MFC | YRP/Borland_Delphi_30_additional | YRP/Borland_Delphi_30_ | YRP/Borland_Delphi_v40_v50 | YRP/Borland_Delphi_v30 | YRP/Borland_Delphi_DLL | YRP/IsPE32 | YRP/IsDLL | YRP/IsWindowsGUI | YRP/HasDebugData | YRP/HasRichSignature | YRP/domain | YRP/contentis_base64 | YRP/anti_dbg | YRP/network_dns | YRP/BASE64_table | YRP/Str_Win32_Winsock2_Library |

**VT Context**

Detections | IoCs | Graph | Attribution — VT Augment by VIRUSTOTAL

58 / 74

-1 Community Score

58 security vendors flagged this file as malicious

trojan.squirelwaffle/genericrxqc

6095f96dd5eca96a3fb9338eec4ab574921c0febb36f6a6db60aae1aeb9ffcab

6095f96dd5eca96a3fb9338eec4ab574921c0febb36f6a6db60aae1aeb9ffcab.exe

pedll | spreader

| File type | File size | Last analysis |
|---|---|---|
| Win32 DLL | 73.7 kB | 18 days ago |

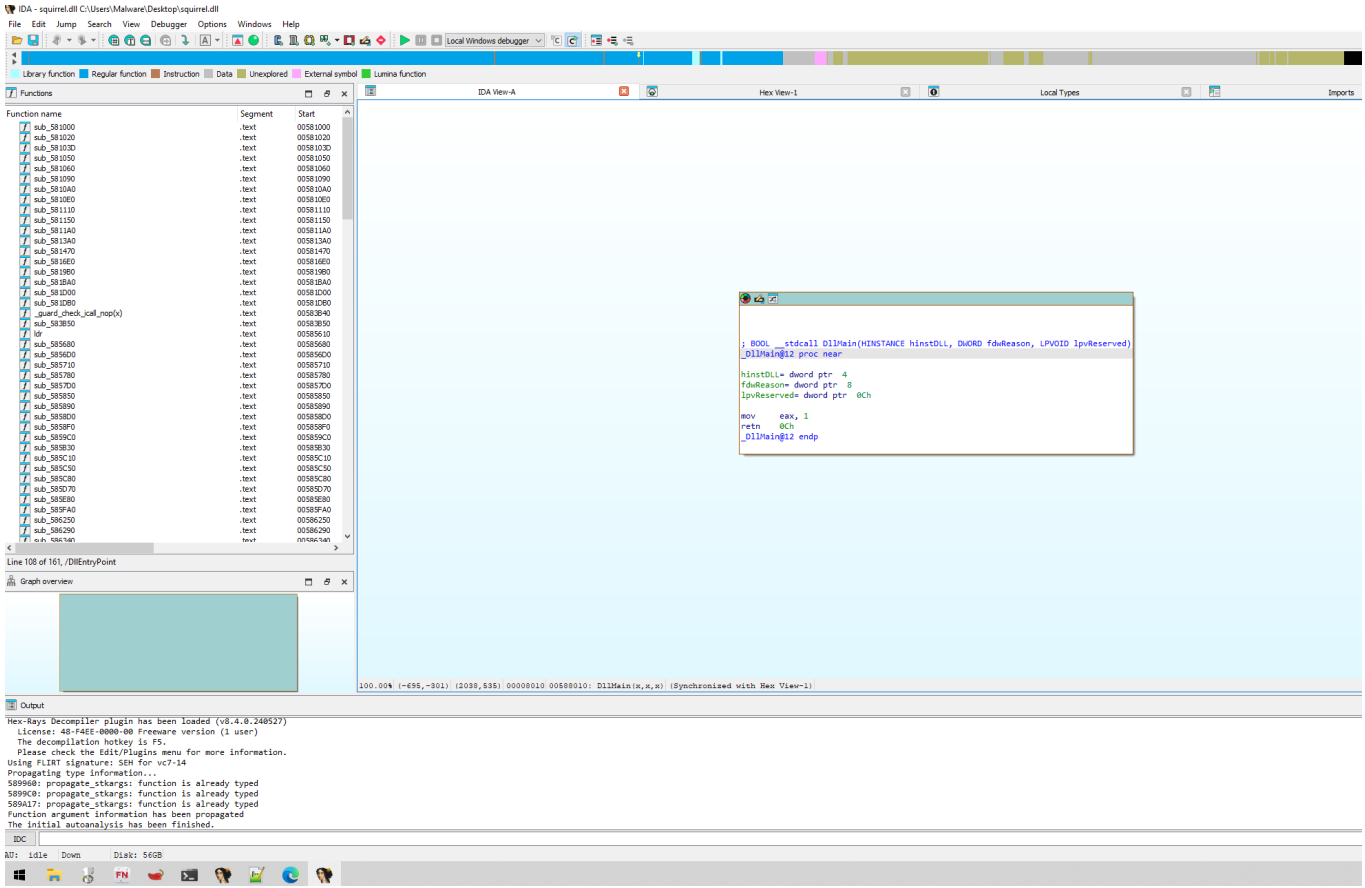
Full report | Similar files | VT Graph

**SECURITY VENDORS SCANNING RESULTS**

Bkav Pro: W32.AIDetectMalware
Elastic: Windows.Trojan.Squirrelwaffle
CTX: dll.trojan.generic
Lionic: Trojan.Win32.Squirelwaffle.a!c
eScan: Trojan.GenericKD.47072948

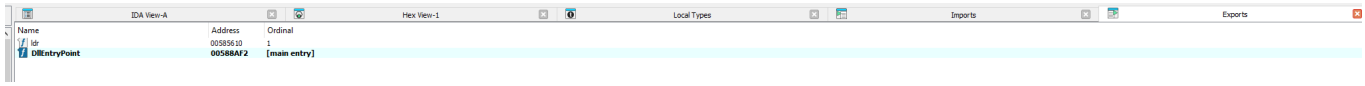
Once downloaded the filename will need to be changed to .dll so that IDA will have an easier time reading the file.

Upon opening IDA click new > select dll file




Click Exports

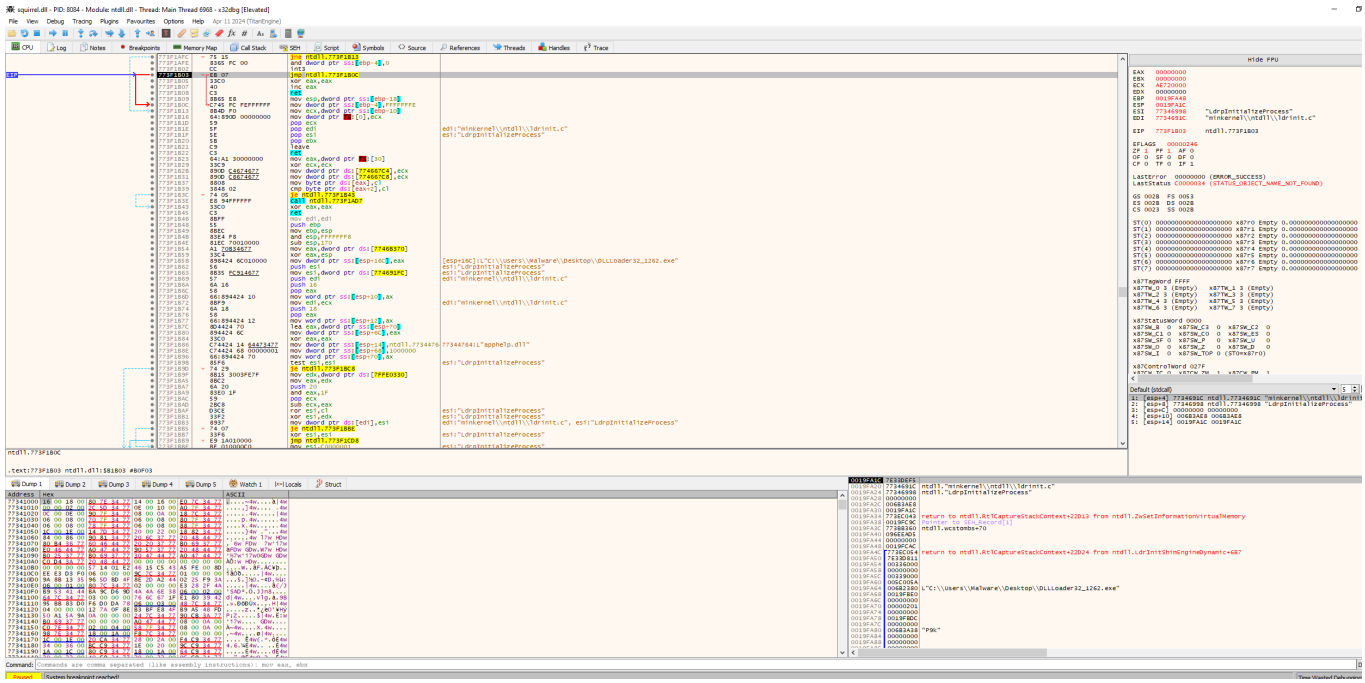
In exports we see two loaders:



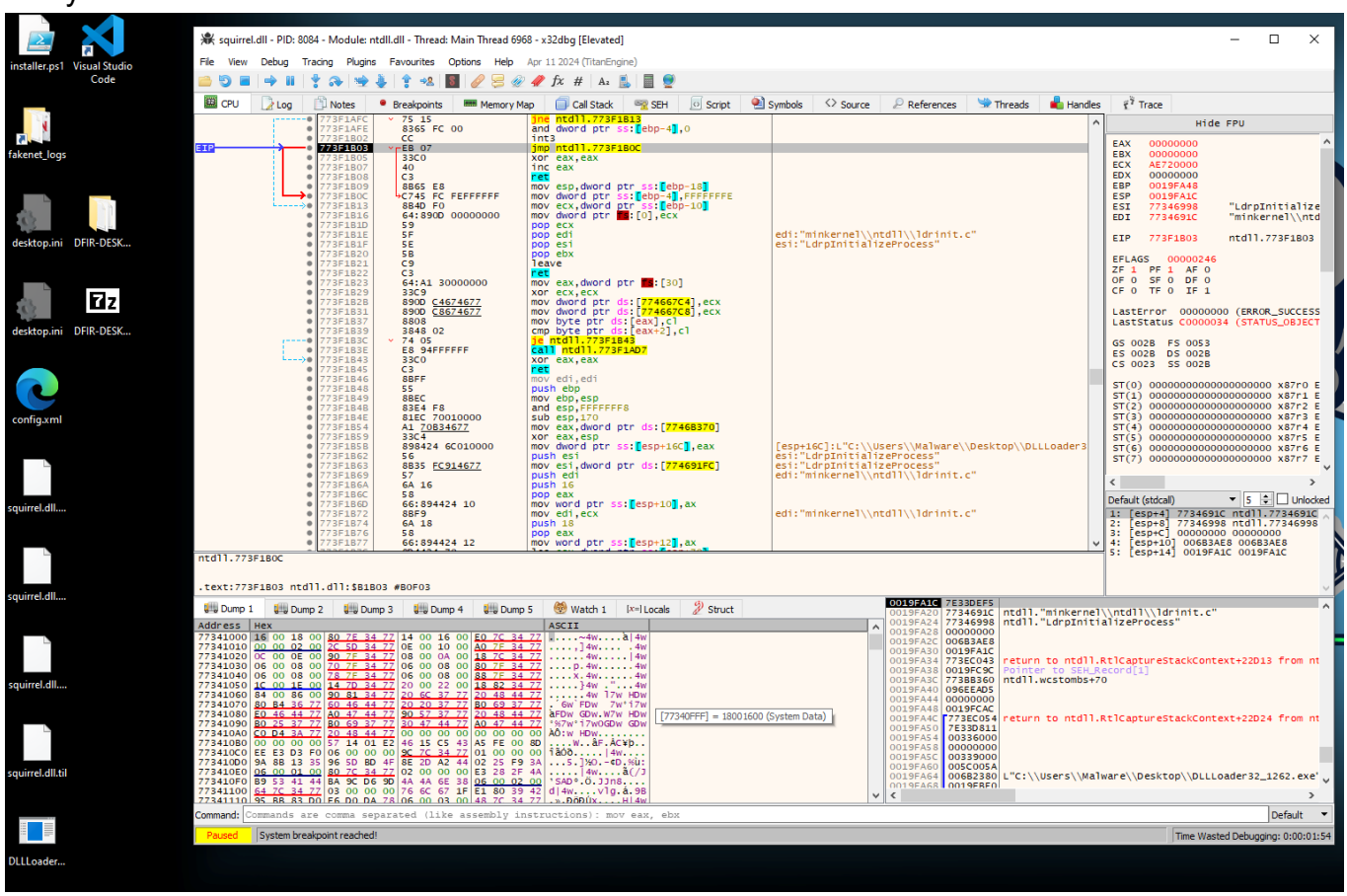

ldr is set as ordinal 1 which is where the config decryption occurs for this dll.

DLLEntryPoint does not have anything interesting stored within it at this time and if we attempted to debug this we wouldn't be able to debug the code within the loader.

Loading the export into x32dbg due to the dll being 32bit.



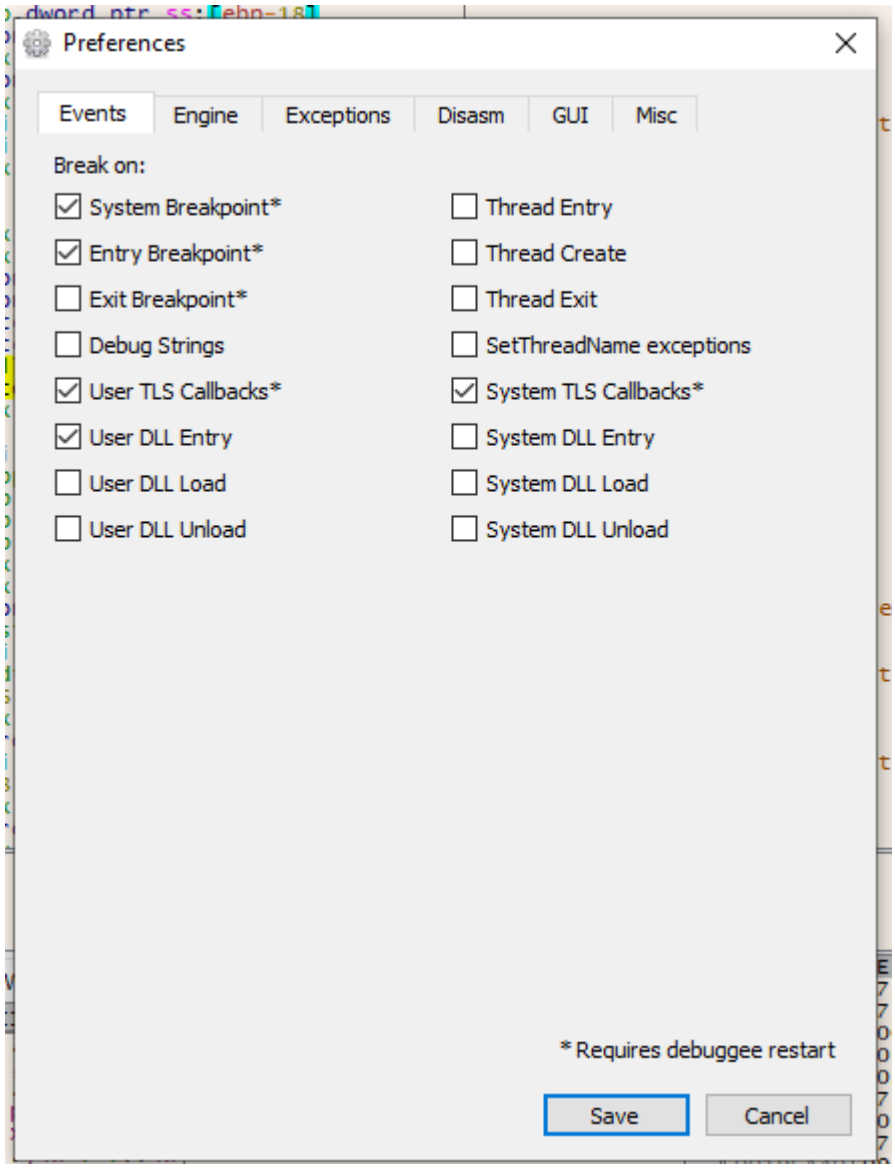
For further testing a PE file is created by x32dbg so that it may load our malicious DLL for analysis.



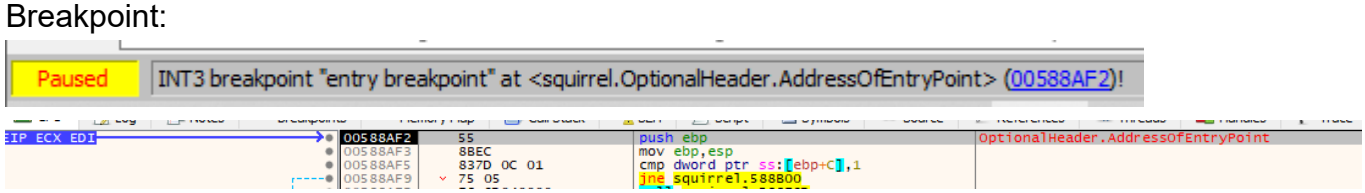
Bottom left ^^^

Right now we want to break the entry point of that DLL so that we may access the code behind the loader itself.

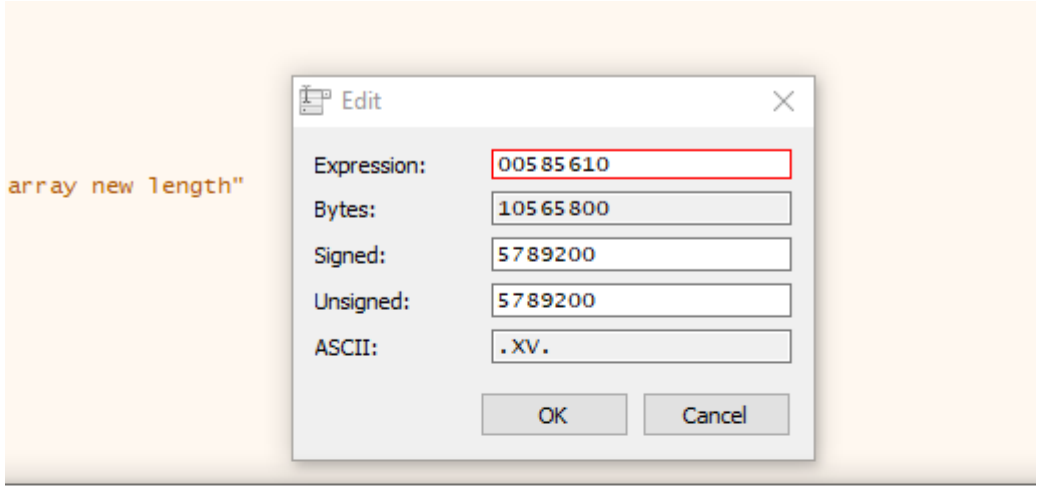
In options you'll want to enable User DLL Entry so that we can set the breakpoint between the two exports. From there we will run the program until we see the breakpoint occur.

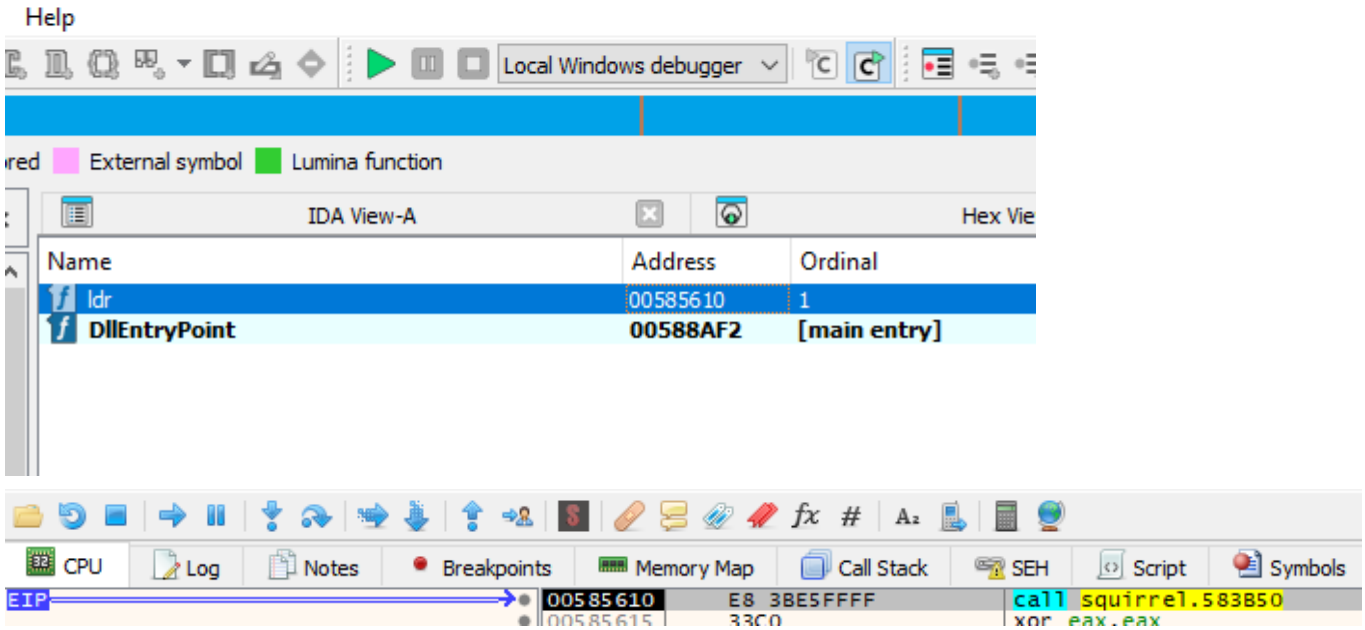



Breakpoint:

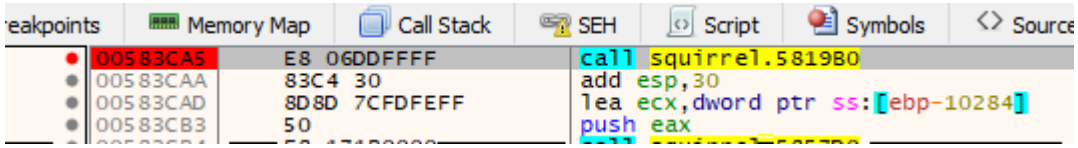



Right now the breakpoint is set to the DLLEntryPoint. We need to change the EIP to match the loader (ldr) and that will call the preferred export.




Now we need to set a new breakpoint at the decryption portion here and then take a look at the return value of eax.




After this we run the debugger and we right click at the bottom and follow DWORD in current dump which will reveal the blocklist IP addresses of the DLL config.

| Address | Hex | | | | | | | | | | | | | | | | ASCII |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00FF28C0 | 39 | 34 | 2E | 34 | 36 | 2E | 31 | 37 | 39 | 2E | 38 | 30 | 0D | 0A | 32 | 30 | 94.46.179.80..20 |
| 00FF28D0 | 36 | 2E | 31 | 38 | 39 | 2E | 32 | 30 | 35 | 2E | 32 | 35 | 31 | 0D | 0A | 38 | 6.189.205.251..8 |
| 00FF28E0 | 38 | 2E | 32 | 34 | 32 | 2E | 36 | 36 | 2E | 34 | 35 | 0D | 0A | 38 | 35 | 2E | 8.242.66.45..85. |
| 00FF28F0 | 37 | 35 | 2E | 31 | 31 | 30 | 2E | 32 | 31 | 34 | 0D | 0A | 38 | 37 | 2E | 31 | 75.110.214..87.1 |
| 00FF2900 | 30 | 34 | 2E | 33 | 2E | 31 | 33 | 36 | 0D | 0A | 32 | 30 | 37 | 2E | 32 | 34 | 04.3.136..207.24 |
| 00FF2910 | 34 | 2E | 39 | 31 | 2E | 31 | 37 | 31 | 0D | 0A | 34 | 39 | 2E | 32 | 33 | 30 | 4.91.171..49.230 |
| 00FF2920 | 2E | 38 | 38 | 2E | 31 | 36 | 30 | 0D | 0A | 39 | 31 | 2E | 31 | 34 | 39 | 2E | .88.160..91.149. |
| 00FF2930 | 32 | 35 | 32 | 2E | 37 | 35 | 0D | 0A | 39 | 31 | 2E | 31 | 34 | 39 | 2E | 32 | 252.75..91.149.2 |
| 00FF2940 | 35 | 32 | 2E | 38 | 38 | 0D | 0A | 39 | 32 | 2E | 32 | 31 | 31 | 2E | 31 | 30 | 52.88..92.211.10 |
| 00FF2950 | 39 | 2E | 31 | 35 | 32 | 0D | 0A | 31 | 37 | 38 | 2E | 30 | 2E | 32 | 35 | 30 | 9.152..178.0.250 |
| 00FF2960 | 2E | 31 | 36 | 38 | 0D | 0A | 38 | 38 | 2E | 36 | 39 | 2E | 31 | 36 | 2E | 32 | .168..88.69.16.2 |
| 00FF2970 | 33 | 30 | 0D | 0A | 39 | 35 | 2E | 32 | 32 | 33 | 2E | 37 | 37 | 2E | 31 | 36 | 30..95.223.77.16 |
| 00FF2980 | 30 | 0D | 0A | 39 | 39 | 2E | 32 | 33 | 34 | 2E | 36 | 32 | 2E | 32 | 33 | 0D | 0..99.234.62.23. |

Resources:

https://malpedia.caad.fkie.fraunhofer.de/details/win.squirrelwaffle

https://blog.talosintelligence.com/squirrelwaffle-emerges/

https://www.trendmicro.com/en_us/research/21/k/Squirrelwaffle-Exploits-ProxyShell-and-ProxyLogon-to-Hijack-Email-Chains.html

https://any.run/malware-trends/squirrelwaffle/

https://www.virustotal.com/gui/file/6095f96dd5eca96a3fb9338eec4ab574921c0febb36f6a6db60aae1aeb9ffcab

https://github.com/mandiant/flare-vm