“VawTrak” Malware

By Ilan Duhin

Published: 2023-03-19 · Archived: 2026-04-05 15:39:08 UTC

Researched by: Ilan Duhin

Executive Summary:

“Vawtrak” is a banking Trojan –malware that attempts to steal credentials from banks.

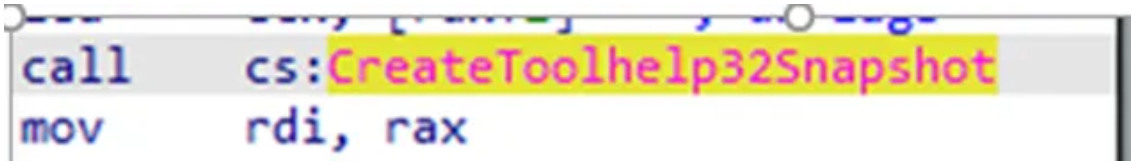
The Banker gains access to bank accounts via custom key logging, utilizing the access of a wide range of login credentials, such as passwords stored in browsers, FTP client private keys, or information stored within remote desktop settings.

To communicate, the Banker utilizes SOCKS connection and exfiltrates information such as screenshots and video captures.

Technical Analysis:

Unpacking Process:

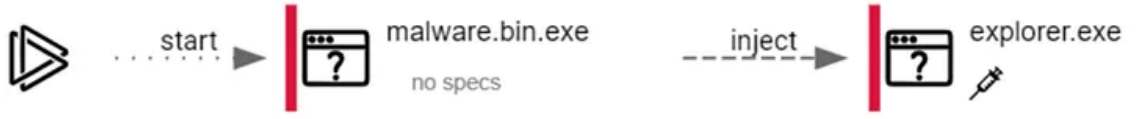
From analyzing the malware in IDA, I see suspicious API such **CreateToolhelp32Snapshoot** call that retrieves running processes, I guess that the malware will use it to get snapshot of them until it finds a legitimate process to inject his malicious code.



using CreateToolhelp32Snapshot

In addition, I have checked on online sandboxes such as Any.run & Hybrid Analysis to see additional info about the injection and I find that it tries to inject into the **explorer.exe process.**

Press enter or click to view image in full size



Process Tree from Any.run

After the conclusions, I choose to put my BP on **WriteProcessMemory** because the malware try to inject her code into other process so this call is perfect to use.

Get Ilan Duhin's stories in your inbox

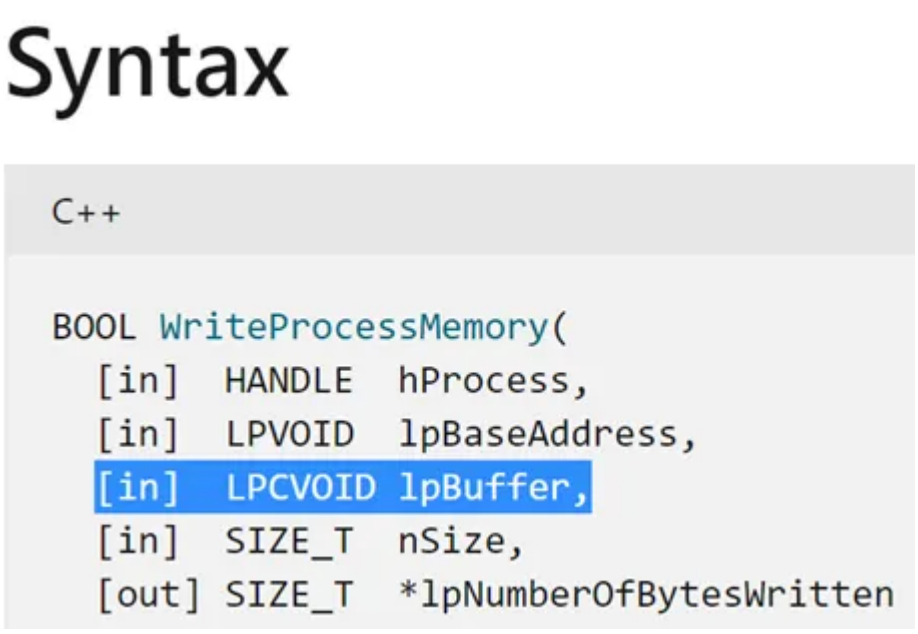
Join Medium for free to get updates from this writer.

Remember me for faster sign in

After placing a breakpoint on **WriteProcessMemory**, in order to catch the injection of the malware, and checking the functionality of the API calls within the code in MSDN, the parameter to dump the MZ header is clearly shown.

Press enter or click to view image in full size

The parameter required to dump the packed information is the third parameter, according to MSDN. The parameter is "lpBuffer" — A pointer to the buffer that contains data to be written in the address space of the specified process or in other words **"holds our unpacking file data".**

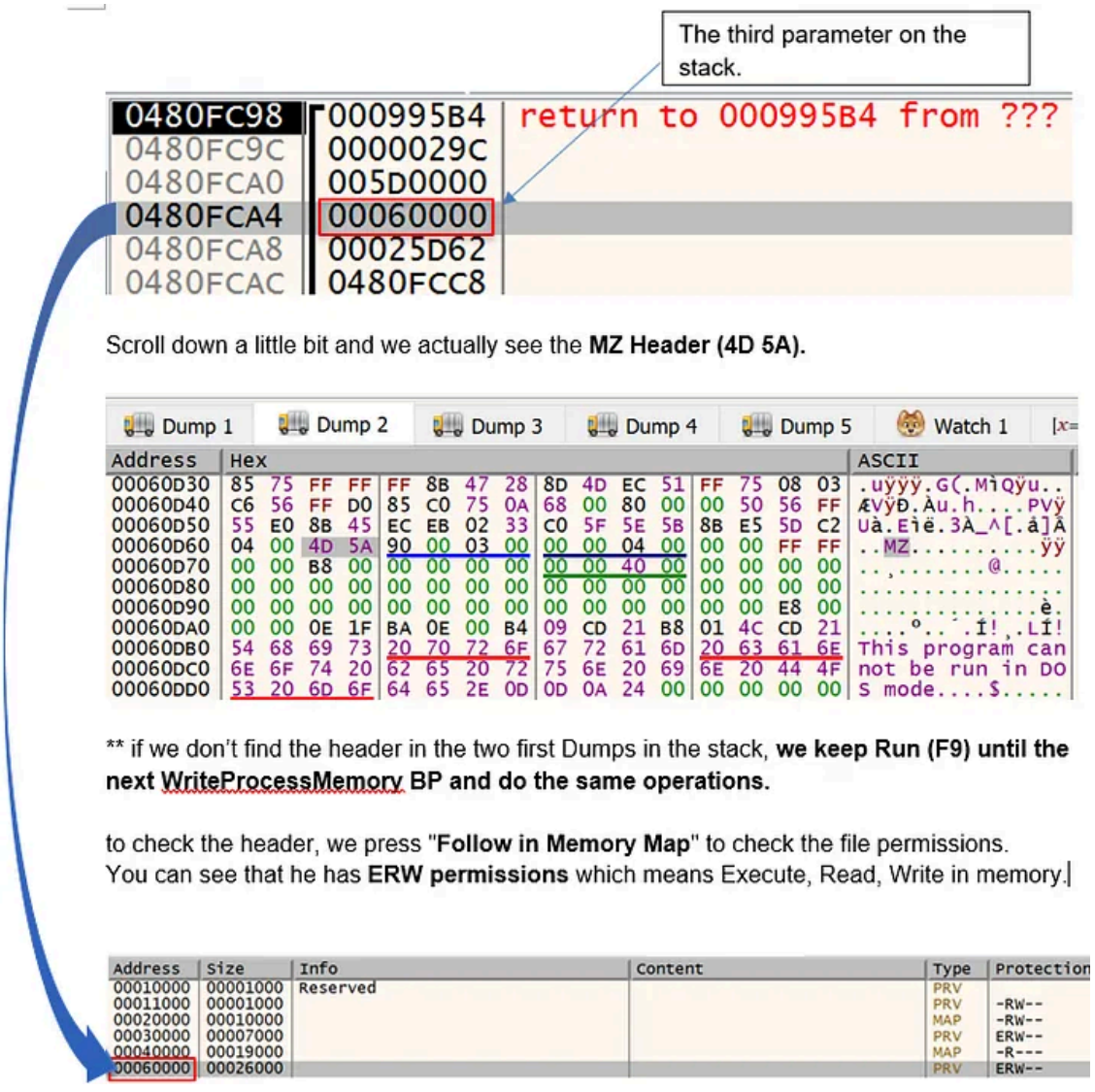


Press enter or click to view image in full size

[in] lpBuffer

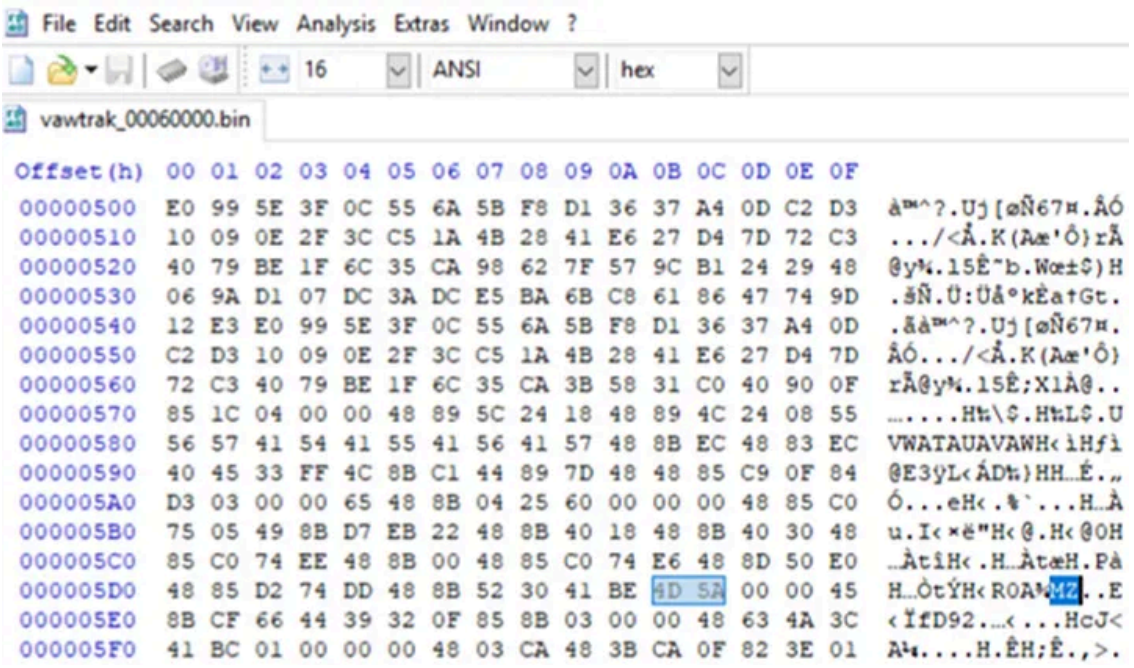
A pointer to the buffer that contains data to be written in the address space of the specified process.

Press enter or click to view image in full size



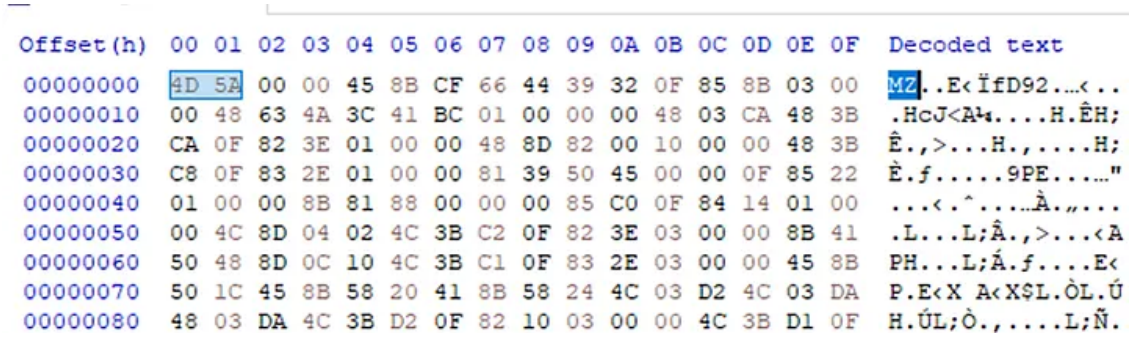
Memory Map permissions

Press enter or click to view image in full size



The dumped memory file:

Press enter or click to view image in full size

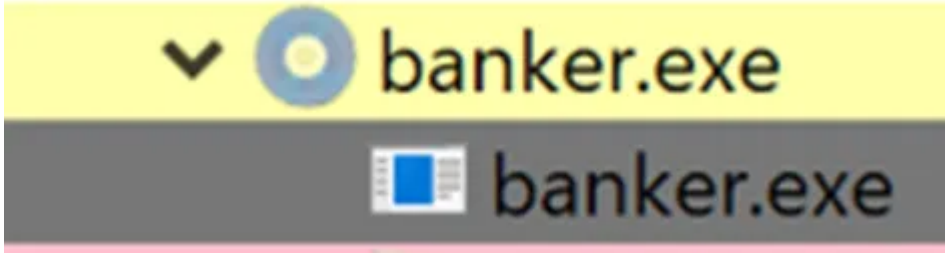


After cleaning the junk code:

the malware immediately writes itself into the autoruns paths, in order to have a foothold on the host upon startup or restart.

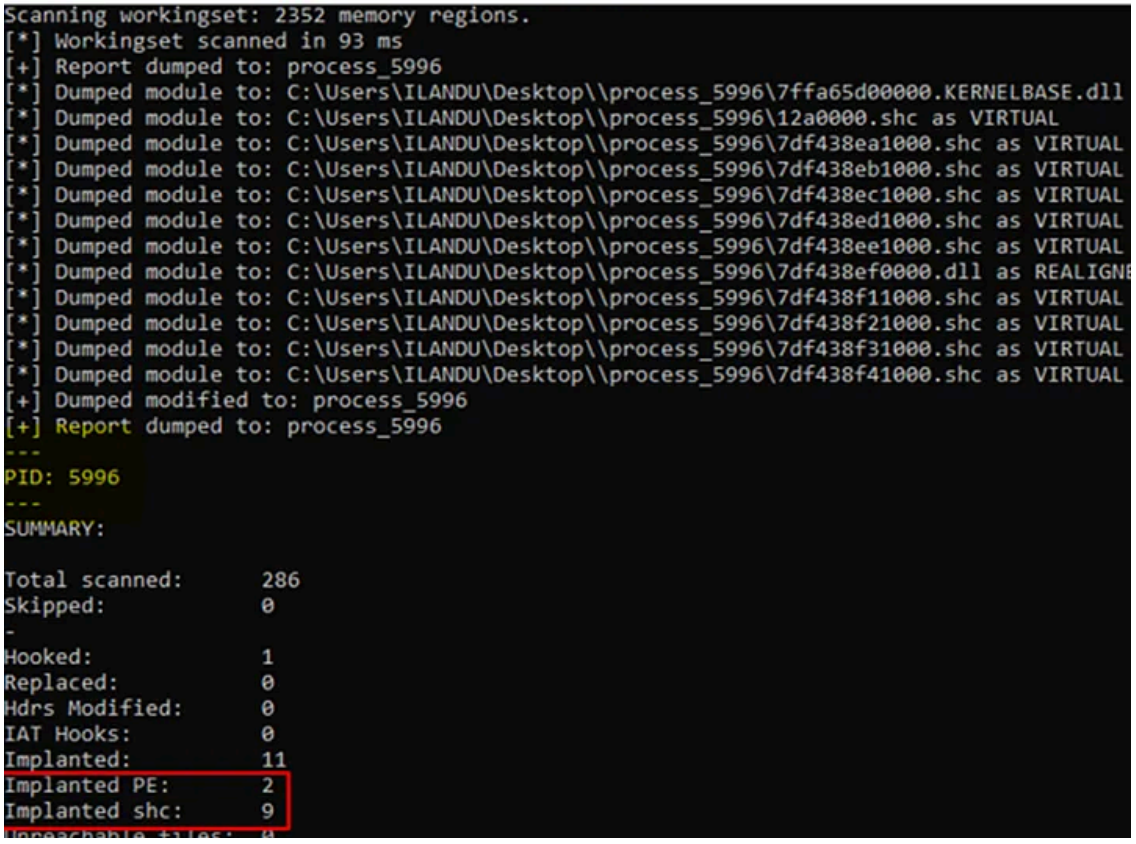
Press enter or click to view image in full size

After running, “Vawtrak” creates a child process with same name as the original running process. 30 seconds into the run, the original malware process terminates itself, and removes itself from the original running path and copies itself into APPDATA\LOCAL\TEMP, **in order to elevate privileges** (because of existence Writing privileges at this path).



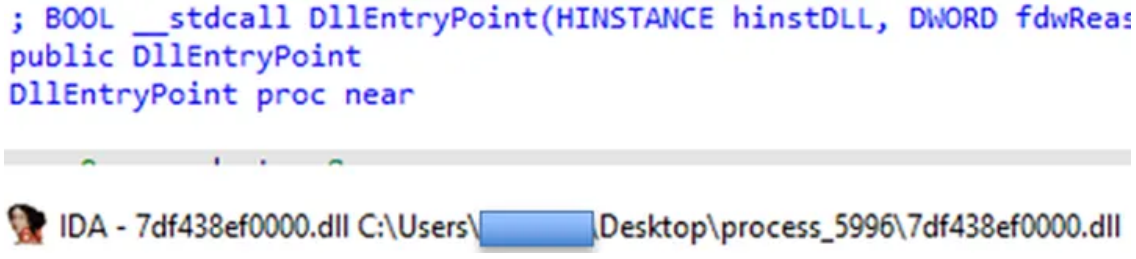
After establishing itself, the malware, through the injected process drops additional PE files, which contain **DLL and an executable**.

Press enter or click to view image in full size



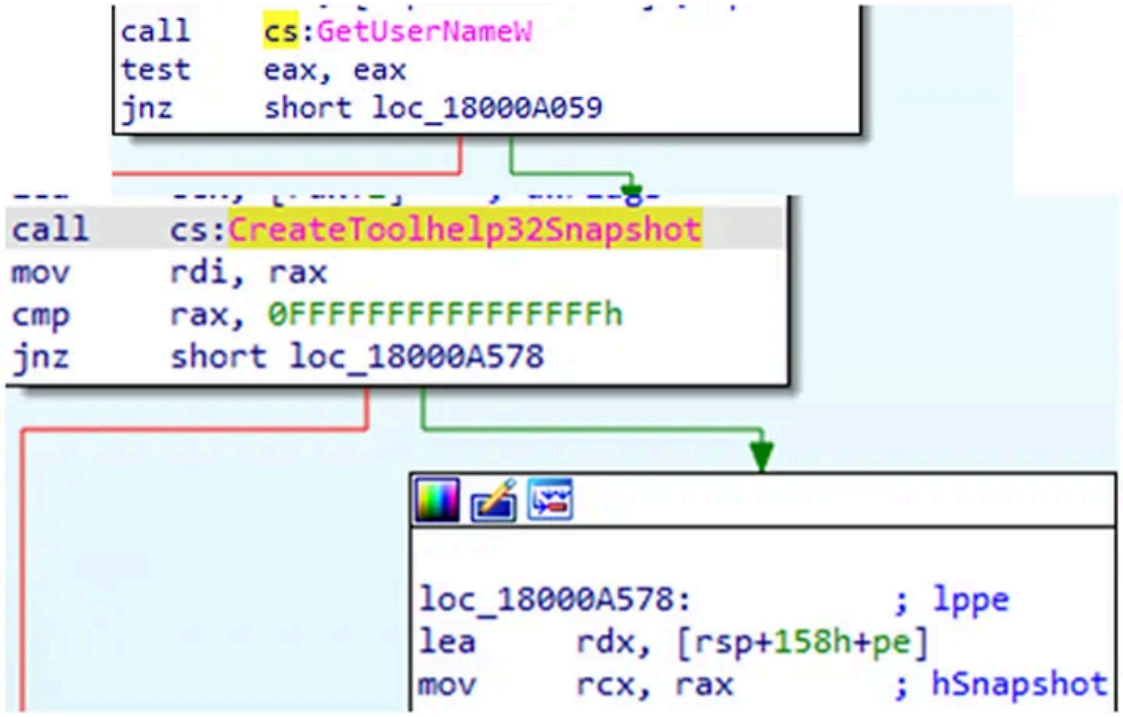
Drop the dll from pe-sieve after I dumped the implemented files into the folder to get more information. IDA also verify us that it is a dll file.

Press enter or click to view image in full size



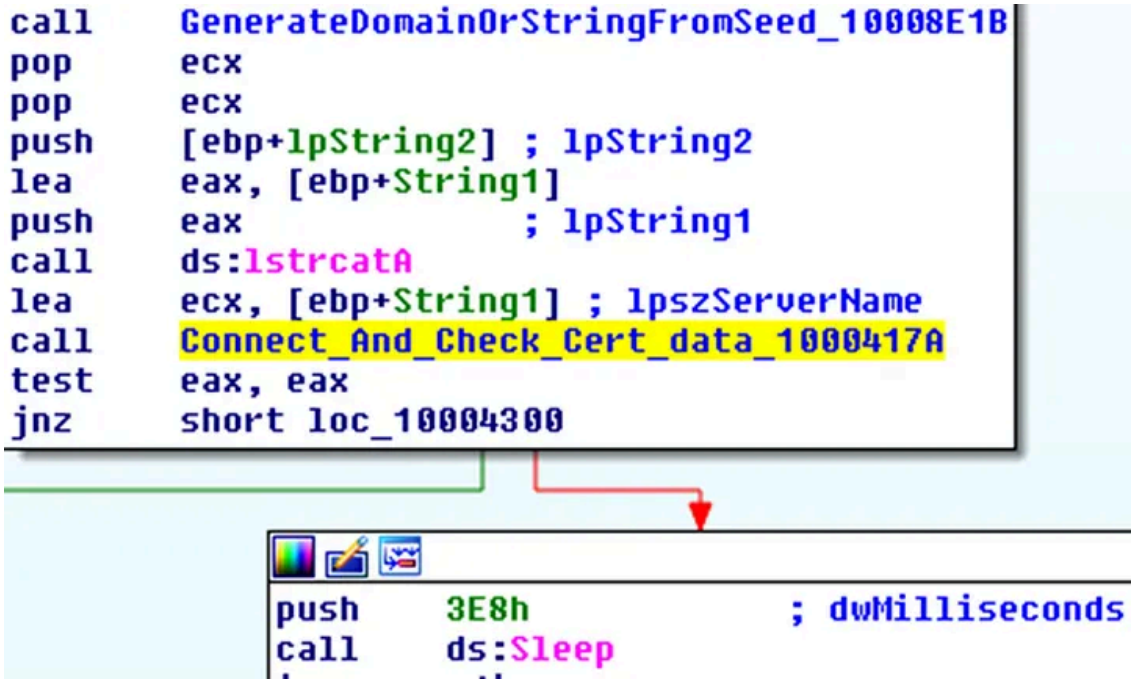
the DLL contains is creating a snapshot and list of all the currently running processes (as we mentioned earlier), this is usually done by reconnaissance malwares in order to target specific artifacts within the host.

Press enter or click to view image in full size



When reconnaissance is complete, the malware extracts its C2 server from a seed that the malware file contains — hard coded. It will perform certificate validation in order to check if the server is still available, if not, the malware goes to sleep for a random amount of time.

Press enter or click to view image in full size



In addition to certificate validation, the Banker checks if any reconnaissance information has been retrieved. If not, the malware does not initiate communication methods.

```
push    offset szVerb   ; "GET"
push    ebp             ; hConnect
mov     [esp+38h+var_4], eax
call    ds:HttpOpenRequestA
```

Press enter or click to view image in full size

```
push    ebx             ; lpszPassword
push    ebx             ; lpszUserName
push    1BBh            ; nServerPort
push    edi             ; lpszServerName
push    esi             ; hInternet
call    ds:InternetConnectA
```

Press enter or click to view image in full size

```
5C 1C 20 00        Seed dd 201C5Ch          ; Seed value
D4 5D 53 2E             dd 2E535DD4h        ; Encrypted data starts
```

Encrypted data start with the C2 server:

Press enter or click to view image in full size

```
DNS     78 Standard query 0x7cfb A cookingwithme.date
DNS     78 Standard query 0x7cfb A cookingwithme.date
DNS     78 Standard query 0x7cfb A cookingwithme.date
DNS     78 Standard query 0x7cfb A cookingwithme.date
```

DNS query to C2 server

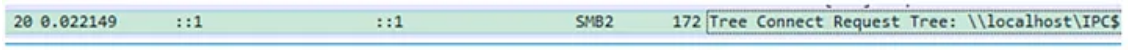
Following all these steps, “VawTrak” will attempt to spread through the network utilizing SMB — a legitimate Windows file-sharing protocol.

Press enter or click to view image in full size

```
SMB2   188 Ioctl Request FSCTL_SRV_ENUMERATE_SNAPSHOTS File: Users\     \Desktop\7e7d0557cc95e3f509f71a72aad9b8ab85d6a681df4a46e1648e928a4be5f4be (2).exe
TCP     64 445 → 49674 [ACK] Seq=3277 Ack=3156 Win=2615808 Len=0
SMB2   196 Ioctl Response FSCTL_SRV_ENUMERATE_SNAPSHOTS File: Users\     \Desktop\7e7d0557cc95e3f509f71a72aad9b8ab85d6a681df4a46e1648e928a4be5f4be (2).exe
TCP     64 49674 → 445 [ACK] Seq=3156 Ack=3409 Win=2615552 Len=0
SMB2   156 Close Request File: Users\     \Desktop\7e7d0557cc95e3f509f71a72aad9b8ab85d6a681df4a46e1648e928a4be5f4be (2).exe
```

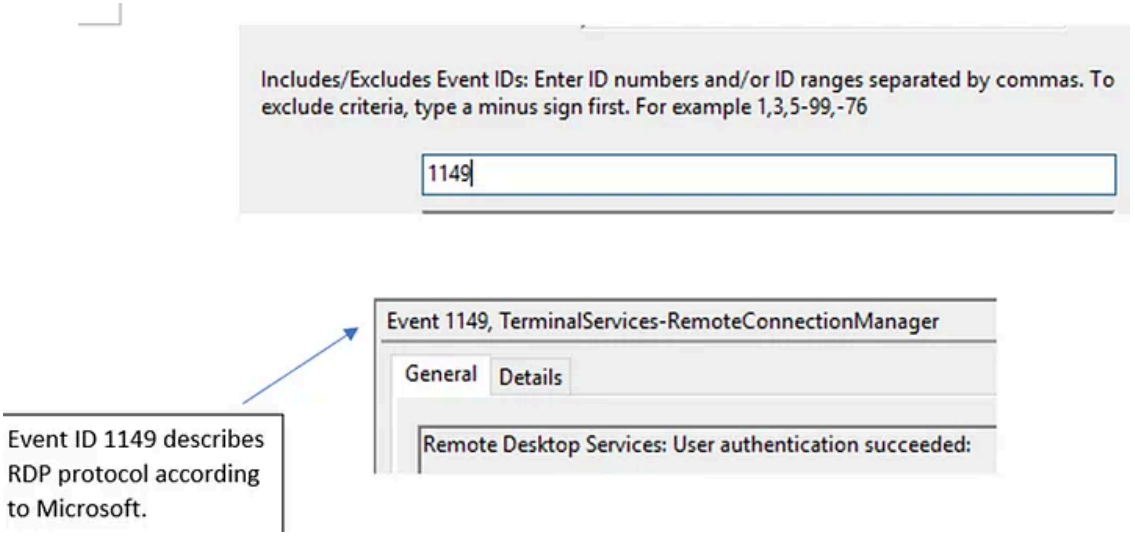
After completing all activities within the host and attempting to preform lateral movement, the malware wipes itself off the host and terminates its process.

Press enter or click to view image in full size



Tries to do lateral movement to another computers via SMB protocol.

Press enter or click to view image in full size



looking for RDP sessions:

reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest \UseLogonCredential / — auth of http protocol, stored in plaintext user credentials.

· **By default the key isn’t shows in registry.**

Press enter or click to view image in full size

Source: https://medium.com/@llandu/vawtrak-malware-824818c1837