Introduction

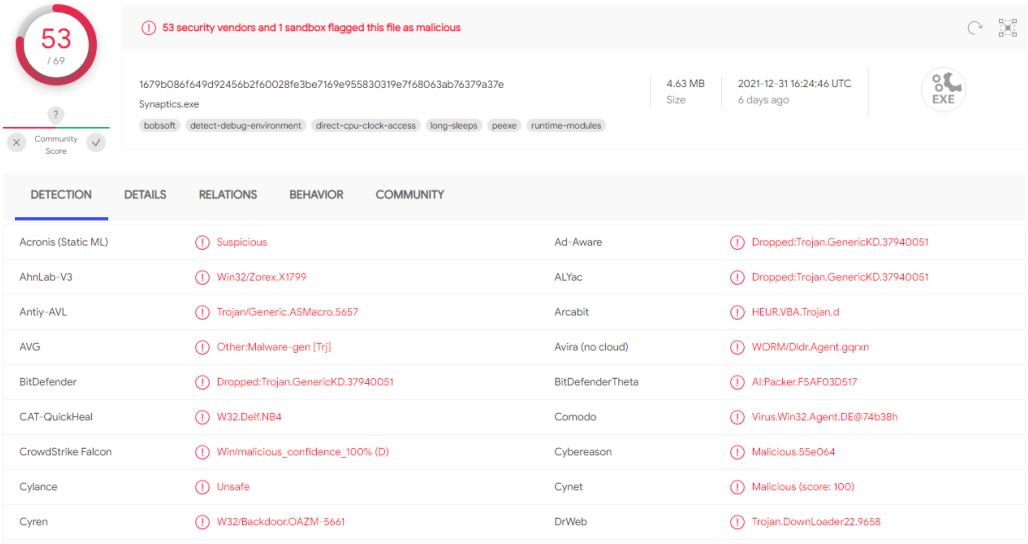
Malware forensic analysis provides the ability to analyze and understand the operation of malicious code (Trojans, viruses, rootkits, etc.) to assess the damage caused and assess the intentions and attacker capabilitie (Or-Meir et al., 2019). Knowing the structure, operation, and interaction of malware will provide valuable information, not only for the design and development of countermeasures effective but also to help identify the source of an attack and assess the detection capacity of the organization's systems at the time of taking the necessary and appropriate response actions.

Two malware analysis procedure are followed in this paper. The static analysis that involves analyzing malware at rest incorporates tools including virustotal, PEview, PEStudio, PEiD, and strings.exe. Dynamic analysis involves analysis while the malware executes. The tools involved include Wireshark, ProcMon, Process Explorer, Regshot, and Fakenet.

Static analysis

Virustotal

The file was uploaded to the virustotal.com to check if the malware was malicious or not. 53 out of 69 antivirus engines flagged the file as malicious as shown in the figure below



The following hash values were identified

MD5 ff7276155e0641b40dfc36e1cf315d70

SHA-1 2fd07b03fda2bf8bc43cd9ea9446ea40aa10b24a

SHA-256 1679b086f649d92456b2f60028fe3be7169e955830319e7f68063ab76379a37e

Basic Properties

MD5	ff7276155e0641b40dfc36e1cf315d70
SHA-1	2fd07b03fda2bf8bc43cd9ea9446ea40aa10b24a
SHA-256	1679b086f649d92456b2f60028fe3be7169e955830319e7f68063ab76379a37e
Vhash	0460866d5c0d5c051565503162z41z32z13z1035z23z40305bz
Authentihash	0f3320d3dbdb717b5fb287667a64e346487899addb592df1af902b2ad647fb9a
Imphash	332f7ce65ead0adfb3d35147033aabe9
SSDEEP	98304:8nsmtk2aN+hfTKQGEpz3xjlZwZC2vJhdO6qTrELwRxNjuAAPgg/ut9OQ9iAm/53X:SLM+hfzzxUJhdOLTrELwRxNjuAAPgg/F
TLSH	T1BD265BF1BDA14462C6131630783DEA78A9FFADA01B34478B529EF9582F323C708E9557
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Executable Borland Delphi 7 (62.2%)
TrID	Windows Control Panel Item (generic) (18.4%)
TrID	Windows ActiveX control (10.9%)
TrID	InstallShield setup (4%)
TrID	Win32 Executable Delphi generic (1.3%)
File size	4.63 MB (4858880 bytes)
PEiD packer	BobSoft Mini Delphi -> BoB / BobSoft

From the figure above it is also identified that the file type is win32 EXE and its size is 4.83 MB. The PEiD packer indicates that the file is packed.

The file makes some network communication as it contacts 5 domains, 2 URLs, and 6 IP addresses as shown in the figure below

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Contacted URLs

Scanned	Detections	Status	URL
2022-01-06	3 / 93	200	http://freedns.afraid.org/api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978
2021-12-31	0 / 93	200	http://pki.goog/gsr1/gsr1.crt

Contacted Domains

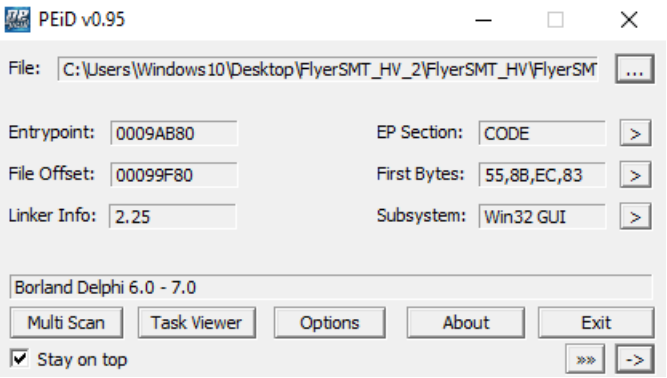
Domain	Detections	Created	Registrar
xred.mooo.com	4 / 90	2000-03-24	Domain.com, LLC
freedns.afraid.org	2 / 90	1999-09-21	ENOM, INC.
pki.goog	0 / 90	2016-06-13	Charleston Road Registry Billable
docs.google.com	0 / 90	1997-09-15	MarkMonitor Inc.
arc.msn.com	0 / 90	1994-11-10	MarkMonitor Inc.

Contacted IP Addresses

IP	Detections	Autonomous System	Country
69.42.215.252	0 / 90	17048	US
216.239.32.29	0 / 90	15169	US
224.0.0.252	0 / 90	-	-
142.250.81.206	0 / 90	15169	US
108.177.127.101	0 / 90	15169	US
20.82.209.183	0 / 90	8075	IE

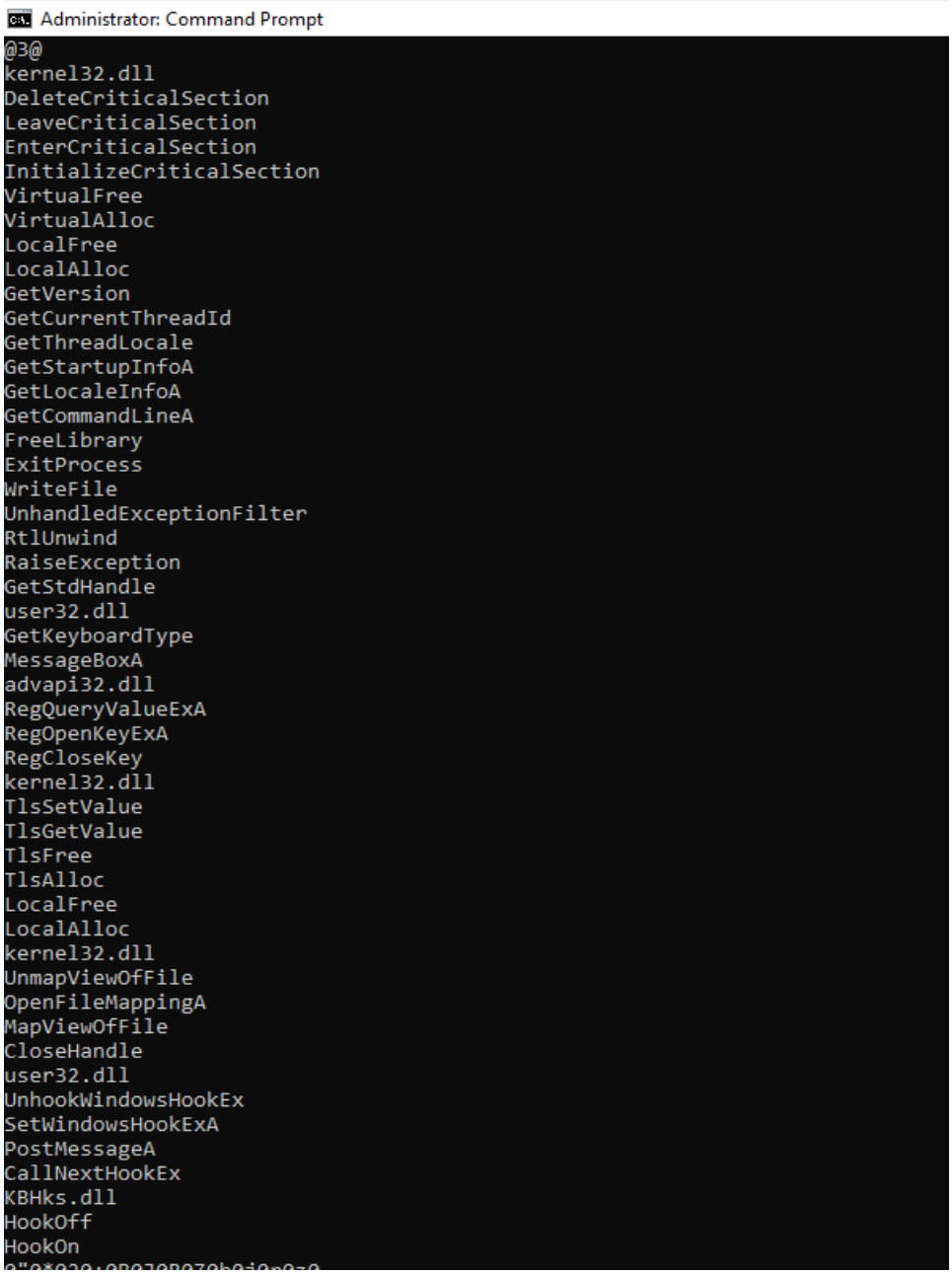
PEiD

Since virustotal.com indicated that the file is packed, PEiD was used to confirm that. It was identified the malware is packed with Borland Delphi 6.0 - 7.0 as shown in the figure below



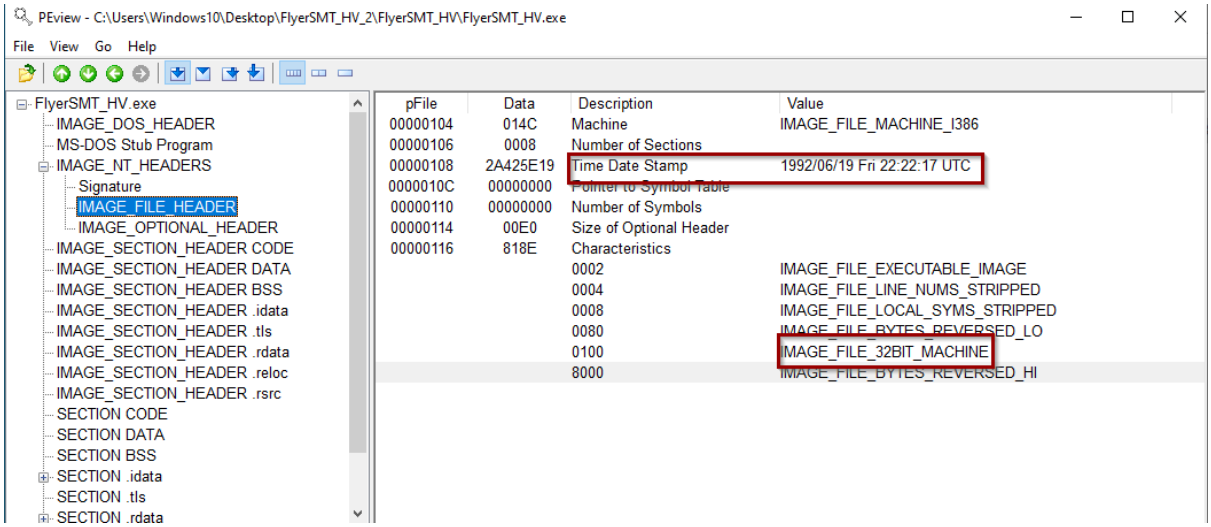
Strings

The strings of interest are as shown in the figure below

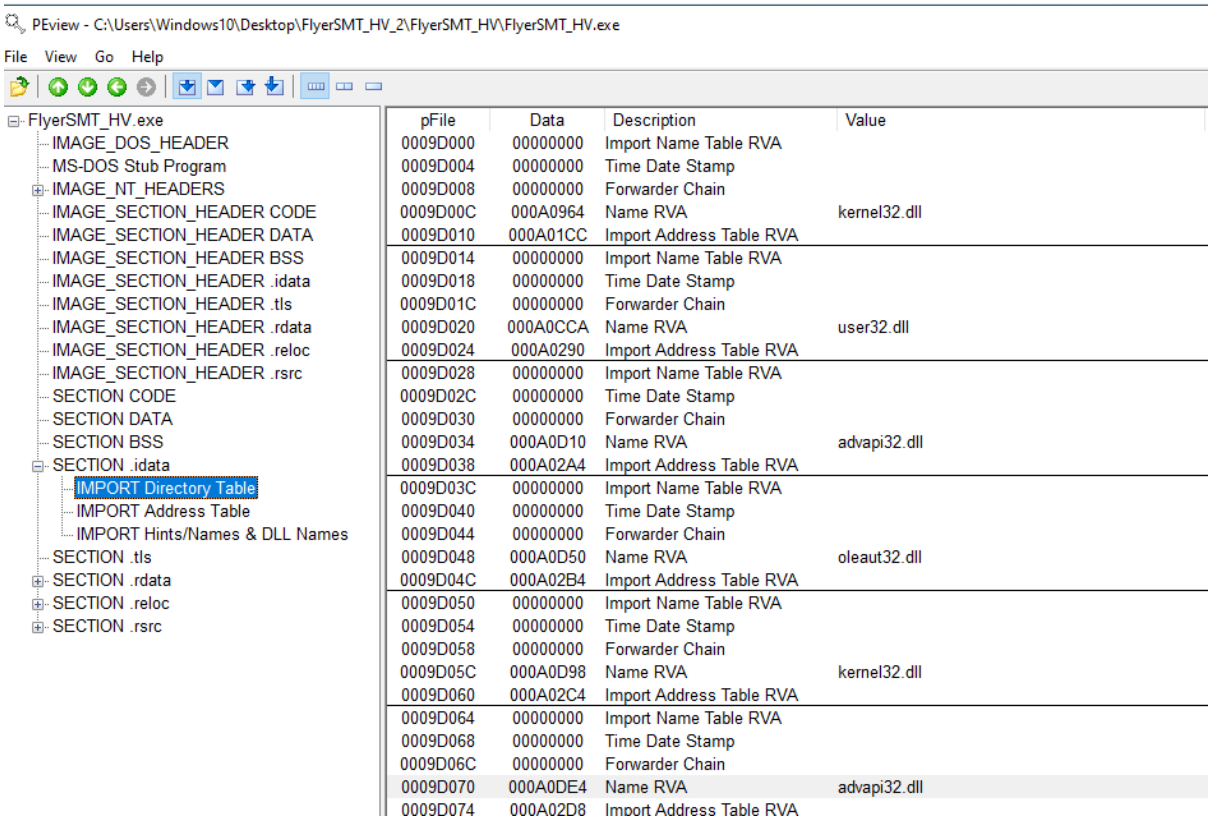


PEView

PEView was used to gain the header information of the malware. It was identified that the malware Time Date Stamp was 1992/06/19 Fri 22:22:17 UTC. The malware runs in 32 bit machine as shown in the figure below.



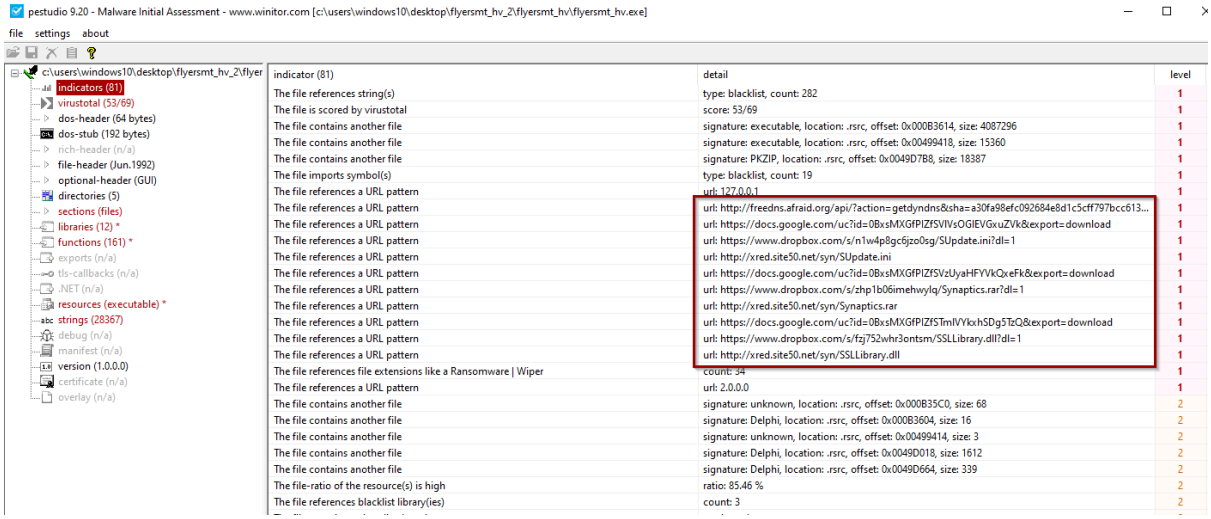
The malware has the following imports



PEStudio

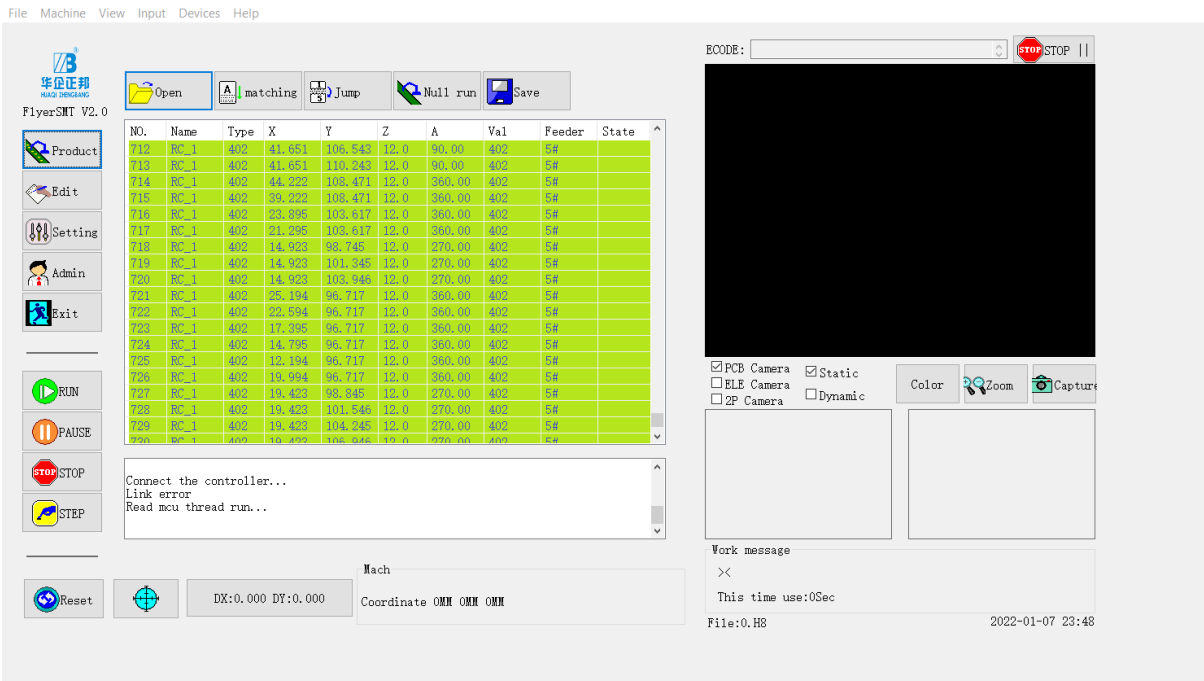
This tool was used to gain more information about the malware. The information gathered includes the indicators, the virustotal flags, and strings. Similar strings as indicated by the

strings.exe tool was identified. There were a total of 81 indicators of comprise, as shown in the figure below



Dynamic analysis

Dynamic analysis involves the analysis of the malware while the program is running. It uses different tools in the process, including procmon, process explorer, and regshot, which are all run before the malware is run (Ucci et al., 2019). Stimulation of the network by fakenet makes the malware run so that the analyst comprehends the analysis of what it does in the. Malware is also analyzed through regshot in the registry files, where the shots are taken simultaneously and compared. When the malware is run, a graphical user interface pops as shown in the figure below



Regshot

This tool allows an analyst to take two snapshots of the registry. The first snapshot is takes before the malware is executed and the second is taken after the malware is executed. The comparison of two snapshots helps the analyst identify the changes the malware makes in the registry, giving more indication as to what the malware is capable of, in case there is any files that are dropped or modified.The malware accesses the registry and makes different actions including deleting registry keys, adding values, and modifying values. There was a total of 221 changes made on the registry as shown in the figure below

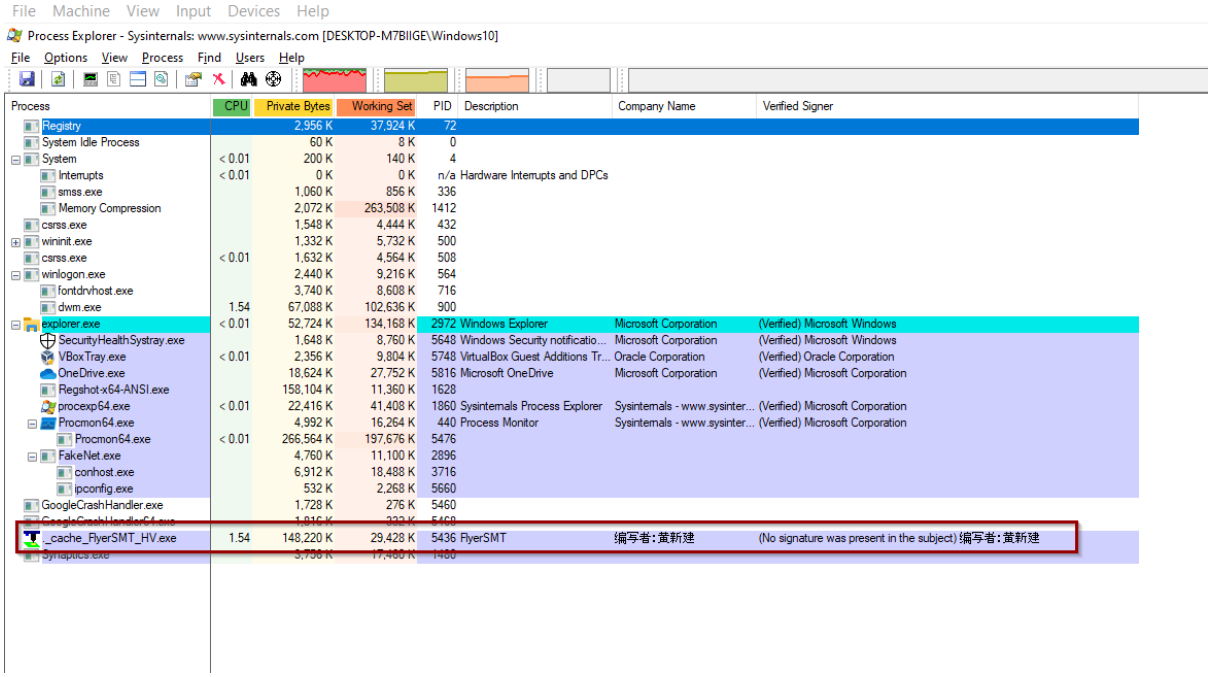
```
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\NcsiUwpApp_8wekyb3d8bbwe\HAM\AUI\App
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\NcsiUwpApp_8wekyb3d8bbwe\HAM\AUI\App
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx:  01 00 00 00 05 00 00 00 08 00 00 00 03 00 00 00 0
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx:  03 00 00 00 01 00 00 00 05 00 00 00 08 00 00 00 0
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\MRUListEx:  01 00 00 00 03 00 00 00 04 00 00 00 02 00 00 00
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\MRUListEx:  03 00 00 00 04 00 00 00 01 00 00 00 02 00 00 00
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1920x950x96(1).x: 0xFFFF8300
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1920x950x96(1).x: 0xFFFFFFFF
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1920x950x96(1).y: 0xFFFF8300
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1920x950x96(1).y: 0xFFFFFFFF
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x950x96(1).left: 0x00000000
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x950x96(1).left: 0x000001A9
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x950x96(1).top: 0x00000002
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x950x96(1).top: 0x00000030
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x950x96(1).right: 0x0000028C
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x950x96(1).right: 0x00000435
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x950x96(1).bottom: 0x000001BF
HKU\S-1-5-21-2081364252-1438397395-3132659045-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x950x96(1).bottom: 0x000001ED

----------------------------------
Total changes: 221
----------------------------------
```

Comparing the two snapshots, it was identified that the malware accesses the Current User Hive.

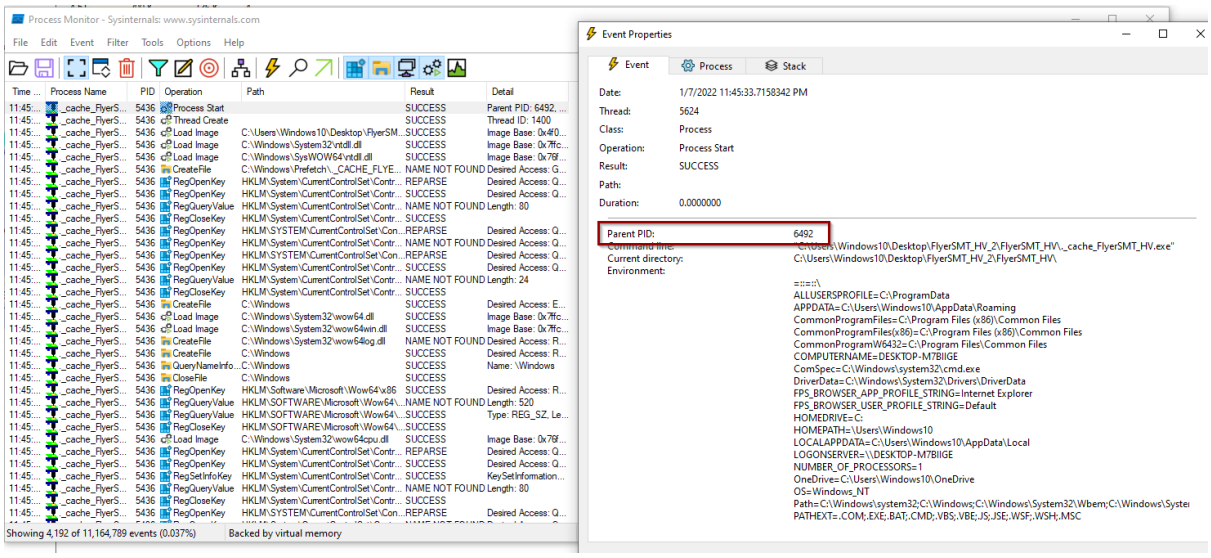
Process Explorer

Process Explorer tool gives access to the information when the malware executes. It offers a range of functionalities that are important to analyze the file (Chakkaravarthy et al., 2019). It was identified that the malware initiates a child process and then it kills the parent process. The child process was running with PID 5436. The color in the tool indicated that the malware is its process and is not packed. When verifying the signature, it was identified that the malware did not have any signature assigned to it as shown in the figure below. It means that the file has a malicious activity.



Procmon

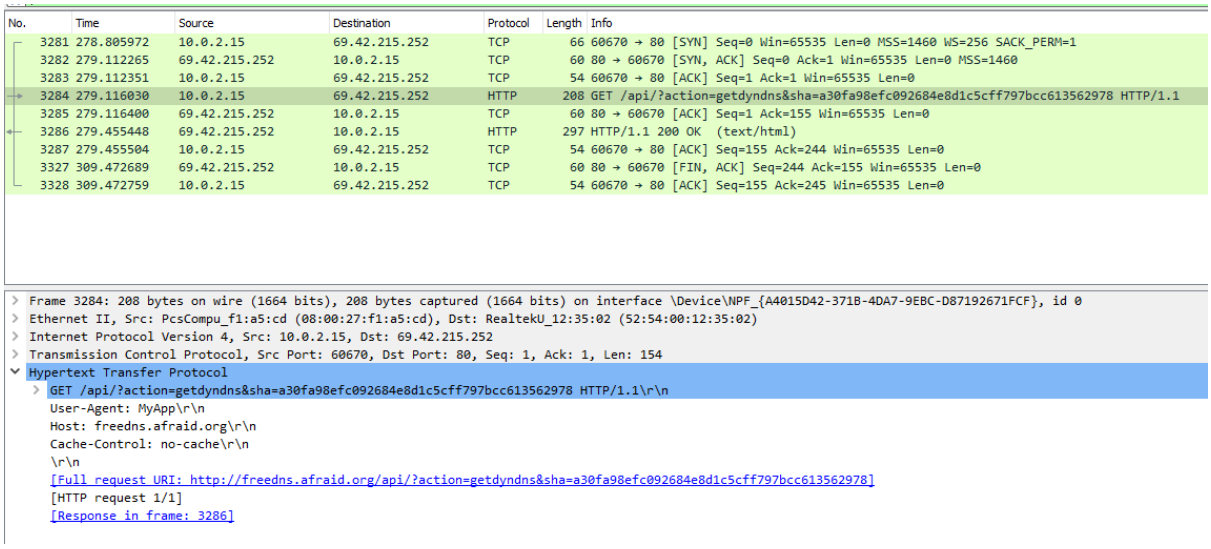
This tool shows the real-time process activities, registry, and file systems. Similar to other malware dynamic analysis tools, ProcMon was executed before malware execution. The malware was filtered using the PID from process explorer and analysis was done to check the registry activities, file activities, and process/thread activities. After filtering the activities, it was identified that the malware's parent PID is 6492 as shown in the figure below. The malware accessed different files including



Wireshark

Wireshark was used to analyze the communication of the malware. It was identified that there is a traffic communication between the source, 10.0.2.15, and the destination, 69.42.215.252.

It initiates a http get method when it gets the dynamic DNS and sends to http://freedns.afraid.org/ as shown in the figure below.



No.	Time	Source	Destination	Protocol	Length	Info
3281	278.805972	10.0.2.15	69.42.215.252	TCP	66	60670 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
3282	279.112265	69.42.215.252	10.0.2.15	TCP	60	80 → 60670 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
3283	279.112351	10.0.2.15	69.42.215.252	TCP	54	60670 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
3284	279.116030	10.0.2.15	69.42.215.252	HTTP	208	GET /api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978 HTTP/1.1
3285	279.116400	69.42.215.252	10.0.2.15	TCP	60	80 → 60670 [ACK] Seq=1 Ack=155 Win=65535 Len=0
3286	279.455448	69.42.215.252	10.0.2.15	HTTP	297	HTTP/1.1 200 OK (text/html)
3287	279.455504	10.0.2.15	69.42.215.252	TCP	54	60670 → 80 [ACK] Seq=155 Ack=244 Win=65535 Len=0
3327	309.472689	69.42.215.252	10.0.2.15	TCP	60	80 → 60670 [FIN, ACK] Seq=244 Ack=155 Win=65535 Len=0
3328	309.472759	10.0.2.15	69.42.215.252	TCP	54	60670 → 80 [ACK] Seq=155 Ack=245 Win=65535 Len=0

```
> Frame 3284: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{A4015D42-371B-4DA7-9EBC-D87192671FCF}, id 0
> Ethernet II, Src: PcsCompu_f1:a5:cd (08:00:27:f1:a5:cd), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 69.42.215.252
> Transmission Control Protocol, Src Port: 60670, Dst Port: 80, Seq: 1, Ack: 1, Len: 154
v Hypertext Transfer Protocol
  > GET /api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978 HTTP/1.1\r\n
    User-Agent: MyApp\r\n
    Host: freedns.afraid.org\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://freedns.afraid.org/api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978]
    [HTTP request 1/1]
    [Response in frame: 3286]
```

Conclusion

The malware analysis presented in this paper has involved static analysis, dynamic analysis, and reverse engineering. The static analysis helped to gather information about the malware when it was at rest. The hash values, flags from antivirus engines, the header information, and the strings of interest are some of the information gathered from the static analysis. Dynamic analysis was used to gather more information about the malware. In the dynamic malware analysis, the malware was analyzed while running. Before its execution, the corresponding tools including regshot, ProcMon, Process explorer, fakenet, and Wireshark were set. The process explorer and procmon helped to know that the malware created a child process and then killed the process. It was also identified that the file did not have the signature but had the company name, and the path, confirming that it is a suspicious file from a legitimate organization. The regshot helped in getting the two snapshots of the registry, one before execution and one after malware execution. Therefore, it can be concluded that the file analyzed contains a trojan spyware which creates a child process that kills the original file when run. The malware collects user information and sends it to http://freedns.afraid.org/.

To remove the malware, follow the following steps

1. Start the PC in safe mode by opening system configuration, navigating to boot and then safe boot.
2. Show hidden files and folders from control panel
3. Remove all files from startup since it may contain autorun apps with trojans

4. Modify regedit file in the folder RUN
5. Clean the Temp folder
6. Start windows normally

References

Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2019). Dynamic malware analysis in the modern era—A state of the art survey. *ACM Computing Surveys (CSUR)*, *52*(5), 1-48.

Ucci, D., Aniello, L., & Baldoni, R. (2019). Survey of machine learning techniques for malware analysis. *Computers & Security*, *81*, 123-147.

Chakkaravarthy, S. S., Sangeetha, D., & Vaidehi, V. (2019). A Survey on malware analysis and mitigation techniques. *Computer Science Review*, *32*, 1-23.