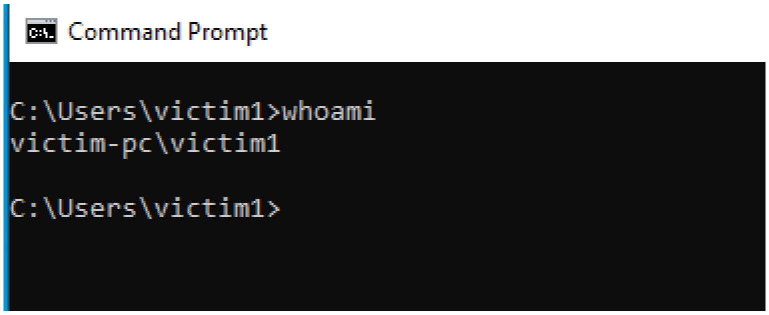
Assignment 3
Submission

Team Members:
Shubham Mazumder (u1320525)
Yeaseen Arafat (u1464680)
Yu Pan (u1320985)
Md Raihan Ahmed (u1374605)

Part A:

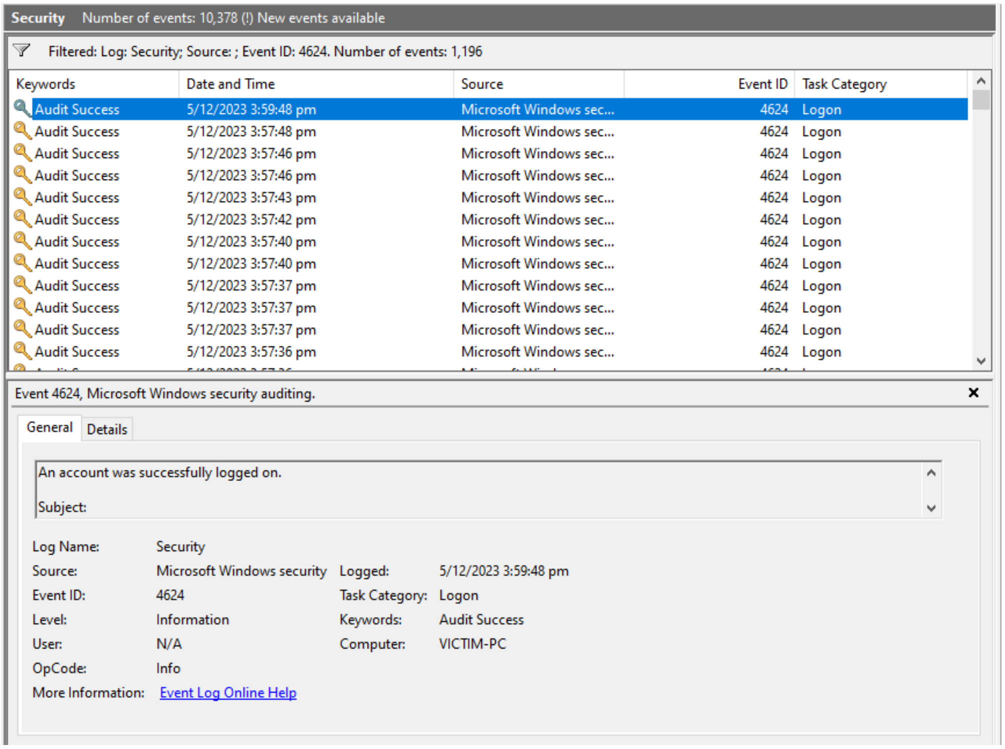
1. What is the machine user's name?



```
C:\Users\victim1>whoami
victim-pc\victim1

C:\Users\victim1>
```

Ans: **victim1**

2. What time was the user's most recent login? Convert the time to UTC.



Filtered: Log: Security; Source: ; Event ID: 4624. Number of events: 1,196

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	5/12/2023 3:59:48 pm	Microsoft Windows sec...	4624	Logon
Audit Success	5/12/2023 3:57:48 pm	Microsoft Windows sec...	4624	Logon
Audit Success	5/12/2023 3:57:46 pm	Microsoft Windows sec...	4624	Logon
Audit Success	5/12/2023 3:57:46 pm	Microsoft Windows sec...	4624	Logon
Audit Success	5/12/2023 3:57:43 pm	Microsoft Windows sec...	4624	Logon
Audit Success	5/12/2023 3:57:42 pm	Microsoft Windows sec...	4624	Logon
Audit Success	5/12/2023 3:57:40 pm	Microsoft Windows sec...	4624	Logon
Audit Success	5/12/2023 3:57:40 pm	Microsoft Windows sec...	4624	Logon
Audit Success	5/12/2023 3:57:37 pm	Microsoft Windows sec...	4624	Logon
Audit Success	5/12/2023 3:57:37 pm	Microsoft Windows sec...	4624	Logon
Audit Success	5/12/2023 3:57:37 pm	Microsoft Windows sec...	4624	Logon
Audit Success	5/12/2023 3:57:36 pm	Microsoft Windows sec...	4624	Logon

Event 4624, Microsoft Windows security auditing.

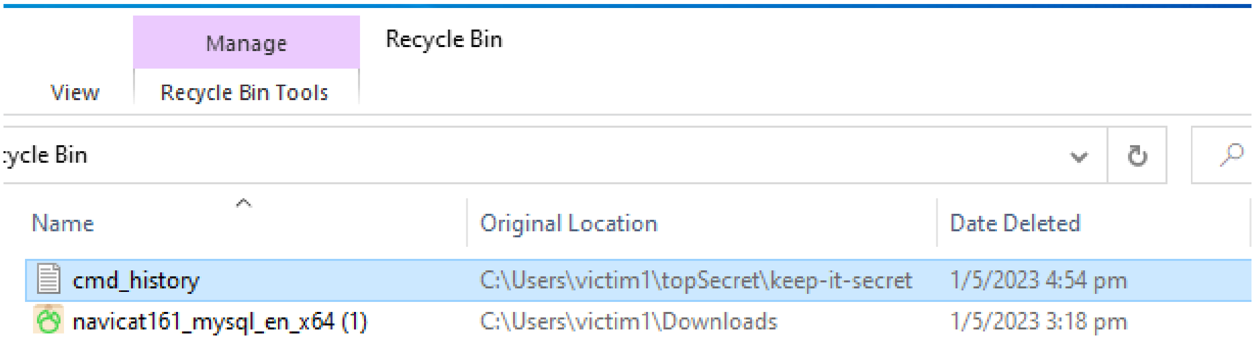
An account was successfully logged on.

Subject:

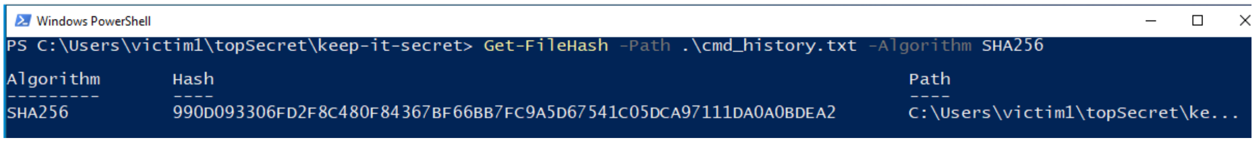
Log Name:	Security		
Source:	Microsoft Windows security	Logged:	5/12/2023 3:59:48 pm
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	VICTIM-PC
OpCode:	Info		
More Information:	Event Log Online Help		

Ans: **21/11/2023 4:34:39 pm** (From Event ID:4624)

3. A TXT file was deleted. What is the SHA256 hash value of the zip file?



Name	Original Location	Date Deleted
cmd_history	C:\Users\victim1\topSecret\keep-it-secret	1/5/2023 4:54 pm
navicat161_mysql_en_x64 (1)	C:\Users\victim1\Downloads	1/5/2023 3:18 pm



```
PS C:\Users\victim1\topSecret\keep-it-secret> Get-FileHash -Path .\cmd_history.txt -Algorithm SHA256

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          990D093306FD2F8C480F84367BF66BB7FC9A5D67541C05DCA97111DA0A0BDEA2       C:\Users\victim1\topSecret\ke...
```

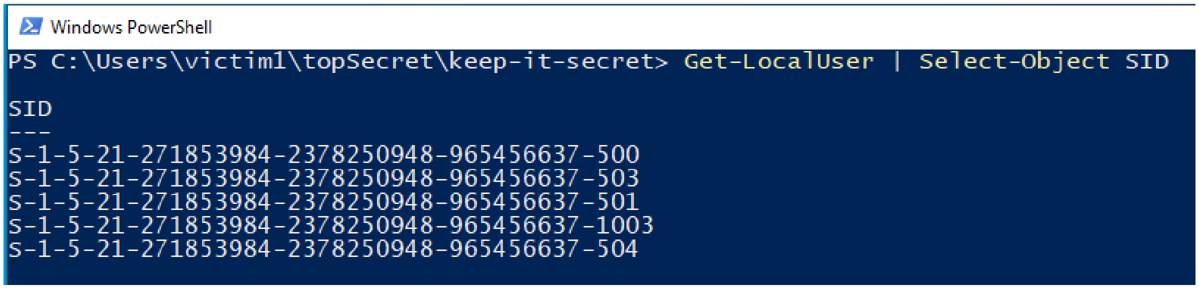
We went to the Recycle Bin and found a file named “**cmd_history.txt**”.

The SHA256 hash of this file is: **“990D093306FD2F8C480F84367BF66BB7FC9A5D67541C05DCA97111DA0A0BDEA2”**.

4. RID questions:

a. How many users have a RID of 1000 or above on the machine?

`Using command: “Get-LocalUser | Select-Object SID”`

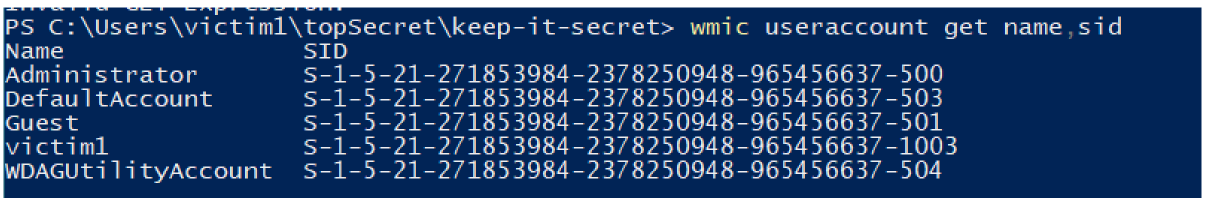


```
PS C:\Users\victim1\topSecret\keep-it-secret> Get-LocalUser | Select-Object SID

SID
---
S-1-5-21-271853984-2378250948-965456637-500
S-1-5-21-271853984-2378250948-965456637-503
S-1-5-21-271853984-2378250948-965456637-501
S-1-5-21-271853984-2378250948-965456637-1003
S-1-5-21-271853984-2378250948-965456637-504
```

Answer: **1 (1003)**

b. What is the account name for RID of 501?

`Using command: “wmic useraccount get name, sid”`



```
PS C:\Users\victim1\topSecret\keep-it-secret> wmic useraccount get name,sid
Name                  SID
Administrator         S-1-5-21-271853984-2378250948-965456637-500
DefaultAccount        S-1-5-21-271853984-2378250948-965456637-503
Guest                 S-1-5-21-271853984-2378250948-965456637-501
victim1               S-1-5-21-271853984-2378250948-965456637-1003
WDAGUtilityAccount    S-1-5-21-271853984-2378250948-965456637-504
```

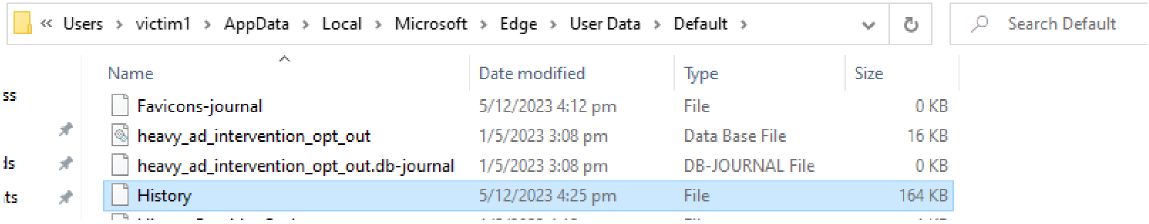
Answer: **Guest**

c. What is the account name for RID of 1003?

`Using command: “wmic useraccount get name, sid”`

Answer: **victim1**

5. **User-specific questions:**

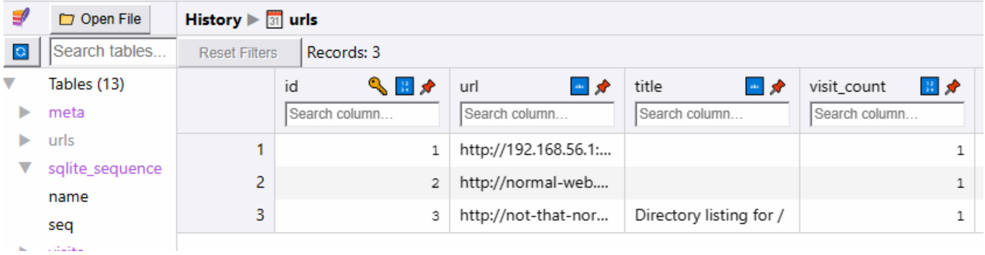


« Users › victim1 › AppData › Local › Microsoft › Edge › User Data › Default ›

Search Default

Name	Date modified	Type	Size
Favicons-journal	5/12/2023 4:12 pm	File	0 KB
heavy_ad_intervention_opt_out	1/5/2023 3:08 pm	Data Base File	16 KB
heavy_ad_intervention_opt_out.db-journal	1/5/2023 3:08 pm	DB-JOURNAL File	0 KB
History	5/12/2023 4:25 pm	File	164 KB

For this, we copied the 'History' DB from "C:\Users\<username>\AppData\Local\Microsoft\Edge\User Data\Default" and opened it on SQLite Viewer.



History ▶ urls

Records: 3

	id	url	title	visit_count
1	1	http://192.168.56.1:...		1
2	2	http://normal-web....		1
3	3	http://not-that-nor...	Directory listing for /	1

a. **How many times did the user visit http://not-that-normal.site?**

   1

b. **How many times did the user visit http://normal-web.site:8000?**

   1

c. **How many times did the user visit https://www.live.com?**

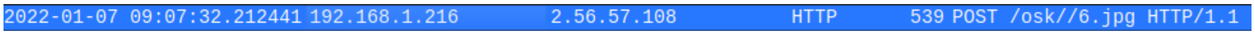
   0

Part B:

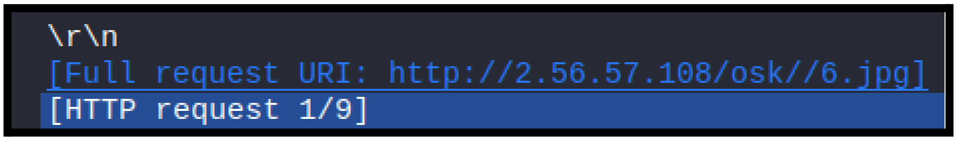
1. What is the security incident?

The security incident is that on 2022-01-07 at 09:07:32 UTC, a Windows host was infected with “**OskiStealer C2**” malware.

We found a suspicious IP in Wireshark through packet analysis in an HTTP request created from 192.168.1.216 at the aforementioned time.

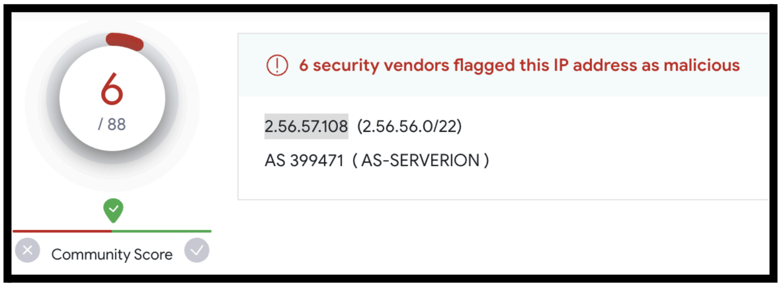


```
2022-01-07 09:07:32.212441 192.168.1.216          2.56.57.108          HTTP        539 POST /osk//6.jpg HTTP/1.1
```



```
\r\n
[Full request URI: http://2.56.57.108/osk//6.jpg]
[HTTP request 1/9]
```

This requested suspicious URI was “http://2.56.57.108/osk//6.jpg”.
We looked up the IP on VirusTotal and saw that the IP is malicious.



6
/ 88

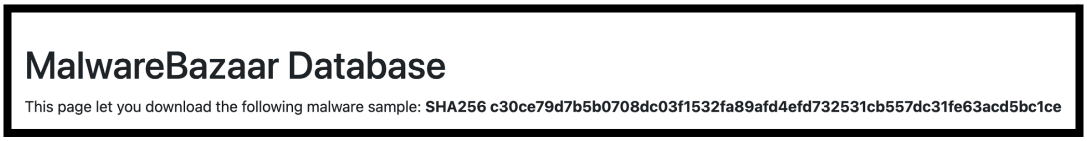
Community Score

6 security vendors flagged this IP address as malicious

2.56.57.108 (2.56.56.0/22)

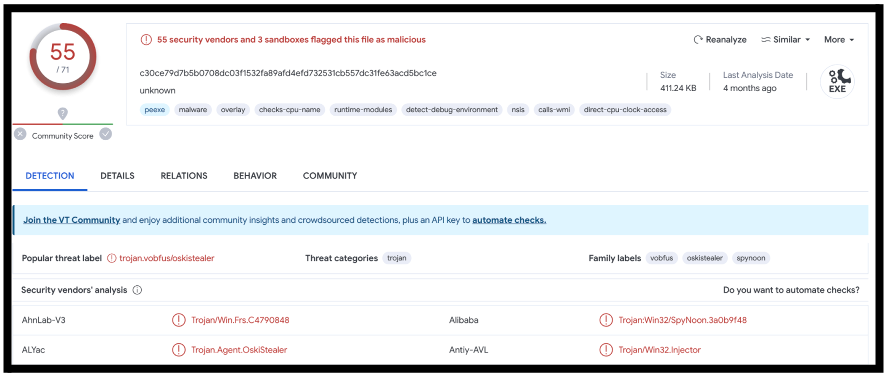
AS 399471 (AS-SERVERION)

We dumped the file from the pcap and submitted it to VirusTotal and got the result as Malicious.



MalwareBazaar Database

This page let you download the following malware sample: **SHA256 c30ce79d7b5b0708dc03f1532fa89afd4efd732531cb557dc31fe63acd5bc1ce**



55
/ 71

Community Score

55 security vendors and 3 sandboxes flagged this file as malicious

c30ce79d7b5b0708dc03f1532fa89afd4efd732531cb557dc31fe63acd5bc1ce

unknown

peexe malware overlay checks-cpu-name runtime-modules detect-debug-environment nsis calls-wmi direct-cpu-clock-access

Size 411.24 KB

Last Analysis Date 4 months ago

EXE

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

Popular threat label trojan.vobfus/oskistealer

Threat categories trojan

Family labels vobfus oskistealer spynoon

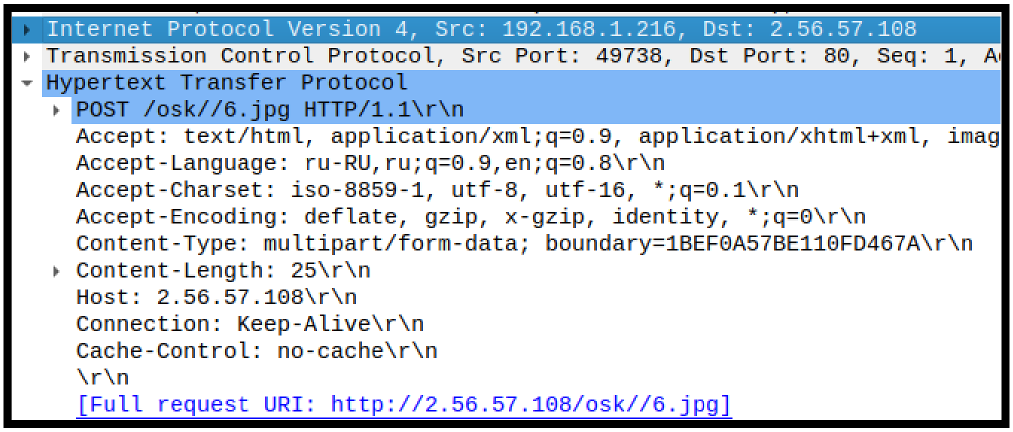
Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win.Frs.C4790848	Alibaba	Trojan:Win32/SpyNoon.3a0b9f48
ALYac	Trojan.Agent.OskiStealer	Antiy-AVL	Trojan/Win32.Injector

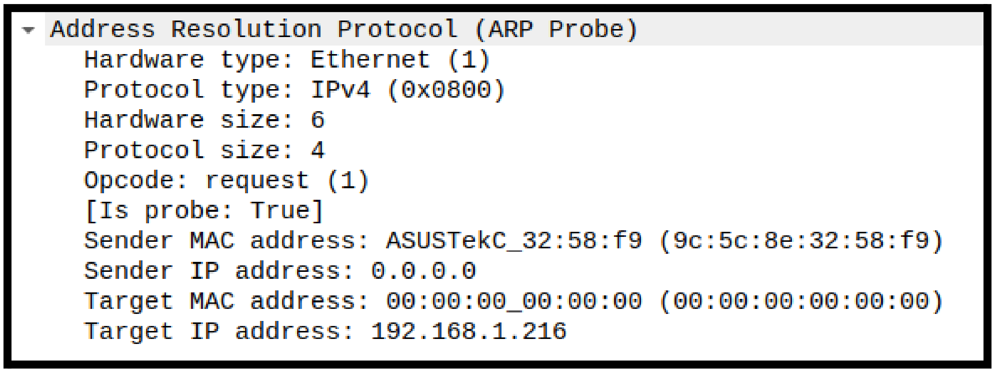
2. What is the identity of the victim?

a. **Victim IP: 192.168.1.216**
Using filter (http) which requests http://2.56.57.108/osk//6.jpg



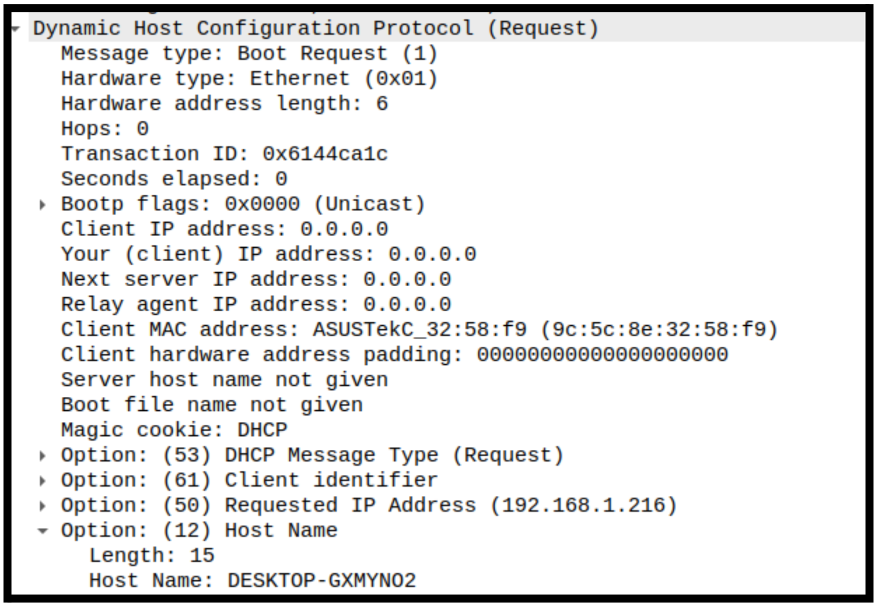
```
▸ Internet Protocol Version 4, Src: 192.168.1.216, Dst: 2.56.57.108
▸ Transmission Control Protocol, Src Port: 49738, Dst Port: 80, Seq: 1, A
▾ Hypertext Transfer Protocol
  ▸ POST /osk//6.jpg HTTP/1.1\r\n
    Accept: text/html, application/xml;q=0.9, application/xhtml+xml, imag
    Accept-Language: ru-RU,ru;q=0.9,en;q=0.8\r\n
    Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1\r\n
    Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0\r\n
    Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A\r\n
  ▸ Content-Length: 25\r\n
    Host: 2.56.57.108\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://2.56.57.108/osk//6.jpg]
```

b. **MAC Address: ASUSTTekC_32:58:f9** (9c:5c:8e:32:58:f9)
Using filter (arp)



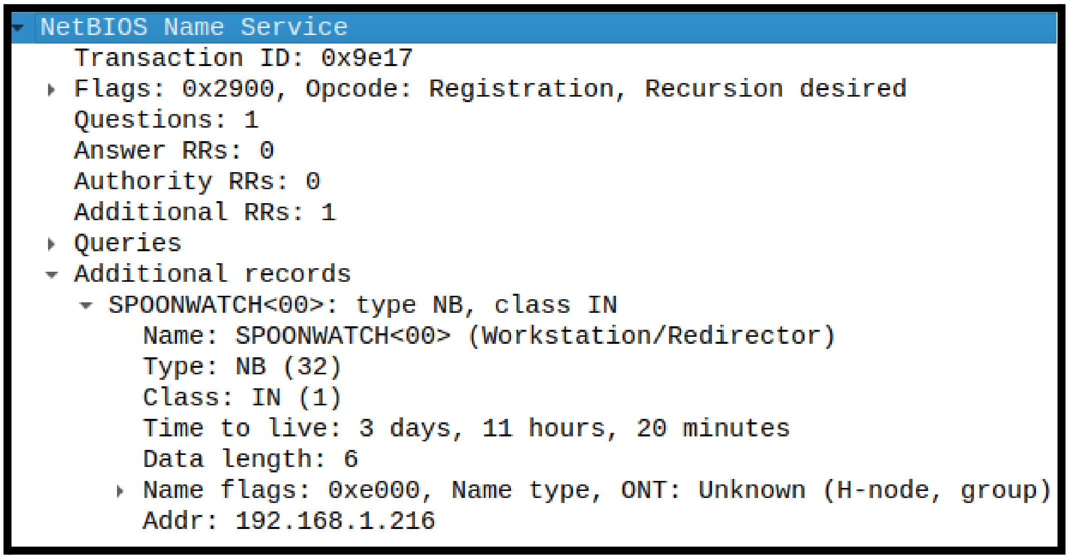
```
▾ Address Resolution Protocol (ARP Probe)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is probe: True]
    Sender MAC address: ASUSTekC_32:58:f9 (9c:5c:8e:32:58:f9)
    Sender IP address: 0.0.0.0
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.216
```

c. **Computer Name: DESKTOP-GXNYNO2**
Using filter (dhcp)



```
▾ Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x6144ca1c
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: ASUSTekC_32:58:f9 (9c:5c:8e:32:58:f9)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Request)
  ▸ Option: (61) Client identifier
  ▸ Option: (50) Requested IP Address (192.168.1.216)
  ▾ Option: (12) Host Name
      Length: 15
      Host Name: DESKTOP-GXMYNO2
```

d. **Username: SPOONWATCH**
Using filter (nbns)

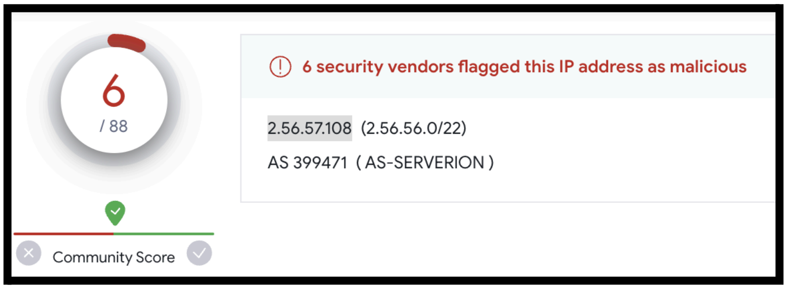


```
▾ NetBIOS Name Service
    Transaction ID: 0x9e17
  ▸ Flags: 0x2900, Opcode: Registration, Recursion desired
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▾ Additional records
    ▾ SPOONWATCH<00>: type NB, class IN
        Name: SPOONWATCH<00> (Workstation/Redirector)
        Type: NB (32)
        Class: IN (1)
        Time to live: 3 days, 11 hours, 20 minutes
        Data length: 6
      ▸ Name flags: 0xe000, Name type, ONT: Unknown (H-node, group)
        Addr: 192.168.1.216
```

3. What is the evidence of attack (i.e., that the machine has been attacked)?

Following the steps in Question 1, we saw that the victim requested URI "http://2.56.57.108/osk//6.jpg".

We looked up the IP in VirusTotal and saw that the IP is malicious.

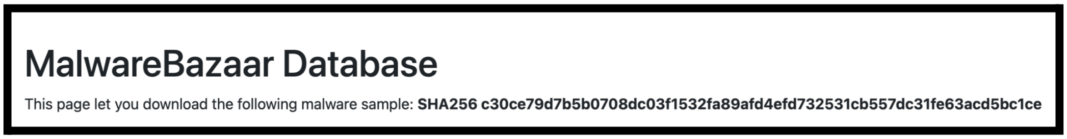


6 security vendors flagged this IP address as malicious

2.56.57.108 (2.56.56.0/22)

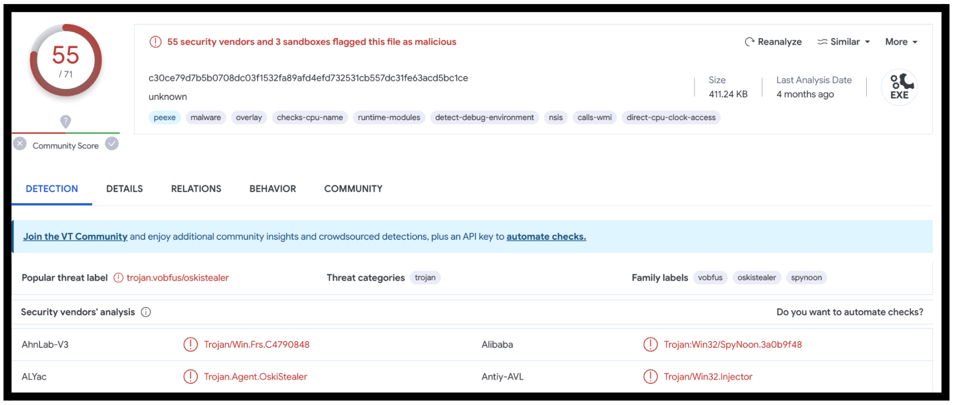
AS 399471 (AS-SERVERION)

We downloaded the file and submitted it to VirusTotal and got the result as Malicious.



MalwareBazaar Database

This page let you download the following malware sample: **SHA256 c30ce79d7b5b0708dc03f1532fa89afd4efd732531cb557dc31fe63acd5bc1ce**



55 security vendors and 3 sandboxes flagged this file as malicious

c30ce79d7b5b0708dc03f1532fa89afd4efd732531cb557dc31fe63acd5bc1ce

unknown

Size 411.24 KB

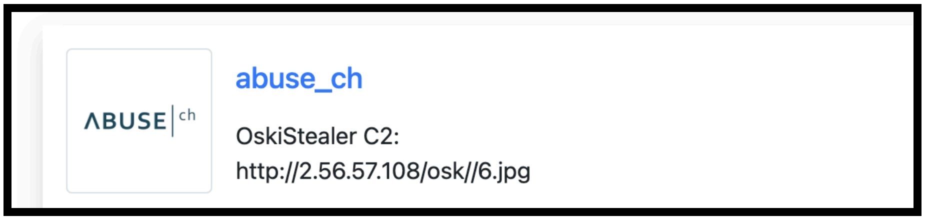
Last Analysis Date 4 months ago

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

Popular threat label trojan.vobfus/oskistealer   Threat categories trojan   Family labels vobfus oskistealer spynoon

Security vendors' analysis   Do you want to automate checks?

AhnLab-V3	Trojan/Win.Frs.C4790848	Alibaba	Trojan:Win32/SpyNoon.3a0b9f48
ALYac	Trojan.Agent.OskiStealer	Antiy-AVL	Trojan/Win32.Injector

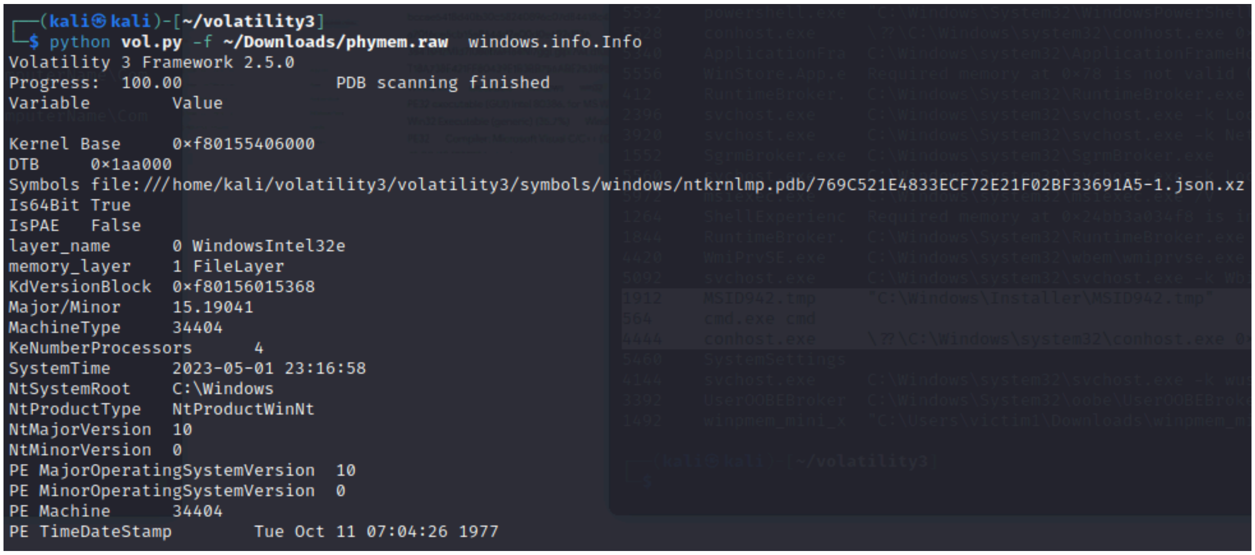


abuse_ch

OskiStealer C2:
http://2.56.57.108/osk//6.jpg

Part C:

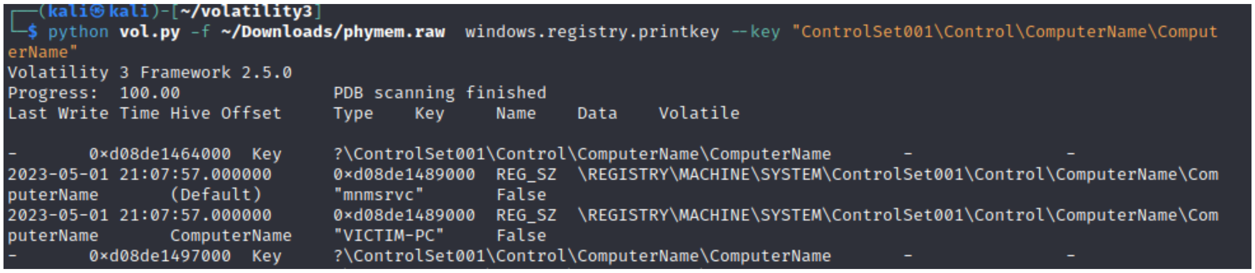
1. **Please identify the Windows Major Version (e.g., XP, Vista, Windows 8, etc.), bit version (32-bit or 64-bit), and the image date/time (please use UTC).**



```
┌──(kali㉿kali)-[~/volatility3]
└─$ python vol.py -f ~/Downloads/phymem.raw  windows.info.Info
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0xf80155406000
DTB     0x1aa000
Symbols file:///home/kali/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/769C521E4833ECF72E21F02BF33691A5-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf80156015368
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      4
SystemTime      2023-05-01 23:16:58
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Tue Oct 11 07:04:26 1977
```

Windows Version: Windows 10
Bit Version: 64 because 64 Bit is True
Image date/time: 2023-05-01 23:16:58

2. What is the name of the computer?

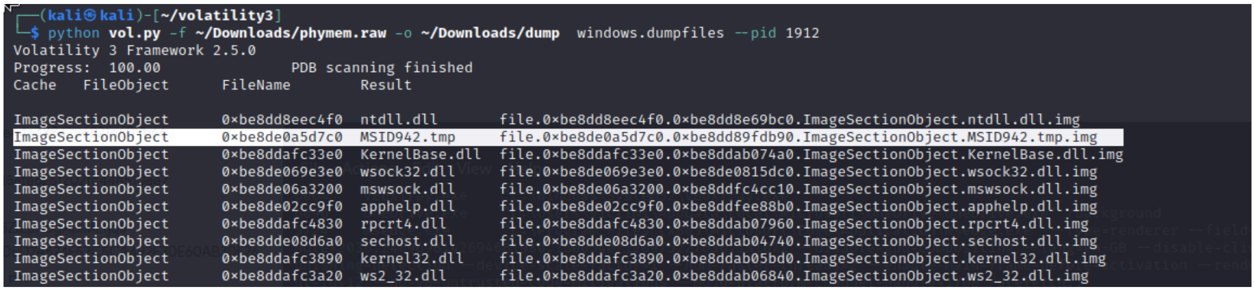


```
┌──(kali㉿kali)-[~/volatility3]
└─$ python vol.py -f ~/Downloads/phymem.raw  windows.registry.printkey --key "ControlSet001\Control\ComputerName\Comput
erName"
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Last Write Time Hive Offset     Type    Key     Name    Data    Volatile

-       0×d08de1464000  Key     ?\ControlSet001\Control\ComputerName\ComputerName       -               -
2023-05-01 21:07:57.000000      0×d08de1489000  REG_SZ  \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\ComputerName\Com
puterName       (Default)       "mnmsrvc"       False
2023-05-01 21:07:57.000000      0×d08de1489000  REG_SZ  \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\ComputerName\Com
puterName       ComputerName    "VICTIM-PC"     False
-       0×d08de1497000  Key     ?\ControlSet001\Control\ComputerName\ComputerName       -               -
```

Computer Name: **VICTIM-PC**

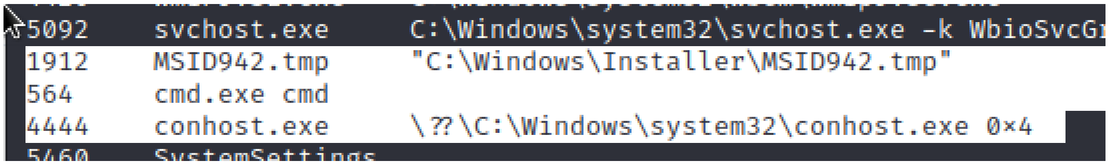
3. What is the name of the malicious process?

The malicious process appears to be **conhost.exe** which is started by **cmd.exe**, which is in turn initiated by **MSID942.tmp** from an abnormal location.



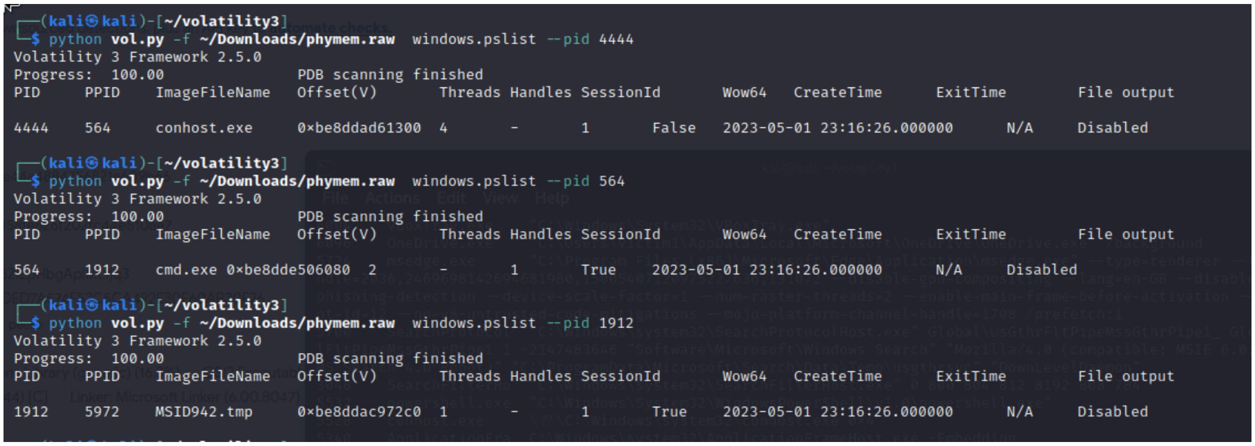
```
┌──(kali㉿kali)-[~/volatility3]
└─$ python vol.py -f ~/Downloads/phymem.raw -o ~/Downloads/dump  windows.dumpfiles --pid 1912
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

ImageSectionObject      0×be8dd8eec4f0  ntdll.dll       file.0×be8dd8eec4f0.0×be8dd8e69bc0.ImageSectionObject.ntdll.dll.img
ImageSectionObject      0×be8de0a5d7c0  MSID942.tmp     file.0×be8de0a5d7c0.0×be8dd89fdb90.ImageSectionObject.MSID942.tmp.img
ImageSectionObject      0×be8ddafc33e0  KernelBase.dll  file.0×be8ddafc33e0.0×be8ddab074a0.ImageSectionObject.KernelBase.dll.img
ImageSectionObject      0×be8de069e3e0  wsock32.dll     file.0×be8de069e3e0.0×be8de0815dc0.ImageSectionObject.wsock32.dll.img
ImageSectionObject      0×be8de06a3200  mswsock.dll     file.0×be8de06a3200.0×be8ddfc4cc10.ImageSectionObject.mswsock.dll.img
ImageSectionObject      0×be8de02cc9f0  apphelp.dll     file.0×be8de02cc9f0.0×be8ddfee88b0.ImageSectionObject.apphelp.dll.img
ImageSectionObject      0×be8ddafc4830  rpcrt4.dll      file.0×be8ddafc4830.0×be8ddab07960.ImageSectionObject.rpcrt4.dll.img
ImageSectionObject      0×be8dde08d6a0  sechost.dll     file.0×be8dde08d6a0.0×be8ddab04740.ImageSectionObject.sechost.dll.img
ImageSectionObject      0×be8ddafc3890  kernel32.dll    file.0×be8ddafc3890.0×be8ddab05bd0.ImageSectionObject.kernel32.dll.img
ImageSectionObject      0×be8ddafc3a20  ws2_32.dll      file.0×be8ddafc3a20.0×be8ddab06840.ImageSectionObject.ws2_32.dll.img
```

MSID942.tmp has a PID of 1912 and runs cmd.exe, which calls conhost.exe.



```
5092    svchost.exe     C:\Windows\system32\svchost.exe -k WbioSvcGr
1912    MSID942.tmp     "C:\Windows\Installer\MSID942.tmp"
564     cmd.exe cmd
4444    conhost.exe     \??\C:\Windows\system32\conhost.exe 0×4
5460    SystemSettings
```

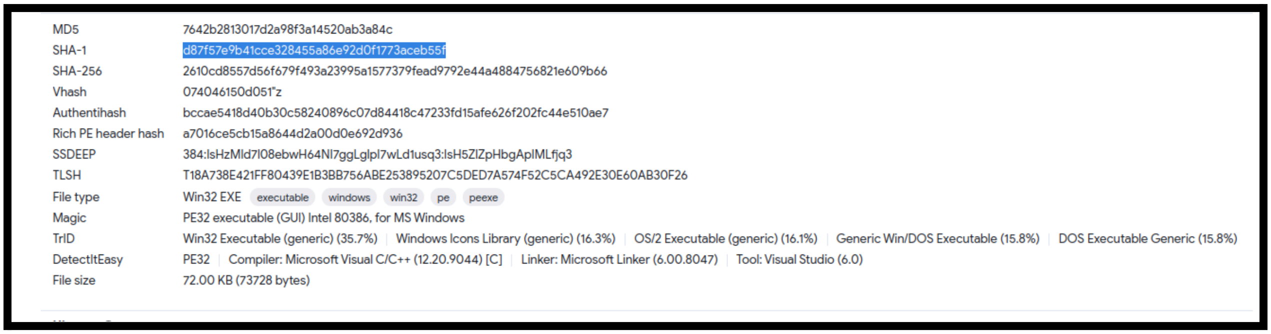
Details of each of these processes:



```
┌──(kali㉿kali)-[~/volatility3]
└─$ python vol.py -f ~/Downloads/phymem.raw  windows.pslist --pid 4444
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4444    564     conhost.exe     0xbe8ddad61300  4       -       1       False   2023-05-01 23:16:26.000000      N/A     Disabled

┌──(kali㉿kali)-[~/volatility3]
└─$ python vol.py -f ~/Downloads/phymem.raw  windows.pslist --pid 564
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

564     1912    cmd.exe 0xbe8dde506080  2       -       1       True    2023-05-01 23:16:26.000000      N/A     Disabled

┌──(kali㉿kali)-[~/volatility3]
└─$ python vol.py -f ~/Downloads/phymem.raw  windows.pslist --pid 1912
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

1912    5972    MSID942.tmp     0xbe8ddac972c0  1       -       1       True    2023-05-01 23:16:26.000000      N/A     Disabled
```

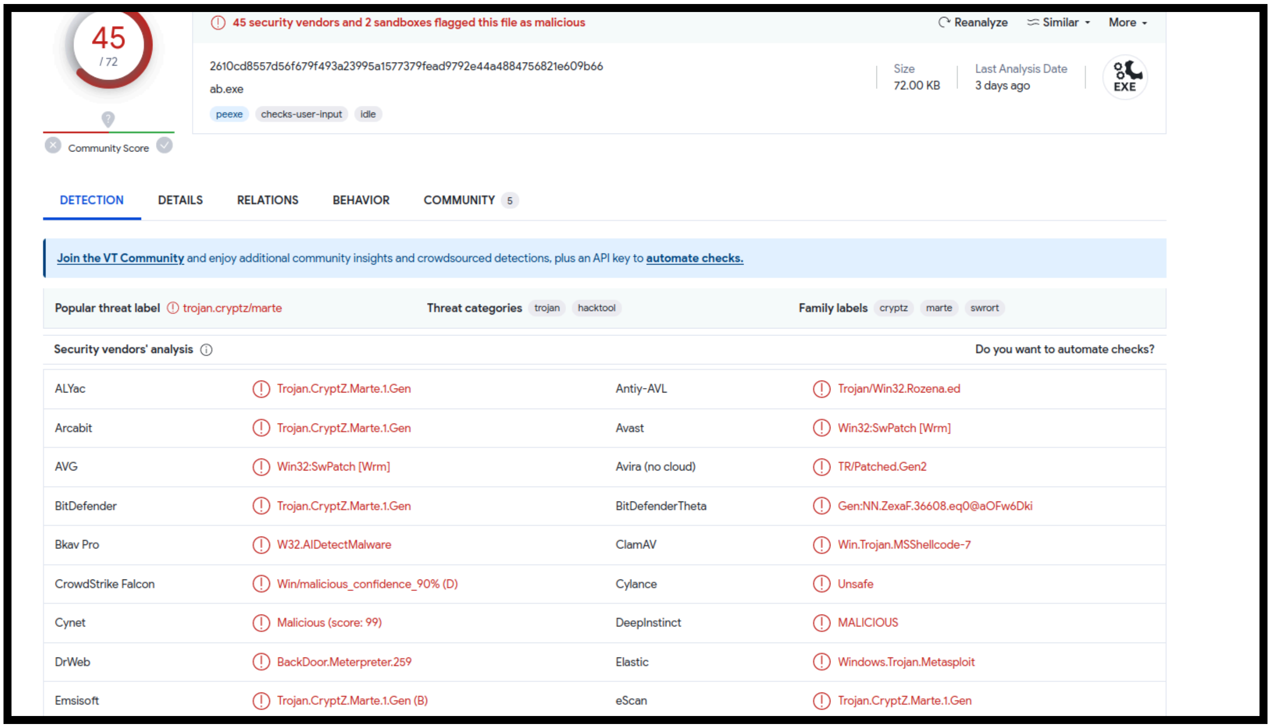
4. **What is the SHA1 checksum of the program supporting the malicious process?**

The SHA1 hash of the malicious program [**MSID942.tmp**] is: **d87f57e9b41cce328455a86e92d0f1773aceb55f**



MD5	7642b2813017d2a98f3a14520ab3a84c
SHA-1	d87f57e9b41cce328455a86e92d0f1773aceb55f
SHA-256	2610cd8557d56f679f493a23995a1577379fead9792e44a4884756821e609b66
Vhash	074046150d051"z
Authentihash	bccae5418d40b30c58240896c07d84418c47233fd15afe626f202fc44e510ae7
Rich PE header hash	a7016ce5cb15a8644d2a00d0e692d936
SSDEEP	384:lsHzMld7l08ebwH64Nl7ggLglpl7wLd1usq3:lsH5ZlZpHbgAplMLfjq3
TLSH	T18A738E421FF80439E1B3BB756ABE253895207C5DED7A574F52C5CA492E30E60AB30F26
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable (generic) (35.7%) | Windows Icons Library (generic) (16.3%) | OS/2 Executable (generic) (16.1%) | Generic Win/DOS Executable (15.8%) | DOS Executable Generic (15.8%)
DetectItEasy	PE32 | Compiler: Microsoft Visual C/C++ (12.20.9044) [C] | Linker: Microsoft Linker (6.00.8047) | Tool: Visual Studio (6.0)
File size	72.00 KB (73728 bytes)

Which is malicious:



(!) 45 security vendors and 2 sandboxes flagged this file as malicious

2610cd8557d56f679f493a23995a1577379fead9792e44a4884756821e609b66

ab.exe

peexe checks-user-input idle

Size
72.00 KB

Last Analysis Date
3 days ago

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

Popular threat label (!) trojan.cryptz/marte   Threat categories trojan hacktool   Family labels cryptz marte swrort

Security vendors' analysis ⓘ   Do you want to automate checks?

ALYac	(!) Trojan.CryptZ.Marte.1.Gen	Antiy-AVL	(!) Trojan/Win32.Rozena.ed
Arcabit	(!) Trojan.CryptZ.Marte.1.Gen	Avast	(!) Win32:SwPatch [Wrm]
AVG	(!) Win32:SwPatch [Wrm]	Avira (no cloud)	(!) TR/Patched.Gen2
BitDefender	(!) Trojan.CryptZ.Marte.1.Gen	BitDefenderTheta	(!) Gen:NN.ZexaF.36608.eq0@aOFw6Dki
Bkav Pro	(!) W32.AIDetectMalware	ClamAV	(!) Win.Trojan.MSShellcode-7
CrowdStrike Falcon	(!) Win/malicious_confidence_90% (D)	Cylance	(!) Unsafe
Cynet	(!) Malicious (score: 99)	DeepInstinct	(!) MALICIOUS
DrWeb	(!) BackDoor.Meterpreter.259	Elastic	(!) Windows.Trojan.Metasploit
Emsisoft	(!) Trojan.CryptZ.Marte.1.Gen (B)	eScan	(!) Trojan.CryptZ.Marte.1.Gen