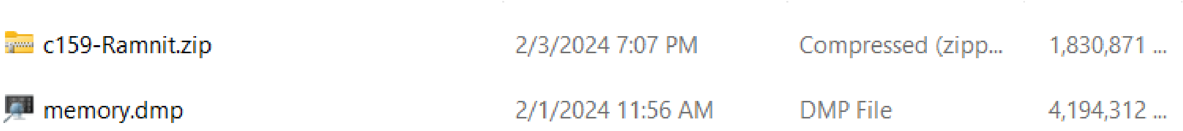
Ramnit Blue Team Lab

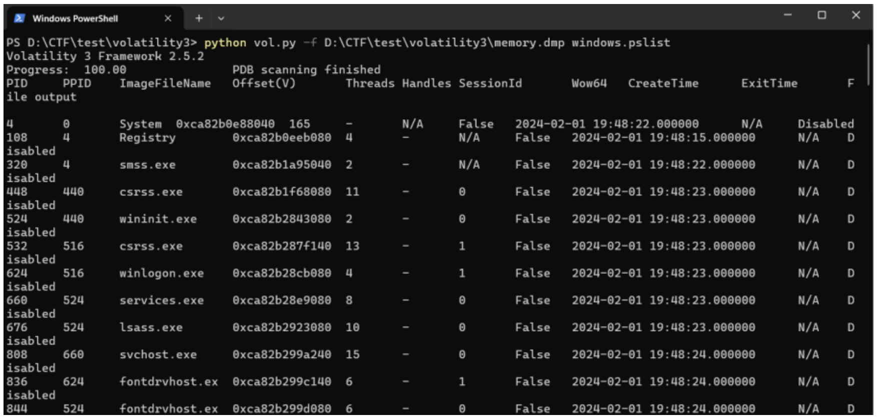
Category: Endpoint Forensics

Volatility Memory



```
c159-Ramnit.zip    2/3/2024 7:07 PM     Compressed (zipp...    1,830,871 ...
memory.dmp         2/1/2024 11:56 AM    DMP File               4,194,312 ...
```

python vol.py -f D:\CTF\test\volatility3\memory.dmp windows.pslist

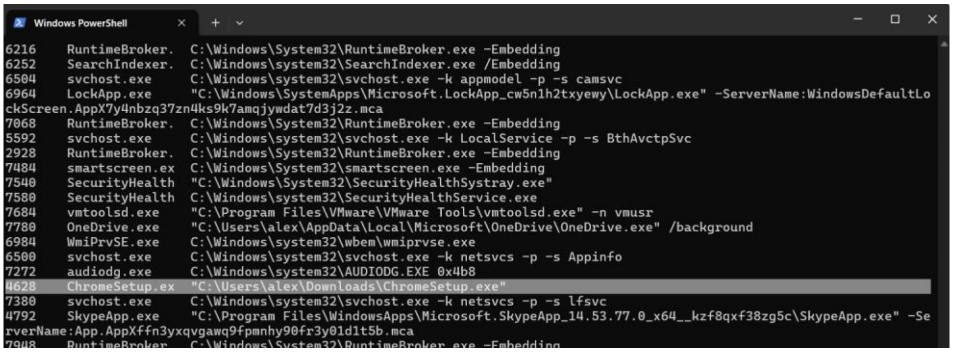


```
PS D:\CTF\test\volatility3> python vol.py -f D:\CTF\test\volatility3\memory.dmp windows.pslist
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        F
ile output

4       0       System  0xca82b0e88040  165     -       N/A     False   2024-02-01 19:48:22.000000      N/A     Disabled
108     4       Registry        0xca82b0eeb080  4       -       N/A     False   2024-02-01 19:48:15.000000      N/A     D
isabled
320     4       smss.exe        0xca82b1a95040  2       -       N/A     False   2024-02-01 19:48:22.000000      N/A     D
isabled
448     440     csrss.exe       0xca82b1f68080  11      -       0       False   2024-02-01 19:48:23.000000      N/A     D
isabled
524     440     wininit.exe     0xca82b2843080  2       -       0       False   2024-02-01 19:48:23.000000      N/A     D
isabled
532     516     csrss.exe       0xca82b287f140  13      -       1       False   2024-02-01 19:48:23.000000      N/A     D
isabled
624     516     winlogon.exe    0xca82b28cb080  4       -       1       False   2024-02-01 19:48:23.000000      N/A     D
isabled
660     524     services.exe    0xca82b28e9080  8       -       0       False   2024-02-01 19:48:23.000000      N/A     D
isabled
676     524     lsass.exe       0xca82b2923080  10      -       0       False   2024-02-01 19:48:23.000000      N/A     D
isabled
808     660     svchost.exe     0xca82b299a240  15      -       0       False   2024-02-01 19:48:24.000000      N/A     D
isabled
836     624     fontdrvhost.ex  0xca82b299c140  6       -       1       False   2024-02-01 19:48:24.000000      N/A     D
isabled
844     524     fontdrvhost.ex  0xca82b299d080  6       -       0       False   2024-02-01 19:48:24.000000      N/A     D
```

I didn`t see anything interesting

So let`s see command line information

python vol.py -f D:\CTF\test\volatility3\memory.dmp windows.cmdline



```
6216    RuntimeBroker.  C:\Windows\System32\RuntimeBroker.exe -Embedding
6252    SearchIndexer.  C:\Windows\system32\SearchIndexer.exe /Embedding
6504    svchost.exe     C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
6964    LockApp.exe     "C:\Windows\SystemApps\Microsoft.LockApp_cw5n1h2txyewy\LockApp.exe" -ServerName:WindowsDefaultLo
ckScreen.AppX7y4nbzq37zn4ks9k7amqjywdat7d3j2z.mca
7068    RuntimeBroker.  C:\Windows\System32\RuntimeBroker.exe -Embedding
5592    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s BthAvctpSvc
2928    RuntimeBroker.  C:\Windows\System32\RuntimeBroker.exe -Embedding
7484    smartscreen.ex  C:\Windows\System32\smartscreen.exe -Embedding
7540    SecurityHealth  "C:\Windows\System32\SecurityHealthSystray.exe"
7580    SecurityHealth  C:\Windows\system32\SecurityHealthService.exe
7684    vmtoolsd.exe    "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
7780    OneDrive.exe    "C:\Users\alex\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
6984    WmiPrvSE.exe    C:\Windows\system32\wbem\wmiprvse.exe
6500    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
7272    audiodg.exe     C:\Windows\system32\AUDIODG.EXE 0x4b8
4628    ChromeSetup.ex  "C:\Users\alex\Downloads\ChromeSetup.exe"
7380    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s lfsvc
4792    SkypeApp.exe    "C:\Program Files\WindowsApps\Microsoft.SkypeApp_14.53.77.0_x64__kzf8qxf38zg5c\SkypeApp.exe" -Se
rverName:App.AppXffn3yxqvgawq9fpmnhy90fr3y01d1t5b.mca
7948    RuntimeBroker.  C:\Windows\System32\RuntimeBroker.exe -Embedding
```

This one is interesting So now we can answer the following questions

Q1:We need to identify the process responsible for this suspicious behavior. What is the name of the suspicious process?

Answer: ChromeSetup.exe

Q2:To eradicate the malware, what is the exact file path of the process executable?

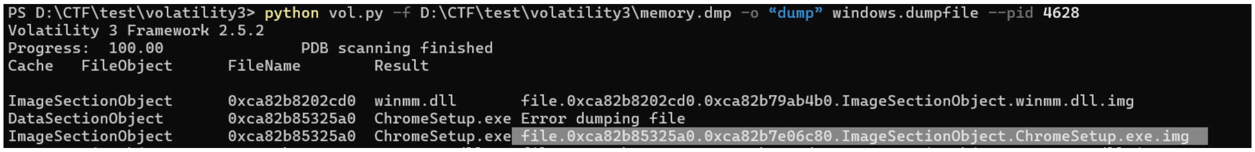
Answer: C:\Users\alex\Downloads\ChromeSetup.exe

Q3 Identifying network connections is crucial for understanding the malware's communication strategy. What is the IP address it attempted to connect to?

python vol.py -f D:\CTF\test\volatility3\memory.dmp windows.netstat

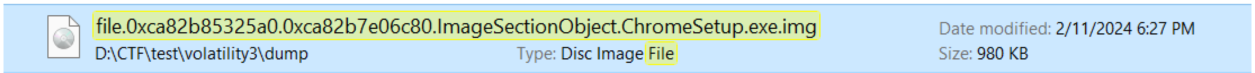
netstat provides statistics about all active connections so you can find out which computers or networks a PC is connected to.

python vol.py -f D:\CTF\test\volatility3\memory.dmp -o “dump” windows.dumpfile --pid 4628



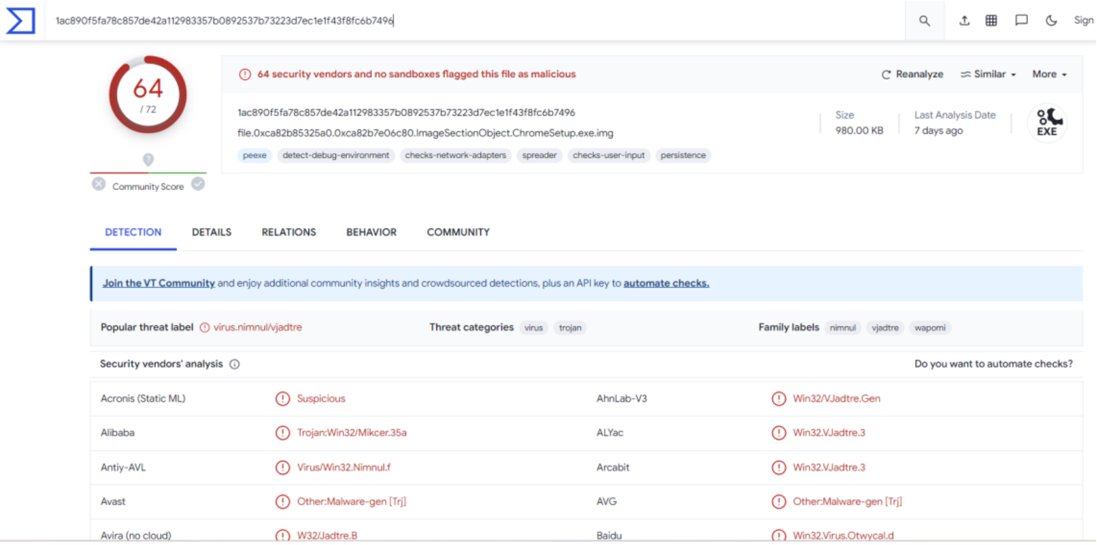
```
PS D:\CTF\test\volatility3> python vol.py -f D:\CTF\test\volatility3\memory.dmp -o “dump” windows.dumpfile --pid 4628
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

ImageSectionObject      0xca82b8202cd0  winmm.dll       file.0xca82b8202cd0.0xca82b79ab4b0.ImageSectionObject.winmm.dll.img
DataSectionObject       0xca82b85325a0  ChromeSetup.exe Error dumping file
ImageSectionObject      0xca82b85325a0  ChromeSetup.exe file.0xca82b85325a0.0xca82b7e06c80.ImageSectionObject.ChromeSetup.exe.img
```

Get the File and Let`s analyze it for virustotal Sandbox



file.0xca82b85325a0.0xca82b7e06c80.ImageSectionObject.ChromeSetup.exe.img
D:\CTF\test\volatility3\dump
Type: Disc Image File
Date modified: 2/11/2024 6:27 PM
Size: 980 KB

Result:



1ac890f5fa78c857de42a112983357b0892537b73223d7ec1e1f43f8fc6b7496

64 / 72

64 security vendors and no sandboxes flagged this file as malicious

1ac890f5fa78c857de42a112983357b0892537b73223d7ec1e1f43f8fc6b7496
file.0xca82b85325a0.0xca82b7e06c80.ImageSectionObject.ChromeSetup.exe.img

peexe detect-debug-environment checks-network-adapters spreader checks-user-input persistence

Size 980.00 KB | Last Analysis Date 7 days ago

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

Popular threat label virus.nimnul/vjadtre | Threat categories virus trojan | Family labels nimnul vjadtre wapomi

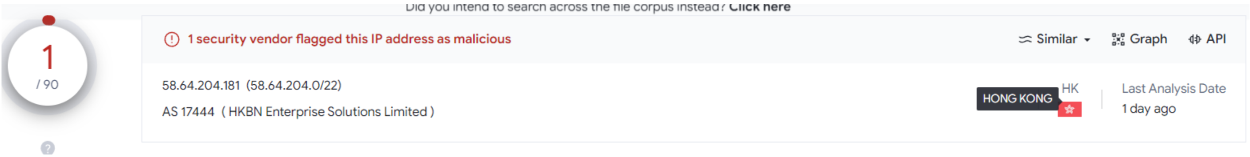
Security vendors' analysis | Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Win32/VJadtre.Gen
Alibaba	Trojan:Win32/Mikcer.35a	ALYac	Win32.VJadtre.3
Antiy-AVL	Virus/Win32.Nimnul.f	Arcabit	Win32.VJadtre.3
Avast	Other:Malware-gen [Trj]	AVG	Other:Malware-gen [Trj]
Avira (no cloud)	W32/Jadtre.B	Baidu	Win32.Virus.Otwycal.d

Let`s Compare The netstat command with Relations in virus total

The matched ip address **Answer:** 58.64.204.181

Q4 To pinpoint the geographical origin of the attack, which city is associated with the IP address the malware communicated with?



Did you intend to search across the file corpus instead? Click here

1 / 90

1 security vendor flagged this IP address as malicious

58.64.204.181 (58.64.204.0/22)

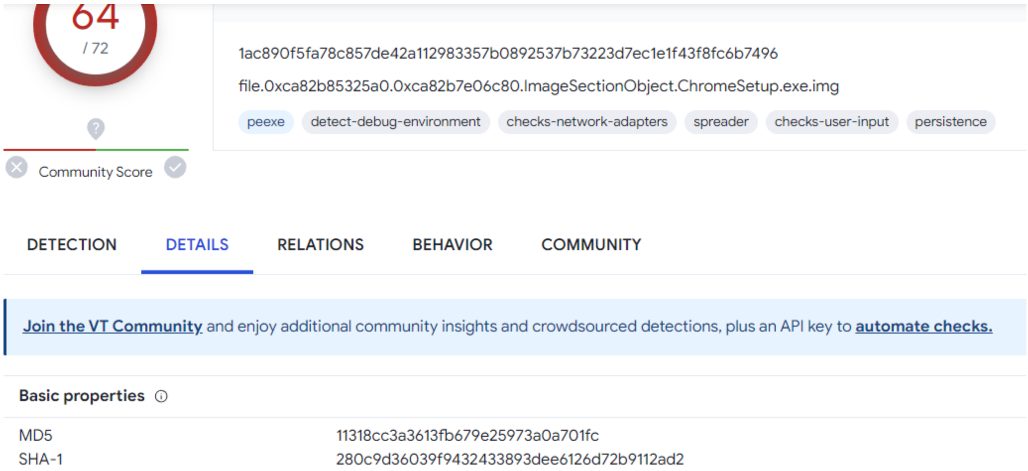
AS 17444 (HKBN Enterprise Solutions Limited)

HONG KONG HK

Last Analysis Date
1 day ago

Answer: HONG KONG

Q5 Hashes provide a unique identifier for files, aiding in detecting similar threats across machines. What is the SHA1 hash of the malware's executable?



64 / 72

1ac890f5fa78c857de42a112983357b0892537b73223d7ec1e1f43f8fc6b7496

file.0xca82b85325a0.0xca82b7e06c80.ImageSectionObject.ChromeSetup.exe.img

peexe detect-debug-environment checks-network-adapters spreader checks-user-input persistence

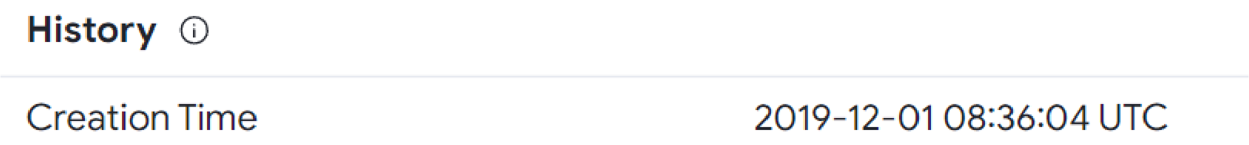
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	11318cc3a3613fb679e25973a0a701fc
SHA-1	280c9d36039f9432433893dee6126d72b9112ad2

Answer: 280c9d36039f9432433893dee6126d72b9112ad2

Q6 Understanding the malware's development timeline can offer insights into its deployment. What is the compilation timestamp of the malware?

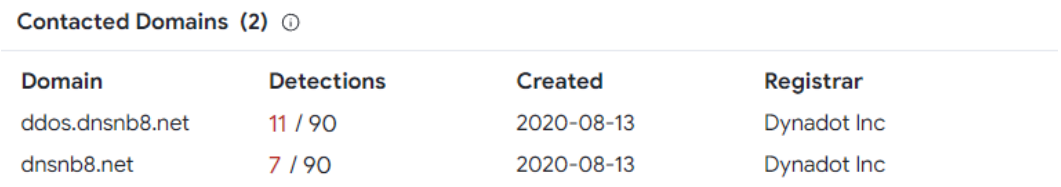


History

Creation Time	2019-12-01 08:36:04 UTC

Q7 Identifying domains involved with this malware helps in blocking future malicious communications and identifying current possible communications with that domain in our network. Can you provide the domain related to the malware?

In virustotal check for Contacted Domains



Contacted Domains (2)

Domain	Detections	Created	Registrar
ddos.dnsnb8.net	11 / 90	2020-08-13	Dynadot Inc
dnsnb8.net	7 / 90	2020-08-13	Dynadot Inc

Answer: dnsnb8.net