Ramnit Challenge

Scenario:

Our intrusion detection system has alerted us to suspicious behavior on a workstation, pointing to a likely malware intrusion. A memory dump of this system has been taken for analysis. Your task is to analyze this dump, trace the malware's actions, and report key findings. This analysis is critical in understanding the breach and preventing further compromise.

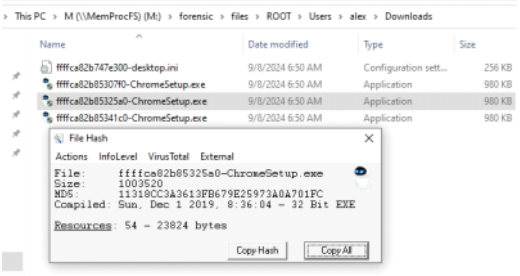
Task 1:
We need to identify the process responsible for this suspicious behavior. What is the name of the suspicious process?

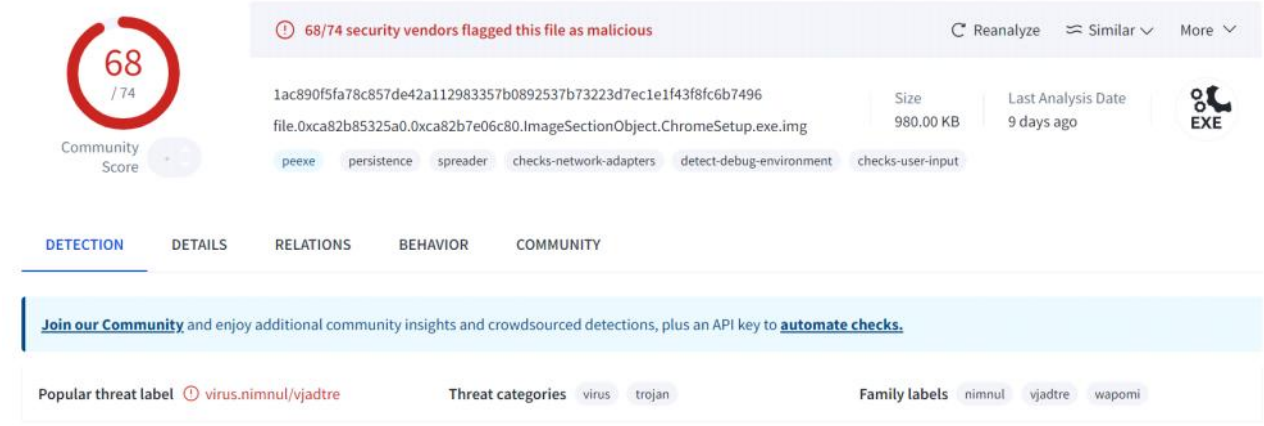
I used the pstree plugin and noticed the "ChromeSetup.exe" so I went to check it out and used the MemProcFS

```
*** 4628        4568    ChromeSetup.ex  0xca82b830a300  4       -       1       True    2024-02-01 19:48:50.000000 UTC  N/A     \Device\HarddiskVolume3\Users\alex\Downloads\ChromeSetup.exe    "C:\Users\alex\Down
loads\ChromeSetup.exe"  C:\Users\alex\Downloads\ChromeSetup.exe
```

```
C:\Users\Bubble\Desktop\MemProcFS_files_and_binaries_v5.9.9-win_x64-20240423>MemProcFS.exe -device C:\Users\Bubble\Desktop\memory.dmp -forensic 1
[SYMBOL]   Functionality may be limited. Extended debug information disabled.
[SYMBOL]   Partial offline fallback symbols in use.
[SYMBOL]   For additional information use startup option: -loglevel symbol:4
[SYMBOL]   Reason: Unable to download kernel symbols to cache from Symbol Server.

Initialized 64-bit Windows 10.0.19041
[FORENSIC] Built-in Yara rules from Elastic are disabled. Enable with: -license-accept-elastic-license-2-0

==============================  MemProcFS  ==============================
 - Author:          Ulf Frisk - pcileech@frizk.net
 - Info:            https://github.com/ufrisk/MemProcFS
 - Discord:         https://discord.gg/pcileech
 - License:         GNU Affero General Public License v3.0
   ------------------------------------------------------------------
   MemProcFS is free open source software. If you find it useful please
   become a sponsor at: https://github.com/sponsors/ufrisk Thank You :)
   ------------------------------------------------------------------
 - Version:         5.9.9 (Windows)
 - Mount Point:     M:\
 - Tag:             19041_7d13663f
 - Operating System: Windows 10.0.19041 (X64)
======================================================================

[FORENSIC] Forensic mode completed in 46s.
```

Then I went to the Downloads folder of the user Alex and took the MD5 hash from the ChromeSetup.exe - 11318CC3A3613FB679E25973A0A701FC and checked it on Virus Total.
The hash was highly reported.





Answer: ChromeSetup.exe

Task 2:
To eradicate the malware, what is the exact file path of the process executable?

Same like task 1, the path is the Downloads folder

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

Task 3:
Identifying network connections is crucial for understanding the malware's communication strategy. What is the IP address it attempted to connect to?

I used the windows.netscan.NetScan plugin and saw the IP with the ChromeSetup.exe

```
0xca82b8bafb30  TCPv4   192.168.19.133  49682   58.64.204.181   5202    CLOSED  4628    ChromeSetup.ex  2024-02-01 19:48:51.000000 UTC
```

Answer: 58.64.204.181

Task 4:
To pinpoint the geographical origin of the attack, which city is associated with the IP address the malware communicated with?

I checked the IP on AbuseIPDB

58.64.204.181 was not found in our database

ISP	NWT IDC Data Service
Usage Type	Data Center/Web Hosting/Transit
Domain Name	newworldtel.com
Country	Hong Kong
City	Hong Kong, Hong Kong

Answer: Hong Kong

Task 5:
Hashes provide a unique identifier for files, aiding in detecting similar threats across machines. What is the SHA1 hash of the malware's executable?

I took it from Virus Total

Basic properties

MD5	11318cc3a3613fb679e25973a0a701fc
SHA-1	280c9d36039f9432433893dee6126d72b9112ad2
SHA-256	1ac890f5fa78c857de42a112983357b0892537b73223d7ec1e1f43f8fc6b7496
Vhash	016056151d155e6070204005200897z60f5z22z982z120a7z
Authentihash	b1602d688dc54ea12ffee69f1805b9e680e50bc71a9d63b749588fcea6fab09f
Imphash	8bdfbe4cf2da0d42d1c4ab2162a7ef85

Answer: 280c9d36039f9432433893dee6126d72b9112ad2

Task 6:
Understanding the malware's development timeline can offer insights into its deployment. What is the compilation UTC timestamp of the malware?

I checked this inside Virus Total

History

Creation Time	2019-12-01 08:36:04 UTC
First Submission	2024-02-03 00:02:57 UTC
Last Submission	2024-09-07 16:07:11 UTC
Last Analysis	2024-08-29 15:46:44 UTC

Answer: 2019-12-01 08:36:04

Task 7:
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?

I checked this inside Virus Total

HTTP Requests

+ GET http://ddos.dnsnb8.net:799/cj//k1.rar
+ GET http://ddos.dnsnb8.net:799/cj/k1.rar
+ GET http://ddos.dnsnb8.net:799/cj/k2.rar
+ GET http://ddos.dnsnb8.net:799/cj/k3.rar
+ GET http://ddos.dnsnb8.net:799/cj/k4.rar

Answer: dnsnb8.net