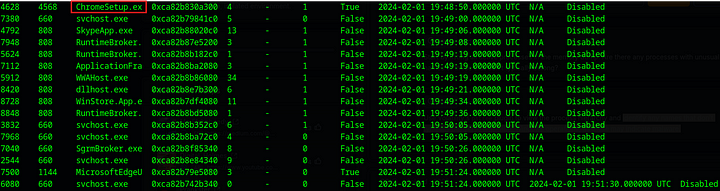
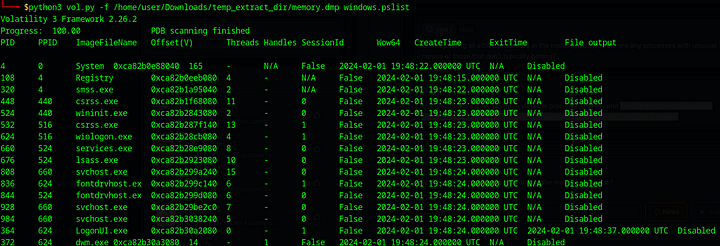
### **Ramnit — CyberDefenders**

**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.

#### **Tasks**

1. **What is the name of the process responsible for the suspicious activity?**

python3 vol.py -f /path/to/memory.dmp windows.pslist



The only process that does not belong to the usual windows processes is ChromeSetup.exe. This could be a target for malware infection.

**Answer:** ChromeSetup.exe

**2. What is the exact path of the executable for the malicious process?**

Let us chek the command line associated with this program.

python3 vol.py -f /path/to/memory.dmp windows.cmdline | grep ChromeSetup.exe



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

**3. Identifying network connections is crucial for understanding the malware’s communication strategy. What IP address did the malware attempt to connect to?**

python3 vol.py -f /path/to/memory.dmp windows.netscan | grep ChromeSetup

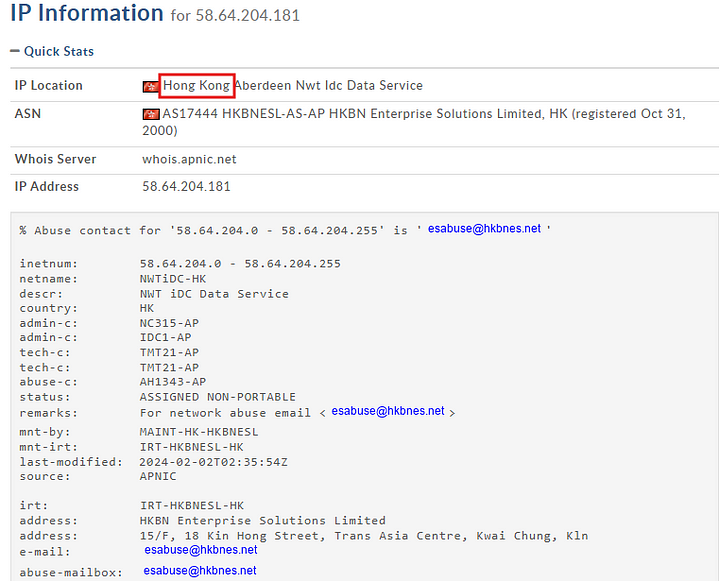
The above command will find any network connections made by the system where the owner or the originator of the connection is ChromeSetup.exe



**Answer:** 58.64.204.181

**4. To determine the specific geographical origin of the attack, Which city is associated with the IP address the malware communicated with?**

We can get more information about the IP address from online tools like<https://whois.domaintools.com/>.

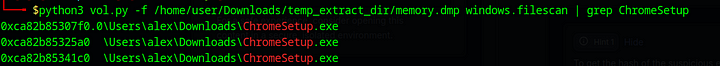


**Answer:** Hong Kong

**5. Hashes serve as unique identifiers for files, assisting in the detection of similar threats across different machines. What is the SHA1 hash of the malware executable?**

python3 vol.py -f /path/to/memory.dmp windows.filescan | grep ChromeSetup

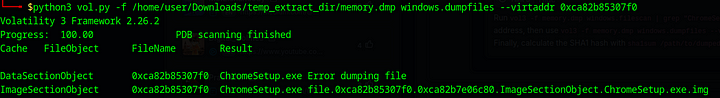
The above command will find the memory address of the required file.



Now copy the memory address and execute the following command

python3 vol.py -f path/to/memory.dmp windows.dumpfiles --virtaddr 0xca82b85307f0

This will dump the files to the local system.



Now calculate the hash of the dumped file.

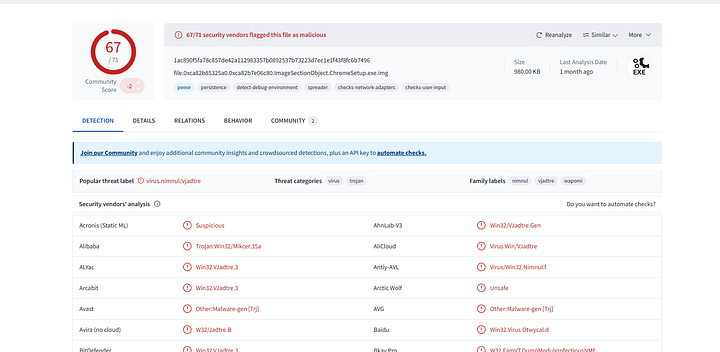
sha1sum <dumped\_file>



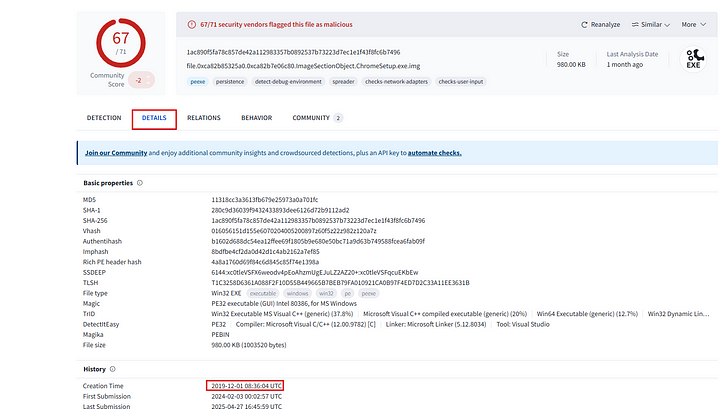
**Answer:** 280c9d36039f9432433893dee6126d72b9112ad2

**6. Examining the malware’s development timeline can provide insights into its deployment. What is the compilation timestamp for the malware?**

To find this we can submit the above calculated hash to VirusTotal.



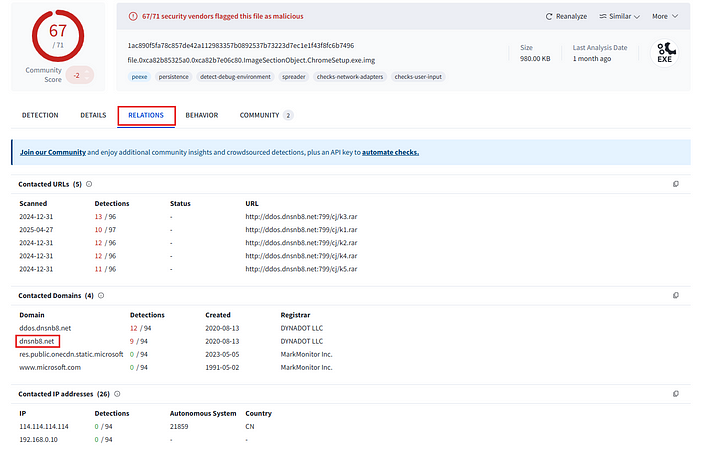
Now, we can go to the Details tab to see the compilation time of this malware.



**Answer:** 2019–12–01 08:36

**7. Identifying the domains associated with this malware is crucial for blocking future malicious communications and detecting any ongoing interactions with those domains within our network. Can you provide the domain connected to the malware?**

In VirusTotal, we can check the Relations tab to see the domains associated with this particular malware.



**Answer:** dnsnb8.net

This is the end of this walkthrough