CyberDefenders: Ramnit Lab

The following writeup is for Ramnit Lab on CyberDefenders, it involves a memory dump using Volatility 3.

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

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

I am going to start off by using the pstree plugin to get the list of processes that were running on the machine and save it to a csv file:

```
python .\vol.py -r csv -f .\memory.dmp windows.pstree > out.csv
```

After exploring the output in timeline explorer, It took a while to identify anything suspicious, however, I eventually determined that ChomeSetup.exe appears suspicious:

3	4628	4568	ChromeSetup.ex	0xca82b830a300	4	-	1

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

In the output of the command used previously, we can find the path:

```
\\Device\\HarddiskVolume3\\Users\\alex\\Downloads\\ChromeSetup.exe
```

This is simply C:\Users\alex\Downloads\ChromeSetup.exe. Alternatively, you can enter the following command and find the file path:

```
python .\vol.py -f .\memory.dmp windows.cmdline
```

```
4628    ChromeSetup.ex  "C:\Users\alex\Downloads\ChromeSetup.exe"
```

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

To identify network connections present at the time of extraction on the host machine, we can use the netscan plugin (you can also use the netstat plugin):

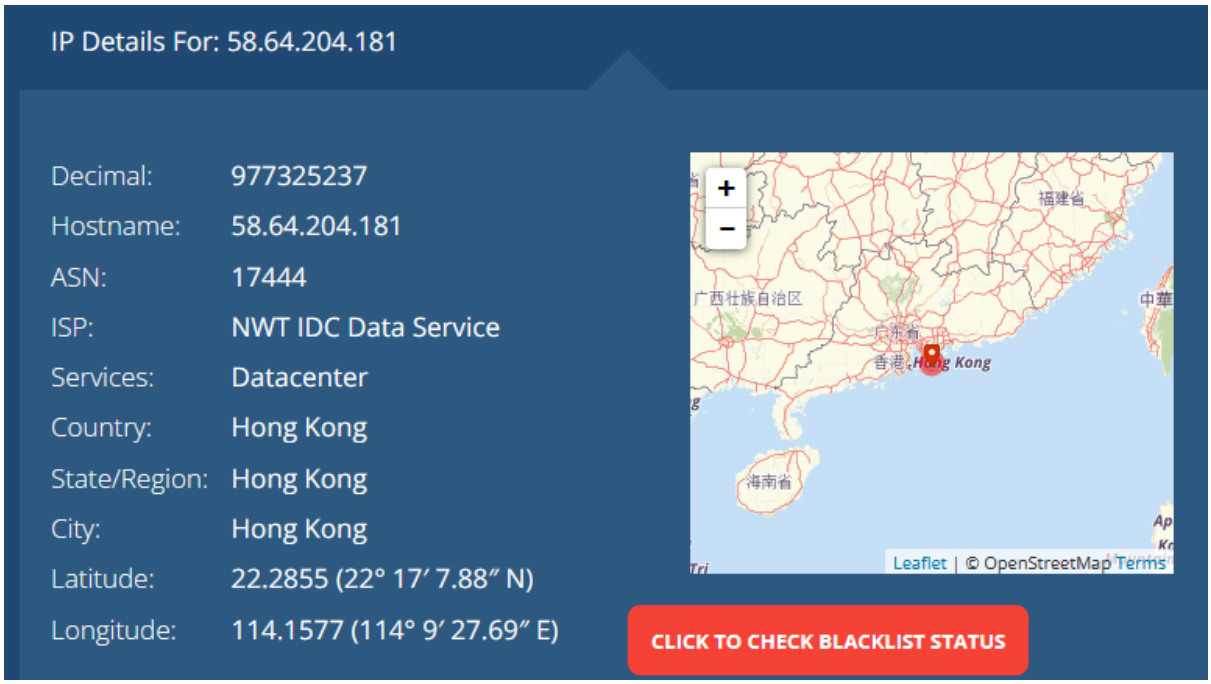
```
python .\vol.py -f .\memory.dmp windows.netscan
```

If you look through the output, we can see that ChromeSetup.exe initiated a connected to 58.64.204.181.

```
TCPv4   192.168.19.133  49682   58.64.204.181   5202    SYN_SENT        4628    ChromeSetup.ex
```

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

Unfortunately, Volatility is not capable of doing an GeoIP lookups, therefore we can use an IP lookup tool such as whattismyipaddress to determine the city associated with 58.64.204.181:



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

To get the SHA1 hash of the malware, we can enter the following command:

```
python .\vol.py -f .\memory.dmp windows.dumpfiles --pid 4628
```

This dumps the ChromeSetup.exe process (aka PID 4628 which we identified in the first question).

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

We can then use the Get-FileHash cmdlet to generate the SHA1 hash of the malware:

```
Get-FileHash -Algorithm SHA1 file.0xca82b85325a0.0xca82b7e06c80.ImageSectionObject.ChromeSetup.exe.img
```

```
Algorithm       Hash
---------       ----
SHA1            280C9D36039F9432433893DEE6126D72B9112AD2
```

280C9D36039F9432433893DEE6126D72B9112AD2

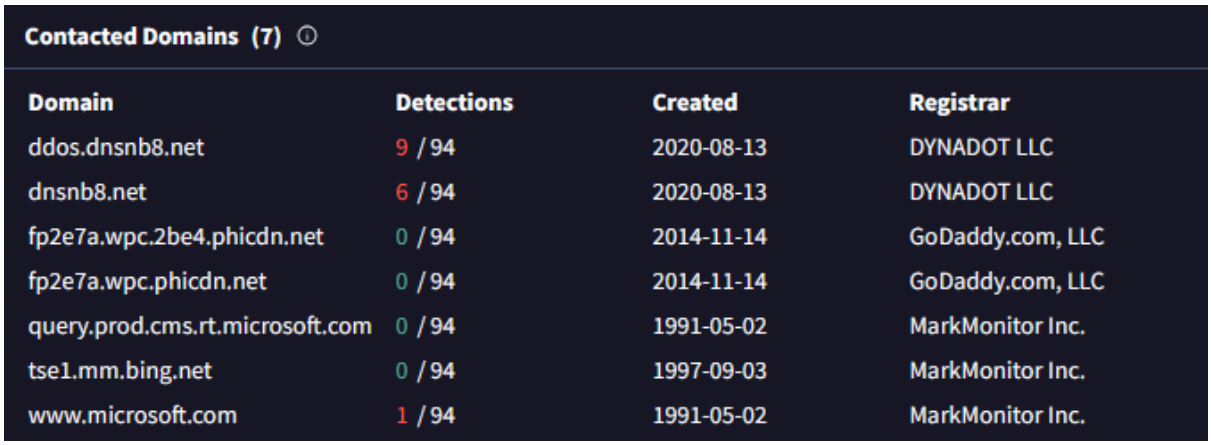
Understanding the malware's development timeline can offer insights into its deployment. What is the compilation UTC timestamp of the malware?

We can find the compilation timestamp by searching for the SHA1 hash in VirusTotal and looking at the header section in the details tab:

Header	
Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2019-12-01 08:36:04 UTC
Entry Point	1138688
Contained Sections	5

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?

If you navigate to the relations tab, we can see the domain related to the malware:



Contacted Domains (7)

Domain	Detections	Created	Registrar
ddos.dnsnb8.net	9 / 94	2020-08-13	DYNADOT LLC
dnsnb8.net	6 / 94	2020-08-13	DYNADOT LLC
fp2e7a.wpc.2be4.phicdn.net	0 / 94	2014-11-14	GoDaddy.com, LLC
fp2e7a.wpc.phicdn.net	0 / 94	2014-11-14	GoDaddy.com, LLC
query.prod.cms.rt.microsoft.com	0 / 94	1991-05-02	MarkMonitor Inc.
tse1.mm.bing.net	0 / 94	1997-09-03	MarkMonitor Inc.
www.microsoft.com	1 / 94	1991-05-02	MarkMonitor Inc.

(the malicious domain is dnsnb8[.]net, make sure to remove the square brackets).

This was a really fun lab; it has been a while since I've used Volatility 3 so it serves as a great refresher. If you are interested in digital forensics I highly recommend this lab.