Lab 3 Solutions

Lab 3 - The case of Backdoor.Nitol

During your investigation of a suspect system, you come across a malicious file (***bllb.exe***). Analyze this file and answer the following questions:

1. What is the name of the file dropped by the malware?
2. Which C2 domains are contacted by the malware?
3. What do you see in the network traffic?
4. How is the malware persisting on the system?

Answers

01. What is the name of the file dropped by the malware?

The malware (Backdoor.Nitol) first drops a file in the %AppData% directory. It then creates a shortcut (.lnk) that points to the dropped file

```
[CreateFile] bllb.exe:3364 > %AppData%\Abcdef Hijklmno Qrs\Abcdef Hijklmno Qrs.exe
[CreateFile] bllb.exe:3364 > %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\Abcdef
 Hijklmno Qrs.exe.lnk
```

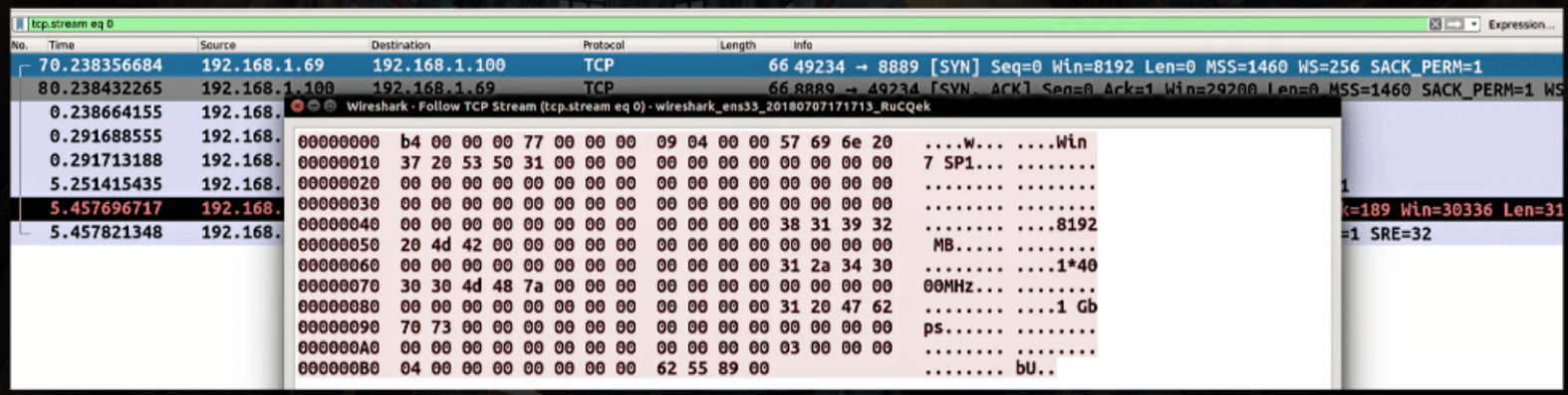
02. Which C2 domains are contacted by the malware?

Upon execution, malware communicates with two C2 domains as shown in the screenshot.

30.027085720	192.168.1.69	192.168.1.100	DNS	74	Standard query 0x90aa A gy9.gyddos.com
40.027486832	192.168.1.69	192.168.1.100	DNS	70	Standard query 0x1c0f A sgv9.ze.am
50.034256261	192.168.1.100	192.168.1.69	DNS	90	Standard query response 0x90aa A gy9.gyddos.com A 192.168.1.100
60.047624767	192.168.1.100	192.168.1.69	DNS	86	Standard query response 0x1c0f A sgv9.ze.am A 192.168.1.100
70.238356684	192.168.1.69	192.168.1.100	TCP	66	49234 → 8889 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
80.238432265	192.168.1.100	192.168.1.69	TCP	66	8889 → 49234 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 W
90.238462985	192.168.1.69	192.168.1.100	TCP	66	49235 → 1004 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
0.238472404	192.168.1.100	192.168.1.69	TCP	66	1004 → 49235 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 W
0.238664155	192.168.1.69	192.168.1.100	TCP	60	49234 → 8889 [ACK] Seq=1 Ack=1 Win=65536 Len=0
0.238710251	192.168.1.69	192.168.1.100	TCP	60	49235 → 1004 [ACK] Seq=1 Ack=1 Win=65536 Len=0
0.291607858	192.168.1.69	192.168.1.100	TCP	242	49235 → 1004 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=188
0.291645972	192.168.1.100	192.168.1.69	TCP	54	1004 → 49235 [ACK] Seq=1 Ack=189 Win=30336 Len=0
0.291688555	192.168.1.69	192.168.1.100	TCP	242	49234 → 8889 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=188

03. What do you see in the network traffic?

In the network traffic, you can see that the malware sends the system information (OS information, size of the RAM, CPU speed, etc) to the attacker.



04. How is the malware persisting on the system?

The malware (Backdoor.Nitol) first drops a file in the ***%AppData%*** directory. It then creates a shortcut (***.lnk***) that points to the dropped file and then adds that shortcut to the Startup folder. This way, when the system starts, the dropped file gets executed via the shortcut (.lnk) file.

```
[CreateFile] bllb.exe:3364 > %AppData%\Abcdef Hijklmno Qrs\Abcdef Hijklmno Qrs.exe
[CreateFile] bllb.exe:3364 > %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\Abcdef
 Hijklmno Qrs.exe.lnk
```