



# Lab 3 Solutions

## Lab 3 - The case of Backdoor.Nitol

During your investigation of a suspect system, you come across a malicious file (**blb.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
```

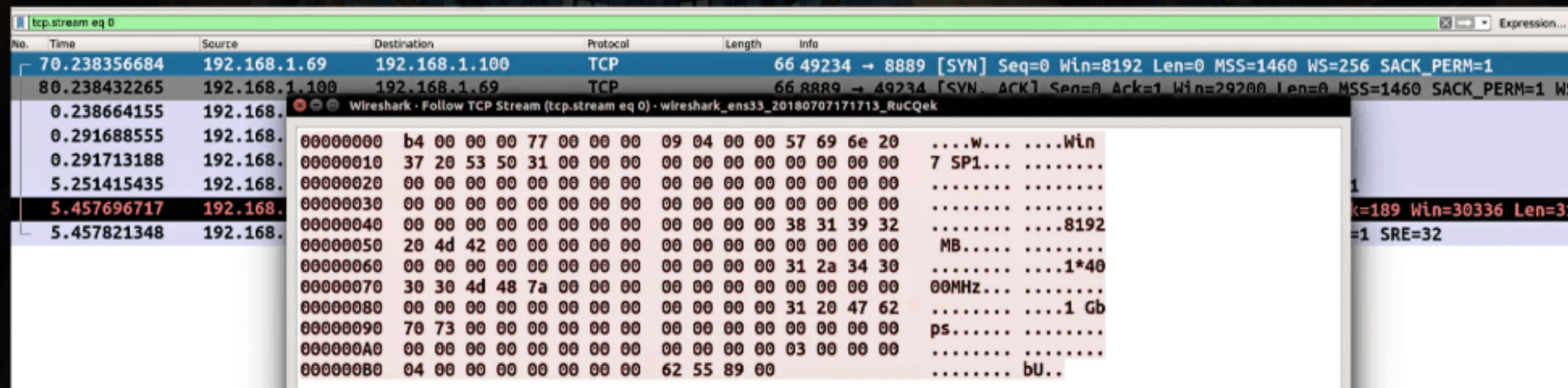
## 02. Which C2 domains are contacted by the malware?

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.



The image shows a Wireshark network traffic capture window. The main pane displays a list of packets, and the packet details pane shows the contents of a selected packet (No. 80). The packet details pane is expanded to show the 'Raw' data, which is a hexadecimal dump of the payload. The payload contains system information, including the operating system (Windows), the system architecture (x64), and the system name (RUCQEK).

No.	Time	Source	Destination	Protocol	Length	Info
70	2.38356684	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	2.38432265	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 WS=256
0	2.38664155	192.168.1.100	192.168.1.69	TCP	66	8889 → 49234 [ACK] Seq=1 Win=0 Len=0
0	2.91688555	192.168.1.100	192.168.1.69	TCP	66	8889 → 49234 [ACK] Seq=1 Win=0 Len=0
0	2.91713188	192.168.1.100	192.168.1.69	TCP	66	8889 → 49234 [ACK] Seq=1 Win=0 Len=0
5	2.51415435	192.168.1.100	192.168.1.69	TCP	66	8889 → 49234 [ACK] Seq=1 Win=0 Len=0
5	4.57696717	192.168.1.100	192.168.1.69	TCP	66	8889 → 49234 [ACK] Seq=1 Win=0 Len=0
5	4.57821348	192.168.1.100	192.168.1.69	TCP	66	8889 → 49234 [ACK] Seq=1 Win=0 Len=0

Offset	Hex	ASCII
0	b4 00 00 00 77 00 00 00	....W... ..Win
4	09 04 00 00 57 69 6e 20	7 SP1... ..
8	00 00 00 00 00 00 00 00	.....
12	00 00 00 00 00 00 00 00	.....
16	00 00 00 00 00 00 00 00	.....
20	00 00 00 00 00 00 00 00	.....
24	00 00 00 00 00 00 00 00	.....
28	00 00 00 00 00 00 00 00	.....
32	00 00 00 00 00 00 00 00	.....
36	00 00 00 00 00 00 00 00	.....
40	00 00 00 00 00 00 00 00	.....
44	00 00 00 00 00 00 00 00	.....
48	00 00 00 00 00 00 00 00	.....
52	00 00 00 00 00 00 00 00	.....
56	00 00 00 00 00 00 00 00	.....
60	00 00 00 00 00 00 00 00	.....
64	00 00 00 00 00 00 00 00	.....
68	00 00 00 00 00 00 00 00	.....
72	00 00 00 00 00 00 00 00	.....
76	00 00 00 00 00 00 00 00	.....
80	00 00 00 00 00 00 00 00	.....
84	00 00 00 00 00 00 00 00	.....
88	00 00 00 00 00 00 00 00	.....
92	00 00 00 00 00 00 00 00	.....
96	00 00 00 00 00 00 00 00	.....
100	00 00 00 00 00 00 00 00	.....
104	00 00 00 00 00 00 00 00	.....
108	00 00 00 00 00 00 00 00	.....
112	00 00 00 00 00 00 00 00	.....
116	00 00 00 00 00 00 00 00	.....
120	00 00 00 00 00 00 00 00	.....
124	00 00 00 00 00 00 00 00	.....
128	00 00 00 00 00 00 00 00	.....
132	00 00 00 00 00 00 00 00	.....
136	00 00 00 00 00 00 00 00	.....
140	00 00 00 00 00 00 00 00	.....
144	00 00 00 00 00 00 00 00	.....
148	00 00 00 00 00 00 00 00	.....
152	00 00 00 00 00 00 00 00	.....
156	00 00 00 00 00 00 00 00	.....
160	00 00 00 00 00 00 00 00	.....
164	00 00 00 00 00 00 00 00	.....
168	00 00 00 00 00 00 00 00	.....
172	00 00 00 00 00 00 00 00	.....
176	00 00 00 00 00 00 00 00	.....
180	00 00 00 00 00 00 00 00	.....
184	00 00 00 00 00 00 00 00	.....
188	00 00 00 00 00 00 00 00	.....
192	00 00 00 00 00 00 00 00	.....
196	00 00 00 00 00 00 00 00	.....
200	00 00 00 00 00 00 00 00	.....
204	00 00 00 00 00 00 00 00	.....
208	00 00 00 00 00 00 00 00	.....
212	00 00 00 00 00 00 00 00	.....
216	00 00 00 00 00 00 00 00	.....
220	00 00 00 00 00 00 00 00	.....
224	00 00 00 00 00 00 00 00	.....
228	00 00 00 00 00 00 00 00	.....
232	00 00 00 00 00 00 00 00	.....
236	00 00 00 00 00 00 00 00	.....
240	00 00 00 00 00 00 00 00	.....
244	00 00 00 00 00 00 00 00	.....
248	00 00 00 00 00 00 00 00	.....
252	00 00 00 00 00 00 00 00	.....
256	00 00 00 00 00 00 00 00	.....
260	00 00 00 00 00 00 00 00	.....
264	00 00 00 00 00 00 00 00	.....
268	00 00 00 00 00 00 00 00	.....
272	00 00 00 00 00 00 00 00	.....
276	00 00 00 00 00 00 00 00	.....
280	00 00 00 00 00 00 00 00	.....
284	00 00 00 00 00 00 00 00	.....
288	00 00 00 00 00 00 00 00	.....
292	00 00 00 00 00 00 00 00	.....
296	00 00 00 00 00 00 00 00	.....
300	00 00 00 00 00 00 00 00	.....
304	00 00 00 00 00 00 00 00	.....
308	00 00 00 00 00 00 00 00	.....
312	00 00 00 00 00 00 00 00	.....
316	00 00 00 00 00 00 00 00	.....
320	00 00 00 00 00 00 00 00	.....
324	00 00 00 00 00 00 00 00	.....
328	00 00 00 00 00 00 00 00	.....
332	00 00 00 00 00 00 00 00	.....
336	00 00 00 00 00 00 00 00	.....
340	00 00 00 00 00 00 00 00	.....
344	00 00 00 00 00 00 00 00	.....
348	00 00 00 00 00 00 00 00	.....
352	00 00 00 00 00 00 00 00	.....
356	00 00 00 00 00 00 00 00	.....
360	00 00 00 00 00 00 00 00	.....
364	00 00 00 00 00 00 00 00	.....
368	00 00 00 00 00 00 00 00	.....
372	00 00 00 00 00 00 00 00	.....
376	00 00 00 00 00 00 00 00	.....
380	00 00 00 00 00 00 00 00	.....
384	00 00 00 00 00 00 00 00	.....
388	00 00 00 00 00 00 00 00	.....
392	00 00 00 00 00 00 00 00	.....
396	00 00 00 00 00 00 00 00	.....
400	00 00 00 00 00 00 00 00	.....
404	00 00 00 00 00 00 00 00	.....
408	00 00 00 00 00 00 00 00	.....
412	00 00 00 00 00 00 00 00	.....
416	00 00 00 00 00 00 00 00	.....
420	00 00 00 00 00 00 00 00	.....
424	00 00 00 00 00 00 00 00	.....
428	00 00 00 00 00 00 00 00	.....
432	00 00 00 00 00 00 00 00	.....
436	00 00 00 00 00 00 00 00	.....
440	00 00 00 00 00 00 00 00	.....
444	00 00 00 00 00 00 00 00	.....
448	00 00 00 00 00 00 00 00	.....
452	00 00 00 00 00 00 00 00	.....
456	00 00 00 00 00 00 00 00	.....
460	00 00 00 00 00 00 00 00	.....
464	00 00 00 00 00 00 00 00	.....
468	00 00 00 00 00 00 00 00	.....
472	00 00 00 00 00 00 00 00	.....
476	00 00 00 00 00 00 00 00	.....
480	00 00 00 00 00 00 00 00	.....
484	00 00 00 00 00 00 00 00	.....
488	00 00 00 00 00 00 00 00	.....
492	00 00 00 00 00 00 00 00	.....
496	00 00 00 00 00 00 00 00	.....
500	00 00 00 00 00 00 00 00	.....
504	00 00 00 00 00 00 00 00	.....
508	00 00 00 00 00 00 00 00	.....
512	00 00 00 00 00 00 00 00	.....
516	00 00 00 00 00 00 00 00	.....
520	00 00 00 00 00 00 00 00	.....
524	00 00 00 00 00 00 00 00	.....
528	00 00 00 00 00 00 00 00	.....
532	00 00 00 00 00 00 00 00	.....
536	00 00 00 00 00 00 00 00	.....
540	00 00 00 00 00 00 00 00	.....
544	00 00 00 00 00 00 00 00	.....
548	00 00 00 00 00 00 00 00	.....
552	00 00 00 00 00 00 00 00	.....
556	00 00 00 00 00 00 00 00	.....
560	00 00 00 00 00 00 00 00	.....
564	00 00 00 00 00 00 00 00	.....
568	00 00 00 00 00 00 00 00	.....
572	00 00 00 00 00 00 00 00	.....
576	00 00 00 00 00 00 00 00	.....
580	00 00 00 00 00 00 00 00	.....
584	00 00 00 00 00 00 00 00	.....
588	00 00 00 00 00 00 00 00	.....
592	00 00 00 00 00 00 00 00	.....
596	00 00 00 00 00 00 00 00	.....
600	00 00 00 00 00 00 00 00	.....
604	00 00 00 00 00 00 00 00	.....
608	00 00 00 00 00 00 00 00	.....
612	00 00 00 00 00 00 00 00	.....
616	00 00 00 00 00 00 00 00	.....
620	00 00 00 00 00 00 00 00	.....
624	00 00 00 00 00 00 00 00	.....
628	00 00 00 00 00 00 00 00	.....
632	00 00 00 00 00 00 00 00	.....
636	00 00 00 00 00 00 00 00	.....
640	00 00 00 00 00 00 00 00	.....
644	00 00 00 00 00 00 00 00	.....
648	00 00 00 00 00 00 00 00	.....
652	00 00 00 00 00 00 00 00	.....
656	00 00 00 00 00 00 00 00	.....
660	00 00 00 00 00 00 00 00	.....
664	00 00 00 00 00 00 00 00	.....
668	00 00 00 00 00 00 00 00	.....
672	00 00 00 00 00 00 00 00	.....
676	00 00 00 00 00 00 00 00	.....
680	00 00 00 00 00 00 00 00	.....
684	00 00 00 00 00 00 00 00	.....
688	00 00 00 00 00 00 00 00	.....
692	00 00 00 00 00 00 00 00	.....
696	00 00 00 00 00 00 00 00	.....
700	00 00 00 00 00 00 00 00	.....
704	00 00 00 00 00 00 00 00	.....
708	00 00 00 00 00 00 00 00	.....
712	00 00 00 00 00 00 00 00	.....
716	00 00 00 00 00 00 00 00	.....
720	00 00 00 00 00 00 00 00	.....
724	00 00 00 00 00 00 00 00	.....
728	00 00 00 00 00 00 00 00	.....
732	00 00 00 00 00 00 00 00	.....
736	00 00 00 00 00 00 00 00	.....
740	00 00 00 00 00 00 00 00	.....
744	00 00 00 00 00 00 00 00	.....
748	00 00 00 00 00 00 00 00	.....
752	00 00 00 00 00 00 00 00	.....
756	00 00 00 00 00 00 00 00	.....
760	00 00 00 00 00 00 00 00	.....
764	00 00 00 00 00 00 00 00	.....
768	00 00 00 00 00 00 00 00	.....
772	00 00 00 00 00 00 00 00	.....
776	00 00 00 00 00 00 00 00	.....
780	00 00 00 00 00 00 00 00	.....
784	00 00 00 00 00 00 00 00	.....
788	00 00 00 00 00 00 00 00	.....
792	00 00 00 00 00 00 00 00	.....
796	00 00 00 00 00 00 00 00	.....
800	00 00 00 00 00 00 00 00	.....
804	00 00 00 00 00 00 00 00	.....
808	00 00 00 00 00 00 00 00	.....
812	00 00 00 00 00 00 00 00	.....
816	00 00 00 00 00 00 00 00	.....
820	00 00 00 00 00 00 00 00	.....
824	00 00 00 00 00 00 00 00	.....
828	00 00 00 00 00 00 00 00	.....
832	00 00 00 00 00 00 00 00	.....
836	00 00 00 00 00 00 00 00	.....
840	00 00 00 00 00 00 00 00	.....
844	00 00 00 00 00 00 00 00	.....
848	00 00 00 00 00 00 00 00	.....
852	00 00 00 00 00 00 00 00	.....
856	00 00 00 00 00 00 00 00	.....
860	00 00 00 00 00 00 00 00	.....
864	00 00 00 00 00 00 00 00	.....
868	00 00 00 00 00 00 00 00	.....
872	00 00 00 00 00 00 00 00	.....
876	00 00 00 00 00 00 00 00	.....
880	00 00 00 00 00 00 00 00	.....
884	00 00 00 00 00 00 00 00	.....
888	00 00 00 00 00 00 00 00	.....
892	00 00 00 00 00 00 00 00	.....
896	00 00 00 00 00 00 00 00	.....
900	00 00 00 00 00 00 00 00	.....
904	00 00 00 00 00 00 00 00	.....
908	00 00 00 00 00 00 00 00	.....
912	00 00 00 00 00 00 00 00	.....
916	00 00 00 00 00 00 00 00	.....
920	00 00 00 00 00 00 00 00	.....
924	00 00 00 00 00 00 00 00	.....
928	00 00 00 00 00 00 00 00	.....
932	00 00 00 00 00 00 00 00	.....
936	00 00 00 00 00 00 00 00	.....
940	00 00 00 00 00 00 00 00	.....
944	00 00 00 00 00 00 00 00	.....
948	00 00 00 00 00 00 00 00	.....
952	00 00 00 00 00 00 00 00	.....
956	00 00 00 00 00 00 00 00	.....
960	00 00 00 00 00 00 00 00	.....
964	00 00 00 00 00 00 00 00	.....
968	00 00 00 00 00 00 00 00	.....

#### 04. How is the malware persisting on the system?

The malware (Backdoor.Nitot) 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
```