



Antivirus Software Analysis Questions

By: Ryan Stewart

Analyzing the provided **Windows Defender** logs:

1. What is the name of the file associated with the "Backdoor" type malware in the log?

```
C:\Users\LetsDefend\AppData\Local\Temp\1\Temp1_win-defender.log.zip\win-defender.log - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
win-defender.log x
=====
1
2 Filename       : executable.8180.exe
3 Detect Time    : 30.09.2022 16:19:00
4 Threat Name    : Trojan:Win32/Swrort.A
5 Severity       : Severe (5)
6 Category       : Trojan (8)
7 Detection User : DESKTOP-9A7S2G1\letsdefend
8 Action         : Not Applicable (9)
9 Origin         : Local machine (1)
10 Process Name  : C:\Program Files\Everything\Everything.exe
11 URL           :
12 Detect Path   : https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Swrort.A&threatid=2147630763
13 Threat ID     : 2147630763
14 Detection ID  : {053B7695-9705-4161-873B-9238EFC8DFC7}
15 Computer Name : DESKTOP-9A7S2G1
16 Event Log Time : 30.09.2022 16:19:00
17
18
19
20 Filename       : program1
21 Detect Time    : 9.09.2022 19:48:56
22 Threat Name    : Backdoor:Linux/GetShell.A!xp
23 Severity       : Severe (5)
24 Category       : Backdoor (6)
25 Detection User : DESKTOP-9A7S2G1\letsdefend
26 Action         : Not Applicable (9)
27 Origin         : Local machine (1)
28 Process Name  : C:\Windows\explorer.exe
29 URL           : https://go.microsoft.com/fwlink/?linkid=37020&name=Backdoor:Linux/GetShell.A!xp&threatid=2147797444
30 Detect Path   : file: C:\Users\letsdefend\Desktop\malware\program1
31 Threat ID     : 2147797444
```

2. In the Windows Defender log, what is the identified type of malware for the file named "executable.8180.exe"?

```
C:\Users\LetsDefend\AppData\Local\Temp\1\Temp1_win-defender.log.zip\win-defender.log - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

win-defender.log x

1 =====
2 Filename      : executable.8180.exe
3 Detect Time   : 30.09.2022 16:19:00
4 Threat Name   : Trojan:Win32/Swrort.A
5 Severity      : Severe (5)
6 Category      : Trojan (8)
7 Detection User : DESKTOP-9A7S2G1\letsdefend
8 Action        : Not Applicable (9)
9 Origin        : Local machine (1)
10 Process Name : C:\Program Files\Everything\Everything.exe
11 URL          :
12 Detect Path   : https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Swrort.A&threatid=214
13 Threat ID     : 2147630763
14 Detection ID  : {053B7695-9705-4161-873B-9238EFC8DFC7}
15 Computer Name : DESKTOP-9A7S2G1
16 Event Log Time : 30.09.2022 16:19:00
17 =====
18
19 =====
20 Filename      : program1
21 Detect Time    : 9.09.2022 19:48:56
22 Threat Name    : Backdoor:Linux/GetShell.A!xp
23 Severity       : Severe (5)
24 Category       : Backdoor (6)
25 Detection User : DESKTOP-9A7S2G1\letsdefend
26 Action        : Not Applicable (9)
27 Origin        : Local machine (1)
28 Process Name   : C:\Windows\explorer.exe
29 URL           :
30 Detect Path    : https://go.microsoft.com/fwlink/?linkid=37020&name=Backdoor:Linux/GetShell.A!xp&threatid=214
31 Threat ID      : 2147797444
```