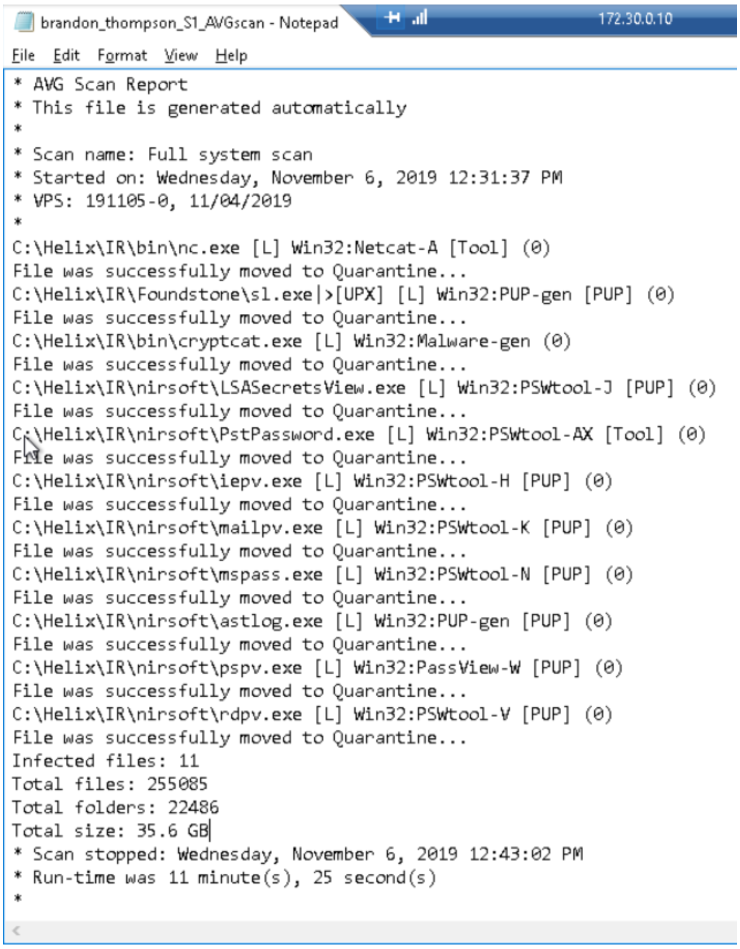
CEN4088.01 Lab 6: Due 11/06/19

Brandon Thompson 5517

November 6, 2019

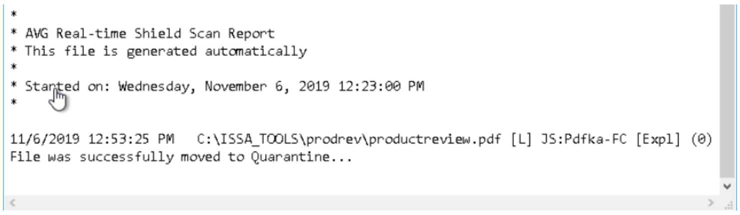
First high severity threat is the Win23:Malware-gen in `C:\Helix\IR\bin\cryptcat.exe`


brandon_thompson_S1_AVGscan - Notepad
172.30.0.10
File Edit Format View Help

```
* AVG Scan Report
* This file is generated automatically
*
* Scan name: Full system scan
* Started on: Wednesday, November 6, 2019 12:31:37 PM
* VPS: 191105-0, 11/04/2019
*
C:\Helix\IR\bin\nc.exe [L] Win32:Netcat-A [Tool] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\Foundstone\sl.exe|>[UPX] [L] Win32:PUP-gen [PUP] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\bin\cryptcat.exe [L] Win32:Malware-gen (0)
File was successfully moved to Quarantine...
C:\Helix\IR\nirsoft\LSASecretsView.exe [L] Win32:PSWtool-J [PUP] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\nirsoft\PstPassword.exe [L] Win32:PSWtool-AX [Tool] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\nirsoft\iepv.exe [L] Win32:PSWtool-H [PUP] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\nirsoft\mailpv.exe [L] Win32:PSWtool-K [PUP] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\nirsoft\mspass.exe [L] Win32:PSWtool-N [PUP] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\nirsoft\astlog.exe [L] Win32:PUP-gen [PUP] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\nirsoft\pspv.exe [L] Win32:PassView-W [PUP] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\nirsoft\rdpv.exe [L] Win32:PSWtool-V [PUP] (0)
File was successfully moved to Quarantine...
Infected files: 11
Total files: 255085
Total folders: 22486
Total size: 35.6 GB
* Scan stopped: Wednesday, November 6, 2019 12:43:02 PM
* Run-time was 11 minute(s), 25 second(s)
*
```

Figure 1: Results of AVG deep scan for section 1.

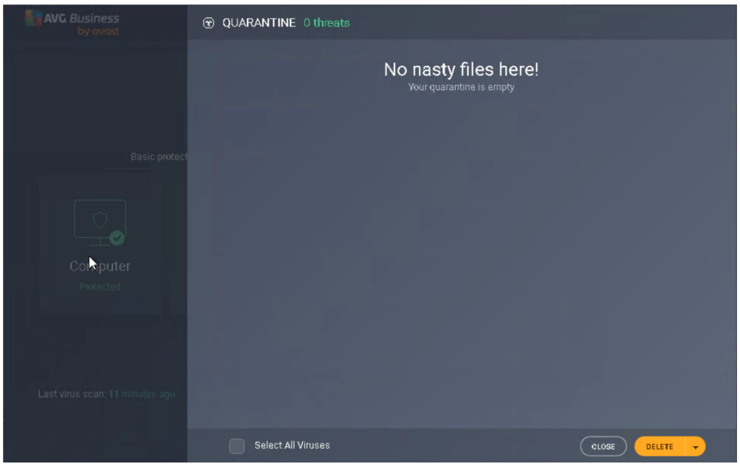
Last high severity threat is the Win32:BO-g [Trj] in `C:\Users\Administrator\AppData\Local\1\BO\BOGUI.EXE`



```
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
* Started on: Wednesday, November 6, 2019 12:23:00 PM
*

11/6/2019 12:53:25 PM   C:\ISSA_TOOLS\prodrev\productreview.pdf [L] JS:Pdfka-FC [Expl] (0)
File was successfully moved to Quarantine...
```

Figure 2: Pdfka-FC threat detection for section 1.

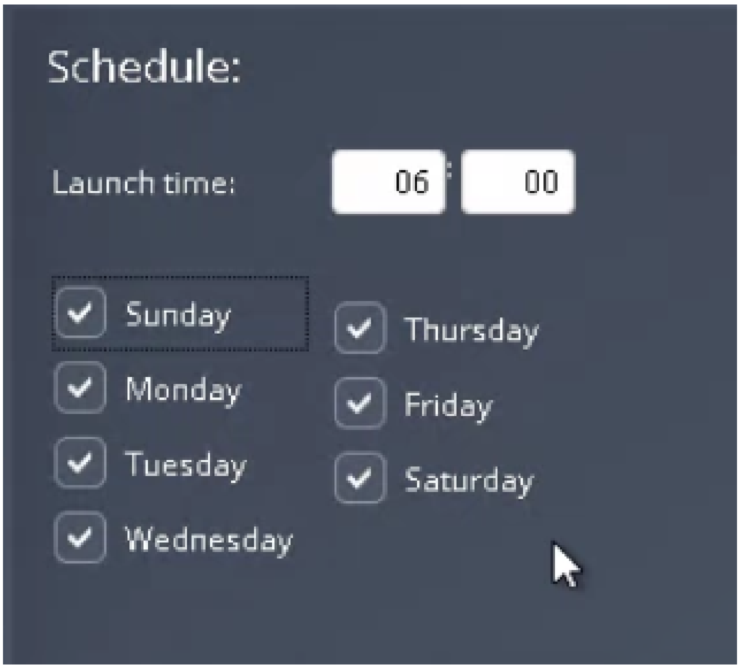


QUARANTINE 0 threats

No nasty files here!

Your quarantine is empty

Figure 3: No viruses in the quarantine for section 1.

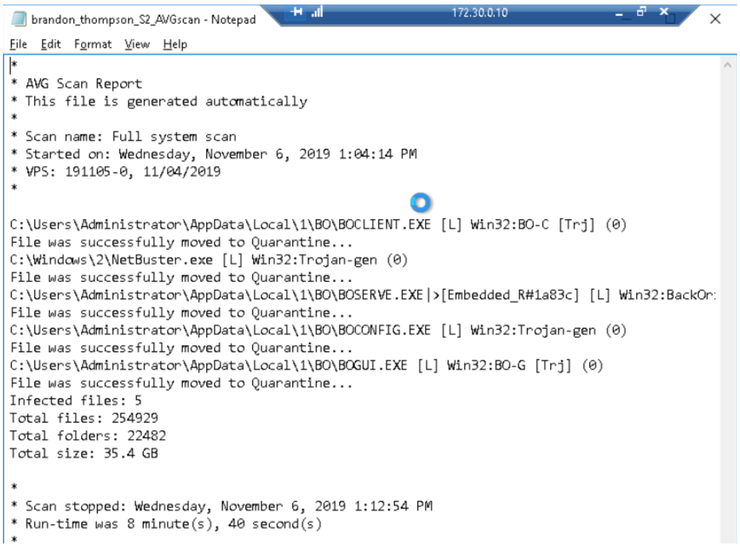


Schedule:

Launch time: 06 : 00

☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

Figure 4: Schedule for deep scan of section 1.



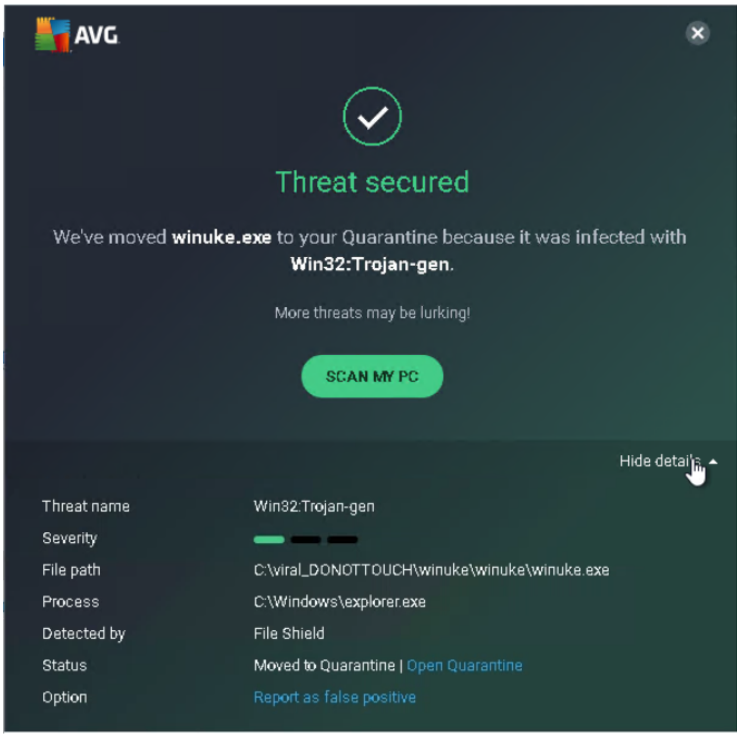
brandon_thompson_S2_AVGscan - Notepad
172.30.0.10
File Edit Format View Help

```
*
* AVG Scan Report
* This file is generated automatically
*
* Scan name: Full system scan
* Started on: Wednesday, November 6, 2019 1:04:14 PM
* VPS: 191105-0, 11/04/2019
*

C:\Users\Administrator\AppData\Local\1\BO\BOCLIENT.EXE [L] Win32:BO-C [Trj] (0)
File was successfully moved to Quarantine...
C:\Windows\2\NetBuster.exe [L] Win32:Trojan-gen (0)
File was successfully moved to Quarantine...
C:\Users\Administrator\AppData\Local\1\BO\BOSERVE.EXE|>[Embedded_R#1a83c] [L] Win32:BackOr:
File was successfully moved to Quarantine...
C:\Users\Administrator\AppData\Local\1\BO\BOCONFIG.EXE [L] Win32:Trojan-gen (0)
File was successfully moved to Quarantine...
C:\Users\Administrator\AppData\Local\1\BO\BOGUI.EXE [L] Win32:BO-G [Trj] (0)
File was successfully moved to Quarantine...
Infected files: 5
Total files: 254929
Total folders: 22482
Total size: 35.4 GB

*
* Scan stopped: Wednesday, November 6, 2019 1:12:54 PM
* Run-time was 8 minute(s), 40 second(s)
*
```

Figure 5: Results of AVG deep scan for section 2.



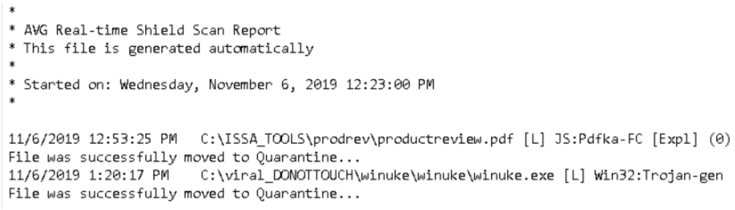
Threat secured

We've moved **winuke.exe** to your Quarantine because it was infected with **Win32:Trojan-gen**.

More threats may be lurking!

Threat name	Win32:Trojan-gen
Severity	▬ ▬ ▬
File path	C:\viral_DONOTTOUCH\winuke\winuke\winuke.exe
Process	C:\Windows\explorer.exe
Detected by	File Shield
Status	Moved to Quarantine | Open Quarantine
Option	Report as false positive

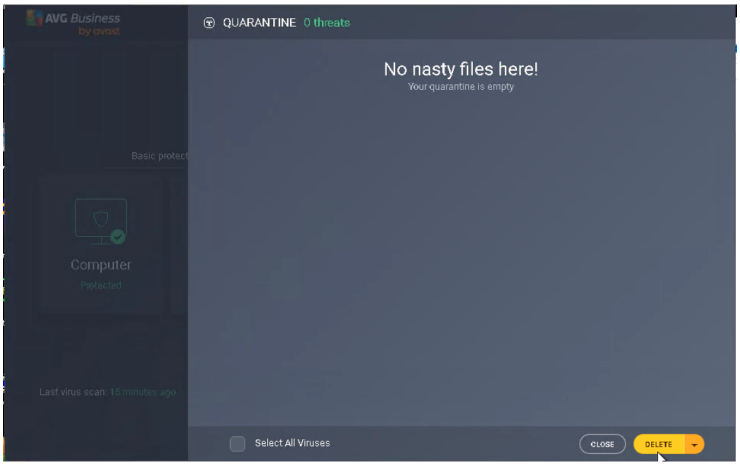
Figure 6: Threat details of `winuke.exe`|



```
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
* Started on: Wednesday, November 6, 2019 12:23:00 PM
*

11/6/2019 12:53:25 PM   C:\ISSA_TOOLS\prodrev\productreview.pdf [L] JS:Pdfka-FC [Expl] (0)
File was successfully moved to Quarantine...
11/6/2019 1:20:17 PM    C:\viral_DONOTTOUCH\winuke\winuke\winuke.exe [L] Win32:Trojan-gen
File was successfully moved to Quarantine...
```

Figure 7: Contents of `FileSystemShield|`



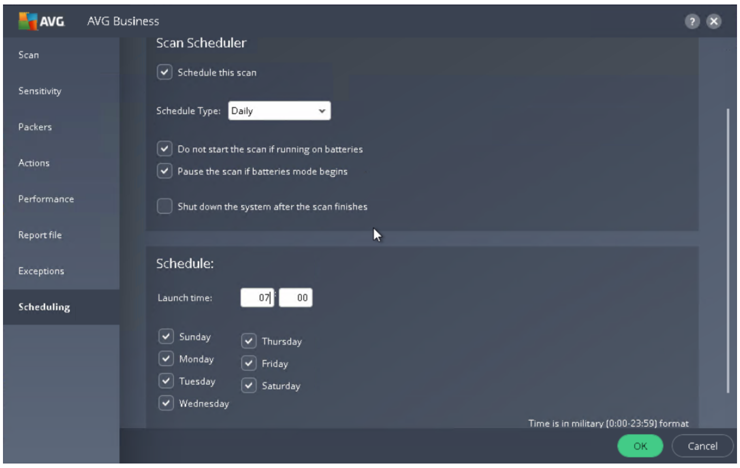
QUARANTINE 0 threats

No nasty files here!

Your quarantine is empty

□ Select All Viruses

Figure 8: Empty quarantine vault for section 2.



Scan Scheduler

☑ Schedule this scan

Schedule Type: Daily

☑ Do not start the scan if running on batteries

☑ Pause the scan if batteries mode begins

□ Shut down the system after the scan finishes

Schedule:

Launch time: 07 : 00

☑ Sunday ☑ Thursday

☑ Monday ☑ Friday

☑ Tuesday ☑ Saturday

☑ Wednesday

Time is in military [0:00-23:59] format

Figure 9: Deep scan scheduled for 7 AM every day.