

## LAB 6: IDENTIFYING AND REMOVING MALWARE ON A WINDOWS SYSTEM

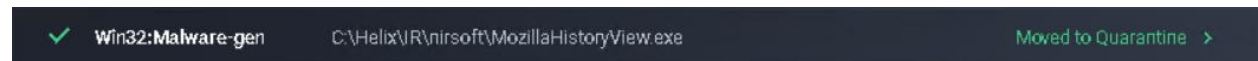
By: Jason Hodge

**Overview:** In this lab I used AVG Business Antivirus software to identify and manage threats to the system. I also analyzed threats in encrypted archive files.

### Section 1:



The first high severity threat is cryptocat.exe which is an open-source application to allow encrypted online chatting.



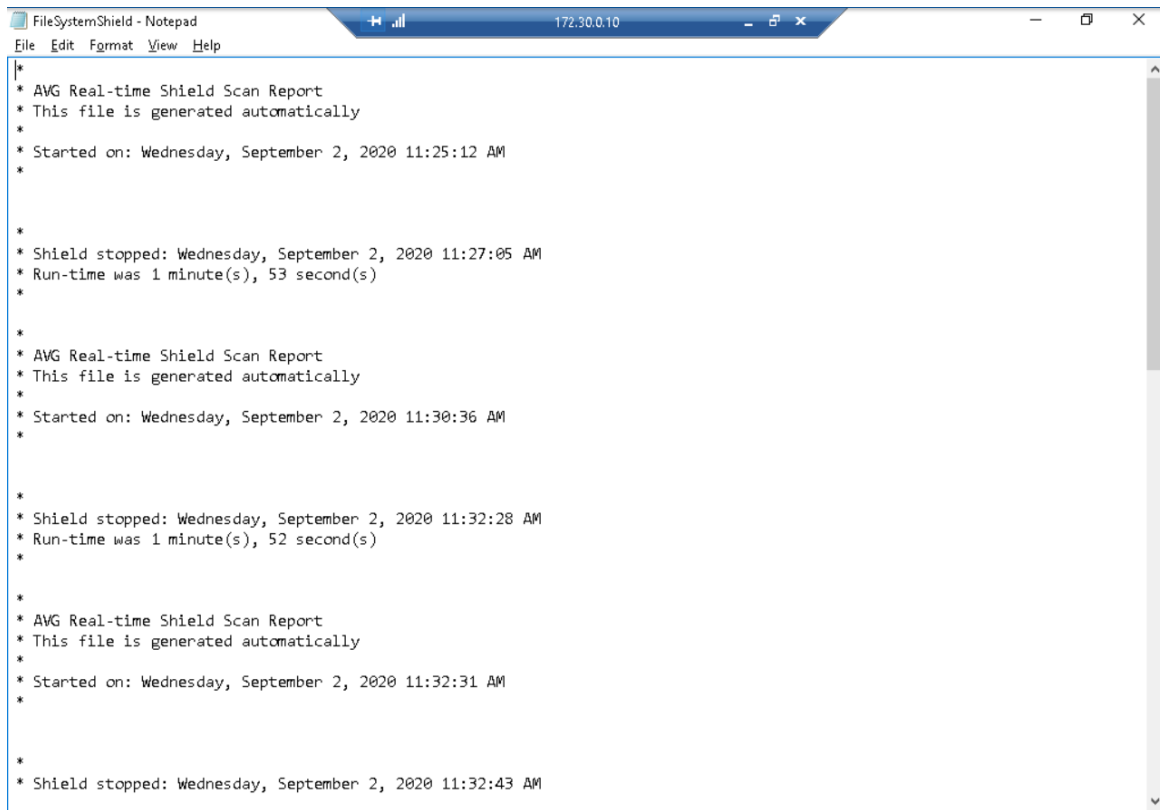
Other high severity threat.

Jason\_S1\_AVGscan file contents

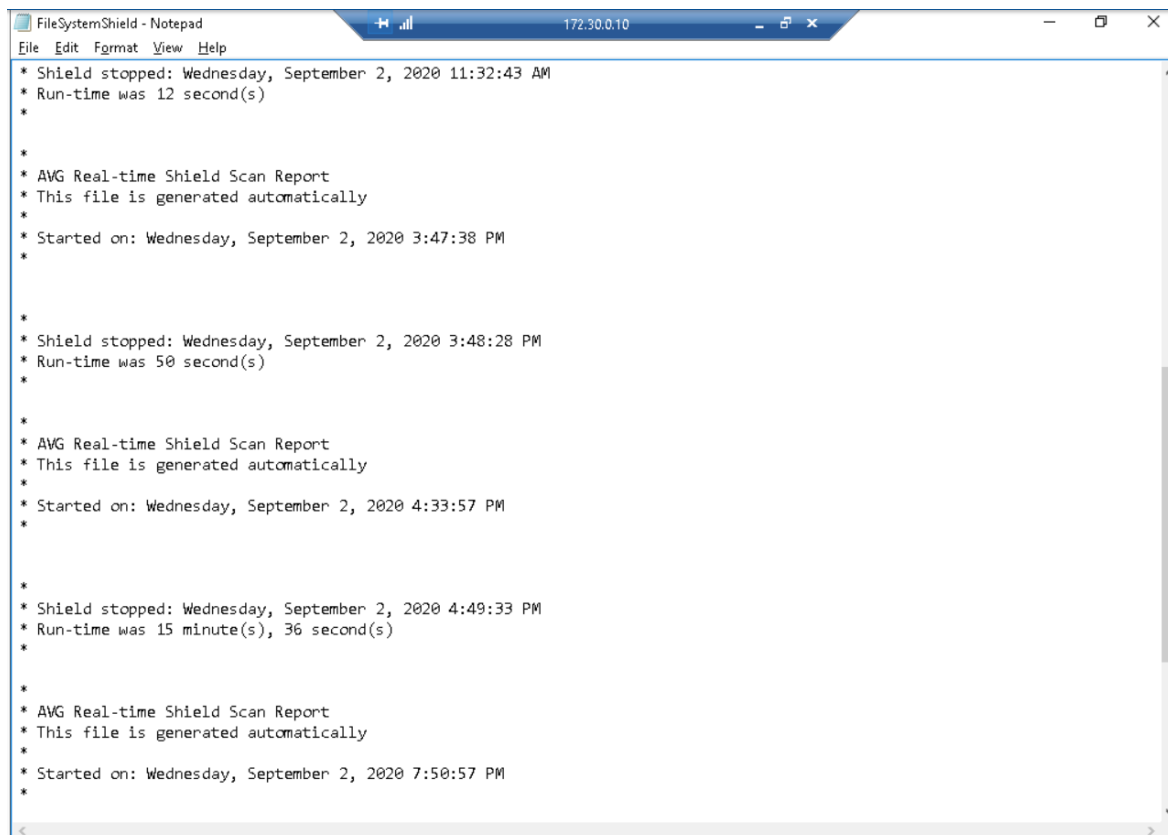
```
Jason_S1_AVGscan - Notepad
File Edit Format View Help
172.30.0.10

* AVG Scan Report
* This file is generated automatically
*
* Scan name: Full system scan
* Started on: Wednesday, April 28, 2021 2:58:34 PM
* VPS: 210423-9, 04/23/2021
*
C:\Helix\IR\Foundstone\sl.exe|>[UPX] [L] Win32:PUP-gen [PUP] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\bin\cryptocat.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\MozillaHistoryView.exe [L] Win32:Malware-gen (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: 10
Total files: 254279
Total folders: 22478
Total size: 37.1 GB
*
* Scan stopped: Wednesday, April 28, 2021 3:04:58 PM
* Run-time was 6 minute(s), 24 second(s)
```

## FileSystemShield file contents



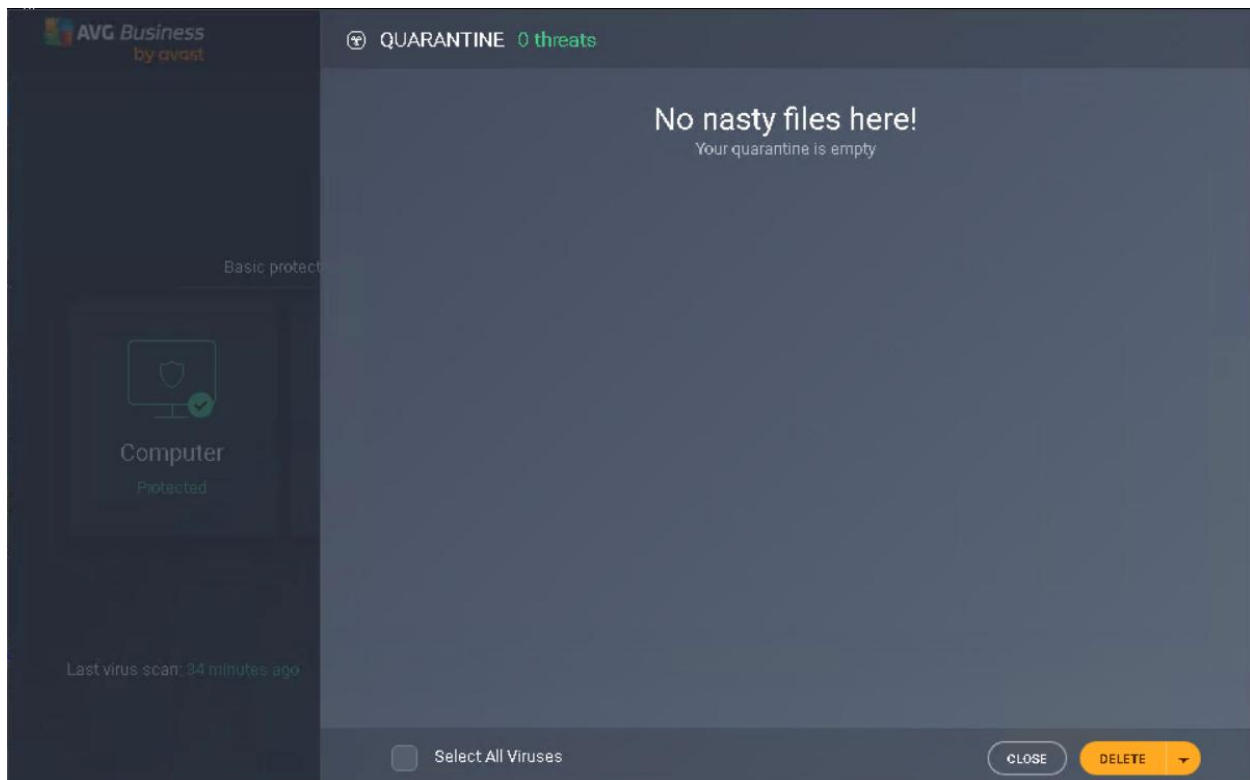
```
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
*
* Started on: Wednesday, September 2, 2020 11:25:12 AM
*
*
*
*
* Shield stopped: Wednesday, September 2, 2020 11:27:05 AM
* Run-time was 1 minute(s), 53 second(s)
*
*
*
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
*
* Started on: Wednesday, September 2, 2020 11:30:36 AM
*
*
*
*
* Shield stopped: Wednesday, September 2, 2020 11:32:28 AM
* Run-time was 1 minute(s), 52 second(s)
*
*
*
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
*
* Started on: Wednesday, September 2, 2020 11:32:31 AM
*
*
*
*
* Shield stopped: Wednesday, September 2, 2020 11:32:43 AM
```



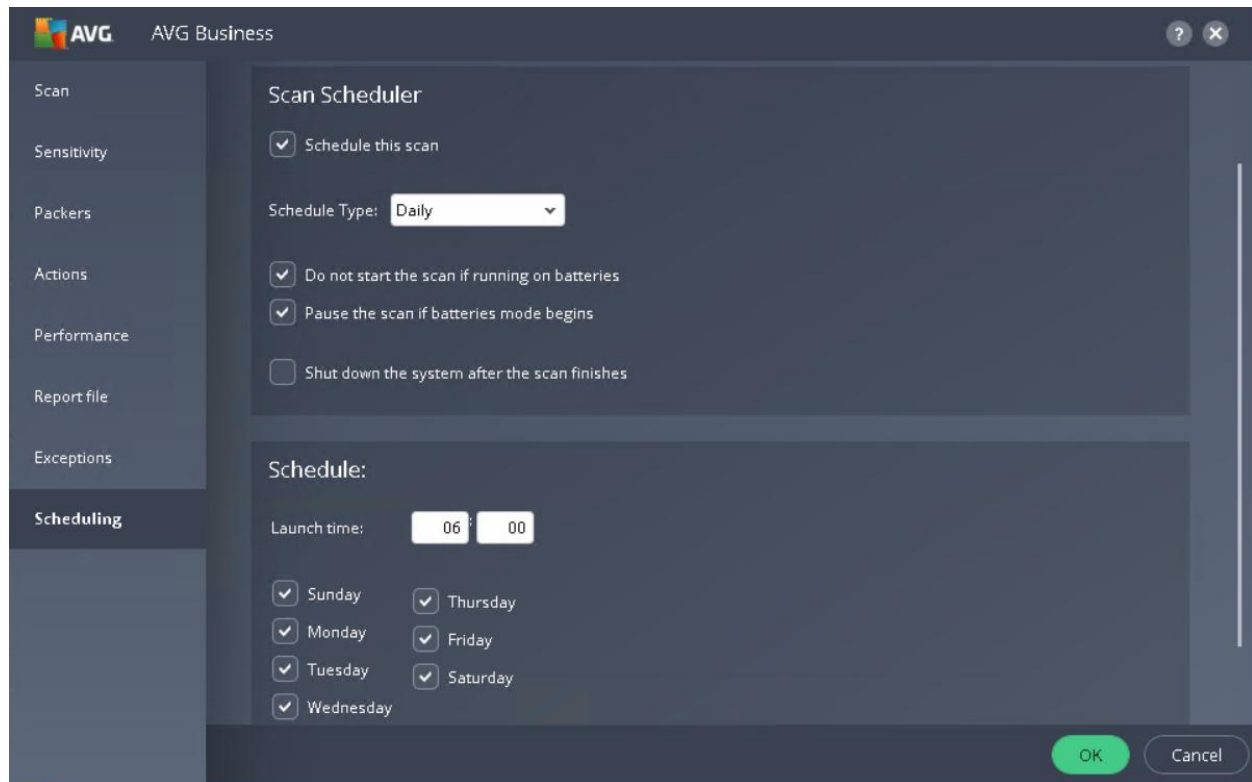
```
* Shield stopped: Wednesday, September 2, 2020 11:32:43 AM
* Run-time was 12 second(s)
*
*
*
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
*
* Started on: Wednesday, September 2, 2020 3:47:38 PM
*
*
*
*
* Shield stopped: Wednesday, September 2, 2020 3:48:28 PM
* Run-time was 50 second(s)
*
*
*
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
*
* Started on: Wednesday, September 2, 2020 4:33:57 PM
*
*
*
*
* Shield stopped: Wednesday, September 2, 2020 4:49:33 PM
* Run-time was 15 minute(s), 36 second(s)
*
*
*
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
*
* Started on: Wednesday, September 2, 2020 7:50:57 PM
*
```

```
*
* Shield stopped: Wednesday, September 2, 2020 7:52:22 PM
* Run-time was 1 minute(s), 25 second(s)
*
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
* Started on: Wednesday, April 28, 2021 2:56:48 PM
*
4/28/2021 3:32:42 PM    C:\ISSA_TOOLS\prodrev\productreview.pdf [L] JS:Pdfka-FC [Exp1] (0)
File was successfully moved to Quarantine...
```

## Empty Quarantine Area



## Scheduled Scan



## Section 2:

### Last high severity threat

|   |                  |   |                       |
|---|------------------|---|-----------------------|
| ✓ | Win32:BO-G [Trj] | C:\Users\Administrator\AppData\Local\1\BO\BOGUI.EXE | Moved to Quarantine > |
|---|------------------|---|-----------------------|

### Other high severity threats

|   |                   |  |                       |
|---|-------------------|--|-----------------------|
| ✓ | Win32:Malware-gen | C:\Helix\IR\nirsoft\MozillaHistoryView.exe | Moved to Quarantine > |
|---|-------------------|--|-----------------------|

|   |                   |                              |                       |
|---|-------------------|------------------------------|-----------------------|
| ✓ | Win32:Malware-gen | C:\Helix\IR\bin\cryptcat.exe | Moved to Quarantine > |
|---|-------------------|------------------------------|-----------------------|

|   |                         |   |                       |
|---|-------------------------|---|-----------------------|
| ✓ | Win32:BO-C [Trj]        | C:\Users\Administrator\AppData\Local\1\BO\BOCLIENT.EXE            | Moved to Quarantine > |
| ✓ | Win32:Trojan-gen        | C:\Windows\2\NetBuster.exe  | Moved to Quarantine > |
| ✓ | Win32:BackOrifice [Trj] | C:\Users\Administrator\AppData\Local\1\BO\BOSERVE.EXE]>[Embedde.. | Moved to Quarantine > |

## Jason\_S2\_AVGscan file contents

```
Jason_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, April 28, 2021 4:45:47 PM
* VPS: 210423-9, 04/23/2021
*


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\BOSERVICE.EXE [L] Win32:BackOrifice [Trj] (0)
File was successfully moved to Quarantine...
C:\Helix\IR\Foundstone\sl.exe [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\MozillaHistoryView.exe [L] Win32:Malware-gen (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:\Users\Administrator\AppData\Local\1\BO\BOGUI.EXE [L] Win32:BO-G [Trj] (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)


C:\Helix\IR\nirsoft\rdpv.exe [L] Win32:PSWtool-V [PUP] (0)
File was successfully moved to Quarantine...
Infected files: 14
Total files: 254276
Total folders: 22480
Total size: 37.1 GB

*
* Scan stopped: Wednesday, April 28, 2021 4:53:08 PM
* Run-time was 7 minute(s), 21 second(s)
*
```

Threat Details







Threat secured

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

More threats may be lurking!

SCAN MY PC

Hide details ▲

|             |   |
|-------------|---|
| Threat name | Win32:Trojan-gen                                      |
| Severity    | <div><div></div><div></div><div></div></div>          |
| File path   | C:\viral_DONOTTOUCH\winuke\winuke\winuke.exe          |
| Process     | C:\Windows\explorer.exe                               |
| Detected by | File Shield   |
| Status      | Moved to Quarantine   <a href="#">Open Quarantine</a> |
| Option      | <a href="#">Report as false positive</a>              |

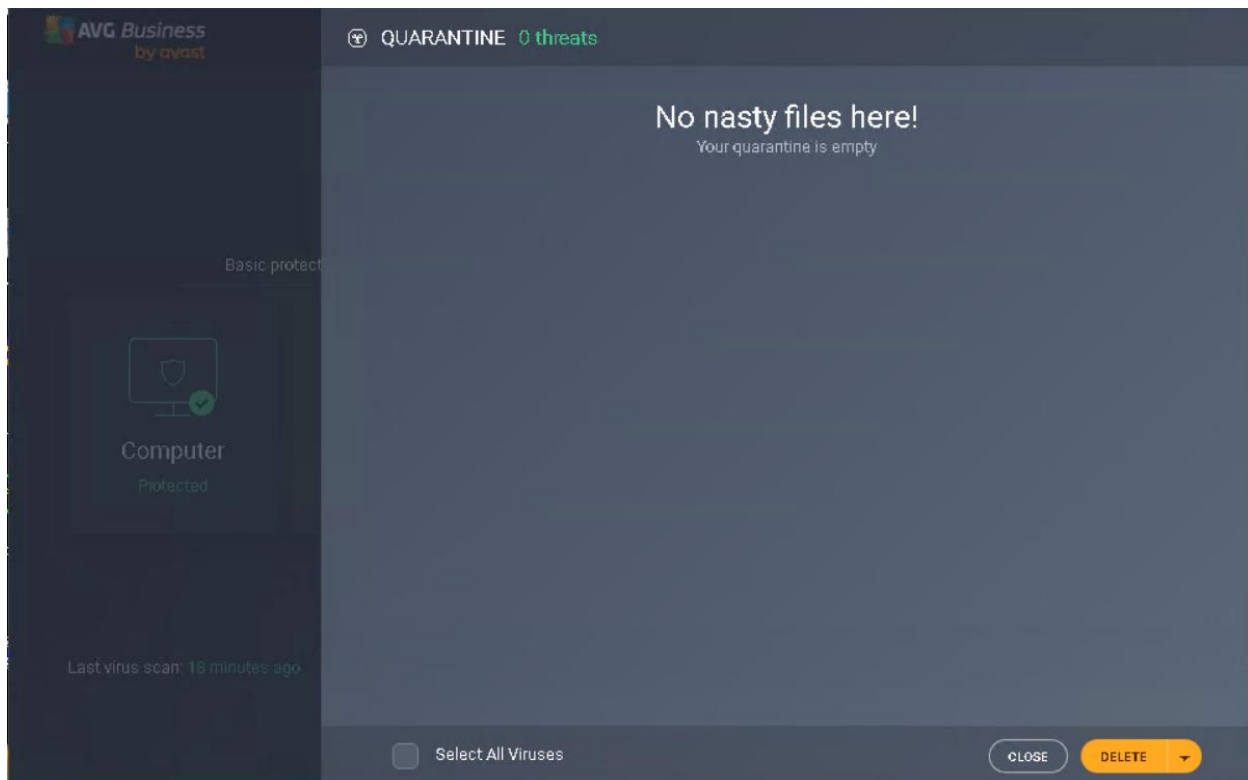
## FileSystemSheild file contents

```
*  
* AVG Real-time Shield Scan Report  
* This file is generated automatically  
*  
* Started on: Wednesday, September 2, 2020 11:25:12 AM  
*  
  
*  
* Shield stopped: Wednesday, September 2, 2020 11:27:05 AM  
* Run-time was 1 minute(s), 53 second(s)  
*  
  
*  
* AVG Real-time Shield Scan Report  
* This file is generated automatically  
*  
* Started on: Wednesday, September 2, 2020 11:30:36 AM  
*  
  
*  
* Shield stopped: Wednesday, September 2, 2020 11:32:28 AM  
* Run-time was 1 minute(s), 52 second(s)  
*  
  
*  
* AVG Real-time Shield Scan Report  
* This file is generated automatically  
*  
* Started on: Wednesday, September 2, 2020 11:32:31 AM  
*  
  
*  
* Shield stopped: Wednesday, September 2, 2020 11:32:43 AM
```

```
FileSystemShield - Notepad
172.30.0.10
File Edit Format View Help
* Shield stopped: Wednesday, September 2, 2020 11:32:43 AM
* Run-time was 12 second(s)
*
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
* Started on: Wednesday, September 2, 2020 3:47:38 PM
*
*
* Shield stopped: Wednesday, September 2, 2020 3:48:28 PM
* Run-time was 50 second(s)
*
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
* Started on: Wednesday, September 2, 2020 4:33:57 PM
*
*
* Shield stopped: Wednesday, September 2, 2020 4:49:33 PM
* Run-time was 15 minute(s), 36 second(s)
*
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
* Started on: Wednesday, September 2, 2020 7:50:57 PM
*
```

```
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
* Started on: Wednesday, April 28, 2021 4:44:32 PM
*
4/28/2021 5:05:39 PM    C:\viral_DONOTTOUCH\winuke\winuke.exe [L] Win32:Trojan-gen (0)
File was successfully moved to Quarantine...
```

## Empty Quarantine Area





## Scheduled Scan

The screenshot shows the 'Scheduled Scan' settings window in AVG Business. The window has a dark theme and a sidebar on the left with navigation options: Scan, Sensitivity, Packers, Actions, Performance, Report file, Exceptions, and Scheduling (which is highlighted). The main area is divided into two sections. The top section, titled 'Schedule this scan', has a checked checkbox and a 'Schedule Type' dropdown menu set to 'Daily'. Below this are three checkboxes: 'Do not start the scan if running on batteries' (checked), 'Pause the scan if batteries mode begins' (checked), and 'Shut down the system after the scan finishes' (unchecked). The bottom section, titled 'Schedule:', shows a 'Launch time' of 07:00. Below the time are seven checkboxes for the days of the week, all of which are checked: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. A note at the bottom right of the schedule section states 'Time is in military (0:00-23:59) format'. At the bottom right of the window are 'OK' and 'Cancel' buttons.

AVG Business

Scan

Sensitivity

Packers

Actions

Performance

Report file

Exceptions

**Scheduling**

☒ 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

OK Cancel