

IST 623 - Intro to Information Security

Homework Assignment 2

Marriah Lewis

Term: Summer, 2021

Topic: Identifying and Removing Malware on a
Windows System

Table of Contents

1	Part 1: Using Antivirus Software to Scan Potentially Infected System	3-5
2	Part 2: Identify Threats in Encrypted Archive Files	5-7

Lab Report #1

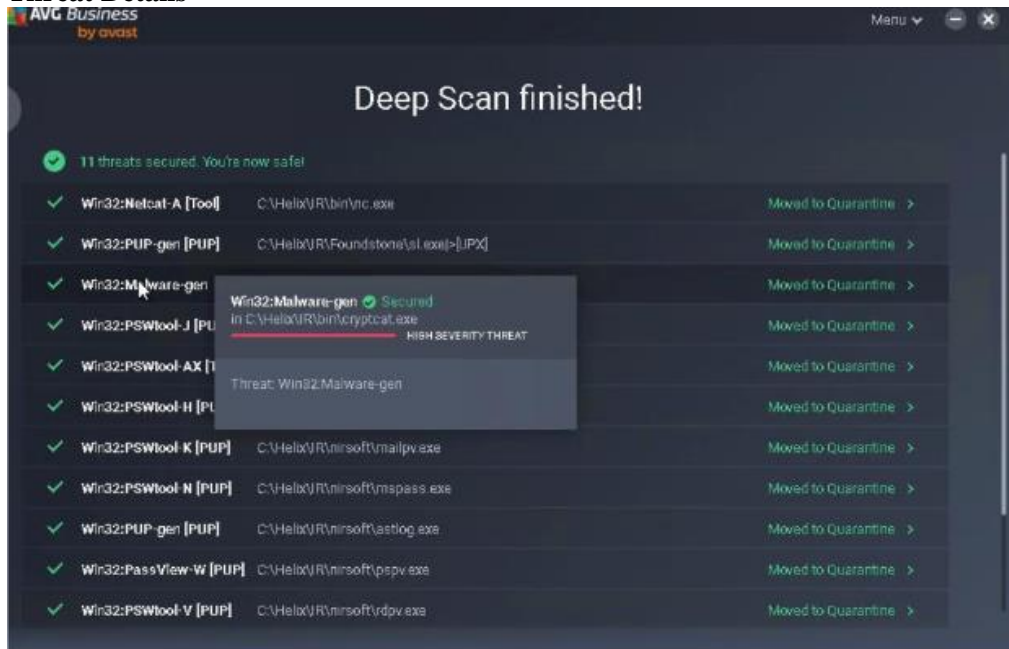
1 Introduction

Malware is computer software that is meant to disrupt, harm, or gain unauthorized access to a system. This harm can take several forms and present itself to the user differently depending on the sort of infection. Malware can have a mild and harmless effect in some circumstances, but it can also be disastrous in others. However, antivirus programs have two approaches that can help stop these attacks. Suspicious behavior and/or dictionary-based detection, these approaches can recognize symptoms of a virus and use a signatures database to identify a virus. This assignment is split up into two sections.

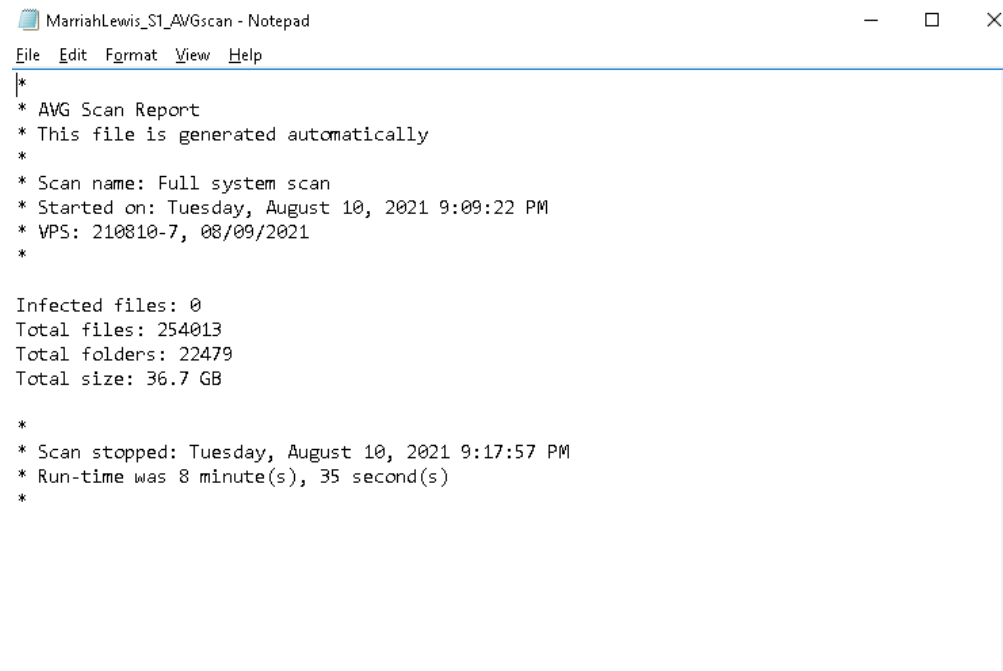
1. Section 1 Part 1: Manually scanning the TargerWindows02 machine with AVG, an antivirus program, to see how AVG and related software products detect malware.
2. Section 1 Part 2: Using AVG to scan a single folder on the TargetWindows2 machine to detect a hidden virus embedded in an encrypted file.
3. Section 2 Part 1: Using Antivirus Software to scan the infected system
4. Section 2 Part 2: Identify Threats in Encrypted Archive Files
5. Section 2 Part 3: Manage AVG Scans and the Quarantine Area

Section 1

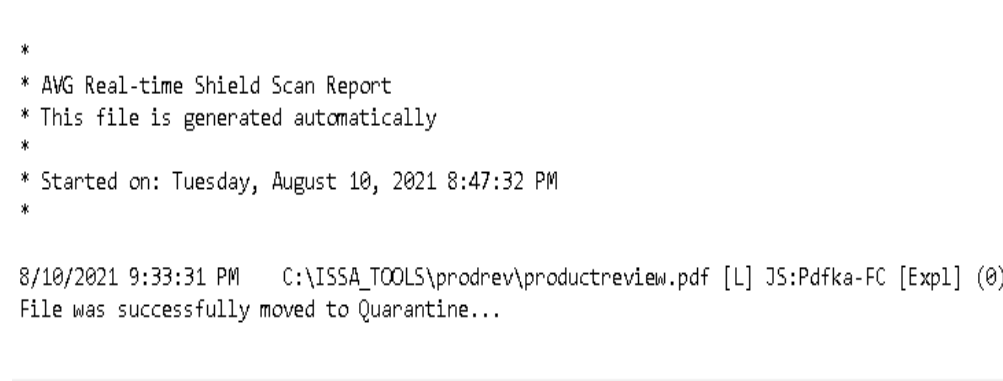
Threat Details



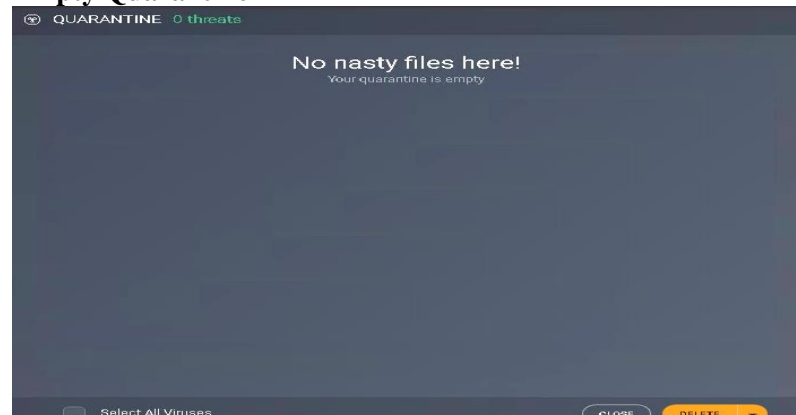
Lab Report #1

Contents of AVG scan file

```
*
* AVG Scan Report
* This file is generated automatically
*
* Scan name: Full system scan
* Started on: Tuesday, August 10, 2021 9:09:22 PM
* VPS: 210810-7, 08/09/2021
*
Infected files: 0
Total files: 254013
Total folders: 22479
Total size: 36.7 GB
*
* Scan stopped: Tuesday, August 10, 2021 9:17:57 PM
* Run-time was 8 minute(s), 35 second(s)
*
```

FileSystemShield File

```
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
* Started on: Tuesday, August 10, 2021 8:47:32 PM
*
8/10/2021 9:33:31 PM C:\ISSA_TOOLS\prodrev\productreview.pdf [L] JS:Pdfka-FC [Exp1] (0)
File was successfully moved to Quarantine...
```

Empty Quarantine

Lab Report #1

Scan Scheduler

Schedule:

Launch time: :

☒ Sunday ☒ Thursday
☒ Monday ☒ Friday
☒ Tuesday ☒ Saturday
☒ Wednesday

Time is in military (0:00-23:59) format

Section 2:

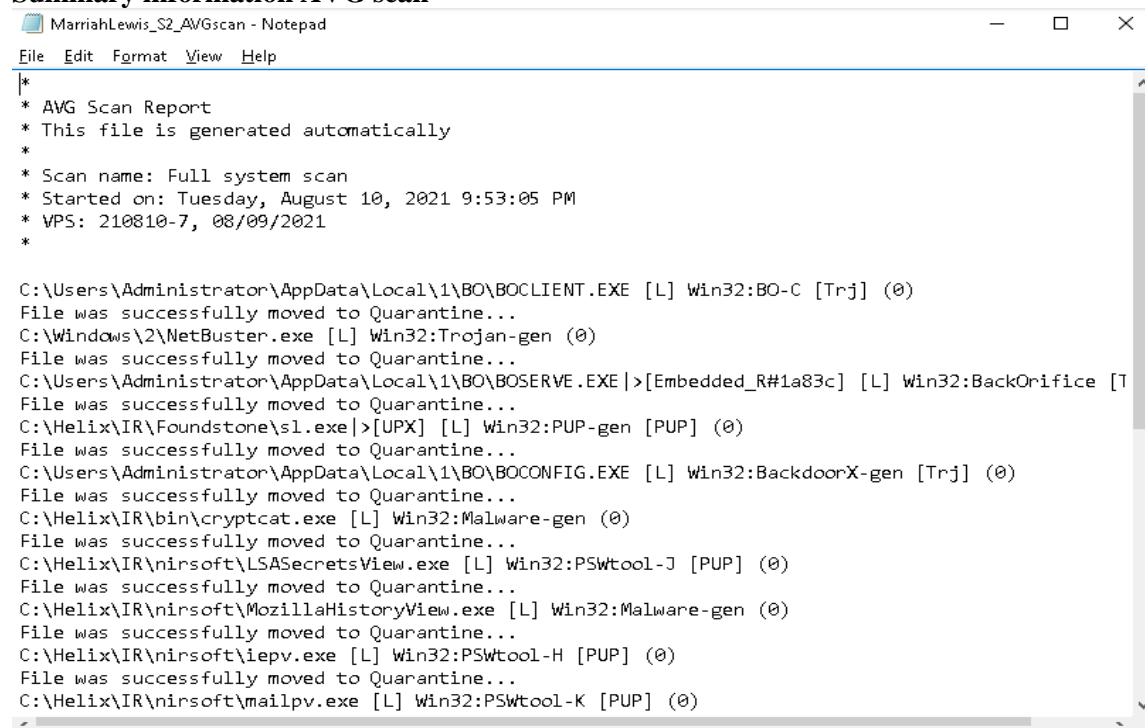
High Severity Threats by AVG

Deep Scan finished!

✓	Win32:PSWtool-J [PUP]	C:\Helix\VR\nirsoft\LSASecretsView.exe	Moved to Quarantine >
✓	Win32:Malware-gen	C:\Helix\VR\nirsoft\MozillaHistoryView.exe	Moved to Quarantine >
✓	Win32:PSWtool-H [PUP]	C:\Helix\VR\nirsoft\lepv.exe	Moved to Quarantine >
✓	Win32:PSWtool-K [PUP]	C:\Helix\VR\nirsoft\mailpv.exe	Moved to Quarantine >
✓	Win32:PSWtool-N [PUP]	C:\Helix\VR\nirsoft\vmsspass.exe	Moved to Quarantine >
✓	Win32:BO-G [Trj]	Win32:BO-G [Trj] Secured in C:\Users\Administrator\AppData\Local\1\BO\BOG UI.EXE	Moved to Quarantine >
✓	Win32:PUP-gen [PUP]	Threat: Win32:BO-G [Trj]	Moved to Quarantine >
✓	Win32:PassView-1		Moved to Quarantine >
✓	Win32:PSWtool-V		Moved to Quarantine >

Lab Report #1

Summary information AVG scan

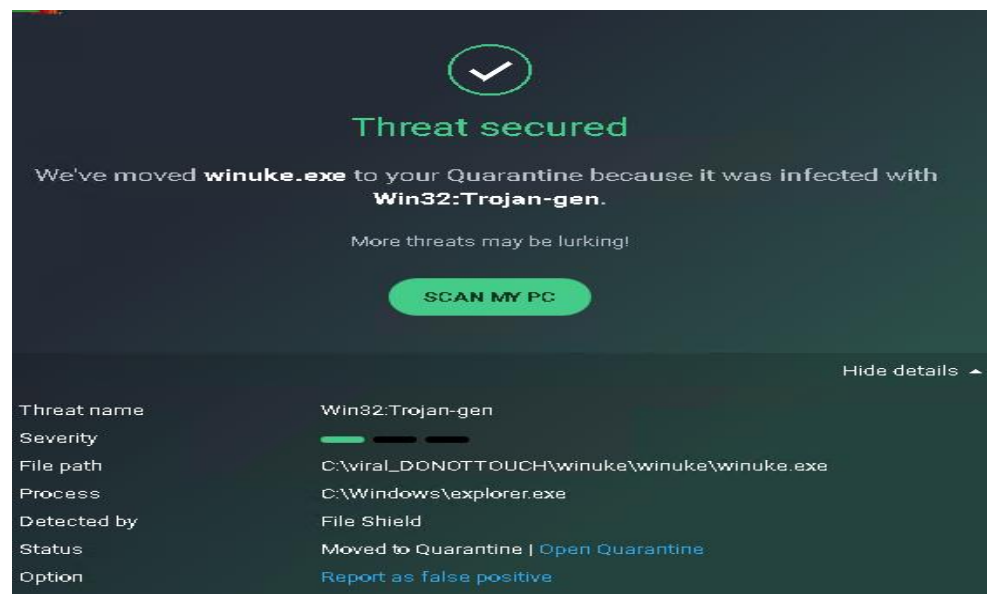


```

MarriahLewis_S2_AVGscan - Notepad
File Edit Format View Help
*
* AVG Scan Report
* This file is generated automatically
*
* Scan name: Full system scan
* Started on: Tuesday, August 10, 2021 9:53:05 PM
* VPS: 210810-7, 08/09/2021
*
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\BOSSERVE.EXE [L] Win32:BackOrifice [T
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:\Users\Administrator\AppData\Local\1\BO\BOCONFIG.EXE [L] Win32:BackdoorX-gen [Trj] (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)

```

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](#)

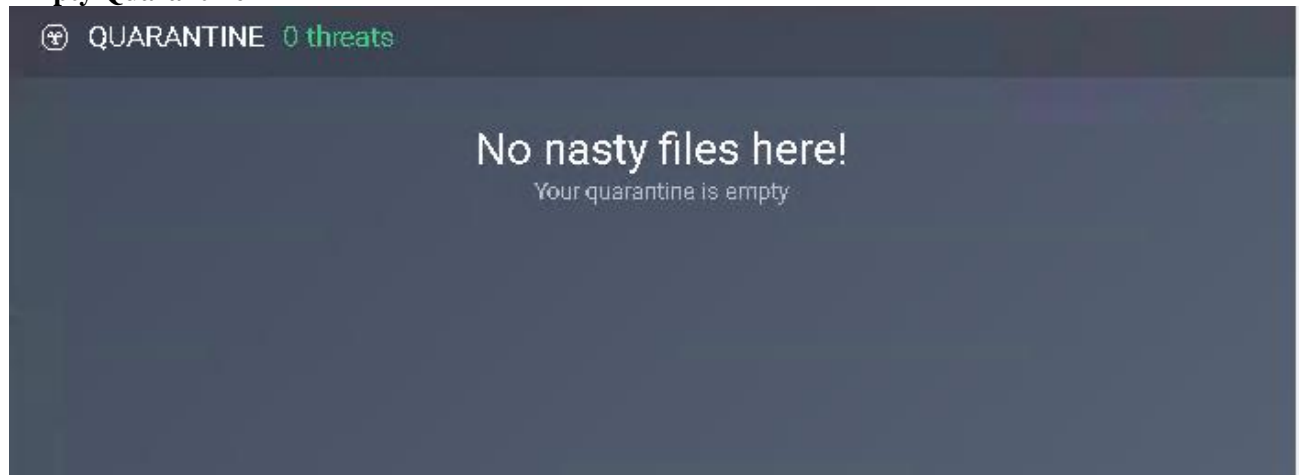
Threat name	Win32:Trojan-gen
Severity	<div><div></div></div>
File path	C:\viral_DONOTTOUCH\winuke\winuke\winuke.exe
Process	C:\Windows\explorer.exe
Detected by	File Shield
Status	Moved to Quarantine Open Quarantine
Option	Report as false positive

Lab Report #1

FileSystemShield file

```
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
* Started on: Tuesday, August 10, 2021 9:49:30 PM
*
```

```
8/10/2021 10:12:50 PM C:\viral_DONOTTOUCH\winuke\winuke\winuke.exe [L] Win32:Trojan-gen (0)
File was successfully moved to Quarantine...
```

Empty Quarantine**Scheduler**