

IST 623 - Intro to Information Security

Homework Lab 1

Ryan Timbrook

NetID: RTIMBROO

Term: Winter, 2020

Date: 2/5/2020

Topic: Identifying and Removing Malware
on a Windows System

Homework Lab 1

Table of Contents

1	Part 1: Using Antivirus Software to Scan the Potentially Infected System	3
1.1	Step #17 Screen Print: Threat Details.....	3
1.2	Step #25 Screen Print: Contents of yourname_S1_AVGscan file	4
2	Part 2: Identify Threats in Encrypted Archive Files	5
2.1	Step #11 Screen Print: Pdffa-FC threat detection	5
3	Part 3: Manage AVG Scans and the Virus Vault	6
3.1	Step #5 Screen Print: Empty Quarantine Area	6
3.2	Step #12 Screen Print: Scheduled Scan	6
4	Part 4: Challenge Question	7

Homework Lab 1

1 Part 1: Using Antivirus Software to Scan the Potentially Infected System

Malware includes anything developed for the purpose of doing harm. If it were easy to find, it wouldn't cause any damage to an individual machine or to an entire network. Ideally, your antivirus software is running automatically and finding malware on its own. However, if you recognize the symptoms of a malware infection, you can manually scan the computer.

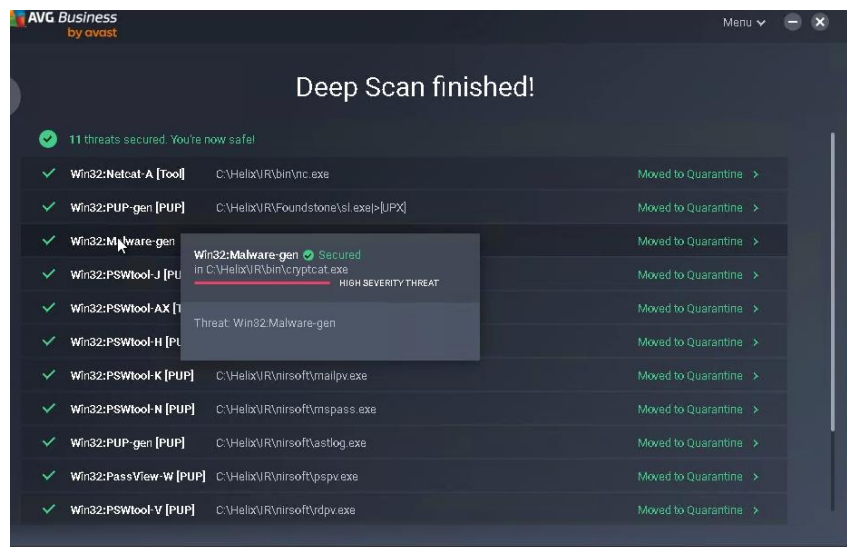
These symptoms include:

- Slow response opening applications or browsing the Internet.
- Applications not working as they normally would.
- Operating system not booting up correctly or not functioning normally.
- Event logs reporting numerous, unusual alerts.
- Antivirus software is disabled, not running, or unable to update its virus definitions.
- Numerous windows popping up when trying to access the Internet or opening a browser.

Deliverable: Provide screenshots from part 1, steps #17 and #25

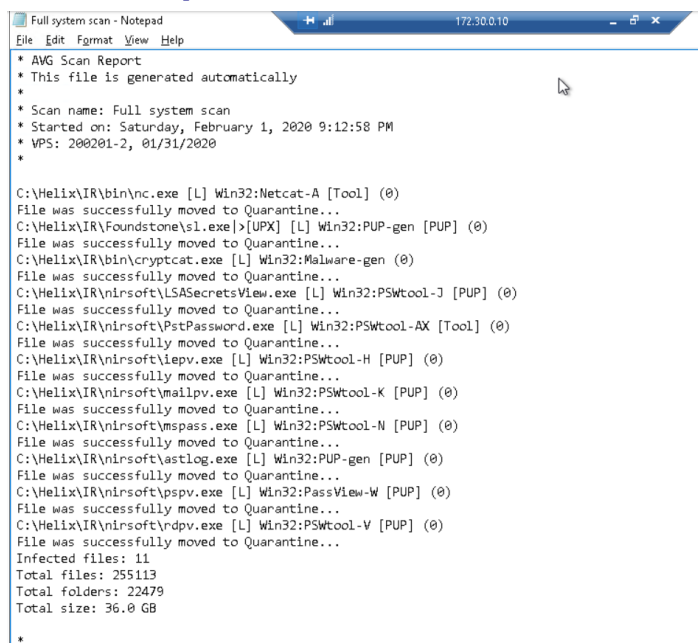
In this section, you will use AVG, an antivirus program, to manually scan the TargetWindows02 machine to see how AVG and similar software programs identify malware.

1.1 Step #17 Screen Print: Threat Details



Homework Lab 1

1.2 Step #25 Screen Print: Contents of yourname_S1_AVGscan file



```
* AVG Scan Report
* This file is generated automatically
*
* Scan name: Full system scan
* Started on: Saturday, February 1, 2020 9:12:58 PM
* VPS: 200201-2, 01/31/2020
*

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\lepv.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: 255113
Total folders: 22479
Total size: 36.0 GB
*
```

Homework Lab 1

2 Part 2: Identify Threats in Encrypted Archive Files

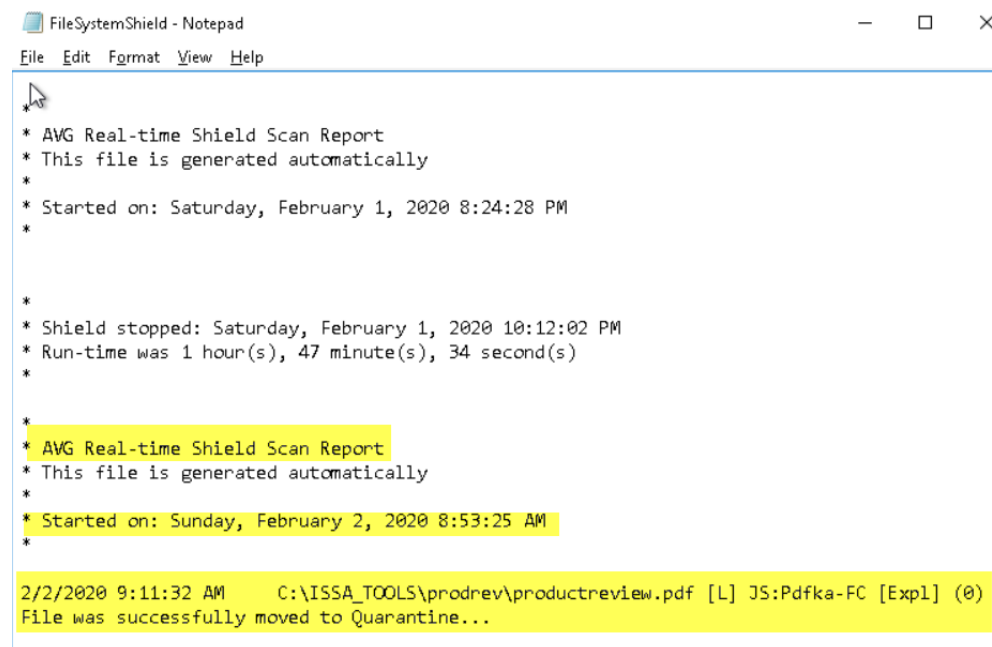
In this section, you will use the AVG to scan a single folder on the TargetWindows2 machine to detect a hidden virus embedded in an encrypted file. First, you will extract the malware from the folder structure to simulate how easily the virus can affect an unknowing victim.

Deliverable: Provide screenshots from part 2, step #11

- Screen capture showing Pdfka-FC threat detection in the FileSystemShield file

2.1 Step #11 Screen Print: Pdfka-FC threat detection

AVG provides information about the actual name of the virus (JS:Pdfka-fc) and reports that the infected file (productreview.pdf, part of the prodrev.zip file) has been deleted and the virus has been moved to the Quarantine area (Virus Vault).



```
FileSystemShield - Notepad
File Edit Format View Help

*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
* Started on: Saturday, February 1, 2020 8:24:28 PM
*
*
*
* Shield stopped: Saturday, February 1, 2020 10:12:02 PM
* Run-time was 1 hour(s), 47 minute(s), 34 second(s)
*
*
*
* AVG Real-time Shield Scan Report
* This file is generated automatically
*
* Started on: Sunday, February 2, 2020 8:53:25 AM
*
*
2/2/2020 9:11:32 AM      C:\ISSA_TOOLS\prodrev\productreview.pdf [L] JS:Pdfka-FC [Exp1] (0)
File was successfully moved to Quarantine...
```

Homework Lab 1

3 Part 3: Manage AVG Scans and the Virus Vault

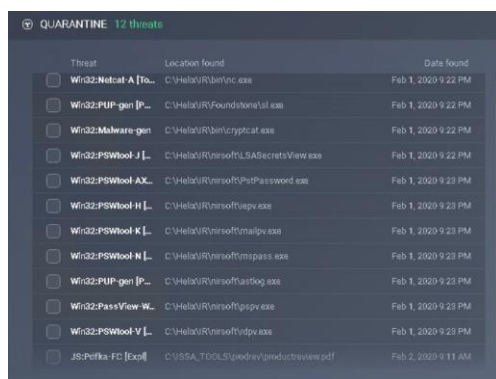
The Quarantine area (previously referred to as the Virus Vault) is where all removed files, virus infected or suspicious, are stored until you take action on them. All of the files in the quarantine area are encrypted and cannot do your computer any harm. The main purpose of the Quarantine area is to keep any suspicious file for a certain period of time, so that you can make sure you do not need the file any more and manually delete it. If you find that the AVG has quarantined a valid file (a false positive), it can be restored easily from this interface.

Deliverable: Provide screenshots from part 3, steps #5 and #12

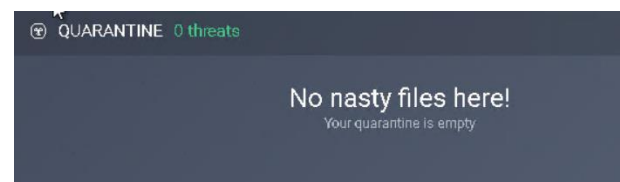
In this section, you will **empty the Quarantine area** and **schedule a complete scan** to run **daily**.

3.1 Step #5 Screen Print: Empty Quarantine Area

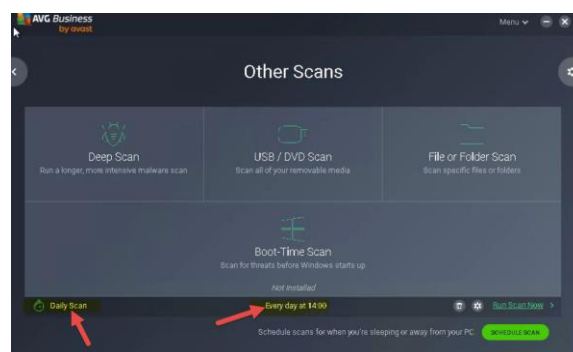
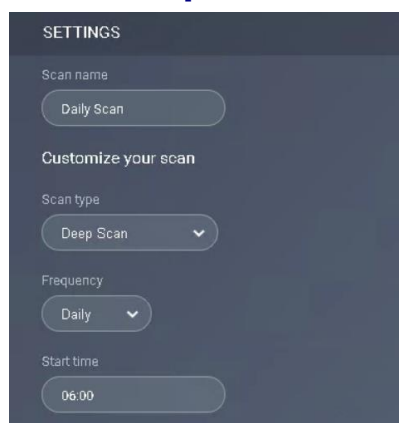
Before Deleting All Quarantined Viruses:



After Deleting All Quarantined Viruses:



3.2 Step #12 Screen Print: Scheduled Scan



4 Part 4: Challenge Question

Explain how the Quarantine mechanism is working in antivirus software packages

When the Quarantine mechanism removes an item such as a file, or registry entry and 'quarantines' it, the system is physically removing that item from its original storage location on the systems hard disk and moving it to a protected container of the Anti-Virus (AV) software package. Both the removed item and its location are stored in the container in a way that the item is rendered immobile and the location of where it was removed from is also restored. This way if the item is found to be a false-positive, (i.e., that it was identified as a virus by the antivirus software but found to actually not be a virus or something malicious), the item removed can be restored to its original and working state. If however the item(s) are found to be justly removed for malicious activity, the quarantine can be 'dumped' such that they can not be restored and the container is cleared of holding the quarantined items selected for deletion.

In many antivirus software packages the quarantined files are stored in internal binary formats. This format helps secure the system by removing any physical connection between the infector file and the system.