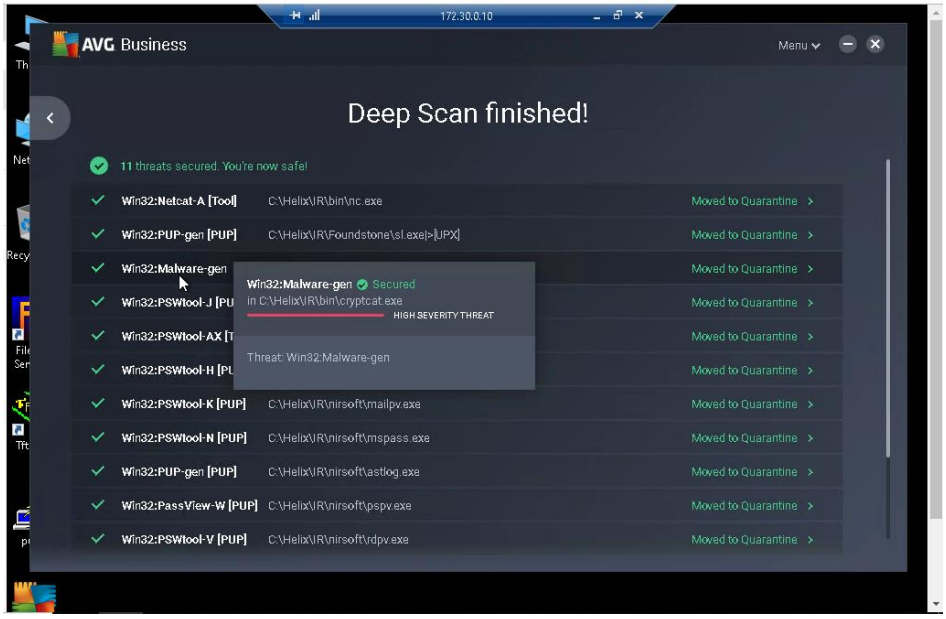
MARYMOUNT UNIVERSITY

Assignment: IT557; Monitoring, Auditing, and Penetration Testing
Assigned: Oct. 28, 2018
Instructor: Professor Ali Bicak
Student Name: George Boakye

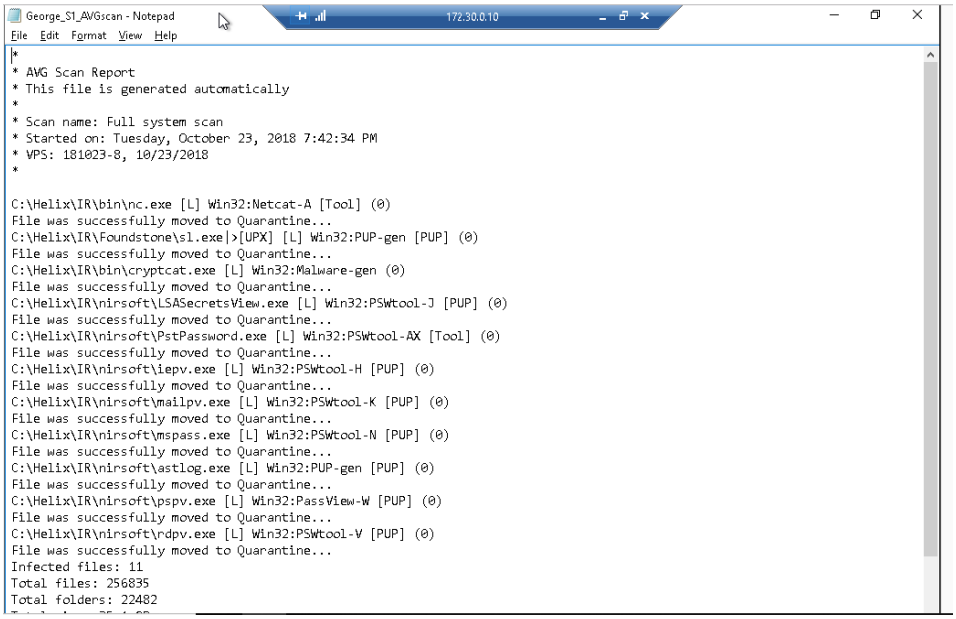
LAB REPORT FILE (LAB6)

SECTION 1

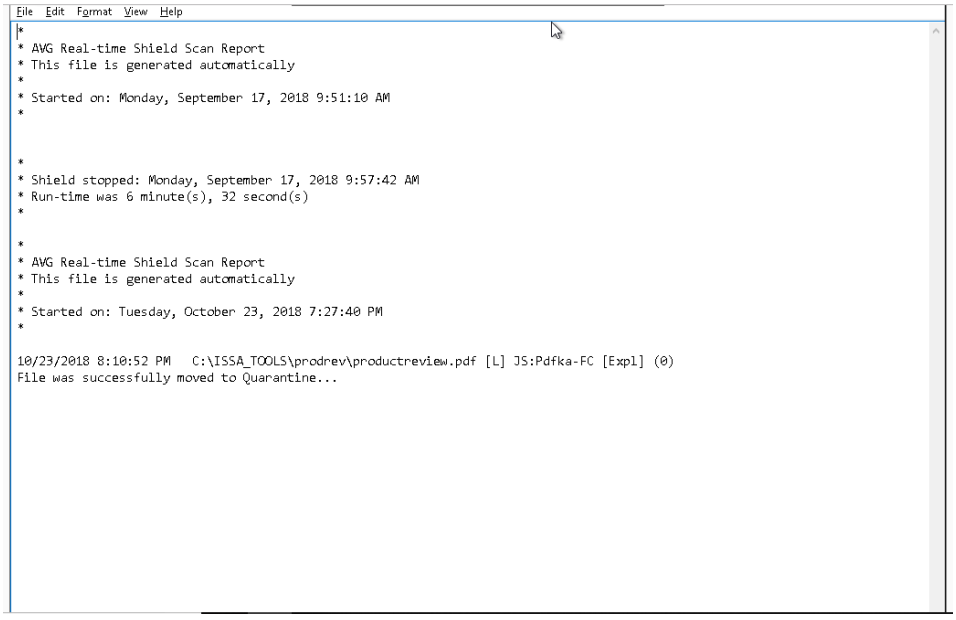
Part 1: Step 17: Details of First High Severity Threat



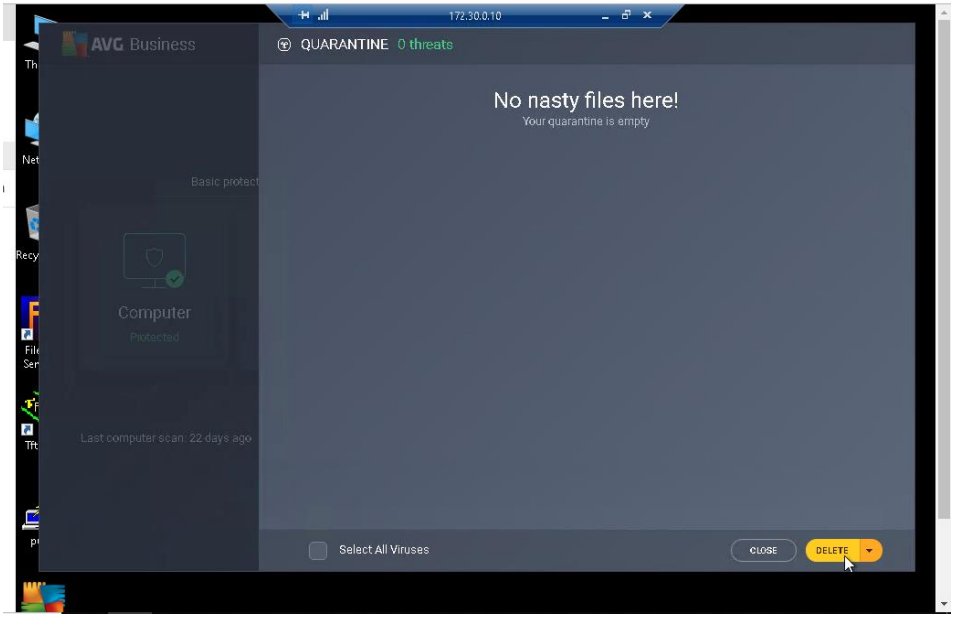
Part 1: Step 25: Contents of George_S1_AVGscan file



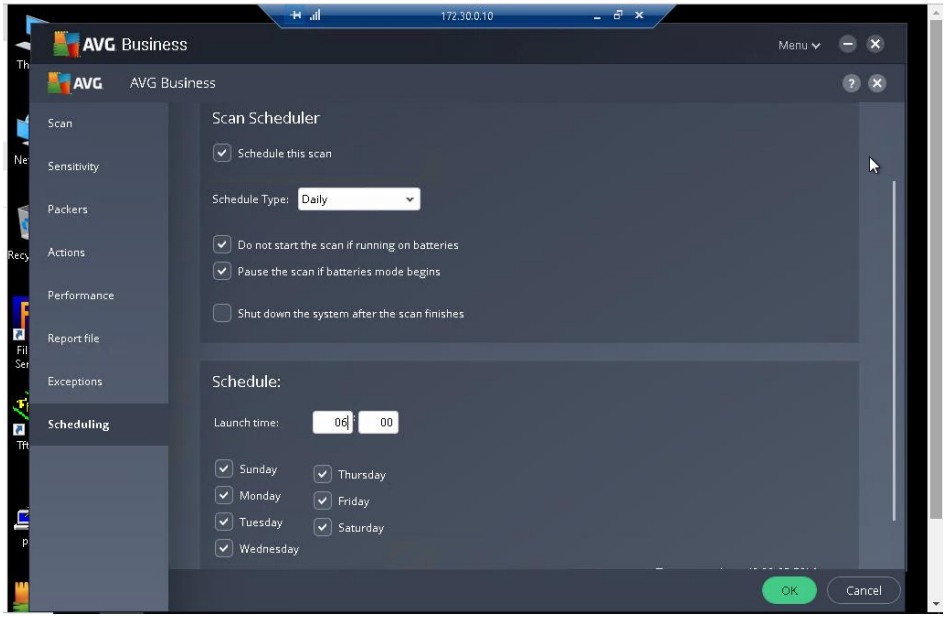
Part 2: Step 11: Pdfka-FC Details file



Part 3: Step 5: Cleared Quarantine Page

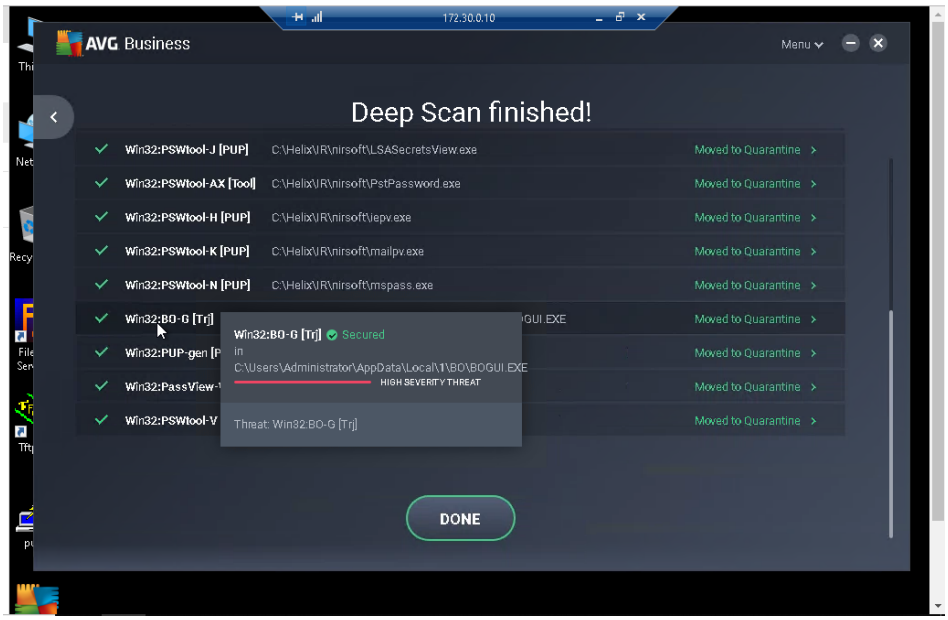


Part 3: Step 12: Scheduled Scan Page

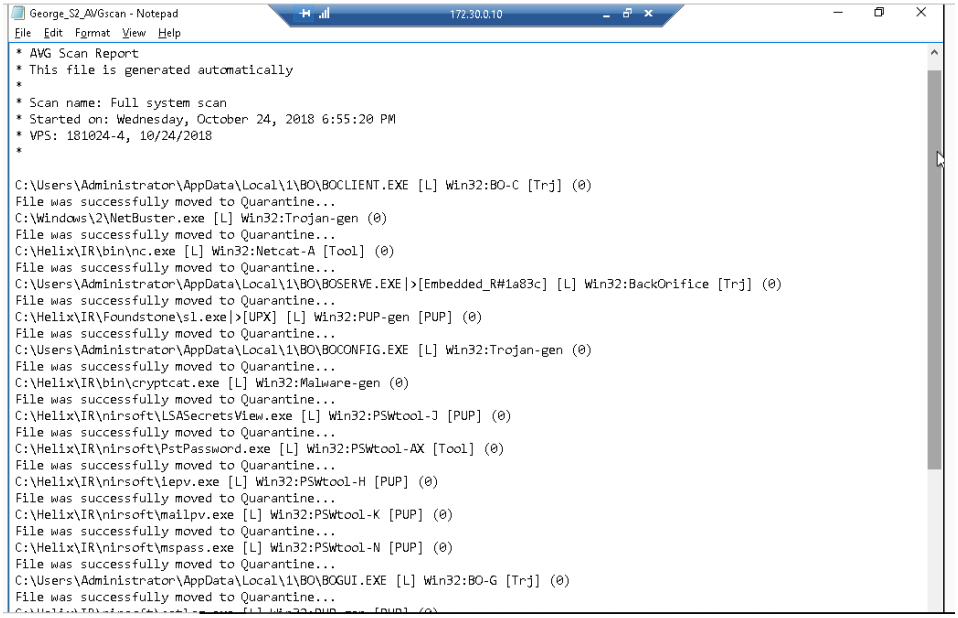


SECTION 2

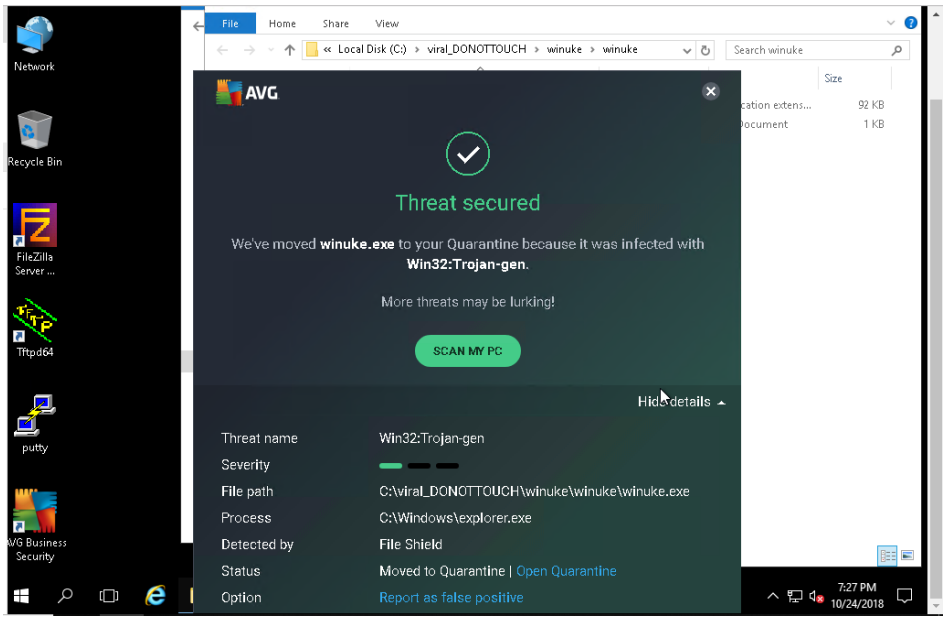
Part 1: Step 9: Details of Last High Severity Threat



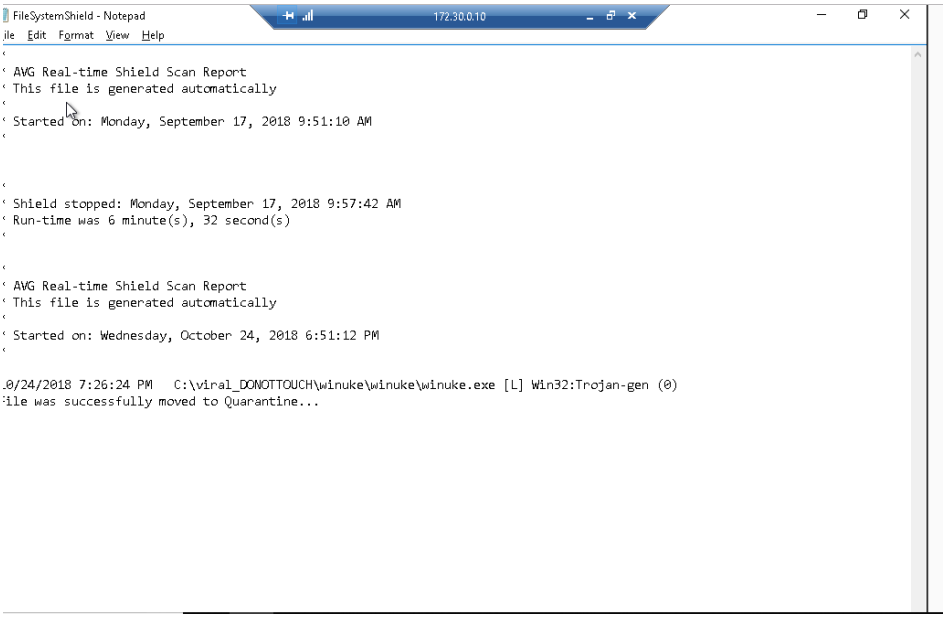
Part 1: Step 15: Contents of George_S2_AVGscan file



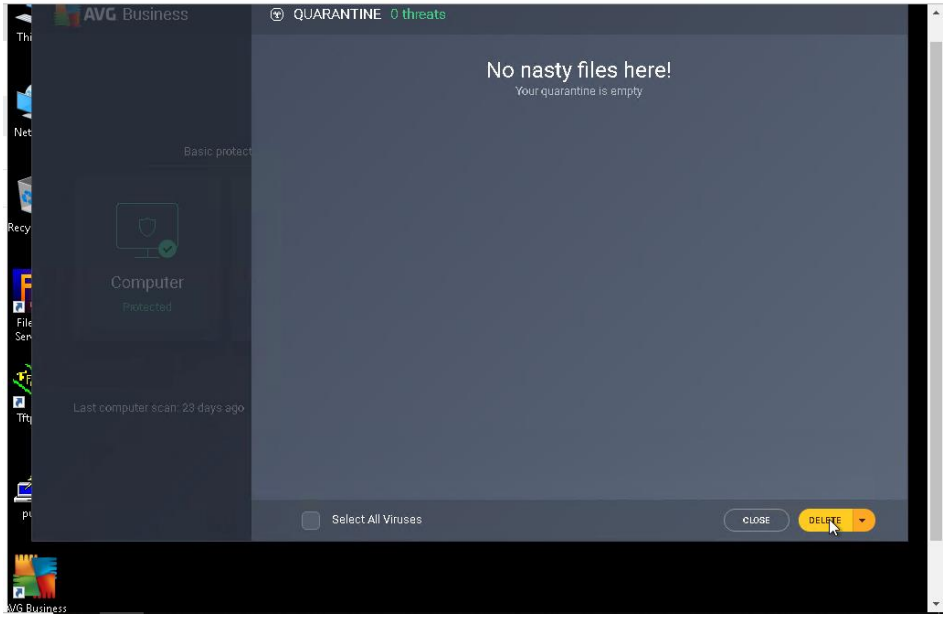
Part 2: Step 5: Win32:Trojan-gen Details



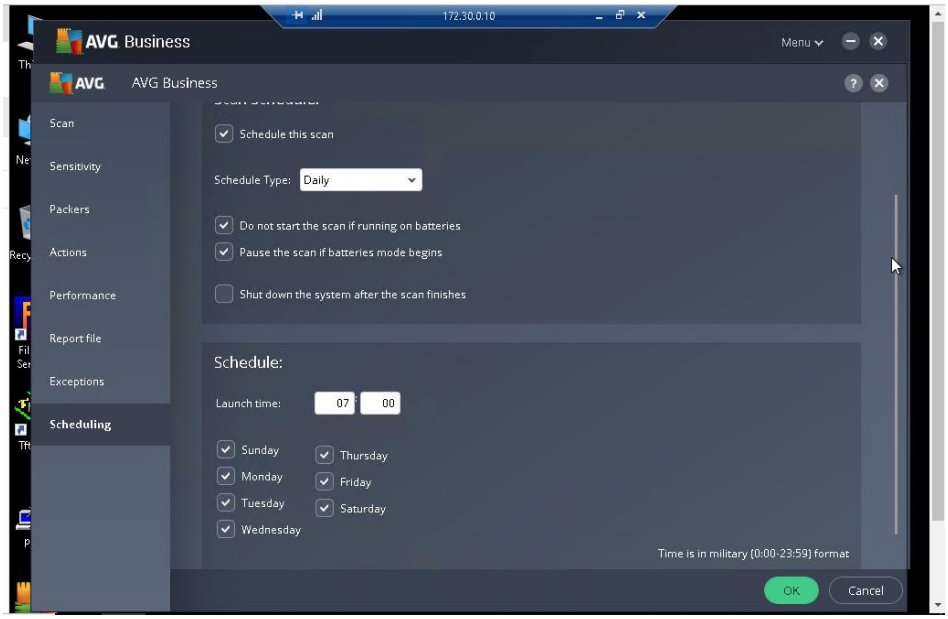
Part 2: Step 5: FileSystemShield content



Part 3: Step 3: Cleared Quarantine Page



Part 3: Step 7: Scheduled Scan Page



SECTION 3

SECTION 3 P1

WinNuke attack is a remote Denial of Service attack which mainly affected older versions of Windows system (Microsoft Windows 95, NT and Microsoft Windows 3.1x computer operating systems.). WinNuke works by sending an Out of Bound packet to port 139. Port 139 is a NetIOS datagram service (A blue screen errors in windows) that can be used to manipulate target host and its NetIOS services. WinNuke exploits the NetIOS port 139 because it does not accept packets unless the flag Out of Bound is set in the incoming packet. Although this malware is outdated, WinNuke was the first DoS widely used to crash Windows systems and utilized a single packet to crash remote machines.

The updated WinNuke malware was designed to send OOB packet to thousands of machines in a single transmission. This caused ISPs and law enforcement officials to consider containing such malware. In such attempt to contain the malware, Microsoft supplied a patch (Filtering all packets with "bewm" to ignored them) to help fix the problem. “bewn” was the WinNuke utility sent as part of the payload in the OOB. Microsoft later was able to issue a real patch that dealt with the WinNuke malwatre.

In preventing the WinNuke attack, two ways were identified. This involved installing the Microsoft patch if a user was running an older version of Windows. It’s interesting to know that Microsoft doesn’t consider WinNuke as a threat anymore hence a zero-search results output is received when keywords like “WinNuke patch” is supplied to Microsoft WinNuke Support

The second means of prevention was to run an external utility such as NukeNabber. This tool offered protection from WinNuke whiles it logged the IP Address of attempting attack and also monitored several other ports looking for several other known Denial of Service attacks.

Despite this attack being somewhat outdate and no more dangerous, knowledge of how it works and how to protect against it is important (Jericho & Mcintyre, 1999). Many Internet service providers are also constantly filtering out the packets, so they don't reach users (Rouse, n.d.).

SECTION 3 P2

The internet is a constant companion for humans in all our endeavors be it home, offices, and even myriad places. AVG is an antivirus protection software dedicated to online security and operated since 1988. AVG protects devices, data, and people – AVG (AVG Profile). The software provides Premium Technical Support, Remote Virus Removal, and Express Install. It also has protections for internet security, fileserver, business antivirus product, and even for Mac users which compatible with the OS X Mountain Lion and later releases (AVG Mac Protection).

Comparing AVG to Norton and McAfee, my ultimate choice would be the AVG antivirus product. With complete protection even to cover Mac and OS X is absolutely incredible especially when Apple claims to be robust to virus exploitation. AVG has gone the length to write an antivirus program that could detect malware in Apple products.

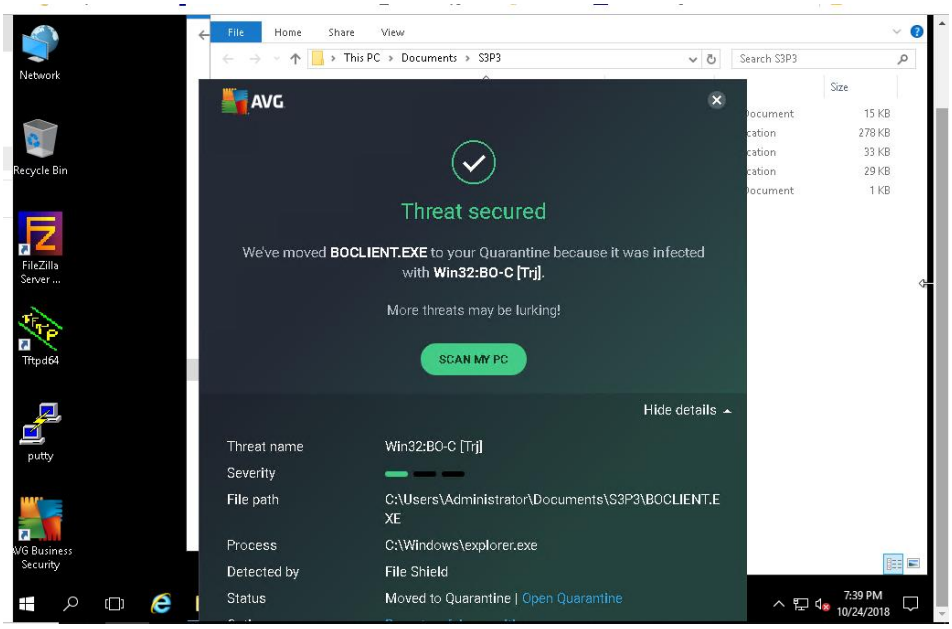
Norton operating for about 25 years focuses on protecting freedom and its explorers. The services therefore comprise reputation protection, and technology leadership. Although Norton offers antivirus protection, its services as advertised are just a breakdown of similar services (e.g. Malware and Ransomware) into different categories just to appeal to regular electronic devices users (Norton Products & Services). Norton is although expensive ($79.99 and up), it doesn't offer remote antivirus protection like AVG - $39.99 and up depending on number of devices.

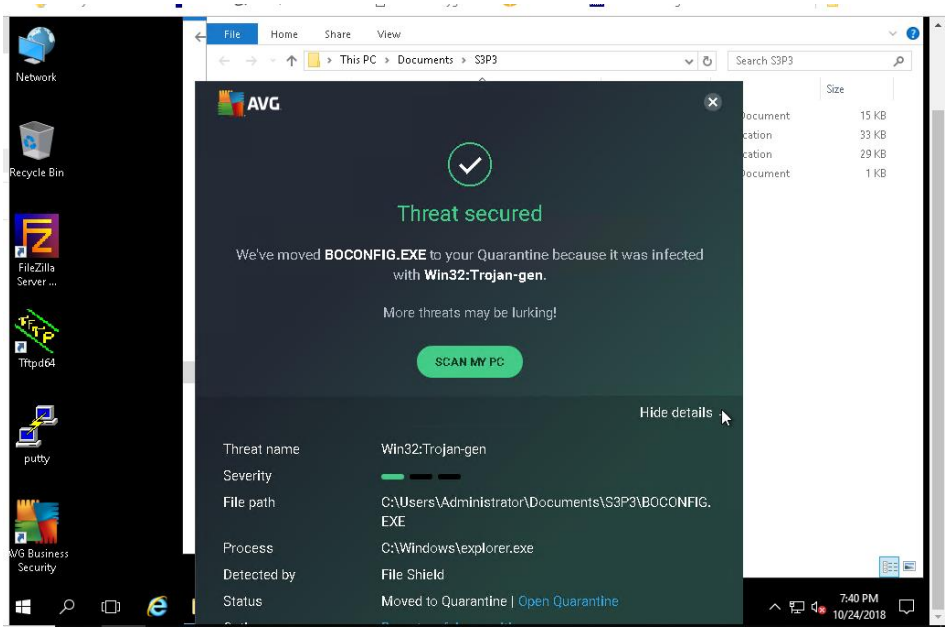
McAfee security has existed for about 30 years offers the most simple and effective means for consumers around the world to protect their data and identity as they navigate their digital lives across their connected devices and constantly analyzing and gathering data on threats from over 300 million endpoints across the globe (McAfee Protection). McAfee could be offered at $44.99 (Original pricing at $99.99) for ten devices. However, McAfee doesn't match up to AVG which has been industry acclaimed and widely used.

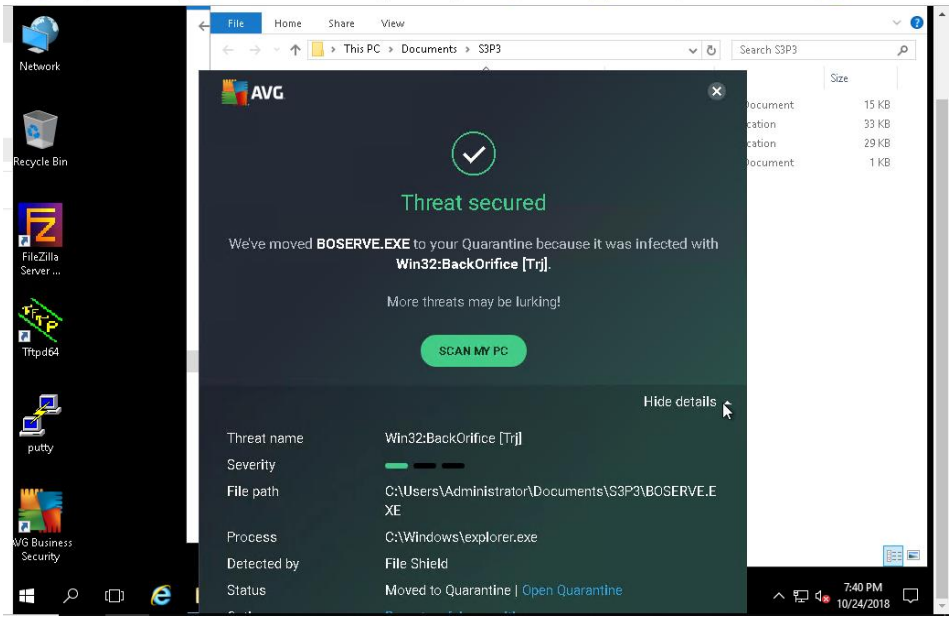
Considering the issues discussed, AVG will be my choice.

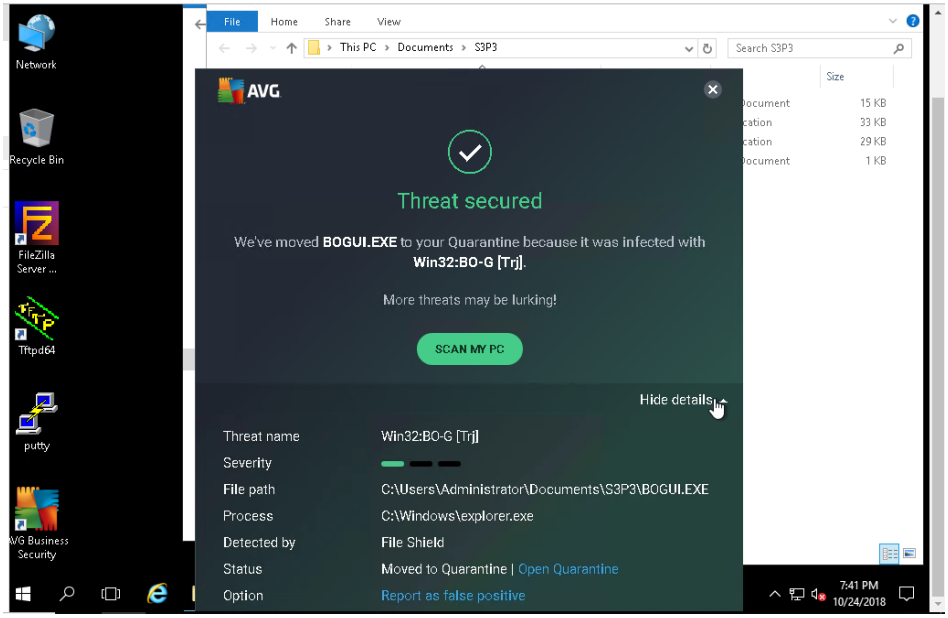
SECTION 3 P3

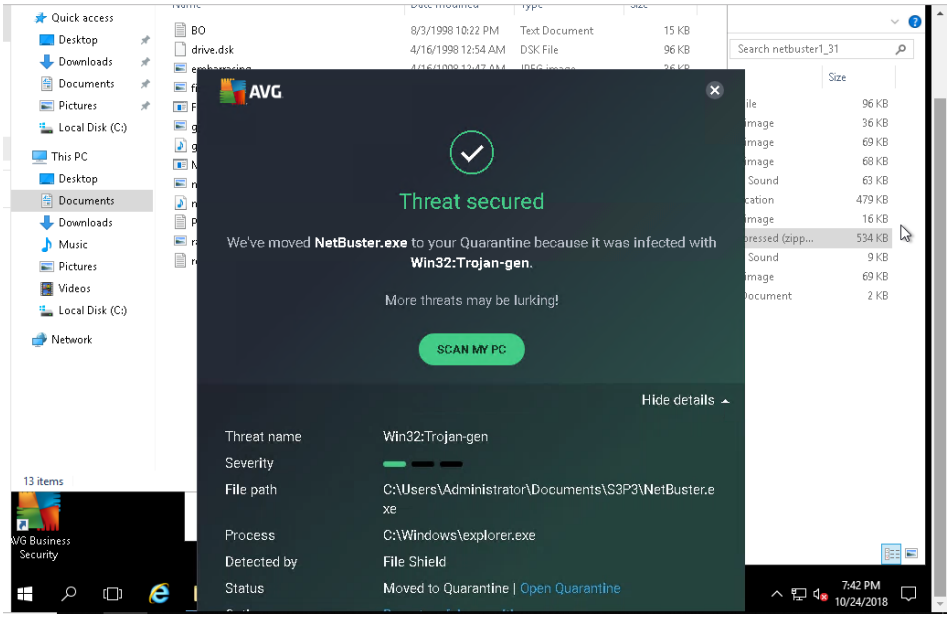
Executing the requested action in Section 3 Part 3 of the lab produced the images below. Since antivirus have no capabilities of scanning zipped folders, the AVG antivirus could not detect the following malware that were hidden in the zipped folders until the files were extracted, offering the malware chances to replicate and cause damage to the system. Since the target system (172.30.0.10) was running on old version of Windows, the Winuke malware could have dropping a remote DoS attack access.

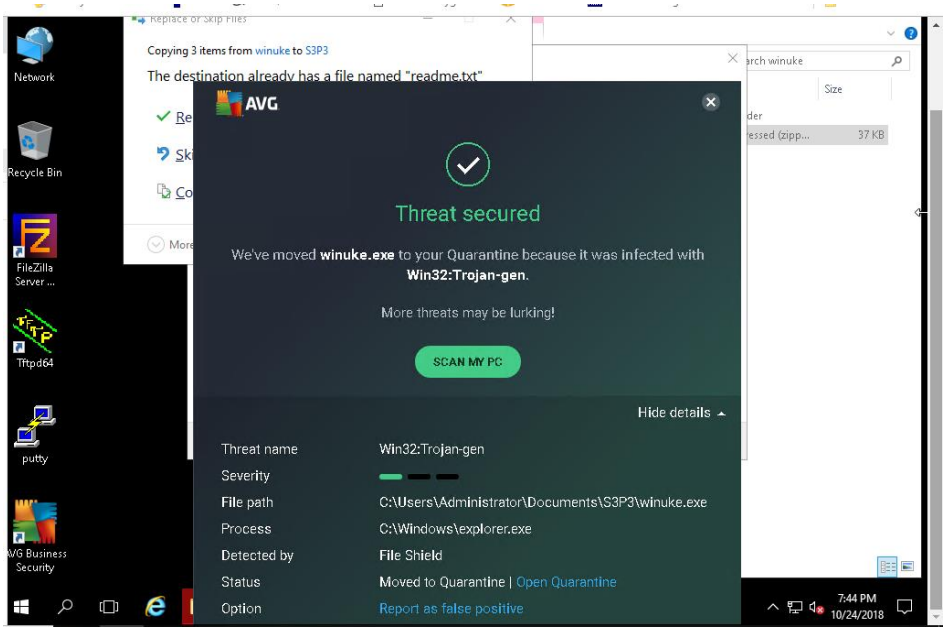



Network
Recycle Bin
FileZilla Server ...
Tftpd64
putty
AVG Business Security
File Home Share View
This PC › Documents › S3P3
Search S3P3
Size
15 KB
33 KB
29 KB
1 KB
AVG
Threat secured
We've moved BOCONFIG.EXE to your Quarantine because it was infected with Win32:Trojan-gen.
More threats may be lurking!
SCAN MY PC
Hide details
Threat name
Win32:Trojan-gen
Severity
File path
C:\Users\Administrator\Documents\S3P3\BOCONFIG.EXE
Process
C:\Windows\explorer.exe
Detected by
File Shield
Status
Moved to Quarantine | Open Quarantine
7:40 PM
10/24/2018


Network
Recycle Bin
FileZilla Server ...
Tftpd64
putty
AVG Business Security
File Home Share View
This PC › Documents › S3P3
Search S3P3
Size
15 KB
33 KB
29 KB
1 KB
AVG
Threat secured
We've moved BOSERVE.EXE to your Quarantine because it was infected with Win32:BackOrifice [Trj].
More threats may be lurking!
SCAN MY PC
Hide details
Threat name
Win32:BackOrifice [Trj]
Severity
File path
C:\Users\Administrator\Documents\S3P3\BOSERVE.EXE
Process
C:\Windows\explorer.exe
Detected by
File Shield
Status
Moved to Quarantine | Open Quarantine
7:40 PM
10/24/2018


Network
Recycle Bin
FileZilla Server ...
Tftpd64
putty
AVG Business Security
File
Home
Share
View
This PC
Documents
S3P3
Search S3P3
Size
15 KB
33 KB
29 KB
1 KB
AVG
Threat secured
We've moved BOGUI.EXE to your Quarantine because it was infected with Win32:BO-G [Trj].
More threats may be lurking!
SCAN MY PC
Hide details
Threat name
Win32:BO-G [Trj]
Severity
File path
C:\Users\Administrator\Documents\S3P3\BOGUI.EXE
Process
C:\Windows\explorer.exe
Detected by
File Shield
Status
Moved to Quarantine | Open Quarantine
Option
Report as false positive
7:41 PM
10/24/2018


Quick access
Desktop
Downloads
Documents
Pictures
Local Disk (C:)
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
13 items
BO
8/3/1998 10:22 PM
Text Document
15 KB
drive.dsk
4/16/1998 12:54 AM
DSK File
96 KB
Search netbuster1_31
Size
96 KB
36 KB
69 KB
68 KB
63 KB
479 KB
16 KB
534 KB
9 KB
69 KB
2 KB
AVG Business Security
AVG
Threat secured
We've moved NetBuster.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
File path
C:\Users\Administrator\Documents\S3P3\NetBuster.exe
Process
C:\Windows\explorer.exe
Detected by
File Shield
Status
Moved to Quarantine | Open Quarantine
7:42 PM
10/24/2018



Zip Files were extracted into C:\S3P3