Christopher Bazyani

CYB 552

Advanced Hacking Prevention

Lab 6

Identifying and Removing Malware on a Windows System

**Section 1: Hands-On Demonstration**

Part 1: Use Antivirus Software to Scan the Infected System

On the vWorkstation desktop, double-click the Connections folder.

In the Connections folder, double-click the TargetWindows02 RDP shortcut to open a remote connection to the TargetWindows02 machine.

If prompted, type the following credentials and click OK.

Username: Administrator

Password: P@ssw0rd!

The remote desktop opens with the IP address of TargetWindows02 (172.30.0.10) in the title bar at the top of the window.

On the TargetWindows02 desktop, double-click the AVG Business Security icon to open the AVG antivirus application.

When the application opens, you will also notice that the application interface includes a warning that the computer is not fully protected and that some components, specifically the Computer component, are not yet active.

On the AVG Home page, click the Fix Now button to enable the antivirus protection on all components.

Website

Description automatically generated with low confidence

Logo

Description automatically generated with medium confidence

AVG will enable the antivirus protection on the unprotected components. You will notice that the warning indicators will change from RED to GREEN when the application is ready to proceed.

For the purposes of this lab, you can disregard any notifications to update the virus definitions. In a real-world situation, you would want to ensure your virus definition files are updated on a regular basis, but they have been blocked in this lab to ensure no additional software updates are pushed out.

Note: Many new malware and viruses are detected every day, and anti-virus vendors usually update their anti-virus signature files several times per week. Updating the antivirus software with the latest virus definitions ensures the software has the latest information to identify and quarantine threats. AVG automatically updates the database on a regular basis, as long as the machine is able to reach the Internet or if there is an update server designated in the network. For the purposes of this lab, this functionality has been deactivated.

In addition to updating the database, it is also important to apply any patches to the antivirus software itself. These patches often address vulnerabilities in the application as well. For the purposes of this lab, this functionality has also been deactivated.

In the lower-right corner of the AVG interface, click the Update Signature Files button (the reverse arrow icon) to check for updates to the signature files.

A picture containing graphical user interface

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

AVG will download and install any required signature files, and confirm that the software is up-to-date.

On the AVG Home page, click the Menu icon, then select Settings from the available options to open the AVG Settings window.

Graphical user interface, application

Description automatically generated

In the AVG Settings window, click the Exceptions header to expand the AVG Exceptions list.

Graphical user interface, application

Description automatically generated

Note: The Exceptions feature of AVG enables you to remove specific files or folders from the scan. Database files and certain software packages add meta-data to a file that interferes with the antivirus program's ability to recognize the file as safe. What may be a correctly-formatted document may appear to the antivirus program as malware. To avoid this type of “false positive” finding, you may choose to exclude folders containing files that the antivirus program cannot interpret. In this case, the checked Helix folder indicates that this folder has already been excluded. You will remove that checkbox to ensure that there are no exceptions to the scan.

From the AVG Exceptions list, scroll down and select the C:\Helix\\* exception, then click the delete button to remove the exception.



In the AVG Settings window, click the OK button to close the AVG Settings window.

On the AVG Home page, click the Configuration button (the gear icon to the right of the Scan Computer button) to open the Other Scans page.

A picture containing text, hitting, screenshot, night sky

Description automatically generated

On the Other Scans page, click the Deep Scan Configuration button (the gear icon to the right of the Deep Scan button) to open the Deep Scan Configuration window.

A picture containing graphical user interface

Description automatically generated

In the Deep Scan Configuration window, click the Report File link in the navigation menu, then click the Generate report file checkbox to configure AVG to output report files.

Graphical user interface, application

Description automatically generated

In the File name field, type yourname\_S1\_AVGscan, replacing yourname with your own name, to name the report file.

In the Deep Scan Configuration window, click the OK button to apply the changes and close the window.

Graphical user interface, application, Teams

Description automatically generated

On the Other Scans page, click the Deep Scan button to begin the scanning process and remove any identified threats.

A screenshot of a computer

Description automatically generated with medium confidence

By default, AVG will scan the whole computer. This process will take approximately 15-20 minutes to complete. Do not touch any keys until the scan is finished. When the scan has completed, AVG will display the Scan Summary (previously called the Report Summary) page showing the number of threats that have been identified and removed. The number of threats is listed at the top of the Scan Summary page.

On the Scan Summary page, hover your cursor over the first threat to view additional details about the threat, including the threat severity.

Graphical user interface, text, application, chat or text message

Description automatically generated

Each threat identified by AVG is given a threat severity rating of high, medium, and low. The page also indicates whether the threat was removed (green checkmark) or not removed (red exclamation mark) from your computer.

Note: Once you have the name and details for a virus, you can use that information to search the antivirus company’s Web site or the Internet, in general, for more information about how the virus entered your network in the first place. You can take measures to protect yourself from a recurrence.

On the Scan Summary page, locate the first high severity threat.

In your Lab Report file, document the threat details.

Review the remaining high severity threats detected by AVG.

On the Scan Summary page, click the Done button to return the AVG Home page.

Minimize the AVG window.

On the TargetWindows02 taskbar, click the File Explorer icon to open a new File Explorer window.

On the File Explorer toolbar, click the View tab, then click the Hidden items checkbox.

Text

Description automatically generated with medium confidence

In the File Explorer window, navigate to C:\ProgramData\Avg\Antivirus\report to access the report generated for your AVG scan.

In the Reports folder, double-click the yourname\_S1\_AVGscan file to open the report in Notepad.

Graphical user interface, text, application, email

Description automatically generated

Make a screen capture showing the contents of the yourname\_S1\_AVGscan file and paste it into your lab report file.

Graphical user interface, text, application, email

Description automatically generated

Close the File Explorer window.

Part 2: Identify Threats in Encrypted Archive Files

From the TargetWindows02 taskbar, click the File Explorer icon to open a new File Explorer window

In the File Explorer window, navigate to the ISSA\_TOOLS folder (C:\ISSA\_TOOLS).

Graphical user interface, text, application, email

Description automatically generated

The password-protected prodrev.zip archive file has been infected with malware.

In the ISSA\_TOOLS folder, right-click the prodrev.zip file and select Extract All from the context menu.

In the Extract Compressed window, click the Extract button to unpack the zip file in the same folder.

Graphical user interface, text, application

Description automatically generated

When prompted for the password, type password123 and click OK to decrypt the zipped file and begin the unpacking process.

Graphical user interface, application

Description automatically generated

AVG, running in the background, will detect the virus within the file and display a detection warning.

In the AVG Detection window, click the See Details link to show additional details about the threat and what was done to secure it.

Graphical user interface, website

Description automatically generated

Graphical user interface, text, application

Description automatically generated

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).

Note: AVG, like other antivirus programs, cannot scan compressed files such as \*.zip files which was why the scan you conducted in Part 1 of this lab did not detect a virus. The File Shield (previously called Resident Shield) feature of AVG, however, scans every single file as it is opened, saved, or copied. Since the process runs in the background, you will never notice unless AVG identifies a threat.

Close the Threat Detection window.

In the File Explorer, the prodrev folder should be empty, verifying that AVG did indeed remove the infected file.

Close the prodrev File Explorer window.

In the ISSA\_TOOLS File Explorer window, navigate to C:\ProgramData\Avg\Antivirus\report to access the File Shield Report.

This report is automatically generated and contains information about the virus detected by the File Shield in the productreview.pdf file.

In the report folder, double-click the FileSystemShield file to open the report in Notepad.

Make a screen capture showing the Pdfka-FC threat detection in the FileSystemShield file and add it to your Lab Report file.

Graphical user interface, text, application, email

Description automatically generated

Close the Notepad window.

Close the File Explorer window.

Part 3: Manage AVG Scans and the Quarantine Area

From the TargetWindows02 taskbar, restore the AVG window.

On the AVG Home page, click the Menu icon, then select Quarantine from the available options to open the Quarantine area.

Graphical user interface, application

Description automatically generated

On the Quarantine area page, use the scrollbar to view the complete list of results. From this screen, you can select individual files to delete or restore in the case of a false positive result, or you can empty the entire contents at once.

On the Quarantine page, click the Select all viruses checkbox to select all viruses in the Quarantine area.

Graphical user interface, text

Description automatically generated

On the Quarantine page, click the Delete button to delete all viruses, malware, and malicious software detected by the application.

Make a screen capture showing the empty Quarantine area (Virus Vault) and paste it into your Lab Report file.

A screenshot of a computer

Description automatically generated with medium confidence

On the Quarantine page, click the Close button to close the Quarantine area and return to the AVG Home page.

On the AVG Home page, click the Configuration button (the gear icon to the right of the Scan Computer button) to open the Other Scans page.

On the Other Scans page, click the Deep Scan Configuration button (the gear icon to the right of the Deep Scan button) to open the Deep Scan Configuration window.

In the Deep Scan Configuration window, locate the Scheduling section and click the Schedule this scan checkbox to configure AVG to run a scheduled scan.

Graphical user interface, text

Description automatically generated

Under the Scan Scheduler header, select Daily from the Schedule Type menu.

Under the Schedule header, use the toggle buttons to set the scheduled run time to 06:00.

Make a screen capture showing the scheduled scan and paste it into your Lab Report file.

Graphical user interface, application

Description automatically generated

In the Deep Scan Configuration window, click OK to apply the changes and return to the AVG home page.

Close the AVG window.

**Section 2: Applied Learning**

Part 1: Use Antivirus Software to Scan the Infected System

Open a remote connection to the TargetWindows02 machine.

Launch the AVG Business Security application.

When the application opens, you will notice that the application interface includes a warning that the computer is not fully protected and that some components, specifically the Computer component, requires an update.

Do not update AVG itself or follow any prompts to Restart the Computer. While AVG can be updated to a newer version, newer versions of AVG may not work with the instructions in this lab guide.

Enable antivirus protection on all unprotected components.

Graphical user interface, application

Description automatically generated

Note: Many new malware and viruses are detected every day, and anti-virus vendors usually update their anti-virus signature files several times per week. Updating the antivirus software with the latest virus definitions ensures the software has the latest information to identify and quarantine threats. AVG automatically updates the database on a regular basis, as long as the machine is able to reach the Internet or if there is an update server designated in the network. For the purposes of this lab, this functionality has been deactivated.

In addition to updating the database, it is also important to apply any patches to the antivirus software itself. These patches often address vulnerabilities in the application as well. For the purposes of this lab, this functionality has also been deactivated.

Remove the following folders from the AVG Exceptions list.

C:\Windows\System32\3

C:\Windows\2\\*

C:\Users\Administrator\AppData\Local\1\\*

C:\Helix\\*

Note: The Exceptions feature of AVG enables you to remove specific files or folders from the scan. Database files and certain software packages add meta-data to a file that interferes with the antivirus program's ability to recognize the file as safe. What may be a correctly-formatted document may appear to the antivirus program as malware. To avoid this type of “false positive” finding, you may choose to exclude folders containing files that the antivirus program cannot interpret. In this case, the checked Helix folder indicates that this folder has already been excluded. You will remove that checkbox to ensure that this folder is not an exception to the scan.

Update the Deep Scan configuration to save a report file titled yourname\_S2\_AVGscan, replacing yourname with your own name.

Graphical user interface, application

Description automatically generated

Run a Deep Scan on the TargetWindows02 machine to remove any identified threats.

A screenshot of a computer

Description automatically generated with medium confidence

By default, AVG will scan the whole computer. This process will take approximately 15-20 minutes to complete. Do not touch any keys until the scan is finished. When the scan has completed, AVG will display a Scan Summary or Report Summary showing the number of threats that have been identified and removed. The number of threats is identified at the top of the summary.

When the scan is complete, review the threats that AVG detected.

Each threat identified by AVG is given a threat severity rating of high, medium, and low. The Scan Summary also indicates whether the threat was removed (green checkmark) or not removed (red exclamation mark) from your computer.

Locate the last high severity threat in the Scan Summary.

Graphical user interface, text, application

Description automatically generated

Note: Once you have the name and details for a virus, you can use that information to search the antivirus company’s website or the Internet, in general, for more information about how the virus entered your network in the first place. You can take measures to protect yourself from a recurrence.

In your Lab Report file, document the threat details.

Review the remaining high severity threats detected by AVG.

Minimize the AVG window.

In a new File Explorer window, navigate to C:\ProgramData\Avg\Antivirus\report and open the yourname\_S2\_AVGscan file.

You will need to check the Hidden files checkbox on the File Explorer View tab to reveal the ProgramData folder.

Make a screen capture showing the summary information at the top of the yourname\_S2\_AVGscan file and paste it into your Lab Report file.

Close the Notepad window.

Close the File Explorer window.

Part 2: Identify Threats in Encrypted Archive Files

Restore the AVG window, then remove the following object from the Exceptions list and apply the changes.

C:\viral\_DONOTTOUCH\\*

Minimize the AVG window, then open a new File Explorer window and navigate to the Winuke folder (C:\Viral\_DONOTTOUCH\winuke).

Extract all files in the winuke.zip archive into the C:\Viral\_DONOTTOUCH\winuke folder.

Graphical user interface, application

Description automatically generated

AVG, still running in the background, will detect the virus within the file and display an alert message.

Click the See details link at the bottom of the AVG Detection window.

A picture containing text, screenshot, electronics, computer

Description automatically generated

Note: AVG, like other antivirus programs, cannot scan compressed files such as \*.zip files. Unlike the whole computer scan, which did not detect a virus in this folder, the Resident Shield feature of AVG scans every single file as it is opened, saved, or copied. Since the process runs in the background, you will never notice unless AVG identifies a threat.

Make a screen capture showing the threat details and paste it into the Lab Report file.

Graphical user interface, text

Description automatically generated

Close the AVG Detection message.

Navigate to C:\ProgramData\Avg\Antivirus\report and open the FileSystemShield file.

Make a screen capture of the contents of FileSystemShield file and paste it into your Lab Report file.

Close the Notepad window, then restore the AVG window.

Part 3: Manage AVG Scans and the Quarantine Area

Open the Quarantine area.

Use the scrollbar to view the complete list of results. From this screen, you can select individual files to delete or restore in the case of a false positive result, or you can empty the entire contents at once.

Empty the Quarantine area to delete all viruses, malware, and malicious software detected by the application.

Graphical user interface, text, application

Description automatically generated

Make a screen capture showing the empty Quarantine area (Virus Vault) and paste it into your Lab Report file.

Graphical user interface, website

Description automatically generated

Close the Quarantine area and return to the AVG Home page

In the next steps, you will schedule a scan to run daily.

Open the Deep Scan Configuration settings.

Enable a scheduled scan that will run every day at 7:00 AM.

Make a screen capture showing the scheduled scan and paste it into your Lab Report file.

Graphical user interface, application, Teams

Description automatically generated

Apply the changes and close any open windows.