Week 10 - Network Security

Project 3-1: Analyze File and URL for File-Based Viruses Using VirusTotal-Part 1

Time Required: 25 minutes

Objective: Given a scenario, analyze potential indicators to determine the type of attack.

Description: VirusTotal is a free online service that analyzes files and URLs to identify potential malware. VirusTotal combines 70 antivirus scanners and URUdomain blacklisting services along with other tools to identify malware.
A wide range of files can be submitted to VirusTotal for examination, such as user data files and documents, executable programs, PDFs, and images. One of the uses of VirusTotal is to provide a "second opinion" on a file or URL that may have been flagged as suspicious by other scanning software. In this project, you use VirusTotal to scan a file and a URL.

1. First view several viruses from 20 years ago and observe their benign but annoying impact. Open your web browser and enter the URL **archive.org/details/malwaremuseum&tab=collection** (if you are no longer able to access the site through the web address, use a search engine to search for "Malware Museum").
2. All of the viruses have been rendered ineffective and will not harm a computer . Click several of the viruses and notice what they do.
3. When finished, close your web browser.
4. Use Microsoft Word to create a document that contains the preceding paragraph description about VirusTotal. Save the document as **VirusTotal.docx.**
5. Exit Word.
6. Open your web browser and enter the URL **www.virustotal.com** (if you are no longer able to access the site through the web address, use a search engine to search for "Virus Total").
7. If necessary, click the **File** tab.
8. Click **Choose File.**
9. Navigate to the location of **VirusTotal.docx** and click **Open.**
10. Click **Confirm upload.**
11. Wait until the upload and analysis arecompleted.
12. Scroll through the list of antivirus (AV) vendors that have been polled regarding this file. A green checkmark means no malware was detected.
13. Click the **DETAILS** tab and read through the analysis.
14. Use your browser's Back button to return to the VirusTotal home page.
15. Now you will analyze a website. Click **URL.**
16. Enter the URL of your school, place of employment, or another site with which you are familiar.
17. Wait until the analysis iscompleted.
18. Click the **DETAILS** tab and read through the analysis.
19. Click Scroll through the list of vendor analysis. Do any of these sites indicate **Unrated site or Malware site?**
20. How could VirusTotal be useful to users? How could it be useful to security researchers? Could it also be used by attackers to test their own malware before distributing it to ensure that it does not trigger an AV alert? What should be the protections against this?
21. Close all windows.

Project 3-2: Analyze Virus File Using VirusTotal-Part 2

Time Required: 20 minutes

Objective: Given a scenario, analyze potential indicators to determine the type of att ack.

Description: What happens when VirusTotal detects a file-based virus? In this project, you will download a file that has a "signature" of a file-based virus into a sandbox in order to upload it to VirusTotal.

1. Open your web browser.
2. Enter the URL **www.eicar.orgnpage_id=3950.**
3. Scroll down to **Download area using the standard protocol http.**
4. Click **eicar.com** to start the download.
5. Your antimalware software on your personal computer should immediately flag this file as malicious and not allow you to download it. Because it cannot (and should not) be downloaded on your regular computer, you will instead want to use the Windows Sandbox or VMware sandbox you created in Module 1.
6. If you are using the Windows Sandbox, click **Start,** scroll down to Windows Sandbox, and then click **Windows Sandbox.**
7. First you will turn off the security protections in Windows Sandb ox. Click **Start** and then **Windows Security.**
8. Click the three horizontal lines at the left of the screen to display the menu options.

9. Click **App & browser control.**
10. For each of the categories, click the **Off** button to turn off security. Remember this will only impact the security within the Windows Sandbox and will have no impact on the underlying computer.
11. Open Internet Explorer in the Windows Sandbox.
12. Enter the URL **www.eicar.orgnpage_id=3950.**
13. Scroll down to **Download area using the standard protocol http.**
14. Click **eicar.com** to start the download.
15. The antimalware software within Windows Sandbox will now allow the file to be downloaded into the Sandbox.
16. Open another tab on the Internet Explorer web browser in the Windows Sandbox, and enter the URL **www.virustotal.com** (if you are no longer able to access the site through the web address, use a search engine to search for 'Virus Total',.
17. If necessary, click the **File** tab.
18. Click **Choose File.**
19. Navigate to the location of **eicar.com** and click **Open.**
20. Click **Confirm upload.**
21. Wait until the upload and analysis are completed .
22. Scroll through the list of AV vendors that have been polled regarding this file. A green checkmark means no malware was detected.
23. Click the **DETAILS** tab and read through the analysis.
24. Close the Windows Sandbox. This will delete the **eicar.com** file and reset the security settings to normal.

Project 3-3: Explore Ransomware Sites

Time Required: 15 minutes

Objective: Given a scenario, analyze potential indicators to determine the type of attack.

Description: A variety of sites provide information about ransomware along with tools for counteracting some types of infection. In this project, you explore different ransomware sites.

1. Open your web browser and enter the URL **www.nomoreransom.org** (if you are not able to access this site open a search engine and search for **"Nomoreransom.org").**
2. Click the **No** button.
3. Read through the Prevention Advice. Do you think it is helpful?
4. Click **Crypto Sheriff.** How could this be useful to a user who has suffered a ransomware infection?
5. Click **Ransomware: Q&A.** Read through the information. Which statements would you agree with? Which statements would you disagree with?
6. Click **Decryption Tools.** This contains a list of different tools that may help restore a computer that has been infected by a specific type of ransomware.
7. Click one of the tools and then click **Download** to download. Note that these tools change frequently based on the latest types of ransomware that is circulating.
8. Run the program to understand how these decryption tools function. Note that you will not be able to complete the process because there are no encrypted files on the computer. Close the program.
9. Now visit another site that provides ransomware information and tools. Open your web browser and enter the URL **id-ransomware.malwarehunterteam.com.**
10. What features does this site provide?
11. How could these sites be useful?
12. Close all windows.

Project 3-4: Use a Software Keylogger

The purpose of this activity is to provide information regarding how these programs function in order that adequate defenses can be designed and implemented. These programs should never be used in a malicious fashion against another user.

Time Required: 25 minutes

Objective: Given a scenario, analyze potential indicators to determine the type of att ack.

Description: A keylogger program captures everything that a user enters on a computer keyboard. In this project, you download and use a software keylogger.

1. Open your web browser and enter the URL **refog.com** (if you are no longer able to access the program through the URL, use a search engine to search for "Refog Keylogger").

2. Click **Features** to see the features of the product.
3. Click **Home.**
4. Click **Download.**
5. Click **Create an account** and enter the requested information.
6. Click **Download.**
7. When the file finishes downloading, run the installation program. Note that you may have to enter the password on the previous page to extract the files.
8. When prompted with **I'm going to use this software to monitor:** select **My own computer.**
9. Click **Hide program icon from Windows tray.** Click **Next.**
10. Click I **Agree.**
11. Click **Select All** and then **Next.**
12. Create a login and password for the online dashboard. Click **Activate.**
13. You will receive a message that the subscription has expired. Click **Yes** to install in offline mode.
14. Click **Install.**
15. Click **Restart Now.**
16. After the computer has restarted, use the keystroke combination **Ctrl + Alt + Shift + K** to launch Refog Keylogger.
17. Click **Tools** and then click **Settings.**
18. Note the default settings regarding what is captured.
19. Click **Back to log.**
20. Minimize Refog Keylogger.
21. Use your computer normally by opening a web browser to surf to a website. Open Microsoft Word and type several sentences. Open and close several programs on the computer.
22. Maximize Keylogger and note the information that was captured.
23. In the left pane, click through the different items that were captured.
24. Under Settings, click **Websites Visited.**
25. Under Websites Visited, click **Make website screenshots.**
26. Click **Apply.**

References:

Ciampa, M., & Computing Technology Industry Association. (2020). *CompTIA security+ guide to network security fundamentals.* (7th ed.). Boston, MA: Cengage Learning.