Logo

Description automatically generated

Digital Forensics Lab 03

Project 1: Analysing Files and URLs for Viruses Using VirusTotal

VirusTotal, a subsidiary of Google, is a free online service that analyses files and URLs to

identify potential malware. VirusTotal scans and detects any type of binary content, including a Windows executable program, Android, PDFs, and images.

VirusTotal is designed 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. Click several of the viruses and notice what they do (all of the viruses have been

rendered ineffective and will not harm a computer).

3. When finished close your web browser.

4. Use Microsoft Word to create a document that contains the above paragraph about

VirusTotal. Save the document as VirusTotal.docx.

5. Now save this document as a PDF. Click File and Save As.

6. Under Save as type: select PDF (\*.pdf).

7. Save this file as YourName-VirusTotal.pdf.

8. Exit Word.

9. 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”).

10. If necessary, click the File tab.

11. Click Choose File.

12. Navigate to the location of YourName-VirusTotal.pdf and click Open.

13. Click Scan it!

14. If the File already analysed dialog box opens, click Reanalyse.

15. Wait until the analysis is completed.

16. Scroll through the list of AV vendors that have been polled regarding this file. A green

checkmark means no malware was detected.

Note

*If you are concerned about installing any of the software in these projects on your*

*regular computer, you can instead install the software in the Windows virtual*

*machine within the virtual machine will not impact the host computer.*

17. Click the File detail tab and read through the analysis.

18. Use your browser’s back button to return to the VirusTotal home page.

19. Click URL.

20. Enter the URL of your school, place of employment, or another site with which you are

familiar.

21. Click Scan it! If the URL already analysed dialog box opens, click Reanalyse.

22. Wait until the analysis is completed.

23. Scroll through the list of vendor analysis. Do any of these sites indicate Unrate site or

Malware site?

24. Click Additional information.

25. 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?

26. Close all windows.

Project 2: Write-Protecting a USB Flash Drive and Disabling a USB Port

Viruses and other malware are often spread from one computer to another by infected USB

flash drives. This can be controlled by either disabling the USB port or by write-protecting the drive so that no malware can be copied to it.

Disabling the port can be accomplished through changing a Windows registry setting, while write-protecting the drive can be done through third-party software that can control USB device permissions.

In this project, you download and install a software-based USB write blocker to prevent data from being written to a USB device and disable the USB port. You will need a USB flash drive for this project.

1. Open your web browser and enter the URL www.irongeek.com/i.php?page=security

/thumbscrew-software-usb-write-blocker (if you are no longer able to access the

program through the URL, use a search engine to search for “Irongeek Thumbscrew”).

2. Click Download Thumbscrew.

3. If the File Download dialog box appears, click Save and follow the instructions to save

this file in a location such as your desktop or a folder designated by your instructor.

4. When the file finishes downloading, extract the files in a location such as your desktop

or a folder designated by your instructor. Navigate to that location and double-click

thumbscrew.exe and follow the default installation procedures.

5. After installation, notice that a new icon appears in the system tray in the lower right

corner of the screen.

6. Insert a USB flash drive into the computer.

7. Navigate to a document on the computer.

8. Right-click the document and then select Send to.

9. Click the appropriate Removable Disk icon of the USB flash drive to copy the file to the

flash drive.

10. Now make the USB flash drive write protected so it cannot be written to. Click the icon

in the system tray.

11. Click Make USB Read Only. Notice that a red circle now appears over the icon to

indicate that the flash drive is write protected.

12. Navigate to a document on the computer.

13. Right-click the document and then select Send to.

14. Click the appropriate Removable Disk icon of the USB flash drive to copy the file to the

flash drive. What happens?

15. Click the icon in the system tray to change the permissions so that the USB drive is no

longer read only.

16. Now disable the USB port entirely. First remove the flash drive from the USB port.

17. In the Windows Run dialog box enter regedit.

18. In the left pane double-click HKEY\_LOCAL\_MACHINE to expand it.

19. Double-click SYSTEM.

20. Double-click ControlSet001.

21. Double-click Services.

22. Double-click USBSTOR as shown in Figure 2-12.

Figure 2-12 Windows Registry Editor

Graphical user interface, text, application, email

Description automatically generated

23. In the right pane double-click Start.

24. In Value data: change the number of 3 to 4. Be sure that Hexadecimal under Base is

selected.

25. Click OK.

26. Now insert a USB flash drive into the USB port. What happens?

27. To reactivate the port, change the Value data: back to 3 and click OK.

28. Close all windows.