# Week 3 task 3.1P

Task 1

a) Explain in your own words about ‘Dyre’ malware.

- The very sophisticated malware known as “Dyre” was created with the express purpose of breaking into computer systems and primarily targeting users who used online banking services. After being placed on a victim’s computer, Dyre functioned covertly and frequently eluded detection by conventional antivirus software. Usually, it used a variety of strategies, such phishing emails or malicious websites, to deceive users into unintentionally downloading and running the virus.
- After being installed, Dyre would record and intercept private data that users entered into banking websites, including account number, login credentials, and personal identity information. Cybercriminals then used this stolen data to send it to distant computers under their control so they could use it for identity theft and other illegal activities that could result in financial benefit.

b) What is a `polymorphic’ virus and why Dyre is a polymorphic virus?

- Malware that is capable of altering its look or code whenever it infects a new file or system is known as a “polymorphic” virus. Because of its capacity for mutation, antivirus software finds it difficult to accurately identify and remove the infection. The polymorphic features of the Dyre malware helped make it resistant to conventional security methods.
- Dyre may avoid detection by antivirus tools that used static signatures or patterns or identify malicious software by continuously altering its code or structure. Dyre’s capacity to adapt allowed him to carry out his harmful operations and infect systems repeatedly, endangering both people and companies.

c) What type of malware is Dyre?

- One classifies the Dyre malware as a Trojan. When attachments with the dangerous Trojan are emailed to victims directly via spear-fishing techniques. As soon as the receivers select the attachment. The system is infected with the Dyre Malware.

d) What is Dyre’s payload? What threat does it pose to a victim?

- The main malicious components in Dyre’s payload were those meant to steal sensitive data, including financial information and banking passwords. The primary risks that dyre presents to its victims are as follows:
  - ✓ Information Theft
  - ✓ Credential Harvesting
  - ✓ Financial Fraud
  - ✓ Identity Theft

## Task 2

a) What is a `Hexadecimal’

- A ”Hexadecimal” is a 16- digit number system that represents values ranging from 0 to 15. Its main applications are in networking and computing.

b) What does the `MZ header’ indicate?

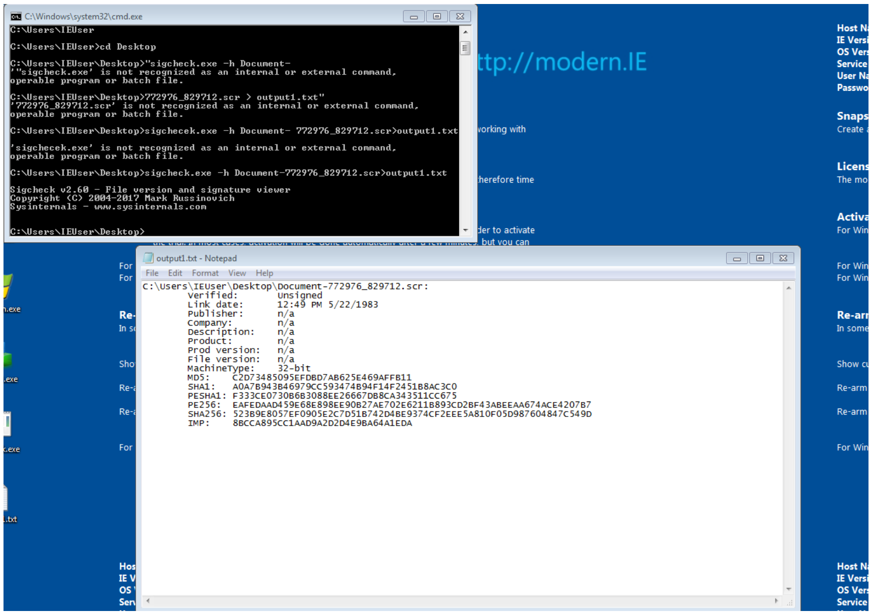
- In the Windows and DOS operating systems, executable files start with a data structure called the “MZ header.” It bears the name mark Zbikowski in Honor of one of the DOS developers. Executable files are recognized and validated using the MZ header. Usually, it is composed of a fixed-length structure that holds data like the executable’s size, the first instruction pointer, and the signature “MZ” which indicates that the file is in the executable format.

## Task 3

a) What does the command `sigcheck.exe’ do?

- A command-line tool called “Sigcheck.exe” was created by Sysinternals, a company that is now a division of Microsoft. Verifying file signatures on files like executables, drivers, and DLLs, is its main function. Among its many functions, This program can determine whether a file has been digitally signed, show comprehensive information regarding digital signatures, and software developers frequently utilize it to guarantee the authenticity and integrity of files on Windows systems.

b) Include a screenshot of the content of “output1.txt” file on Windows 7 VM Desktop – hint: you can use your host OS screenshot tools to capture.



```
C:\Users\IEUser

C:\Users\IEUser>cd Desktop

C:\Users\IEUser\Desktop>"sigcheck.exe -h Document-
'"sigcheck.exe' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\IEUser\Desktop>772976_829712.scr > output1.txt"
'772976_829712.scr' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\IEUser\Desktop>sigchecek.exe -h Document- 772976_829712.scr>output1.txt

'sigchecek.exe' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\IEUser\Desktop>sigcheck.exe -h Document-772976_829712.scr>output1.txt

Sigcheck v2.60 - File version and signature viewer
Copyright (C) 2004-2017 Mark Russinovich
Sysinternals - www.sysinternals.com


C:\Users\IEUser\Desktop>
```

```
C:\Users\IEUser\Desktop\Document-772976_829712.scr:
        Verified:       Unsigned
        Link date:      12:49 PM 5/22/1983
        Publisher:      n/a
        Company:        n/a
        Description:    n/a
        Product:        n/a
        Prod version:   n/a
        File version:   n/a
        MachineType:    32-bit
        MD5:    C2D73485095EFDBD7AB625E469AFFB11
        SHA1:   A0A7B943B46979CC593474B94F14F2451B8AC3C0
        PESHA1: F333CE0730B6B3088EE26667DB8CA343511CC675
        PE256:  EAFEDAAD459E68E898EE90B27AE702E6211B893CD2BF43ABEEAA674ACE4207B7
        SHA256: 523B9E8057EF0905E2C7D51B742D4BE9374CF2EEE5A810F05D987604847C549D
        IMP:    8BCCA895CC1AAD9A2D2D4E9BA64A1EDA
```

Task 4

a) Why a second process is added by `Dyre'?
   - In order to accomplish process hollowing, a method for avoiding detection and complicating analysis, the Dyre virus introduces a second process. Process hollowing is a technique whereby Dyre first establishes a valid process in a suspended state, after which malicious code takes over the legitimate process's memory. This enables the malware to operate in the shadow of a genuine process, evading detection by security software that may be keeping an eye out for unusual activity.

b) What does it aim to accomplish?
   - The Dyre malware uses process hollowing and the addition of a second process to achieve a number of goals;
     - ✓ Evasion of detection: Dyre can avoid being discovered by security solutions that depend on identifying suspicious processes by executing malicious code inside the framework of a genuine process.
     - ✓ Persistence: This method aids in the malware's continued presence on the compromised machine. Because the malicious code is injected into what seems to be a legal process, security defenses are less likely to detect it and terminate it
     - ✓ Privilege Escalation: the malicious code can run with elevated rights if the genuine process that is hollowed out has higher privileges.

Task 5

a) What is the path where googleupdaterr.exe is stored?
   - "C:\Users\IEUser\AppData\Local\googleupdaterr.exe"

b) How does this hash stored in output2.txt compare with the hash stored in output1.txt what does the comparison indicate?
   - Although output1.txt mentions the digital footprint, output2.text states that no matching files were discovered.

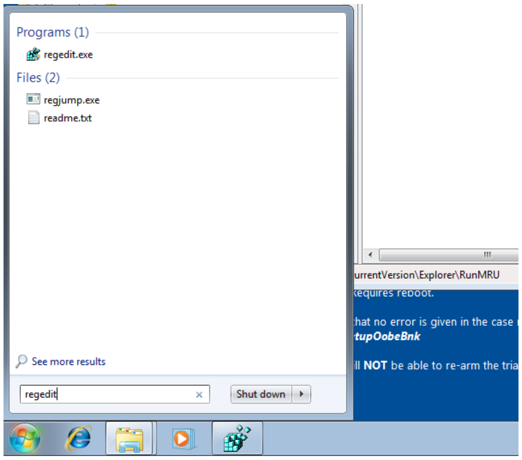
Task 6

a) What is `Windows Registry? What is it used for?

- Applications that choose to use the registry as well as configuration settings and options for the Windows operating system are kept in a hierarchical database called the Windows Registry. It includes settings and data for the majority of non-operating system applications, hardware, and operating system software.
- The Windows registry has a number of important applications, some of which include;

  - ✓ Configuration: It houses the operating system and application configuration parameters. This covers user preferences, system settings, hardware settings, and more.
  - ✓ The System Information section contains details about the hardware, installed software, device drivers, and system resources of the computer.
  - ✓ Customization: To alter the way the operating system and installed software behave, users and applications can change registry settings.
  - ✓ System Optimization: To improve system speed or fix problems, advanced users and system administrators can adjust registry settings.
  - ✓ Application Settings: The registry is where a lot of programs keep their configurations and settings. They are able to maintain user settings and preferences between sessions as a result.

b) How do you open Windows Registry in Windows 7 VM? Include screenshot of accessing the Windows Registry.



regedit

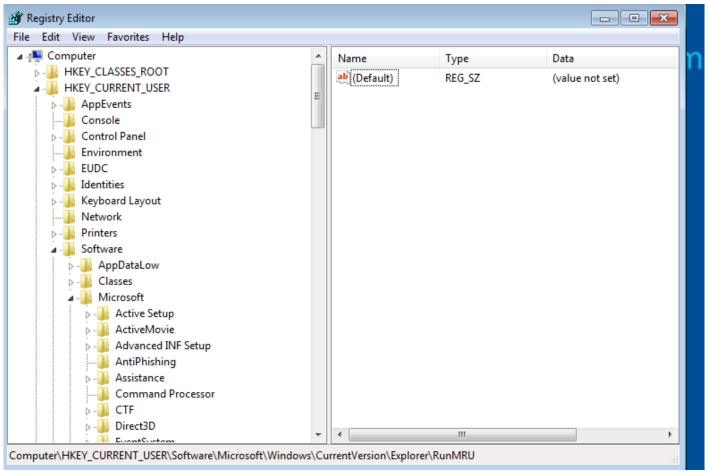
urrentVersion\Explorer\RunMRU

equires reboot.

hat no error is given in the case

tupOobeBnk

ll **NOT** be able to re-arm the tria



| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

c) The malware analysis you tried in this task was `Static' or `Dynamic' – justify with reference to Week 2's lecture.
    - We have to run the Dyre malware for this task in order to monitor its behavior with tools like Process Monitor and Regshot. You can keep an eye on the modifications made during the malware's operation with these tools. This challenge also forced us to use a hex editor to examine the malware's code without running it. As a result, we can state that it combines both dynamic and static

Task 7

a) The ransomware attack covered in the article makes use of a cutting-edge method to avoid being discovered by conventional security measures. On the victim's computer, the attackers set up a virtual machine and use this controlled environment to run the ransomware. By doing this, the ransomware works without the host computer's security software noticing it and may not check what happens inside the virtual machine. This technique makes the ransomware a complex and difficult threat to counter since it enables it to encrypt the victim's files without interruption.

b) Reflection: Write a paragraph (100-200 words) summarizing what you learned in this week's task. How did task 3.1P complement the lecture content in Week 2?
    - I learned how to analyze malware practically this week, which was a great supplement to the academic material we studied in class. The practical exercises comprised configuring a virtual computer, executing malware securely, and analyzing the Dyre malware's activity with tools like Process Monitor, Sigcheck, and Regshot. My comprehension of important ideas, such as the distinction between static and dynamic analysis, the significance of isolating malware in a controlled environment, and the particular methods malware uses to penetrate and modify system resources, was strengthened by this hands-on approach.
    - I gained knowledge about the polymorphic nature of the Dyre malware, how it starts new processes, and the kind of payload it delivers by dissecting it. Hex editors and process monitoring tools were used to gain insight into the malware's low-level actions. Furthermore, the comparison of registry modifications made prior to and following malware execution using Regshot demonstrated how malware can modify system settings in order to remain persistent or inflict harm.
      Overall, this exercise demonstrated the value of a careful and rigorous approach to cybersecurity malware analysis. It underlined the importance of being watchful and having the skills necessary to identify and evaluate hostile activity using a variety of tools and procedures.