

## Malware Analysis: Task 2.1P

Name of Student

Institutional Affiliation

## **Question 1**

**Investigate about 'Dyre' malware and answer the questions**

**a. When was this malware first identified?**

First discovered by researchers in June 2014.

**b. What is a 'polymorphic' virus and why Dyre is a polymorphic virus?**

Polymorphic viruses are complex file infectors that can create modified versions of itself to avoid detection yet retain the same basic routines after every infection. To vary their physical file makeup during each infection, polymorphic viruses encrypt their codes and use different encryption keys every time.

Once Dyre infects a host machine, it replicates and sends itself out to everyone in your contact list. Anyone that gets infected in turn sends out an entirely new variant.

**c. What type of malware is Dyre? (Hint: refer to Week 2 lecture)**

Dyre is a banking Trojan that targets Windows computers and can steal banking and other credentials by attacking all three major web browsers.

**d. What is Dyre's payload? What threat does it pose to a victim?**

The Dyre malware is packed and obfuscated in multiple layers, and it is divided into two modules: the dropper and the main DLL module. The DLL module is stored in two distinct resources named payload32 and payload64, which Dyre activates on 32-bit or 64-bit Windows platforms, respectively.

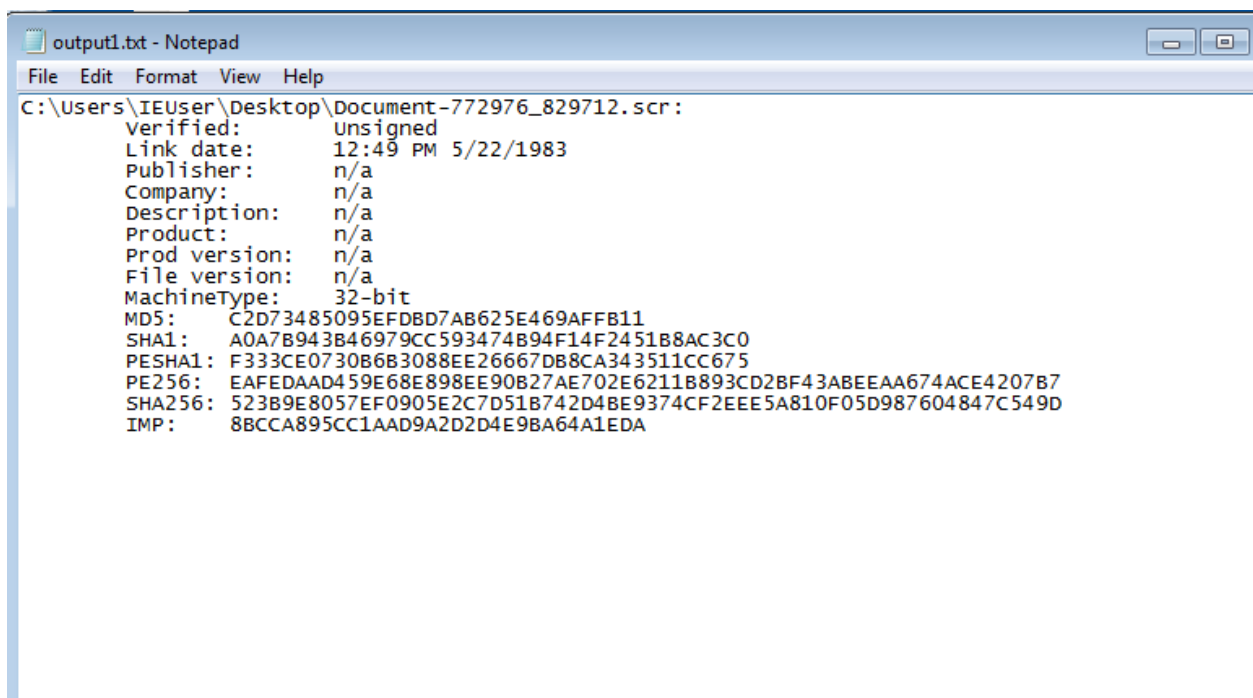
Once the infected attachment is opened, the Trojan is installed onto the user's machine and then uses web injects to insert objects such as log-in error messages onto pages and intercept banking credentials and other sensitive information that is keyed in.

### Question 3

#### a. What does the command `sigcheck.exe` do?

Sigcheck is a command-line utility that shows file version number, timestamp information, and digital signature details, including certificate chains.

#### b. Include a screenshot of the content of "output1.txt" file on Windows 7 VM Desktop



```
output1.txt - Notepad
File Edit Format View Help
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:     A0A7B943B46979CC593474894F14F245188AC3C0
PESHA1:   F333CE0730B6B3088EE26667DB8CA343511CC675
PE256:    EAFEDAAD459E68E898EE90B27AE702E6211B893CD2BF43ABEEAA674ACE4207B7
SHA256:   523B9E8057EF0905E2C7D51B742D4BE9374CF2EEE5A810F05D987604847C549D
IMP:      8BCCA895CC1AAD9A2D2D4E9BA64A1EDA
```

#### Question 4:

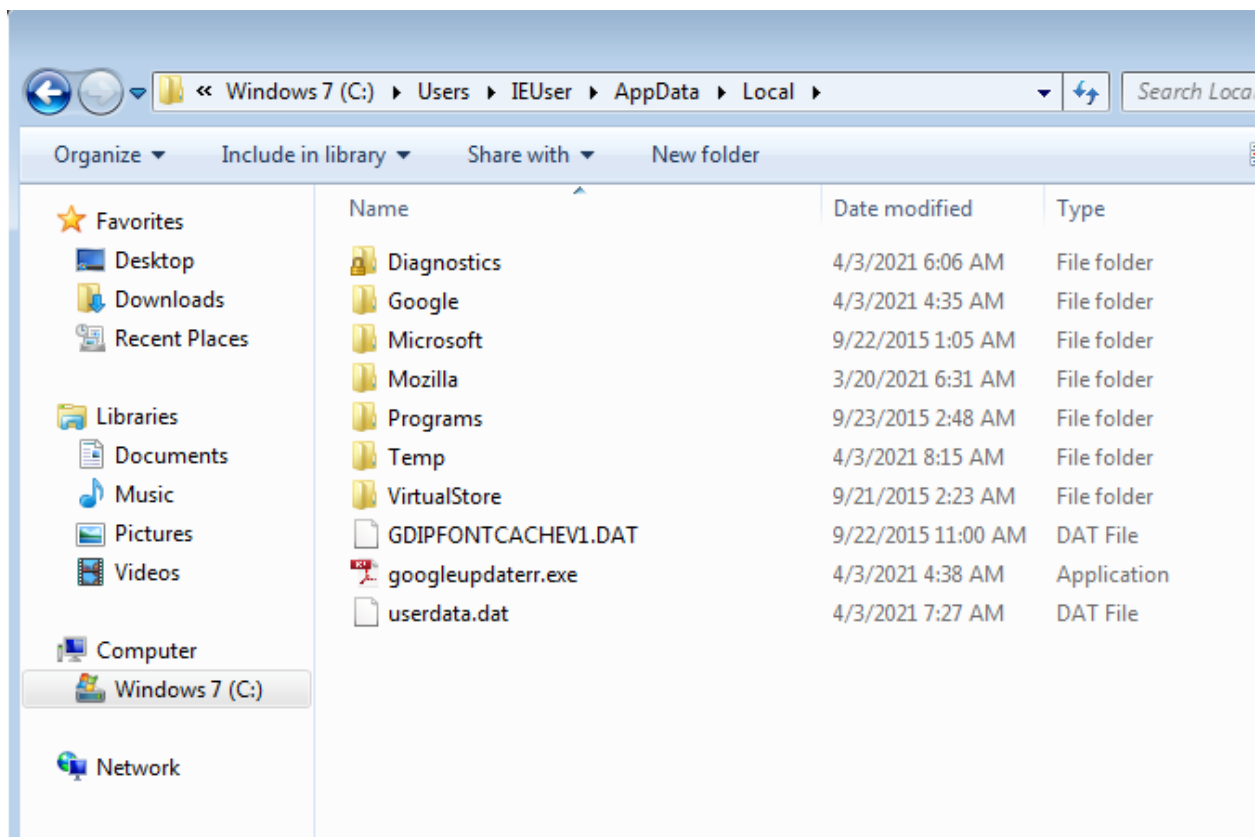
With reference to Week 2's lecture, why a second process is added by 'Dyre'? What does it aim to accomplish?

Once Dyre infects a host machine, it replicates and sends itself out to everyone in your contact list. Anyone that gets infected in turn sends out an entirely new variant.

#### Question 5:

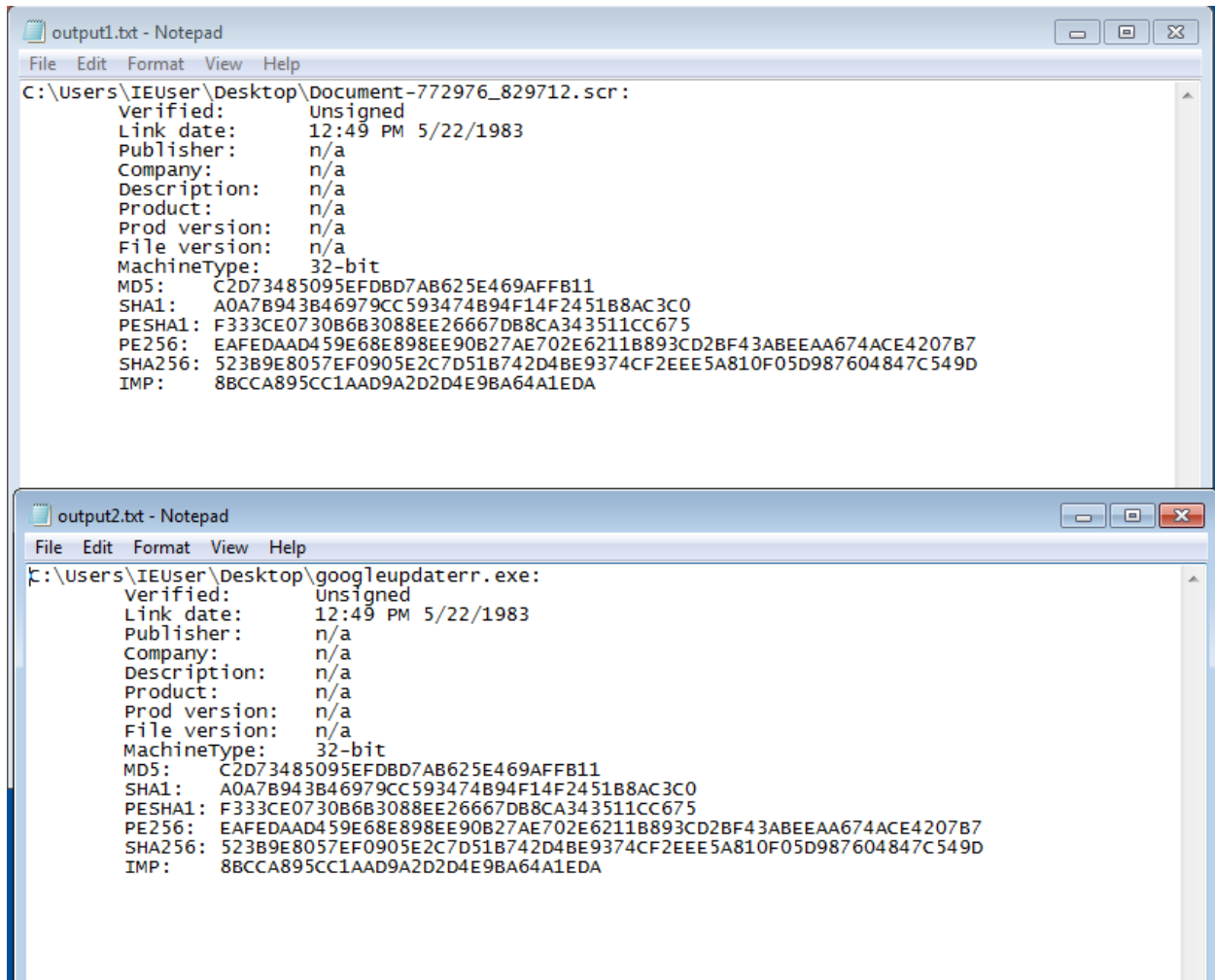
a. What is the path where googleupdaterr.exe is stored?

C:\Users\IEUser\AppData\Local



**b. How does this hash stored in output2.txt compare with the hash stored in output1.txt?**

**What is the meaning?**



```
output1.txt - Notepad
File Edit Format View Help
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:           C2D73485095EFD8D7AB625E469AFFB11
  SHA1:          A0A7B943B46979CC593474B94F14F2451B8AC3C0
  PESH1:         F333CE0730B6B3088EE26667DB8CA343511CC675
  PE256:         EAFEDAAD459E68E898EE90B27AE702E6211B893CD2BF43ABEEAA674ACE4207B7
  SHA256:        523B9E8057EF0905E2C7D51B742D48E9374CF2EEE5A810F05D987604847C549D
  IMP:           8BCCA895CC1AAD9A2D2D4E9BA64A1EDA

output2.txt - Notepad
File Edit Format View Help
C:\Users\IEUser\Desktop\googleupdaterr.exe:
  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:           C2D73485095EFD8D7AB625E469AFFB11
  SHA1:          A0A7B943B46979CC593474B94F14F2451B8AC3C0
  PESH1:         F333CE0730B6B3088EE26667DB8CA343511CC675
  PE256:         EAFEDAAD459E68E898EE90B27AE702E6211B893CD2BF43ABEEAA674ACE4207B7
  SHA256:        523B9E8057EF0905E2C7D51B742D48E9374CF2EEE5A810F05D987604847C549D
  IMP:           8BCCA895CC1AAD9A2D2D4E9BA64A1EDA
```

This means that the googleupdaterr.exe file is the same as the Document-772976\_829712.scr file.

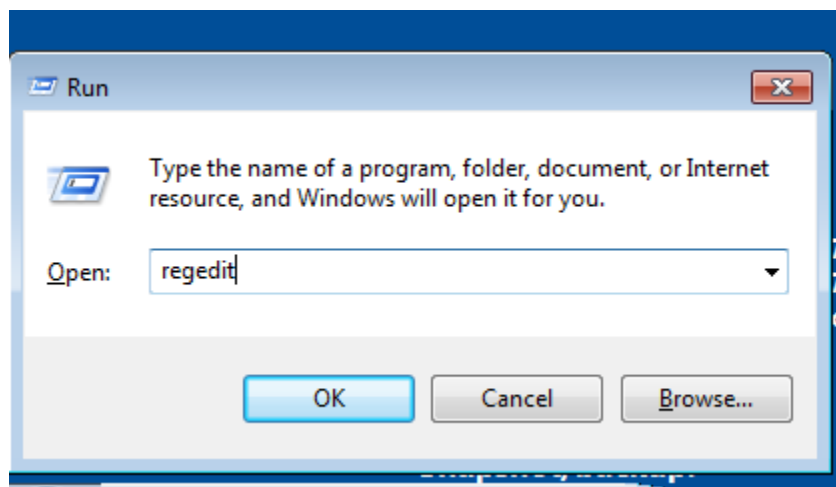
### Question 6:

#### a. What is 'Windows Registry?' What is it used for?

The Windows Registry is a hierarchical database that stores low-level settings for the Microsoft Windows operating system and for applications that opt to use the registry. The kernel, device drivers, services, Security Accounts Manager, and user interfaces can all use the registry.

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

The regedit command opens the windows registry



#### c. What "Regshot.exe" is used for?

Regshot is a small registry compare utility that allows you to take a snapshot of your registry make changes to your system (such as installing a program) and then taking a second snapshot to compare.

**d. What did the malware do to the registration tree and what was that for?**

The malware will modify the registry to make sure it can launch itself after a reboot, to better hide, or to integrate with an existing legitimate process

**e. The malware analysis you tried in this task was 'Static' or 'Dynamic' – justify with reference to Week 2's lecture.**

The analysis is a dynamic malware analysis. In contrast to static analysis, dynamic malware analysis allows the malware analyst to monitor the execution of malware at each step. The malware is typically executed in a sandbox or VM.

**Question 7:**

**a. Refer to <https://nakedsecurity.sophos.com/2020/05/22/the-ransomware-thatattacks-you-from-inside-a-virtual-machine/>. Write a paragraph in your own words summarizing how the attack worked.**

The assault was carried out by the Ragnar Locker group, which broke up company networks, managed recognition, deleted backups and manually deployed ransomware, before requesting multi-million-dollar ransoms. Like many criminals who execute similar "tough" or "big game" ransomware attacks in a tactical way called "leaving the field" the Ragnar Locker gang seeks to escape detections when working inside a victim's network (Monnappa, 2018). The gang has been using an attack to perform the Microsoft Installer with a Windows GPO task which downloaded an MSI containing a number of files including the VirtualBox copy and the Ragnar Locker running a Windows XP virtual machine inside it.

**b. Reflection: Write a paragraph (100-200 words) summarizing what you learned in this week's task. How did task 2.1P complement the lecture content in Week 2?**

The report helped me understand that some malwares are solely command-line based and do not have a GUI component (Kleymenov & Thabet, 2021). When such samples are executed, they run in the background and will not interact with any windows. For malwares with GUI components, they may interact with one or more windows during their execution. When a malware sample is executed, it can spawn multiple sub-processes in the background or may also inject itself into other legitimate processes. Processes running on the system can be tracked through Process Explorer. The assignment helped a lot in helping me understand the working of malware and analyzing the hex values using multiple tools such as sigcheck, procmon, and regshot (Sikorski & Honig, 2020).



## References

- Kleymenov, A., & Thabet, A. (2021). *Mastering Malware Analysis: The Complete Malware Analyst's Guide to Combating Malicious Software, APT, Cybercrime, and IoT Attacks*. Packt Publishing.
- Monnappa. (2018). *Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware*. Packt Publishing.
- Sikorski, M., & Honig, A. (2020). *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. No Starch Press.