Deon Perera

Analysis of “Dyre” malware

The Dyre malware was detected on 28 June 2016.

It is important to understand that antivirus software uses signatures (characteristics, distinctive patterns) to identify malware.

Polymorphic malware takes many forms in an effort to obfuscates itself from antivirus solutions. The malware code is encrypted with unique key; therefore the malware may not be detected by antivirus solutions. ‘This way, traditional security solutions may not easily catch them because they do not use a static, unchanging code’ (Trend Micro n.d:para.2). Malware creators can employ various encryption algorithms or create their own.

Dyre virus propagates itself to contacts stored on the computer and each new infection computer receives a variant of the malware. This therefore meets our definition of a ‘polymorphic virus’.

The payload

A payload is the malicious piece of code that a malware creator intends deliver to the victim’s computer. It is responsible for the adverse effect to the victim’s computer.

The Dyre virus primarily targets online banking websites, to try creating financial incentives for malware creators. ‘Dyre is capable of attacking the three most commonly used Windows web browsers (Internet Explorer, Chrome, and Firefox) in order to steal credentials.’ (Symantec 2015:pg.8)

The malware is capable of:

- Man-in-the-browser functionality
- Back connect proxy functionality

The Man-in-the-browser is similar in nature to the Man-in-the-middle-attack. The attacker acts as a proxy, placed between the victim’s browser and the website. The malware ‘hooks into the most popular web browsers to intercept traffic from a victim's system, stealing information and manipulating website content before it is rendered by the browser’ (Secureworks 2014:para.2).

To elaborate, when the victim connects to a banking website and inserts their banking credentials, packets are sent to the attacker (which acts as a proxy). From this information, the attacker has obtained the victim’s banking credentials. The attacker can then decide to forward the packets to the banking server, which responds with the website’s content. To avoid arousing suspicion, the attacker can enable normal behaviour of the website.

Man-in-the-browser simulates our packet analysis practical Task 1.4P. However, instead of simply analysing the packets, the data maybe manipulated to somehow defraud the victim.

Back connect proxy functionality enables a threat actor to access banking websites through the victim’s computer.

Deon Perera

Hex Editor

A Hex Editor enables the manipulation of the fundamental binary data that constitutes a computer file.

A computer operates through machine code (binary operations). However, it is not feasible for humans to create programming scripts in binary. To solve this issue, we use human readable programming languages. For instance, imagine a program is written in Python. Next, the program is compiled into assembly code. Then, the assembly code is converted into machine code that is understood by computer systems.

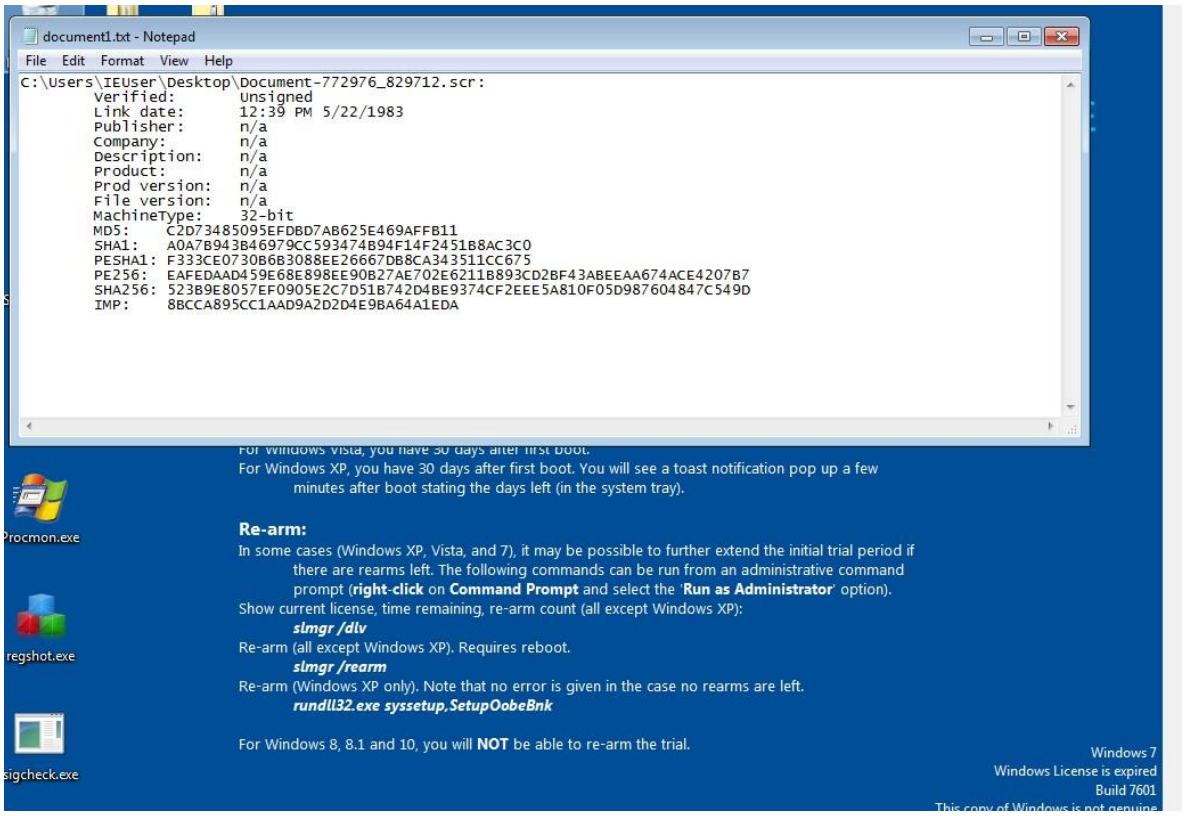
This implies the 'hex editors show you the raw data of a file, not the interpretation of that data, hex editors can open absolutely any type of file, allowing you to dig around and find out what they really are.' (UltraEdit 2018: sec.5). This means that in theory, we can modify the binary data to meet our needs, although this is a difficult task as machine code is difficult to comprehend.

The Hex Editor shows a file's data in Hexadecimal format. This simplifies the otherwise incomprehensible binary data. Hexadecimal refers to the base 16 number system.

MZ header

The MZ header indicates the file is an executable format. It can be identified by "4D 5A" Hex data. 'MZ' denotes the initials of Mark Zbikowski, one of the leading developers of Microsoft Disk Operating System.

By applying this knowledge, we can understand that despite the file taking the appearance of a PDF, the binary code indicates the file is an executable. This should raise some level of suspicion.



The output

The output shows the cryptographic hash functions (CHF) value of the file.
The CHF is a mathematical algorithm that maps data of an arbitrary size to a fixed length output. The algorithm only works one way, and it is not practical to convert the hash value to the original data.

If two files contain the same hash value, they are the exact same file. However, a metadata of a file such as file name does not change the hash value.

Process Monitor

Process Monitor is a tool from Windows Sysinternals utility suite. The software monitors file system, Registry, process and thread activity in real time. It includes features to examine activities.

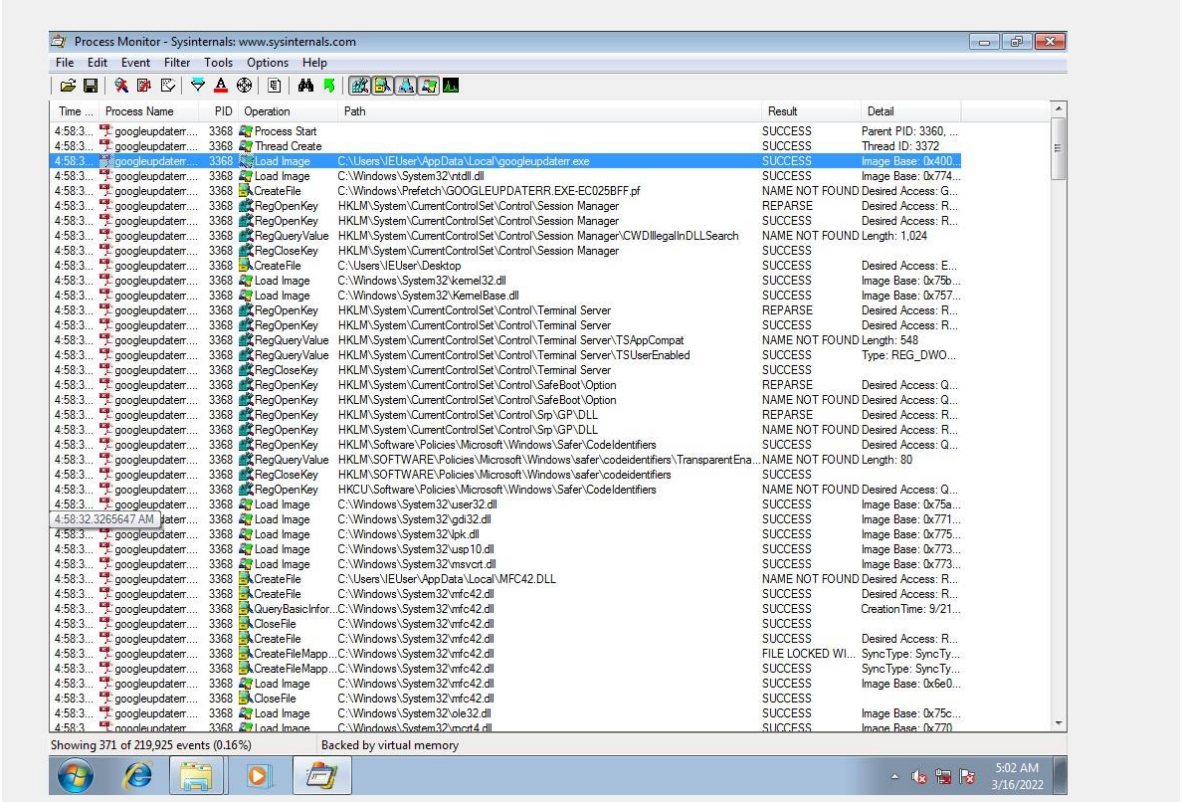
In our case study, we use Process Monitor to monitor actions performed by the malware.

What does it aim to accomplish?

The second process added by Dyre virus is an obfuscation technique named 'Process Hallowing'. This approach involves injecting malicious code into another process in an effort to evade security solutions.

This technique is 'used by malware in which a legitimate process is loaded on the system solely to act as a container for hostile code' (Fortuna 2017.para1).

Using Procmon to analyse the malware



The original malware and the new sample have different hash values. The hash value discrepancy demonstrates the malware' polymorphic capability.

Windows Registry

Windows Registry is a hierarchical database that 'stores much of the information and settings for software programs, hardware devices, user preferences, and operating-system configurations' (Fisher 2021:para.1).

The Registry Editor can be used to modify more settings than what is conventionally allowed by standard applications. For instance, we can change the task bar colour, add customised logos, disable Windows updates, disable Cortana and change a myriad of other settings. We can use the Registry Editor to change granular settings of our computer.

Most computers have five main branches in the registry, these are called hives. The hives are named as:

1. HKCR (HKEY_CLASSES_ROOT - Contains settings for file types and file extensions.
2. HKCU (HKEY_CURRENT_USER) – Contains the current user's settings on Windows.
3. HKLM (HKEY_LOCAL_MACHINE) – Contains settings for information for hardware software installed. This rootkey is the accessed.
4. HKU (HKEY_USERS) – Contains settings for information for users that log on to the computer.
5. HKEY_CURRENT_CONFIG (HKCC) – Contains settings for information input and output hardware attached.

The registry is structured in a tree format, each folder in the tree is called a key. Each key can house a subkey and a value. Types of values may include: • Binary value (0 or 1) – denoting on or off.

Regshot

Regshot is dynamic malware analysis tool. The tool functions by creating a snapshot of the Windows Registry before and after a malware file has been executed. Subsequently, we can view the changes a malware has created to the Windows Registry.

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

The virus added 3 values and modified 5 other values.

The final entry created a value in the Run registry key. 'The Run key makes the program run every time the user logs on' (Microsoft 2022:para.1)

The key is as follows:

'……..\AppData\Local\googleupdaterr.exe'

As previously established, 'googleupdaterr.exe' is an encrypted sample of the malware.

Furthermore, I used SigCheck to obtain the hash value of googleupdaterr.exe. Then I executed googleupdaterr.exe and checked the file's hash value again. The result was interesting: the two files had different hash values. This demonstrates the virus' polymorphic capabilities.

Therefore, the evidence suggests the during bootup, the googleupdaterr.exe (malware) is executed. Then, the malware replaces itself with a sample that is encrypted with a new key.

Deon Perera

References

Kaspersky. c.2016. 'TROJAN-BANKER.WIN32.DYRE'. https://threats.kaspersky.com/en/threat/Trojan-Banker.Win32.Dyre. Accessed: 15 March 2022.

Trend Micro. n.d. 'Polymorphic virus'. https://www.trendmicro.com/vinfo/us/security/definition/Polymorphic-virus. Accessed: 15 March 2022.

Zemana. n.d. 'Dyre Malware'. https://www.zemana.com/removal-guide/dyre-malware-removal. Accessed: 15 March 2022.

Symantec, 2015. 'Dyre: Emerging threat on financial fraud landscape'. https://docs.broadcom.com/doc/dyre-emerging-threat. Accessed: 15 March 2022.

Secureworks. 2014. 'Dyre Banking Trojan'. https://www.secureworks.com/research/dyre-banking-trojan. Accessed: 15 March 2022.

Kaspersky. c.2016. 'TROJAN-BANKER.WIN32.DYRE'. https://threats.kaspersky.com/en/threat/Trojan-Banker.Win32.Dyre/. Accessed: 15 March 2022.

Zemana. n.d. 'Dyre Malware'. https://www.zemana.com/removal-guide/dyre-malware-removal. Accessed: 15 March 2022.

UltraEdit. 2018. 'What is a Hex Editor, and Why Might You Use One?'. https://www.ultraedit.com/company/blog/community/what-is-a-hex-editor-why-use-one.html. Accessed: 15 March 2022.

Alex Verboon. 2009. 'The "MZ" header in EXE files'. https://en-academic.com/dic.nsf/enwiki/11603046. Accessed: 15 March 2022.

Microsoft. 2022. 'Process Monitor v3.89'. https://docs.microsoft.com/en-us/sysinternals/downloads/procmon. Accessed: 15 March 2022.

Andrea Fortuna. 2017. 'Understanding Process Hollowing'. https://andreafortuna.org/2017/10/09/understanding-process-hollowing/. Accessed: 16 March 2022

Tim Fisher. 2021. 'What Is the Windows Registry?'. https://www.lifewire.com/windows-registry-2625992. Accessed: 15 March 2022.

Computer Hope. 2022. 'Registry'. https://www.computerhope.com/jargon/r/registry.htm. Accessed: 15 March 2022

Microsoft, 2022. 'Run and RunOnce Registry Keys'. https://docs.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys. Accessed March 2022