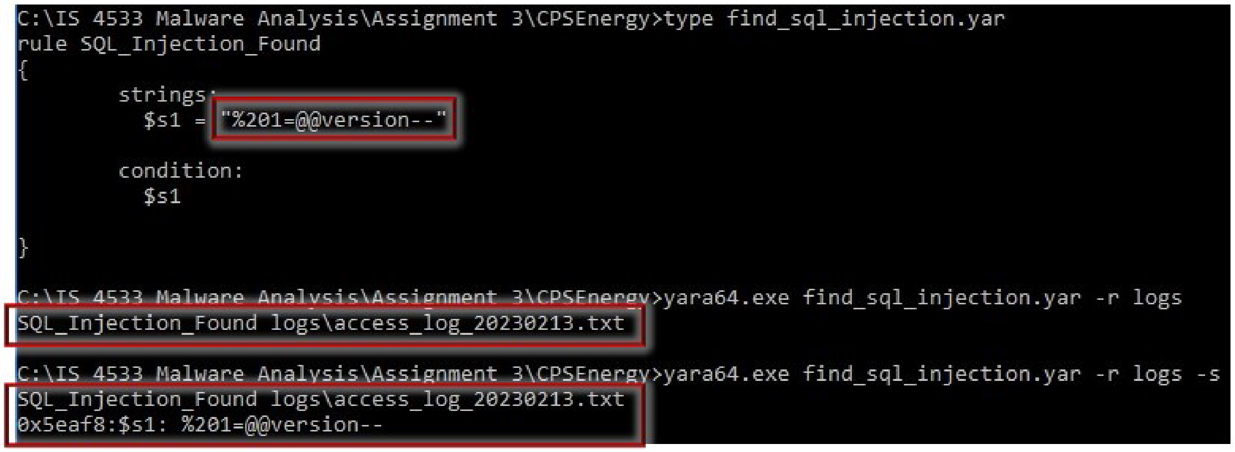
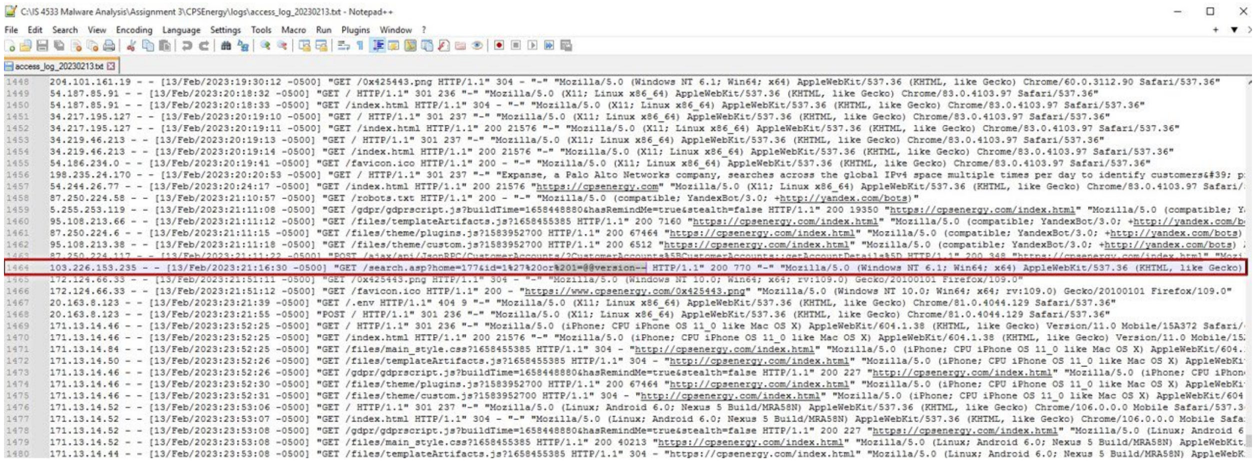
1. Using `find_sql_injection` via command terminal I discovered `access_log_20230213.txt` contains the SQL Injection attack `%201=@@version--`.



```
C:\IS 4533 Malware Analysis\Assignment 3\CPSEnergy>type find_sql_injection.yar
rule SQL_Injection_Found
{
        strings:
          $s1 = "%201=@@version--"

        condition:
          $s1

}

C:\IS 4533 Malware Analysis\Assignment 3\CPSEnergy>yara64.exe find_sql_injection.yar -r logs
SQL_Injection_Found logs\access_log_20230213.txt

C:\IS 4533 Malware Analysis\Assignment 3\CPSEnergy>yara64.exe find_sql_injection.yar -r logs -s
SQL_Injection_Found logs\access_log_20230213.txt
0x5eaf8:$s1: %201=@@version--
```

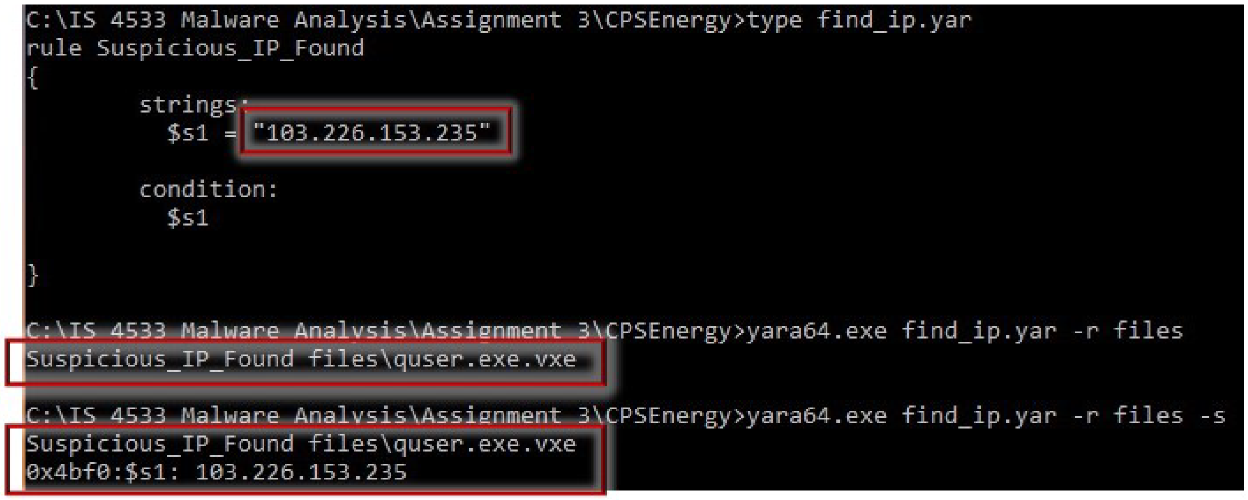
Opening `access_log_20230213.txt` via Notepad++, searching for `%201=@@version--`, I discovered IP `103.226.153.235` was responsible.



C:\IS 4533 Malware Analysis\Assignment 3\CPSEnergy\logs\access_log_20230213.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
access_log_20230213.txt

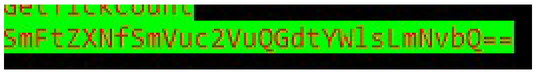
```
204.101.161.19 - - [13/Feb/2023:19:30:12 -0500] "GET /0x425443.png HTTP/1.1" 304 - "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36"
54.187.85.91 - - [13/Feb/2023:20:18:32 -0500] "GET / HTTP/1.1" 301 236 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97 Safari/537.36"
54.187.85.91 - - [13/Feb/2023:20:18:33 -0500] "GET /index.html HTTP/1.1" 304 - "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97 Safari/537.36"
34.217.195.127 - - [13/Feb/2023:20:19:10 -0500] "GET / HTTP/1.1" 301 237 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97 Safari/537.36"
34.217.195.127 - - [13/Feb/2023:20:19:11 -0500] "GET /index.html HTTP/1.1" 200 21576 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97 Safari/537.36"
34.219.46.213 - - [13/Feb/2023:20:19:13 -0500] "GET / HTTP/1.1" 301 237 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97 Safari/537.36"
34.219.46.213 - - [13/Feb/2023:20:19:14 -0500] "GET /index.html HTTP/1.1" 200 21576 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97 Safari/537.36"
54.186.234.0 - - [13/Feb/2023:20:19:41 -0500] "GET /favicon.ico HTTP/1.1" 200 - "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97 Safari/537.36"
198.235.24.170 - - [13/Feb/2023:20:20:53 -0500] "GET / HTTP/1.1" 301 237 "-" "Expanse, a Palo Alto Networks company, searches across the global IPv4 space multiple times per day to identify customers&#39; p
54.244.26.77 - - [13/Feb/2023:20:24:17 -0500] "GET /index.html HTTP/1.1" 200 21576 "https://cpsenergy.com" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97 Safari/
87.250.224.58 - - [13/Feb/2023:21:10:57 -0500] "GET /robots.txt HTTP/1.1" 200 - "-" "Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)"
5.255.253.119 - - [13/Feb/2023:21:11:08 -0500] "GET /gdpr/gdprscript.js?buildTime=1658448880&hasRemindMe=true&stealth=false HTTP/1.1" 200 19350 "https://cpsenergy.com/index.html" "Mozilla/5.0 (compatible; Y
95.108.213.66 - - [13/Feb/2023:21:11:12 -0500] "GET /files/templateArtifacts.js?1658455385 HTTP/1.1" 200 7160 "https://cpsenergy.com/index.html" "Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/b
87.250.224.6 - - [13/Feb/2023:21:11:15 -0500] "GET /files/theme/plugins.js?1583952700 HTTP/1.1" 200 67464 "https://cpsenergy.com/index.html" "Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)
95.108.213.38 - - [13/Feb/2023:21:11:18 -0500] "GET /files/theme/custom.js?1583952700 HTTP/1.1" 200 6512 "https://cpsenergy.com/index.html" "Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)
87.250.224.117 - - [13/Feb/2023:21:11:22 -0500] "POST /ajax/api/JsonRPC/CustomerAccounts/?CustomerAccounts%5BCustomerAccounts::getAccountDetails%5D HTTP/1.1" 200 348 "https://cpsenergy.com/index.html" "Mozi
103.226.153.235 - - [13/Feb/2023:21:16:30 -0500] "GET /search.asp?home=177&id=1%27%20or%201=@@version-- HTTP/1.1" 200 770 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
172.124.66.33 - - [13/Feb/2023:21:51:11 -0500] "GET /0x425443.png HTTP/1.1" 304 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0"
172.124.66.33 - - [13/Feb/2023:21:51:12 -0500] "GET /favicon.ico HTTP/1.1" 200 - "https://www.cpsenergy.com/0x425443.png" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0"
20.163.8.123 - - [13/Feb/2023:23:21:39 -0500] "GET /.env HTTP/1.1" 404 9 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36"
20.163.8.123 - - [13/Feb/2023:23:21:55 -0500] "POST / HTTP/1.1" 301 236 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36"
171.13.14.46 - - [13/Feb/2023:23:52:25 -0500] "GET / HTTP/1.1" 301 236 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 11_0 like Mac OS X) AppleWebKit/604.1.38 (KHTML, like Gecko) Version/11.0 Mobile/15A372 Safari/
171.13.14.46 - - [13/Feb/2023:23:52:25 -0500] "GET /index.html HTTP/1.1" 200 21576 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 11_0 like Mac OS X) AppleWebKit/604.1.38 (KHTML, like Gecko) Version/11.0 Mobile/15
171.13.14.84 - - [13/Feb/2023:23:52:25 -0500] "GET /files/main_style.css?1658455385 HTTP/1.1" 304 - "http://cpsenergy.com/index.html" "Mozilla/5.0 (iPhone; CPU iPhone OS 11_0 like Mac OS X) AppleWebKit/604.
171.13.14.50 - - [13/Feb/2023:23:52:26 -0500] "GET /files/templateArtifacts.js?1658455385 HTTP/1.1" 304 - "http://cpsenergy.com/index.html" "Mozilla/5.0 (iPhone; CPU iPhone OS 11_0 like Mac OS X) AppleWebKi
171.13.14.46 - - [13/Feb/2023:23:52:26 -0500] "GET /gdpr/gdprscript.js?buildTime=1658448880&hasRemindMe=true&stealth=false HTTP/1.1" 200 227 "http://cpsenergy.com/index.html" "Mozilla/5.0 (iPhone; CPU iPhon
171.13.14.46 - - [13/Feb/2023:23:52:30 -0500] "GET /files/theme/plugins.js?1583952700 HTTP/1.1" 200 67464 "http://cpsenergy.com/index.html" "Mozilla/5.0 (iPhone; CPU iPhone OS 11_0 like Mac OS X) AppleWebKi
171.13.14.46 - - [13/Feb/2023:23:52:31 -0500] "GET /files/theme/custom.js?1583952700 HTTP/1.1" 304 - "http://cpsenergy.com/index.html" "Mozilla/5.0 (iPhone; CPU iPhone OS 11_0 like Mac OS X) AppleWebKit/604
171.13.14.52 - - [13/Feb/2023:23:53:06 -0500] "GET / HTTP/1.1" 301 237 "-" "Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Mobile Safari/537.3
171.13.14.52 - - [13/Feb/2023:23:53:07 -0500] "GET /index.html HTTP/1.1" 304 - "-" "Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Mobile Safa
171.13.14.52 - - [13/Feb/2023:23:53:08 -0500] "GET /gdpr/gdprscript.js?buildTime=1658448880&hasRemindMe=true&stealth=false HTTP/1.1" 200 227 "https://cpsenergy.com/index.html" "Mozilla/5.0 (Linux; Android 6
171.13.14.52 - - [13/Feb/2023:23:53:08 -0500] "GET /files/main_style.css?1658455385 HTTP/1.1" 200 40213 "https://cpsenergy.com/index.html" "Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit
171.13.14.44 - - [13/Feb/2023:23:53:08 -0500] "GET /files/templateArtifacts.js?1658455385 HTTP/1.1" 304 - "https://cpsenergy.com/index.html" "Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebK
```

2. After modifying `find_ip.yar` to search for IP `103.226.153.235`, I executed `find_ip.yar` in the command terminal to find `103.226.153.235` in the executable files. `quser.exe.vxe` contains the suspicious IP `103.226.153.235`.



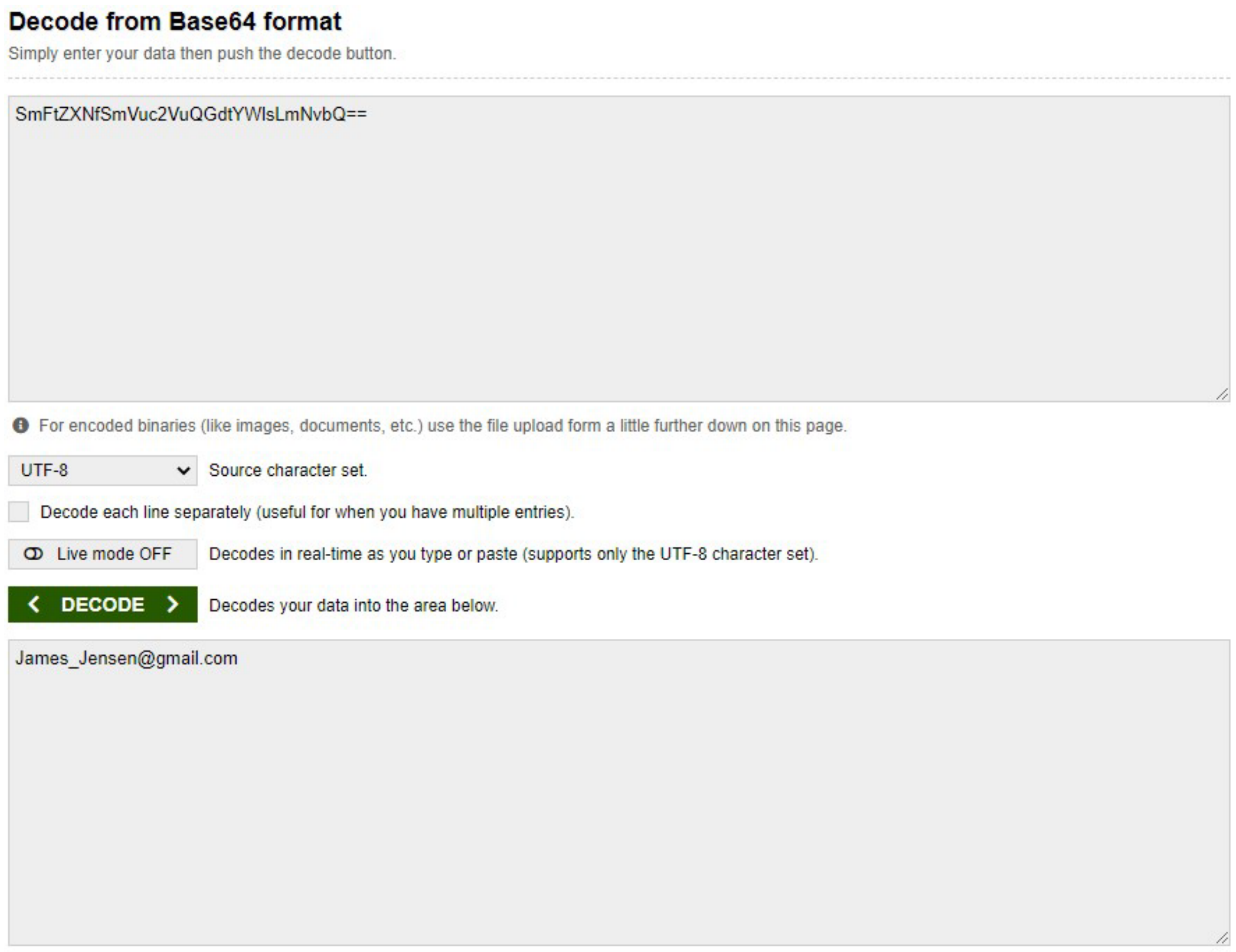
```
C:\IS 4533 Malware Analysis\Assignment 3\CPSEnergy>type find_ip.yar
rule Suspicious_IP_Found
{
        strings:
          $s1 = "103.226.153.235"

        condition:
          $s1

}

C:\IS 4533 Malware Analysis\Assignment 3\CPSEnergy>yara64.exe find_ip.yar -r files
Suspicious_IP_Found files\quser.exe.vxe

C:\IS 4533 Malware Analysis\Assignment 3\CPSEnergy>yara64.exe find_ip.yar -r files -s
Suspicious_IP_Found files\quser.exe.vxe
0x4bf0:$s1: 103.226.153.235
```

3. Using the Bstrings utility, I executed `bstrings -f quser.exe.vxe --lr b64` in the command terminal. Examining the output, I determined `SmFtZXNfSmVuc2VuQGdtYWlsLmNvbQ==` as likely Base64.



```
GetTickCount
SmFtZXNfSmVuc2VuQGdtYWlsLmNvbQ==
```

Decoded `SmFtZXNfSmVuc2VuQGdtYWlsLmNvbQ==` via *base64decode.org*, which revealed `James_Jensen@gmail.com` as the critical email used by actors to exfiltrate CPSEnergy data.



Decode from Base64 format

Simply enter your data then push the decode button.

```
SmFtZXNfSmVuc2VuQGdtYWlsLmNvbQ==
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

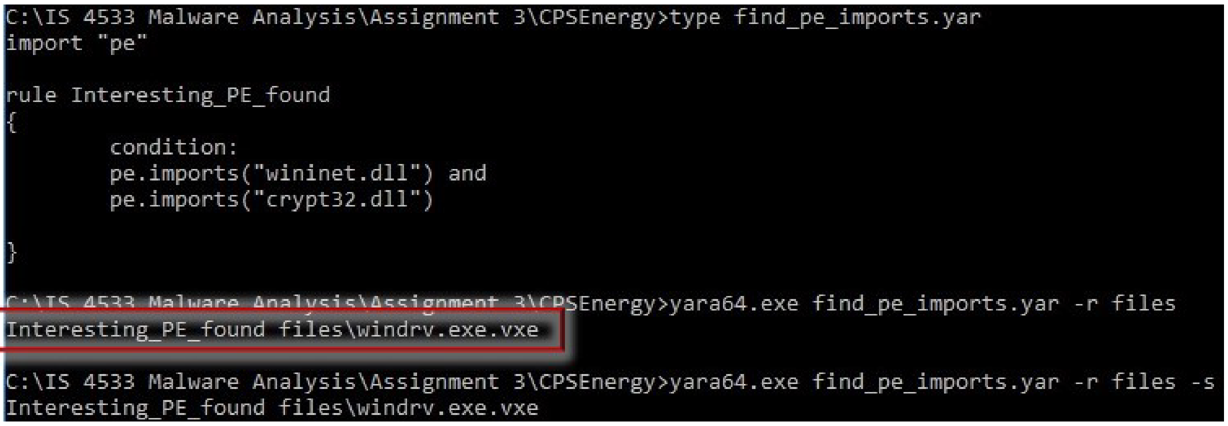
Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

```
James_Jensen@gmail.com
```

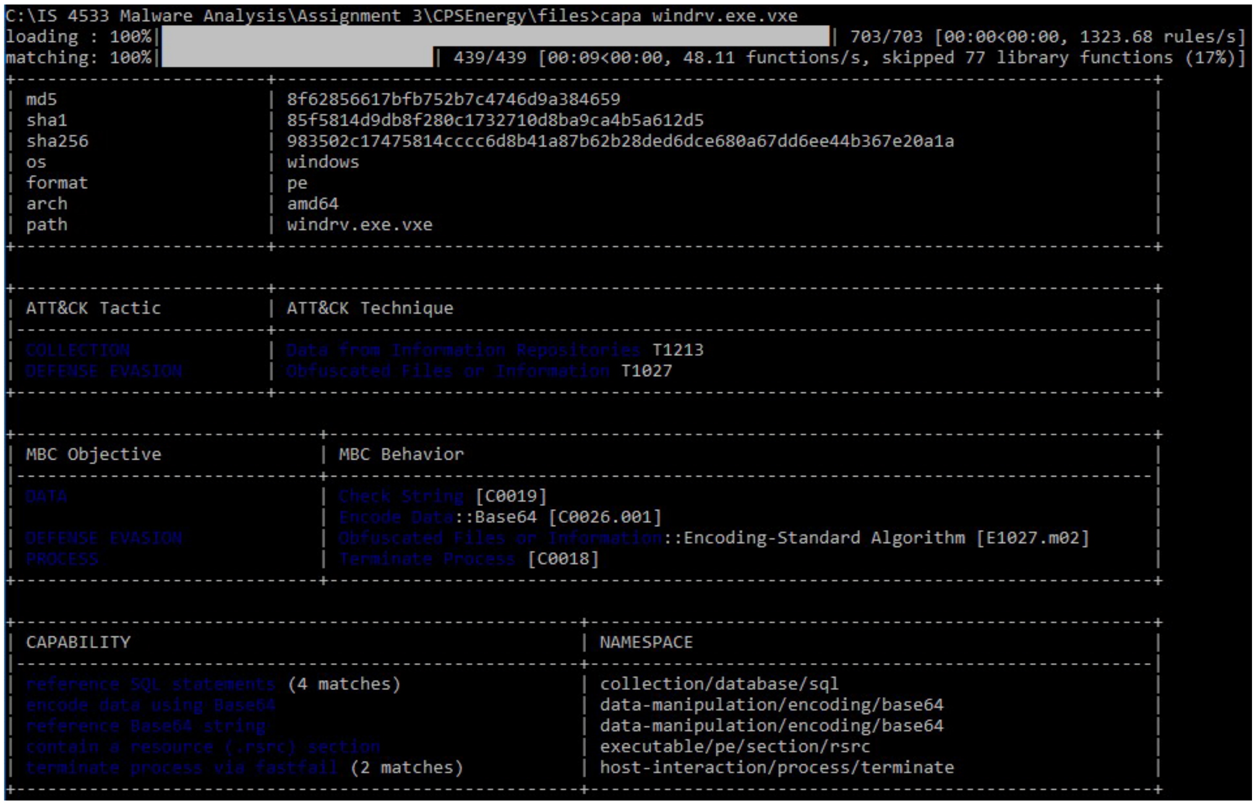
BONUS

Using `find_pe_imports.yar` YARA rule to look for `wininet.dll` and `cyrpt32.dll`, I discovered that `windrv.exe.vxe` is the potential malware that contains both.



```
C:\IS 4533 Malware Analysis\Assignment 3\CPSEnergy>type find_pe_imports.yar
import "pe"

rule Interesting_PE_found
{
        condition:
        pe.imports("wininet.dll") and
        pe.imports("crypt32.dll")

}

C:\IS 4533 Malware Analysis\Assignment 3\CPSEnergy>yara64.exe find_pe_imports.yar -r files
Interesting_PE_found files\windrv.exe.vxe

C:\IS 4533 Malware Analysis\Assignment 3\CPSEnergy>yara64.exe find_pe_imports.yar -r files -s
Interesting_PE_found files\windrv.exe.vxe
```

Below is the output of using the CAPA tool against `windrv.exe.vxe` via command terminal, revealing its capabilities.



```
C:\IS 4533 Malware Analysis\Assignment 3\CPSEnergy\files>capa windrv.exe.vxe
loading : 100%|████████████████████████████████████████████████████████████████| 703/703 [00:00<00:00, 1323.68 rules/s]
matching: 100%|█████████████████████████| 439/439 [00:09<00:00, 48.11 functions/s, skipped 77 library functions (17%)]
+-------------------------+------------------------------------------------------------------------------+
| md5                     | 8f62856617bfb752b7c4746d9a384659                                             |
| sha1                    | 85f5814d9db8f280c1732710d8ba9ca4b5a612d5                                     |
| sha256                  | 983502c17475814cccc6d8b41a87b62b28ded6dce680a67dd6ee44b367e20a1a             |
| os                      | windows                                                                      |
| format                  | pe                                                                           |
| arch                    | amd64                                                                        |
| path                    | windrv.exe.vxe                                                               |
+-------------------------+------------------------------------------------------------------------------+

+-------------------------+------------------------------------------------------------------------------+
| ATT&CK Tactic           | ATT&CK Technique                                                             |
|-------------------------+------------------------------------------------------------------------------|
| COLLECTION              | Data from Information Repositories T1213                                     |
| DEFENSE EVASION         | Obfuscated Files or Information T1027                                        |
+-------------------------+------------------------------------------------------------------------------+

+------------------------------+-------------------------------------------------------------------------+
| MBC Objective                | MBC Behavior                                                            |
|------------------------------+-------------------------------------------------------------------------|
| DATA                         | Check String [C0019]                                                    |
|                              | Encode Data::Base64 [C0026.001]                                         |
| DEFENSE EVASION              | Obfuscated Files or Information::Encoding-Standard Algorithm [E1027.m02] |
| PROCESS                      | Terminate Process [C0018]                                               |
+------------------------------+-------------------------------------------------------------------------+

+-----------------------------------------------------+--------------------------------------------------+
| CAPABILITY                                          | NAMESPACE                                        |
|-----------------------------------------------------+--------------------------------------------------|
| reference SQL statements (4 matches)                | collection/database/sql                          |
| encode data using Base64                            | data-manipulation/encoding/base64                |
| reference Base64 string                             | data-manipulation/encoding/base64                |
| contain a resource (.rsrc) section                  | executable/pe/section/rsrc                       |
| terminate process via fastfail (2 matches)          | host-interaction/process/terminate               |
+-----------------------------------------------------+--------------------------------------------------+
```

Raymond Ng
JQG999
IS 4533 – 001 Spring 2023