A new ransomware group, OnyxCrew, has crippled networks at Valero Energy Corporation Headquarters (San Antonio)!

Intelligence reports that the OnyxCrew malware demands ransom in Bitcoin and, once paid, the malware reaches out to a website to retrieve a Bitcoin Wallet address embedded on the site to deposit the ransom. One other particular IOC (Indicator of Compromise) is that the OnyxCrew likes to pack their ransomware with UPX.

Valero IT staff have exported executable files from an infected system to a thumbdrive (valero_thumbdrive.vhd).

It's all up to you! Can you find the malware associated with this attack?

Assignment -- Your mission should you choose to accept it:

--Download the virtual thumbdrive from Professor Ervin's OneDrive account. (double-click the valero_thumbdrive.vhd in windows to open and mount it).

--There is also a copy of the upx, peid, and bstrings utilities that you may find useful.

--To assist you, please reference Prof Ervin's lecture that demonstrates how to identify packed executables with PEID and UPX...and how to extract artifacts from files using the bstrings utility.

GRADING RUBRIC -- To receive full credit for this assignment, you must answer the following:

1. Which of the executable files is the OnyxCrew malware? Submit a screenshot supporting your findings.

```
raserver.exe.vxe
```

2. Once unpacked, what is Autorun persistence registry key embedded within the malware? (Submit a screenshot supporting your findings)

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\raserver.exe
```

3. What is the windows file path embedded within the malware? (Submit a screenshot supporting your findings)

```
c:\OnyxCrew\ransware\raserver\Release\
```

4. What is the URL embedded within the malware? (Submit a screenshot supporting your findings)

```
https://tinyurl.com/2p865z29
```

5. After visiting the URL, what is the Bitcoin Wallet address embedded at the website? (Submit a screenshot supporting your findings)

```
bc1q7cyrfmck2ffu2ud3rn5l5a8yv60chkp0zpemf
```

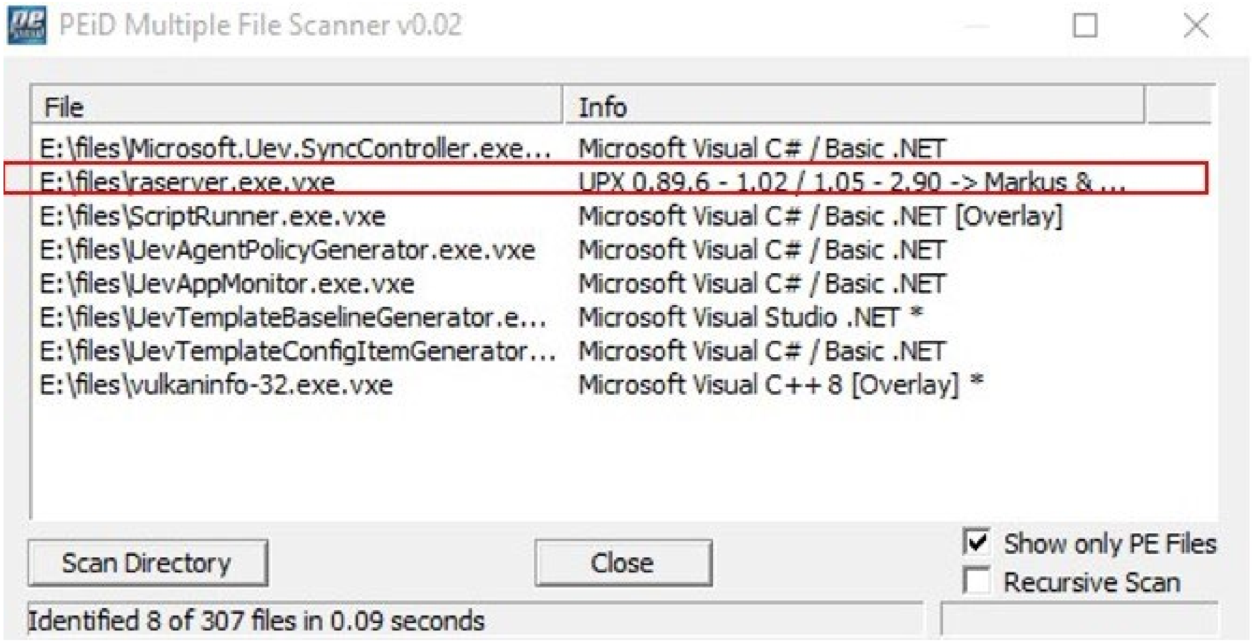
BONUS (5-pts)

Do your own research and determine how much total in bitcoin (if any) is currently in OnyxCrew's Bitcoin Wallet. What is it approximately worth today in US Dollars? Submit a screenshot showing your findings.

Raymond Ng
JQG999
IS 4533 - 001
February 8, 2023

Assignment 2

1. `raserver.exe.vxe` is the executable file that is the OnyxCrew malware.

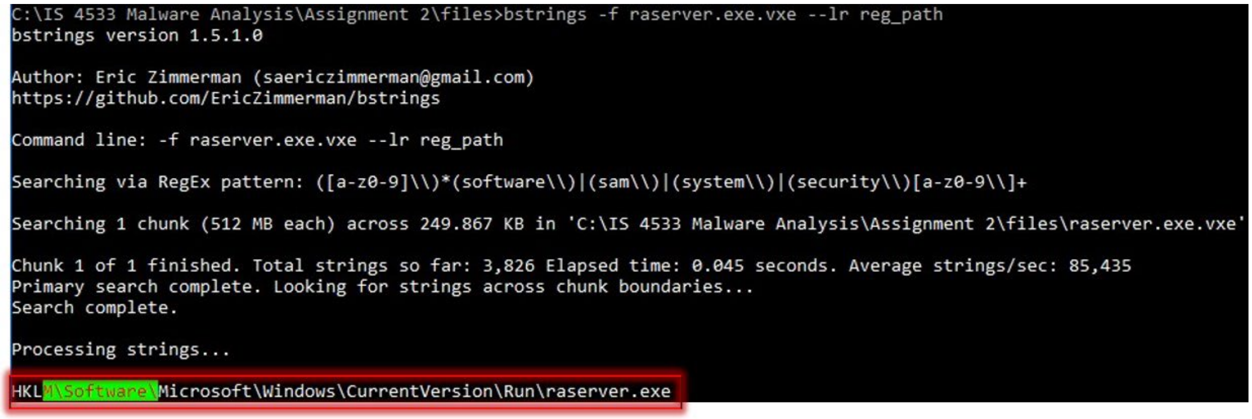


File	Info
E:\files\Microsoft.Uev.SyncController.exe...	Microsoft Visual C# / Basic .NET
E:\files\raserver.exe.vxe	UPX 0.89.6 - 1.02 / 1.05 - 2.90 -> Markus & ...
E:\files\ScriptRunner.exe.vxe	Microsoft Visual C# / Basic .NET [Overlay]
E:\files\UevAgentPolicyGenerator.exe.vxe	Microsoft Visual C# / Basic .NET
E:\files\UevAppMonitor.exe.vxe	Microsoft Visual C# / Basic .NET
E:\files\UevTemplateBaselineGenerator.e...	Microsoft Visual Studio .NET *
E:\files\UevTemplateConfigItemGenerator...	Microsoft Visual C# / Basic .NET
E:\files\vulkaninfo-32.exe.vxe	Microsoft Visual C++ 8 [Overlay] *

☑ Show only PE Files
□ Recursive Scan

Identified 8 of 307 files in 0.09 seconds

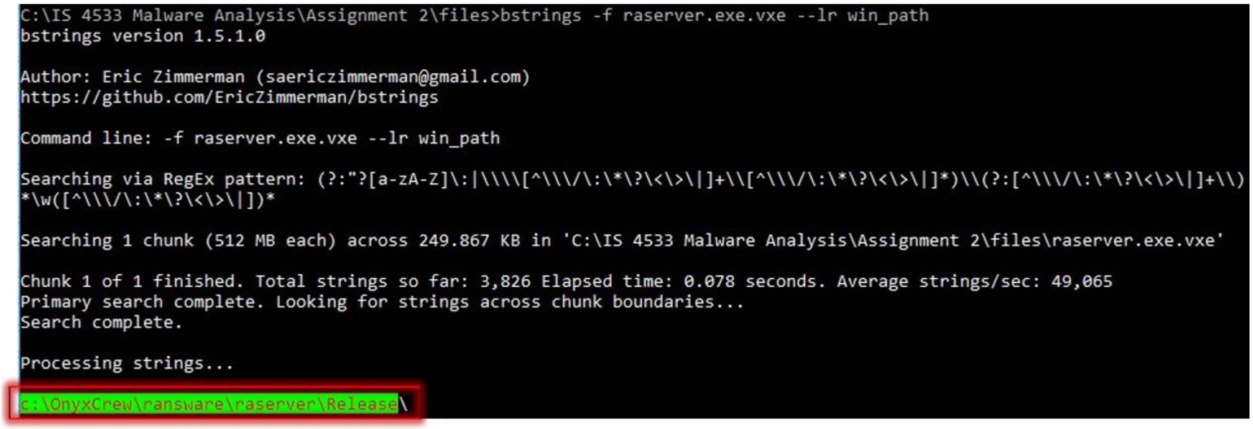
2. `HKLM\Software\Microsoft\Windows\CurrentVersion\Run\` is the Autorun persistence registry kye embedded within the malware.



```
C:\IS 4533 Malware Analysis\Assignment 2\files>bstrings -f raserver.exe.vxe --lr reg_path
bstrings version 1.5.1.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/bstrings

Command line: -f raserver.exe.vxe --lr reg_path

Searching via RegEx pattern: ([a-z0-9]\\)*(software\\)|(sam\\)|(system\\)|(security\\)[a-z0-9\\]+

Searching 1 chunk (512 MB each) across 249.867 KB in 'C:\IS 4533 Malware Analysis\Assignment 2\files\raserver.exe.vxe'

Chunk 1 of 1 finished. Total strings so far: 3,826 Elapsed time: 0.045 seconds. Average strings/sec: 85,435
Primary search complete. Looking for strings across chunk boundaries...
Search complete.

Processing strings...

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\raserver.exe
```

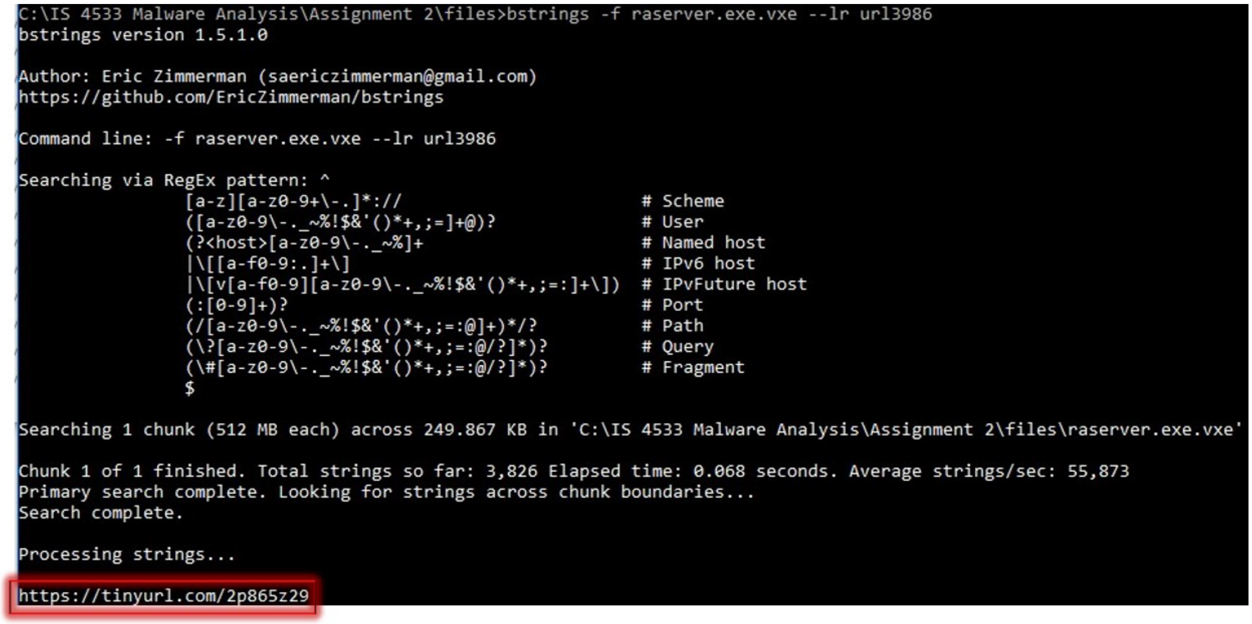
Raymond Ng
JQG999
IS 4533 - 001
February 8, 2023

3. `c:\OnyxCrew\ransware\raserver\Release\` is the file path embedded within the malware.



```
C:\IS 4533 Malware Analysis\Assignment 2\files>bstrings -f raserver.exe.vxe --lr win_path
bstrings version 1.5.1.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/bstrings

Command line: -f raserver.exe.vxe --lr win_path

Searching via RegEx pattern: (?:"?[a-zA-Z]\:|\\\\[^\\\/\:\*\?\<\>\|]+\\[^\\\/\:\*\?\<\>\|]*)\\(?:[^\\\/\:\*\?\<\>\|]+\\)
*\w([^\\\/\:\*\?\<\>\|])*

Searching 1 chunk (512 MB each) across 249.867 KB in 'C:\IS 4533 Malware Analysis\Assignment 2\files\raserver.exe.vxe'

Chunk 1 of 1 finished. Total strings so far: 3,826 Elapsed time: 0.078 seconds. Average strings/sec: 49,065
Primary search complete. Looking for strings across chunk boundaries...
Search complete.

Processing strings...

c:\OnyxCrew\ransware\raserver\Release\
```

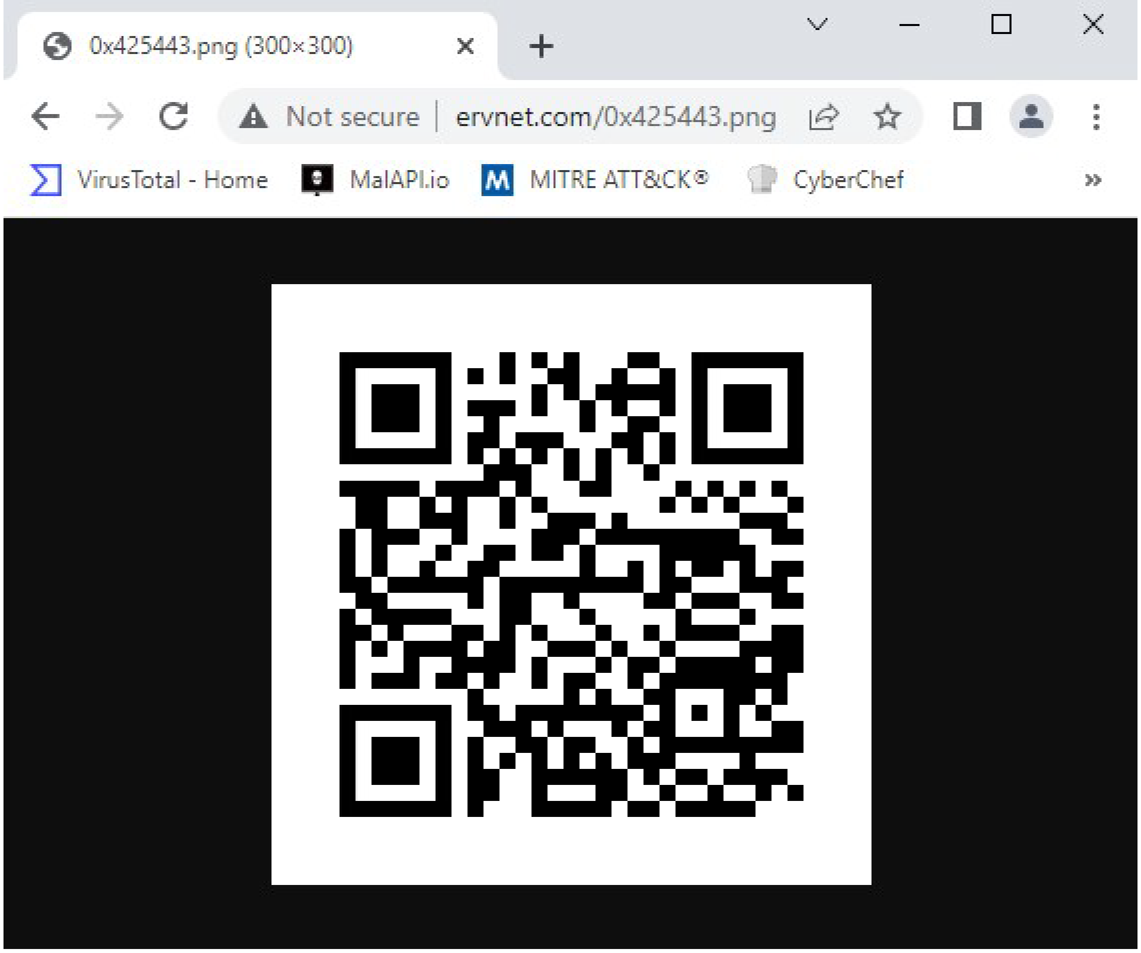
4. `https://tinyurl.com/2p865z29` is the URL embedded within the malware.



```
C:\IS 4533 Malware Analysis\Assignment 2\files>bstrings -f raserver.exe.vxe --lr url3986
bstrings version 1.5.1.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/bstrings

Command line: -f raserver.exe.vxe --lr url3986

Searching via RegEx pattern: ^
                [a-z][a-z0-9+\-.]*://                         # Scheme
                ([a-z0-9\-._~%!$&'()*+,;=]+@)?                # User
                (?<host>[a-z0-9\-._~%]+                       # Named host
                |\[[a-f0-9:.]+\]                              # IPv6 host
                |\[v[a-f0-9][a-z0-9\-._~%!$&'()*+,;=:]+\])    # IPvFuture host
                (:[0-9]+)?                                    # Port
                (/[a-z0-9\-._~%!$&'()*+,;=:@]+)*/?            # Path
                (\?[a-z0-9\-._~%!$&'()*+,;=:@/?]*)?           # Query
                (\#[a-z0-9\-._~%!$&'()*+,;=:@/?]*)?           # Fragment
                $

Searching 1 chunk (512 MB each) across 249.867 KB in 'C:\IS 4533 Malware Analysis\Assignment 2\files\raserver.exe.vxe'

Chunk 1 of 1 finished. Total strings so far: 3,826 Elapsed time: 0.068 seconds. Average strings/sec: 55,873
Primary search complete. Looking for strings across chunk boundaries...
Search complete.

Processing strings...

https://tinyurl.com/2p865z29
```

Raymond Ng
JQG999
IS 4533 - 001
February 8, 2023

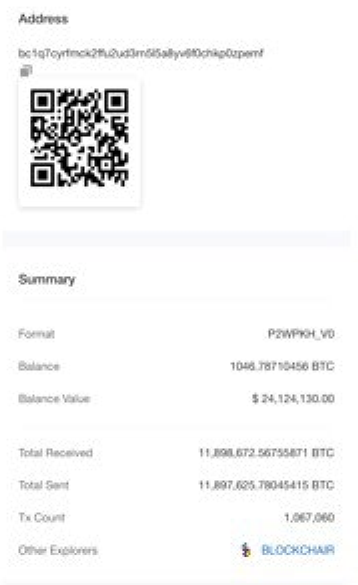
5. After visiting `https://tinyurl.com/2p865z29`, an image of QR code generated via web browser (image below). After scanning the QR code with a mobile device's camera, a new web browser with results connected to a Bitcoin wallet address: `bc1q7cyrfmck2ffu2ud3rn5l5a8yv60chkp0zpemf`.



Raymond Ng
JQG999
IS 4533 - 001
February 8, 2023

BONUS (5-pts)

After reviewing the search results that generated from scanning the QR code, I assess OnyxCrew's Bitcoin wallet has a balance of approximately 1044-1046 bitcoin, which is equivalent to approximately $24,000,000 US dollars.

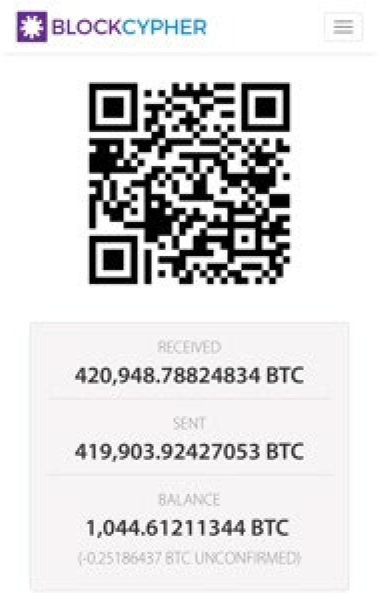


Address

bc1q7cyrfmck2ffu2ud3rn5l5a8yv6f0chkp0zpemf

Summary

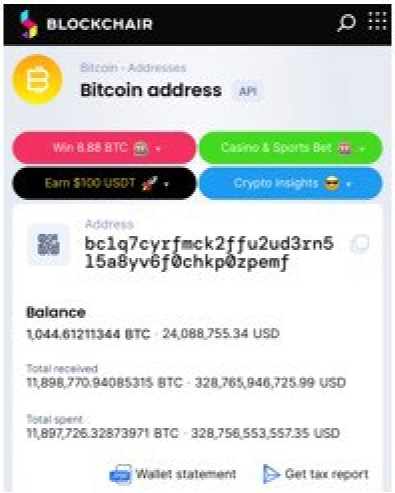
Format	P2WPKH_V0
Balance	1046.78710456 BTC
Balance Value	$ 24,124,130.00
Total Received	11,898,672.56755871 BTC
Total Sent	11,897,625.78045415 BTC
Tx Count	1,067,060
Other Explorers	BLOCKCHAIR



RECEIVED
420,948.78824834 BTC

SENT
419,903.92427053 BTC

BALANCE
1,044.61211344 BTC
(-0.25186437 BTC UNCONFIRMED)



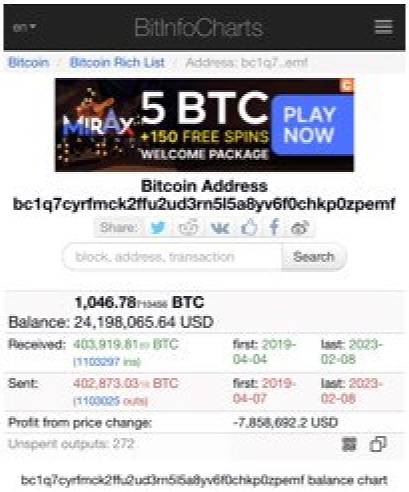
Bitcoin address API

Address
bc1q7cyrfmck2ffu2ud3rn5l5a8yv6f0chkp0zpemf

Balance
1,044.61211344 BTC · 24,088,755.34 USD

Total received
11,898,770.94085315 BTC · 328,765,946,725.99 USD

Total spent
11,897,726.32873971 BTC · 328,756,553,557.35 USD



en
BitInfoCharts
Bitcoin / Bitcoin Rich List / Address: bc1q7...emf
MIRAX 5 BTC +150 FREE SPINS WELCOME PACKAGE PLAY NOW
Share:
block, address, transaction
Search

Bitcoin Address
bc1q7cyrfmck2ffu2ud3rn5l5a8yv6f0chkp0zpemf

1,046.78710456 BTC
Balance: 24,198,065.64 USD

Received:	403,919.81[illegible] BTC (1103297 ins)	first: 2019-04-04	last: 2023-02-08
Sent:	402,873.03[illegible] BTC (1103025 outs)	first: 2019-04-07	last: 2023-02-08
Profit from price change:		-7,858,692.2 USD	
Unspent outputs: 272			

bc1q7cyrfmck2ffu2ud3rn5l5a8yv6f0chkp0zpemf balance chart