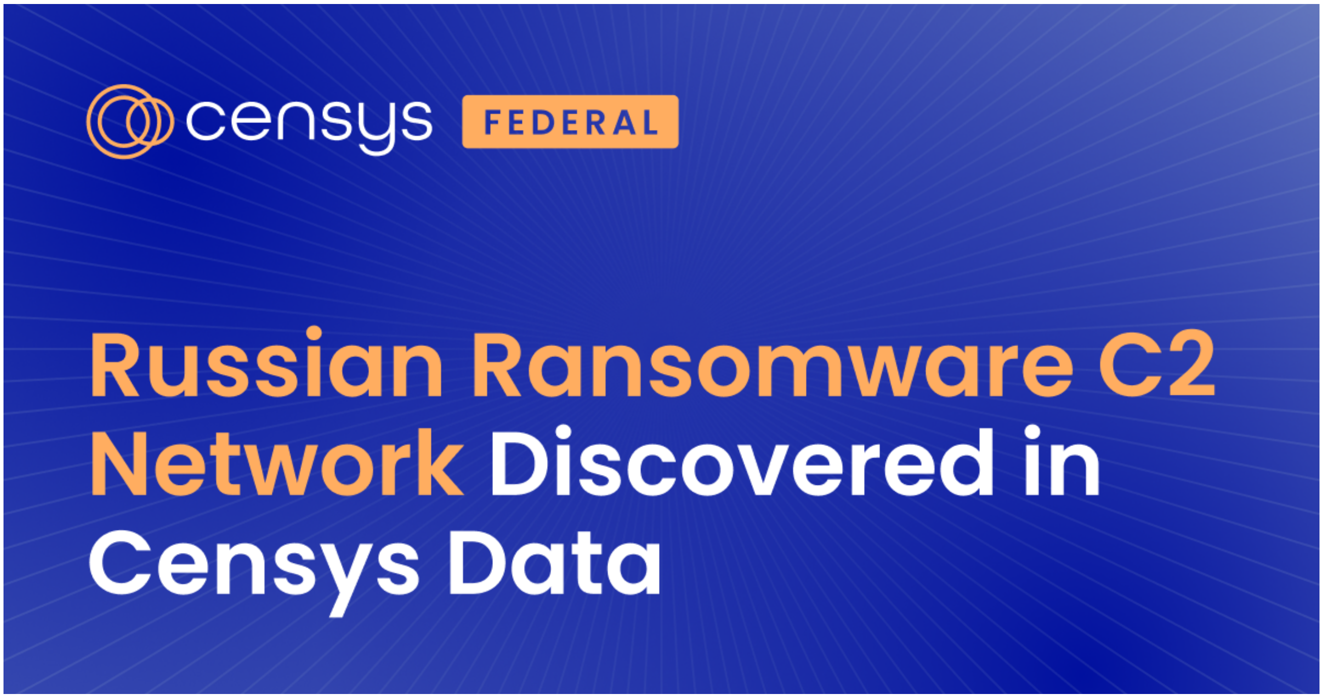
Russian Ransomware C2 Network Discovered in Censys Data

censys.com/russian-ransomware-c2-network-discovered-in-censys-data/

July 21, 2022



Around June 24 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 U.S., 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.

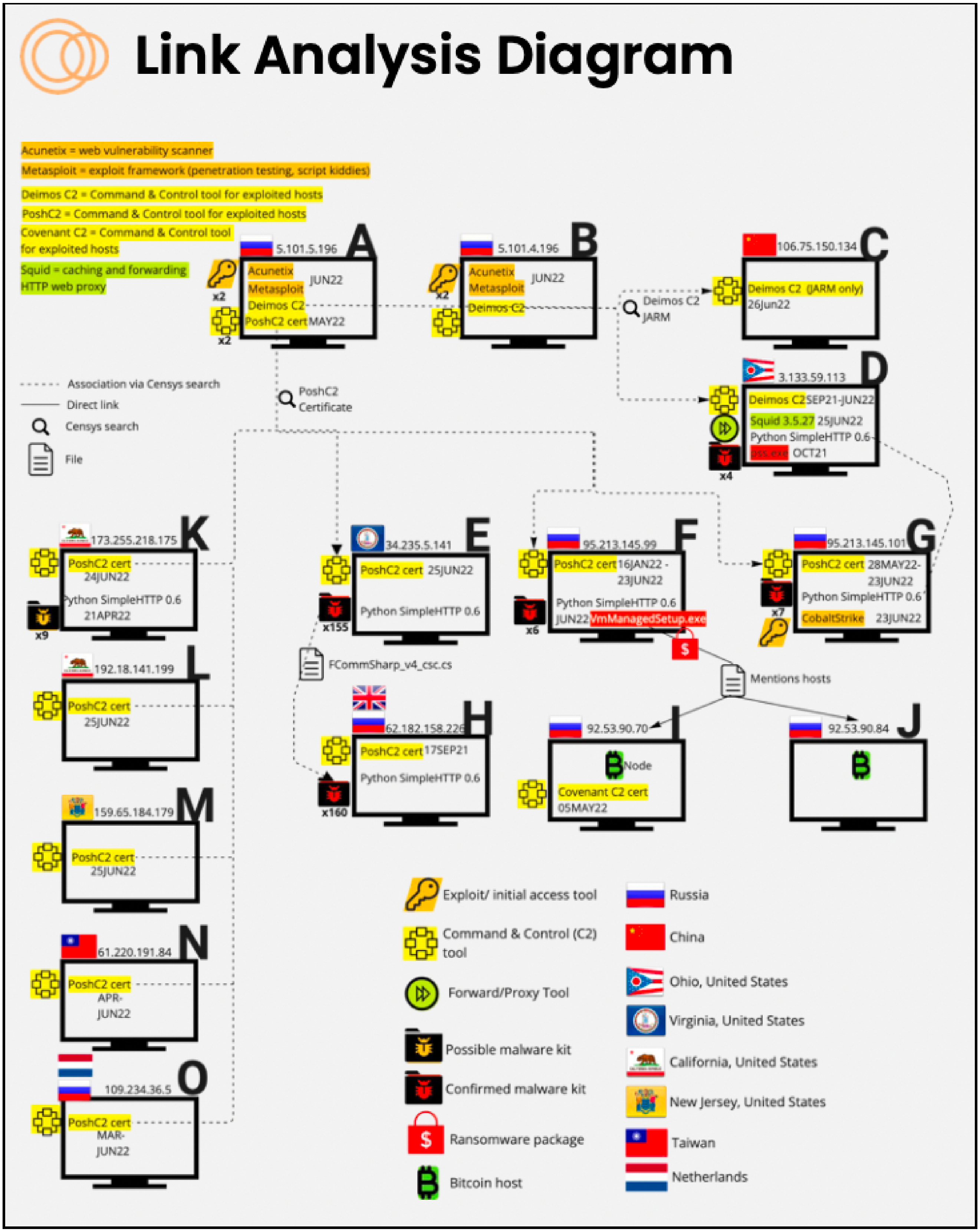
Assessment

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.

Below, you can find the Link Analysis Diagram, as well as excerpts from the report on Hosts F & G; you can find the whole report here.



Software search in Russia and Metasploit discovery

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.

See it for yourself — Run this query:

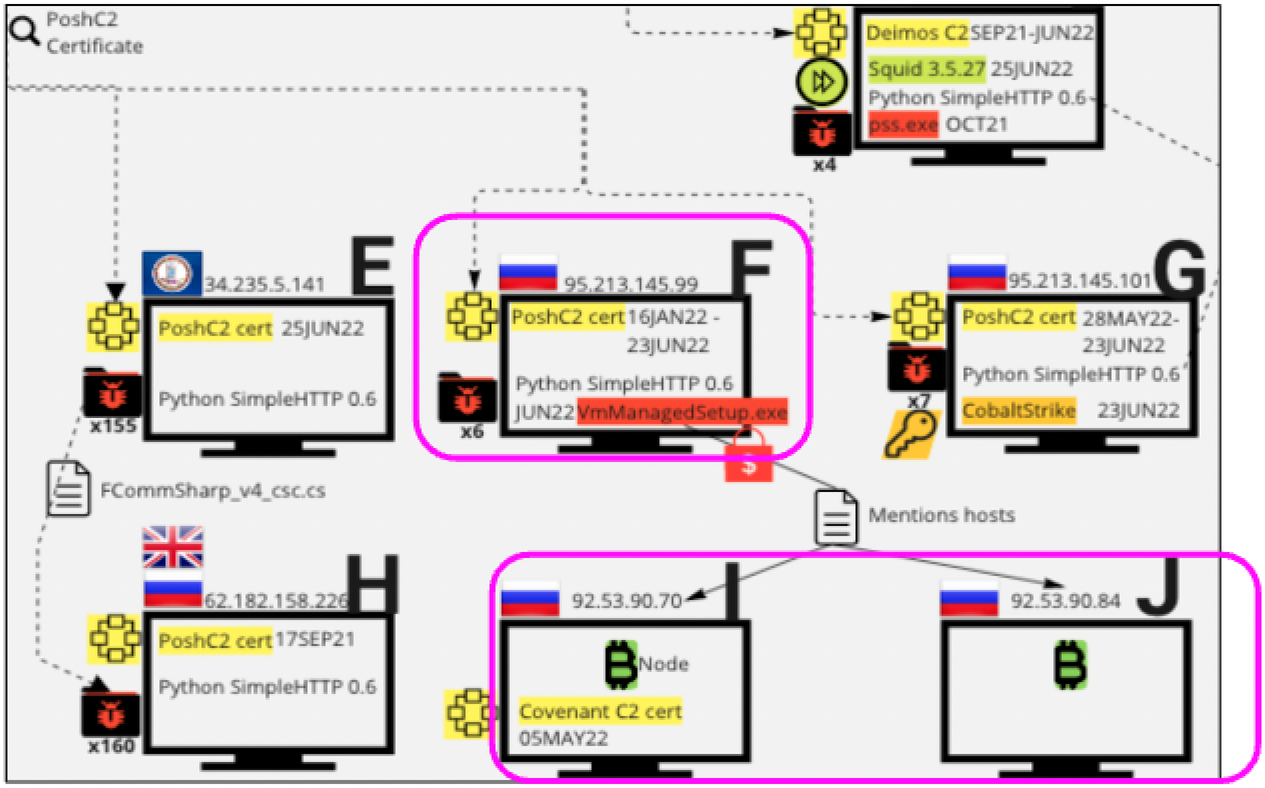
(location.country= `Russia`) and services.software.product=`Metasploit`

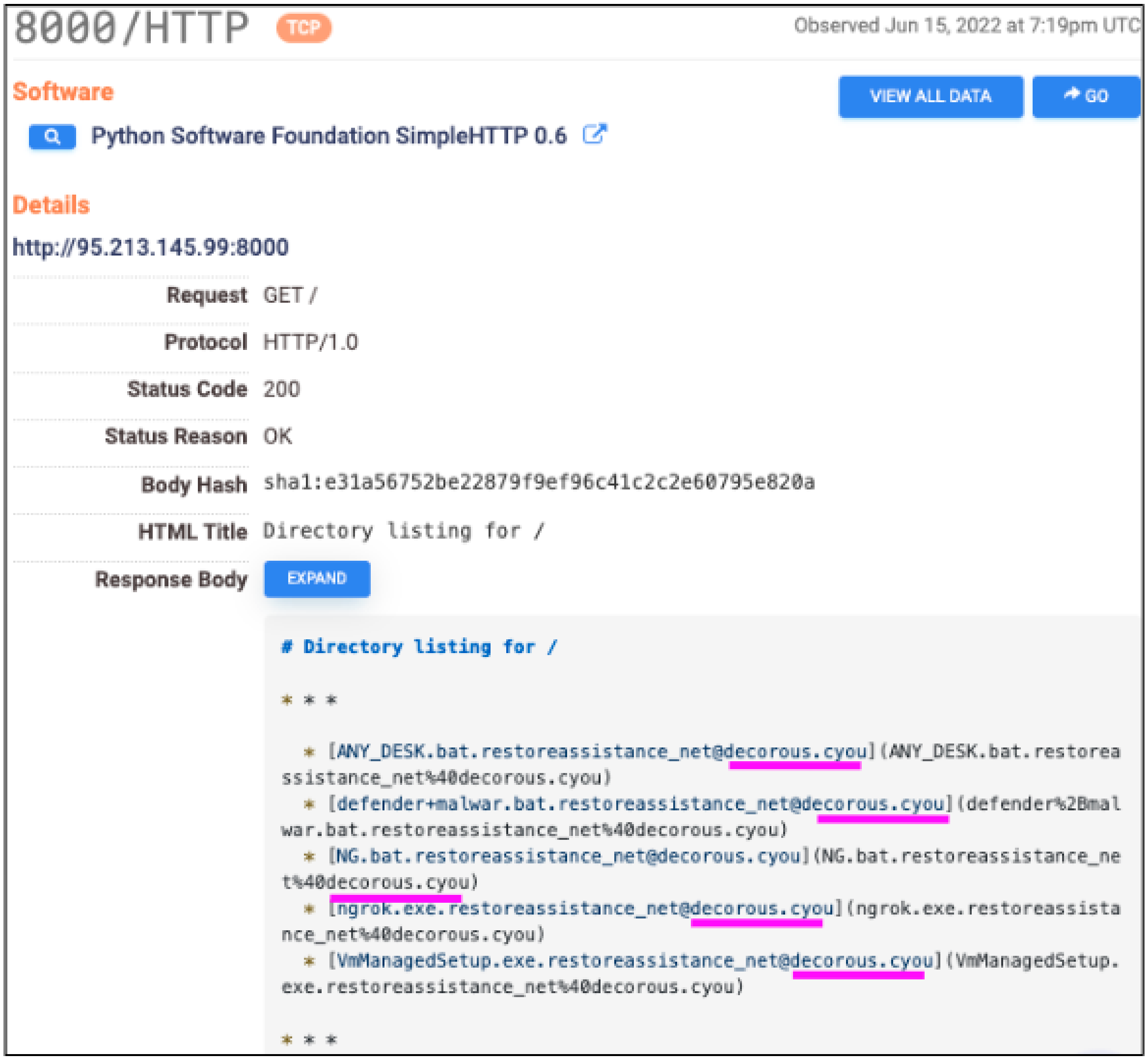
Russian Host F with Posh C2

Host F was presenting the PoshC2 HTTP response and certificate as recently as June 22, 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 July 7, 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 May 5, 2022. A full malware analysis of the kit found on Host F can be found in Appendix A (in the full report).

Through a historical analysis of the malware kit on port 8000, Censys discovered that on June 15, 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).


PoshC2
Certificate
Deimos C2 SEP21-JUN22
Squid 3.5.27 25JUN22
Python SimpleHTTP 0.6
pss.exe OCT21
x4
34.235.5.141
E
PoshC2 cert 25JUN22
Python SimpleHTTP 0.6
x155
95.213.145.99
F
PoshC2 cert 16JAN22 - 23JUN22
Python SimpleHTTP 0.6
JUN22 VmManagedSetup.exe
x6
95.213.145.101
G
PoshC2 cert 28MAY22- 23JUN22
Python SimpleHTTP 0.6
CobaltStrike 23JUN22
x7
FCommSharp_v4_csc.cs
Mentions hosts
62.182.158.226
H
PoshC2 cert 17SEP21
Python SimpleHTTP 0.6
x160
92.53.90.70
I
Node
Covenant C2 cert
05MAY22
92.53.90.84
J



8000/HTTP TCP Observed Jun 15, 2022 at 7:19pm UTC

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

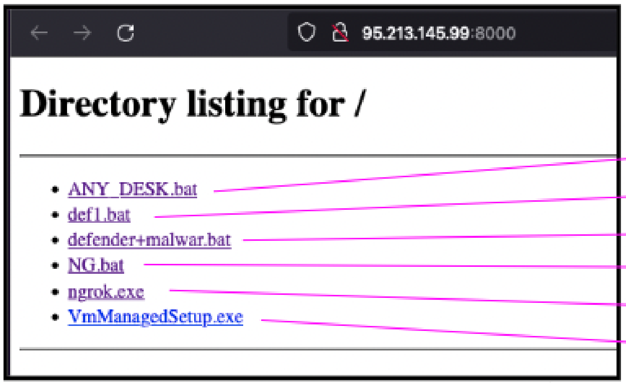
```
# Directory listing for /

* * *

  * [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

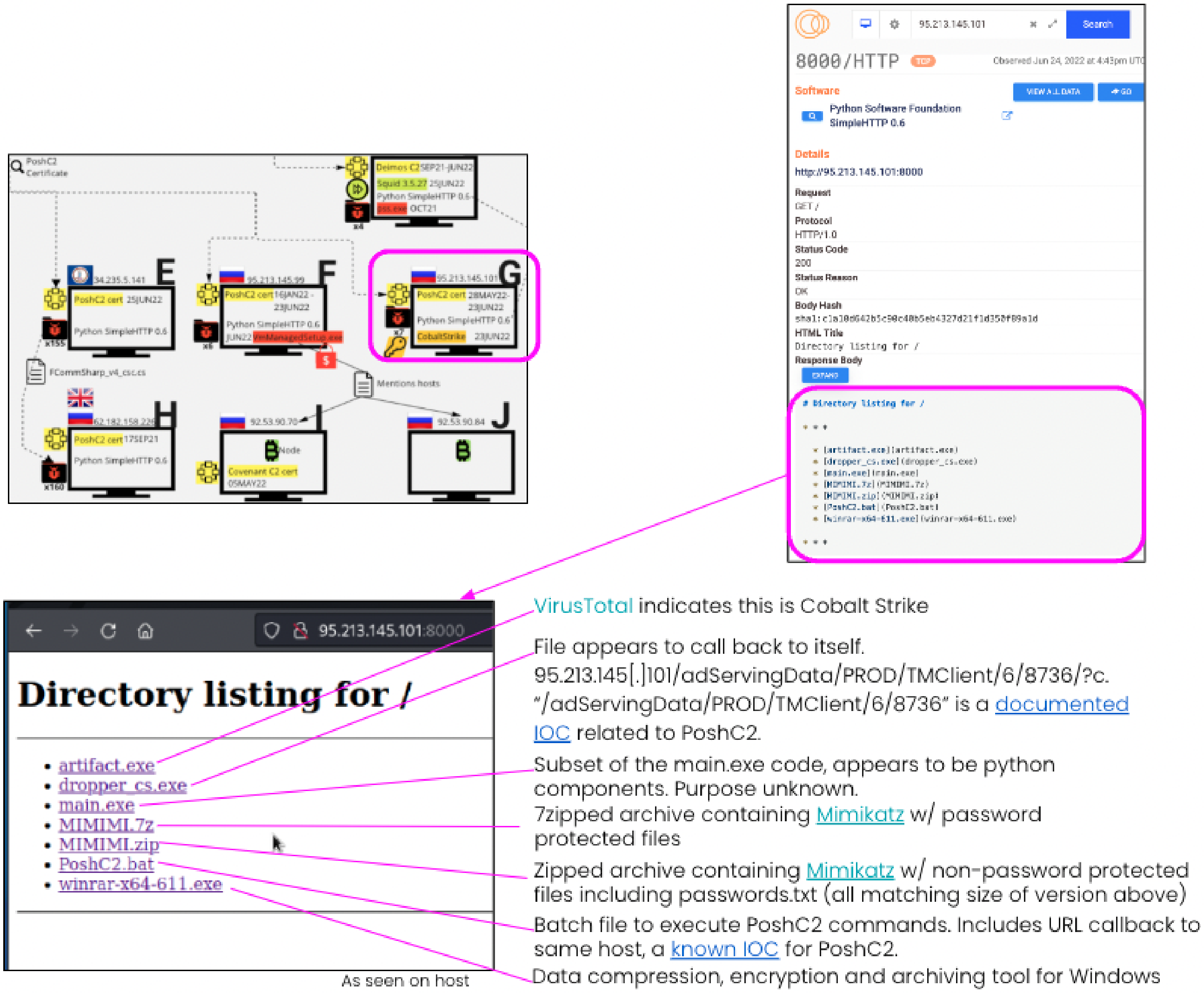
Trojan (Virus Total). Callback to Bitcoin Hosts I & J

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 in the full report.



95.213.145.101 Search

8000/HTTP TCP Observed Jun 24, 2022 at 4:43pm UTC

Software VIEW ALL DATA GO

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:c1a10d642b5c90c40b5eb4327d21f1d350f09a1d

HTML Title
Directory listing for /

Response Body
EXPAND

```
# 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

To review the full report as well as the steps to proactively hunting ransomware, you can access it below (no email required). If you’d like to reach out to the Censys team, you can email us at federal@censys.io.

Download the Report

About the Author

Matt Lembright

Director of Federal Applications

Matt Lembright is the Director of Federal Applications at Censys. Matt has been in cybersecurity for over 11 years, starting in the Army as an intelligence officer, helping build the Army Cyber Opposing Forces and USCYBERCOM’s Cyber Mission Forces.