THROUGH THE EYES OF A RESEARCHER: USING THREAT INTELLIGENCE TO COMBAT THE ADVERSARIES

WILL THOMAS

SECURITY RESEARCHER

TLP:WHITE ○

TLP:GREEN ▨

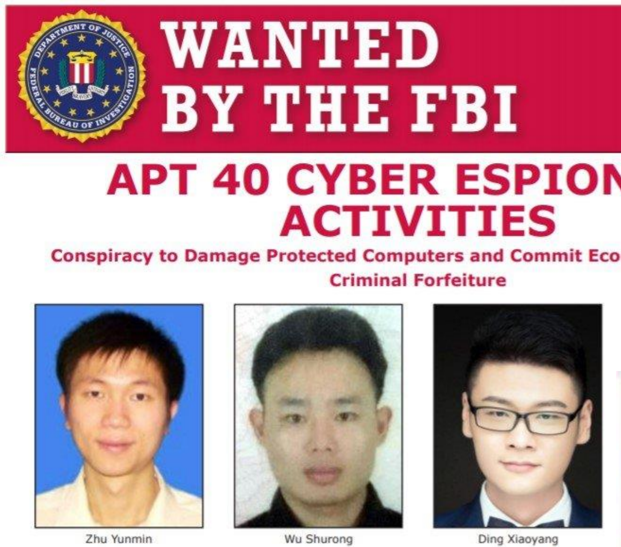
TLP:AMBER ▨

TLP:RED ▨

WHAT IS CTI? LIKE CIA, BUT FOR COMPANIES

CENTRAL INTELLIGENCE AGENCY
CIA
CENTRAL INTELLIGENCE AGENCY
CENTRAL INTELLIGENCE AGENCY
CENTRAL INTELLIGENCE AGENCY

CTI – TRACKING ESPIONAGE & CYBERCRIME



WANTED BY THE FBI

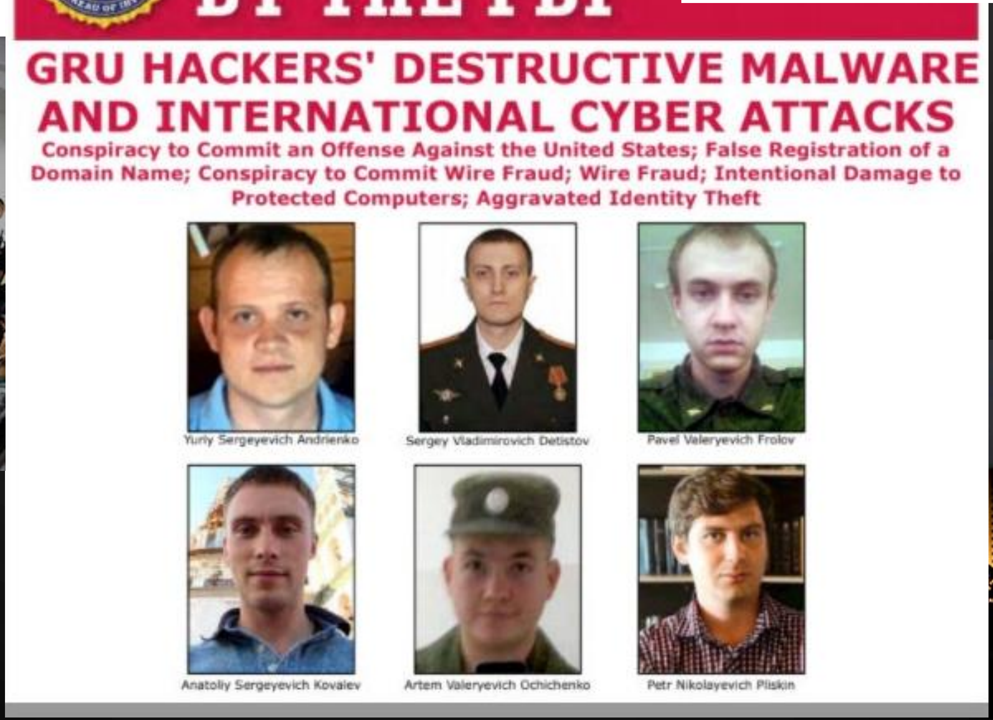
APT 40 CYBER ESPIONAGE ACTIVITIES

Conspiracy to Damage Protected Computers and Commit Economic Espionage; Criminal Forfeiture

Zhu Yunmin

Wu Shurong

Ding Xiaoyang



WANTED BY THE FBI

GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS

Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft

Yuriy Sergeyevich Andrienko

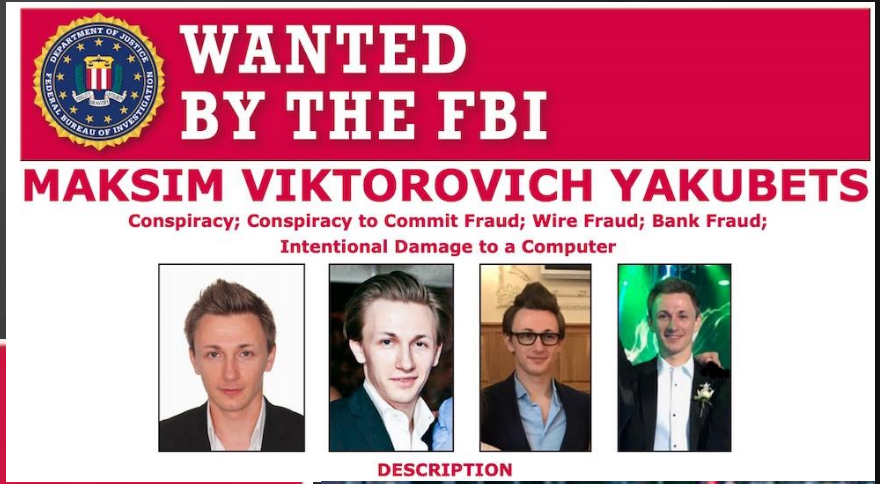
Sergey Vladimirovich Detistov

Pavel Valeryevich Frolov

Anatoliy Sergeyevich Kovalev

Artem Valeryevich Ochichenko

Petr Nikolayevich Pliskin



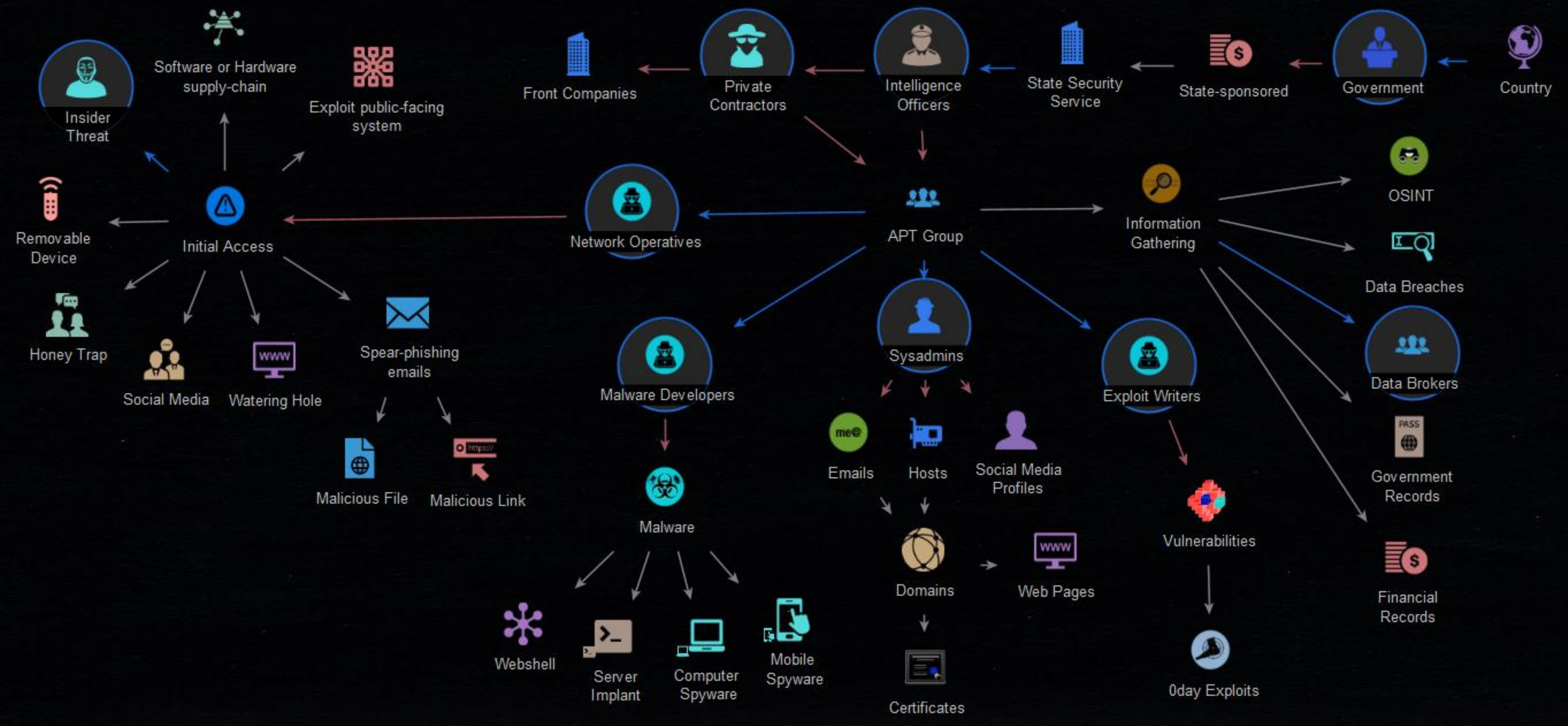
WANTED BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

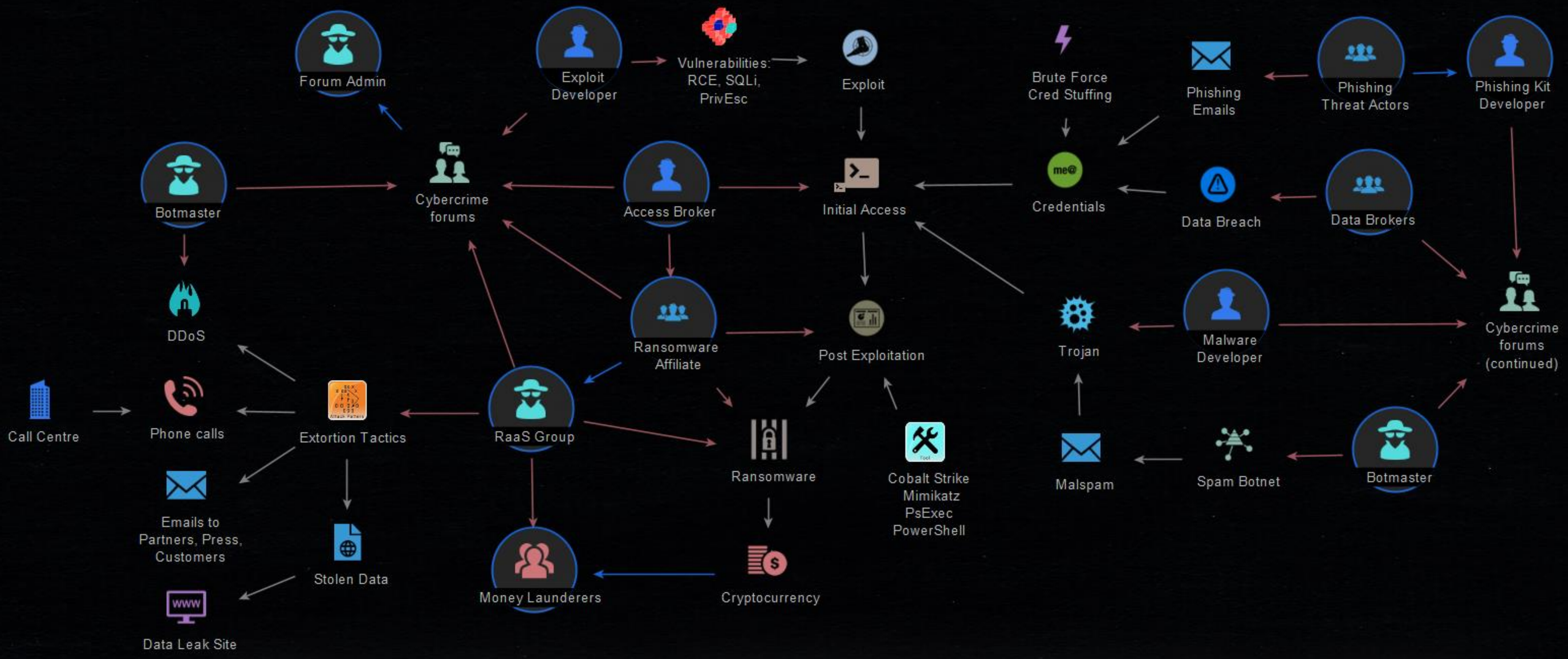
Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer

DESCRIPTION

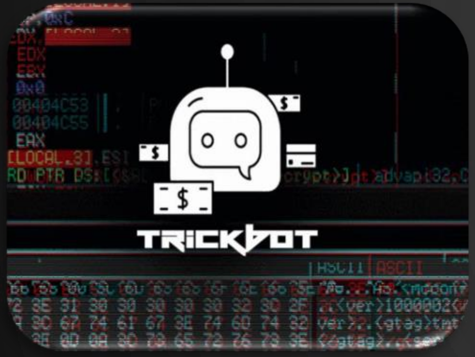
ESPIONAGE - APT29, APT10, APT35



CYBERCRIME – REVIL, CONTI, LOCKBIT



CYBERCRIME – THE REST OF IT



11:29

+1 (760) 963-4579

Text Message
Yesterday 3:30 PM

Hello mate, your FEDEX package with tracking code GB-6412-GH83 is waiting for you to set delivery preferences: c1cor.info/[illegible]

JokerStash
Vendor of:
Dumps
CVV Seller

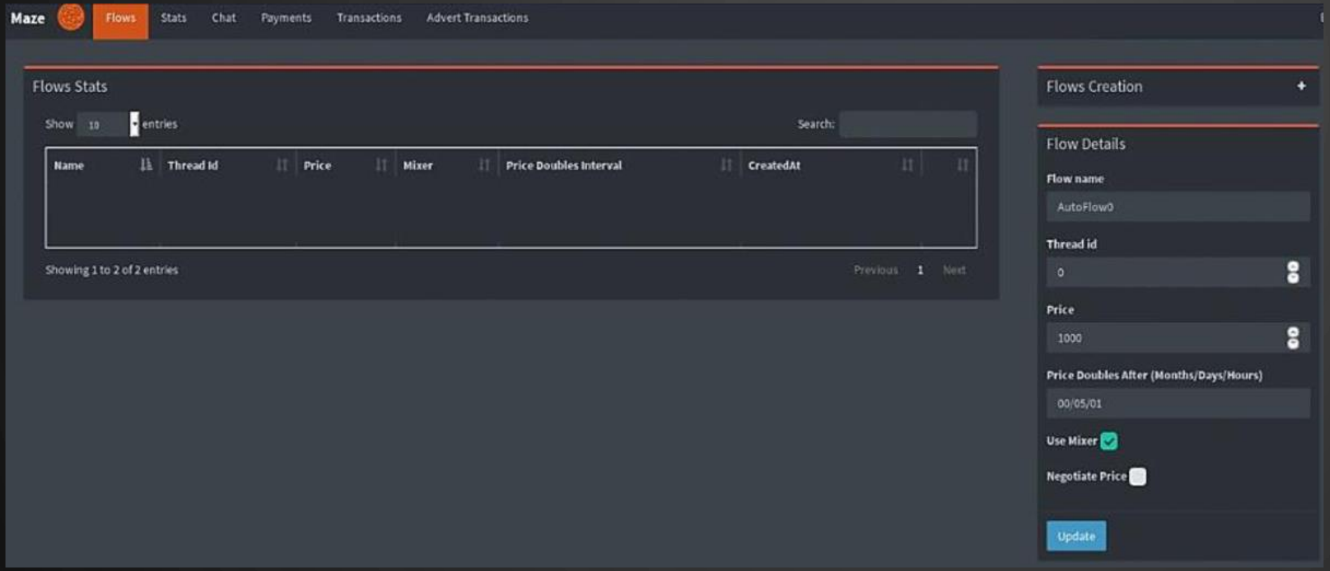
Join Date: Mar 2017

Posts: 6,392

Reputation: 385 (+/-)

Balance: 0.00$

DARKNET/FORUMS - RAAS, MAAS, IAB



Flows Stats

Show 10 entries Search:

Name	Thread Id	Price	Mixer	Price Doubles Interval	CreatedAt	

Showing 1 to 2 of 2 entries Previous 1 Next

Flows Creation +

Flow Details

Flow name: AutoFlow0

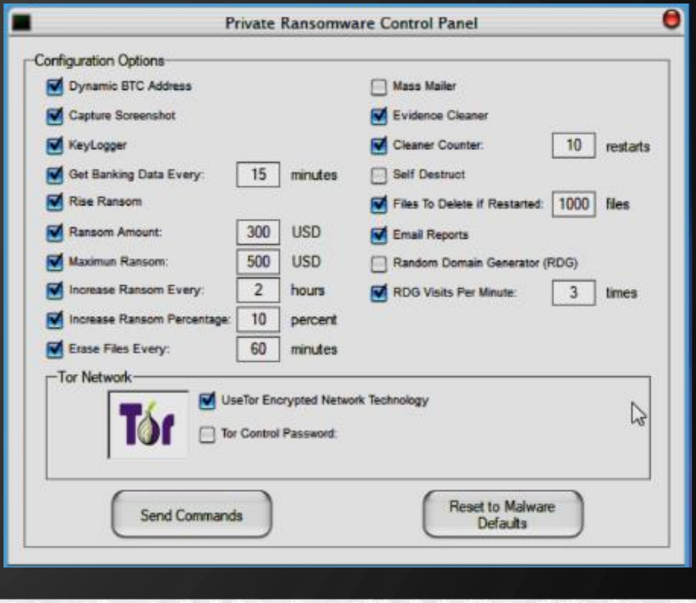
Thread id: 0

Price: 1000

Price Doubles After (Months/Days/Hours): 00/05/01

Use Mixer ☑

Negotiate Price □

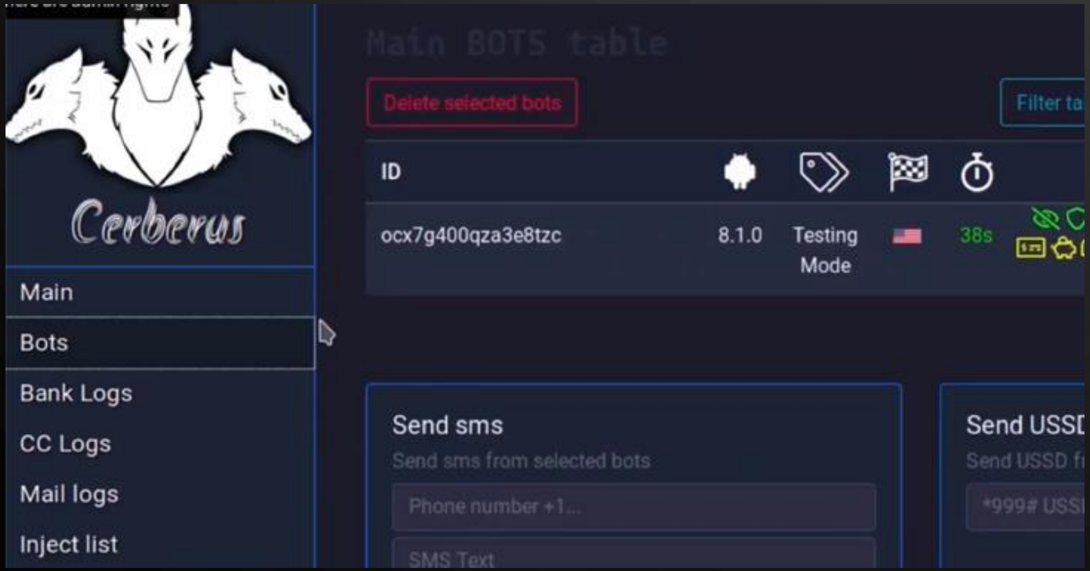


Configuration Options

- ☑ Dynamic BTC Address
- ☑ Capture Screenshot
- ☑ KeyLogger
- ☑ Get Banking Data Every: 15 minutes
- ☑ Rise Ransom
- ☑ Ransom Amount: 300 USD
- ☑ Maximun Ransom: 500 USD
- ☑ Increase Ransom Every: 2 hours
- ☑ Increase Ransom Percentage: 10 percent
- ☑ Erase Files Every: 60 minutes
- □ Mass Mailer
- ☑ Evidence Cleaner
- ☑ Cleaner Counter: 10 restarts
- □ Self Destruct
- ☑ Files To Delete if Restarted: 1000 files
- ☑ Email Reports
- □ Random Domain Generator (RDG)
- ☑ RDG Visits Per Minute: 3 times

Tor Network

- ☑ UseTor Encrypted Network Technology
- □ Tor Control Password:



Main BOTS table

ID				
ocx7g400qza3e8tzc	8.1.0	Testing Mode		38s

Send sms

Send sms from selected bots

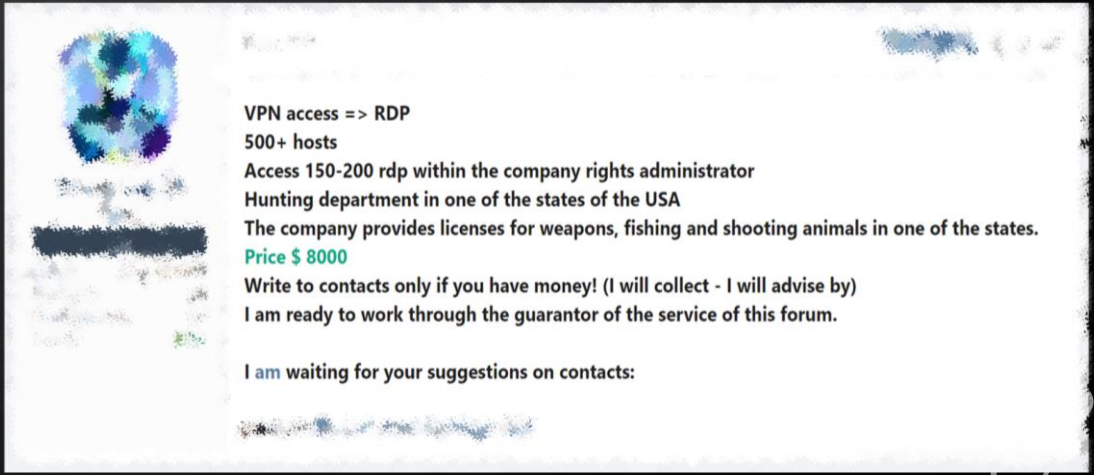
Phone number +1...

SMS Text

Send USSD

Send USSD f

*999# USS



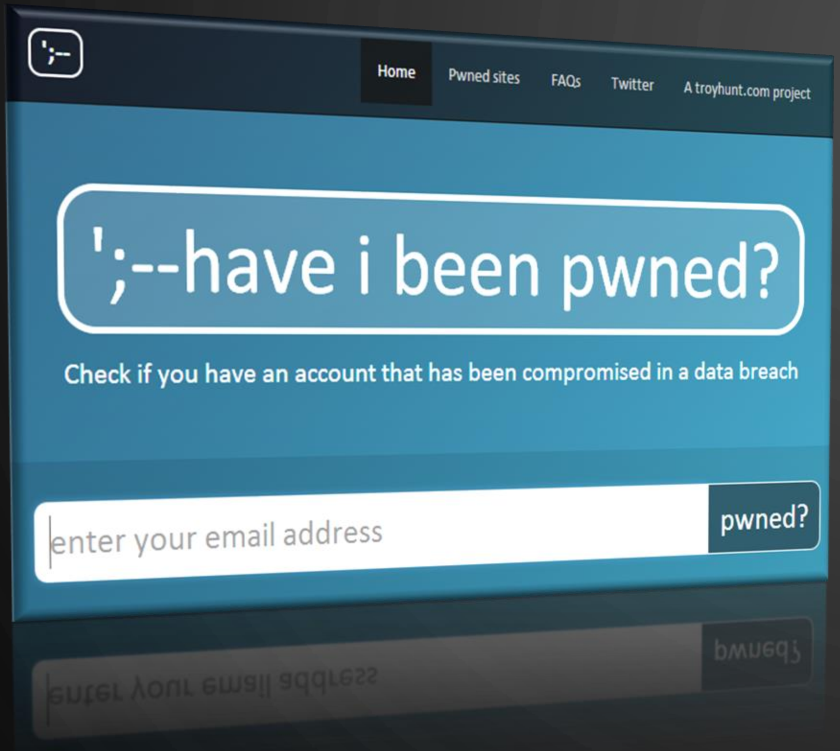
[redacted]

VPN access => RDP
500+ hosts
Access 150-200 rdp within the company rights administrator
Hunting department in one of the states of the USA
The company provides licenses for weapons, fishing and shooting animals in one of the states.
Price $ 8000
Write to contacts only if you have money! (I will collect - I will advise by)
I am ready to work through the guarantor of the service of this forum.

I am waiting for your suggestions on contacts:

[redacted]

DATA BREACHES



Home | Pwned sites | FAQs | Twitter | A troyhunt.com project

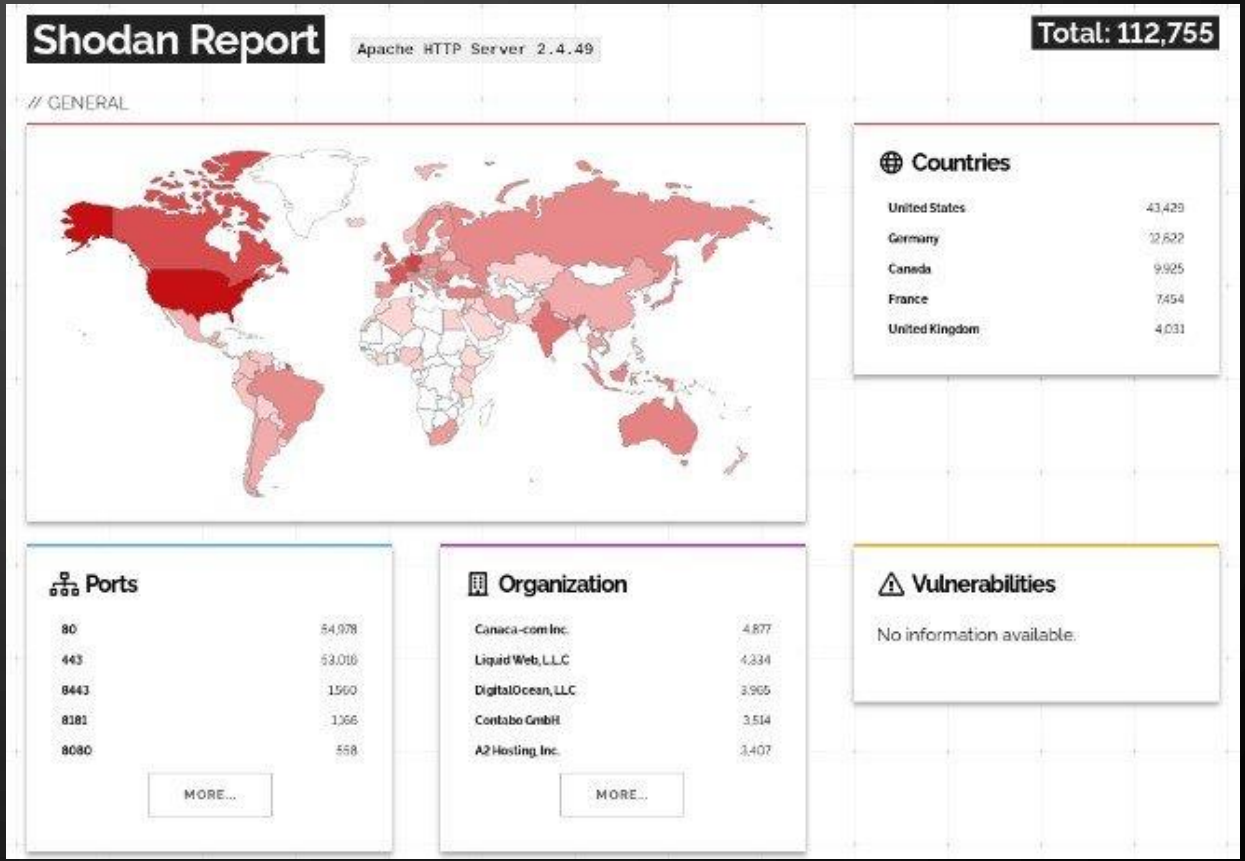
';--have i been pwned?

Check if you have an account that has been compromised in a data breach

enter your email address | pwned?

Empire Market
Due to on-going DDOS attacks against our servers, you must complete a captcha challenge to prove you are human.
VERIFY

0DAY VULNERABILITIES AND EXPLOITS



Shodan Report Apache HTTP Server 2.4.49 **Total: 112,755**

// GENERAL

Countries

United States	43,429
Germany	12,622
Canada	9,925
France	7,454
United Kingdom	4,031

Ports

80	54,978
443	53,016
8443	1,560
8181	1,066
8080	558

MORE...

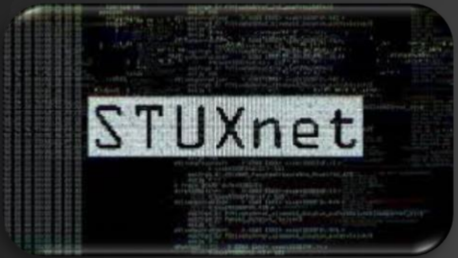
Organization

Canaca-com Inc.	4,877
Liquid Web, L.L.C	4,334
DigitalOcean, LLC	3,965
Contabo GmbH	3,514
A2 Hosting, Inc.	3,407

MORE...

Vulnerabilities

No information available.



BIGGEST INCIDENTS

Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.
We continue till our request be met.
We've obtained all your internal data including your secrets and top secre
If you don't obey us, we'll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Data Link :
https://www.sonypicturesstockfootage.com/SPEData.zip
http://dmiplaewh36.spe.sony.com/SPEData.zip
http://www.ntcnt.ru/SPEData.zip
http://www.thammasatpress.com/SPEData.zip
http://moodle.universidadebematech.com.br/SPEData.zip

- Sony Pictures, Bangladesh Bank Heist, WannaCry
- NotPetya, BadRabbit, Olympic Destroyer
- Democratic National Committee, World Anti-Doping Authority
- Industroyer, BlackEnergy, Triton, Stuxnet
- Shamoon
- SolarWinds, ProxyLogon, Colonial Pipeline, Kaseya, PolyNetwork (just in 2021!)

Ooops, your files have been encrypted!

English

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   [illegible]

If you already purchased your key, please enter it below.
Key: _
```

DUTY OF A CTI RESEARCHER: SIMPLIFIED

CTI TOOLS

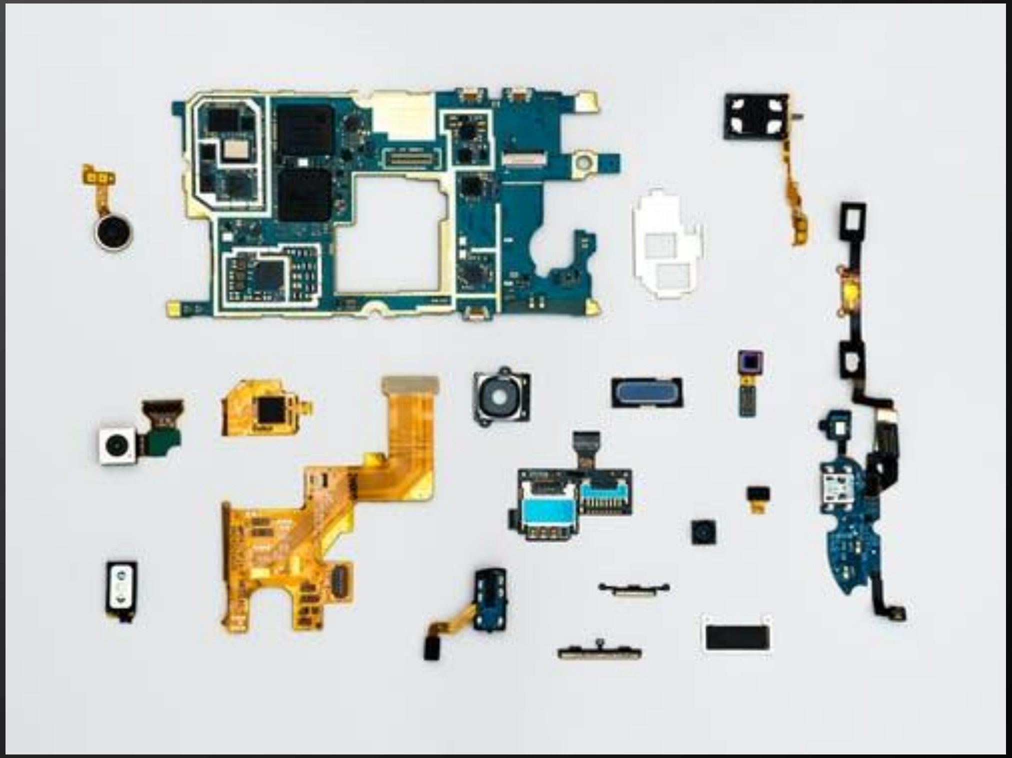
- VirusTotal, AnyRun, URLscan, Shodan, OTX AlienVault, APKLab, Maltego, Twitter

The search engine for the Web

Shodan is the world's first search engine for Internet-connected devices.

IOC, TTP, IOA

- Indicators of Compromise
- Tactics, Techniques, and Procedures
- Indicators of Attack (New)



SCENARIO PART I

- At one time, a user work station connected to 5 different IP addresses in 5 different countries. What does the SOC do?
- They isolate the device, check netflow history of the device and others on the network, nature of the traffic (which port), device context (user privileges), check what was it doing before it reached out to the Ips
- Collection -> Analysis -> Judgement -> Action

SCENARIO PART II

- What can CTI provide about these IP addresses?
- Use open sources/paid sources e.g. VirusTotal, AbuseIPDB, IPinfo, URLscan, AnyRun, OTX, Abuse.ch, or Shodan
- Find out the owner, the type of system, its previous activity, files contacting the IP, URLs on the IP, domains on the IP, the IPs ports, running services
- Do these overlap with any known threats e.g. APTs, malware families
- Share related TTPs, campaigns, objectives, and impact

THREAT INTELLIGENCE PLATFORMS

ANOMALI

CYJAX

digital shadows_

ADVINTEL

Recorded Future

INTEL471

KELA

FLASHPOINT

SpyCloud

CTI-AS-A-SERVICE

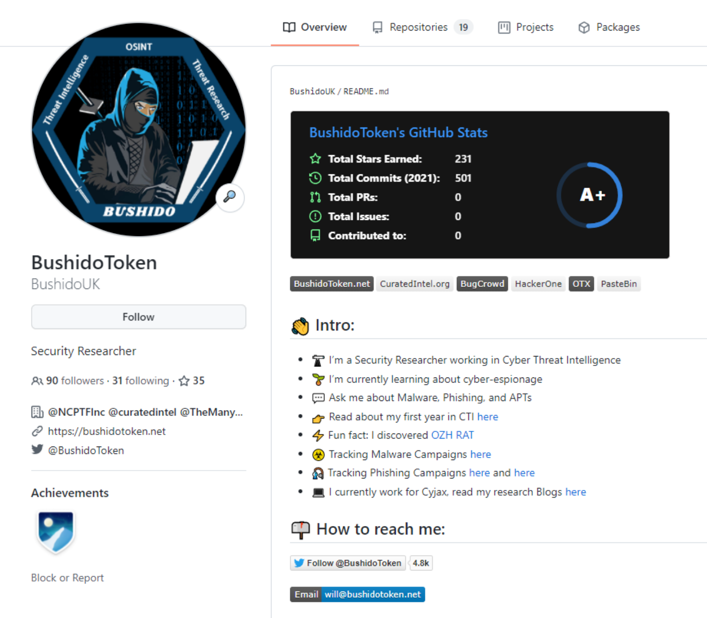
VENDOR VS ORGANISATION

CTI-AS-A-SERVICE,
CONSULTANTS,
RESEARCHERS

FORTUNE 1000,
PUBLIC SECTOR,
CRITICAL INFRASTRUCTURE

HOW TO GET INTO THE INDUSTRY

- Create a Blog and GitHub page
- Be active in the community (Twitter, LinkedIn, Discord, Slack)
- Attend Virtual Conferences
- Practice OSINT
- Always Be Learning - Listen to Podcasts & Read Books
- Do Research - I started by looking at SMS phish and phishing kits
- CTFs - TraceLabs Global Search Part OSINT CTF
- Join non-profits – I am a member of the NCPTF



BushidoToken
BushidoUK

Security Researcher

90 followers · 31 following · 35

@NCPTFInc @curatedintel @TheMany...
https://bushidotoken.net
@BushidoToken

Achievements

BushidoUK / README.md

BushidoToken's GitHub Stats

Total Stars Earned:	231
Total Commits (2021):	501
Total PRs:	0
Total Issues:	0
Contributed to:	0

A+

BushidoToken.net CuratedIntel.org BugCrowd HackerOne OTX PasteBin

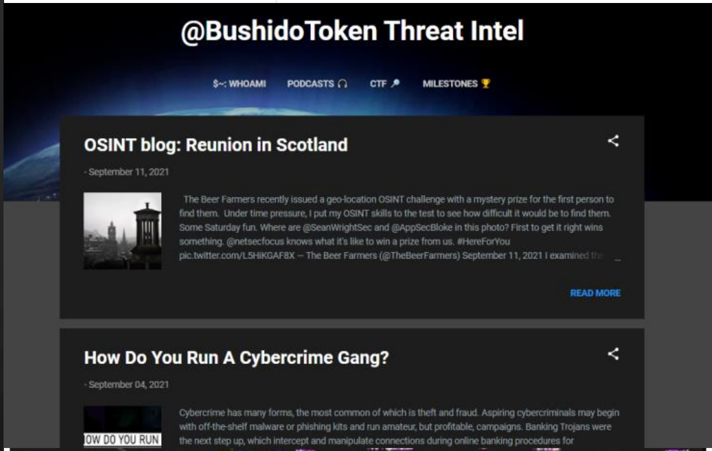
Intro:

- I'm a Security Researcher working in Cyber Threat Intelligence
- I'm currently learning about cyber-espionage
- Ask me about Malware, Phishing, and APTs
- Read about my first year in CTI here
- Fun fact: I discovered OZH RAT
- Tracking Malware Campaigns here
- Tracking Phishing Campaigns here and here
- I currently work for Cyjax, read my research Blogs here

How to reach me:

Follow @BushidoToken 4.8k

Email will@bushidotoken.net



@BushidoToken Threat Intel

OSINT blog: Reunion in Scotland

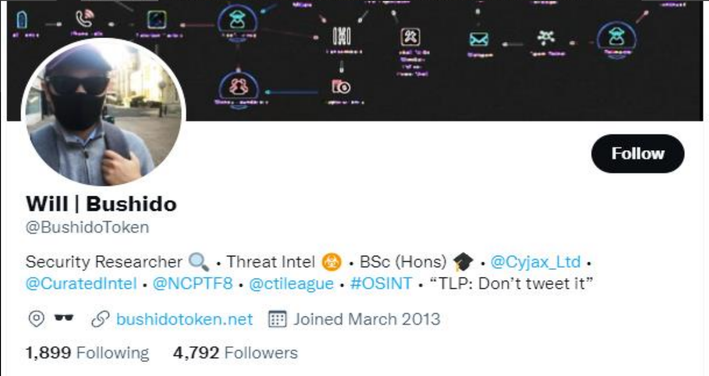
- September 11, 2021

The Beer Farmers recently issued a geo-location OSINT challenge with a mystery prize for the first person to find them. Under time pressure, I put my OSINT skills to the test to see how difficult it would be to find them. Some Saturday fun. Where are @SeanWrightSec and @AppSecBloke in this photo? First to get it right wins something. @netsecfocus knows what it's like to win a prize from us. #HereForYou pic.twitter.com/L5HIKGAF8X — The Beer Farmers (@TheBeerFarmers) September 11, 2021 I examined th

How Do You Run A Cybercrime Gang?

- September 04, 2021

Cybercrime has many forms, the most common of which is theft and fraud. Aspiring cybercriminals may begin with off-the-shelf malware or phishing kits and run amateur, but profitable, campaigns. Banking Trojans were the next step up, which intercept and manipulate connections during online banking procedures for



Will | Bushido
@BushidoToken

Security Researcher · Threat Intel · BSc (Hons) · @Cyjax_Ltd · @CuratedIntel · @NCPTF8 · @ctileague · #OSINT · "TLP: Don't tweet it"

bushidotoken.net Joined March 2013

1,899 Following 4,792 Followers

THANK YOU

twitter.com/@BushidoToken

github.com/BushidoUK

bushidotoken.net