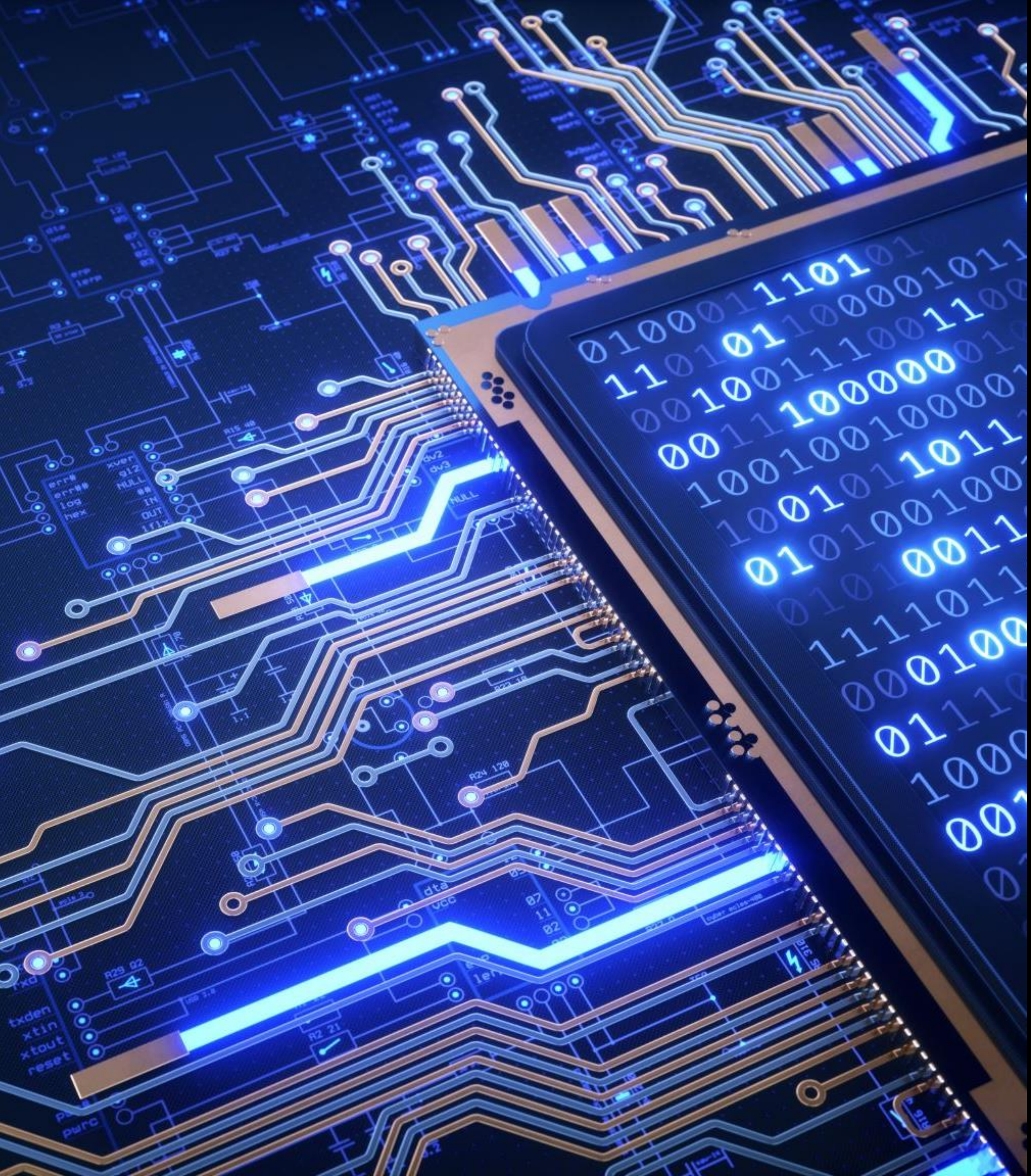
The Dynamic Duo: When Russian and Western Cybercriminals Combine

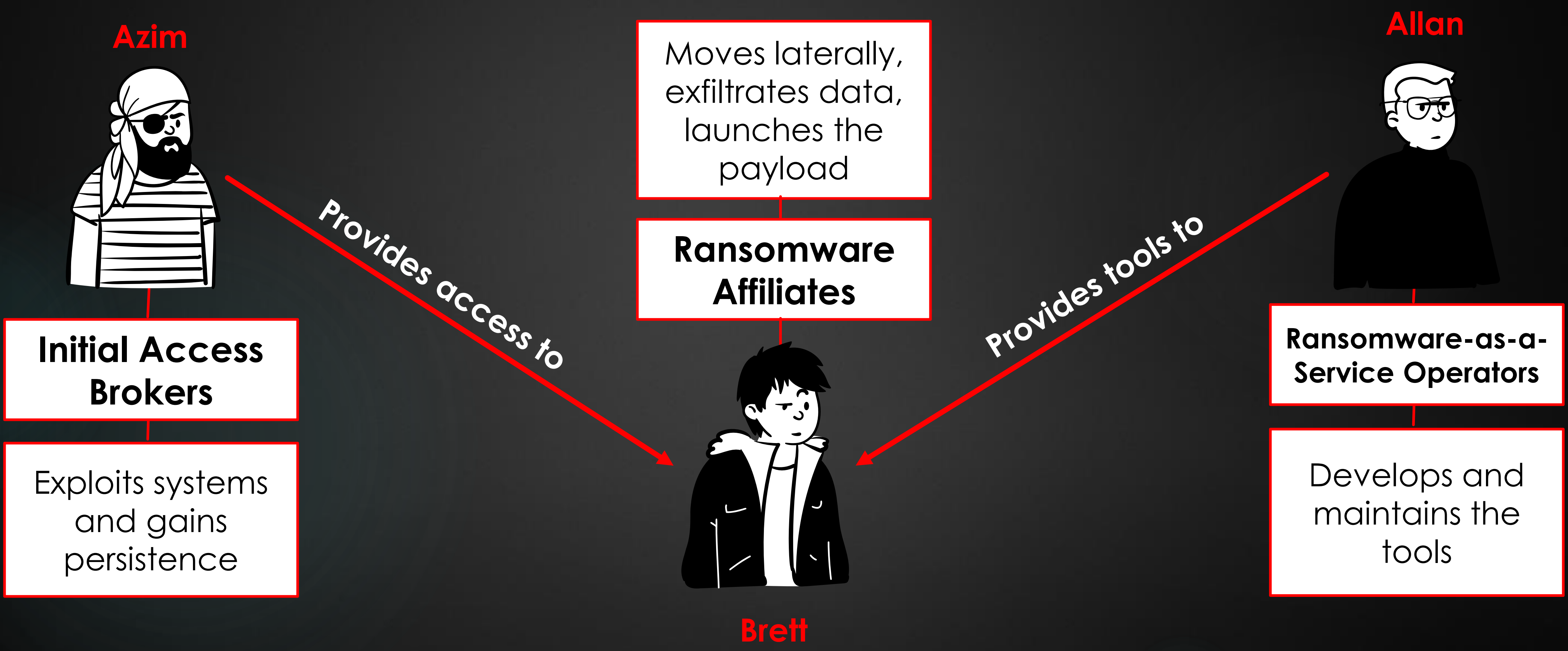
BY WILL THOMAS



~$whoami

- Cyber Threat Intelligence Researcher for Equinix
- Co-author SANS FOR589: Cybercrime Intelligence
- Co-founder Curated Intelligence trust group

The Ransomware Gig Economy



Azim

Initial Access Brokers

Exploits systems and gains persistence

Provides access to

Moves laterally, exfiltrates data, launches the payload

Ransomware Affiliates

Brett

Provides tools to

Allan

Ransomware-as-a-Service Operators

Develops and maintains the tools

Comparing Western and Russian Cybercriminals

- English-speaking threat actors that launch cyberattacks
  - Like **Arion Kurtaj** from Lapsus$
- Russian-speaking threat actors that run cybercriminal services
  - Like **Maksim Yakubets** from EvilCorp

Gamers and bored adolescents

Professional criminals

Introduction of the Western Cybercriminals

Known as Scattered Spider (aka 0ktapus, UNC3944, Storm-0875)

- Native-level English-speakers – but it’s not certain which country
  - Based on their voices during phone calls
- They share a lot of techniques with the underground account hacking and selling community – they likely evolved from there
- Such as:
  - SMS-based credential phishing
  - Social engineering victims over the phone (aka voice phishing/vishing)
  - SIM swapping (social engineering mobile provider IT people)

Beware of SIM swapping

- **Kroll breach:**
  - "a cyber threat actor targeted a **T-Mobile account** belonging to a **Kroll employee** in a highly sophisticated "SIM swapping" attack.
  - Specifically, T-Mobile, without any authority from or contact with Kroll or its employee, transferred that employee's phone number to the **threat actor's phone** at their request.
  - As a result, it appears the threat actor gained access to certain files containing personal information of bankruptcy claimants in the matters of BlockFi, FTX and Genesis.
  - Immediate actions were taken to secure the three affected accounts. Affected individuals have been notified by email. "
- Not confirmed to be related to Scattered Spider, but a recent case study of SIM swapping in the wild

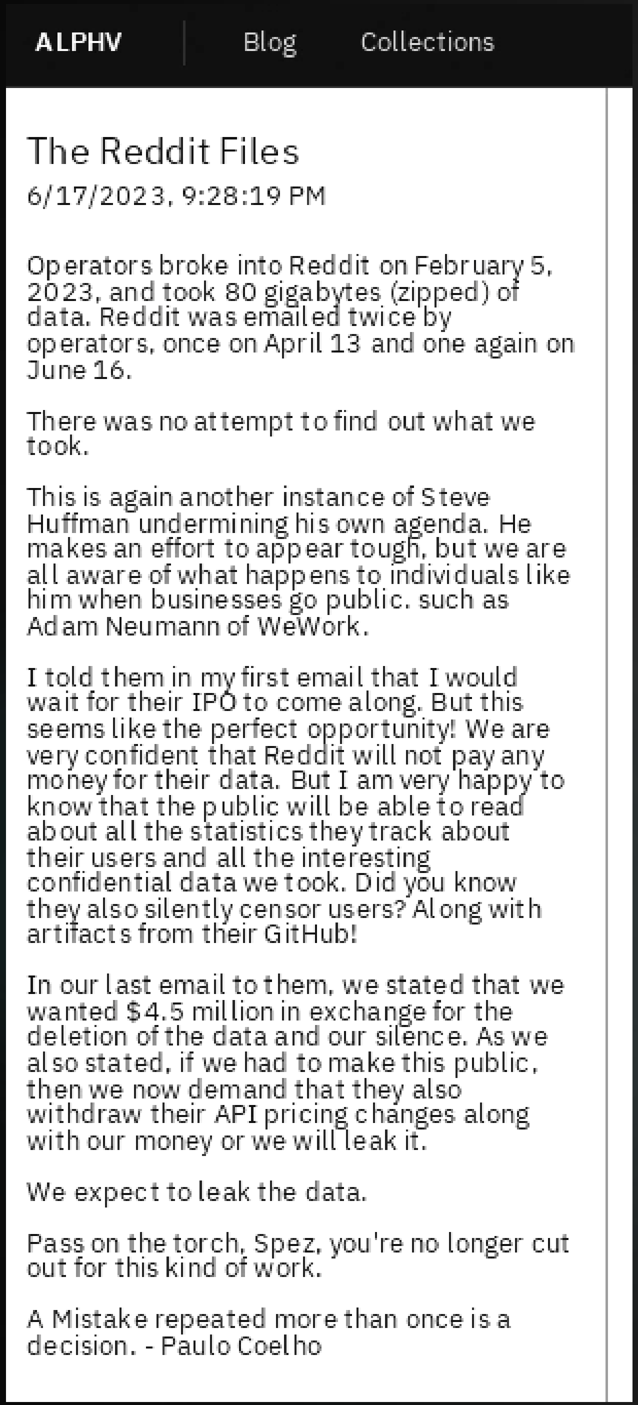
Research into Scattered Spider's well-known tradecraft

Initial Access Methods - SMS phishing text messages - Cloned Single Sign-On (SSO) portals - Phone calls and social engineering	**Credential Access Methods** - One-Time Passcode (OTP) stealing Telegram phishing kit - Multi-factor authentication (MFA) fatigue - SIM Swapping
Defense Evasion Methods - Remote Monitoring & Management Tools - Malicious Signed Drivers - Vulnerable Signed Drivers - Firmware Bootkits	**Campaign Infrastructure** - Anonymous VPNs - Single Sign-On (SSO) themed domains - Tor - Online file-sharing services

The Coinbase attacker (Feb. 2023)

Coinbase attacker TTPs	Known Scattered Spider TTPs?
SMS phishing messages	✅
Target-themed credential phishing	✅
Single Sign-On (SSO) themed domains	✅
Phone calls to harvest their credentials	✅
RMM tools (AnyDesk & ISL Online)	✅
File-sharing services (riseup.net)	✅
Third-party VPN provider (MullvadVPN)	✅

Case Study: The Reddit Attack (Feb. 2023)



The Reddit Files

6/17/2023, 9:28:19 PM

Operators broke into Reddit on February 5, 2023, and took 80 gigabytes (zipped) of data. Reddit was emailed twice by operators, once on April 13 and one again on June 16.

There was no attempt to find out what we took.

This is again another instance of Steve Huffman undermining his own agenda. He makes an effort to appear tough, but we are all aware of what happens to individuals like him when businesses go public. such as Adam Neumann of WeWork.

I told them in my first email that I would wait for their IPO to come along. But this seems like the perfect opportunity! We are very confident that Reddit will not pay any money for their data. But I am very happy to know that the public will be able to read about all the statistics they track about their users and all the interesting confidential data we took. Did you know they also silently censor users? Along with artifacts from their GitHub!

In our last email to them, we stated that we wanted $4.5 million in exchange for the deletion of the data and our silence. As we also stated, if we had to make this public, then we now demand that they also withdraw their API pricing changes along with our money or we will leak it.

We expect to leak the data.

Pass on the torch, Spez, you're no longer cut out for this kind of work.

A Mistake repeated more than once is a decision. - Paulo Coelho

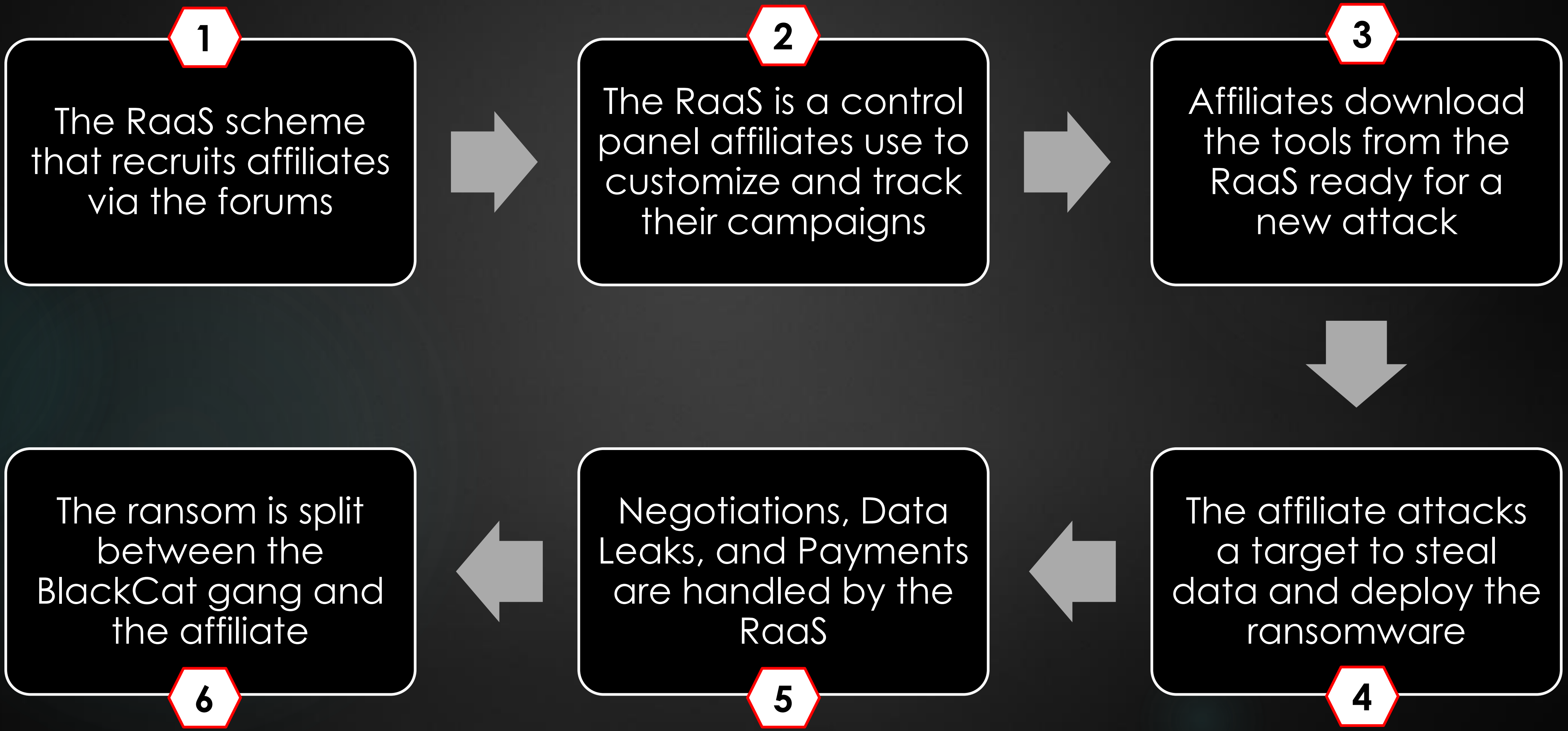
- On **5 February 2023**, Reddit experienced a data breach
- Employees were sent via SMS phishing messages
- It went to a phishing website impersonating Reddit's SSO page
- An employee's credentials and OTP were stolen
- The attacker gained access and stole internal documents and code
- On **16 June 2023**, Reddit appeared on the **ALPHV/BlackCat** data leak site
  - The attackers said they gained access on **5 February 2023**
  - They claimed they stole 80GB of files
  - They demanded a $4.5 million ransom for the deletion of data and their silence

Introduction of the Russian Cybercriminals

Known interchangeably as **BlackCat** or **ALPHV** (pronounced "Alpha")

- Confirmed Russia-based organized cybercriminals
- Known for currently running a **Ransomware-as-a-Service (RaaS)** operation with multiple of Ransomware affiliates
- Is affiliated with multiple other threat groups:
  - **DarkSide** – responsible for the Colonial Pipeline attack in July 2023 (the worst cyberattack on US critical national infrastructure in history)
  - **BlackMatter** – after the Colonial Pipeline attack, DarkSide shutdown, but came back and rebranded in November 2021

How does the BlackCat RaaS normally work?



1. The RaaS scheme that recruits affiliates via the forums

2. The RaaS is a control panel affiliates use to customize and track their campaigns

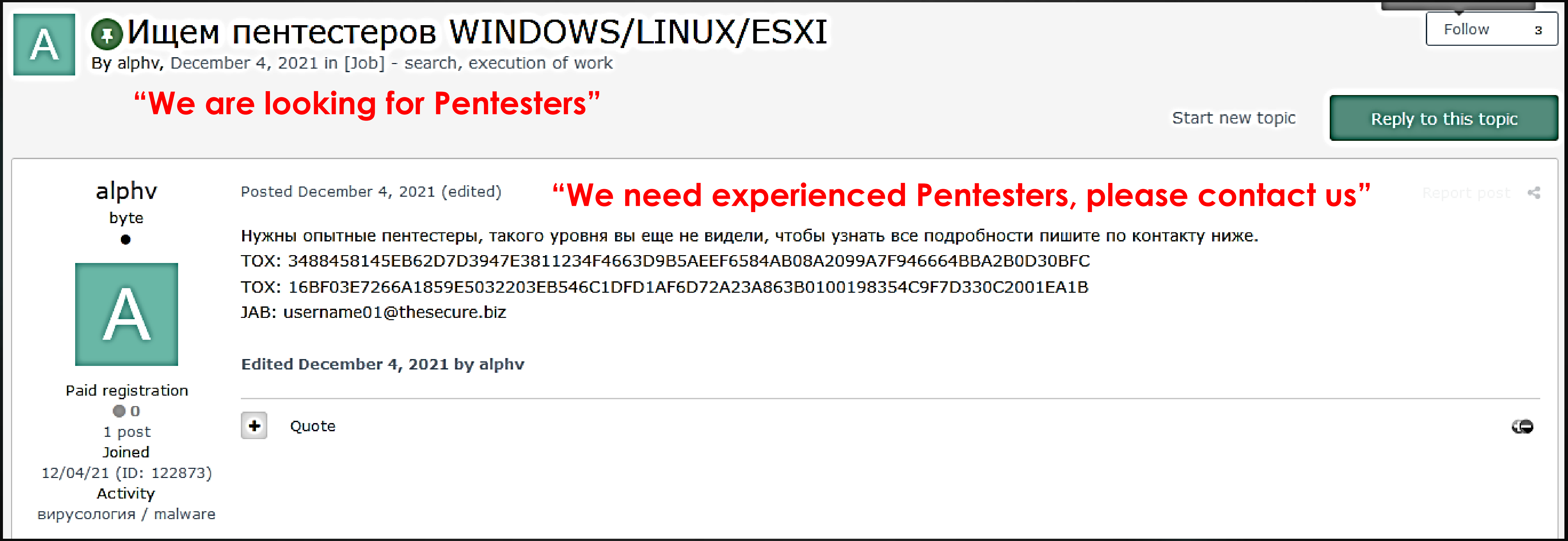
3. Affiliates download the tools from the RaaS ready for a new attack

4. The affiliate attacks a target to steal data and deploy the ransomware

5. Negotiations, Data Leaks, and Payments are handled by the RaaS

6. The ransom is split between the BlackCat gang and the affiliate

BlackCat recruiting affiliates on the cybercrime underground



Ищем пентестеров WINDOWS/LINUX/ESXI

By alphv, December 4, 2021 in [Job] - search, execution of work

“We are looking for Pentesters”

alphv
byte

Paid registration
0
1 post
Joined
12/04/21 (ID: 122873)
Activity
вирусология / malware

Posted December 4, 2021 (edited)

“We need experienced Pentesters, please contact us”

Нужны опытные пентестеры, такого уровня вы еще не видели, чтобы узнать все подробности пишите по контакту ниже.
TOX: 3488458145EB62D7D3947E3811234F4663D9B5AEEF6584AB08A2099A7F946664BBA2B0D30BFC
TOX: 16BF03E7266A1859E5032203EB546C1DFD1AF6D72A23A863B0100198354C9F7D330C2001EA1B
JAB: username01@thesecure.biz

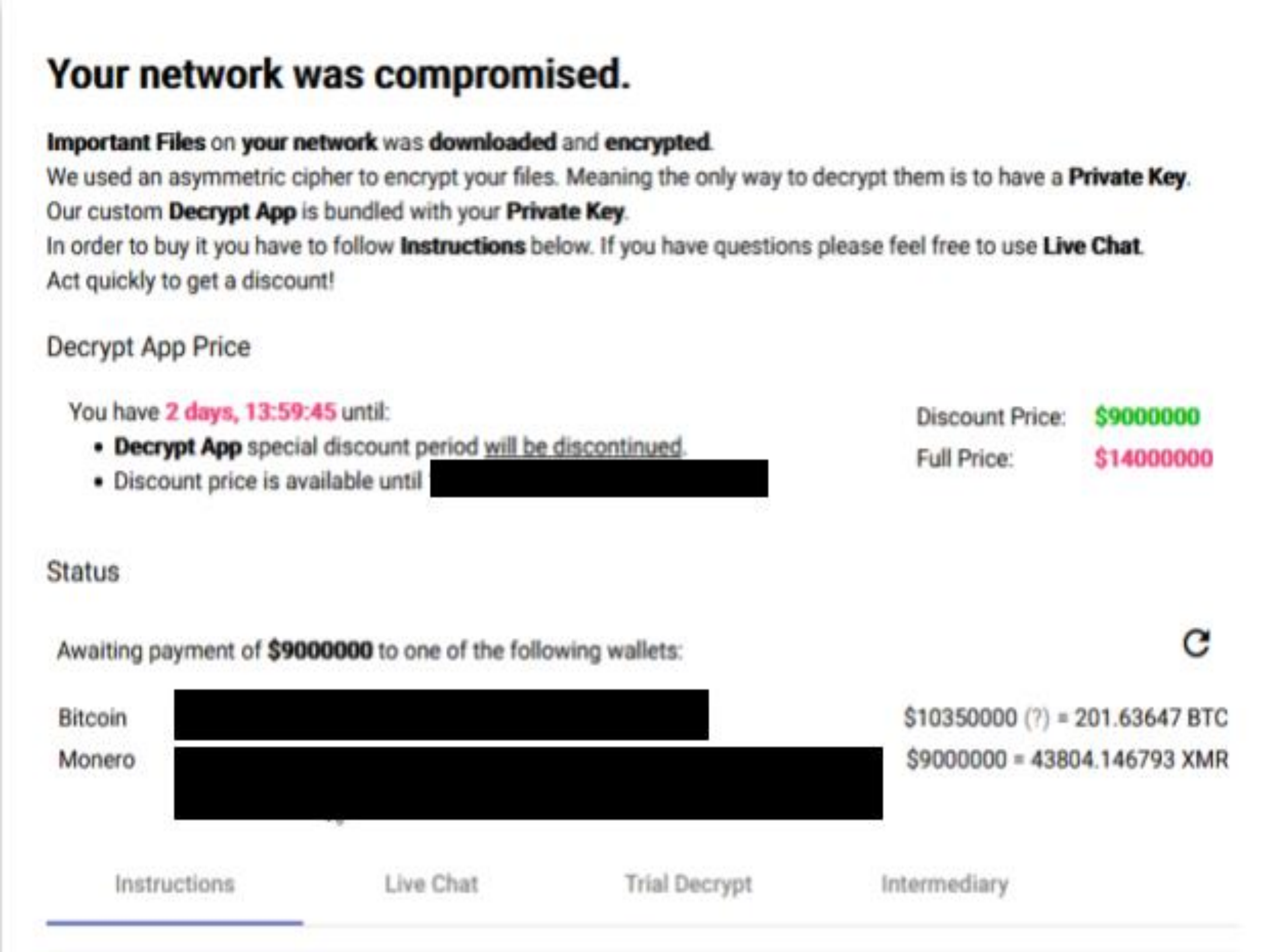
Edited December 4, 2021 by alphv

The BlackCat RaaS

This is what the victim sees ➡️

<u>BlackCat affiliates can:</u>

- Generate a new payload for Windows or Linux
- Set the countdown timer
- Set the ransom demand
- Generate a URL for a Tor chat negotiation site
- Decrypt one file as a test
- Publish stolen files via the leak site



Your network was compromised.

Important Files on **your network** was **downloaded** and **encrypted**.
We used an asymmetric cipher to encrypt your files. Meaning the only way to decrypt them is to have a **Private Key**.
Our custom **Decrypt App** is bundled with your **Private Key**.
In order to buy it you have to follow **Instructions** below. If you have questions please feel free to use **Live Chat**.
Act quickly to get a discount!

Decrypt App Price

You have **2 days, 13:59:45** until:
- **Decrypt App** special discount period <u>will be discontinued</u>.
- Discount price is available until [redacted]

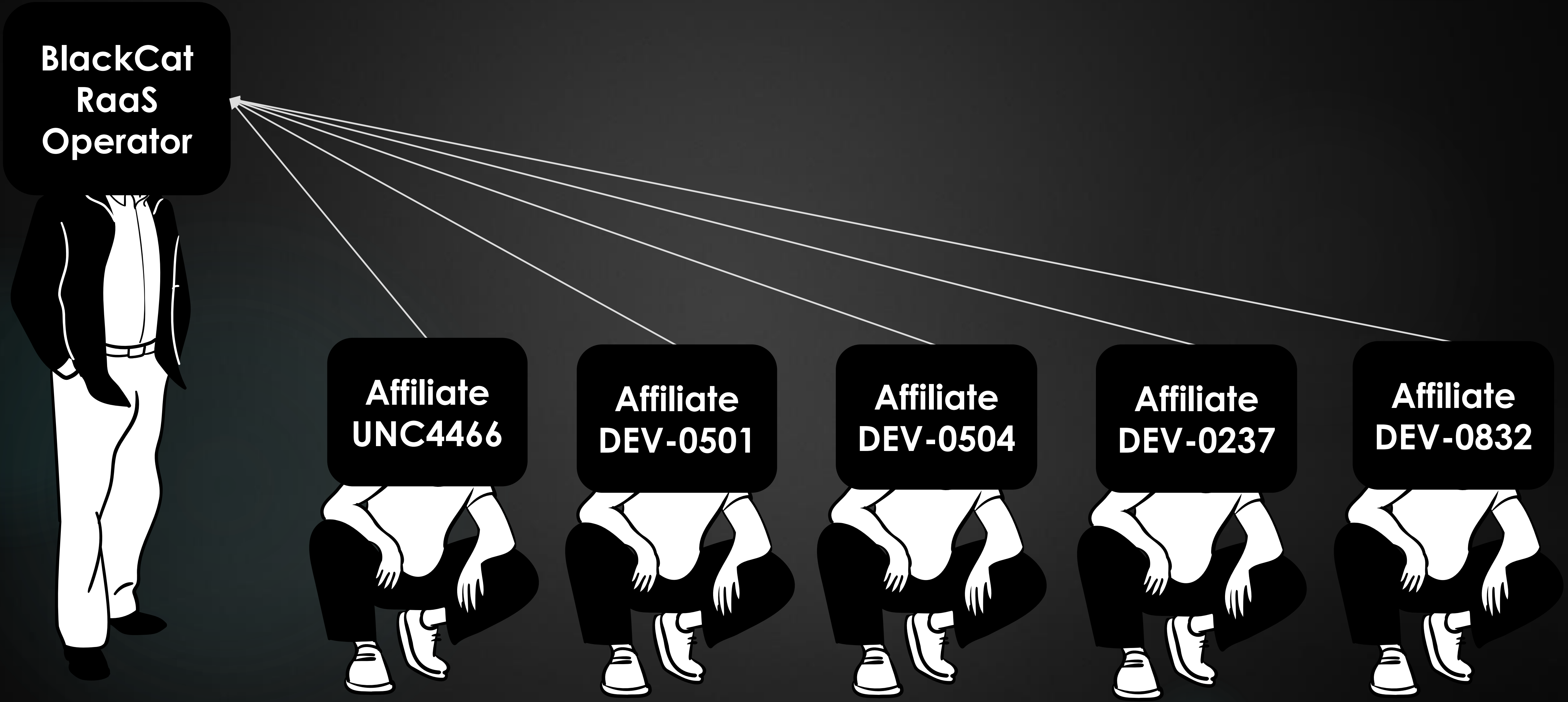
Discount Price: **$9000000**
Full Price: **$14000000**

Status

Awaiting payment of **$9000000** to one of the following wallets:

Bitcoin [redacted] $10350000 (?) = 201.63647 BTC
Monero [redacted] $9000000 = 43804.146793 XMR

Known BlackCat RaaS affiliates



BlackCat RaaS Operator

Affiliate UNC4466

Affiliate DEV-0501

Affiliate DEV-0504

Affiliate DEV-0237

Affiliate DEV-0832

Canadian Gov alert about BlackCat attacks in Canada 🍁

- On 25 July 2023, the Canadian Centre for Cybersecurity (CCCS) warned about BlackCat ransomware attacking companies in Canada ⚠️
- The CCCS shared that
  - BlackCat affiliates have attacked Canadian organizations between January 2022 and June 2023
  - BlackCat often employ a triple-extortion tactic:
    - making individual ransom demands for the decryption of infected files;
    - for not publishing stolen data;
    - and for not launching denial of service (DoS) attacks

The Similarities Emerge 🔎

BlackCat affiliate TTPs against Canada shared by the CCCS 🍁	Known Scattered Spider TTPs?
SMS phishing messages	✅
Target-themed credential phishing	✅
Single Sign-On (SSO) themed domains	✅
Phone calls to harvest their credentials	✅
MFA fatigue attacks	✅
RMM tools (Fleetdeck.io & Level.io)	✅
File-sharing services (temp.sh, storj.io & gofile.io)	✅
Third-party VPN provider (ExpressVPN)	✅

A combined threat 🤝

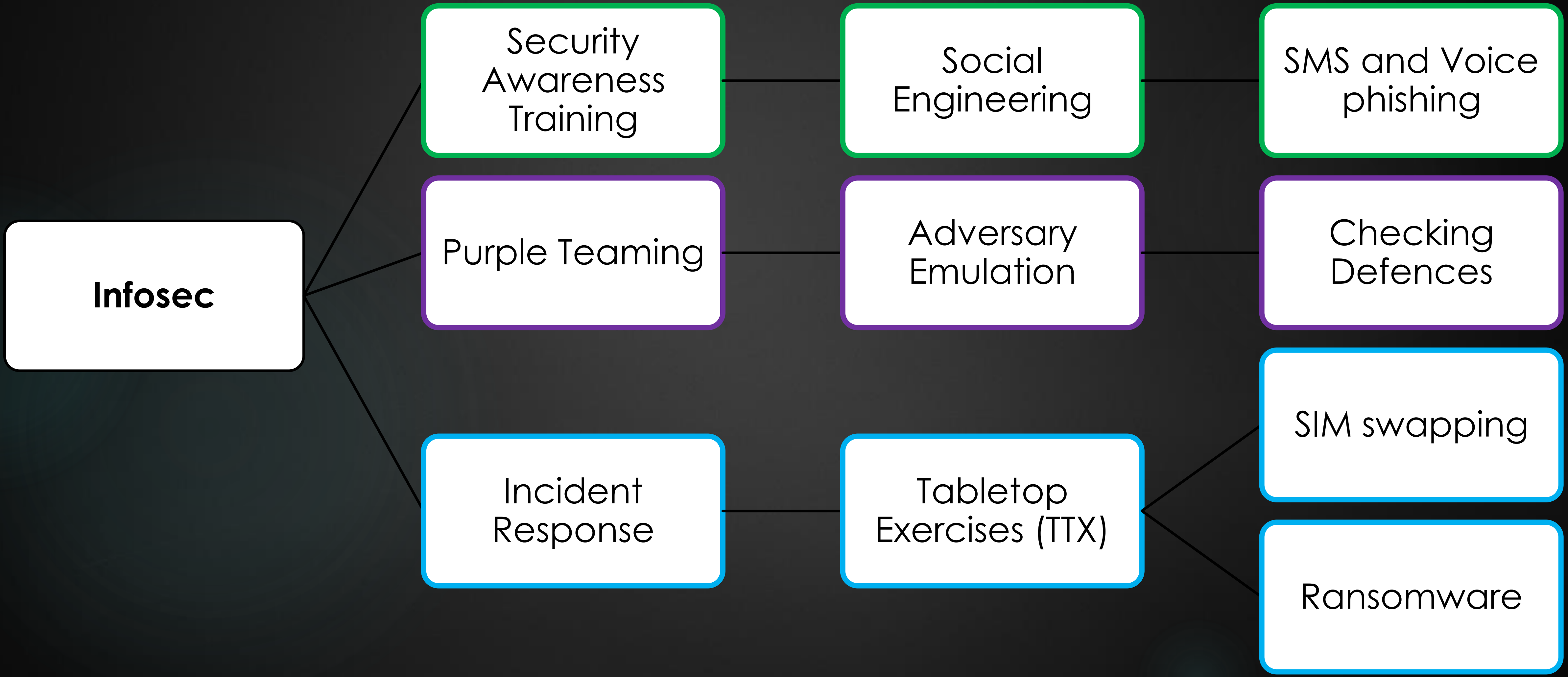
- Scattered Spider’s highly effective methodology to access a company
- The effectiveness of ransomware and extortion schemes by BlackCat
- Highly likely to continue successfully extorting victim companies for ransoms

More Ransom Payments

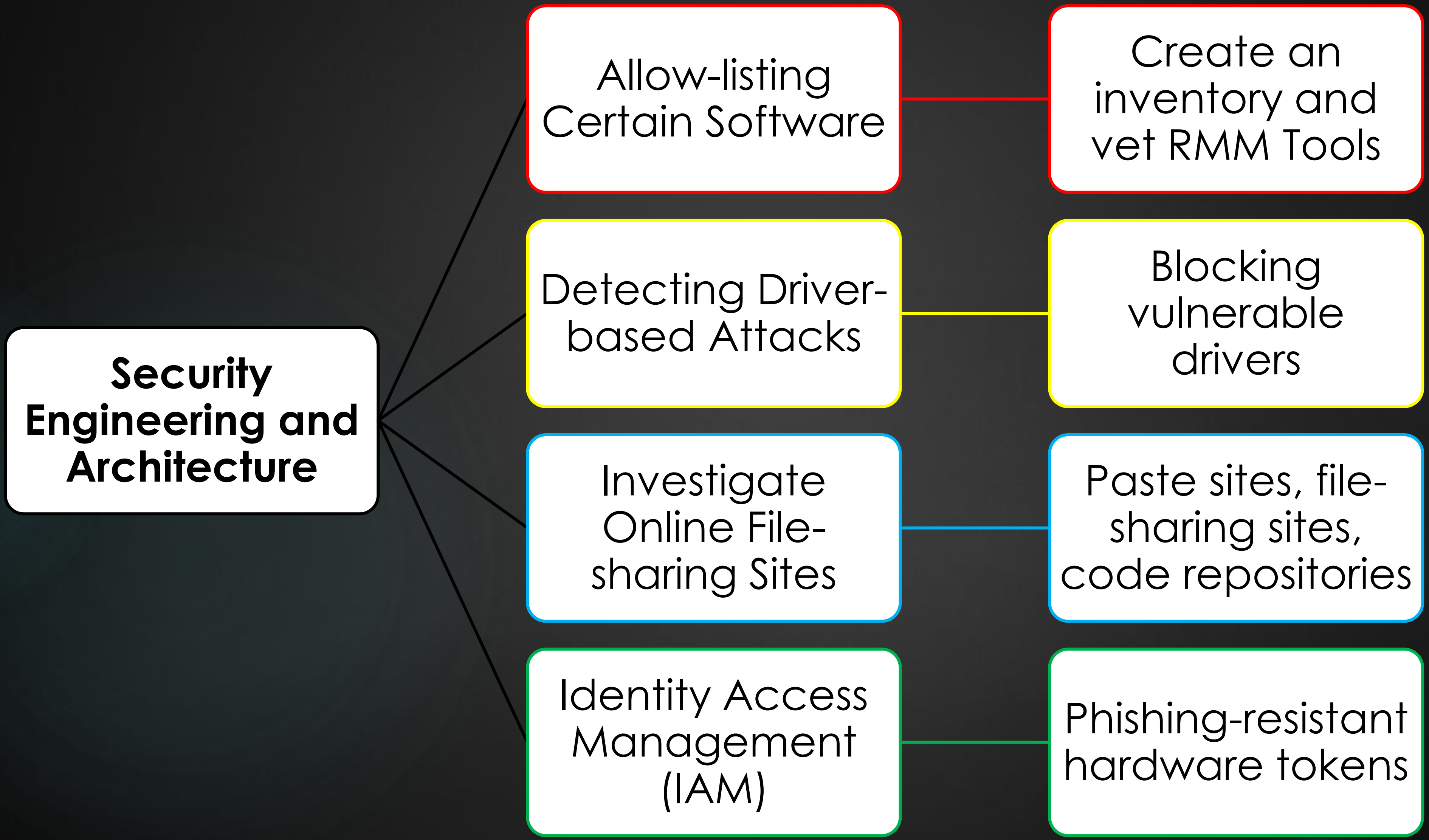
Scatted Spider

BlackCat

How to mitigate this threat 🛡️



Engineering the problem away 🪛



Security Engineering and Architecture

Allow-listing Certain Software

Create an inventory and vet RMM Tools

Detecting Driver-based Attacks

Blocking vulnerable drivers

Investigate Online File-sharing Sites

Paste sites, file-sharing sites, code repositories

Identity Access Management (IAM)

Phishing-resistant hardware tokens

Thank You For Listening!

- If you want to see more of my CTI Research:
  - **Bushidotoken.net**
    - Personal blog containing latest research
  - **Github.com/BushidoUK**
    - Contains all my previous talks, podcasts, projects, and more!