Where did the threat actor go?

…they RAN-SOM-WARE

A journey into the heart of ransomware gangs, from the trade craft used to bypass defenses, to the anatomy of attack.

Intro

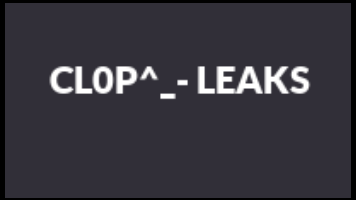
- Hi! I’m M4x!
- I am a hacker
- About a decade working in the Cybersecurity industry
- Published offensive tools on Github
- Spoke at DEFCON’s Recon Village about normalizing breach-data research
- Taught lock-picking at BlackHat USA, 2022
- Red Team Operations, Malware development, and Threat Hunting research

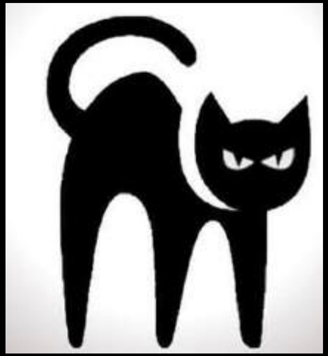
Who are threat actors?

- The OG’s
  - REvil – Sodinokibi
    - First observed in 2019
    - Dismantled in 2022
  - Conti
    - First observed in 2019
    - Rebranded and disbanded in 2022
  - HIVE
    - First observed in 2021
    - Rebranded to Hunters International in 2024

Who are threat actors?

- The Top Dogs
  - LockBit
  - INCRansomware
  - ALPHV/BlackCat
  - CL0P
  - Qilin
  - Akira
  - Hunters International – previously HIVE
  - Medusa
  - Play
  - Ransomhouse
  - Rhysida



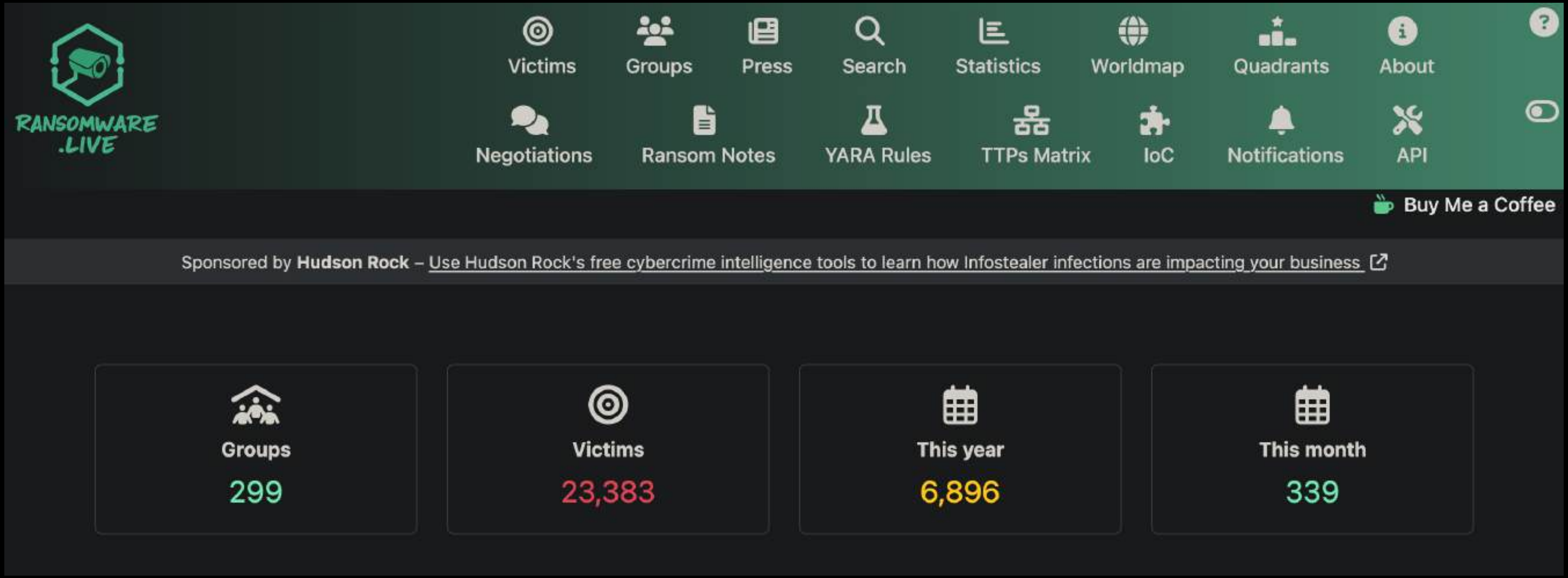


Who are threat actors?

- The rookies
    - Scattered Spider
    - Cactus
    - Everest
    - Silent
    - Stormous
    - Skira
    - Embargo

Who are threat actors?

- Find out more on resources like:
  - https://ransomware.live/



Sponsored by **Hudson Rock** – Use Hudson Rock's free cybercrime intelligence tools to learn how Infostealer infections are impacting your business

Groups	Victims	This year	This month
299	23,383	6,896	339

What motivates the bad guys?

- Money
  - …mostly money

What motivates the bad guys?

- Fame & clout

What motivates the bad guys?

- Politics
  - Mostly Russian speaking
  - Cahoots with the Kremlin
  - Chinese/North Korean ties
  - Speculation of state-sponsorship

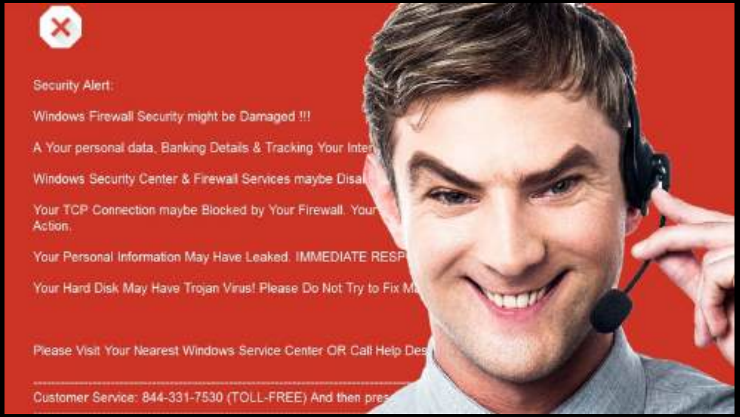
What is ransomware?

- Cryptovirology
  - *From Wikipedia, the free encyclopedia*
  - *Cryptovirology refers to the study of cryptography use in malware, such as ransomware and asymmetric backdoors. Traditionally, cryptography and its applications are defensive in nature, and provide privacy, authentication, and security to users. Cryptovirology employs a twist on cryptography, showing that it can also be used offensively. It can be used to mount extortion-based attacks that cause loss of access to information, loss of confidentiality, and information leakage, tasks which cryptography typically prevents.*
  - Reference: https://en.wikipedia.org/wiki/Cryptovirology

How do they do it?

- Tactics, Techniques, and Procedures (TTP)
  - “Trade tools”
    - Trusted tools used for remote support and network administration
    - NOT MALWARE*
    - Bypass *most* defenses due to inherent trust
    - Signed by trusted vendors (including Microsoft)

Used by this guy 😊



Security Alert:

Windows Firewall Security might be Damaged !!!

A Your personal data, Banking Details & Tracking Your Inter

Windows Security Center & Firewall Services maybe Disal

Your TCP Connection maybe Blocked by Your Firewall. Your
Action.

Your Personal Information May Have Leaked. IMMEDIATE RESP

Your Hard Disk May Have Trojan Virus! Please Do Not Try to Fix M

Please Visit Your Nearest Windows Service Center OR Call Help Des

Customer Service: 844-331-7530 (TOLL-FREE) And then pres

… and this guy 😈

How do they do it?

- Tactics, Techniques, and Procedures (TTP)
  - Discovery
    - ADExplorer
    - ADRecon
    - PingCastle
    - Nbtscan
    - SoftPerfect NetScan
    - SoftPerfect LanSearchPro

How do they do it?

- Tactics, Techniques, and Procedures (TTP)
  - Remote Monitoring and Management (RMM)
    - AnyDesk
    - SecureConnect
    - LogMeIn
    - Splashtop
    - TightVNC

How do they do it?

- Tactics, Techniques, and Procedures (TTP)
    - Defense Evasion
        - Defender Control
        - ProcessHacker
        - TDSKiller
        - FileShredder
        - PowerTool

How do they do it?

- Tactics, Techniques, and Procedures (TTP)
  - Credential Theft
    - BetterSaftyKatz
    - DonPAPI
    - GrabChrome / GrabFF
    - LaZagne / Trufflehog
    - NirSoft* - Password recovery tools
    - Mimikatz / SharpKatz
    - ProcDump
    - GoSecretsDump

How do they do it?

- Tactics, Techniques, and Procedures (TTP)
  - OffSec
    - Metasploit
    - Brute Ratel C4
    - Cobalt Strike
    - CrackMapExec / NetExec
    - Koadic
    - LAPS Toolkit
    - Rubeus
    - Impacket
    - Evilginx2

How do they do it?

- Tactics, Techniques, and Procedures (TTP)
  - Networking
    - Chisel
    - OpenSSH/Putty/Plink
    - Ligolo / Ligolo-ng / Ligolo-mg
    - Ngrok
    - Rsocks

How do they do it?

- Tactics, Techniques, and Procedures (TTP)
  - Living-Off-the-Land Binary Applications (LOLBAS)
    - BCDEdit
    - BITSAdmin
    - NTDS Utility
    - PsExec / PAExec
    - Windows Event Utility
    - WinExe
    - WMIC

How do they do it?

- Tactics, Techniques, and Procedures (TTP)
  - Exfiltration
    - Anonfiles
    - Dropbox / Google Drive
    - FileZilla / WinSCP
    - Gofile.io / File.io
    - MEGA Upload
    - Restic
    - Rclone

How did you learn all this?

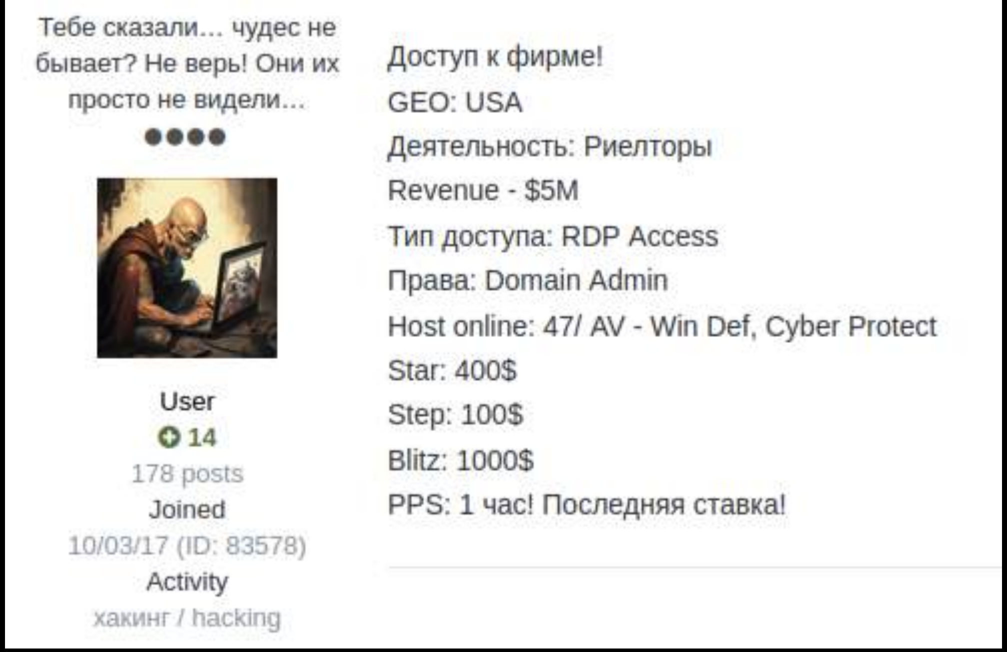
- Lots of research, both on my part and many others
  - Shout out to Will Thomas (BushidoUK) for his research against CISA’s Threat Actor profile showcases.
  - Check out his Github: https://github.com/BushidoUK
    - Especially the Ransomware-Tool-Matrix
    - …and the Russian-Threat-Actor-Tool-Matrix

How did you learn all this?

- Hacker Forums
  - Proceed with caution!
    - Actively monitored by Law Enforcement
    - Do NOT engage with THREAT ACTORS!!
    - FAFO 👀
  - Russian
    - Учите русский! Это помогает!

~/ XSS.is

RAMP



Тебе сказали… чудес не бывает? Не верь! Они их просто не видели…
●●●●

User
⊕ 14
178 posts
Joined
10/03/17 (ID: 83578)
Activity
хакинг / hacking

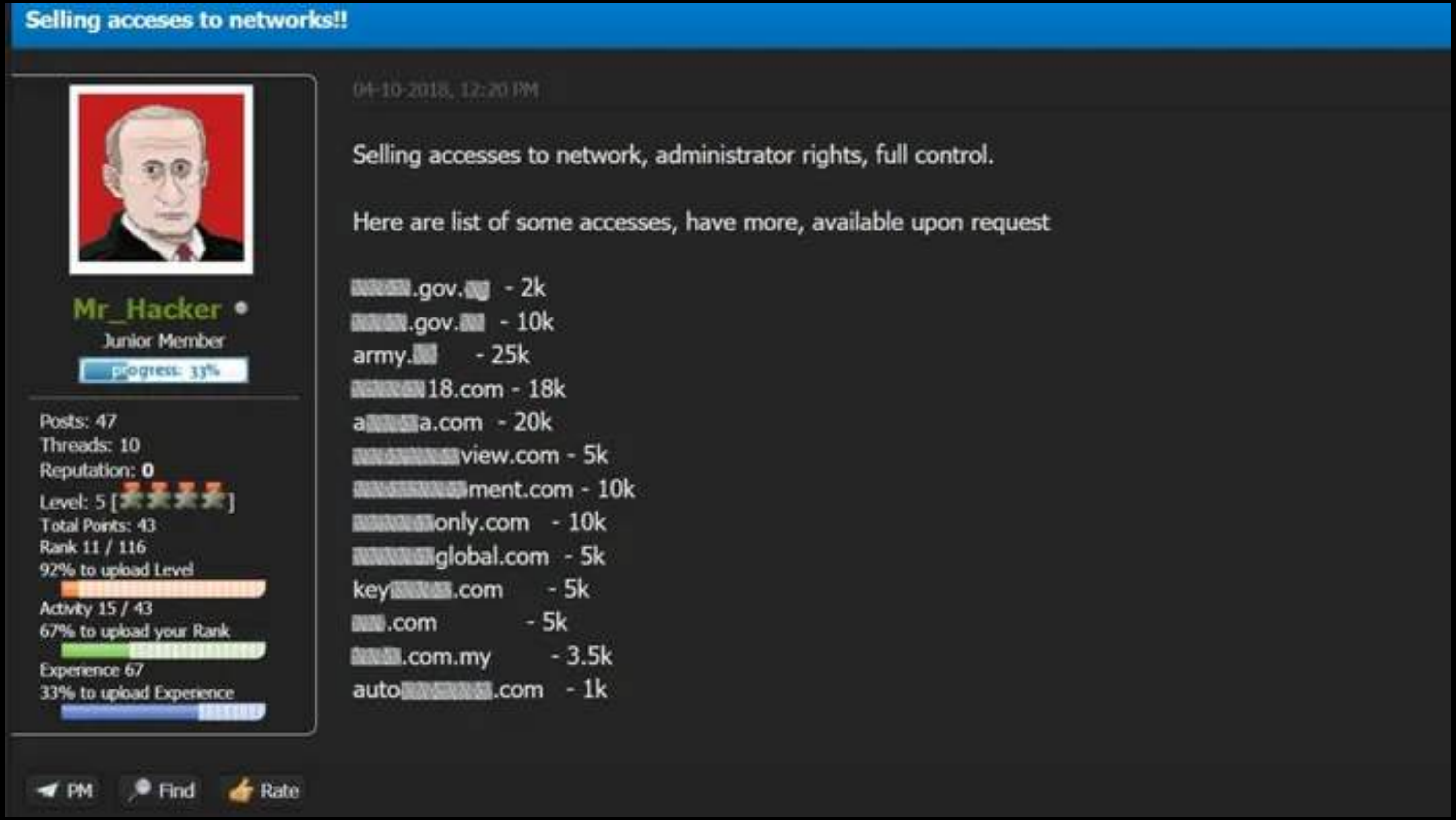
Доступ к фирме!
GEO: USA
Деятельность: Риелторы
Revenue - $5M
Тип доступа: RDP Access
Права: Domain Admin
Host online: 47/ AV - Win Def, Cyber Protect
Star: 400$
Step: 100$
Blitz: 1000$
PPS: 1 час! Последняя ставка!

How does it all work?

- It’s simple, really…

How does it all work?

- Access brokers



Selling acceses to networks!!

Mr_Hacker

Junior Member

Progress: 33%

Posts: 47
Threads: 10
Reputation: **0**
Level: 5 [ ]
Total Points: 43
Rank 11 / 116
92% to upload Level
Activity 15 / 43
67% to upload your Rank
Experience 67
33% to upload Experience

04-10-2018, 12:20 PM

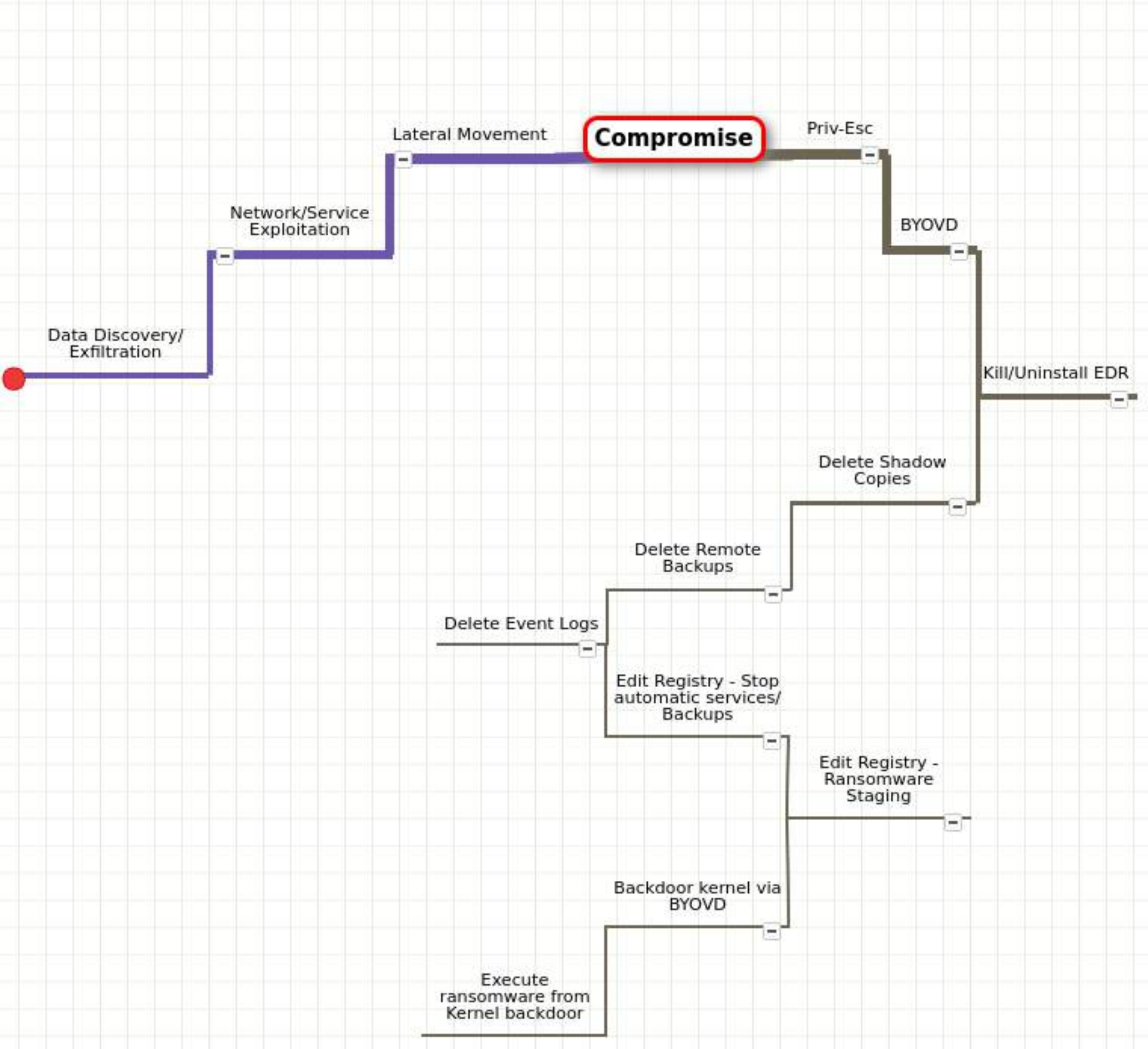
Selling accesses to network, administrator rights, full control.

Here are list of some accesses, have more, available upon request

[redacted].gov.[redacted] - 2k
[redacted].gov.[redacted] - 10k
army.[redacted] - 25k
[redacted]18.com - 18k
a[redacted]a.com - 20k
[redacted]view.com - 5k
[redacted]ment.com - 10k
[redacted]only.com - 10k
[redacted]global.com - 5k
key[redacted].com - 5k
[redacted].com - 5k
[redacted].com.my - 3.5k
auto[redacted].com - 1k

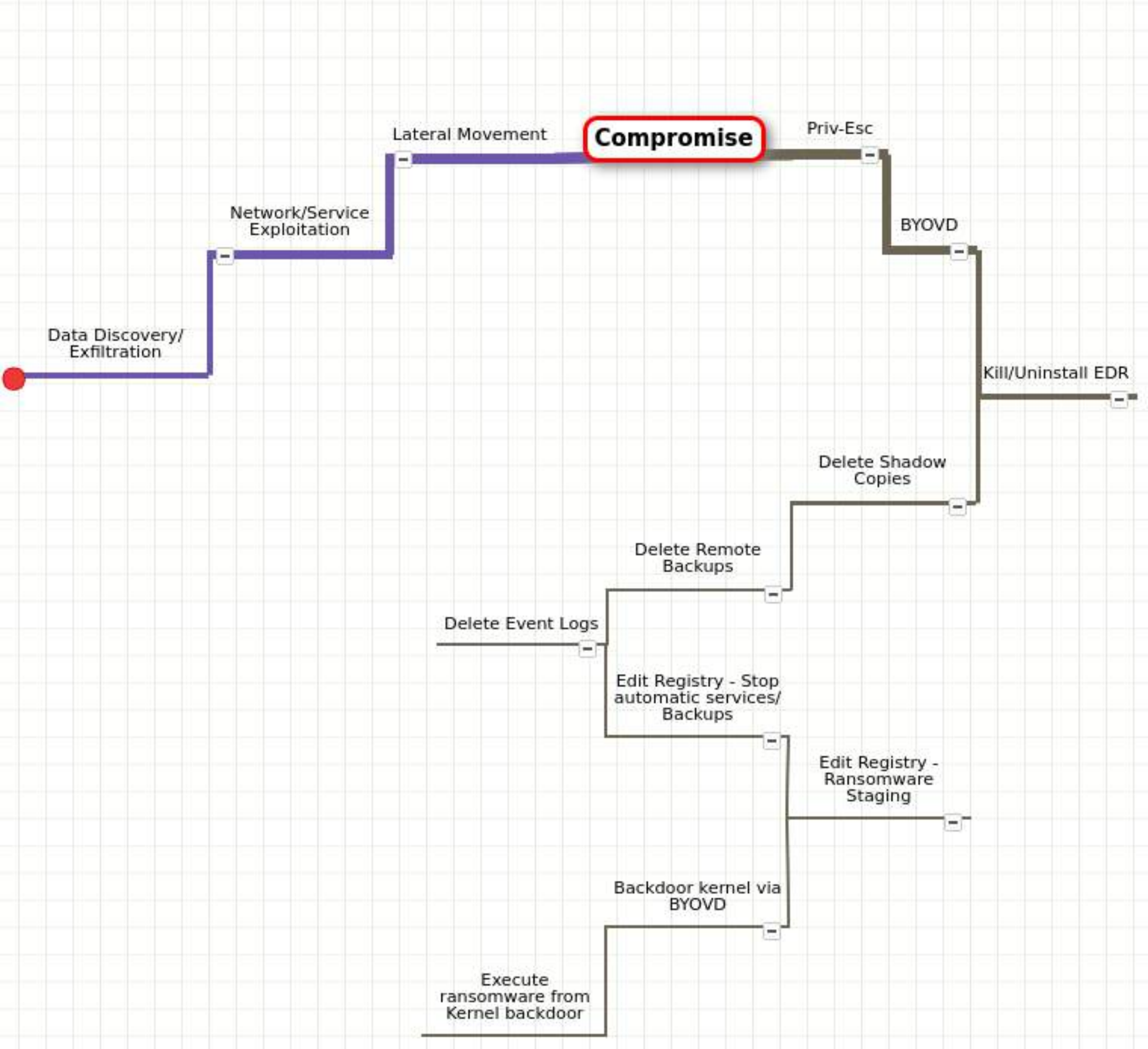
How does it all work?

- The anatomy of a ransomware attack
- Compromise
  - Brokered Access
  - Social Engineering
  - VPN Credentials
  - 0-Day Exploit
- Network level enumeration
  - Network Service Exploitation
  - Data Discovery/Exfiltration
- Privilege Escalation/Lateral Movement
  - ZeroLogon
  - BlueKeep
  - Potatoes
  - BYOVD


Lateral Movement
Compromise
Priv-Esc
Network/Service Exploitation
BYOVD
Data Discovery/ Exfiltration
Kill/Uninstall EDR
Delete Shadow Copies
Delete Remote Backups
Delete Event Logs
Edit Registry - Stop automatic services/ Backups
Edit Registry - Ransomware Staging
Backdoor kernel via BYOVD
Execute ransomware from Kernel backdoor

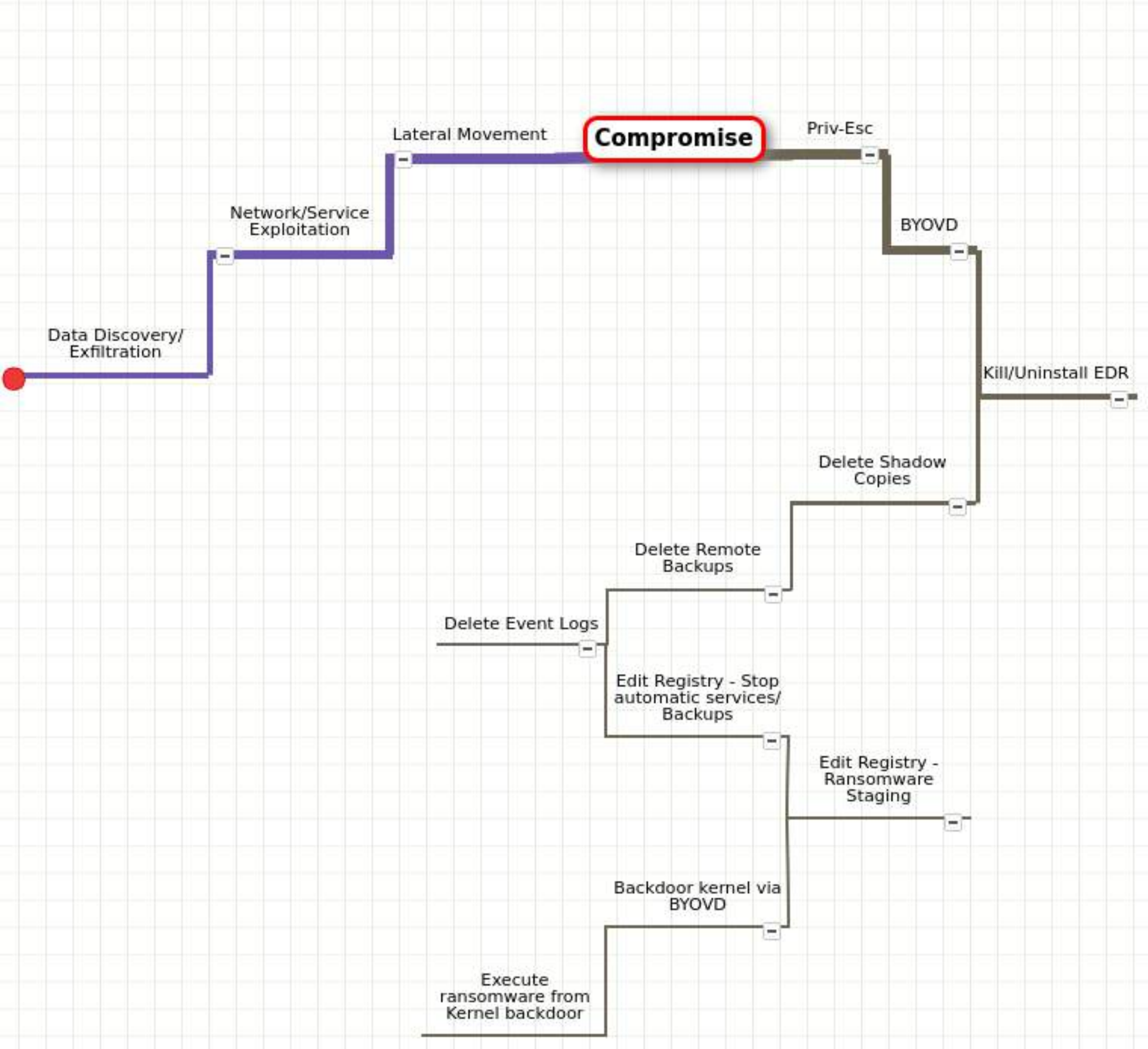
How does it all work?

- Kill/Uninstall EDR
  - EDRSandblaster
  - Remove Defender
  - BYOAV
- Delete Shadow Copies
  - Anti-forensics and recovery
- Delete Remote Backups
  - Cloud
  - Veeam
- Delete Event Logs
  - Cover tracks
- Stop backup and security services
  - Modify registry to stop automatic services


Lateral Movement
Compromise
Priv-Esc
Network/Service Exploitation
BYOVD
Data Discovery/ Exfiltration
Kill/Uninstall EDR
Delete Shadow Copies
Delete Remote Backups
Delete Event Logs
Edit Registry - Stop automatic services/ Backups
Edit Registry - Ransomware Staging
Backdoor kernel via BYOVD
Execute ransomware from Kernel backdoor

How does it all work?

- Ransomware Staging
  - Edit registry to find ransomware ICON file dropped to disk
  - Change wallpaper background via GPO
- Backdoor kernel
  - Rootkit/bootkit for persistent access
  - Maintain control of victim system
- Execute ransomware
  - Protect ransomware process via PPL
  - Execute as a hidden process via kernel modification
- Extortion campaign
  - Tox client for communications
  - TOR address to view proof of compromise
  - Crypto currency used for payment
  - Campaign ends once the negotiations have been met



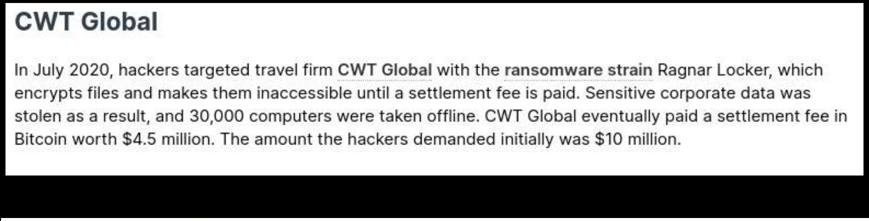
Compromise
Lateral Movement
Network/Service Exploitation
Data Discovery/ Exfiltration
Priv-Esc
BYOVD
Kill/Uninstall EDR
Delete Shadow Copies
Delete Remote Backups
Delete Event Logs
Edit Registry - Stop automatic services/ Backups
Edit Registry - Ransomware Staging
Backdoor kernel via BYOVD
Execute ransomware from Kernel backdoor

How does it all work? - Summary

1. Initial access
2. Pillage Data
3. Escalate privileges
4. Remove defenses
5. Detonate Ransomware
6. Rinse and repeat…

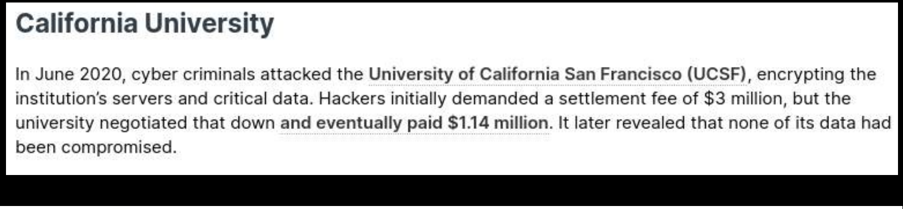
Who pays these people???

- Too many people



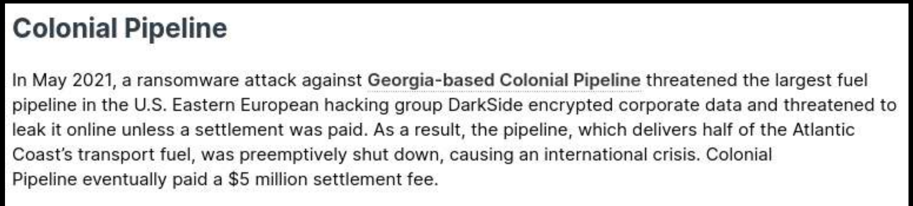
CWT Global

In July 2020, hackers targeted travel firm **CWT Global** with the **ransomware strain** Ragnar Locker, which encrypts files and makes them inaccessible until a settlement fee is paid. Sensitive corporate data was stolen as a result, and 30,000 computers were taken offline. CWT Global eventually paid a settlement fee in Bitcoin worth $4.5 million. The amount the hackers demanded initially was $10 million.



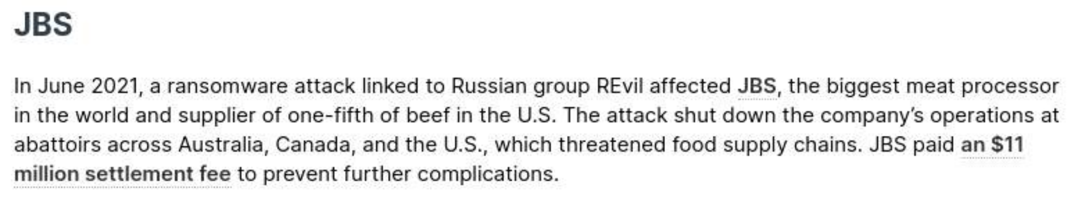
California University

In June 2020, cyber criminals attacked the **University of California San Francisco (UCSF)**, encrypting the institution's servers and critical data. Hackers initially demanded a settlement fee of $3 million, but the university negotiated that down **and eventually paid $1.14 million**. It later revealed that none of its data had been compromised.



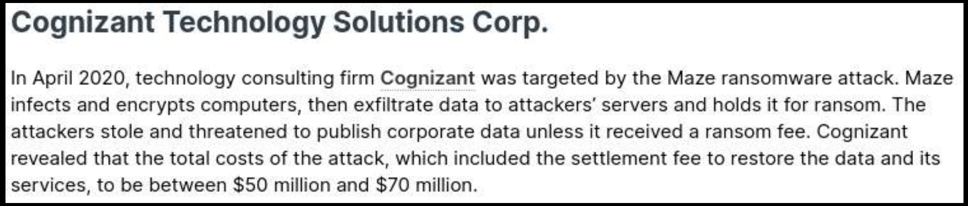
Colonial Pipeline

In May 2021, a ransomware attack against **Georgia-based Colonial Pipeline** threatened the largest fuel pipeline in the U.S. Eastern European hacking group DarkSide encrypted corporate data and threatened to leak it online unless a settlement was paid. As a result, the pipeline, which delivers half of the Atlantic Coast's transport fuel, was preemptively shut down, causing an international crisis. Colonial Pipeline eventually paid a $5 million settlement fee.



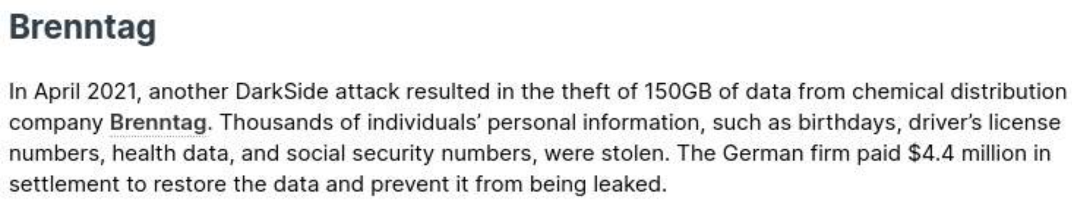
JBS

In June 2021, a ransomware attack linked to Russian group REvil affected **JBS**, the biggest meat processor in the world and supplier of one-fifth of beef in the U.S. The attack shut down the company's operations at abattoirs across Australia, Canada, and the U.S., which threatened food supply chains. JBS paid **an $11 million settlement fee** to prevent further complications.



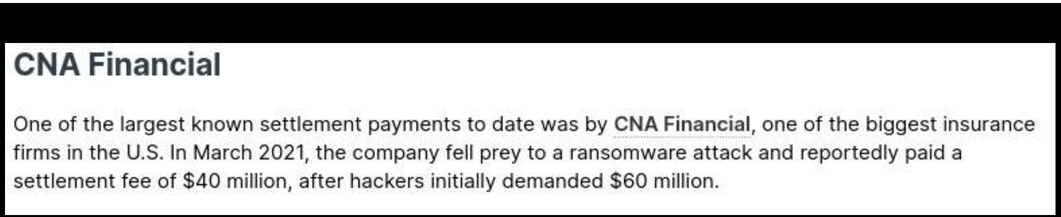
Cognizant Technology Solutions Corp.

In April 2020, technology consulting firm **Cognizant** was targeted by the Maze ransomware attack. Maze infects and encrypts computers, then exfiltrate data to attackers' servers and holds it for ransom. The attackers stole and threatened to publish corporate data unless it received a ransom fee. Cognizant revealed that the total costs of the attack, which included the settlement fee to restore the data and its services, to be between $50 million and $70 million.



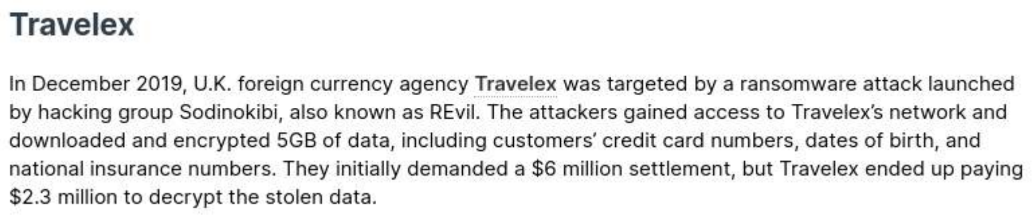
Brenntag

In April 2021, another DarkSide attack resulted in the theft of 150GB of data from chemical distribution company **Brenntag**. Thousands of individuals' personal information, such as birthdays, driver's license numbers, health data, and social security numbers, were stolen. The German firm paid $4.4 million in settlement to restore the data and prevent it from being leaked.



CNA Financial

One of the largest known settlement payments to date was by **CNA Financial**, one of the biggest insurance firms in the U.S. In March 2021, the company fell prey to a ransomware attack and reportedly paid a settlement fee of $40 million, after hackers initially demanded $60 million.



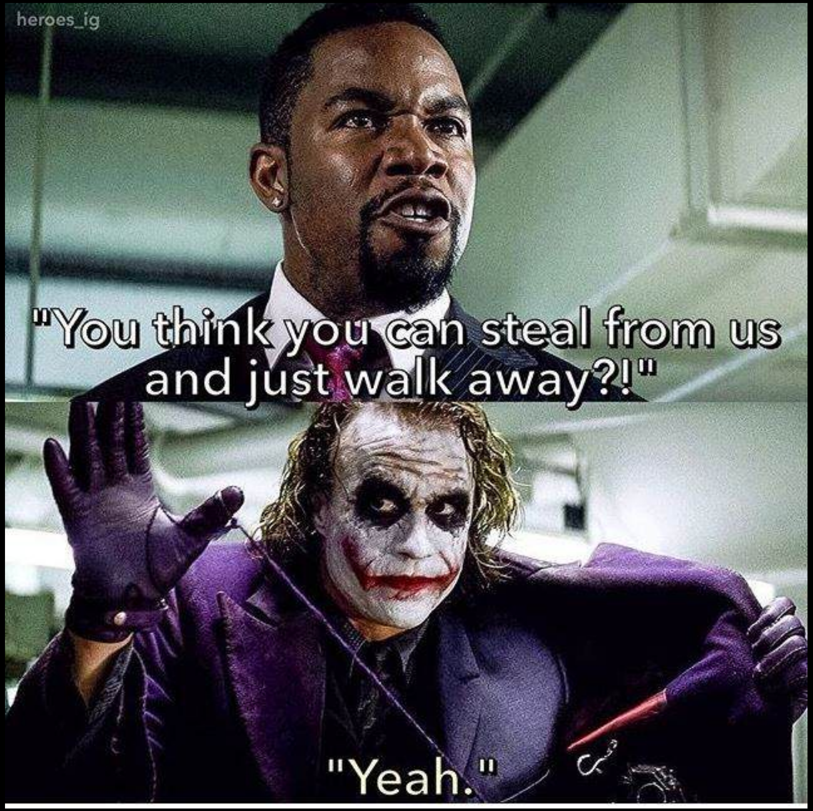
Travelex

In December 2019, U.K. foreign currency agency **Travelex** was targeted by a ransomware attack launched by hacking group Sodinokibi, also known as REvil. The attackers gained access to Travelex's network and downloaded and encrypted 5GB of data, including customers' credit card numbers, dates of birth, and national insurance numbers. They initially demanded a $6 million settlement, but Travelex ended up paying $2.3 million to decrypt the stolen data.

Resource: https://www.fortinet.com/resources/cyberglossary/recent-ransomware-settlements

WHY!?

IF YOU'RE GOOD AT SOMETHING
NEVER DO IT FOR FREE


heroes_ig
"You think you can steal from us and just walk away?!"
"Yeah."

WHY!?

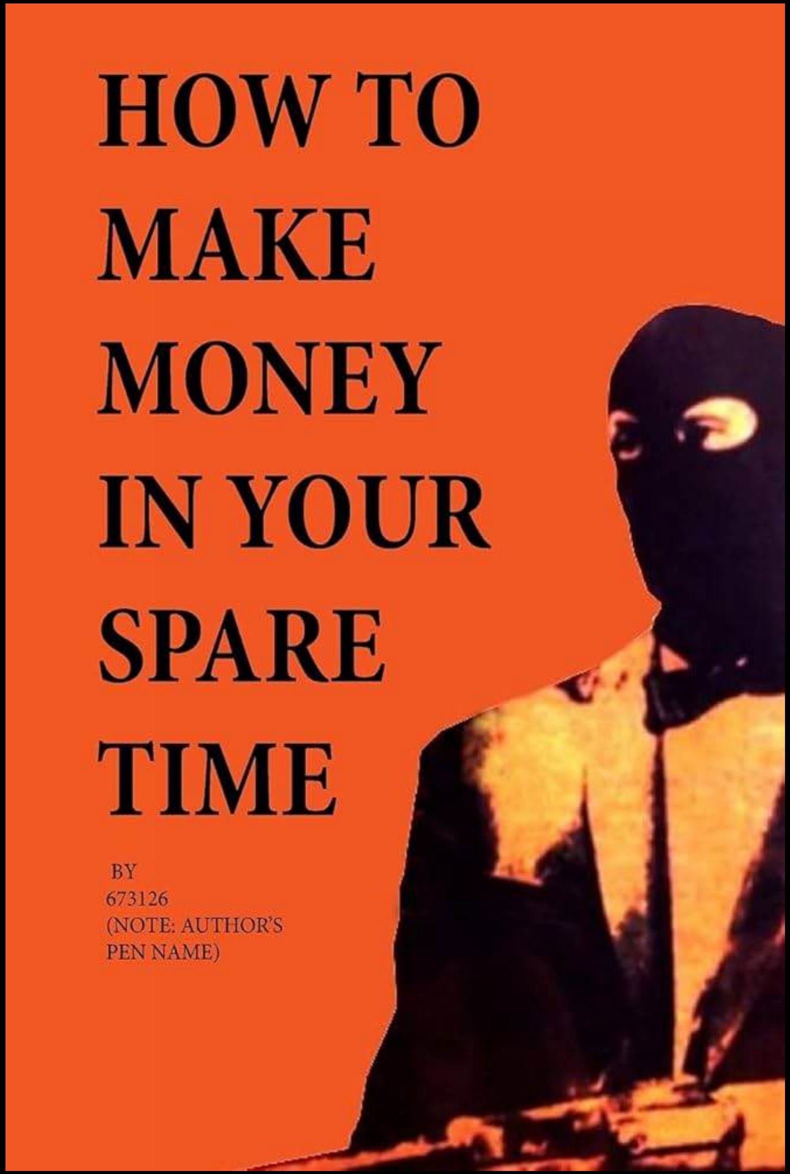
CREATE RANSOMWARE GROUP
JOIN NSA
MALWARE DEVELOPERS

How do we stop them?

- "Only you can prevent *forest* fires..." ~ Smokey, the D.A.
- CISA - #StopRansomware
- NCA/Interpol
- Operation Endgame
- Research IoC's!!!

Are they here to stay?

- Organized crime is as old as time...



Outro

- *The most dangerous enemy in the world is the one you do not recognize. ~ Tess Gerritsen*