Cyber Threat Landscape Now and Future

Gerald Auger, PhD

Introduction

> “Those who cannot remember the past are condemned to repeat it. ”
>
> -George Santayana

Cybersecurity is Mission Critical

Change Healthcare, (Feb 2024), Ransomware

Ardent Health Services, (Nov 2023), Ransomware

Prospect Medical Holdings, (Aug 2023), Ransomware

HCA Healthcare, (Jul 2023), Data breach

Medstar Health, (Apr 2023), Ransomware

Community Health Systems, (Mar 2023), Data breach

CommonSpirit Health, (Oct 2022), Ransomware

Shields Health Care Group, (Jun 2022), Data breach

Broward Health, (Jan 2022), Data breach

Cybersecurity is Mission Critical

Fairfield Memorial Hospital, (July 2024), Ransomware attack by LockBit gang

Lurie Children's Hospital, Chicago, (January 2024), Cyberattack affecting electronic health records

Ascension Illinois hospitals, (May 2024), Cyberattack disrupting electronic systems

St. Margaret's Health-Spring Valley, (2024), Cyberattack leading to *hospital closure*

Cook County Health, (2024), Implementing cybersecurity measures against potential attacks

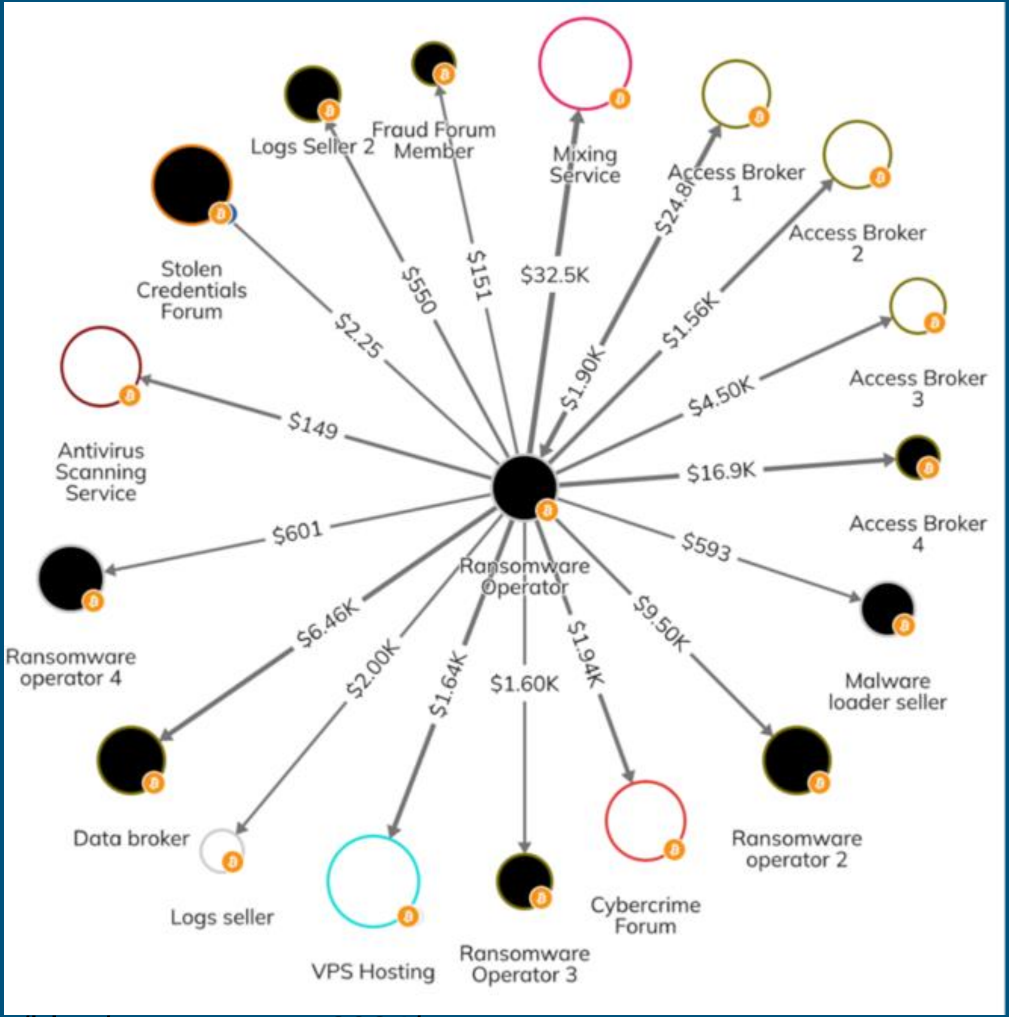
Chicago safety-net hospital, (Early 2024), Ransomware demand of $900,000 (declined to pay)

Ascension Alexian Brothers-Elk Grove Village, (May 2024), Cyberattack causing ambulance diversion

Illinois rural hospitals, (2023-2024), Increased targeting by cybercriminals

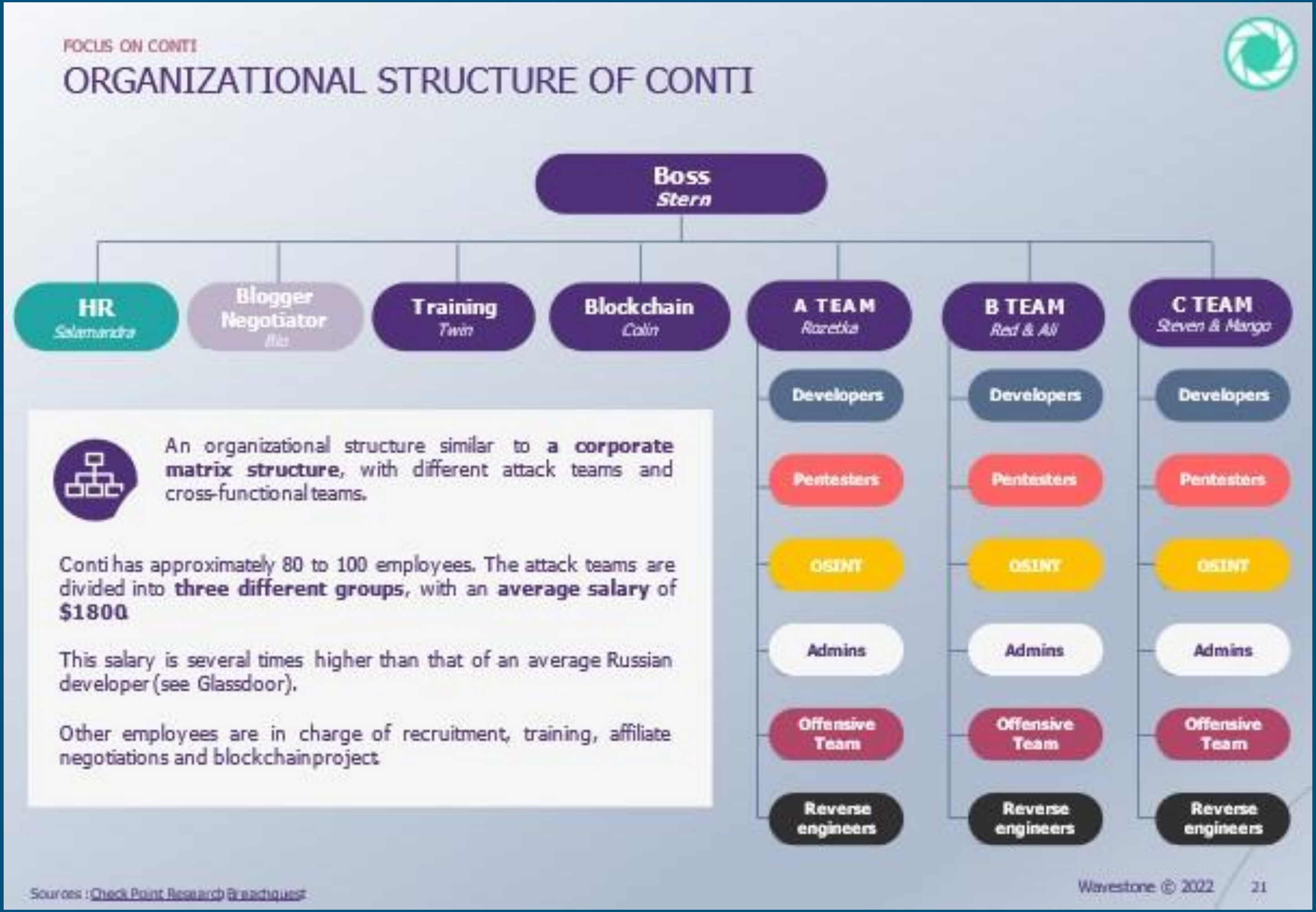
Threat Actors Were….

Threat Actors Are….



https://www.chainalysis.com/blog/ransomware-2024/

Threat Actors Will Be....



FOCUS ON CONTI

ORGANIZATIONAL STRUCTURE OF CONTI

An organizational structure similar to a **corporate matrix structure**, with different attack teams and cross-functional teams.

Conti has approximately 80 to 100 employees. The attack teams are divided into **three different groups**, with an **average salary** of **$1800.**

This salary is several times higher than that of an average Russian developer (see Glassdoor).

Other employees are in charge of recruitment, training, affiliate negotiations and blockchainproject.

Sources : Check Point Research Breachquest

Wavestone © 2022 21

https://www.riskinsight-wavestone.com/wp-content/uploads/2022/06/EN4.jpg

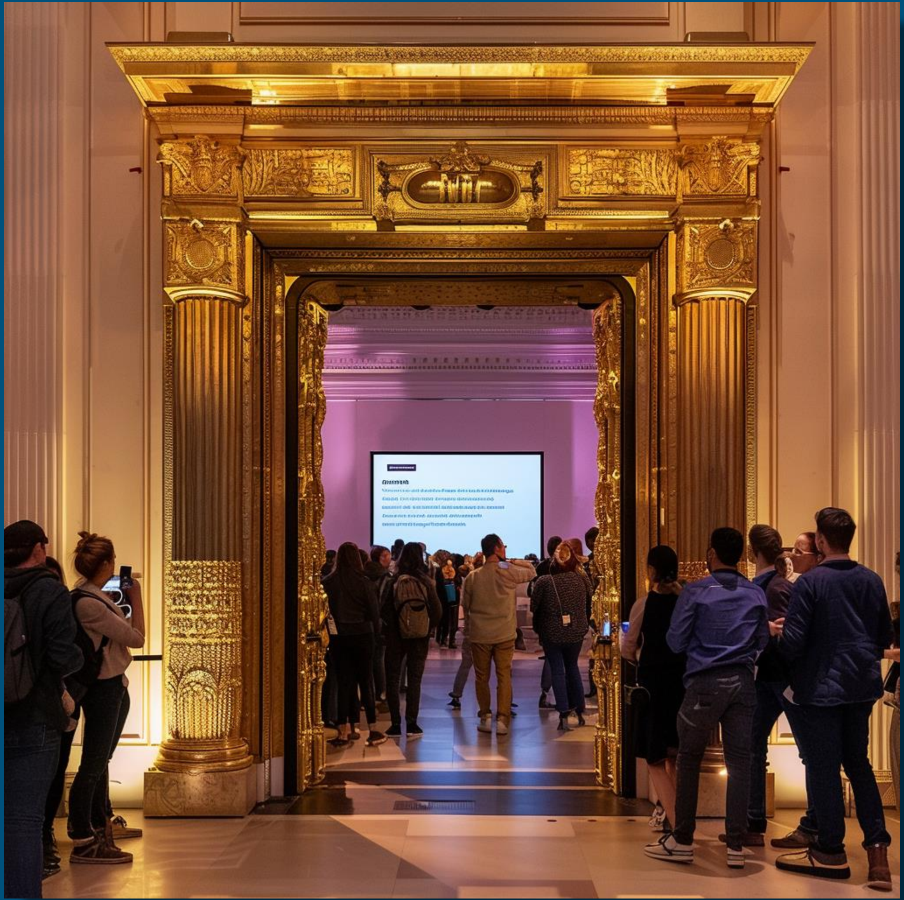
Objective of the Talk

Ransomware

Third-Party Risk

AI

Workforce Development



Learning Outcomes

Acquire Situational Understanding

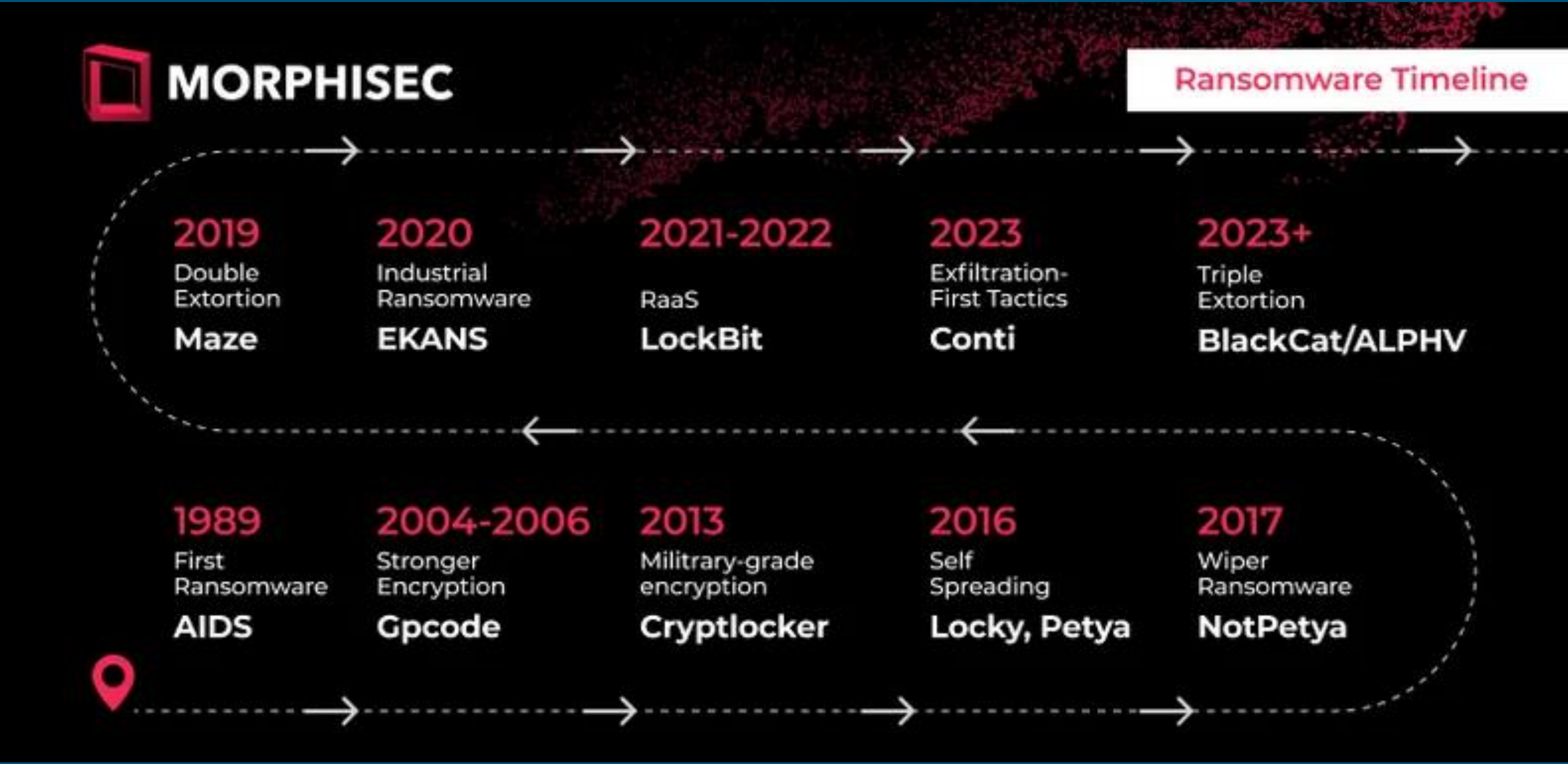
Equip YOU with Actionable Steps

Connect with Resources and Community

Ransomware Evolution and Mitigation

Modern Ransomware

Triple Extortion, RaaS, Specialized Operators



MORPHISEC

Ransomware Timeline

1989
First Ransomware
AIDS

2004-2006
Stronger Encryption
Gpcode

2013
Military-grade encryption
Cryptlocker

2016
Self Spreading
Locky, Petya

2017
Wiper Ransomware
NotPetya

2019
Double Extortion
Maze

2020
Industrial Ransomware
EKANS

2021-2022
RaaS
LockBit

2023
Exfiltration-First Tactics
Conti

2023+
Triple Extortion
BlackCat/ALPHV

https://blog.morphisec.com/ransomware-history-evolution-of-attacks-and-defenses

$896M

2023 Prediction: Organizations will pay in ransomware

$1.1B

2023 Actual: Organizations paid in ransomware

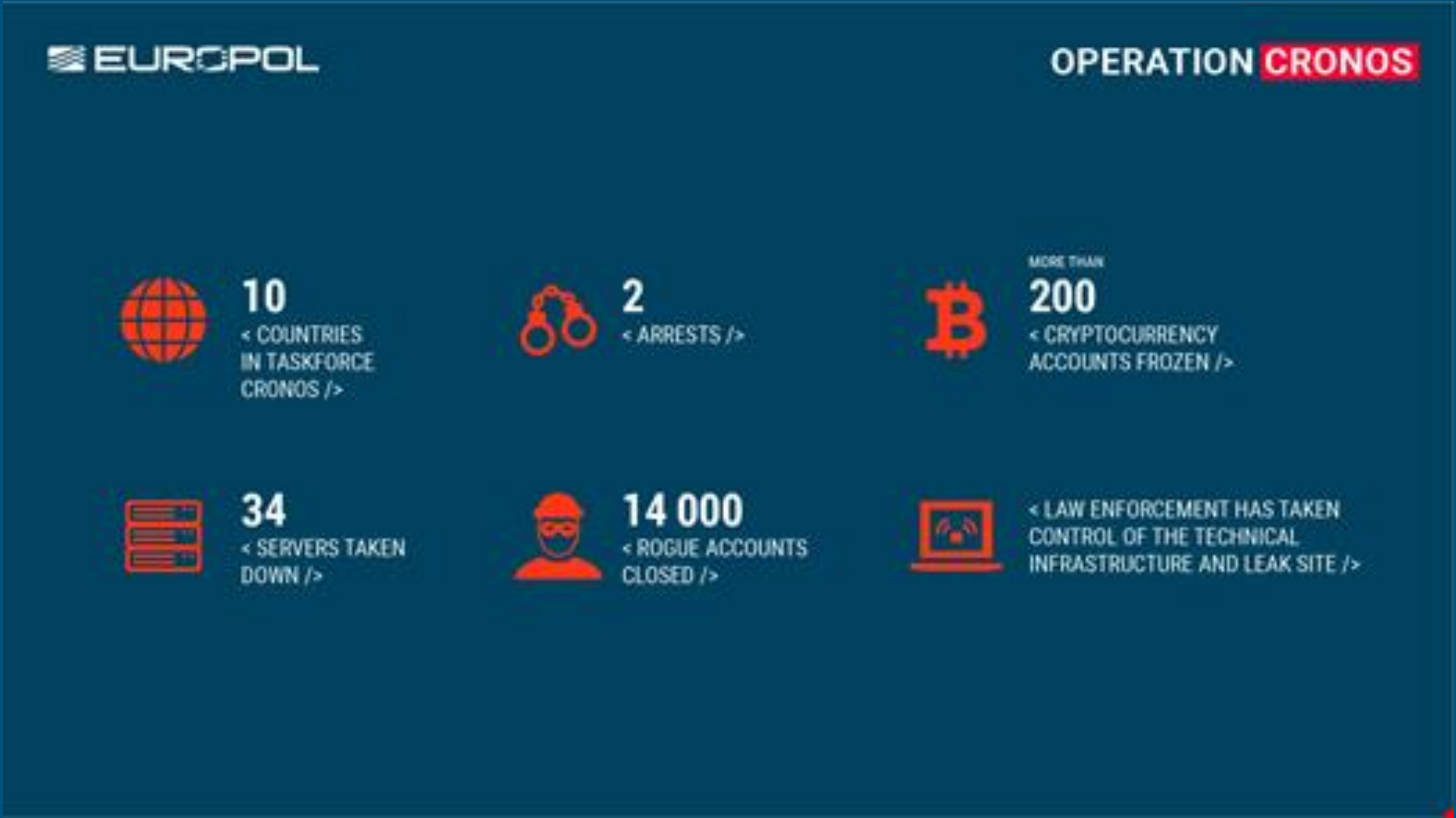
~33%

All breaches involved Ransomware or some other Extortion technique in 2023

“Verizon 2024 Data Breach Investigations Report

Law Enforcement

Shut It Down!



EUROPOL

OPERATION CRONOS

10
< COUNTRIES IN TASKFORCE CRONOS />

2
< ARRESTS />

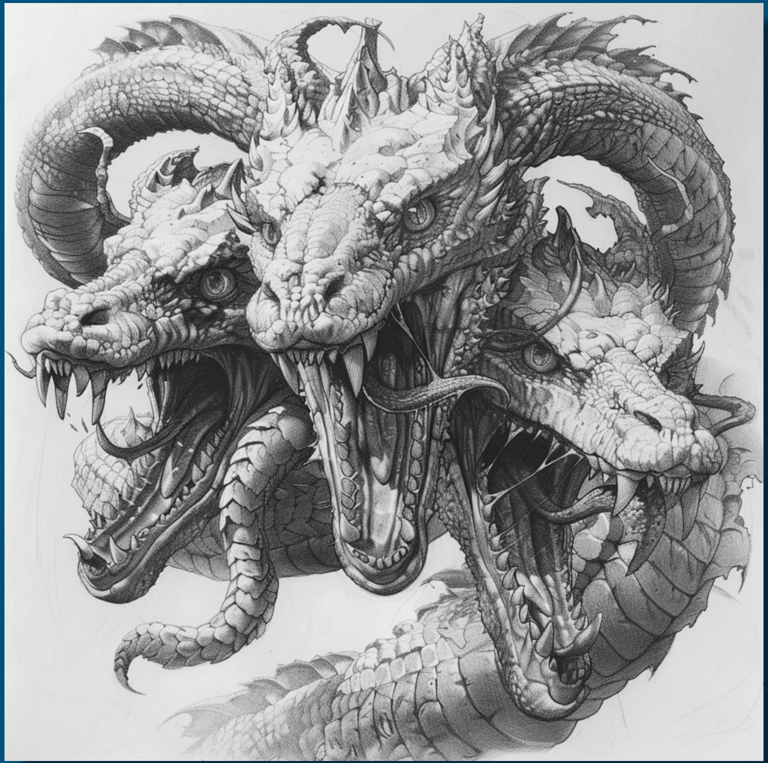
MORE THAN
200
< CRYPTOCURRENCY ACCOUNTS FROZEN />

34
< SERVERS TAKEN DOWN />

14 000
< ROGUE ACCOUNTS CLOSED />

< LAW ENFORCEMENT HAS TAKEN CONTROL OF THE TECHNICAL INFRASTRUCTURE AND LEAK SITE />

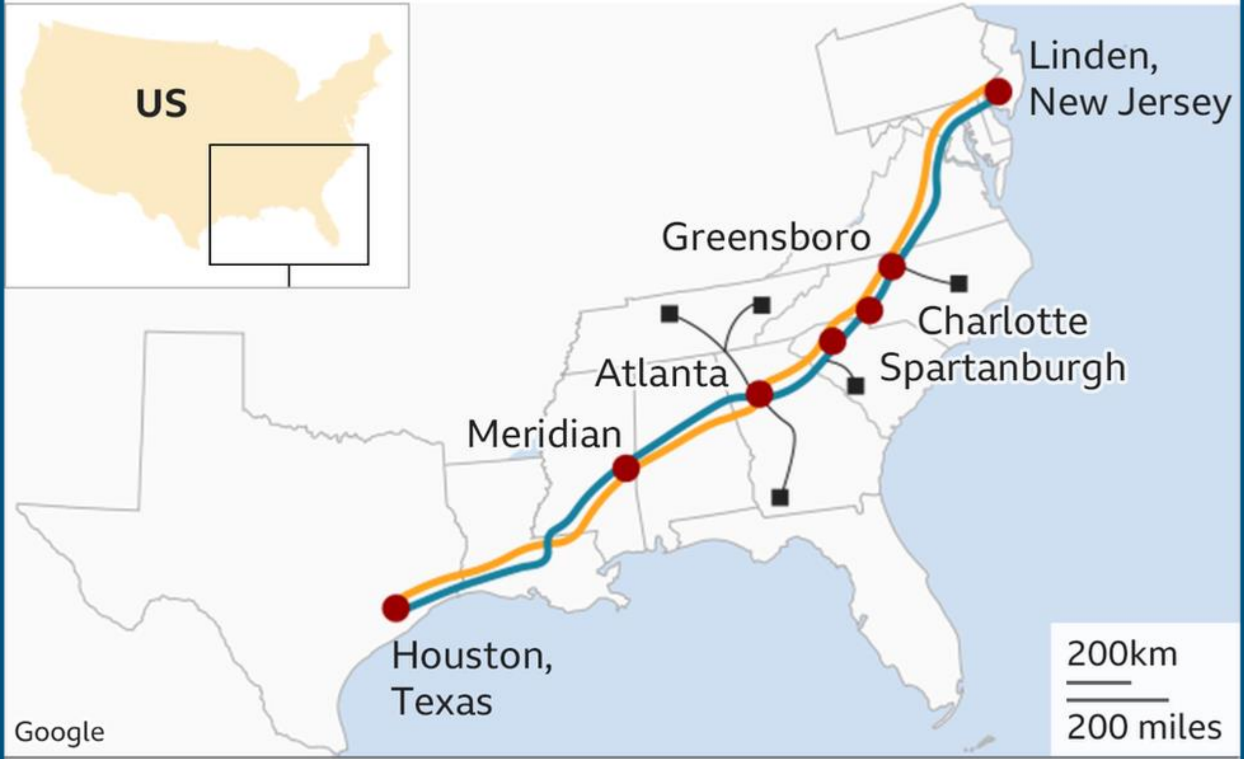
Quick Case Study



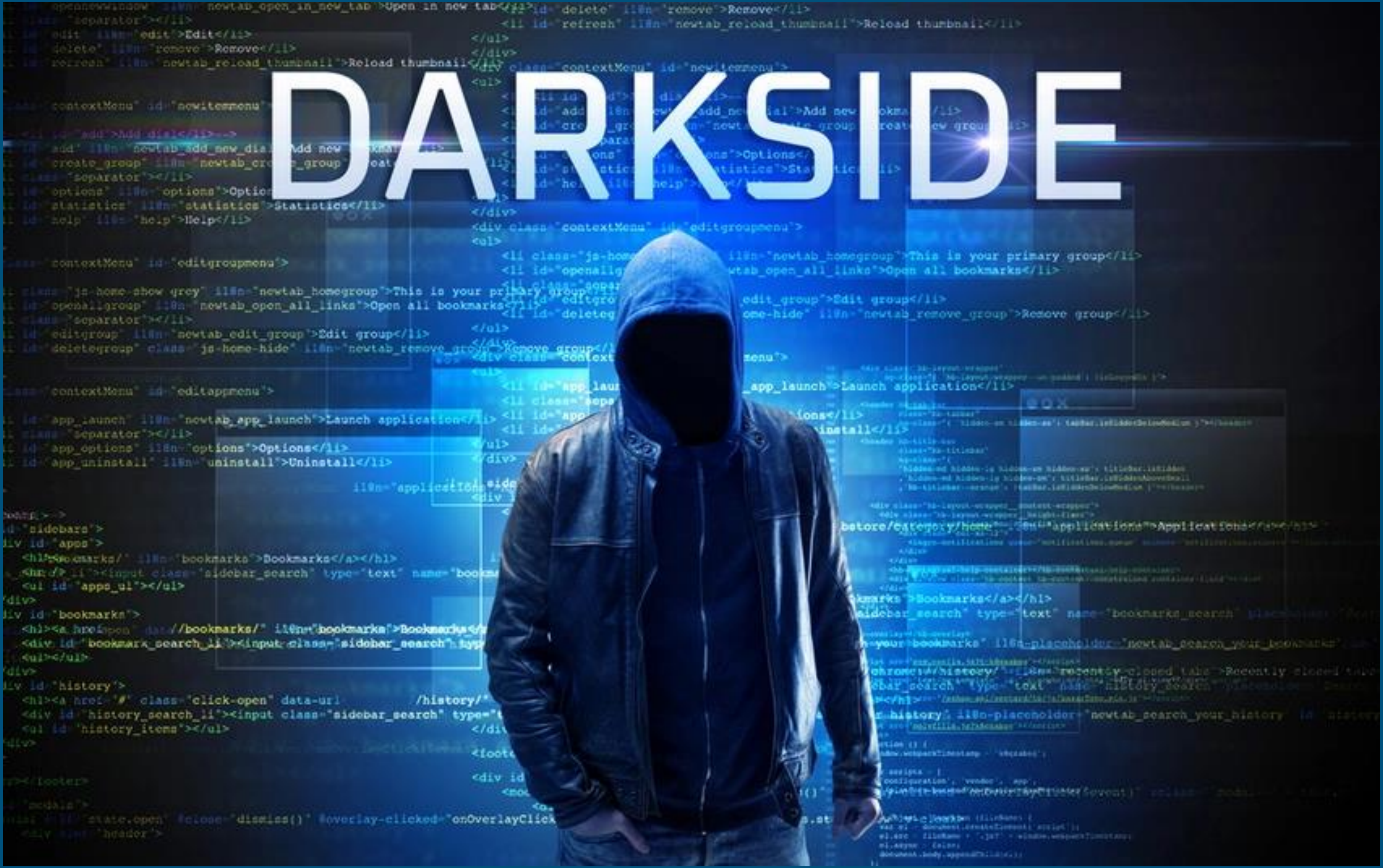
Colonial Pipeline system map

🟧 Pipeline system — Sublines

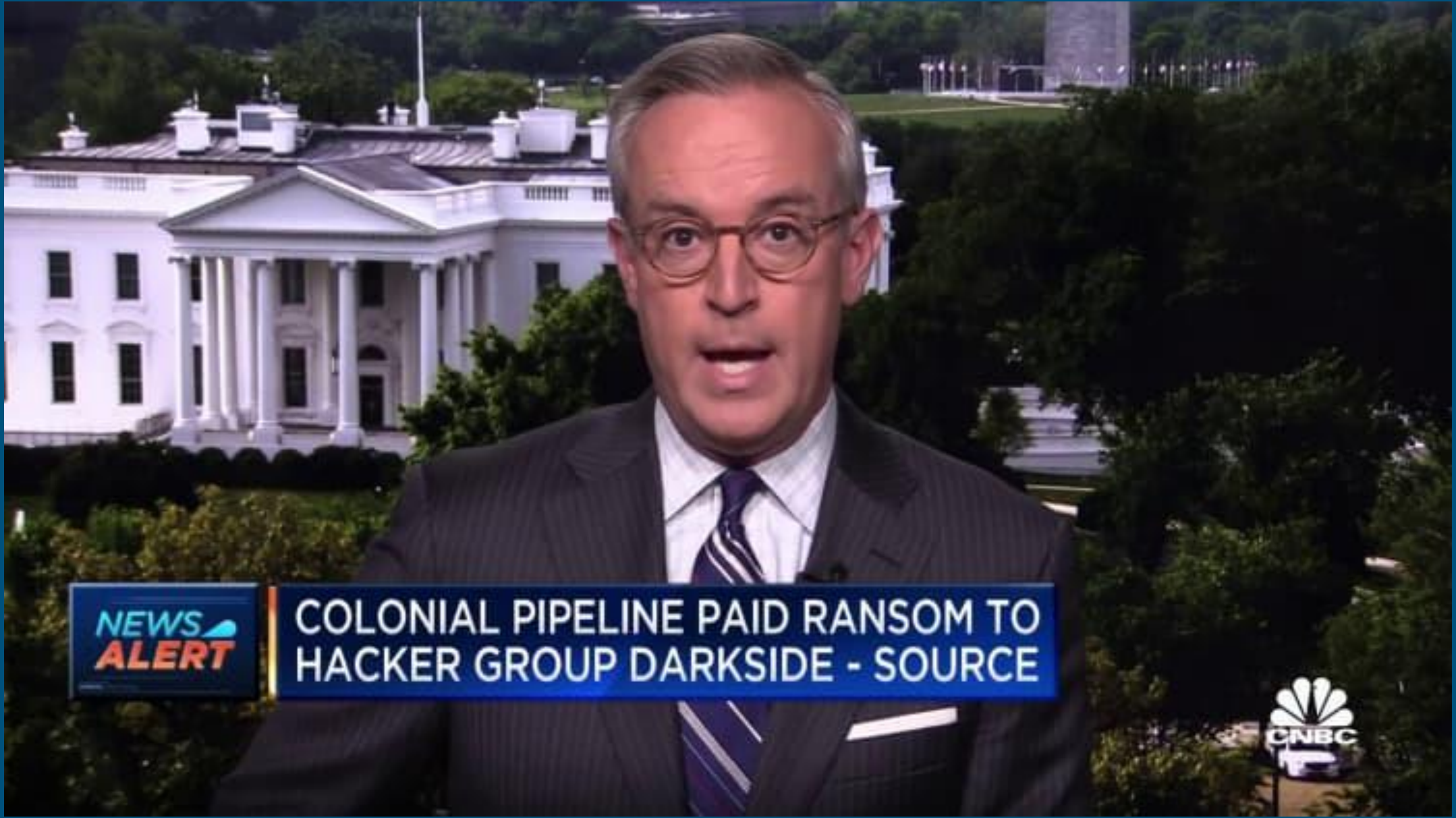
● Main weekend delivery locations



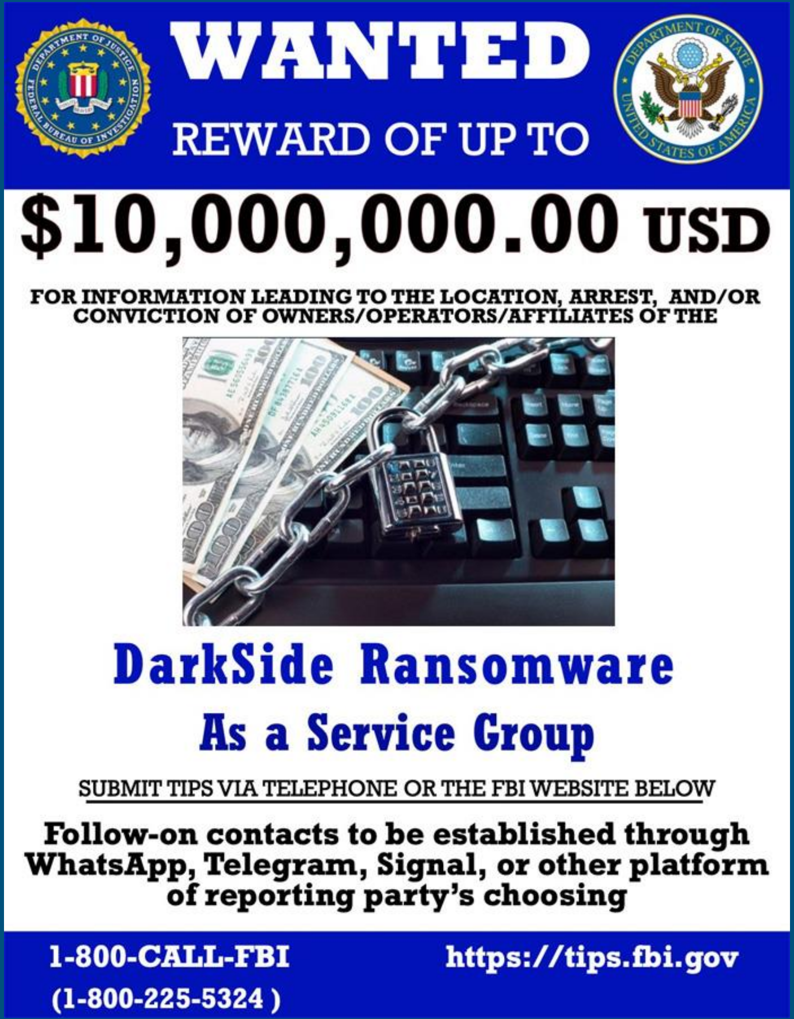
Source: Colonial Pipeline Company


DARKSIDE

BUY 3, SAVE
10¢
ON GAS
RED BULL
STOP
ENGINE
NO
SMOKING
PERSONS USING
DISPENSERS
WITH HOLD-OPEN
LATCHES MUST
REMAIN AT THE
REFUELING POINT
DURING REFUELING
IT IS UNLAWFUL
TO DISPENSE
GASOLINE INTO
UNAPPROVED
CONTAINERS
WARNING - FIRE HAZARD
DIESEL
UNLEADED
UNLEADED PLUS
PREMIUM
87
89
93
25,000
SURE can



COLONIAL PIPELINE PAID RANSOM TO HACKER GROUP DARKSIDE - SOURCE



WANTED

REWARD OF UP TO

$10,000,000.00 USD

FOR INFORMATION LEADING TO THE LOCATION, ARREST, AND/OR CONVICTION OF OWNERS/OPERATORS/AFFILIATES OF THE

DarkSide Ransomware As a Service Group

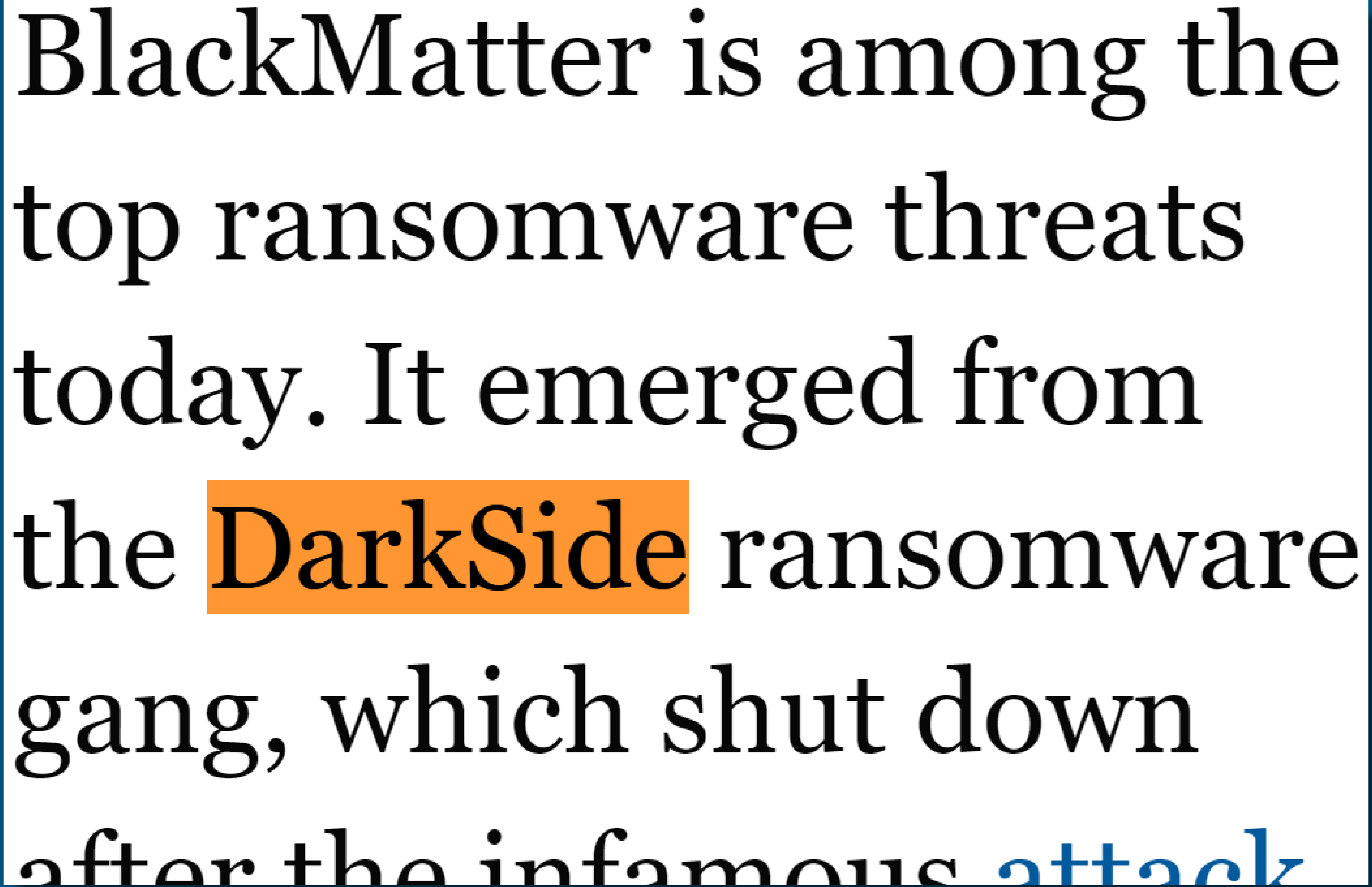
SUBMIT TIPS VIA TELEPHONE OR THE FBI WEBSITE BELOW

Follow-on contacts to be established through WhatsApp, Telegram, Signal, or other platform of reporting party's choosing

1-800-CALL-FBI
(1-800-225-5324)

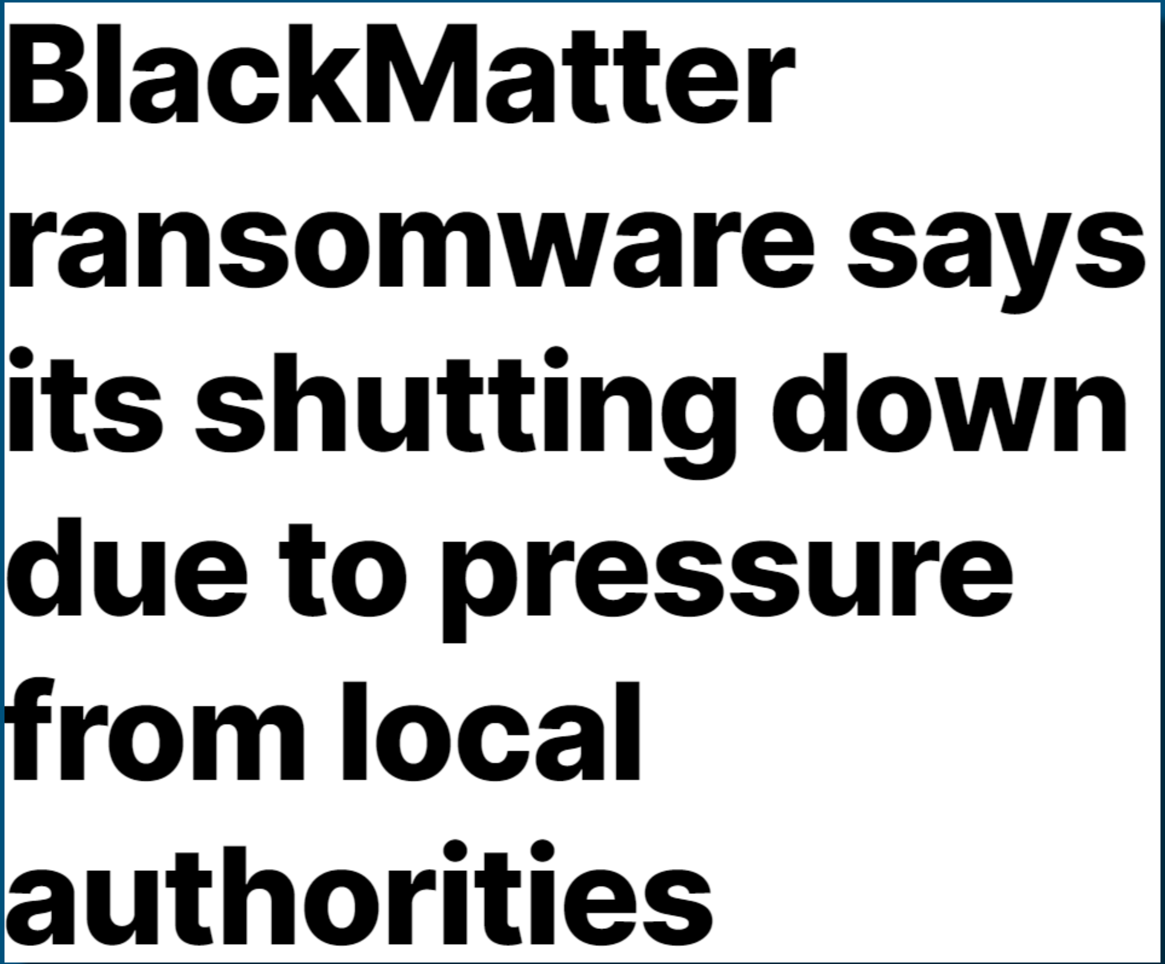
https://tips.fbi.gov

THIS IS
FINE



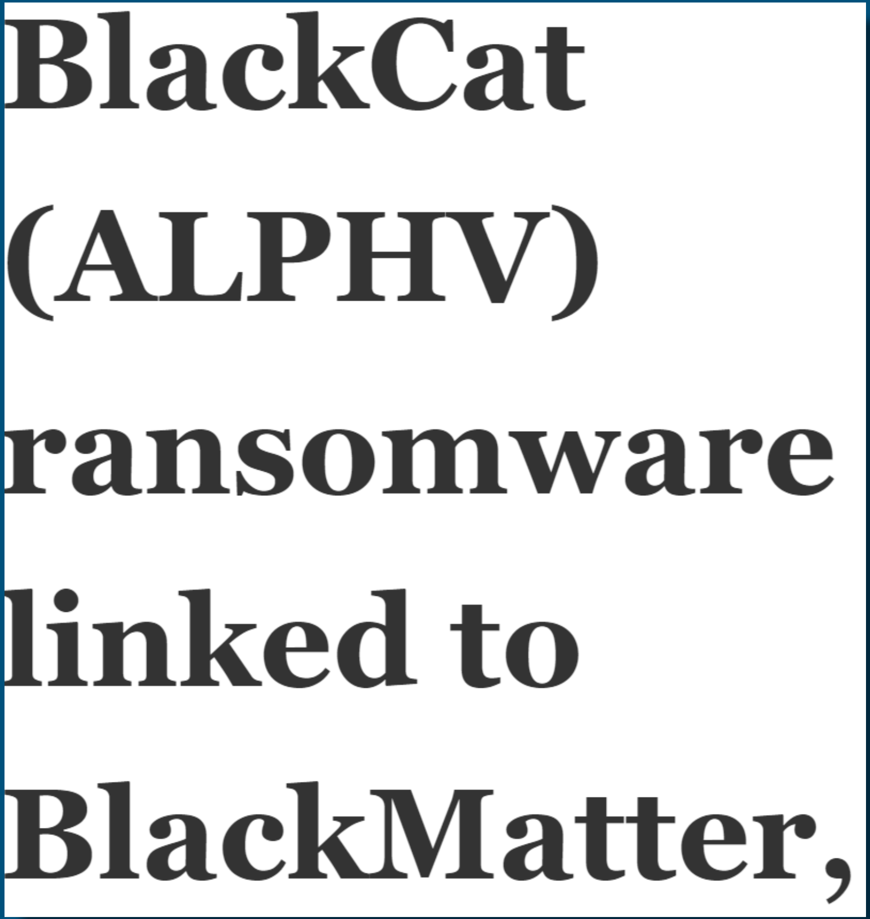
BlackMatter is among the top ransomware threats today. It emerged from the DarkSide ransomware gang, which shut down after the infamous attack

https://www.bleepingcomputer.com/news/security/fbi-cisa-nsa-share-defense-tips-for-blackmatter-ransomware-attacks/



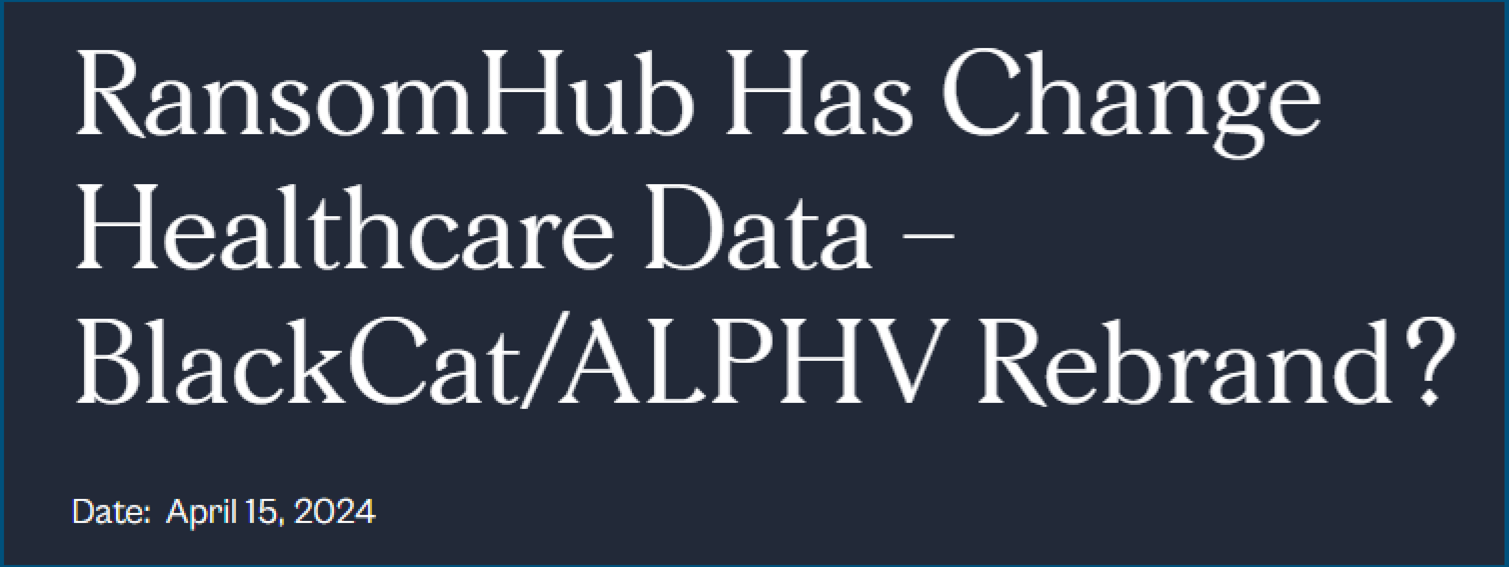
BlackMatter ransomware says its shutting down due to pressure from local authorities

https://therecord.media/blackmatter-ransomware-says-its-shutting-down-due-to-pressure-from-local-authorities



BlackCat (ALPHV) ransomware linked to BlackMatter,

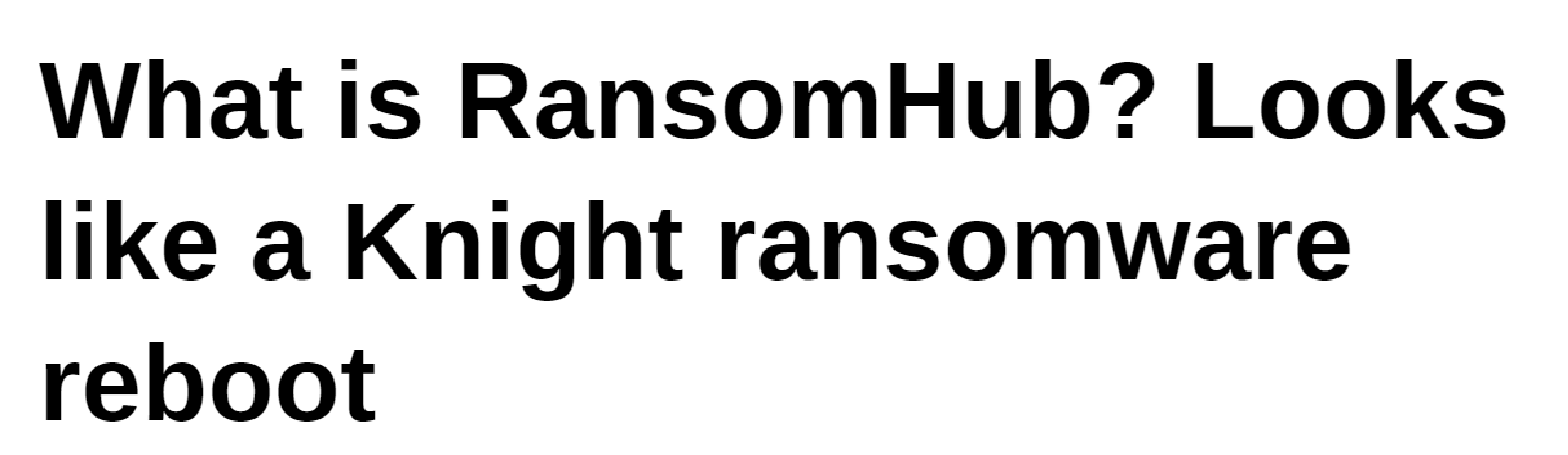
https://www.bleepingcomputer.com/news/security/blackcat-alphv-ransomware-linked-to-blackmatter-darkside-gangs/



RansomHub Has Change Healthcare Data – BlackCat/ALPHV Rebrand?

Date: April 15, 2024

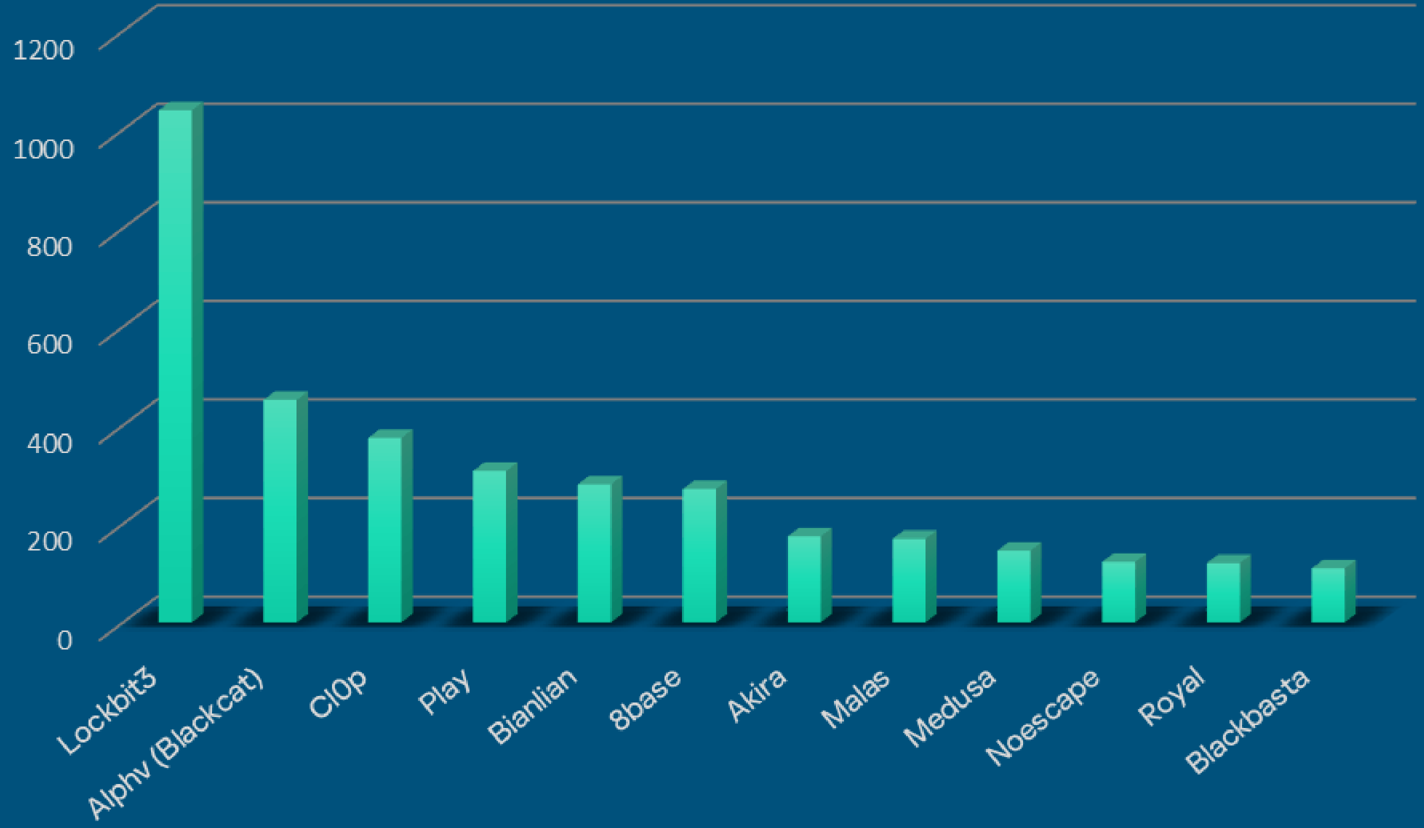
https://ransomwareattacks.halcyon.ai/news/ransomhub-has-change-healthcare-data---blackcat-alphv-rebrand



What is RansomHub? Looks like a Knight ransomware reboot

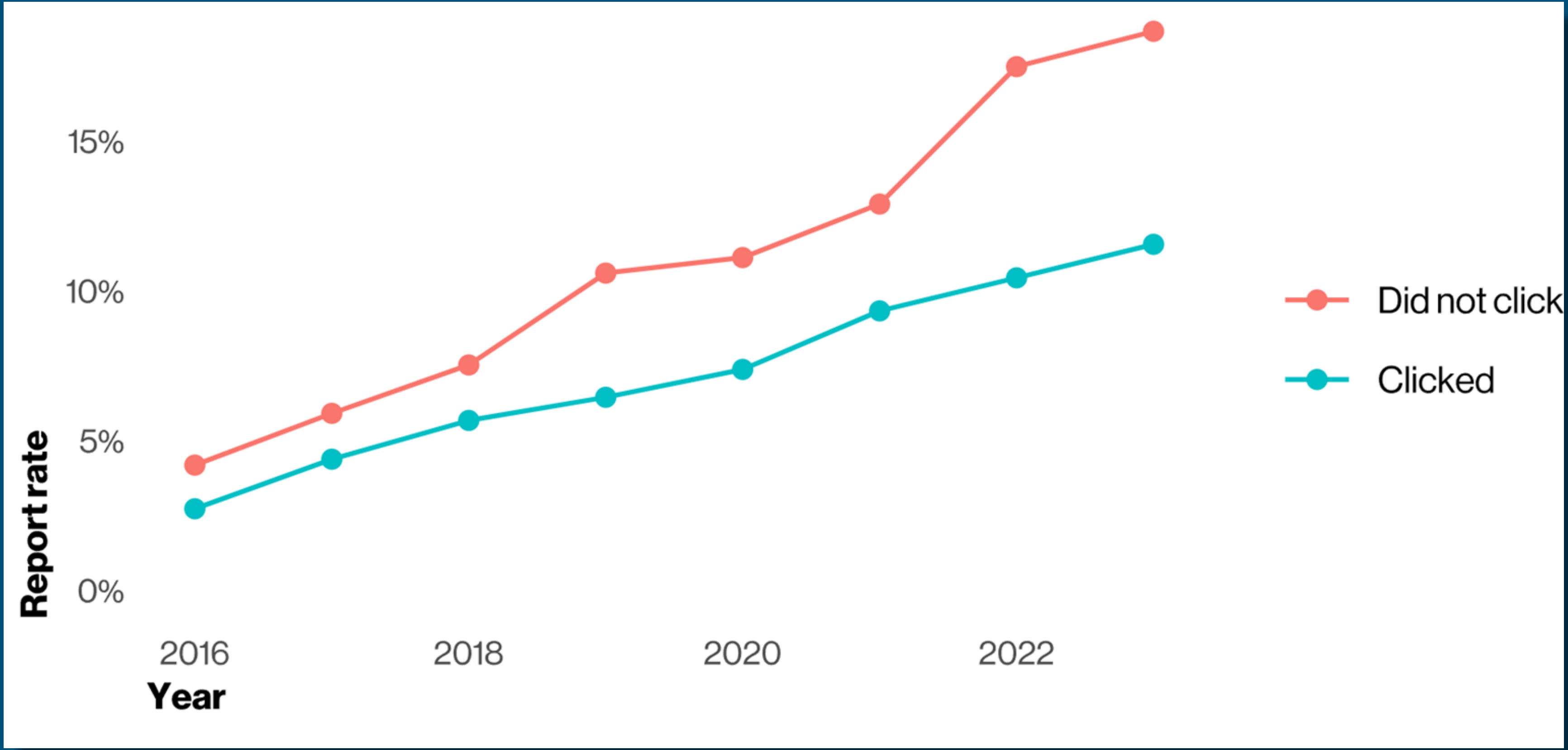
https://www.theregister.com/2024/06/05/ransomhub_knight_reboot/

Ransomware Threat Landscape



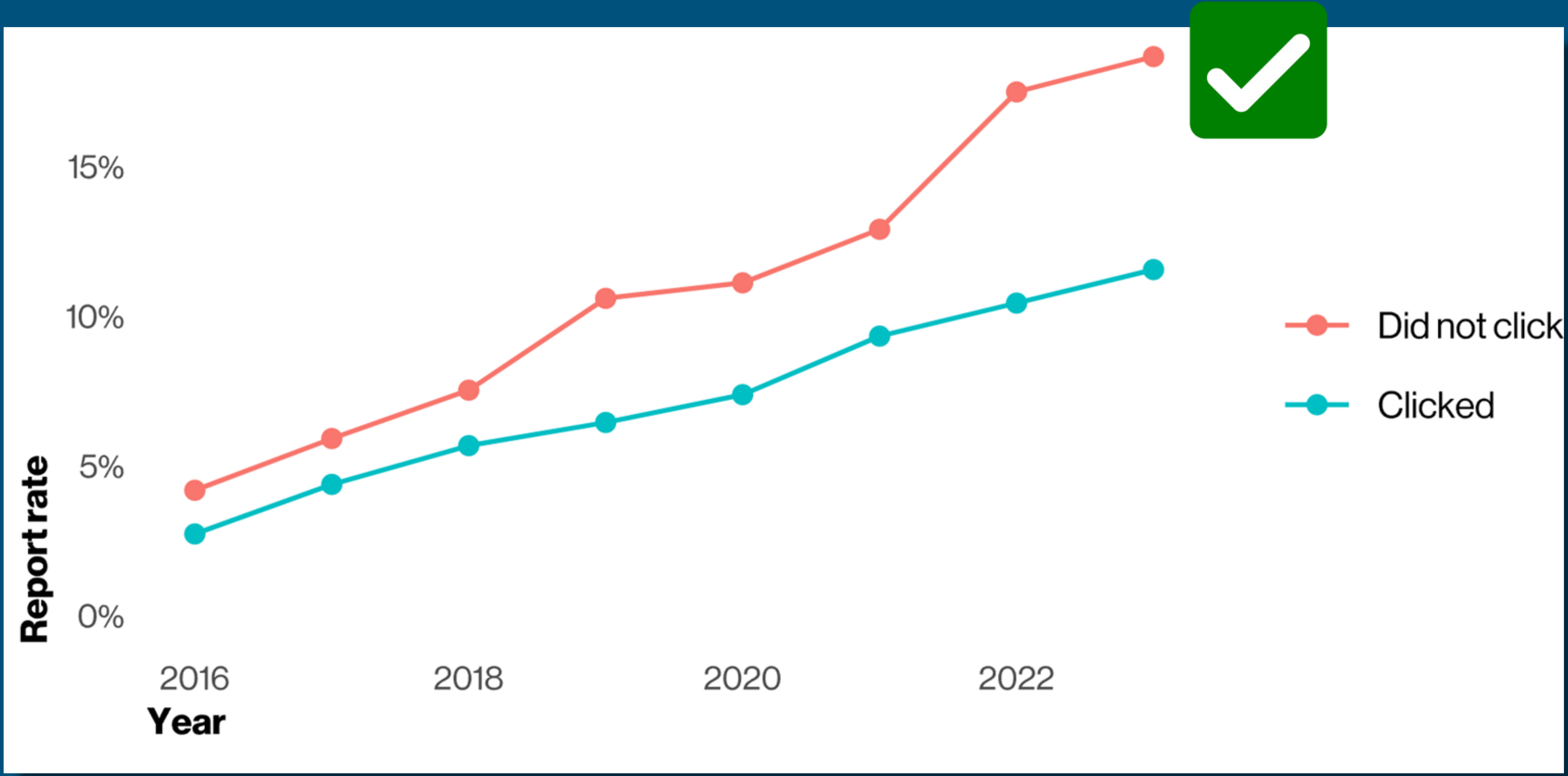
https://securelist.com/state-of-ransomware-2023/112590/

Technique Trends



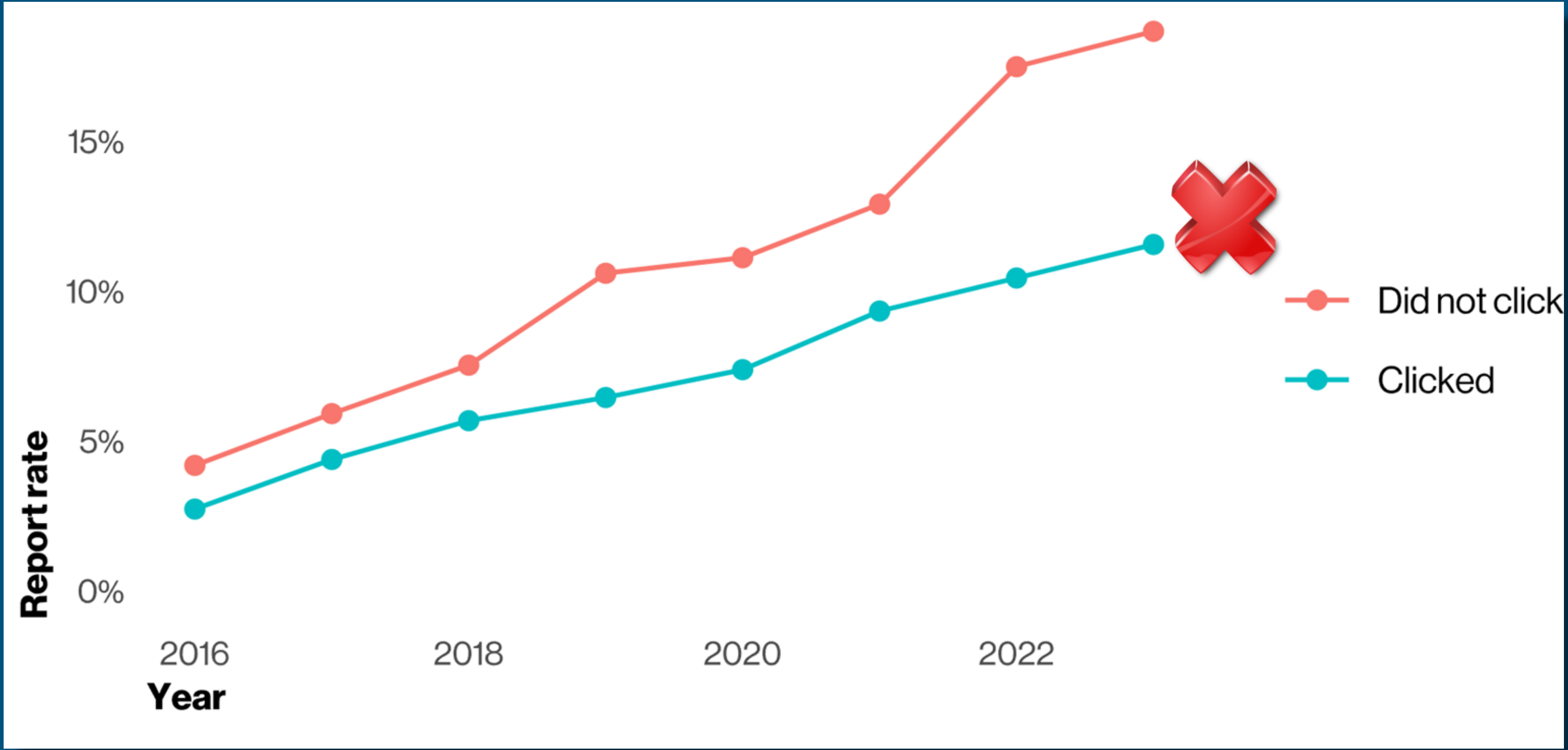
Phishing email report rate by click status

Verizon 2024 Data Breach Investigations Report



Phishing email report rate by click status

Verizon 2024 Data Breach Investigations Report



Phishing email report rate by click status

Verizon 2024 Data Breach Investigations Report

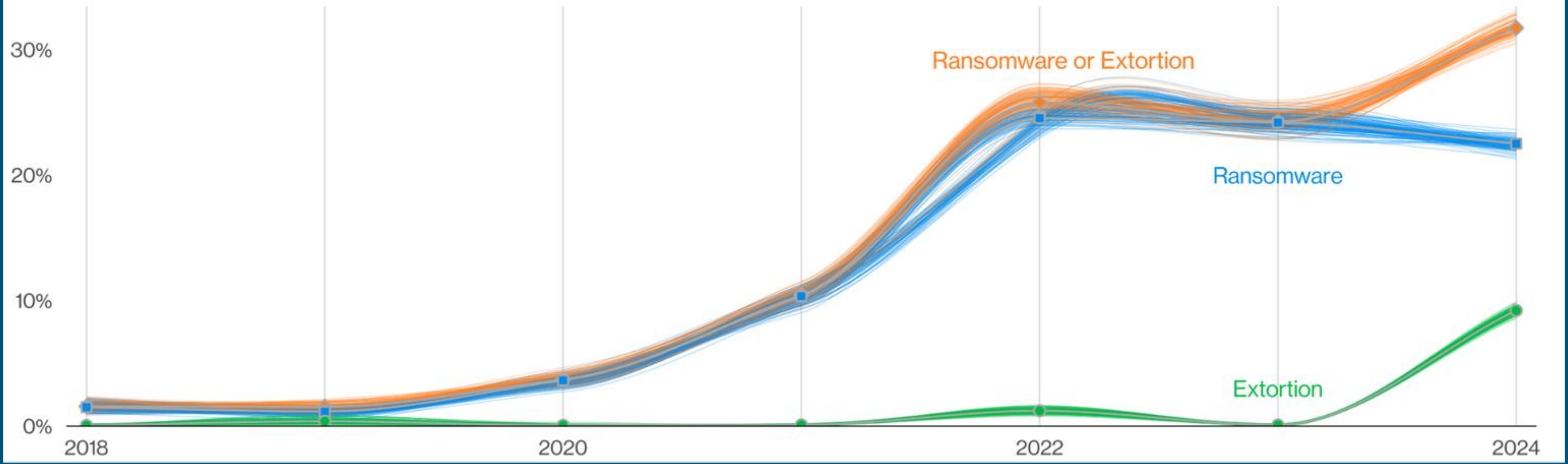
Quick Definition

Ransomware

Malicious software that encrypts a victim's files, rendering them inaccessible, and demands a ransom payment for the decryption key.

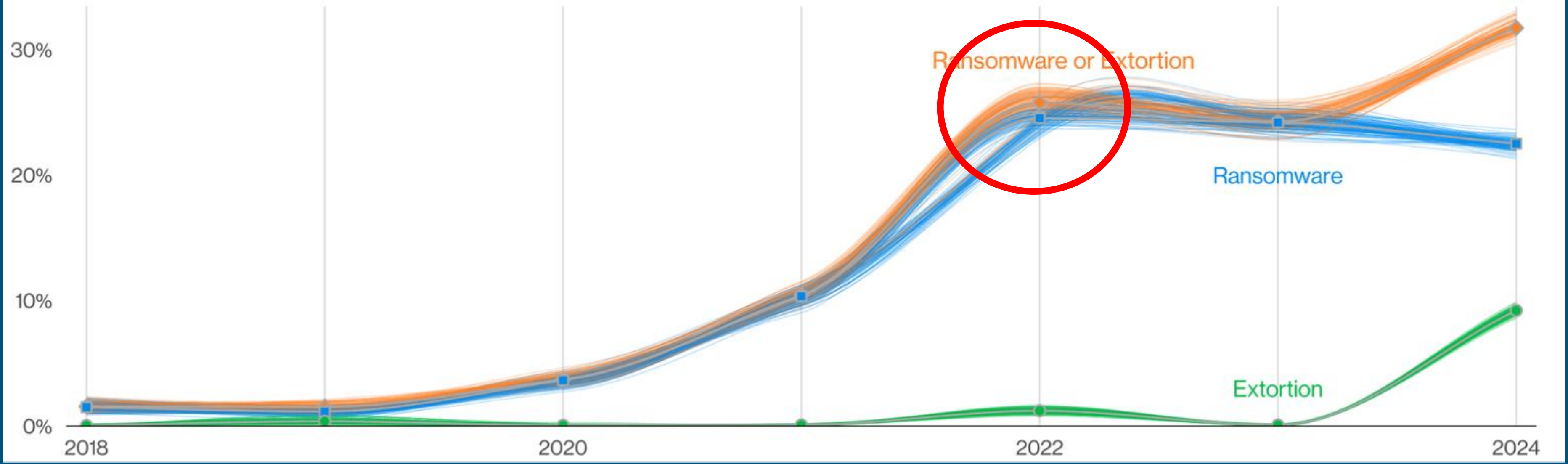
Extortion

Threatening to release sensitive data or disrupt services unless a payment is made.



Ransomware and Extortion breaches over time

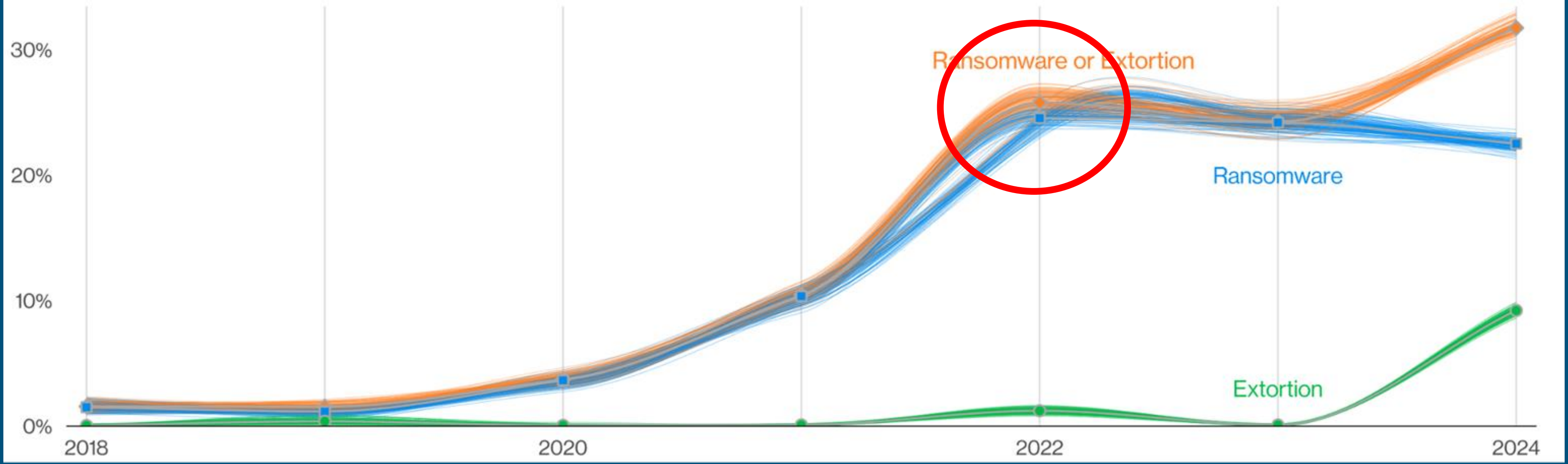
Verizon 2024 Data Breach Investigations Report



Ransomware and Extortion breaches over time

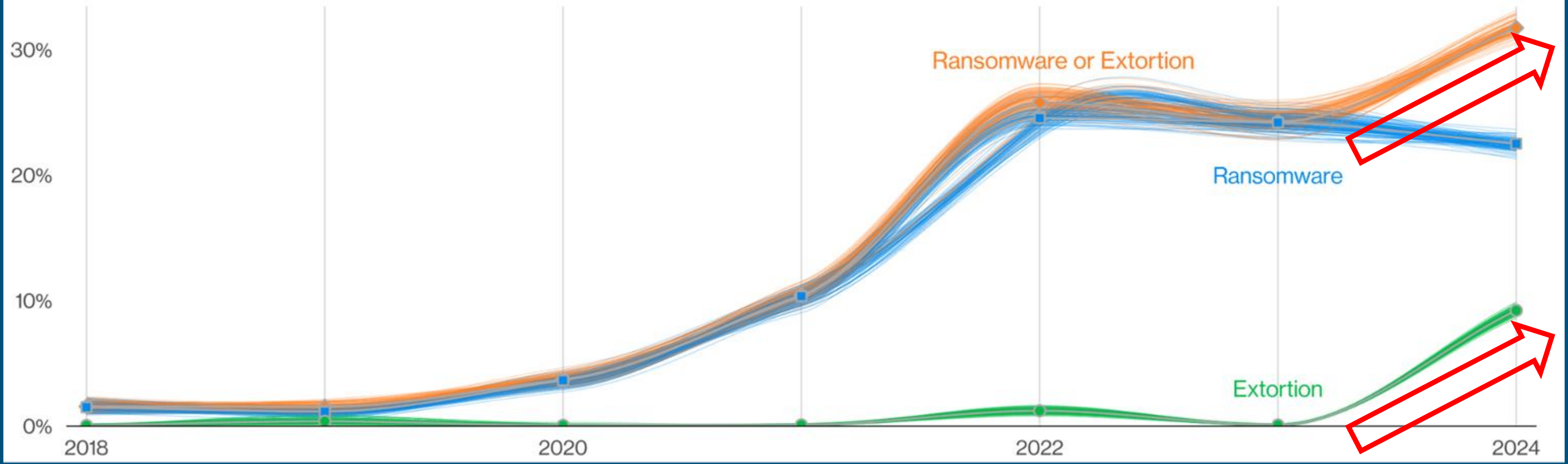
Verizon 2024 Data Breach Investigations Report

Misleading Industry Statistics



Ransomware and Extortion breaches over time

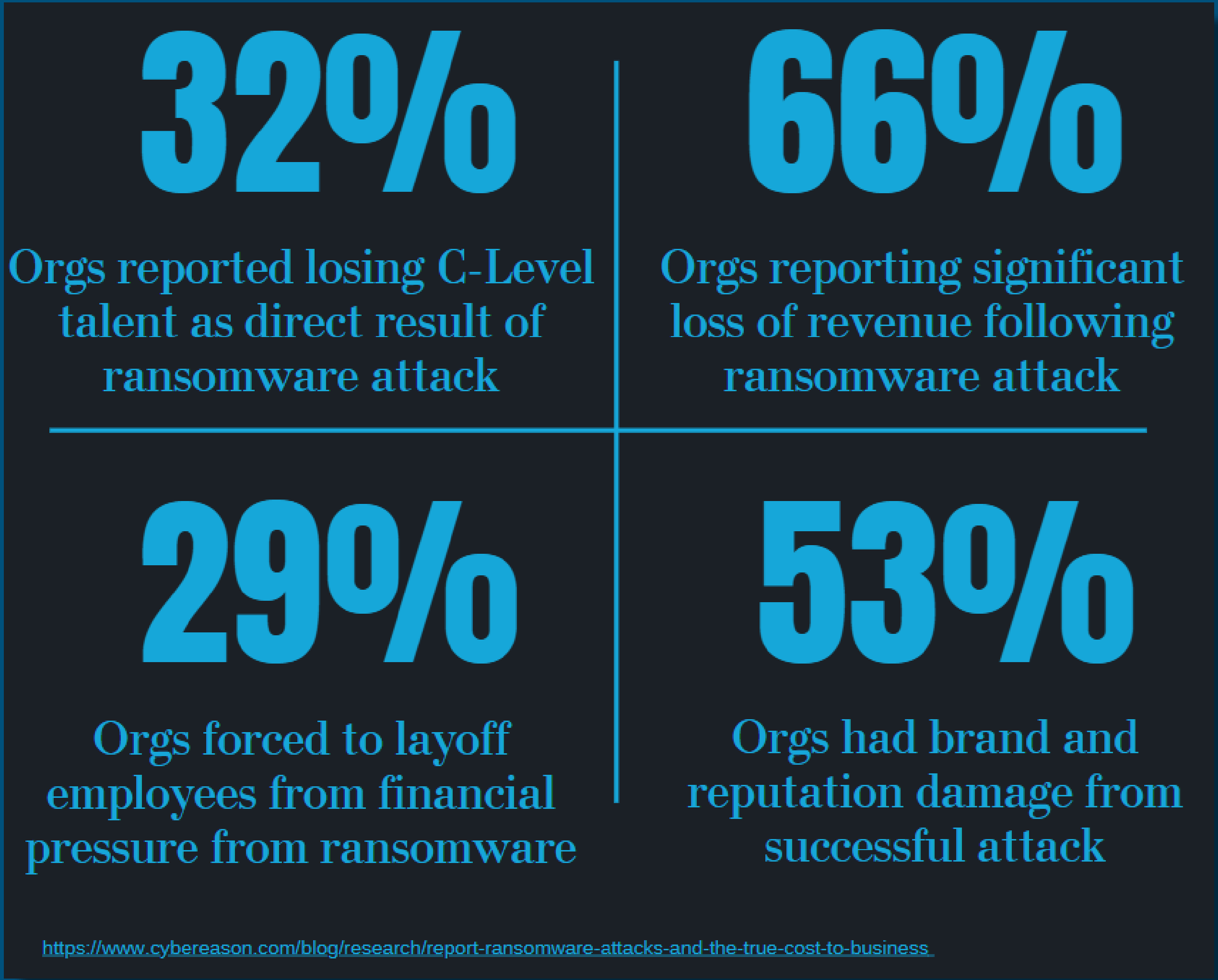
Verizon 2024 Data Breach Investigations Report



Ransomware and Extortion breaches over time

Verizon 2024 Data Breach Investigations Report

Quantified Impact



32%

Orgs reported losing C-Level talent as direct result of ransomware attack

66%

Orgs reporting significant loss of revenue following ransomware attack

29%

Orgs forced to layoff employees from financial pressure from ransomware

53%

Orgs had brand and reputation damage from successful attack

https://www.cybereason.com/blog/research/report-ransomware-attacks-and-the-true-cost-to-business

Ransomware Future

Continued division of skill (Specialists)

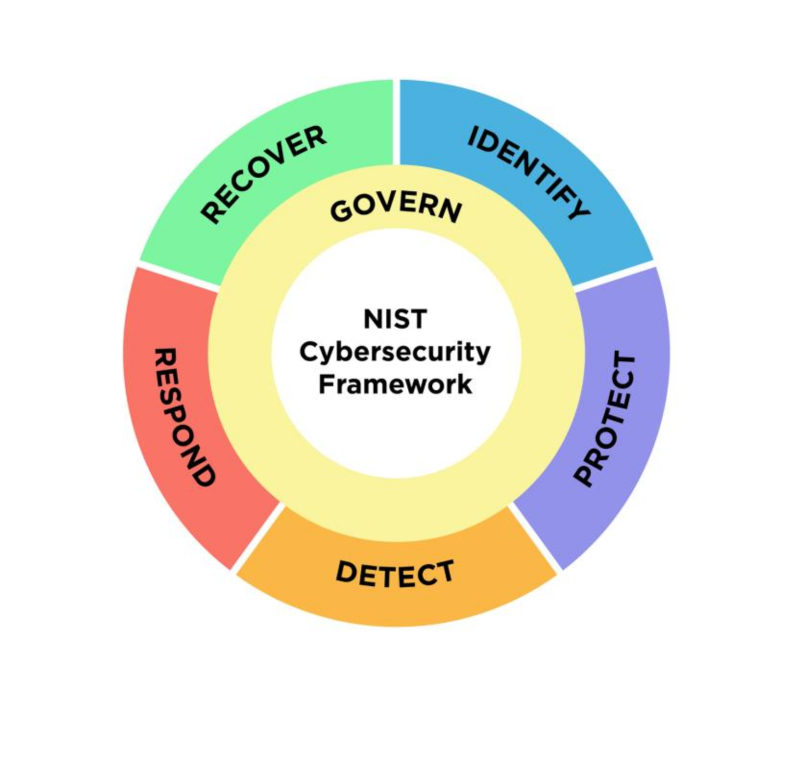
Decline in ransom payment

Increase in extortion (Data Exfil)

Increase in international law enforcement / OFAC

HOT TAKE - Overall threat decline in 3 years

Best Practices for Mitigation



Identify/Protect

PEOPLE

Phishing

TTX

PROCESS

Backups (Taken, Tested, Documented)

TECHNOLOGY

EDR

MFA

Patch Management

Detect/Respond/Recover

PEOPLE

“Activation” Triggers

Defined Roles

PROCESS

Restoration Order

Lessons Learned

TECHNOLOGY

Quarantine / Threat Hunt

Supply Chain and Data Governance

85%

By 2025, 85% of business apps will be SaaS-based.

https://pages.bettercloud.com/rs/719-KZY-706/images/2020_StateofSaaSOpsReport.pdf

Not all Cloud

On-premise IT vendor managed solutions

Like What?

Solarwinds Orion

This supply chain attack affected thousands of organizations, including U.S. federal agencies.

MoveIT

Zero-day in the MOVEit file transfer software

OSF Healthcare Data Breach | MOVEit Class Action Lawsuit

WRITTEN BY JOSEPH LYON ON MARCH 7, 2024. POSTED IN DATA BREACH.

Log4j

Critical vulnerability in the widely-used Log4j logging library, allowing remote code execution

Let’s Control This…

Identifying Vulnerabilities

Security questionnaires…

Identifying Vulnerabilities

We are not going to:

1. Phish our supply chain
2. Vulnerability Scan and Exploit our supply chain
3. Mail USB Malware to our supply chain

Pentest Report?

Building Resilience

Access Control

1. Federated authentication where possible
2. MFA (lowkey requirement)
3. Network Segmentation (on-prem)
4. Zero Trust Architecture (ZTA)

Building Resilience

Data Governance

1. End user training (easy to do, tough implementation)
   a. Dummy / Limited data sets for pilots
2. Data retention / deletion contractual requirements
3. “This data” is breached TTX

Managing Exposure Risks

Managing Exposure Risks

Fundamentals

Managing Exposure Risks

Educate business on data use

Multiple Audiences (Execs, Workforce, Researchers)

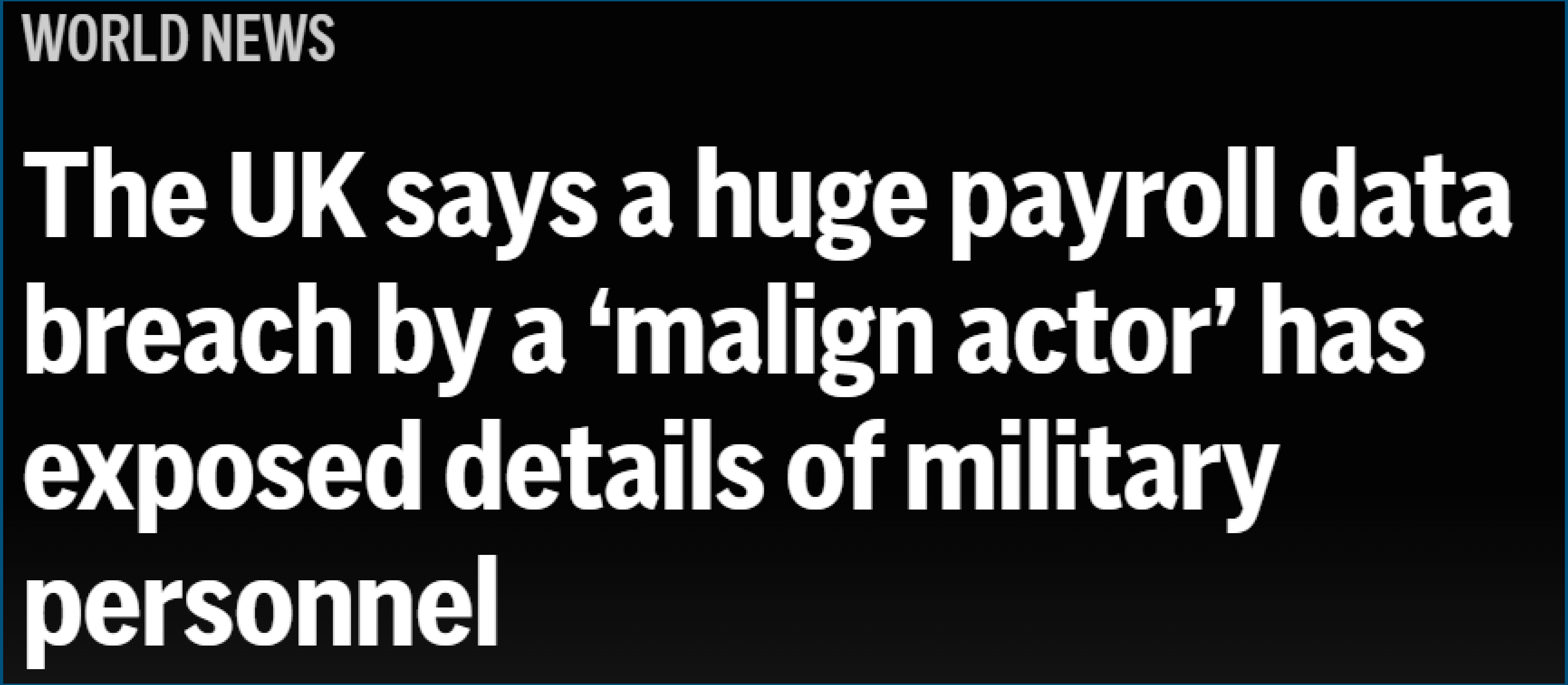
SDLC

Include Site-to-Site Network Connections

Data Retention at Vendor, Contract Language

….and Validation

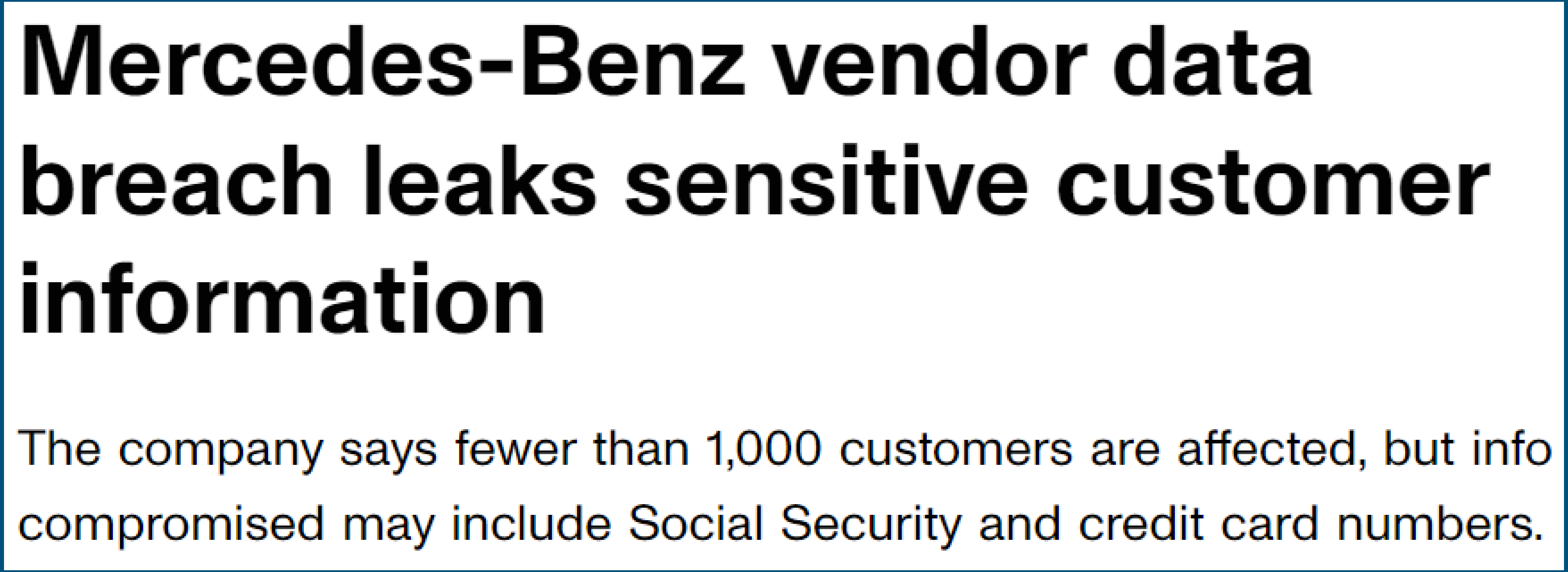
A Quick Note To You “Contract Risk Pass Through”



WORLD NEWS

The UK says a huge payroll data breach by a ‘malign actor’ has exposed details of military personnel

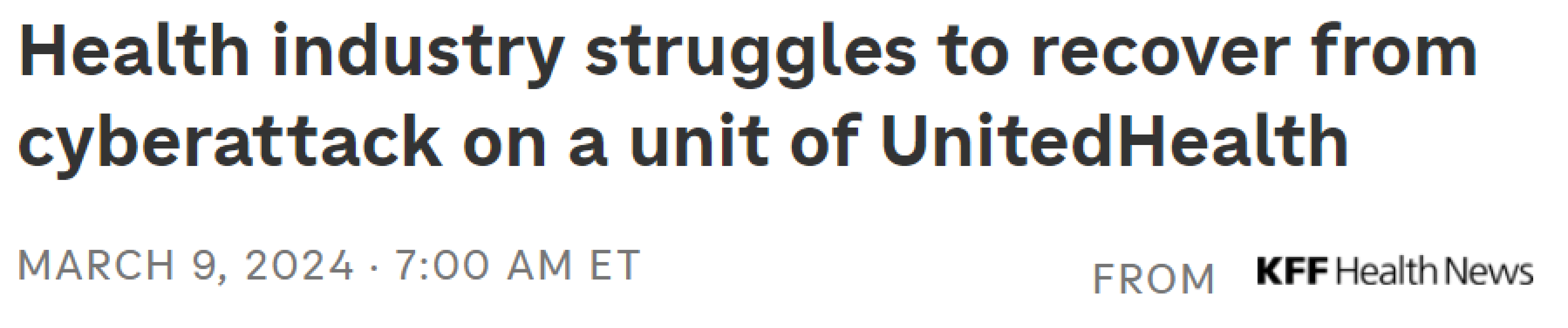
A Quick Note To You “Contract Risk Pass Through”



Mercedes-Benz vendor data breach leaks sensitive customer information

The company says fewer than 1,000 customers are affected, but info compromised may include Social Security and credit card numbers.

A Quick Note To You "Contract Risk Pass Through"



Health industry struggles to recover from cyberattack on a unit of UnitedHealth

MARCH 9, 2024 · 7:00 AM ET

FROM KFF Health News

Leveraging Artificial Intelligence in Cybersecurity

AI in Security Operations (SecOps)

- Threat Detection and Response
  - Anomaly Detection
  - Automated Incident Response
- SIEM
  - Predictive Threat Intelligence
- IAM
  - Behavioral Biometrics
  - Adaptive Authentication

Threat Actors and AI

Automated Vulnerability Scanning and Exploitation

- Scanners with context on findings
- Automated Exploit Generation

Social Engineering

- AI-Generated Phishing Campaigns
    - Chatbots for Scams

Obfuscation

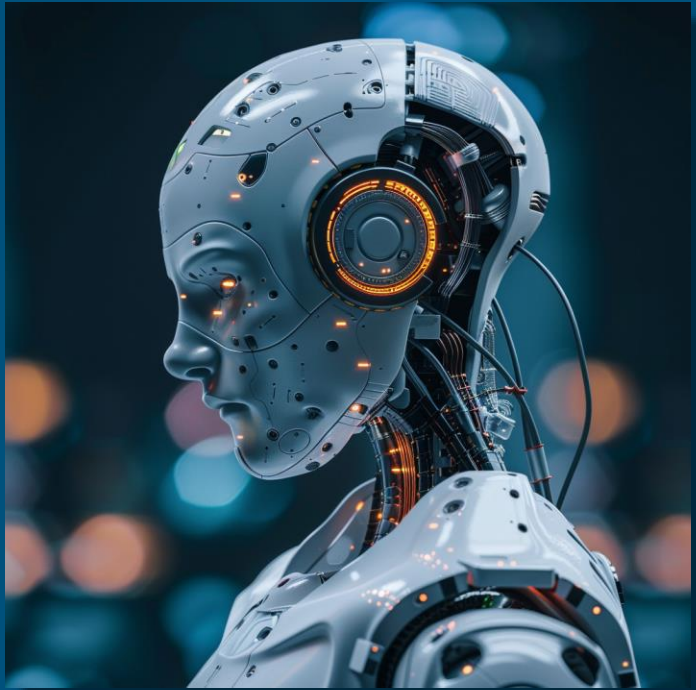
- Synthetic Media
- Deepfakes

Balancing AI Opportunities and Risks

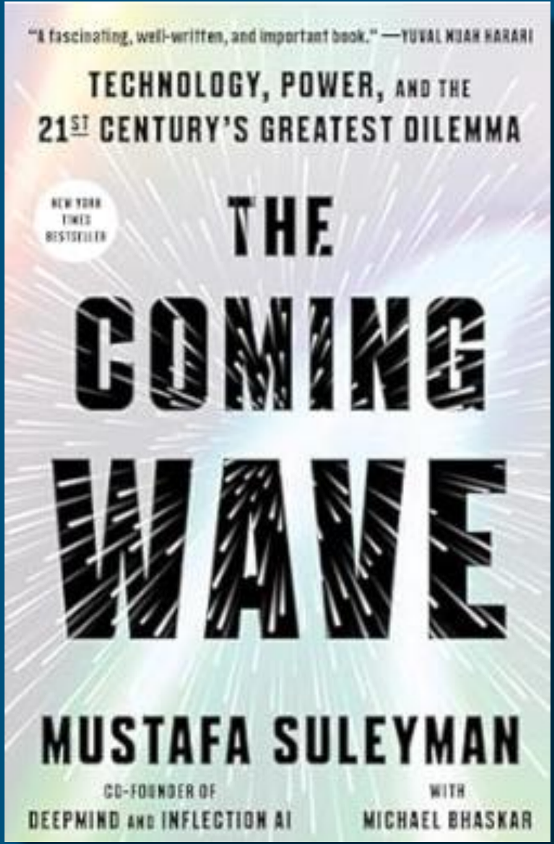
Bias and Ethics

Balance AI Automation and Human Oversight

Chief AI Officer



Cyber AI Future



"A fascinating, well-written, and important book." —YUVAL NOAH HARARI

TECHNOLOGY, POWER, AND THE 21ST CENTURY'S GREATEST DILEMMA

NEW YORK TIMES BESTSELLER

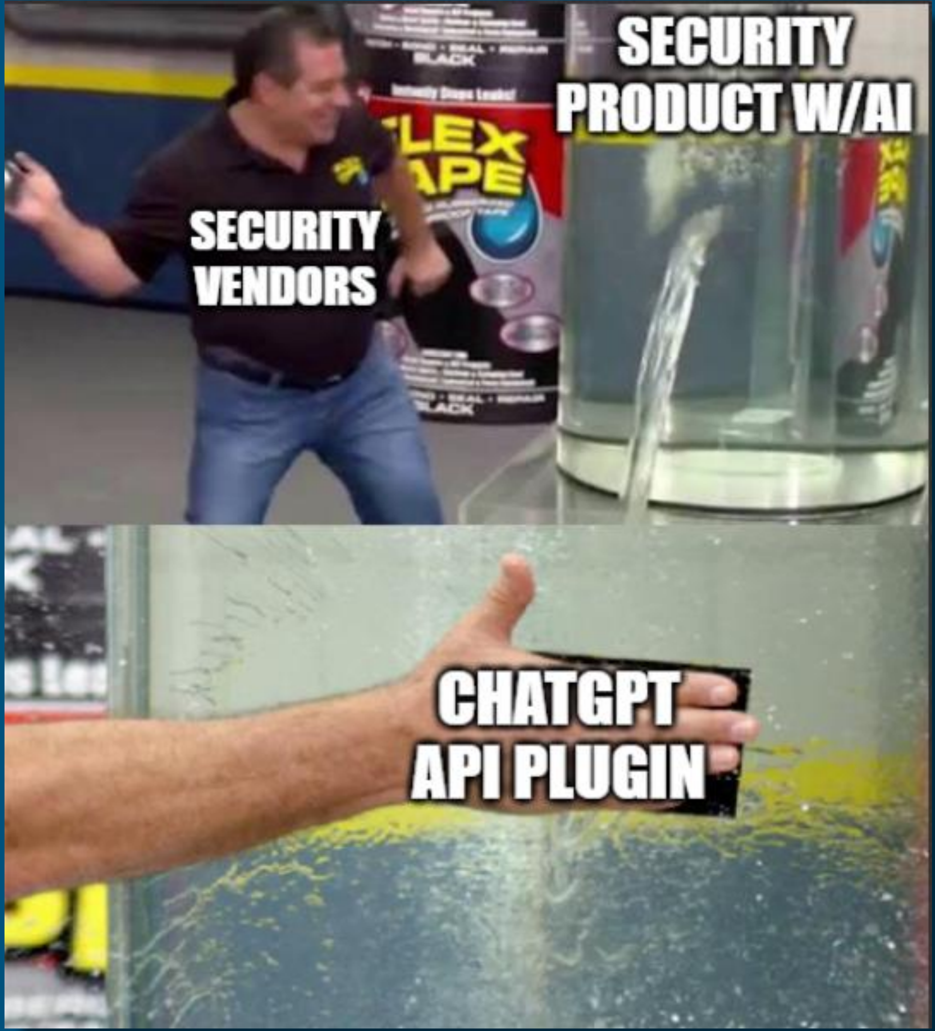
THE COMING WAVE

MUSTAFA SULEYMAN

CO-FOUNDER OF DEEPMIND AND INFLECTION AI

WITH MICHAEL BHASKAR

A Word of Caution...



Actually, 2 Words of Caution...

Dear CIO,

What is our position on AI?

-Everybody

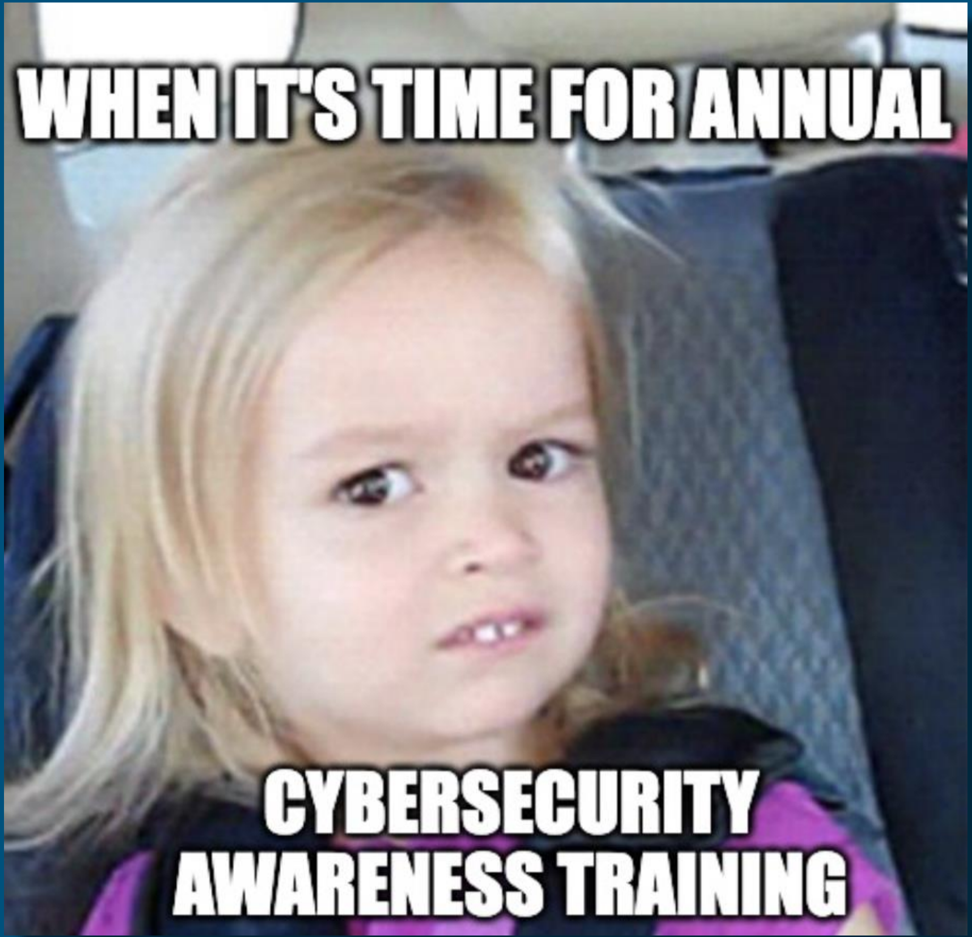
Empowering the Workforce for Cyber Resilience

Cyber Awareness Culture

What has 2 Thumbs and Loves the Impact of Effective Cyber Awareness Training?

This Guy!

WRONG!


WHEN IT'S TIME FOR ANNUAL
CYBERSECURITY AWARENESS TRAINING

Cyber Awareness Culture

Empowers Staff

Educates Staff

Connects a “Human” to Cyber

Beyond Phishing

Education needs to be relatable

Answers ”So what?”

Key point needs to be digestible

Beyond Phishing

1 Point in Messaging

Tie to Personal (Finances, Family)

2-3 Sentences, Graphic

Leverage “Salacious”, “Mainstream”

How This Drives Cyber Risk Reduction

Modifying Personal Behaviors

More Likely to Self Report

See Something / Say Something

Workforce Future...

Learning Outcomes and Actionable Steps

Recap of Learning Outcomes

Ransomware (and adjacent) Continues to Crush

Supply Chain Wicked Hard to Control Risk

AI……Ride the Lightning

Effective Workforce Training → Material ROI

Implementing Strategies

Holistic Frameworks and Vigilance for Ransomware

“The Coming Wave” Mustafa Suleyman: Book for AI Future

Data Governance for Supply Chain (Real convos with leadership)

Impactful Awareness Program

Resources and Community Engagement

Simply Cyber: Daily Cyber Threat Brief
https://simplycyber.io/streams

Mitre ATT&CK
https://attack.mitre.org/

NIST CSF 2.0
https://www.nist.gov/cyberframework

H-ISAC
https://h-isac.org/

CISA Known Exploited Vulns Catalog
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Thank You

Gerald Auger, PhD

Gerald@SimplyCyber.io

SimplyCyber.io/Socials