Learning from History: What Past Cyber Attacks Can Teach Us

Jeff Foresman, President of Services

QUADRANT
INFORMATION SECURITY

Agenda

- The State of Cybersecurity
- Cyber Attack Case Studies
- A “Newish” Defense-in-Depth Approach

QUADRANT
INFORMATION SECURITY

2A 3732C20616E642070617463
2C10766C6206C6974746C65 16E
C3100A16C20Data BreachE2046 5
12202E6F61636865732046C6974
7 01Cyber Attack696EA1 486F

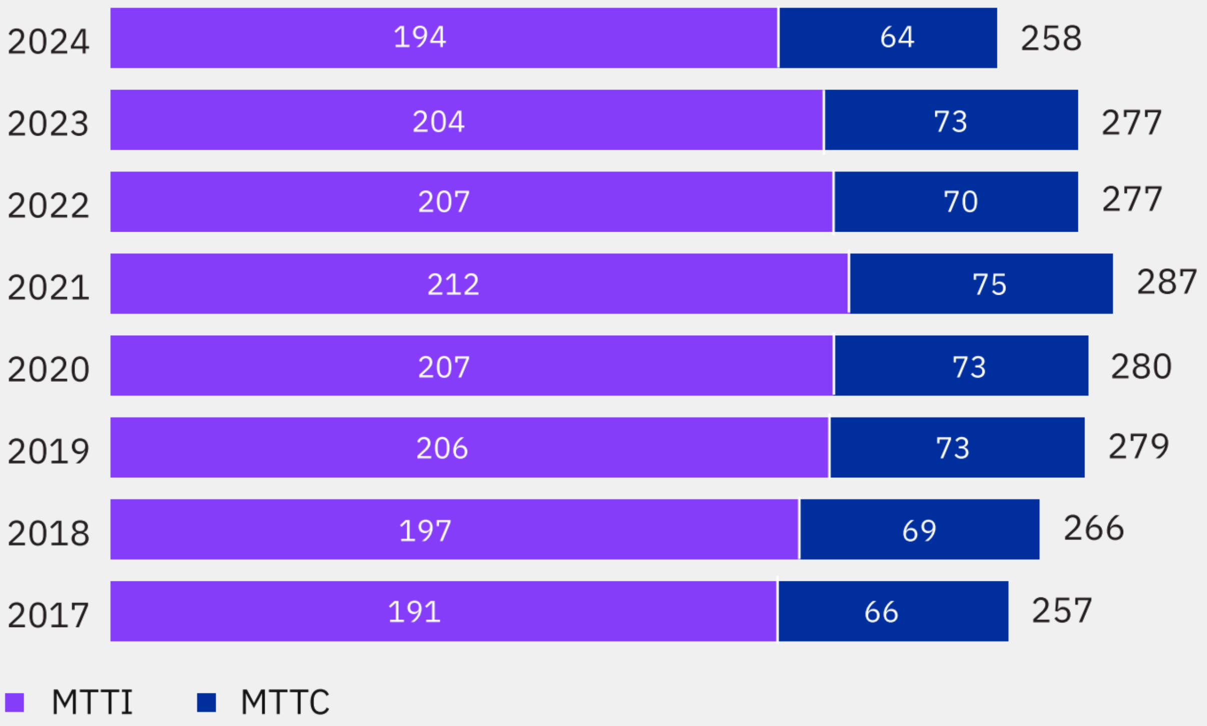
The State of Cybersecurity

QUADRANT
INFORMATION SECURITY

State of Cybersecurity

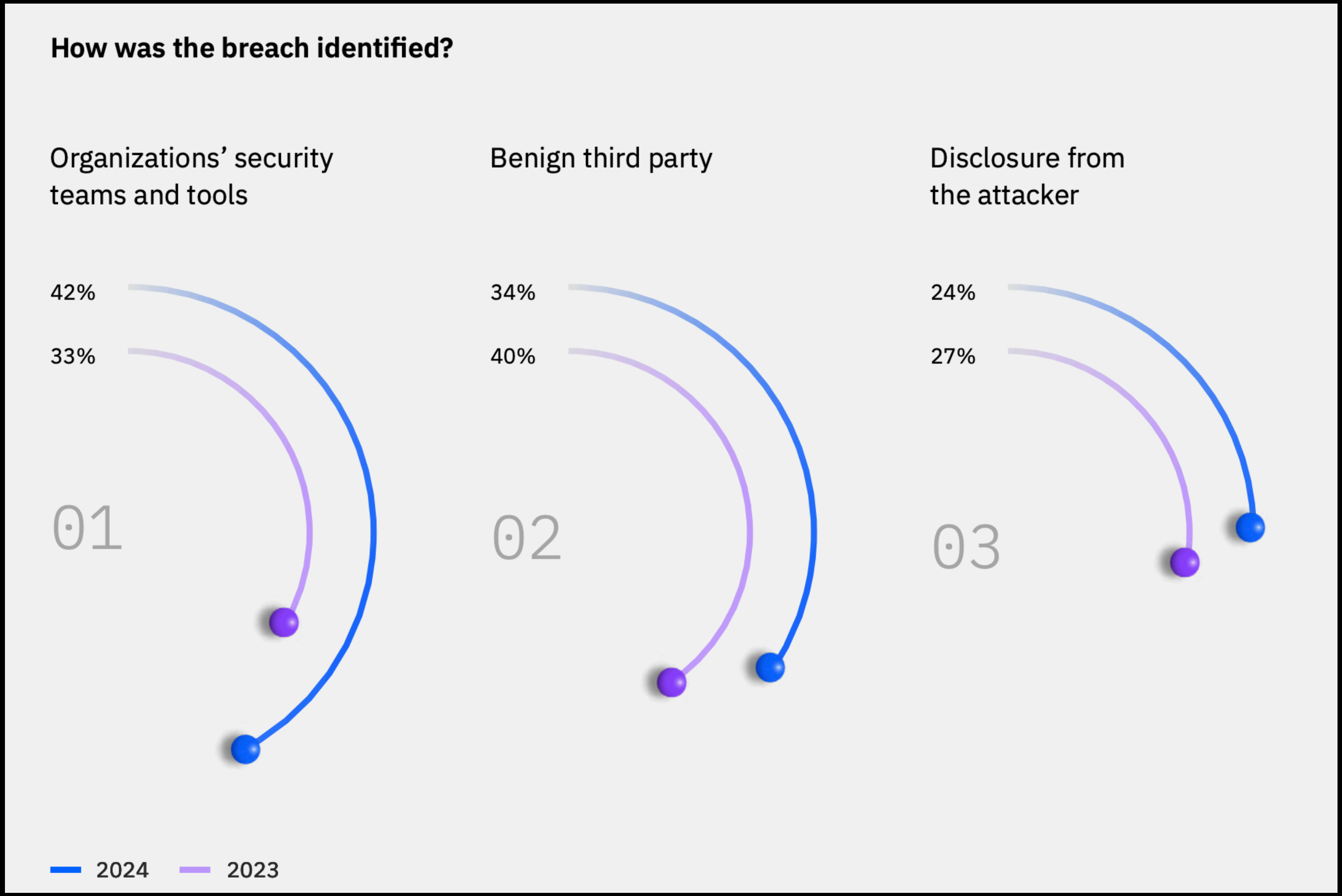
- **$4.88 Million**
  The average global cost of a data breach
- **$9.36 Million**
  The average cost of a data breach in the US
- **258 Days**
  average time to identify and contain a data breach

Time to identify and contain a data breach



IBM Cost of a Data Breach Report 2024

Are we getting better at detecting attacks?

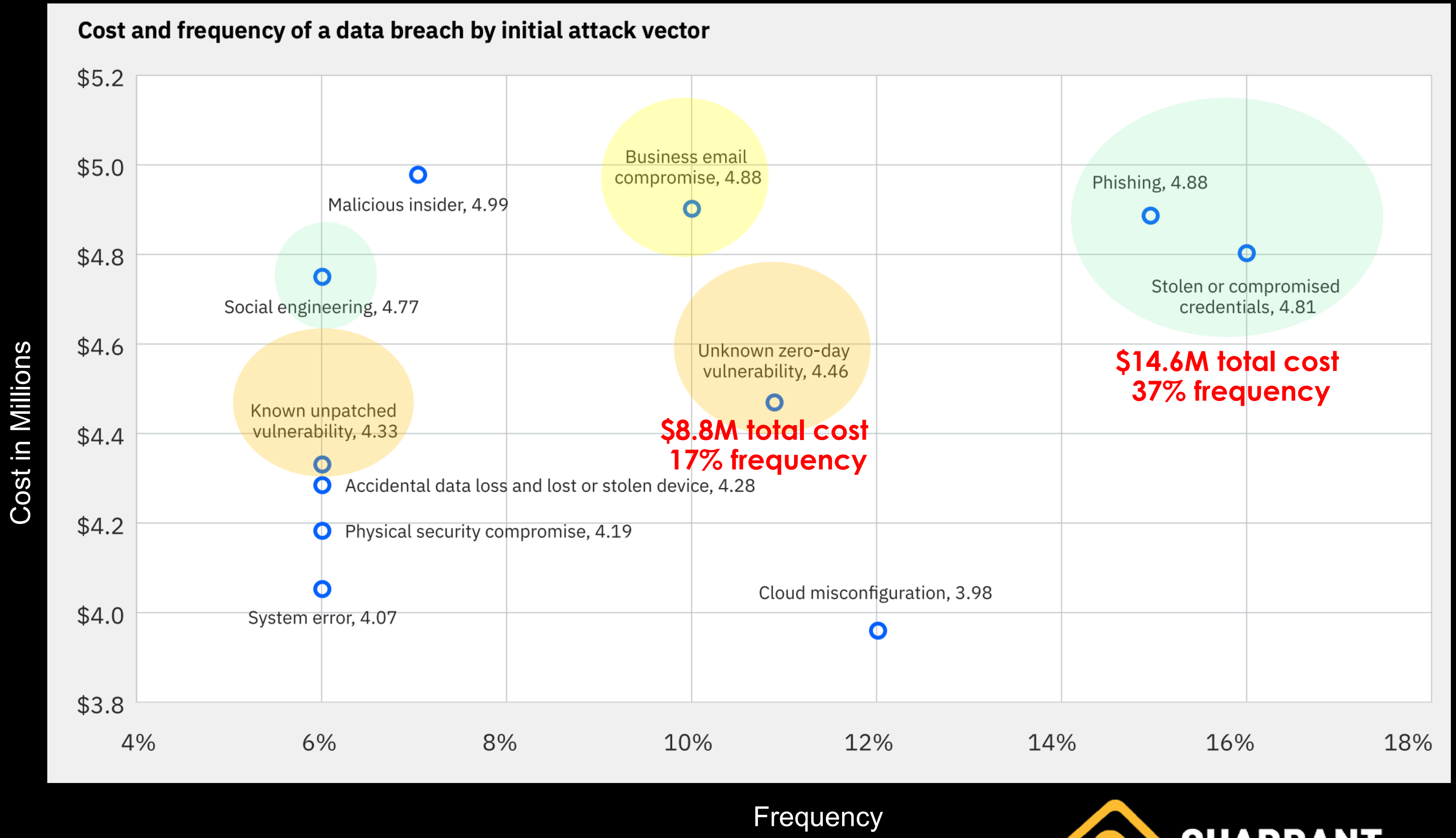


- YES!
- 42% of breaches were identified by the organization's security teams and tools
- 24% of breaches were disclosed by the attacker

Cost and Frequency of Cyberattacks

- We need to understand the cost versus frequency of cyber attacks in developing our security programs
- 74% of breaches involve a human element
- External actors are involved in 83% of attacks

Cost and frequency of a data breach by initial attack vector



$14.6M total cost
37% frequency

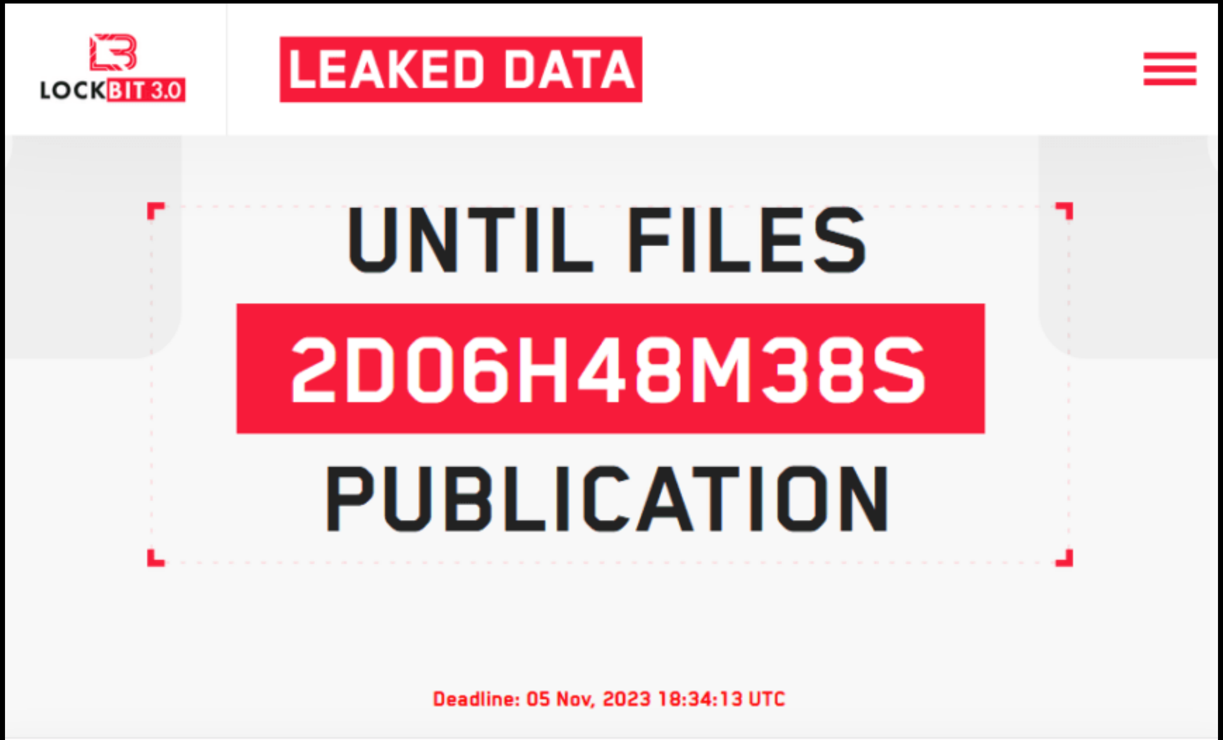
$8.8M total cost
17% frequency

IBM Cost of a Data Breach Report 2024

QUADRANT
INFORMATION SECURITY

Ransomware

- In 2015, ransomware accounted for less than 1% of monthly cyber attacks
- In 2023, ransomware attacks accounted for over half (52%) of monthly attacks
- In five years, the typical loss from Ransomware incidents has grown from $686K to $3.7M
- Total estimated losses from Ransomware have grown 140X over the last 10 years



UNTIL FILES
2D06H48M38S
PUBLICATION

Deadline: 05 Nov, 2023 18:34:13 UTC

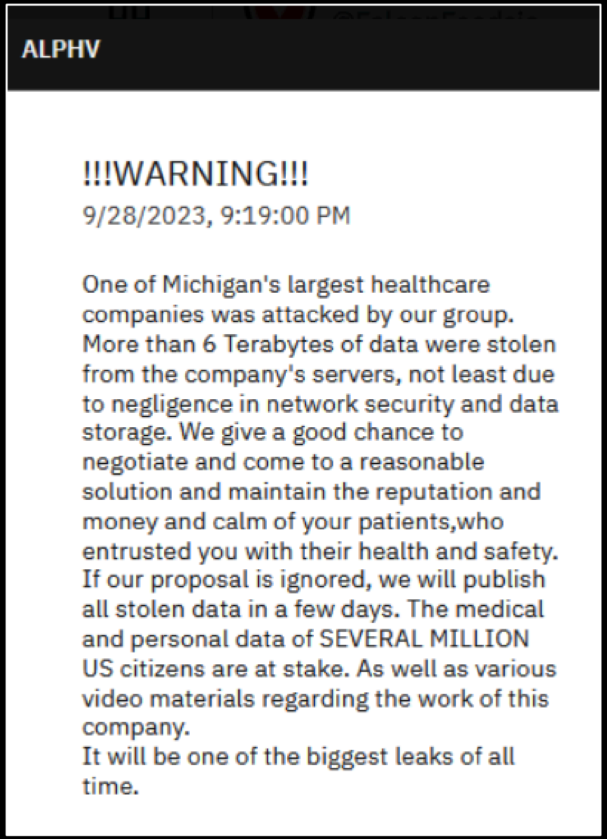
Cyentia Institute – 2024 CISA Ransomware Report

Cyber Attack
Case Studies

QUADRANT
INFORMATION SECURITY

Human Vulnerabilities - Scattered Spider & ALPHV

- Threat Actor group Scattered Spider has joined forces with the Ransomware group APLHV using BlackCat Ransomware
- Scattered Spider used ransomware from ALPHV (BlackCat), a ransomware-as-a-service operation, to carry out the MGM and Caesars breaches and many Healthcare attacks over the last year
- Scattered Spider is skilled in social engineering, using persuasive voice phone calls (vishing) to gain system access
- Scattered Spider uses employee information from sources such as LinkedIn and the Dark Web to call the target victim's IT help desk to reset their password and/or MFA account



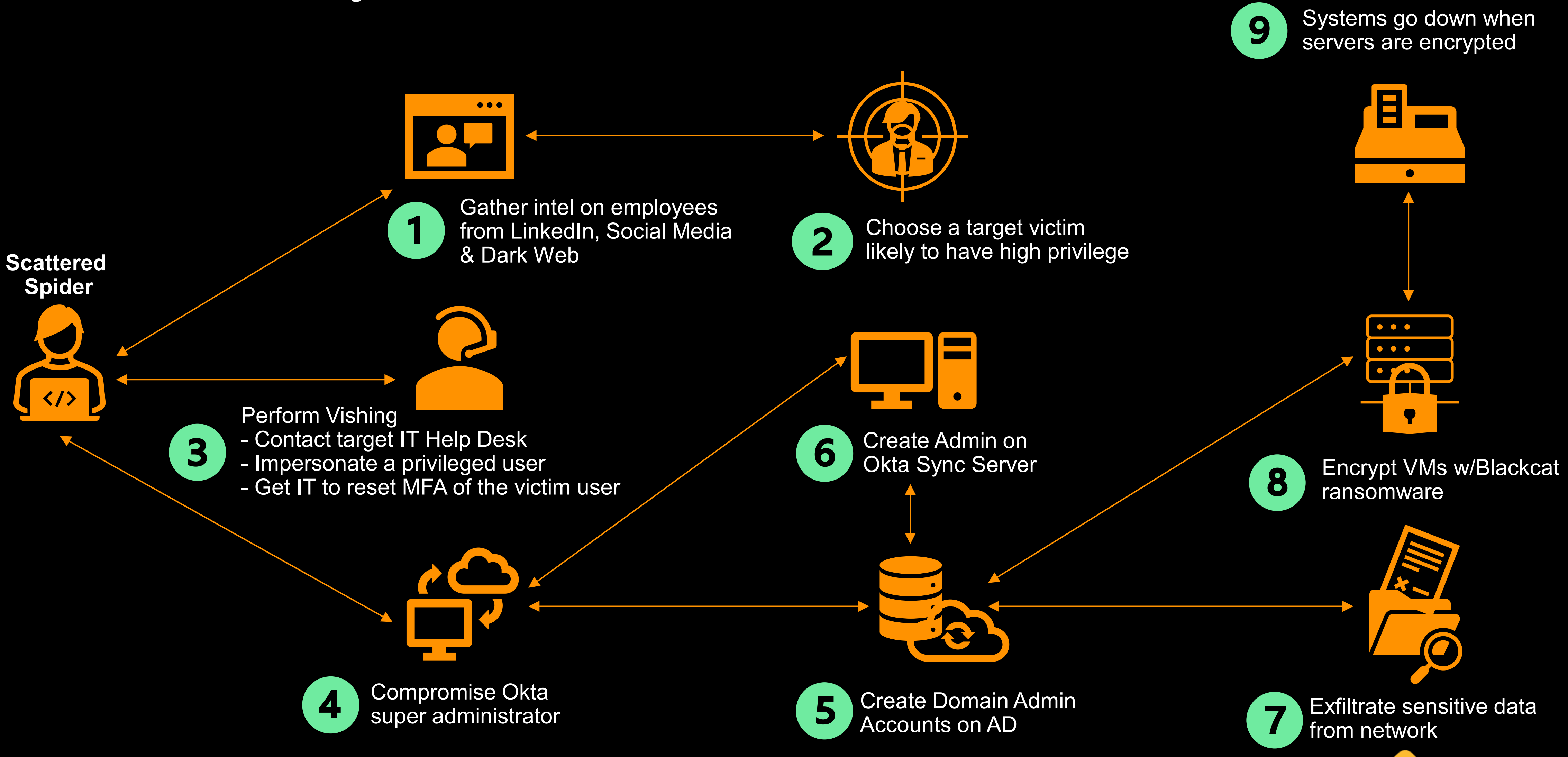
ALPHV

!!!WARNING!!!

9/28/2023, 9:19:00 PM

One of Michigan's largest healthcare companies was attacked by our group. More than 6 Terabytes of data were stolen from the company's servers, not least due to negligence in network security and data storage. We give a good chance to negotiate and come to a reasonable solution and maintain the reputation and money and calm of your patients,who entrusted you with their health and safety. If our proposal is ignored, we will publish all stolen data in a few days. The medical and personal data of SEVERAL MILLION US citizens are at stake. As well as various video materials regarding the work of this company.
It will be one of the biggest leaks of all time.

Scattered Spider Attack



Scattered Spider

1 Gather intel on employees from LinkedIn, Social Media & Dark Web

2 Choose a target victim likely to have high privilege

3 Perform Vishing
- Contact target IT Help Desk
- Impersonate a privileged user
- Get IT to reset MFA of the victim user

4 Compromise Okta super administrator

5 Create Domain Admin Accounts on AD

6 Create Admin on Okta Sync Server

7 Exfiltrate sensitive data from network

8 Encrypt VMs w/Blackcat ransomware

9 Systems go down when servers are encrypted

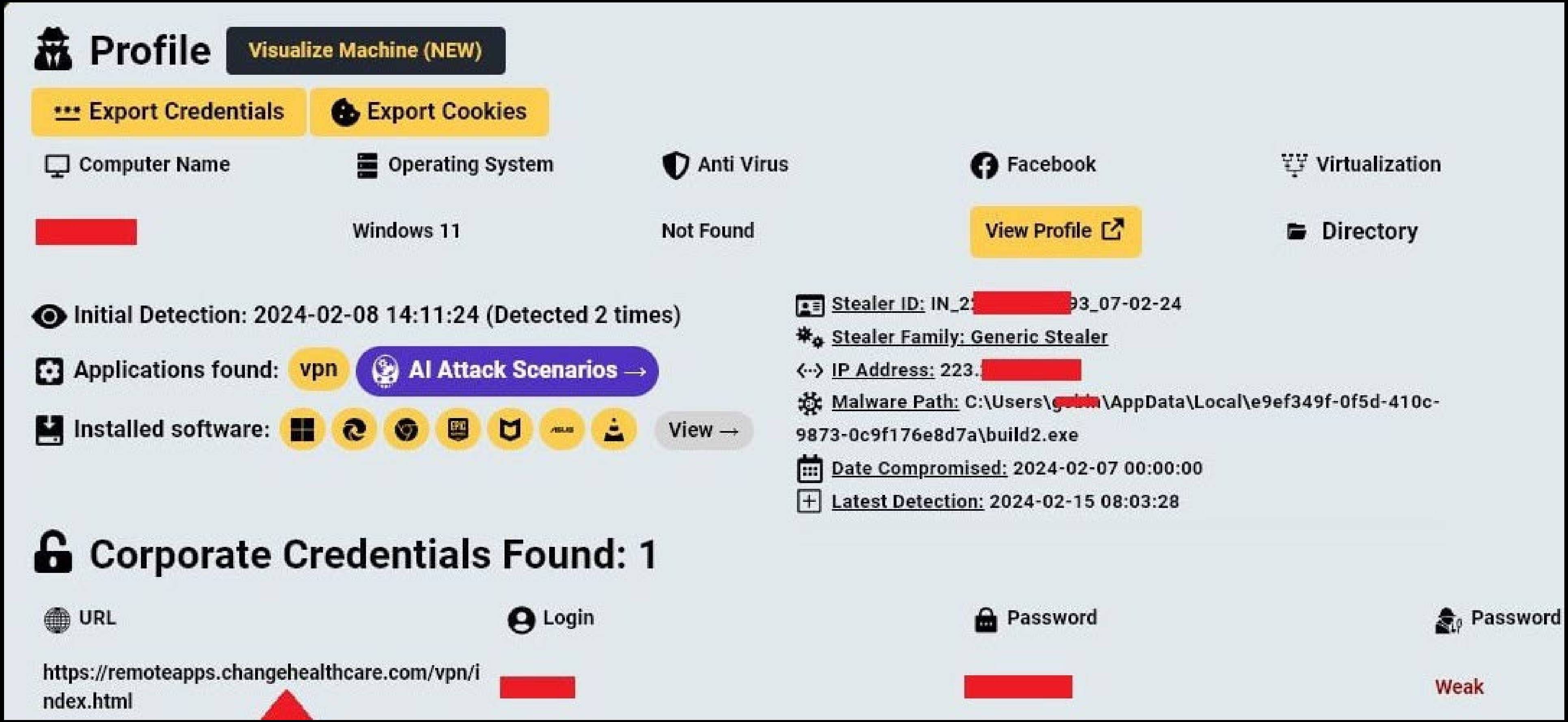
QUADRANT
INFORMATION SECURITY

Human Vulnerabilities – Stolen Credentials

- February 8th – Change Healthcare employee credential for Citrix remote access found on the Dark Web
- February 17th – ALPHV/BlackCat gained access to the Change Healthcare network through their Citrix Server
- February 21st - Change Healthcare reported "enterprise-wide connectivity" issues early in the morning.
- Later in the day, Optum said Change Healthcare was experiencing a network disruption due to a cybersecurity threat, and it immediately disconnected its systems
- On March 1st, Change Healthcare paid a 22-Million-dollar ransomware payment to ALPHV/BlackCat
- On April 8th Ransomhub demanded a second payment, or they will release 4TB of stolen data
- The total cost of the response is now predicted to be between $2.3 billion and $2.45 billion this year

QUADRANT
INFORMATION SECURITY

Human Vulnerabilities – Stolen Credentials



Profile

Computer Name	Operating System	Anti Virus	Facebook	Virtualization
[redacted]	Windows 11	Not Found	View Profile	Directory

Initial Detection: 2024-02-08 14:11:24 (Detected 2 times)

Applications found: vpn

Installed software:

Stealer ID: IN_2[redacted]93_07-02-24
Stealer Family: Generic Stealer
IP Address: 223.[redacted]
Malware Path: C:\Users\[redacted]\AppData\Local\e9ef349f-0f5d-410c-9873-0c9f176e8d7a\build2.exe
Date Compromised: 2024-02-07 00:00:00
Latest Detection: 2024-02-15 08:03:28

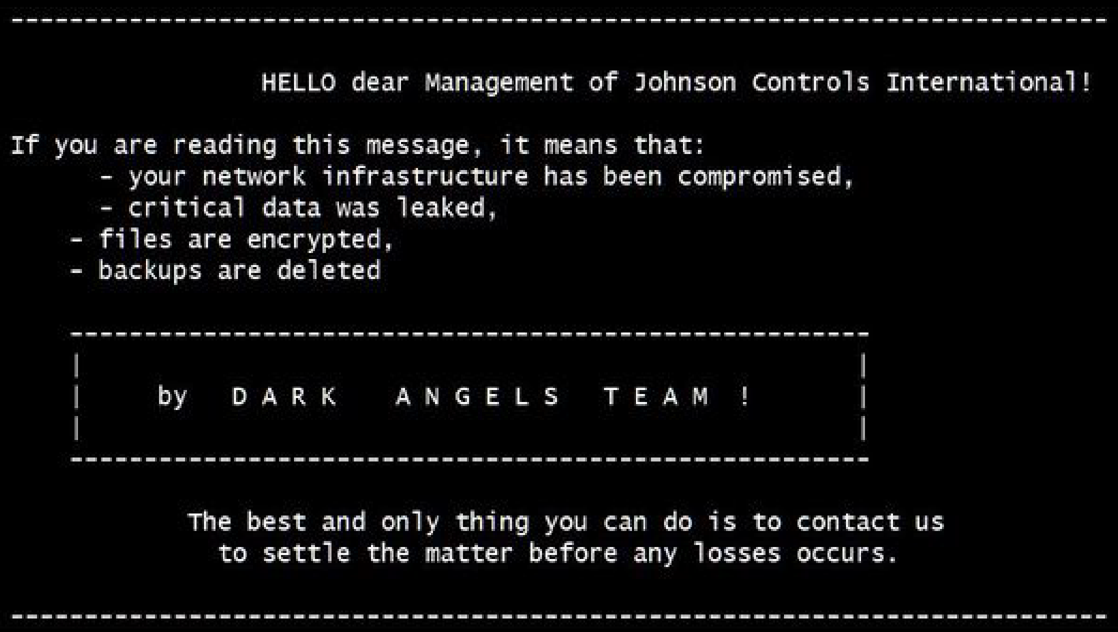
Corporate Credentials Found: 1

URL	Login	Password	Password
https://remoteapps.changehealthcare.com/vpn/index.html	[redacted]	[redacted]	Weak

Stolen Change Healthcare Citrix Credentials - Source: Hudson Rock

Known Vulnerabilities – Johnson Controls attack

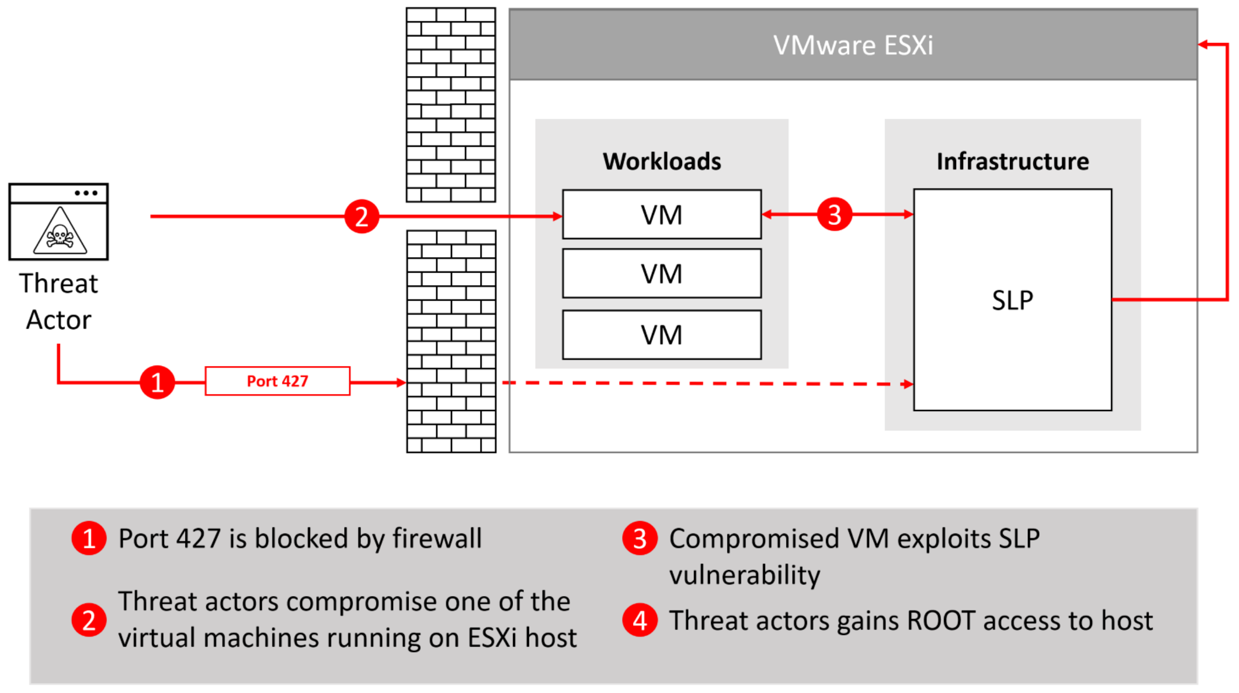
- Johnson Controls suffered a massive ransomware attack on September 22 – 25, 2023
- Johnson Controls is a multinational conglomerate that manufactures industrial control systems, security equipment, air conditioners, and fire safety equipment
- Dark Angels ransomware group posted this message and demanded $51 Million to provide the decryptor and delete stolen data
- Dark Angels claim to have stolen over 27 TB of corporate data and encrypted the company's VMWare ESXi virtual machines during the attack



```
-------------------------------------------------------------------------

                 HELLO dear Management of Johnson Controls International!

If you are reading this message, it means that:
      - your network infrastructure has been compromised,
      - critical data was leaked,
    - files are encrypted,
    - backups are deleted

    -----------------------------------------------------
    |                                                   |
    |     by   D A R K    A N G E L S    T E A M  !     |
    |                                                   |
    -----------------------------------------------------

               The best and only thing you can do is to contact us
                 to settle the matter before any losses occurs.

-------------------------------------------------------------------------
```

Known Vulnerabilities – Johnson Controls attack

- There are two primary ways attackers can target ESXi servers
  - Exploit CVE-2021-29174
  - Obtain AD Domain account to create ESXi root account
- VMware disclosed the ESXi vulnerability in February 2021 and simultaneously issued a patch for it
- Since then, attackers have targeted it heavily, making CVE-2021-29174 one of the most exploited vulnerabilities in 2021 and 2022



1 Port 427 is blocked by firewall

2 Threat actors compromise one of the virtual machines running on ESXi host

3 Compromised VM exploits SLP vulnerability

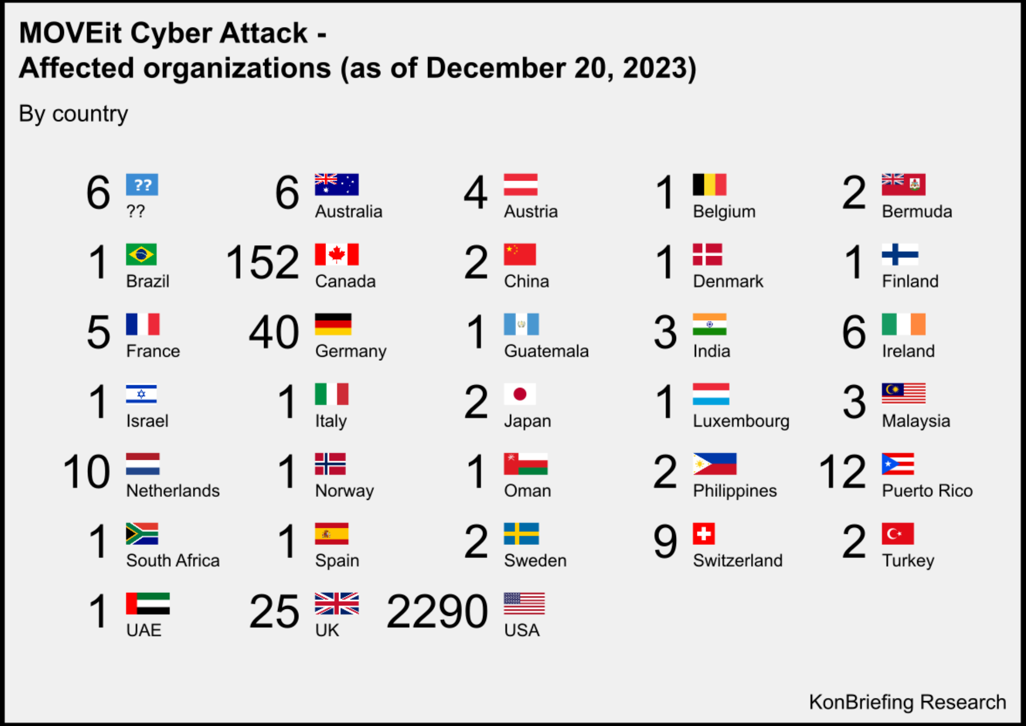
4 Threat actors gains ROOT access to host

Zero-day Vulnerabilities – MOVEit breach

- Progress Software published an advisory on Wednesday, May 31, 2023, warning of a critical SQL injection vulnerability in their MOVEit Transfer solution
- The original MOVEit Transfer zero-day vulnerability was assigned CVE-2023-34362 on June 2, 2023
- Additional MOVEit Transfer CVEs were disclosed and patched on June 9, 15, and July 6, 2023
- The Cl0p ransomware gang claimed credit for the breach of the MOVEit file transfer program
- The vulnerability allowed attackers to download the data on the file transfer servers

MOVEit overview

So far, 2,611 organizations have fallen victim to the MOVEit attack, affecting approximately 89 million individuals.

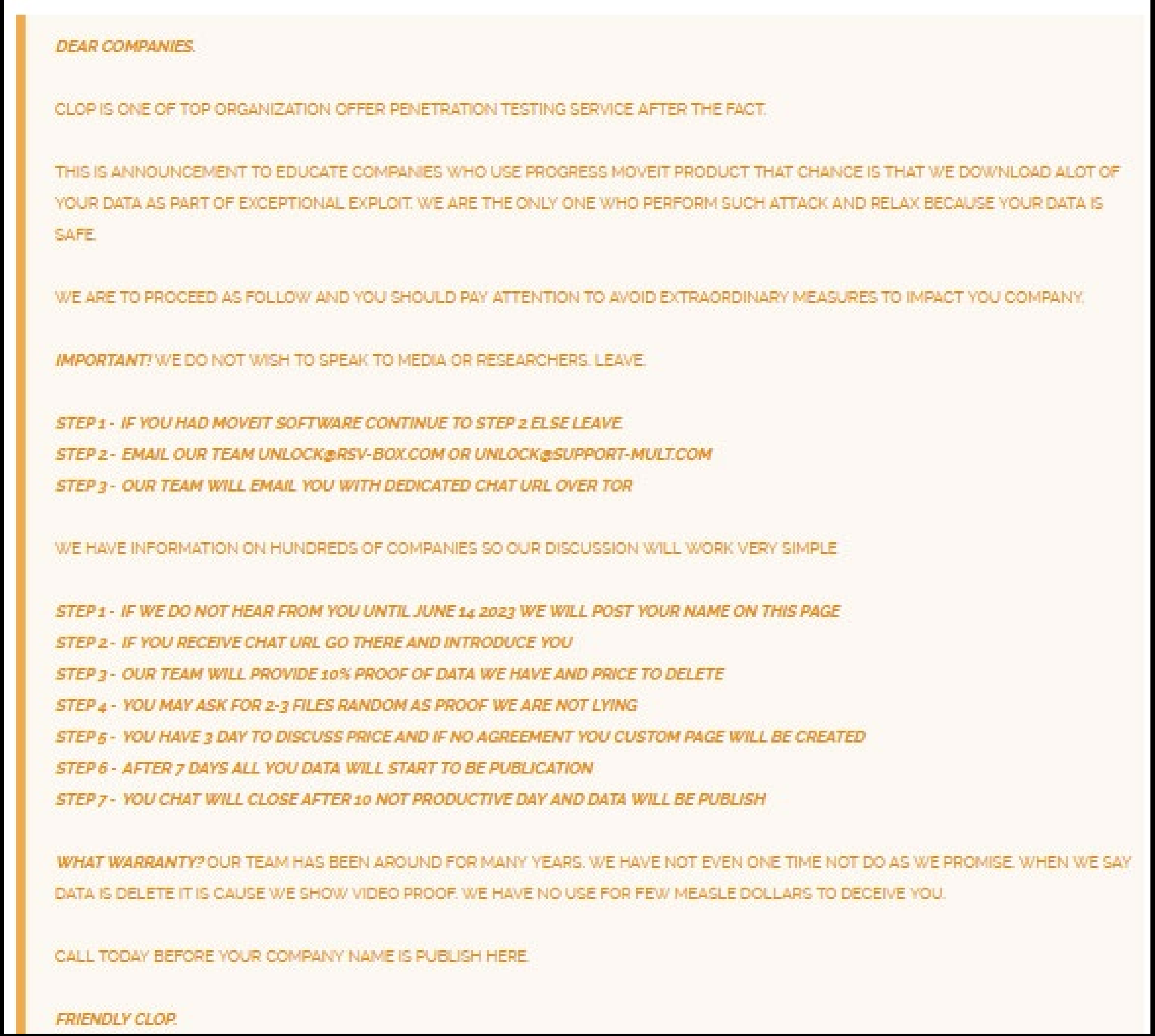


MOVEit Cyber Attack -
Affected organizations (as of December 20, 2023)

By country

6 ??	6 Australia	4 Austria	1 Belgium	2 Bermuda
1 Brazil	152 Canada	2 China	1 Denmark	1 Finland
5 France	40 Germany	1 Guatemala	3 India	6 Ireland
1 Israel	1 Italy	2 Japan	1 Luxembourg	3 Malaysia
10 Netherlands	1 Norway	1 Oman	2 Philippines	12 Puerto Rico
1 South Africa	1 Spain	2 Sweden	9 Switzerland	2 Turkey
1 UAE	25 UK	2290 USA		

KonBriefing Research



DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

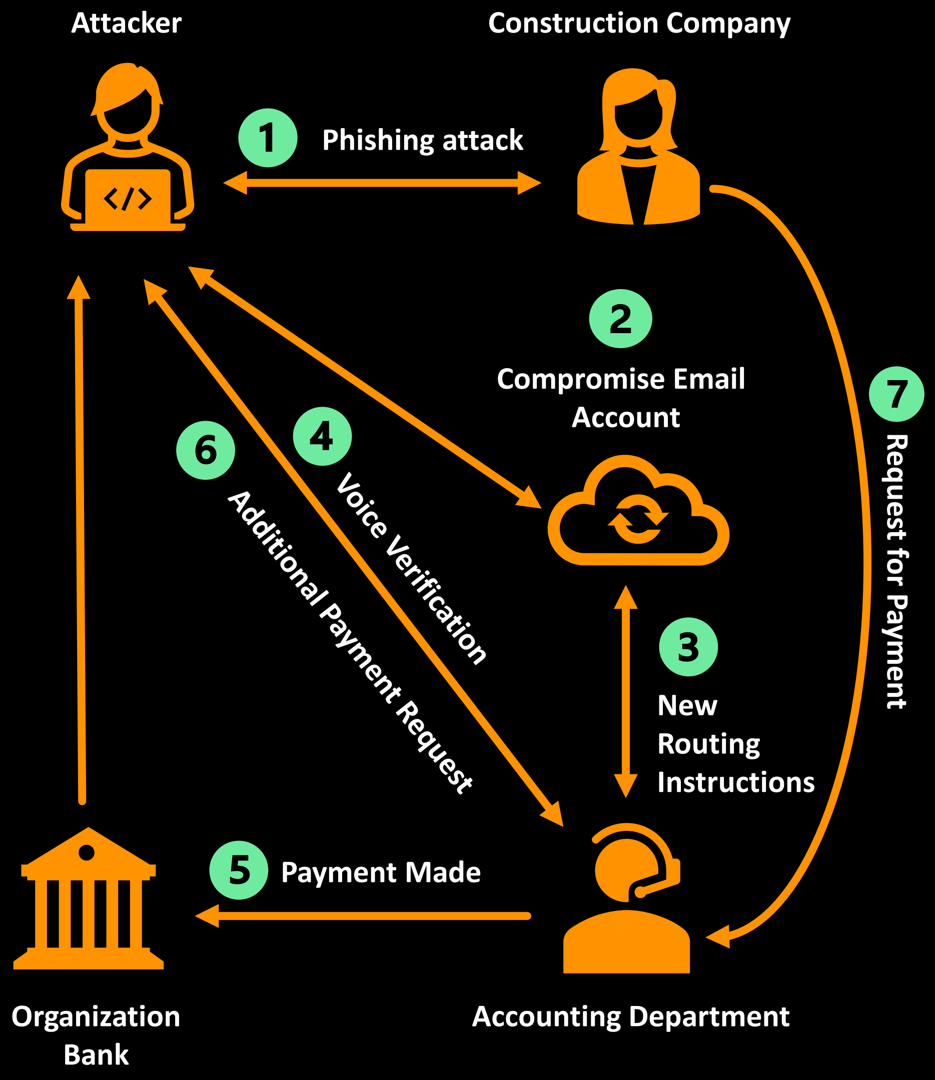
WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

FRIENDLY CLOP.

Business Email Compromise

- Business Email Compromise has now reached an all-time high and has become much more sophisticated.
- It was observed in 2023 that there was a 167% increase in advanced email attacks, including business email compromise (BEC), phishing, malware, and extortion
- Attackers are making voice calls to provide new bank routing instructions, and they are set up to accept voice verification calls from their targets



Conclusions

- Attacks will continue to increase in number, size, and complexity as the payouts continue to increase
  - Cybercrime is predicted to cost the world $9.5 trillion in 2024 (Cybersecurity Ventures)
- Attackers will focus more on human weakness with social engineering attacks such as phone calls, texting, and QR codes
  - Criminal organizations are motivated by the large payouts
- Zero Day attacks will continue to increase as criminal organizations invest in software testing and vulnerability research
  - Cl0p made hundreds of millions off the MoveIT breach

QUADRANT INFORMATION SECURITY

Compliance Standards

Zero Trust

More People

What is the solution?

More Budget

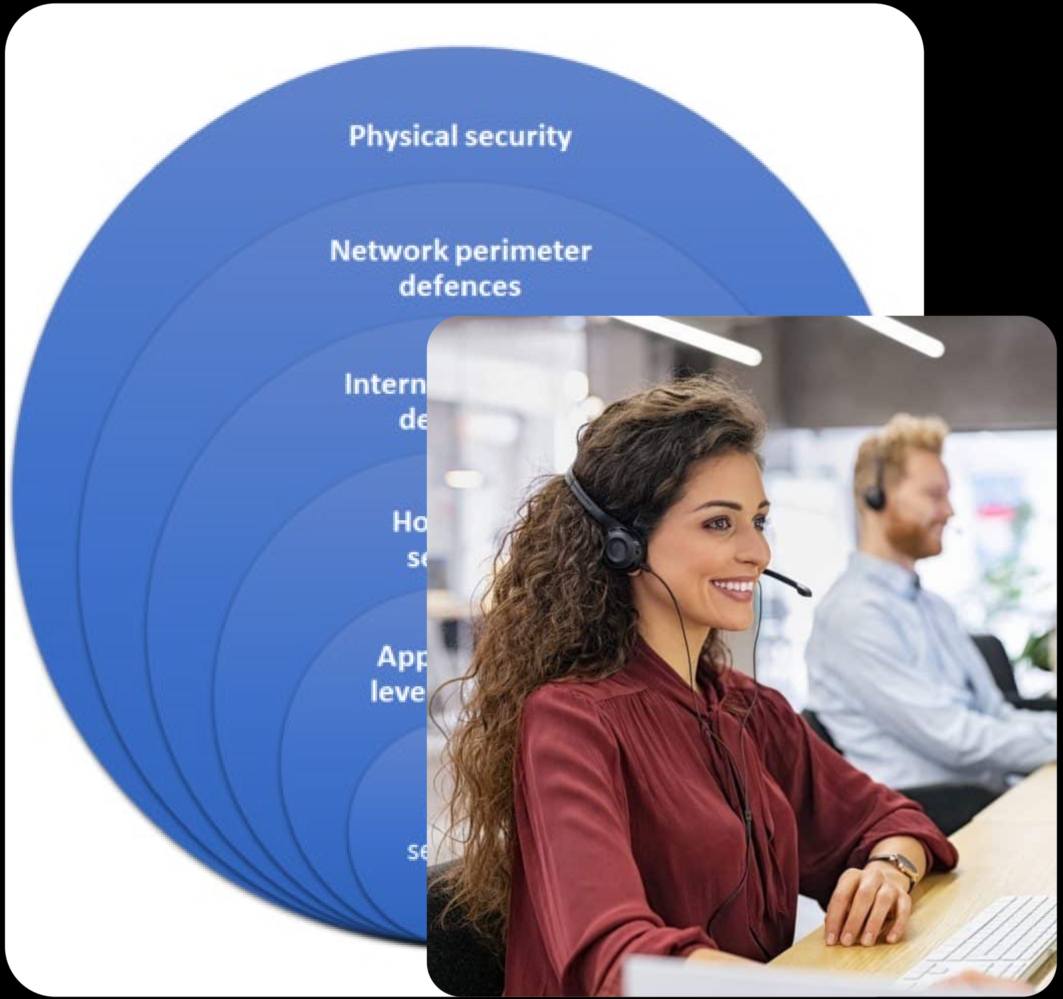
Defense-in-Depth

AI

Cyber Resilience

Defense-in-Depth?

- **Defense-in-Depth**: The application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another.



A New Defense-in-Depth Approach

Information security strategy integrating **people**, **technology**, and **operations** capabilities to establish multiple layers that Identify, Protect, Detect, Respond, and Recover from cyberattacks.

Human

Culture | Policy | Training | Testing

Technology

Identity | Network | End-Point | Application | Data

Operations

Intelligence | Patching | Monitoring | Response | Recovery

QUADRANT
INFORMATION SECURITY

Human

Culture | Policies | Training | Testing

- **As organizations have improved their security postures, attackers have shifted focus to employees**
- **Culture**: Develop and maintain a culture of cybersecurity and awareness of threats supported by senior management.
- **Policies**: Implement policies to guide staff in safe cyber behaviors and operations based on job roles.
- **Training**: Provide ongoing staff training on threats to the business, safe user behaviors, and personal cybersecurity.
- **Testing**: Regular tests are performed to measure the effectiveness of training. Retrain and/or reassign users based on testing results.

QUADRANT
INFORMATION SECURITY

Technology

Identity | Network | End-Point | Application | Data

- **Technology solutions should have the ability to prevent, stop, and detect cyber attacks.**
- **Identity**: Implement advanced Identity and Access Management solutions to protect the network, endpoints, applications, and data.
- **Network**: Implement network and cloud protection to prevent, stop, and detect malicious activity. Also, monitor for configuration changes.
- **End-Point**: Implement End-Point protection to prevent, stop, and detect malicious activity. Also, monitor for configuration changes.
- **Application**: Implement application protection to prevent, stop, and detect malicious activity. Also, implement secure-by-design application development.
- **Data**: Implement solutions to identify, prevent, encrypt, and monitor data. Perform air-gapped backups of data.

QUADRANT
INFORMATION SECURITY

Operations

Intelligence | Patch | Monitor | Response | Recovery

- **A robust security operations program is essential for preventing, detecting, and responding to cyber attacks.**
- **Intelligence**: Implement a Threat Intelligence function to monitor for cyber threats and vulnerabilities to the business, employees, and customers.
- **Patching**: Implement a prioritized vulnerability management and patching program based on threat intelligence and Zero-day announcements.
- **Monitoring**: Monitor IT systems, applications, cybersecurity technology solutions, and human user behavior for malicious activity.
- **Response**: Develop and test procedures for responding to all major types of attacks, including containing the attack, extortion decisions, and legal requirements.
- **Recovery**: Develop and test procedures for backing up and restoring all data to recover from a data breach or ransomware attack.

QUADRANT
INFORMATION SECURITY

Questions

Jeff Foresman
Email: jforesman@quadrantsec.com
www.quadrantsec.com

"The best way to predict the future is to create it."

- Abraham Lincoln