CYBER DEEP DIVE

COVID-19 and Other Threats to the Healthcare Sector

April 2020

Private and Confidential

POLSINELLI

Kroll | A Division of DUFF & PHELPS

DISCLAIMER

Any positions presented in this session are those of the panelists and do not represent the official position of Duff & Phelps, LLC. This material is offered for educational purposes with the understanding that neither the authors nor Duff & Phelps, LLC or its affiliates are engaged in rendering legal, accounting or any other professional service through presentation of this material.

Polsinelli PC provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.

Speakers

ANDREAS CHRYSOSTOMOU

Managing Director,
Valuation Advisory,
Duff & Phelps

KEITH WOJCIESZEK

Managing Director, Cyber Risk, Kroll

LAURIE IACONO

VP,
Cyber Risk, Kroll

NICOLE SETTE

Senior VP,
Cyber Risk, Kroll

BRUCE A. RADKE

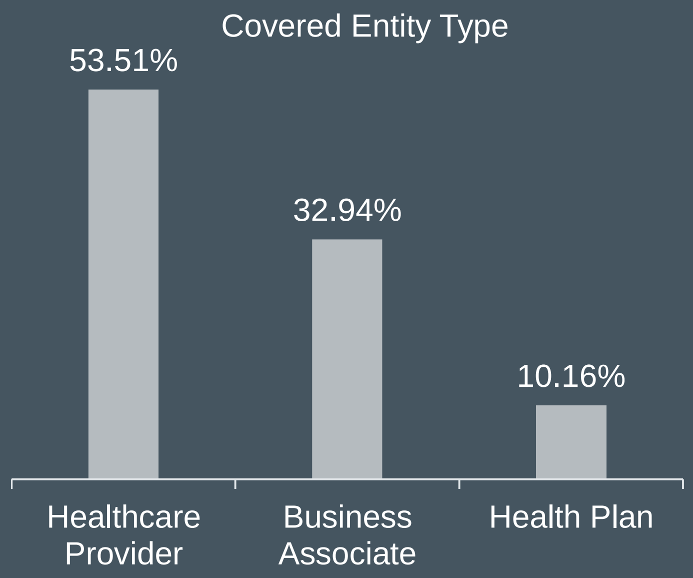
Shareholder, Co-Chair,
Privacy and
Cybersecurity practice,
Polsinelli

$65B+

GLOBAL HEALTHCARE CYBER SECURITY SPENDING 2017-2021*

46.8M

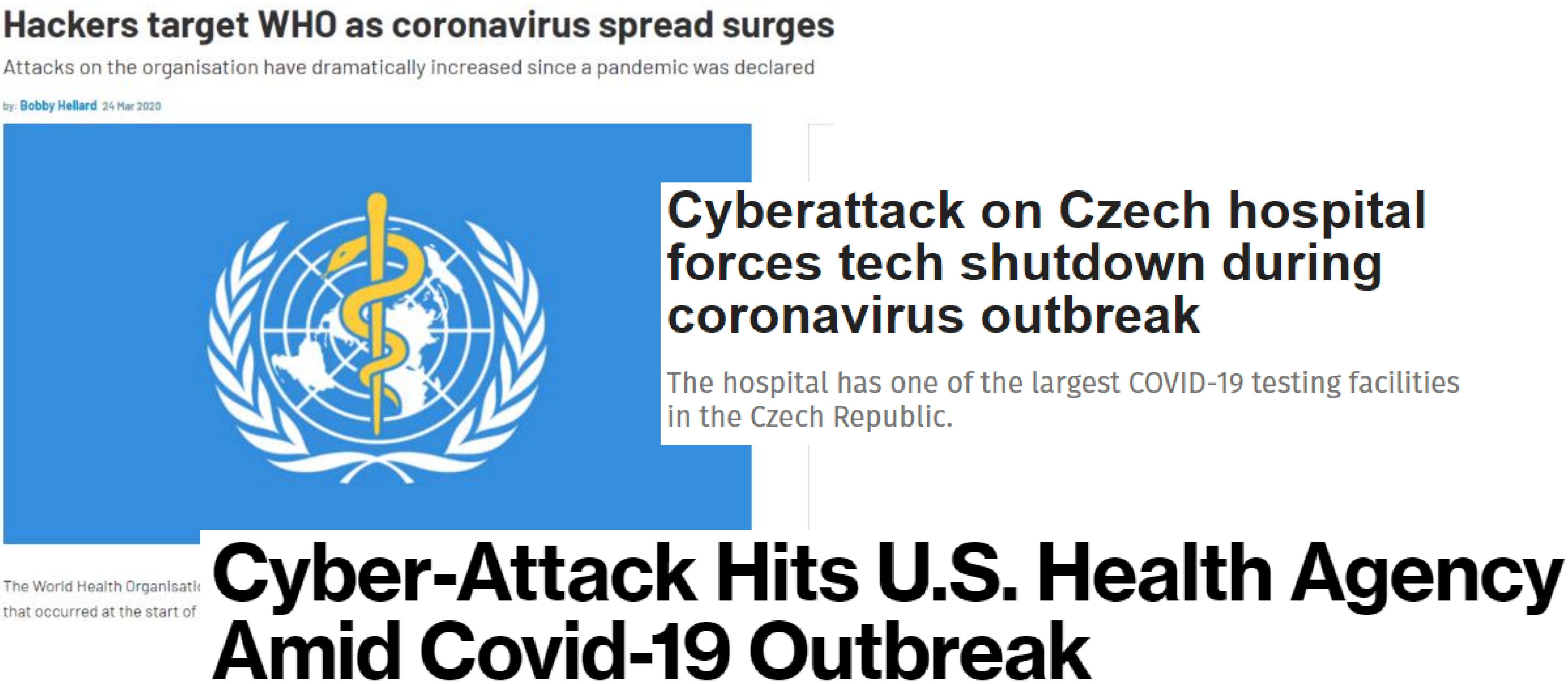
AMERICANS AFFECTED*



* Cybersecurity Ventures' Healthcare Cybersecurity Report

* As of March 2020, according to HHS OCR Portal

Covid-19 and the Healthcare Sector



Hackers target WHO as coronavirus spread surges

Attacks on the organisation have dramatically increased since a pandemic was declared

by: Bobby Hellard 24 Mar 2020

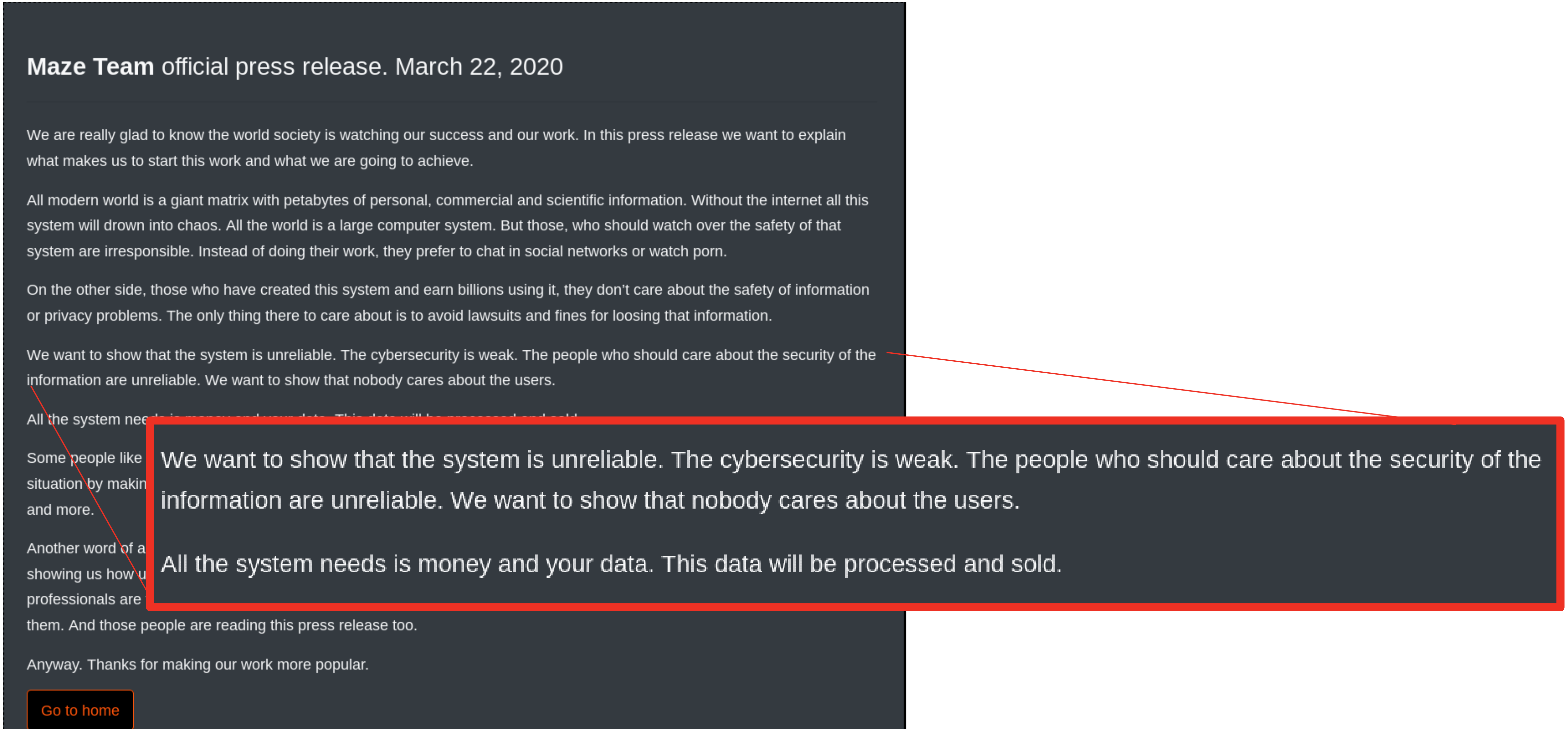
The World Health Organisati
that occurred at the start of

Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak

The hospital has one of the largest COVID-19 testing facilities in the Czech Republic.

Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak

Ransomware Group Makes Promise



Maze Team official press release. March 22, 2020

We are really glad to know the world society is watching our success and our work. In this press release we want to explain what makes us to start this work and what we are going to achieve.

All modern world is a giant matrix with petabytes of personal, commercial and scientific information. Without the internet all this system will drown into chaos. All the world is a large computer system. But those, who should watch over the safety of that system are irresponsible. Instead of doing their work, they prefer to chat in social networks or watch porn.

On the other side, those who have created this system and earn billions using it, they don't care about the safety of information or privacy problems. The only thing there to care about is to avoid lawsuits and fines for loosing that information.

We want to show that the system is unreliable. The cybersecurity is weak. The people who should care about the security of the information are unreliable. We want to show that nobody cares about the users.

All the system nee

Some people like
situation by makin
and more.

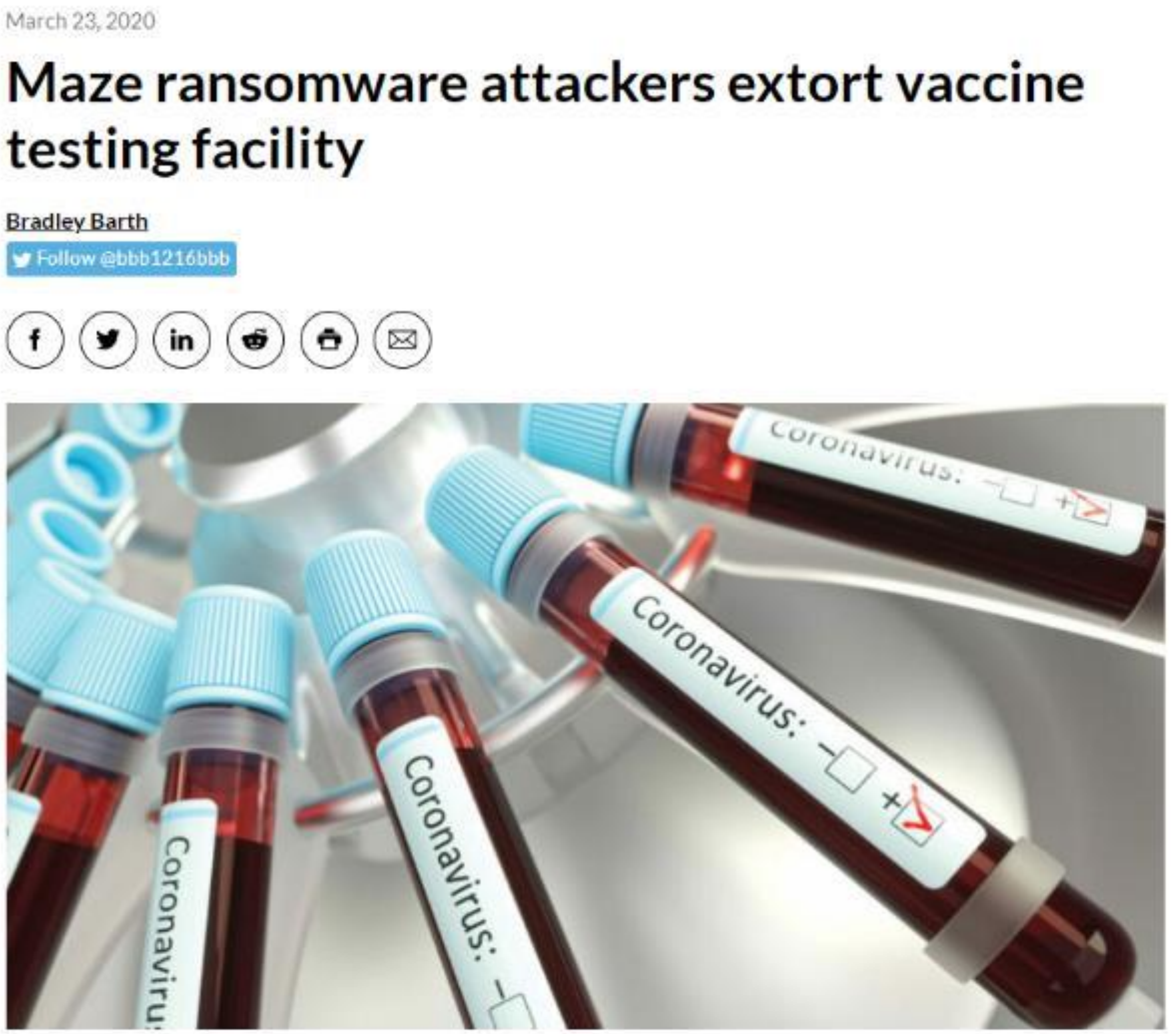
Another word of a
showing us how u
professionals are
them. And those people are reading this press release too.

Anyway. Thanks for making our work more popular.

We want to show that the system is unreliable. The cybersecurity is weak. The people who should care about the security of the information are unreliable. We want to show that nobody cares about the users.

All the system needs is money and your data. This data will be processed and sold.

One Day Later…



March 23, 2020

Maze ransomware attackers extort vaccine testing facility

Bradley Barth

Follow @bbb1216bbb

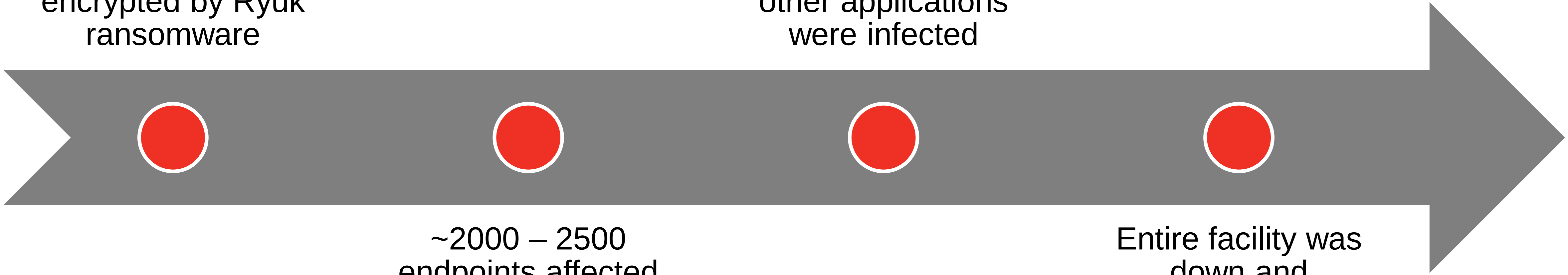
COVID-19 as a Threat Delivery Vector

Malware	Delivery method
Ryuk/Trickbot	Fake statement about a new case of COVID-19
Remcos	.exe posing as a PDF containing COVID-19 safety measures
AZORult	COVID-19 email campaign involved information stealing malware
Parallax RAT	Distributed using COVID-19 themed documents
Lokibot	Distributed via an email purportedly sent from the Chinese Minister of Health
CoronaVirus Ransomware and Kpot Infostealer	Fake version of the WiseCleaner website delivered ransomware and infostealer when a link was used to download purported utilities for Windows

⚠

Attackers are aggressively relying on COVID-19 news for phishing campaigns. Educate staff to triple-check sources

Grim Reality:



In the midst of the Covid-19 crisis, a medical center was encrypted by Ryuk ransomware

~2000 – 2500 endpoints affected

All desktops, Virtual Machine farms and other applications were infected

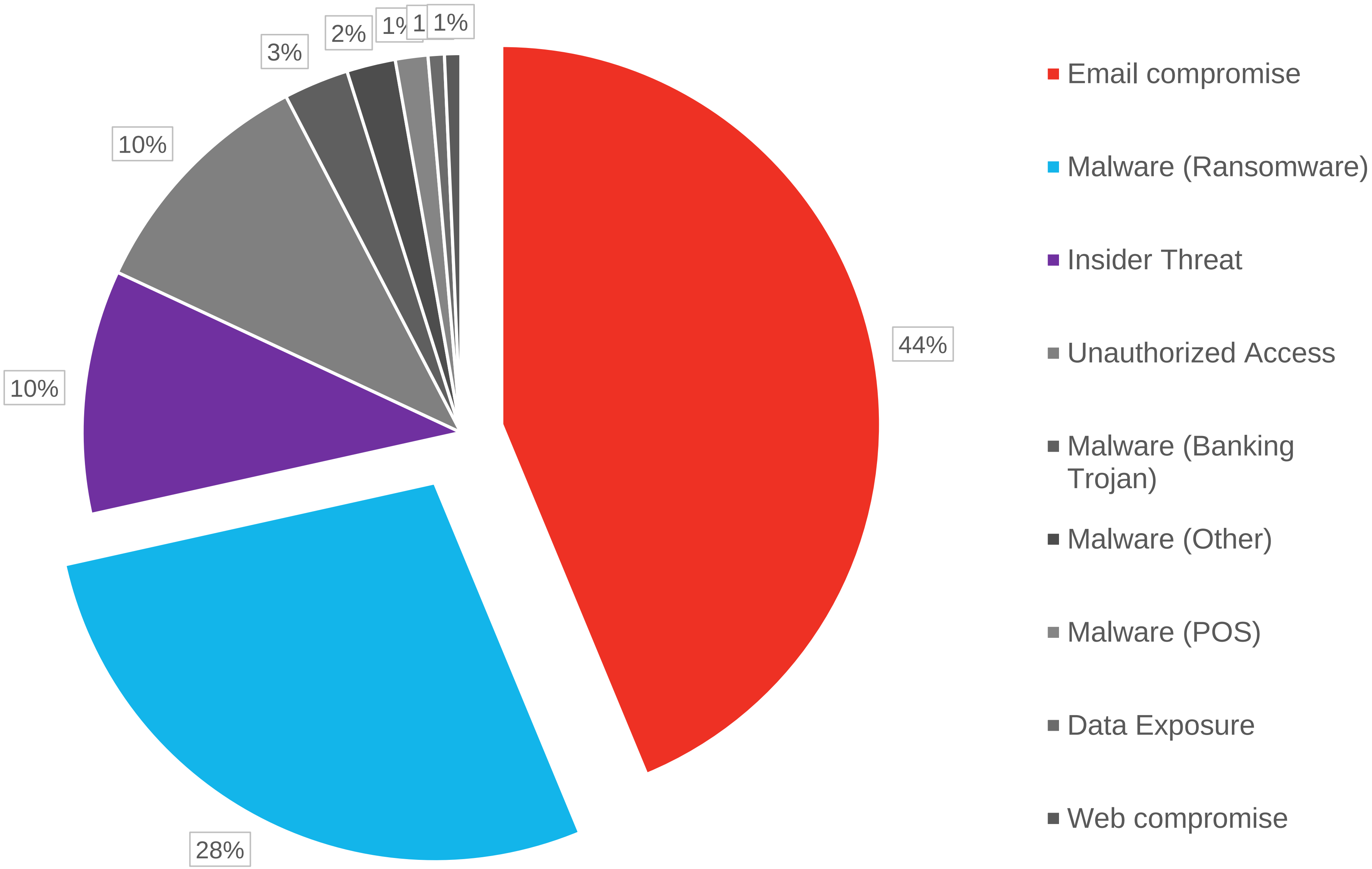
Entire facility was down and disconnected from the internet including email and electronic health records

THE HEALTHCARE CYBER THREAT LANDSCAPE

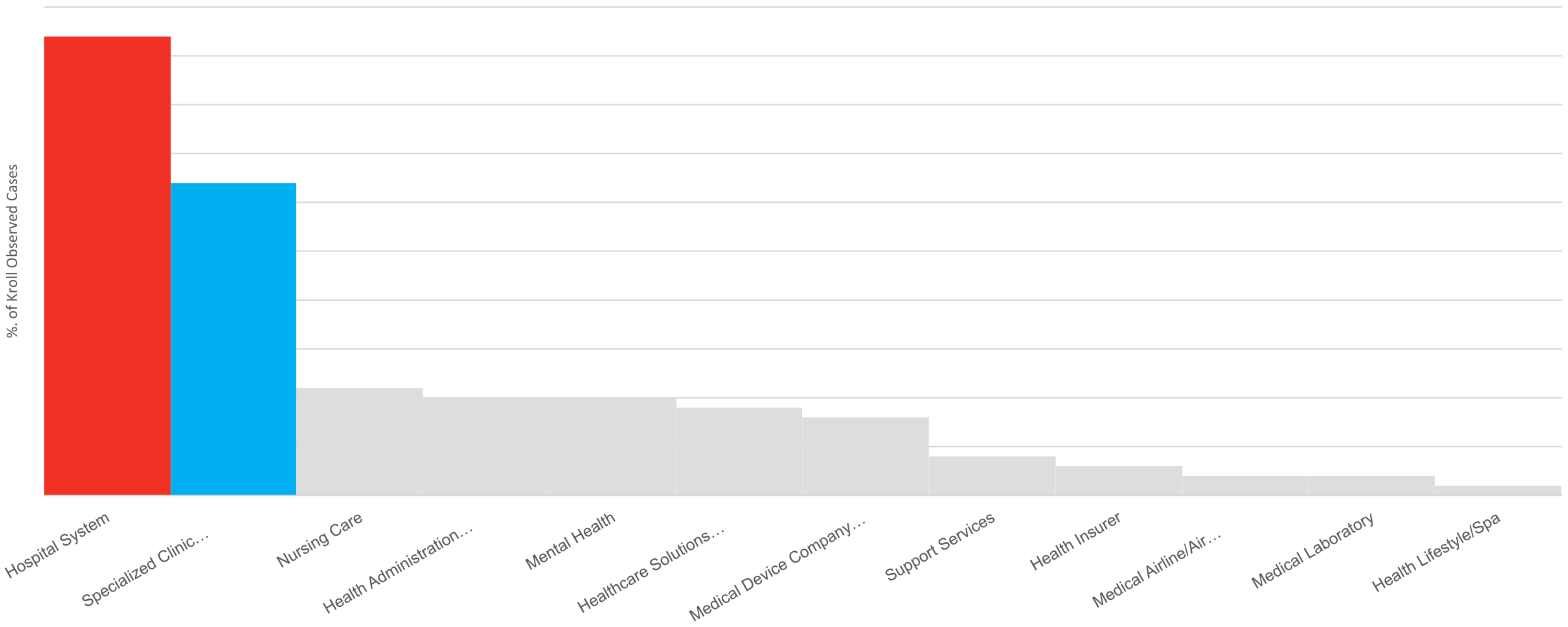
Based on Kroll intake data

- Healthcare was the single most targeted industry in 2019 and Q1 2020
- Hospital Systems are the most frequently targeted discipline within the healthcare industry
- Email Compromise is the most observed threat, followed by Ransomware attacks
- Ransomware eclipses Email Compromise as the most observed threat only for Specialized Clinics and Support Services
- Medical Laboratories and Medical Device Companies are largely spared from ransomware – likely due to the attack context (primarily for IP and sensitive data theft and/or monetary gain via false invoicing and payment requests)

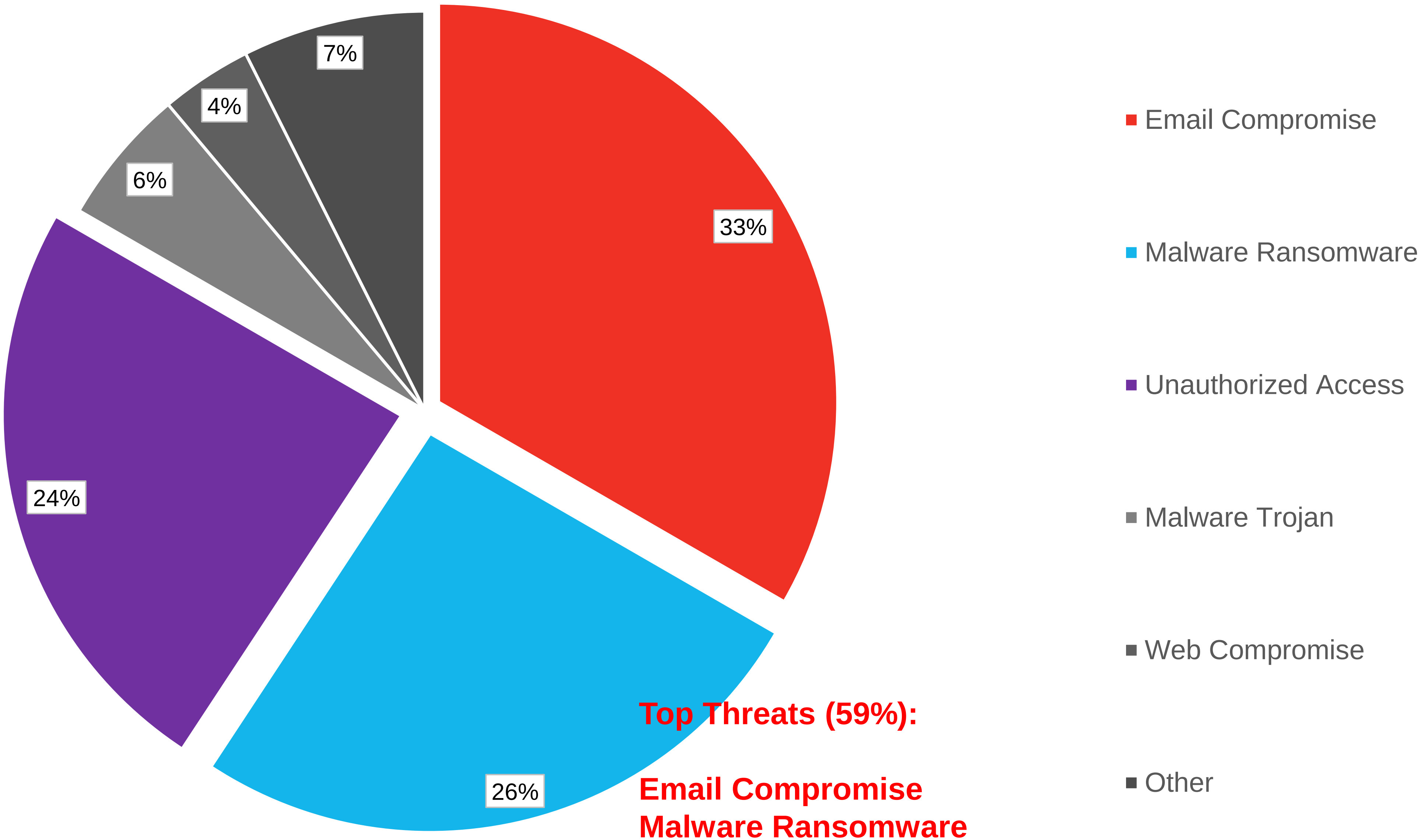
2019: Healthcare – Threat Incident Types



Targeted Disciplines within Healthcare



Q1 2020 Threat Incident Types



Top Threats (59%):

Email Compromise
Malware Ransomware

2020

Legal and Regulatory Landscape

REGULATORY LANDSCAPE

BREACHES AS OPPORTUNITY TO AUDIT PRIVACY PRACTICES

- Massachusetts – WISP
- Indiana – Questions re. security pre- and post-incident and employee training

FTC/STATE AG OFTEN RELY ON CONSUMER FRAUD STATUTES

- It is thus important to be cautious with public facing statements about the organization’s data security

BREACH INVESTIGATIONS

OCR ALMOST AUTOMATICALLY INVESTIGATES 500+ PEOPLE BREACHES

- Underlying cause of the breach
- Actions taken to respond to the breach (including compliance with breach notification requirements) and prevent future incidents
- Entity’s compliance prior to breach

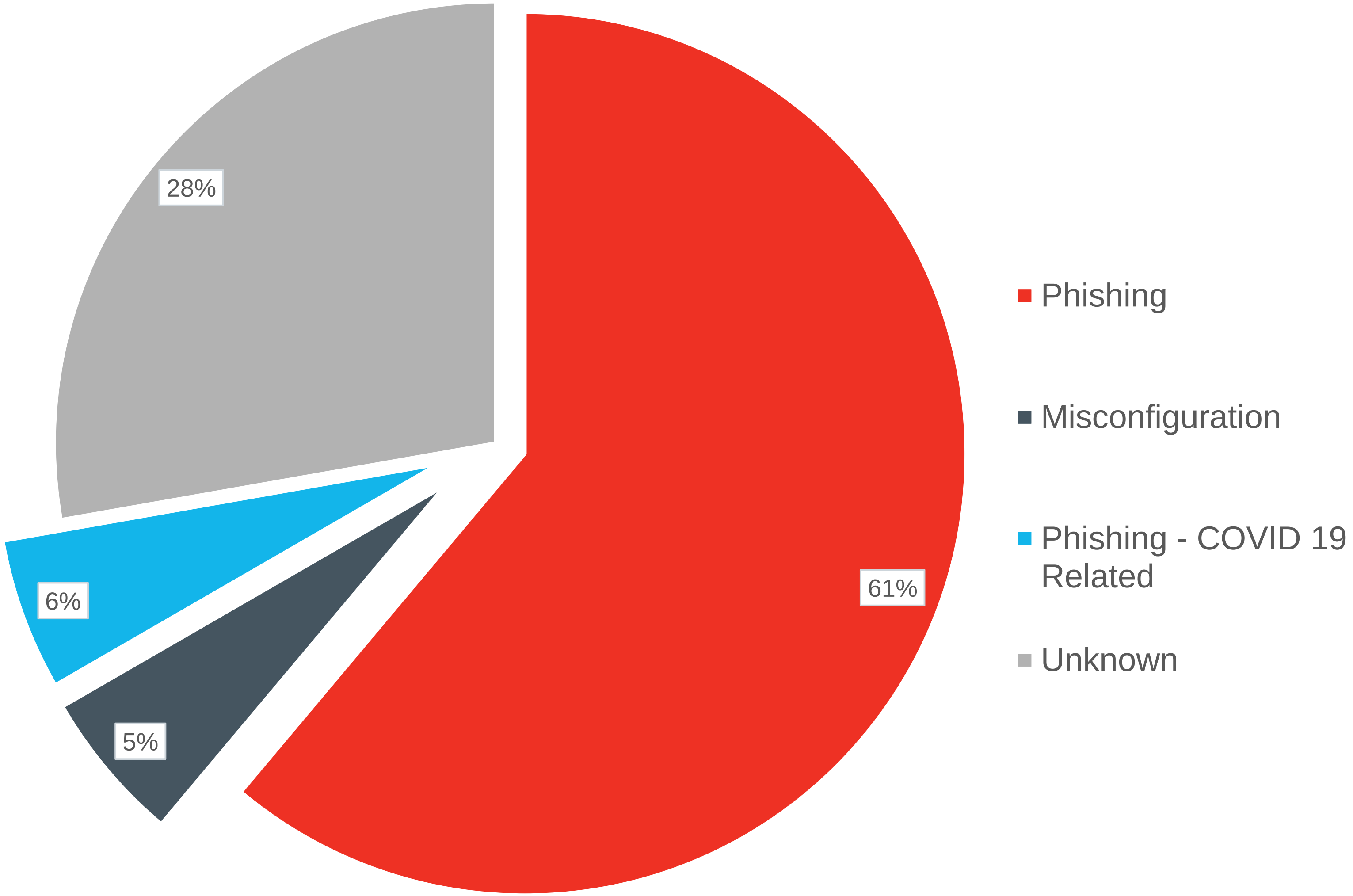
Recurring OCR Compliance Issues

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal
- Insufficient Data Backup and Contingency Planning

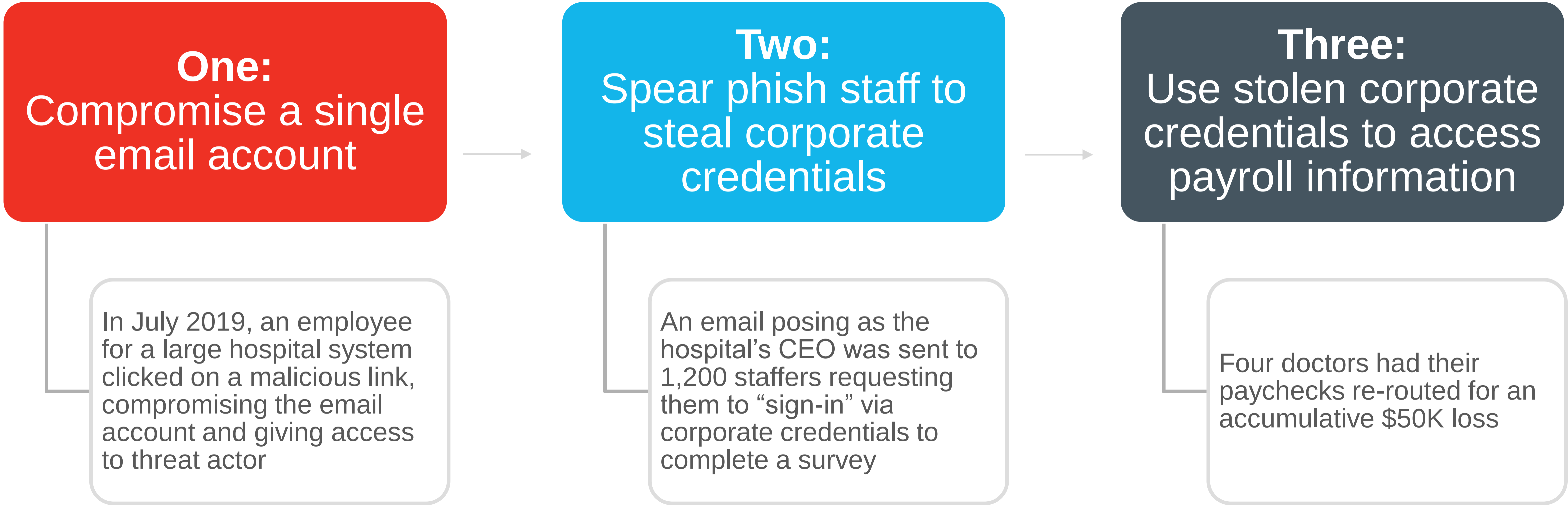
Private Enforcement of the **CCPA**

- Unlike the GDPR, the CCPA gives plaintiffs a "**private right of action**" and allows recovery of statutory damages for data breaches, even where no harm is shown.
- Statutory damages are **"$100 to $750 per consumer per incident.**"
    - Easier to establish concrete injury and standing
    - Federal Law
    - State Law
    - Easier to support Class Certification

Q1 2020 Email Compromise by Suspected Infection Vector



Case Study: The Phishing Journey



One:
Compromise a single email account

In July 2019, an employee for a large hospital system clicked on a malicious link, compromising the email account and giving access to threat actor

Two:
Spear phish staff to steal corporate credentials

An email posing as the hospital's CEO was sent to 1,200 staffers requesting them to "sign-in" via corporate credentials to complete a survey

Three:
Use stolen corporate credentials to access payroll information

Four doctors had their paychecks re-routed for an accumulative $50K loss

LEGAL IMPLICATIONS

Email compromises

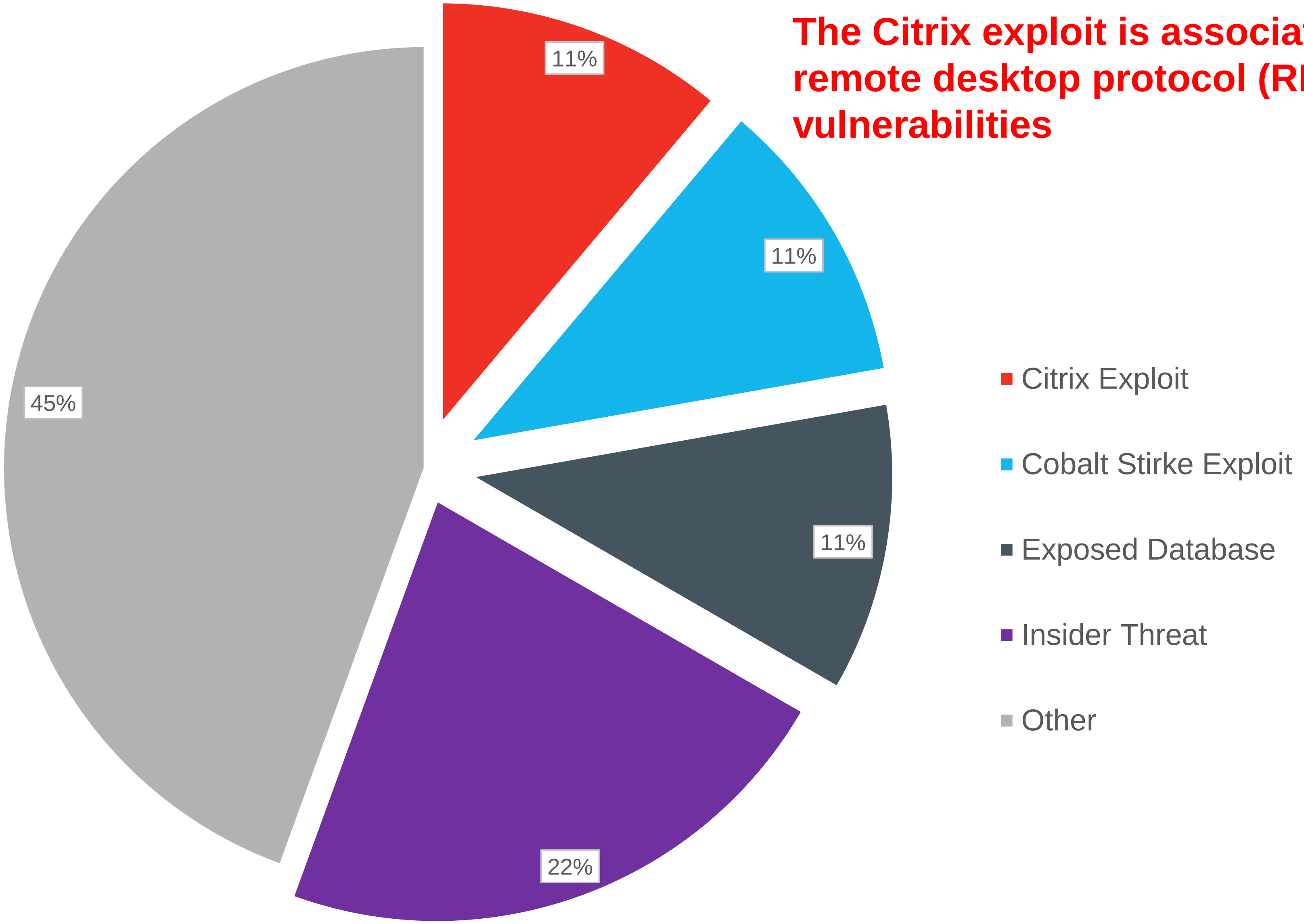
UNAUTHORIZED ACCESS OF INFORMATION

- Statutory data breach notification obligations to individuals, regulators and business partners
  - This may include notification to investors, key customers, unfriendly parties (e.g., litigation adversaries)
- Contractual obligations to third parties

WIRE FRAUD

- Recent lawsuits in which companies are sued due to wire and other fraud perpetrated from compromised account
- If someone suffers a monetary loss because your account was compromised, you may be sued

Q1 2020 Unauthorized Access – Healthcare



The Citrix exploit is associated with remote desktop protocol (RDP) vulnerabilities

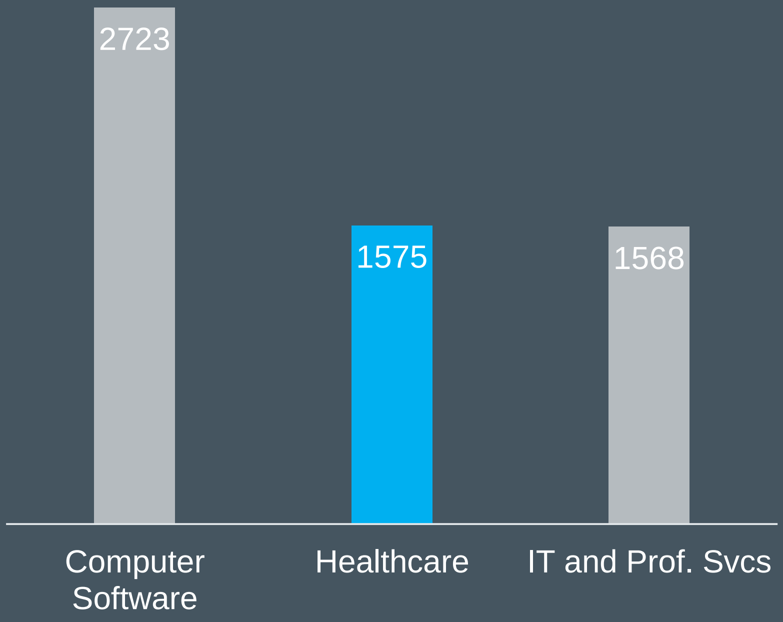
Case Study: Citrix Exploit CVE-2019-19781

Jan 2020: healthcare company notified by Citrix about the vulnerability

Engineers slated to deploy patch discover potential compromise, contact Kroll

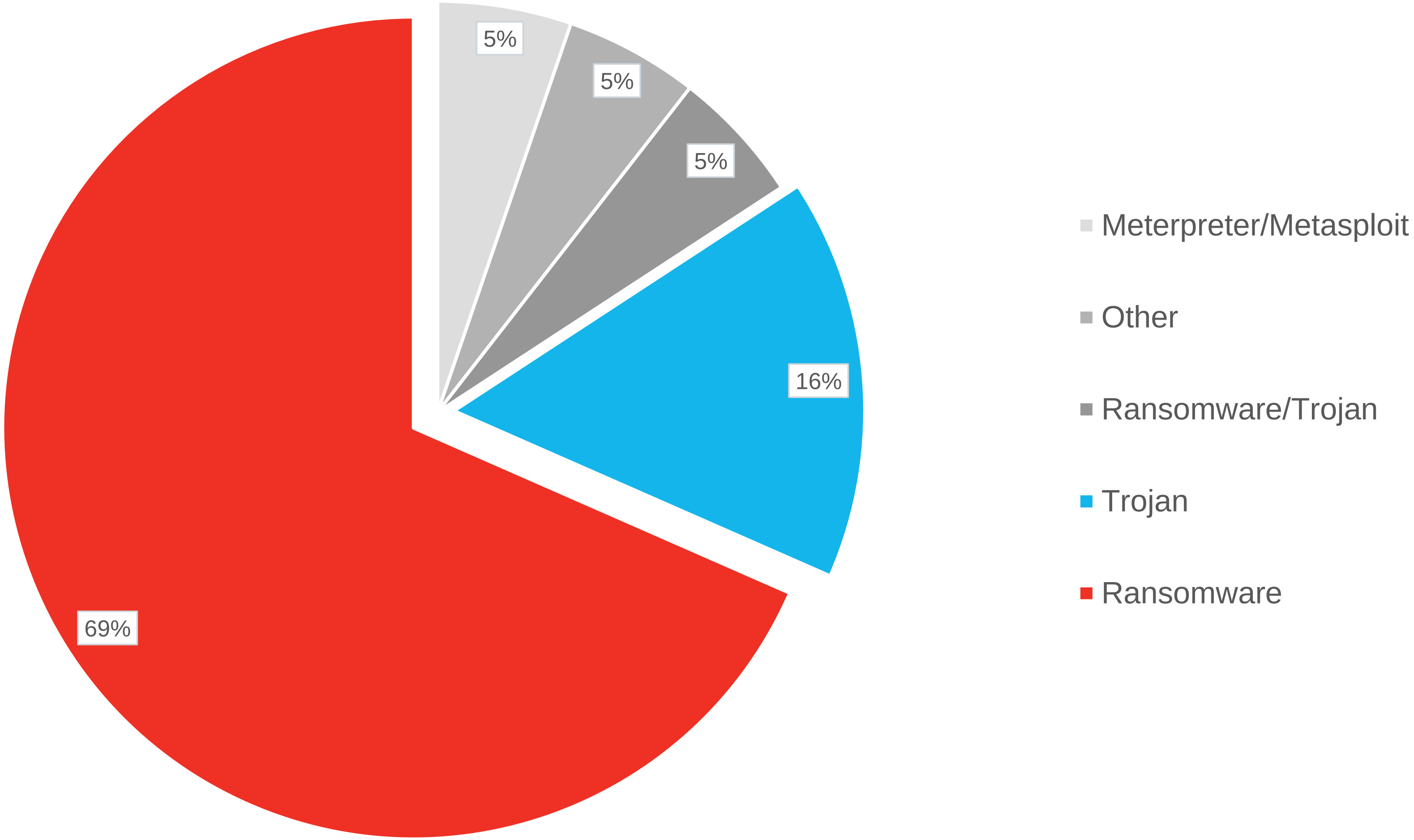
Kroll found actors’ Linux commands to initiate a cron job (a task scheduler), instructing periodic data exfiltration

The healthcare industry has the 2nd largest Citrix userbase*

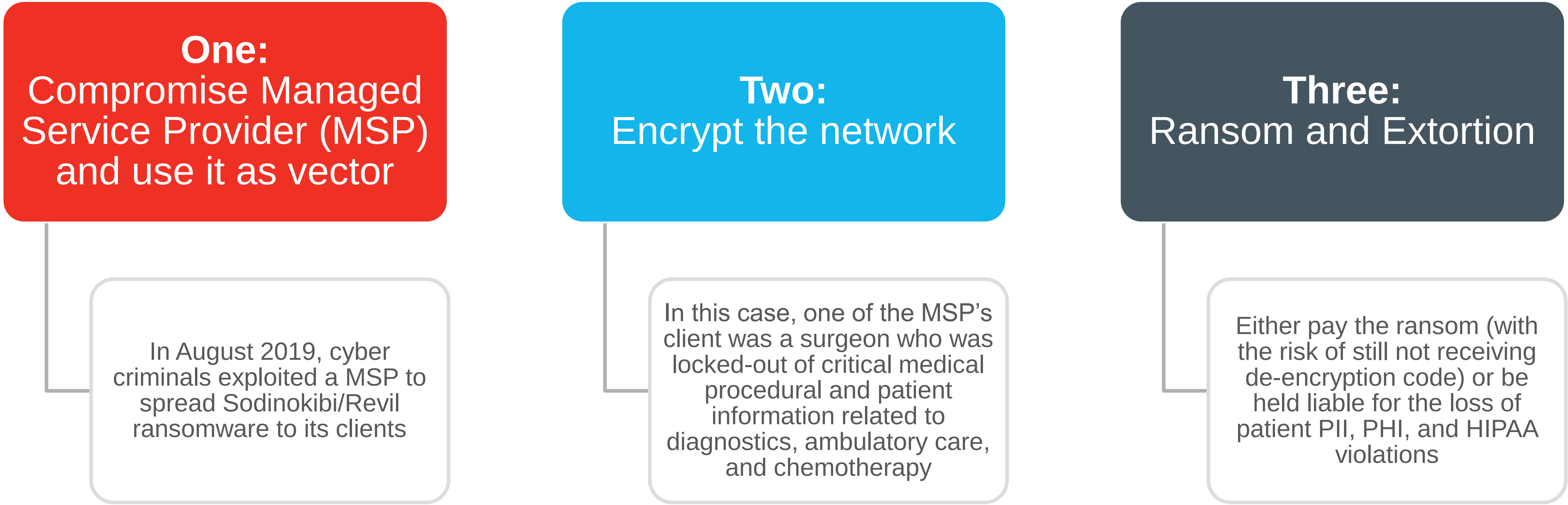


** Enlyft study as of 4/20/20 - enlyft.com/tech/products/citrix-xenapp*

Q1 2020 Malware – Healthcare



Case Study: Sodinokibi/Revil exploiting MSP vulnerabilities



One:
Compromise Managed Service Provider (MSP) and use it as vector

In August 2019, cyber criminals exploited a MSP to spread Sodinokibi/Revil ransomware to its clients

Two:
Encrypt the network

In this case, one of the MSP’s client was a surgeon who was locked-out of critical medical procedural and patient information related to diagnostics, ambulatory care, and chemotherapy

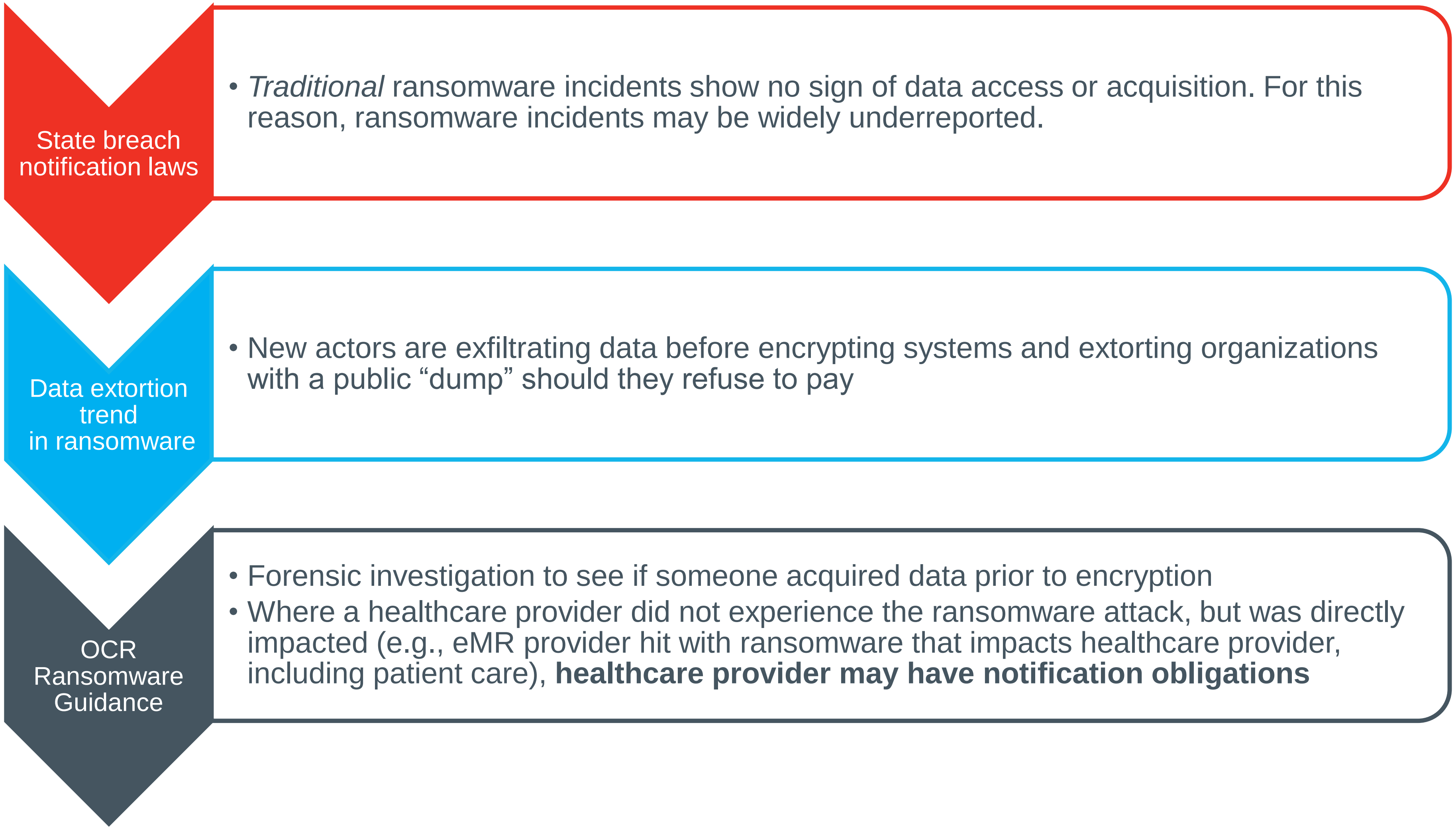
Three:
Ransom and Extortion

Either pay the ransom (with the risk of still not receiving de-encryption code) or be held liable for the loss of patient PII, PHI, and HIPAA violations

⚠ The largest ransom seen by Polsinelli was **$18 million**
(MSP whose business customers were impacted by the incident)

RANSOMWARE BREACH NOTIFICATION

Legal perspective and latest trends



State breach notification laws

- *Traditional* ransomware incidents show no sign of data access or acquisition. For this reason, ransomware incidents may be widely underreported.

Data extortion trend in ransomware

- New actors are exfiltrating data before encrypting systems and extorting organizations with a public "dump" should they refuse to pay

OCR Ransomware Guidance

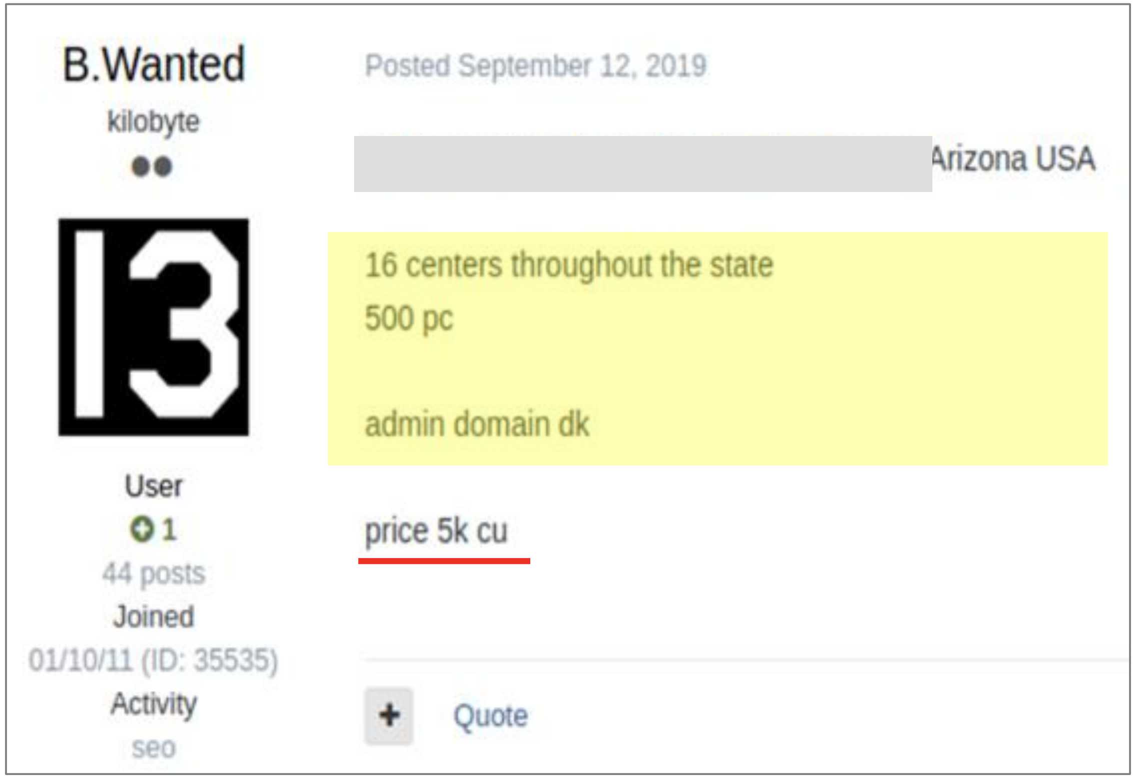
- Forensic investigation to see if someone acquired data prior to encryption
- Where a healthcare provider did not experience the ransomware attack, but was directly impacted (e.g., eMR provider hit with ransomware that impacts healthcare provider, including patient care), **healthcare provider may have notification obligations**

2020

Dark Web Landscape

*“electronic healthcare records were selling for **$50 per chart** on the black market, compared to $1 for a stolen social security number or credit card number.”*
- FBI Cyber Division Alert

Example 1: Access to healthcare providers



B.Wanted

kilobyte

●●

User

1

44 posts

Joined

01/10/11 (ID: 35535)

Activity

seo

Posted September 12, 2019

[redacted] Arizona USA

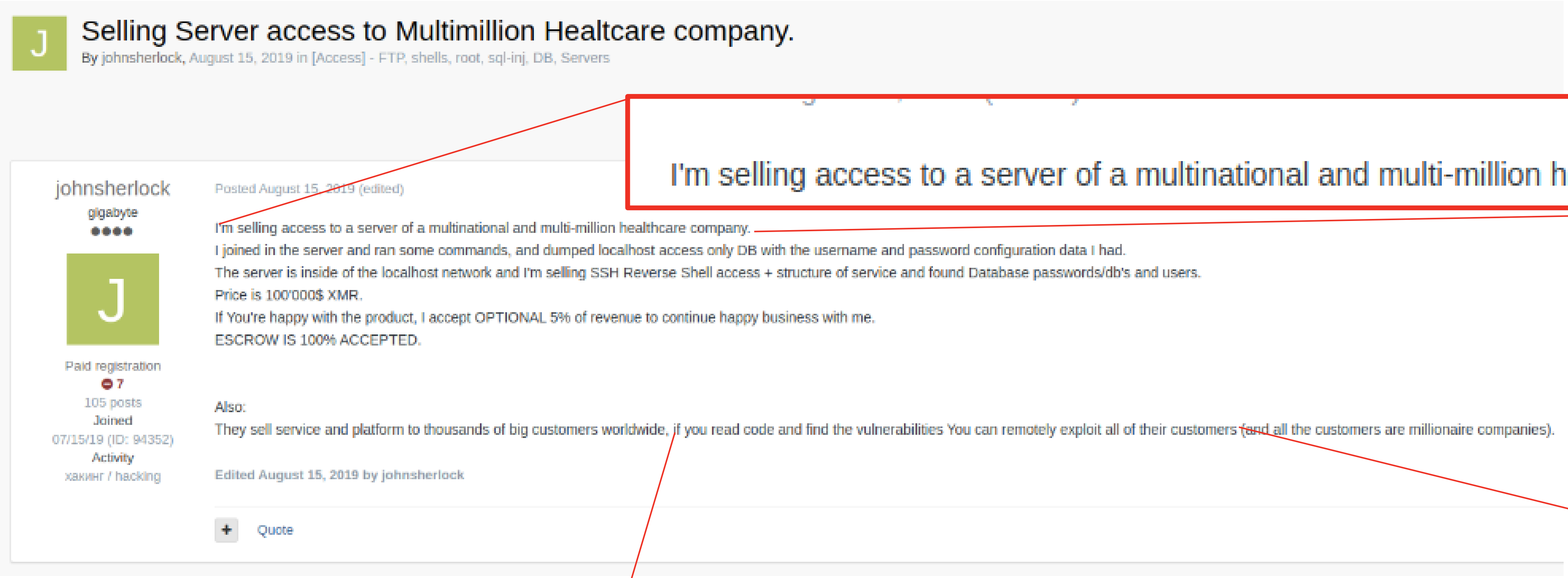
16 centers throughout the state

500 pc

admin domain dk

price 5k cu

Example 2: Access to healthcare providers



Selling Server access to Multimillion Healtcare company.

By johnsherlock, August 15, 2019 in [Access] - FTP, shells, root, sql-inj, DB, Servers

johnsherlock
gigabyte
●●●●
J
Paid registration
⊖ 7
105 posts
Joined
07/15/19 (ID: 94352)
Activity
хакинг / hacking

Posted August 15, 2019 (edited)

I'm selling access to a server of a multinational and multi-million healthcare company.
I joined in the server and ran some commands, and dumped localhost access only DB with the username and password configuration data I had.
The server is inside of the localhost network and I'm selling SSH Reverse Shell access + structure of service and found Database passwords/db's and users.
Price is 100'000$ XMR.
If You're happy with the product, I accept OPTIONAL 5% of revenue to continue happy business with me.
ESCROW IS 100% ACCEPTED.

Also:
They sell service and platform to thousands of big customers worldwide, if you read code and find the vulnerabilities You can remotely exploit all of their customers (and all the customers are millionaire companies).

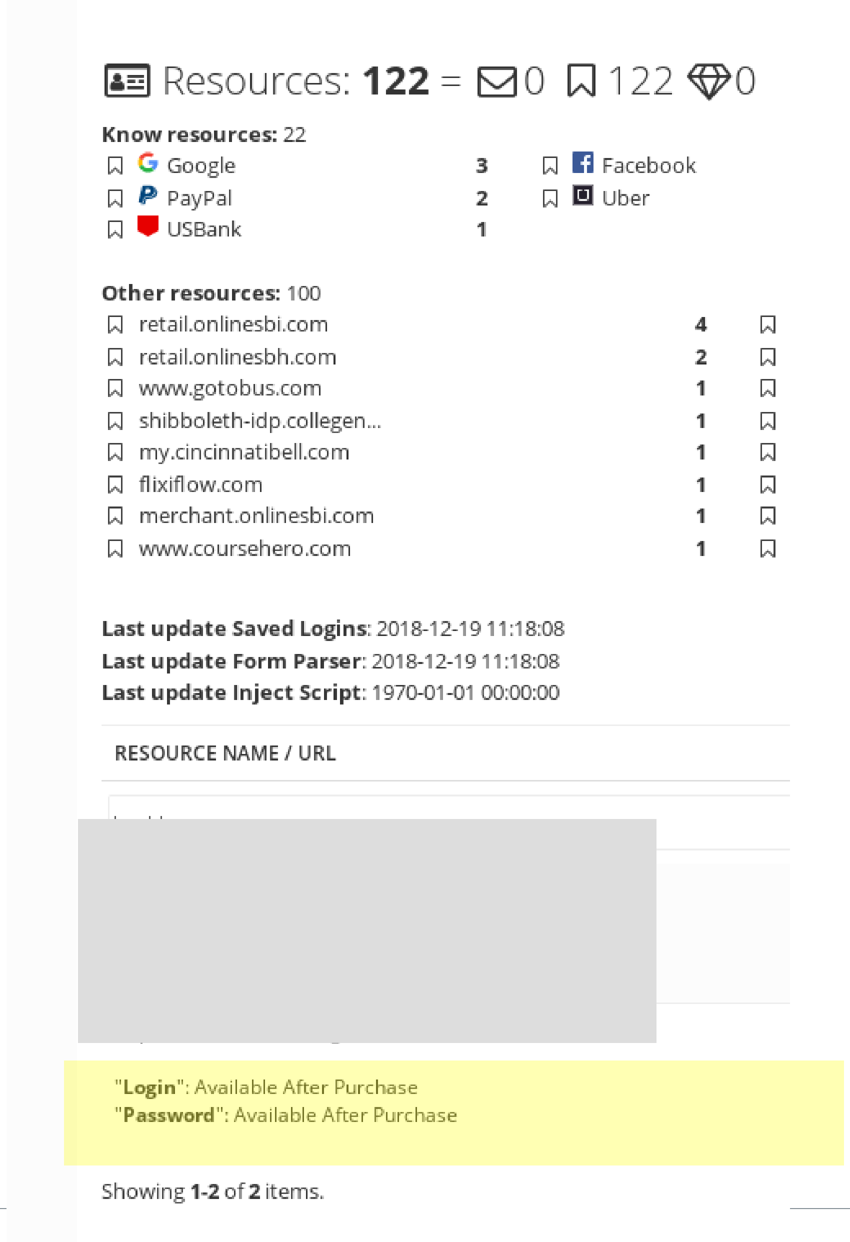
Edited August 15, 2019 by johnsherlock

I'm selling access to a server of a multinational and multi-million healthcare company.

if you read code and find the vulnerabilities You can remotely exploit all of their customers

Example 3: Health Insurance Marketplace Credentials

Genesis Market: log-in and password credentials for sale may give buyers access to protected health information as well as payment information



Resources: **122** = 0 122 0

Know resources: 22

Google	3	Facebook	
PayPal	2	Uber	
USBank	1		

Other resources: 100

retail.onlinesbi.com	4
retail.onlinesbh.com	2
www.gotobus.com	1
shibboleth-idp.collegen...	1
my.cincinnatibell.com	1
flixiflow.com	1
merchant.onlinesbi.com	1
www.coursehero.com	1

Last update Saved Logins: 2018-12-19 11:18:08
Last update Form Parser: 2018-12-19 11:18:08
Last update Inject Script: 1970-01-01 00:00:00

RESOURCE NAME / URL

[redacted]

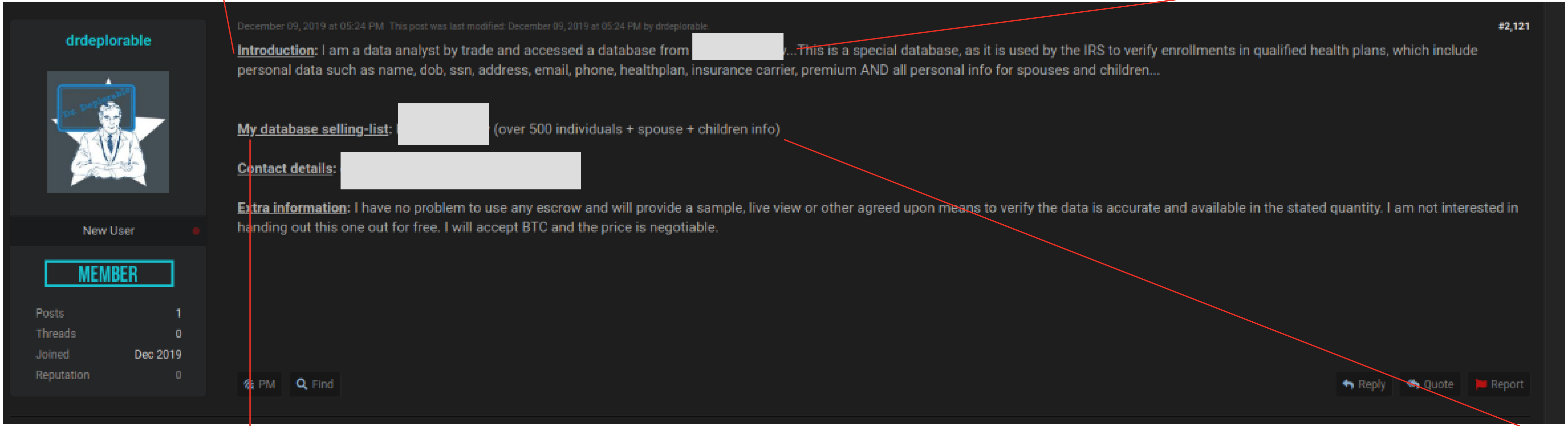
"**Login**": Available After Purchase
"**Password**": Available After Purchase

Showing **1-2** of **2** items.

Smaller dataset from health insurance marketplace

Potential insider threat:

Introduction: I am a data analyst by trade and accessed a database from [redacted] ..



drdeplorable

December 09, 2019 at 05:24 PM This post was last modified: December 09, 2019 at 05:24 PM by drdeplorable

#2,121

Introduction: I am a data analyst by trade and accessed a database from [redacted] ...This is a special database, as it is used by the IRS to verify enrollments in qualified health plans, which include personal data such as name, dob, ssn, address, email, phone, healthplan, insurance carrier, premium AND all personal info for spouses and children...

My database selling-list: [redacted] (over 500 individuals + spouse + children info)

Contact details: [redacted]

Extra information: I have no problem to use any escrow and will provide a sample, live view or other agreed upon means to verify the data is accurate and available in the stated quantity. I am not interested in handing out this one out for free. I will accept BTC and the price is negotiable.

New User

MEMBER

Posts	1
Threads	0
Joined	Dec 2019
Reputation	0

My database selling-list: [redacted] (over 500 individuals + spouse + children info)

Beware

> *In all **the 7 times that we've been hit** by this [Ransomware], this is the only time it's hit our backups"*

Kroll healthcare client

Preparation and Planning

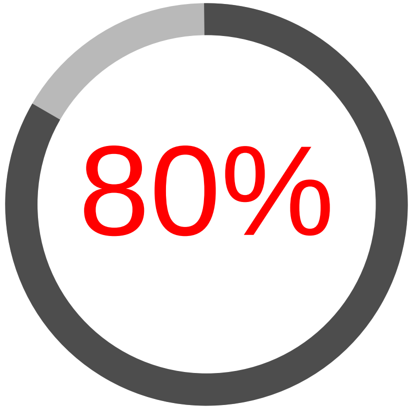
PREPAREDNESS

- Develop and refine incident response plan (IRP)
- Consider adequate insurance
- Establish legal, forensic providers (retainers)
- Multi-factor authentication everywhere!
- Secure, offline backups
- Routine assessments, vulnerability scanning, pen testing
- Managed detection and response
- Block SMB (port 445) and RDP (port 3389)
- Configure file integrity monitoring

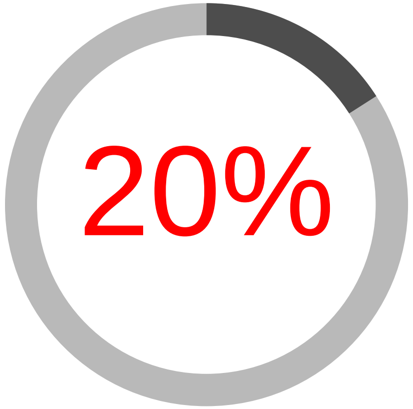
DETECTION / RESPONSE

- Isolate and disconnect
- Identify infection
- Report incident (law enforcement, insurance)
- Think before you pay
- Retain all log data
- Restore systems

The 80 / 20 Rule for a Strong Security Culture



of security safeguards rely on the user adhering to safe computing practices



of security safeguards are technical

Example:

Locking the door before you come to work

- The Lock on the door is the 20%
- Remembering to shut the door, turning the key, checking to make sure the door is locked, and confirming that others don't leave the door unlocked is the 80%.
- The best lock is worthless if SOMEONE isn't locking it properly every single time!

Q&A

KEITH WOJCIESZEK
Managing Director, Cyber Risk, Kroll

Keith.Wojcieszek@kroll.com

ANDREAS CHRYSOSTOMOU
Managing Director, Valuation Advisory, Duff & Phelps

Andreas.Chrysostomou@duffandphelps.com

BRUCE A. RADKE
Shareholder, Co-Chair, Privacy and Cybersecurity practice, Polsinelli

bradke@polsinelli.com

LAURIE IACONO
VP,
Cyber Risk, Kroll

Laurie.Iacono@kroll.com

NICOLE SETTE
Senior VP,
Cyber Risk, Kroll

Nicole.Sette@kroll.com

Kroll | A Division of DUFF & PHELPS

POLSINELLI

For more information about our global locations and services, please visit:

www.kroll.com

www.polsinelli.com

About Kroll

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security, and data and information management services. For more information, visit www.kroll.com.

About Duff & Phelps

Duff & Phelps is the global advisor that protects, restores and maximizes value for clients in the areas of valuation, corporate finance, investigations, disputes, cyber security, compliance and regulatory matters, and other governance-related issues. We work with clients across diverse sectors, mitigating risk to assets, operations and people. With Kroll, a division of Duff & Phelps since 2018, our firm has nearly 3,500 professionals in 28 countries around the world. For more information, visit www.duffandphelps.com.