2022 Healthcare Cybersecurity Year in Review, and a 2023 Look-Ahead

February 9, 2023

2022 Healthcare Cybersecurity Year in Review and a 2023 Look-Ahead

What events impacted healthcare cybersecurity in 2022, and what do they mean for your organization today and into the future?

- Introduction
- Cybersecurity Events Leading Up to 2022
- Cybersecurity Events of 2022
- Predictions for 2023 and Beyond
- Defense and Mitigation Recommendations
- References

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

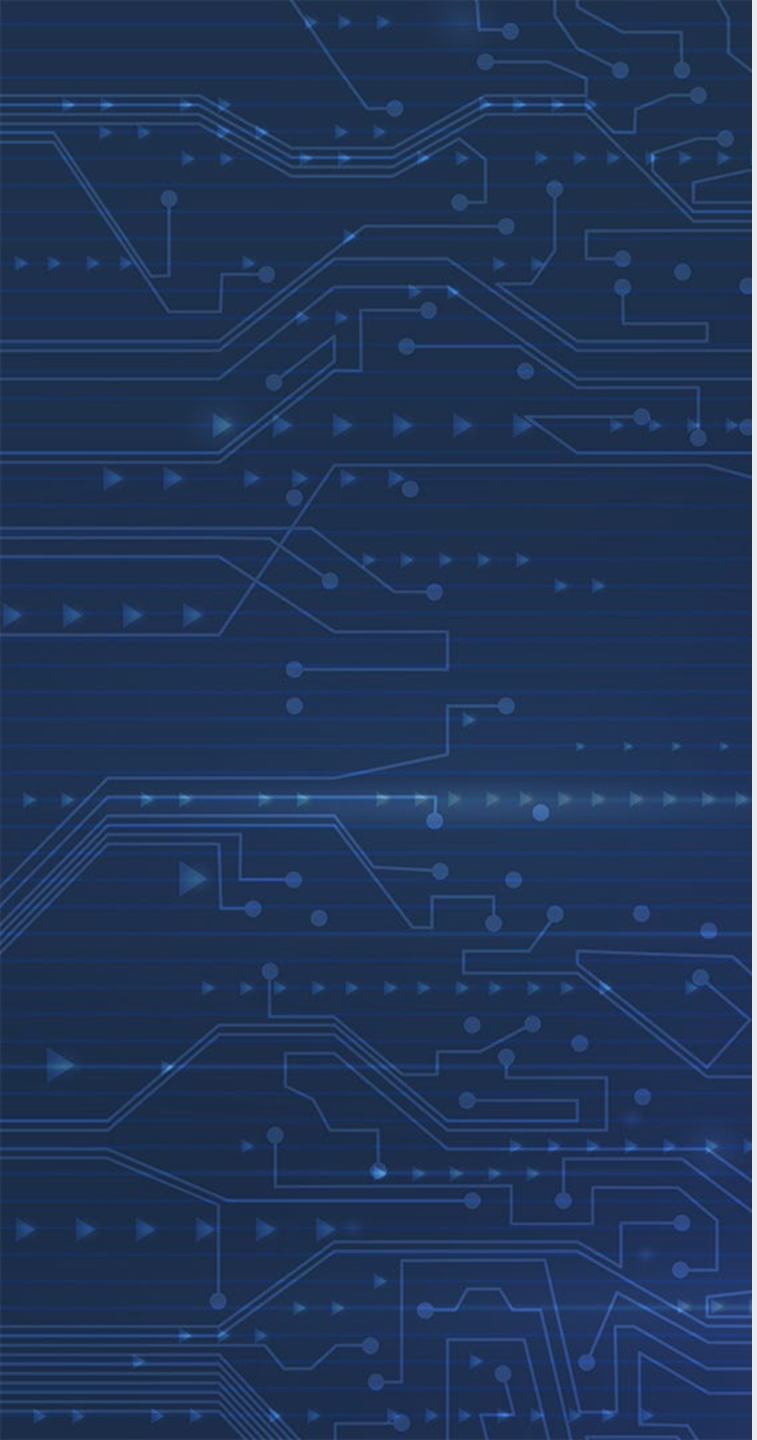
Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Questions to Consider

We will be looking at recent events related to healthcare cybersecurity, directly or indirectly, and examine what they mean for securing the health sector and HPH organizations.

- What technology and threat actor trends exist, and how will they impact HPH security?
- How can geopolitical events impact healthcare cybersecurity?
- What is the U.S. government and its international allies doing about these threats, and what impact will they have?

Image Source: Medical IT Services



Moving into 2022

What did the healthcare cybersecurity environment look like going into the year 2022?

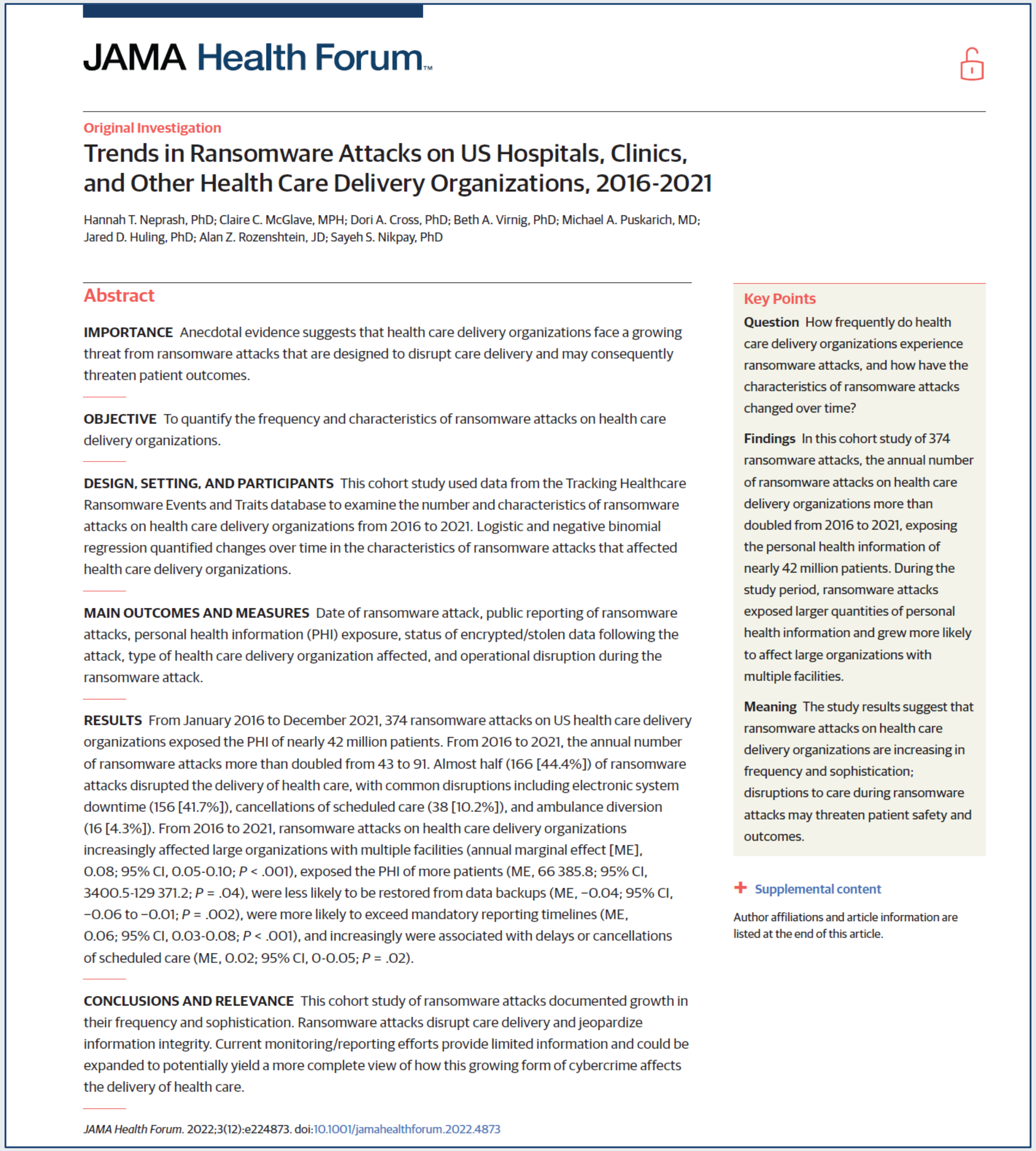
Research: Ransomware vs. Healthcare Delivery Organizations

A cohort study published in *The Journal of the American Medical Association* in December of 2022 examined ransomware attacks vs. healthcare delivery orgs. from 2016–2021.

The study leveraged data from the Tracking Healthcare Ransomware Events and Traits (THREAT) database.

<u>Conclusion</u>: Ransomware attacks targeting healthcare delivery orgs. doubled from 2016 to 2021.

The report can be accessed by clicking here.



JAMA Health Forum™

Original Investigation

Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021

Hannah T. Neprash, PhD; Claire C. McGlave, MPH; Dori A. Cross, PhD; Beth A. Virnig, PhD; Michael A. Puskarich, MD; Jared D. Huling, PhD; Alan Z. Rozenshtein, JD; Sayeh S. Nikpay, PhD

Abstract

IMPORTANCE Anecdotal evidence suggests that health care delivery organizations face a growing threat from ransomware attacks that are designed to disrupt care delivery and may consequently threaten patient outcomes.

OBJECTIVE To quantify the frequency and characteristics of ransomware attacks on health care delivery organizations.

DESIGN, SETTING, AND PARTICIPANTS This cohort study used data from the Tracking Healthcare Ransomware Events and Traits database to examine the number and characteristics of ransomware attacks on health care delivery organizations from 2016 to 2021. Logistic and negative binomial regression quantified changes over time in the characteristics of ransomware attacks that affected health care delivery organizations.

MAIN OUTCOMES AND MEASURES Date of ransomware attack, public reporting of ransomware attacks, personal health information (PHI) exposure, status of encrypted/stolen data following the attack, type of health care delivery organization affected, and operational disruption during the ransomware attack.

RESULTS From January 2016 to December 2021, 374 ransomware attacks on US health care delivery organizations exposed the PHI of nearly 42 million patients. From 2016 to 2021, the annual number of ransomware attacks more than doubled from 43 to 91. Almost half (166 [44.4%]) of ransomware attacks disrupted the delivery of health care, with common disruptions including electronic system downtime (156 [41.7%]), cancellations of scheduled care (38 [10.2%]), and ambulance diversion (16 [4.3%]). From 2016 to 2021, ransomware attacks on health care delivery organizations increasingly affected large organizations with multiple facilities (annual marginal effect [ME], 0.08; 95% CI, 0.05-0.10; $P < .001$), exposed the PHI of more patients (ME, 66 385.8; 95% CI, 3400.5-129 371.2; $P = .04$), were less likely to be restored from data backups (ME, −0.04; 95% CI, −0.06 to −0.01; $P = .002$), were more likely to exceed mandatory reporting timelines (ME, 0.06; 95% CI, 0.03-0.08; $P < .001$), and increasingly were associated with delays or cancellations of scheduled care (ME, 0.02; 95% CI, 0-0.05; $P = .02$).

CONCLUSIONS AND RELEVANCE This cohort study of ransomware attacks documented growth in their frequency and sophistication. Ransomware attacks disrupt care delivery and jeopardize information integrity. Current monitoring/reporting efforts provide limited information and could be expanded to potentially yield a more complete view of how this growing form of cybercrime affects the delivery of health care.

JAMA Health Forum. 2022;3(12):e224873. doi:10.1001/jamahealthforum.2022.4873

Key Points

Question How frequently do health care delivery organizations experience ransomware attacks, and how have the characteristics of ransomware attacks changed over time?

Findings In this cohort study of 374 ransomware attacks, the annual number of ransomware attacks on health care delivery organizations more than doubled from 2016 to 2021, exposing the personal health information of nearly 42 million patients. During the study period, ransomware attacks exposed larger quantities of personal health information and grew more likely to affect large organizations with multiple facilities.

Meaning The study results suggest that ransomware attacks on health care delivery organizations are increasing in frequency and sophistication; disruptions to care during ransomware attacks may threaten patient safety and outcomes.

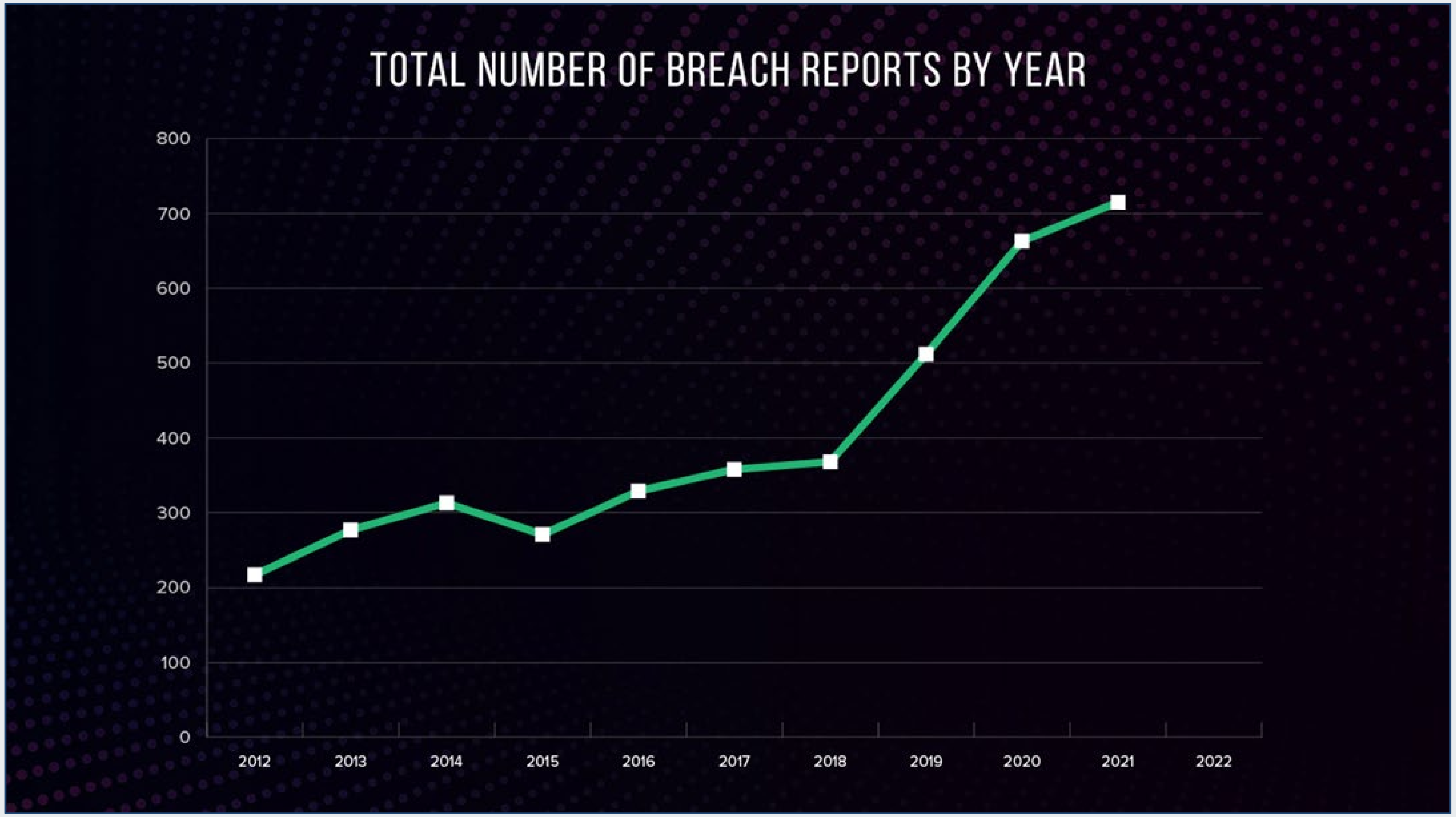
+ Supplemental content

Author affiliations and article information are listed at the end of this article.

Source: JAMA database

Healthcare Data Breaches

- Healthcare data breaches have consistently trended upward from 2012–2021.
- Healthcare data breaches have doubled in 3 years.



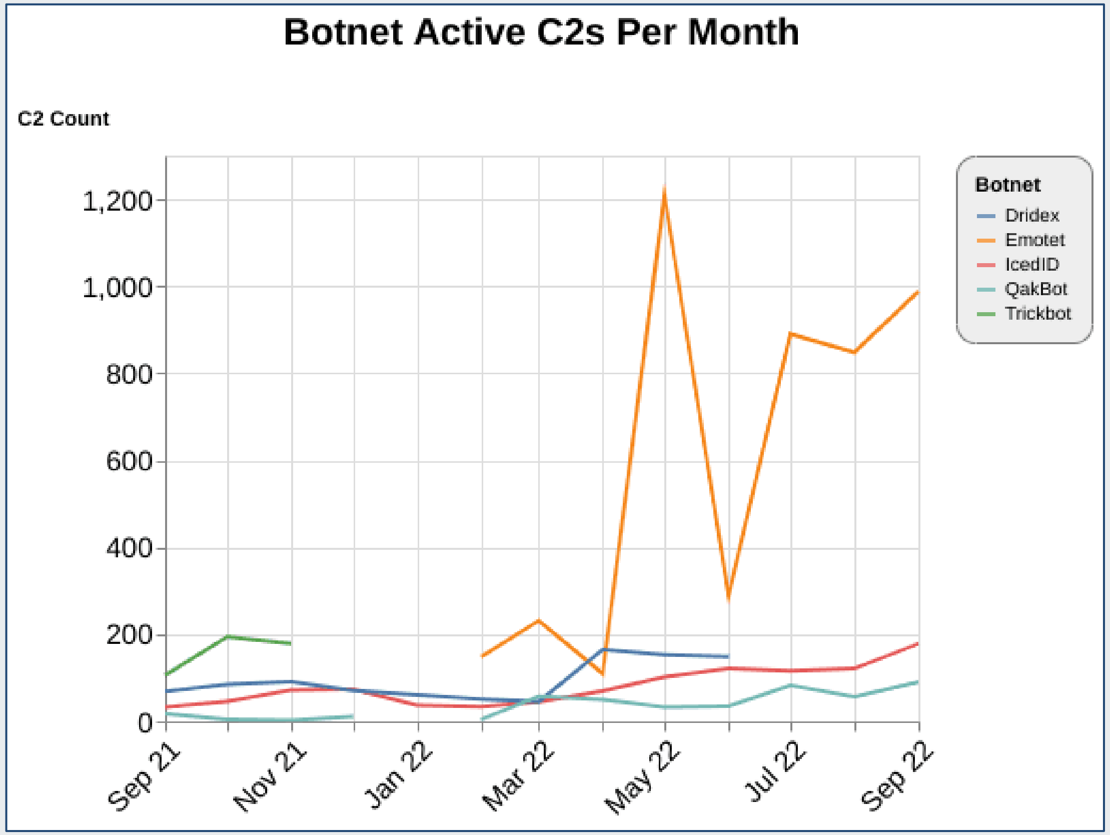
Healthcare data breaches trending upward. *(Source: BankInfoSecurity)*

Emotet Returns After Disruption

Emotet is a malware variant that has historically been a prolific threat to the health sector, and is often used as part of a cyberattack to deliver ransomware.

Recent history of Emotet:

- Taken down in January 2021, wiped April 2021
- Returned November 2021
- Spiked in late Spring 2022, dropped off
- Returned late 2022
- Currently used to drop Quantum and BlackCat ransomware



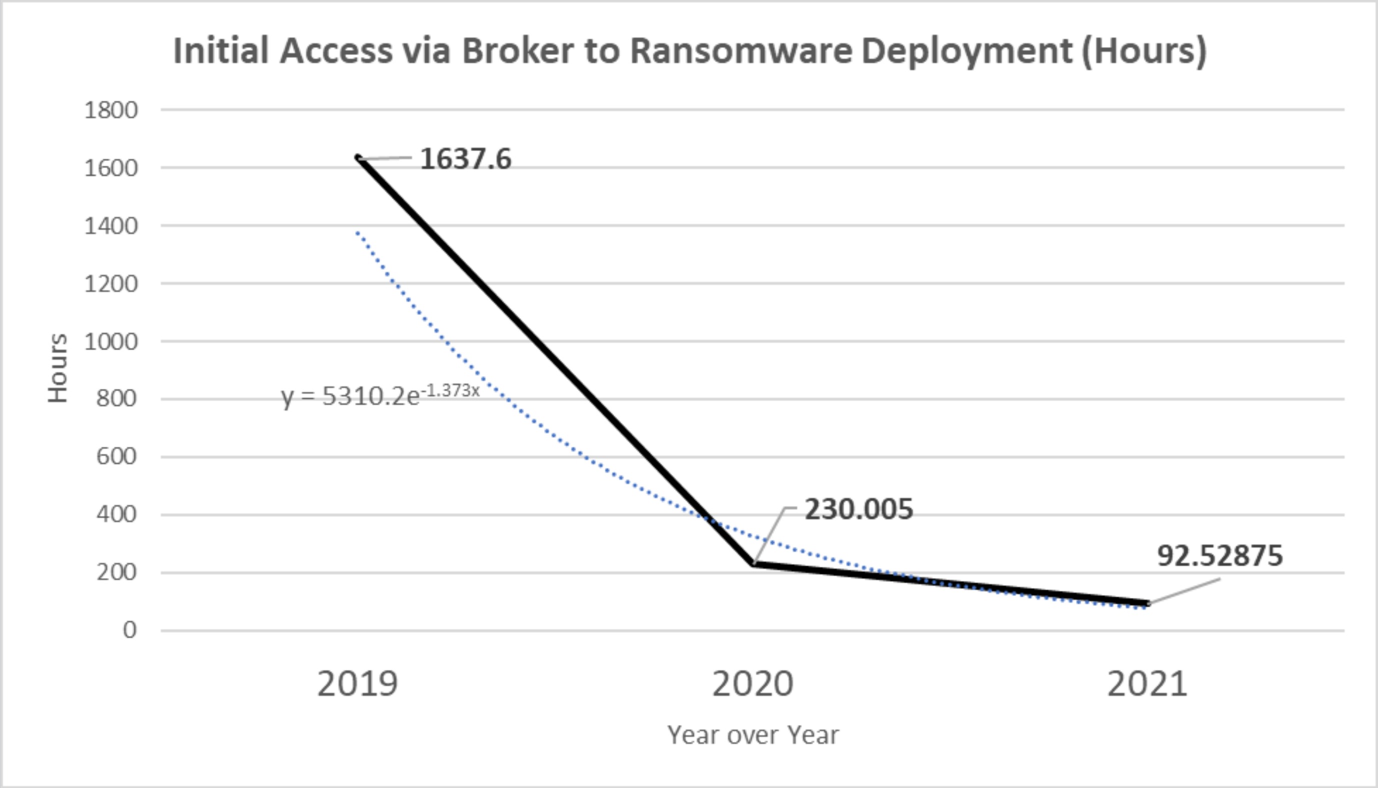
Emotet activity from late 2021 to late 2022. *(Source: Recorded Future)*

IBM: Ransomware Sophistication Study

According to IBM, ransomware attacks are increasing in their speed, especially when measuring the “time on target”.

IBM Ransomware study (June 2022)

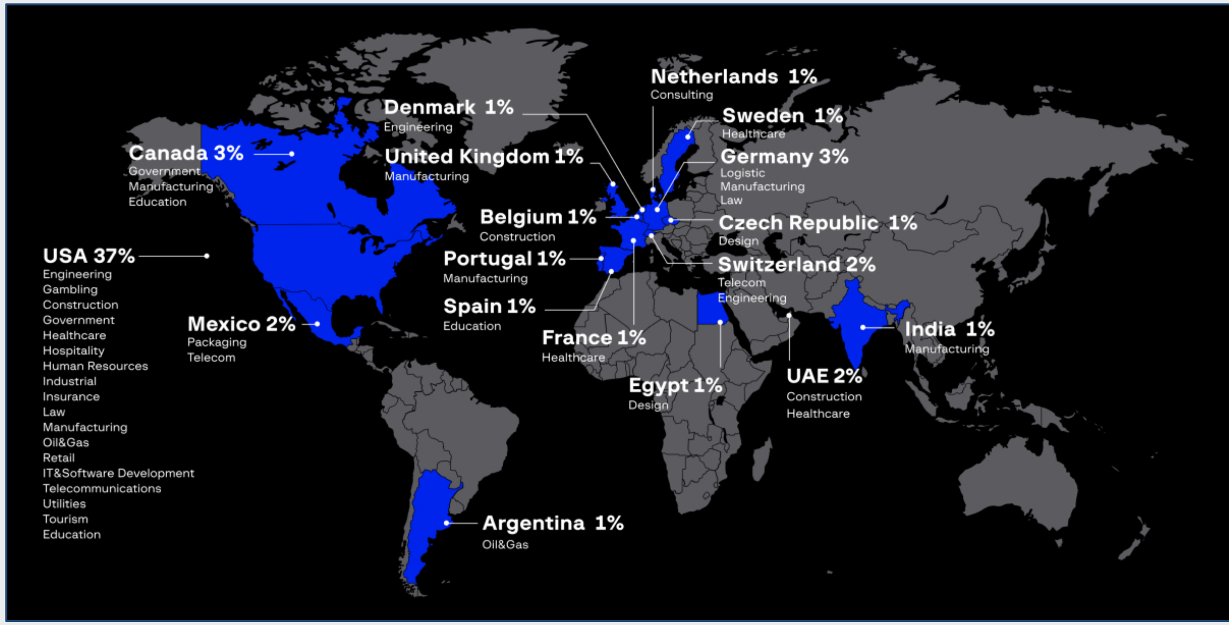
- Ransomware attacks need less than four days to encrypt systems
- 94% decrease in time-to-encrypt from 2019 to 2021
- Why?
  - Large scale malspam
  - Increased speed to transition access to affiliates



Group-IB: Ransomware Uncovered

Group IB Ransomware study (May 2022)

- Average ransom demand grew by 45% from 2020 to 2021, when it was $247,000.
- Highest ransom demands increased dramatically in 2021.
  - Largest ransom in 2020: $30M
  - Jumped to $70M in mid-2021 (Revil/Kaseya)
  - $240M for Hive attack in November 2021
- Downtime increased
  - 18 days in 2020 to 22 days in 2021



CISA and Australian Cyber Security Centre: 2021 Top Malware Strains

- CISA and the ACSC released their top malware strains for 2021.
- The list includes remote access Trojans (RATs), Trojans, information stealers, & ransomware droppers.
- The most prolific malware users are cyber criminals, motivated by theft of personal and financial information.
- Many of these are used to target the health sector.

The report can be accessed by clicking here.

Malware variant	Summary
Agent Tesla	RAT, information stealer
AZORult	Information stealer
FormBook	Information stealer
Ursnif	Also known as Gozi, information stealer and persistence
LokiBot	Information stealer
MOUSEISLAND	Macro downloader; often used as first stage
NanoCore	RAT, information stealer
Qakbot	Reconnaissance, lateral movement, gathering/exfiltrating data, dropping payloads
Remcos	Marketed as legitimate remote management and pen testing tool
TrickBot	Leveraged by a botnet; highly modular, multi-stage; Often used to drop ransomware
GootLoader	Often used as first stage; dropper

Emsisoft: The State of Ransomware in the US 2020 and 2021

- Annual total of ransomware attacks across industries, and specifically impacting healthcare.

The reports can be accessed by clicking here:

2020 2021

YEAR	Total	HPH	PHI	Notes
2020	2,354	560	12	Maze was only ransomware gang conducting double extortion at beginning if year; no less than 17 other gangs had adopted the tactic by the end of 2020.
2021	2,323	1,203	Unk.	One single attack targeted a provider that maintains over 600 locations; One single HPH compromise cost over $110 million.

2021 Government Action Summary

- Coordinated international law enforcement disruption of Netwalker ransomware gang by the DoJ (January 2021)
- Department of Justice charges Latvian national for her role with Trickbot (February 2021)
- Sentencing (10 years in prison) of FIN7 administrator, Fedir Hladyr, for conspiracy to commit wire fraud, computer hacking (April 2021)
- Department of Homeland Security issues new cybersecurity requirements for critical pipeline owners/operators (May 2021)
    - Requires critical pipeline owners/operators to report cybersecurity incidents, designate cybersecurity coordinators, and report risks, security gaps, and remediation measures to the federal government within 30 days
    - Response to Colonial Pipeline cyberattack

2021 Government Action Summary, Part 2

- Department of Justice elevates ransomware cases to the same priority given to terrorism (June 2021)
  - U.S. attorney's offices around the country handling ransomware attacks will be expected to share both updated case details and active technical information with leaders in Washington
- Stopransomware.gov launched – intended to be a hub of resources for the public to defend against ransomware (July 2021)
- The Department of State announced a $10 million reward for information related to the identification of state-sponsored cyber attackers as part of their Rewards for Justice Program. (July 2021) Specifically, these actions include:
  - Transmitting extortion threats as part of a ransomware attack
  - Intentional unauthorized access to a system to obtain information from it
  - Knowingly transmitting code or commands which cause damage to a system
- The U.S. and allies attributed the Microsoft Exchange (ProxyLogon) hacking campaign to China (July 2021)
  - The attacks targeted over a quarter of a million Exchange servers, belonging worldwide

2021 Government Action Summary, Part 3

- The White House announced a cross-government task force to coordinate both offensive and defensive measures against ransomware attacks. (July 2021) Some of the responsibilities of the task force include:
  - Promoting digital resilience among critical infrastructure companies
  - Working to halt ransom payments made through cryptocurrency platforms
  - Coordinating various actions with U.S. allies
- The Justice Department released an indictment for four members of the Chinese cyber threat group APT40 for cyberattacks related to theft of trade secrets and intellectual property (July 2021)

2021 Government Action Summary, Part 4

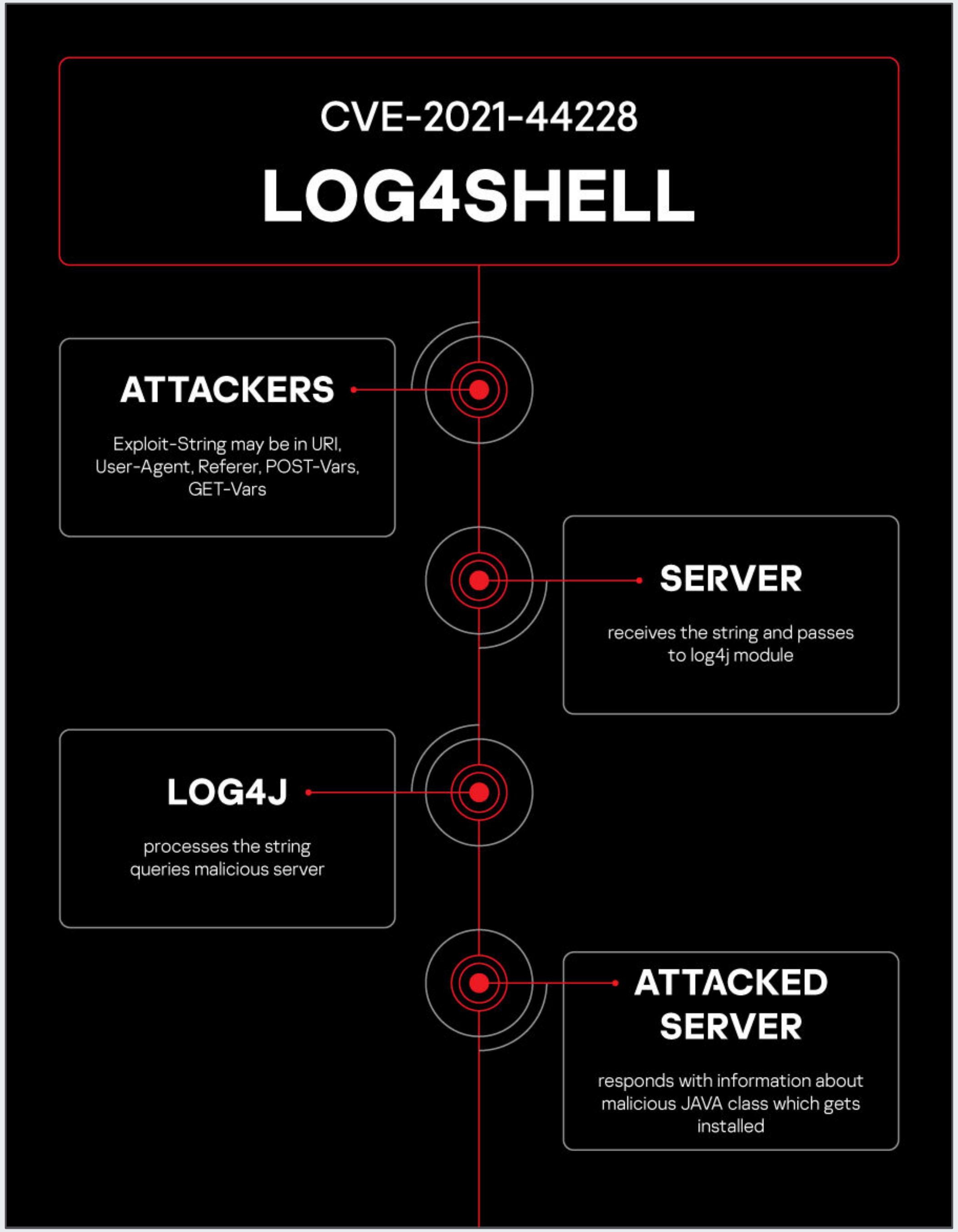
Trickbot developer arrested in South Korea. (September 2021)

- 38-year-old Vladimir Dunaev was alleged to be a malware developer that supervised the creation of TrickBot's browser injection module. He is facing charges that could get him 60 years in prison. (October 2021)
- The Biden administration convened a meeting of 30 countries to collaborate against ransomware operators including improving law enforcement cooperation, reducing illicit use of cryptocurrency and diplomatic engagement. (October 2021)
- Justin Johnson sentenced to seven years in prison for the 2014 hack of the University of Pittsburgh Medical Center. (October 2021)
- The Department of State announced a $10,000,000 reward for the identification or location of DarkSide ransomware members (or any rebrand group) operating in key leadership positions. (November 2021)
- The Department of State announced a reward of $10 million for information leading to the identification or location of individuals holding a leadership position in the REvil ransomware group – 7 REvil operators or affiliates arrested since February (November 2021)
- The U.S. Treasury Department announced sanctions on the cryptocurrency exchange Chatex for "facilitating financial transactions for ransomware actors". (November 2021)

Log4Shell

Log4J: Ubiquitous, Java-based, logging tool

- Initially discovered in November 2021
- Primary vulnerability tracked as CVE-2021-44228
- Multiple vulnerabilities discovered in November/December 2021, including several remote code execution flaws
- CISA Director Jen Easterly called the Log4Shell vulnerability the worst she's seen in her career
- CISA has documented Log4J's presence in more than 2,800 distinct commercial products
  - Likely present in hundreds of millions of IT systems



CVE-2021-44228
LOG4SHELL
ATTACKERS
Exploit-String may be in URI, User-Agent, Referer, POST-Vars, GET-Vars
SERVER
receives the string and passes to log4j module
LOG4J
processes the string queries malicious server
ATTACKED SERVER
responds with information about malicious JAVA class which gets installed

Log4Shell attack path. *(Source: Kaspersky)*

CVE	TYPE	Description/Notes
CVE-2021-44228	Remote Code Execution	Rated Critical; present in Log4j2 2.0-beta9 to 2.12.1 and 2.13.0 through 2.15.0; called Log4Shell; CVSS: 10 of 10; fixed in version 2.15.0
CVE 2021-45046	Denial of Service	Fix to address CVE-2021-44228 in 2.15.0 was incomplete in certain non-default configurations; fixed in version 2.16.0
CVE-2021-4104	Remote Code Execution	Rated High; present in versions 1.x; CVSS: 7.5; fixed in version 2.17.0 (no fix for Log4J version 1 - EoL)
CVE-2021-42550	Arbitrary Code Execution	Rated Moderate; present in Logback logging framework (successor to the Log4j 1.x); fixed with Logback versions, 1.3.0-alpha11 and 1.2.9
CVE-2021-45105	Denial of Service	Versions 2.0-alpha1 through 2.16.0 did not protect from uncontrolled recursion from self-referential lookups; CVSS: 7.5 of 10; fixed in version 2.17.0
CVE-2021-44832	Remote Code Execution	Present in version 2.17.0; CVSS score of 6.6; fixed in version 2.17.1

Five Vulnerabilities in Log4J (Plus One in Logback Framework)

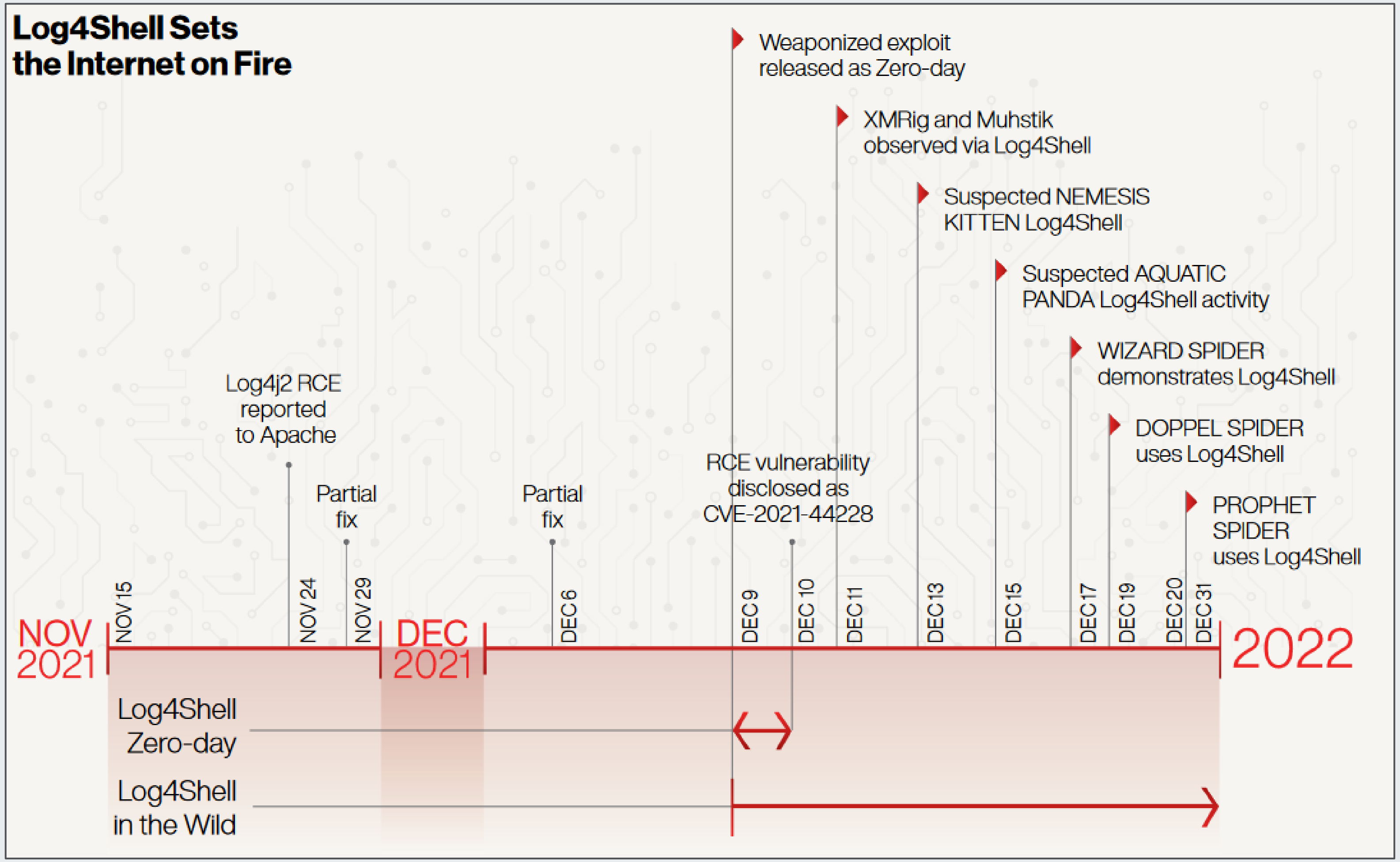
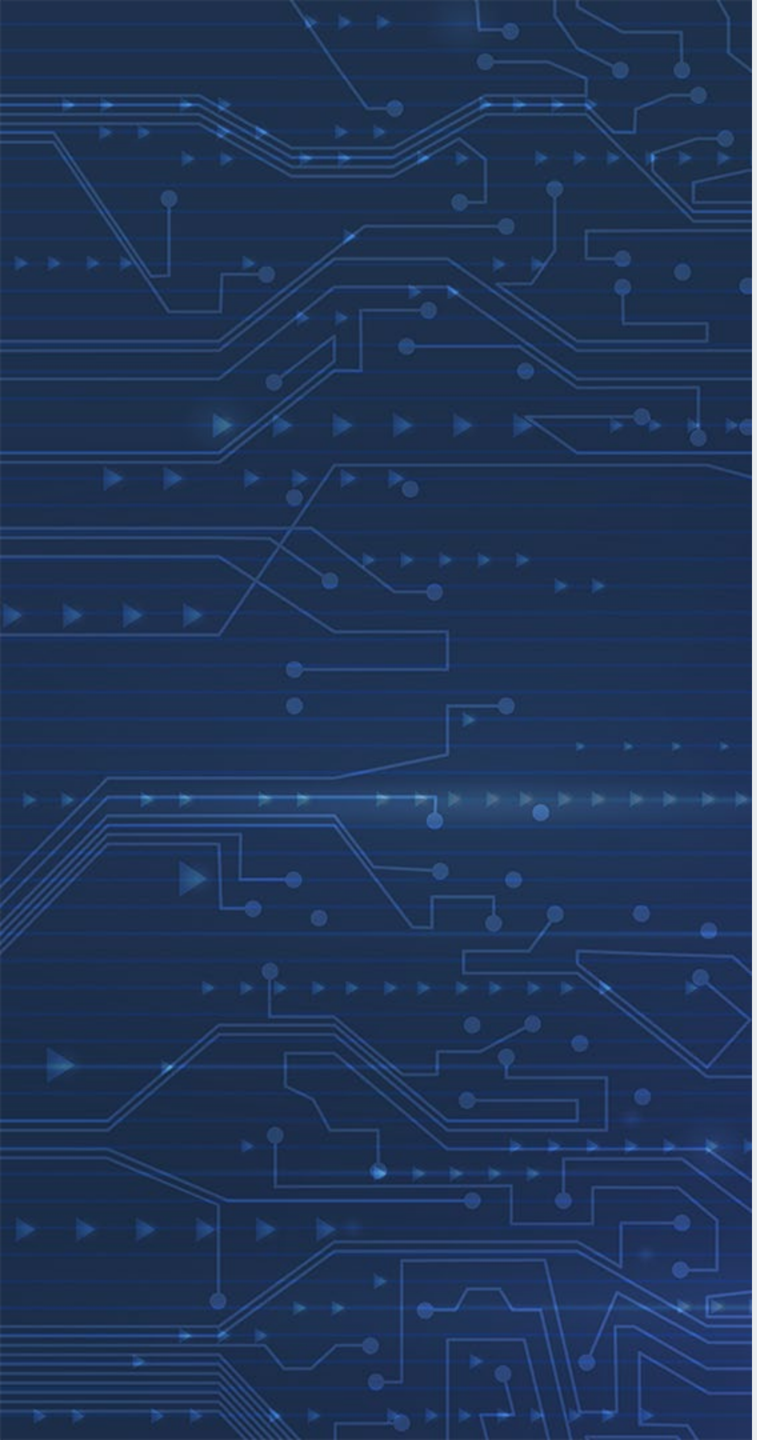


Image source: Crowdstrike

Log4Shell Timeline



2022: Events Relevant to Healthcare Cybersecurity

What events in 2022 had significant implications for health sector cybersecurity?

Emotet and TrickBot Continue to March Forward

Blackberry releases a report on increasing Emotet activity:

- The Emotet operators are “now setting the stage for future actions”
- New campaign being dropped by Trickbot

IBM recently released some research on Trickbot. New capabilities:

- Server-side injections as a delivery technique
  - More agile and more difficult to acquire for analysis
- JavaScript loader to communicate with the inject server
  - Operational security: HTTPS to C2 server
- Anti-debugging features added to JavaScript code
- Obfuscation
  - Rendering code unreadable to humans, string abstraction/replacement, hex representation

"They’re [Trickbot] trying to infect as many people as possible.“
– Limor Kessem, IBM Security

REvil Bust

- The Russian Federal Security Service arrested 12 members of the REvil ransomware gang in mid-January 2022
  - The FSS detained 14 suspected REvil members/affiliates and confiscated money and items:
    - More than 426 million rubles (approximately $5.5 million)
    - 600,000 U.S. dollars
    - 500,000 Euros (approximately $570,000)
    - 20 luxury cars purchased with money obtained from cyberattacks
    - Computer equipment and cryptocurrency wallets
  - Dmitri Alperovitch of CrowdStrike called it “ransomware diplomacy”, arguing that Russia was attempting to encourage the United States not intervene in their Ukraine incursion, and that they can be helpful in stopping ransomware.

Image source: HackRead

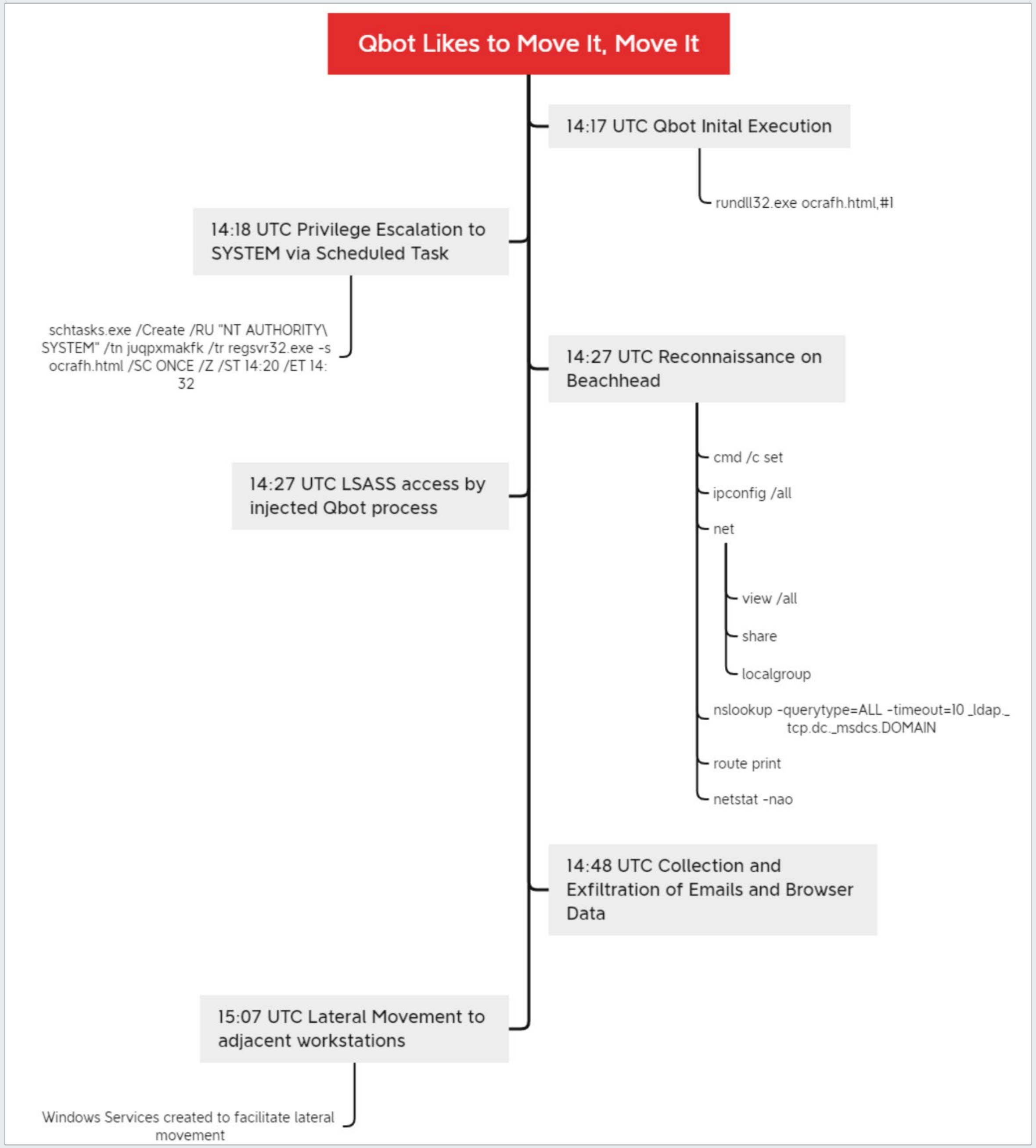
QBot: 30 Minutes to Compromise Data

DFIR released an analysis noting that Qbot can compromise data within 30 minutes of initial infection.

Qbot has been used aggressively to target the U.S. health sector.

Qbot is often used in multi-stage attacks, and to drop ransomware.

The original DFIR report can be accessed by clicking here.



Qbot Likes to Move It, Move It

14:17 UTC Qbot Inital Execution

```
rundll32.exe ocrafh.html,#1
```

14:18 UTC Privilege Escalation to SYSTEM via Scheduled Task

```
schtasks.exe /Create /RU "NT AUTHORITY\
SYSTEM" /tn juqpxmakfk /tr regsvr32.exe -s
ocrafh.html /SC ONCE /Z /ST 14:20 /ET 14:
32
```

14:27 UTC Reconnaissance on Beachhead

```
cmd /c set
ipconfig /all
net
  view /all
  share
  localgroup
nslookup -querytype=ALL -timeout=10 _ldap._
tcp.dc._msdcs.DOMAIN
route print
netstat -nao
```

14:27 UTC LSASS access by injected Qbot process

14:48 UTC Collection and Exfiltration of Emails and Browser Data

15:07 UTC Lateral Movement to adjacent workstations

Windows Services created to facilitate lateral movement

Qbot 30-minute infection lifecycle. *(Source: DFIR report)*

FBI Continues to Develop Crypto Capabilities

- The FBI announced the first director of the new National Cryptocurrency Enforcement Unit, Eun Young Choi.
  - Choi has a background as a federal prosecutor and has focused on cybersecurity cases.
    - Led the prosecution of a Russian national convicted of stealing data from over 100 million customers of several U.S. financial firms
  - The team includes over a dozen prosecutors, some of whom were involved in the Bitfinex cryptocurrency exchange case that allegedly involved the laundering of about $4.5 billion worth of stolen cryptocurrency.
  - Much of the team is made up of attorneys from across the Justice Department, with backgrounds in cryptocurrency, cybercrime, money laundering and forfeiture.

Image source: Tripwire

Russian Incursion into Ukraine

- On 24 February 2022, Russia launched a military invasion of Ukraine.
  - The U.S., Canada and European allies expelled some Russian banks from the SWIFT network
  - The European Union shut down airspace to Russian airlines and added several Russian oligarchs to their sanction list
  - European countries sent weapons to Ukraine
- In cyberspace:
  - A continuous wave of DDoS attacks against Ukrainian sites
  - Digital wipers observed in use against Ukrainian targets
  - Anonymous announced its opposition to Russia and released an anti-Putin video
  - Ukraine accused Belarusian hackers of targeting their infrastructure
  - The Conti ransomware operators came out in support of Russia but backed off initial comments

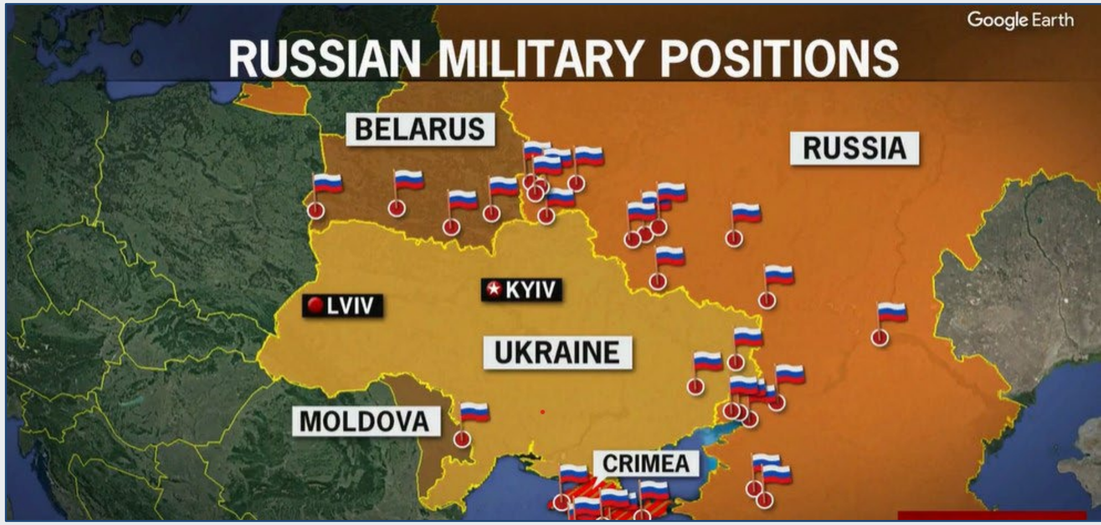


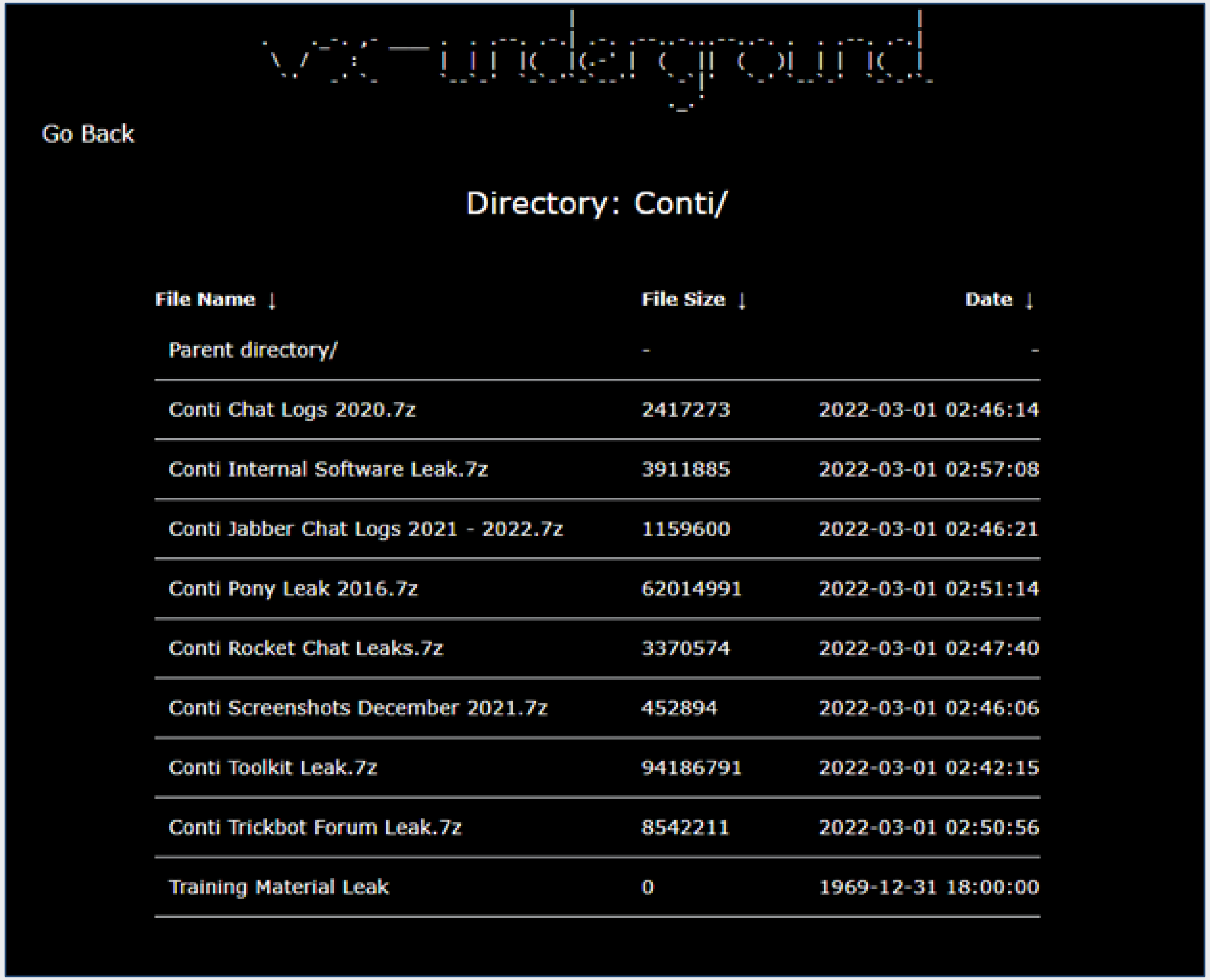
Image source: Google Earth

Conti Leaks

Conti ransomware decryptor leaked

- Internal chat logs – private communications within the group and between members were leaked
- Documentation related to tactics
- Source code and some decryptors
- One of the members was Ukrainian with strong patriotic loyalties

TrickBot source code also leaked



Go Back

Directory: Conti/

File Name ↓	File Size ↓	Date ↓
Parent directory/	-	-
Conti Chat Logs 2020.7z	2417273	2022-03-01 02:46:14
Conti Internal Software Leak.7z	3911885	2022-03-01 02:57:08
Conti Jabber Chat Logs 2021 - 2022.7z	1159600	2022-03-01 02:46:21
Conti Pony Leak 2016.7z	62014991	2022-03-01 02:51:14
Conti Rocket Chat Leaks.7z	3370574	2022-03-01 02:47:40
Conti Screenshots December 2021.7z	452894	2022-03-01 02:46:06
Conti Toolkit Leak.7z	94186791	2022-03-01 02:42:15
Conti Trickbot Forum Leak.7z	8542211	2022-03-01 02:50:56
Training Material Leak	0	1969-12-31 18:00:00

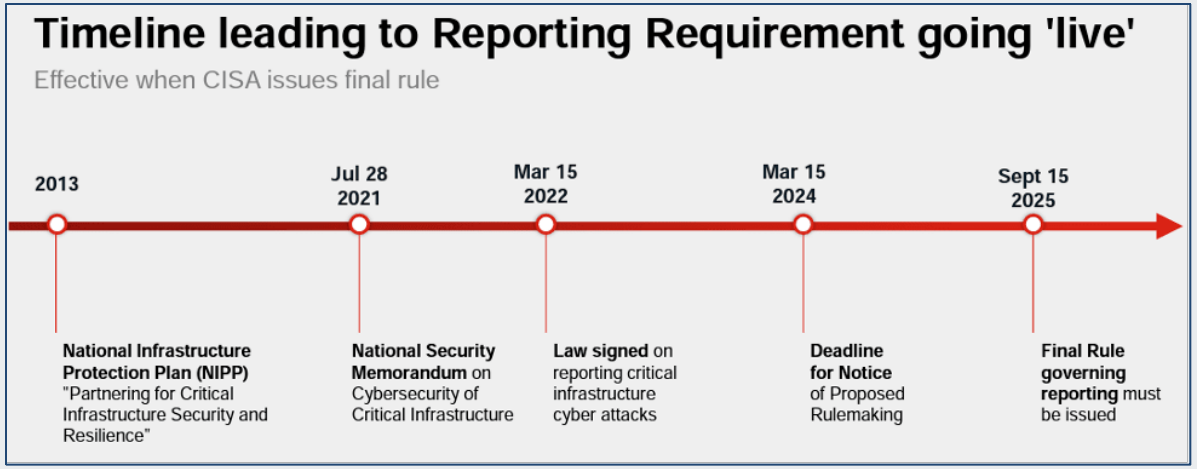
Image source: ThreatPost

Cyber Incident Reporting for the Critical Infrastructure Act

The White House signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022.

- The HPH is a covered entity – this law is applicable to public and private health organizations; once the proper standards are developed, the following will be in effect:
  - Critical infrastructure entities must report cyberattacks to CISA within 72 hours of discovery.
  - Critical infrastructure entities must report ransomware payments made within 24 hours.
- The seven requested items include:
  - Description of the incident
  - Description of the vulnerability
  - Security defenses maintained
  - Tactics, techniques, and procedures
  - Identifying information for a threat actor
  - Compromised information
  - Contact information for a covered entity

CISA's CIRCIA website: https://www.cisa.gov/circia



Timeline leading to Reporting Requirement going 'live'

Effective when CISA issues final rule

2013 – **National Infrastructure Protection Plan (NIPP)** "Partnering for Critical Infrastructure Security and Resilience"

Jul 28 2021 – **National Security Memorandum** on Cybersecurity of Critical Infrastructure

Mar 15 2022 – **Law signed** on reporting critical infrastructure cyber attacks

Mar 15 2024 – **Deadline for Notice** of Proposed Rulemaking

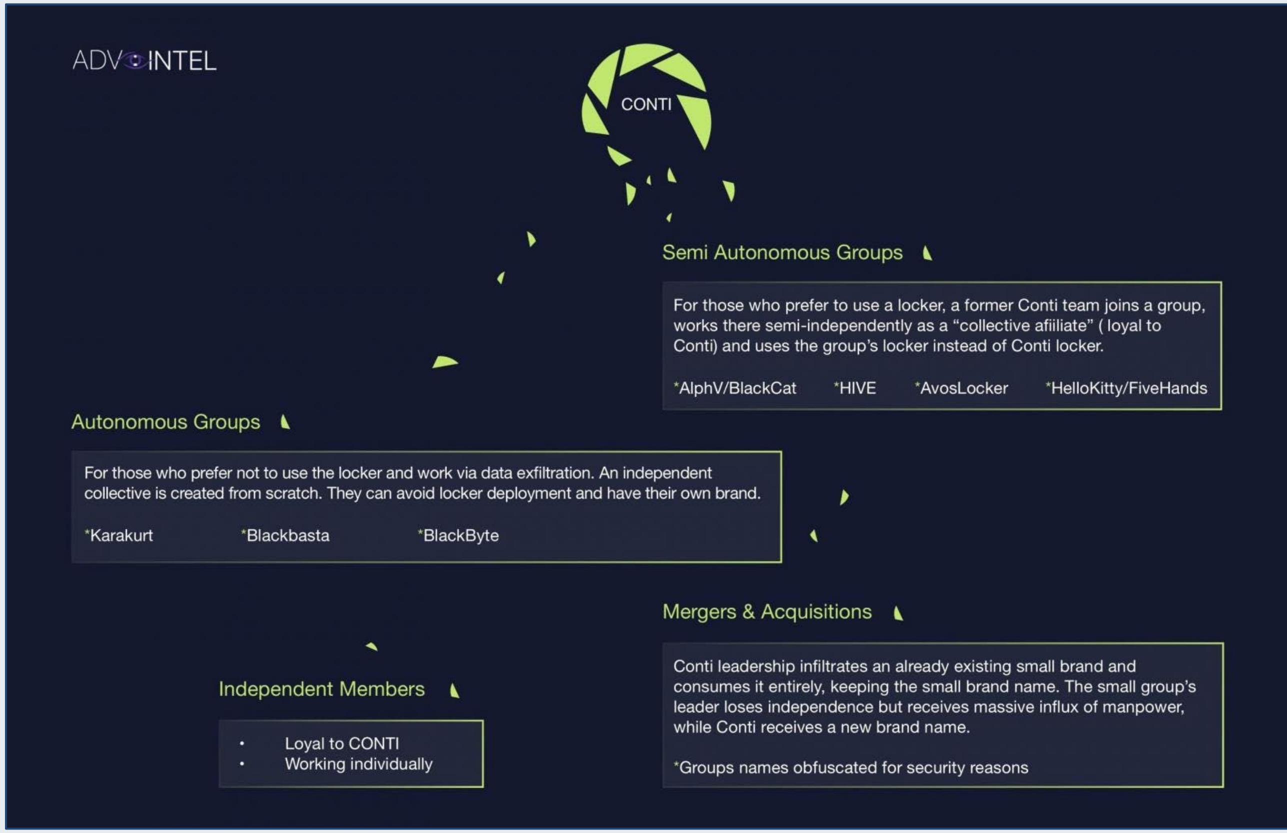
Sept 15 2025 – **Final Rule governing reporting** must be issued

Image source: ThreatPost

Conti Ransomware Gang Dismantles Infrastructure

The Conti ransomware operators dismantled their backend infrastructure, including their command and control.

- They are believed to have extorted at least $18M in ransoms since 2021.
- Pressure from other cybercriminal groups likely meant continuing operations were unfeasible.
  - Their support for the Russian incursion into Ukraine, despite retraction, was likely a factor.
  - Promises they would retaliate against Western critical infrastructure was also likely a factor.
  - Rebranding was likely not going to repair the “public relations” damage.
  - VM farms were believed to be cleared; servers were disabled.



Semi Autonomous Groups

For those who prefer to use a locker, a former Conti team joins a group, works there semi-independently as a “collective afiiliate” (loyal to Conti) and uses the group’s locker instead of Conti locker.

*AlphV/BlackCat *HIVE *AvosLocker *HelloKitty/FiveHands

Autonomous Groups

For those who prefer not to use the locker and work via data exfiltration. An independent collective is created from scratch. They can avoid locker deployment and have their own brand.

*Karakurt *Blackbasta *BlackByte

Mergers & Acquisitions

Conti leadership infiltrates an already existing small brand and consumes it entirely, keeping the small brand name. The small group’s leader loses independence but receives massive influx of manpower, while Conti receives a new brand name.

*Groups names obfuscated for security reasons

Independent Members

- Loyal to CONTI
- Working individually

Image source: ThreatPost

Log4Shell Continues to Be Exploited

In March of 2022, Log4Shell exploits were used mostly by DDoS botnets and cryptominers, according to Barracuda Networks.

- Barracuda observed that Log4Shell was exploited for both DDoS and cryptomining attacks.
  - They noted the use of DDoS malware variants such as Bill Gates and Muhstik.
  - They also observed frequent use of XMRig and Kinsing cryptominers, along with Log4Shell compromises.

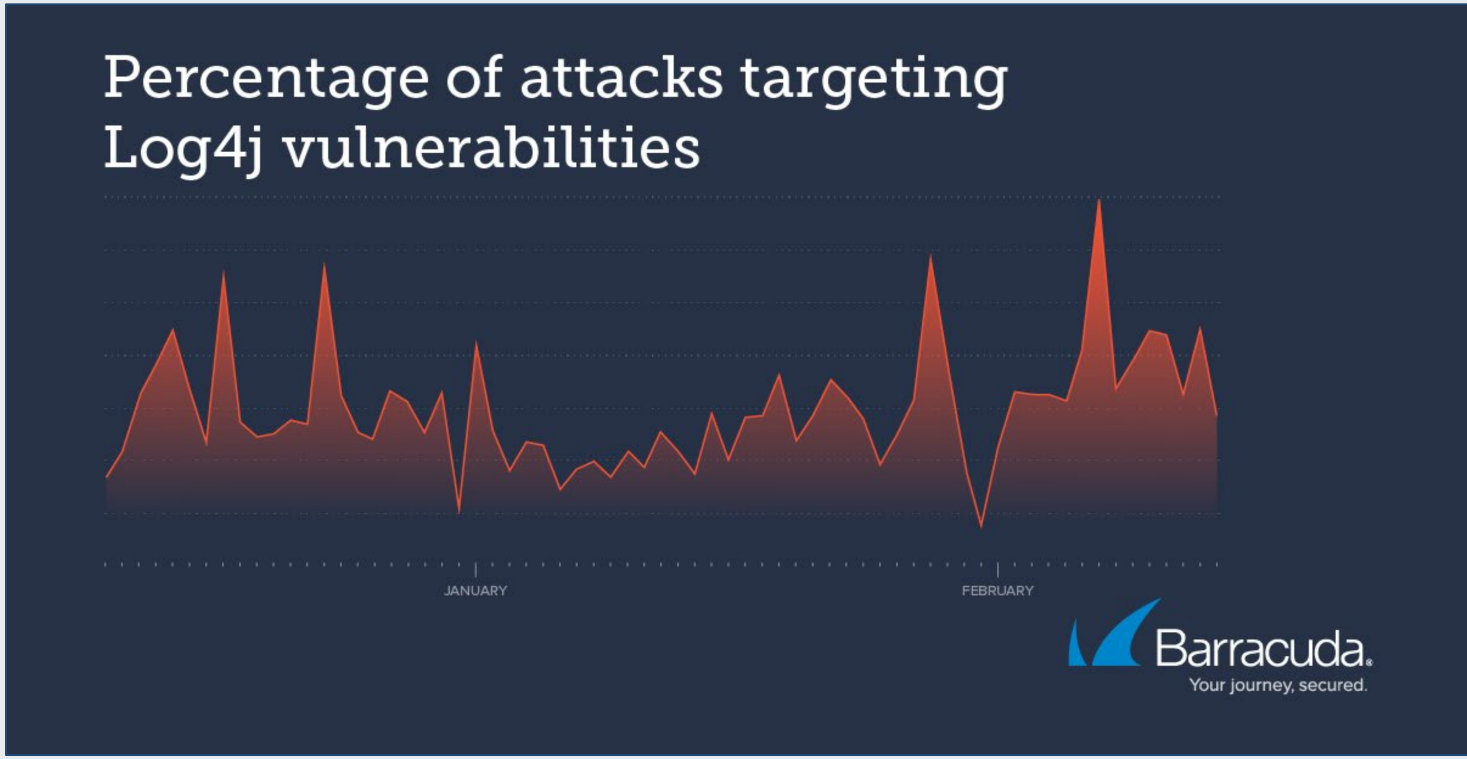


Image source: Barracuda Networks

Russia-Ukraine Cyberwar Heats Up

Imperva research on the cyber aspects of the Russia-Ukraine conflict:

- They looked at cyberattacks from March 7th and 8th and determined that almost 90% of the cyberattacks in the world were targeting either Russian or Ukrainian targets.
  - Specifically, of the over 6 billion cyberattacks they observed during those two days, 61% targeted Russa while 23% targeted Ukraine.
- ESET – CaddyWiper: New wiper malware discovered in use against Ukraine
  - Destroys data and partition information on any attached drives of a victim system
- The attackers appear to attempt to fully compromise a network before releasing the wiper.
- ESET has also discovered HermeticWiper and IsaacWiper.
- Microsoft also identified Whispergate earlier as well.

Image source: Webz.io

Emotet Continues

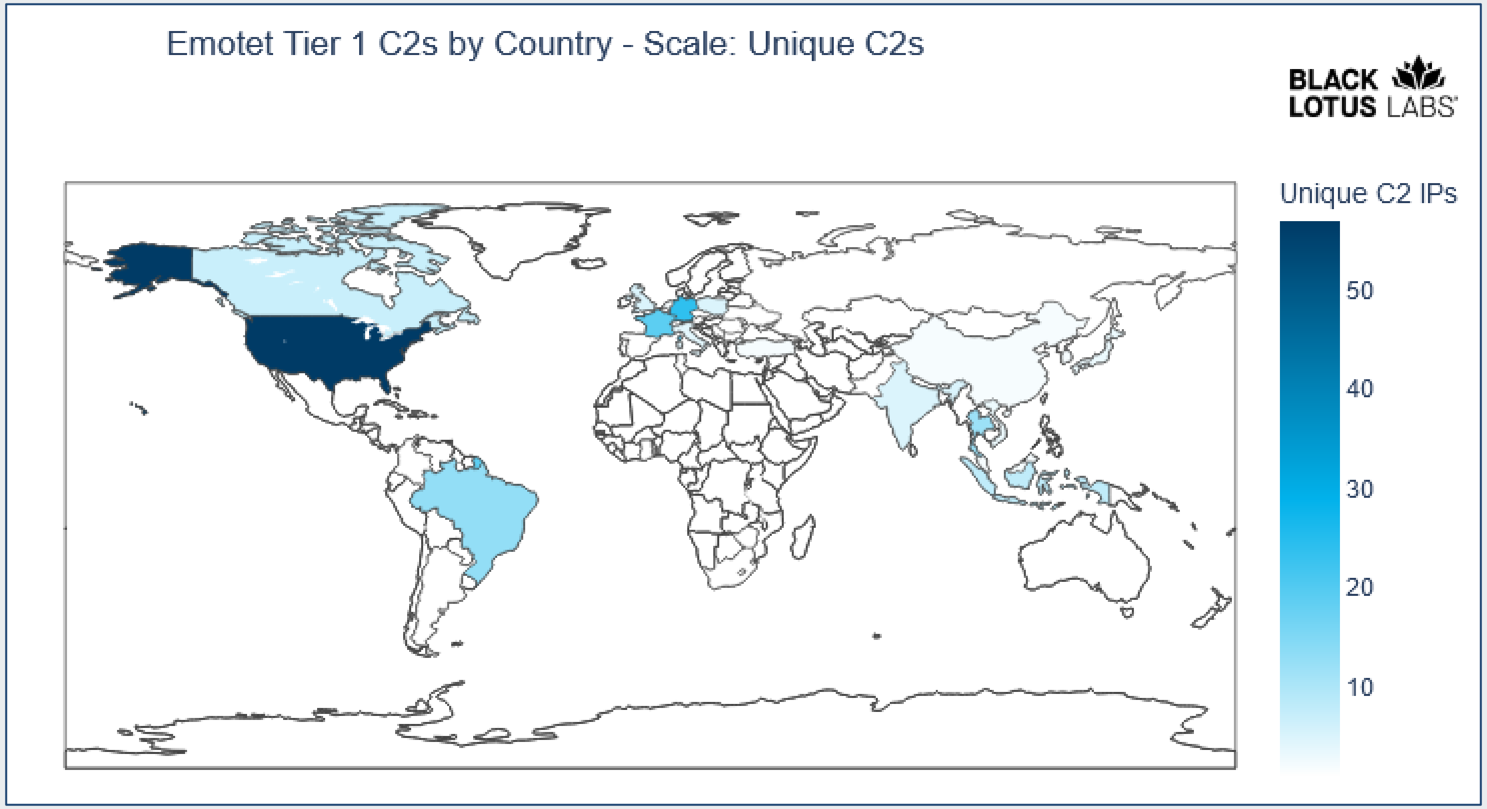
Lumen research:

- Emotet continues to uptrend
- The botnet now contains a total of approximately 130,000 unique bots spread across 179 countries.

CheckPoint research: Emotet was the most prolific malware variant in the month of February.

The original Lumen report can be found here.

The original CheckPoint report can be found here.



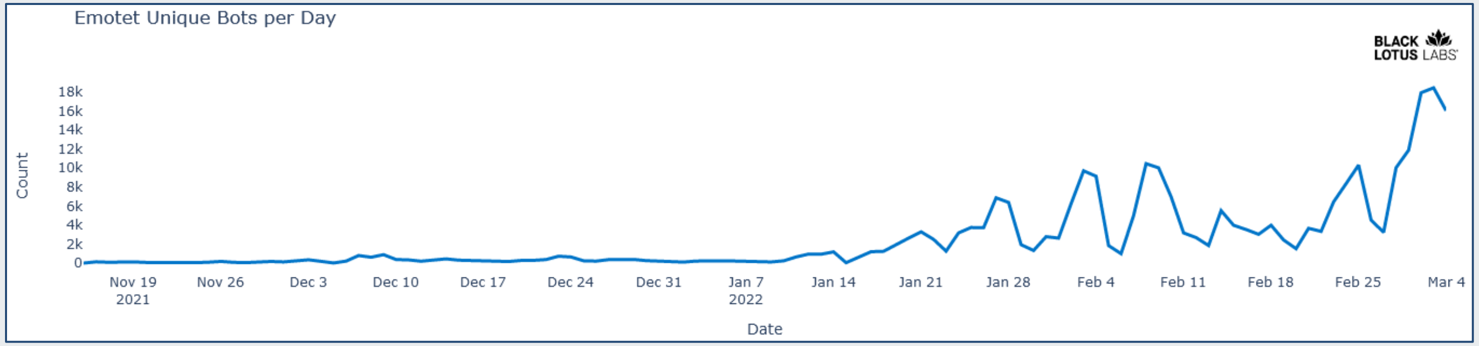


Image sources: Lumen

FBI Indicts Russian FSB Cyber Operators

The Department of Justice indicted four Russian government employees, three of whom are intelligence officers.

- Those three intel officers allegedly work for Russia’s Federal Security Service (FSB).
  - Specifically, they are accused of working for Military Unit 71330, or 'Center 16' of the FSB. This hacking group is tracked under multiple names, including Dragonfly, Berzerk Bear, Energetic Bear, and Crouching Yeti.
- They were accused of hacking into critical infrastructure targets around the world from 2012 to 2017.
- They were accused of targeting thousands of computers, at hundreds of organizations, in ~135 countries.

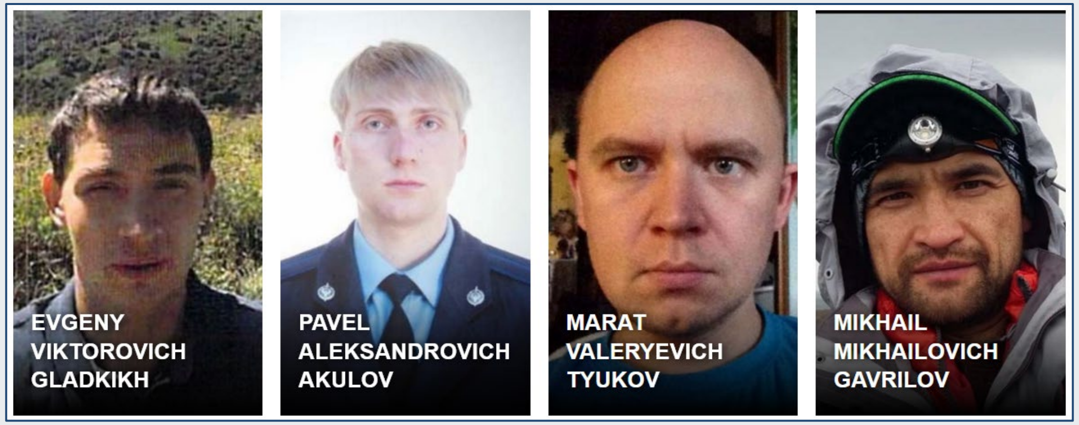

EVGENY VIKTOROVICH GLADKIKH
PAVEL ALEKSANDROVICH AKULOV
MARAT VALERYEVICH TYUKOV
MIKHAIL MIKHAILOVICH GAVRILOV

Image source: FBI

Healthcare Cybersecurity Act of 2022

On Capitol Hill, Senators Jacky Rosen, D-NV, and Bill Cassidy, R-LA sponsored a bill, S. 3904, the Healthcare Cybersecurity Act of 2022.

- This would require CISA and HHS to collaborate around improving cybersecurity in the healthcare and public health sectors, with CISA ultimately charged with the specifics.
- Part of that includes a detailed study on cybersecurity risks for the health sector, and how to manage these risks with a shortage of qualified cybersecurity workers.
- CISA would be responsible to make resources, including cyber-threat indicators and appropriate defense measures, available to federal and nonfederal entities that receive information through HHS programs.
- As it is currently written, it also authorizes new training for healthcare asset owners.
- As of the date of this briefing, the last action on the bill is “Reported to the Senate” which occurred on 10/18/2022.

Protecting and Transforming Cyber Health Care Act

Senators Tammy Baldwin, D-WI, and Bill Cassidy, R-LA introduced S.3983 – Protecting and Transforming Cyber Health Care Act, the PATCH Act

- This law is specifically focused on new requirements for medical device and network security.
- Specifically, this bill is designed for a few things:
  - Implement cybersecurity requirements for medical device manufacturers by requiring premarket approval through the Food and Drug Administration.
  - Require a Software Bill of Materials for devices that will be provided to users.
  - Require development of plans to identify and address postmarket cybersecurity vulnerabilities.
  - Enable manufacturers to design, develop and maintain processes and procedures to update and patch the device and related systems throughout device lifecycles.
- There is already companion legislation in the House of Representatives, H.H. 7084, sponsored by Reps. Michael Burgess, R-Texas, and Angie Craig, D-Minnesota.
- Last status: Introduced in the Senate

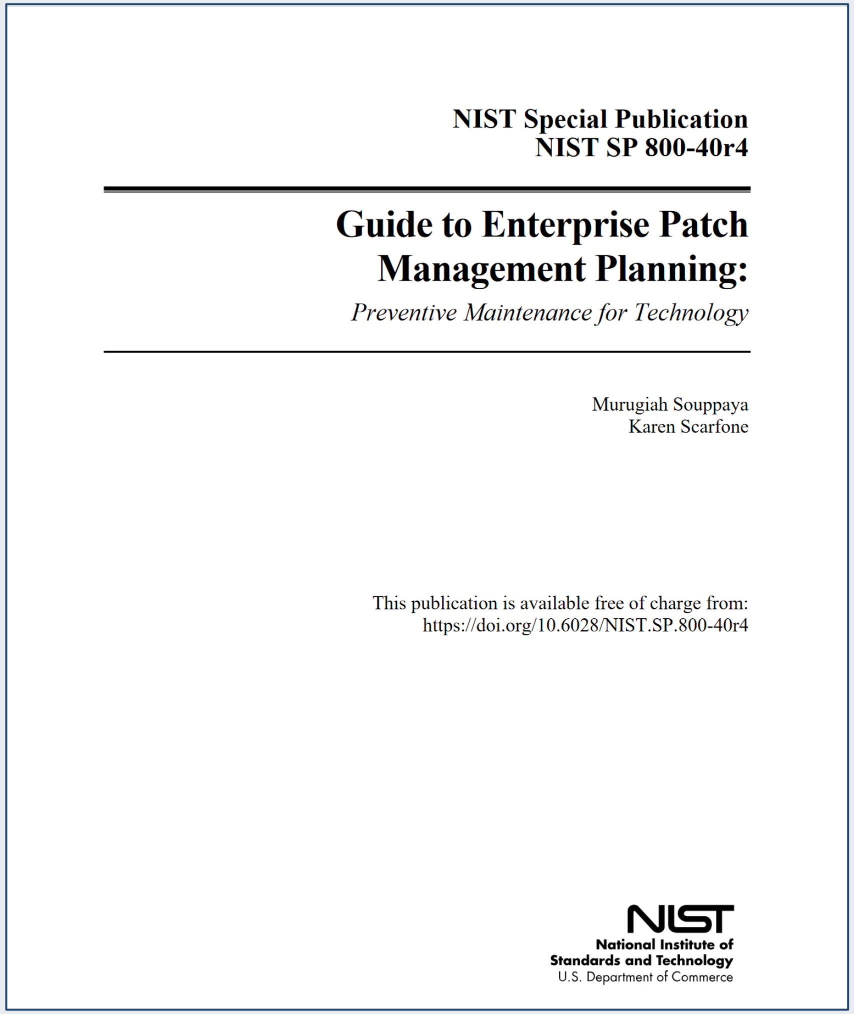
Sandworm Activity and State Department Bounty

Researchers at ESET and the Ukrainian Computer Emergency Response Team released research indicating an attempt by Russian state-sponsored threat actor Sandworm to blackout Ukraine.

- The Sandworm operators reportedly used a version of Industroyer (ICS malware customized for the target high-voltage electrical substations) to bring down a large Ukrainian energy provider.
- They then tried to erase their tracks by using a number of wipers, including CaddyWiper, Orcshred, Soloshred, and Awfulshred.
- The U.S. State Department Rewards for Justice program announced a $10 million bounty for anyone who can assist them in identifying/locating six Russian members of Sandworm.
  - Accused of having role in high-profile cyberattacks, including against U.S. critical infrastructure.
  - Believed to be behind cyberattacks on Ukrainian critical infrastructure in 2015 and 2016.
  - Believed to be behind the NotPetya attacks in 2017, which infected computers around the world, including hospitals, other medical facilities, and a large U.S. pharmaceutical manufacturer. The total damage is believed to be ~$1 billion.

NIST SP 800-40 Revision 4 Released

- The National Institute of Standards and Technology released an update to their patch management guide.
- They released revision 4 of SP 800-40: Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology.
  - Revision 3 was released back in July of 2013.
- Unpatched vulnerabilities are a major infection vector for both ransomware attacks and data breaches targeting the health sector.
- Version 4 can be found here.



NIST Special Publication
NIST SP 800-40r4

Guide to Enterprise Patch Management Planning:

Preventive Maintenance for Technology

Murugiah Souppaya
Karen Scarfone

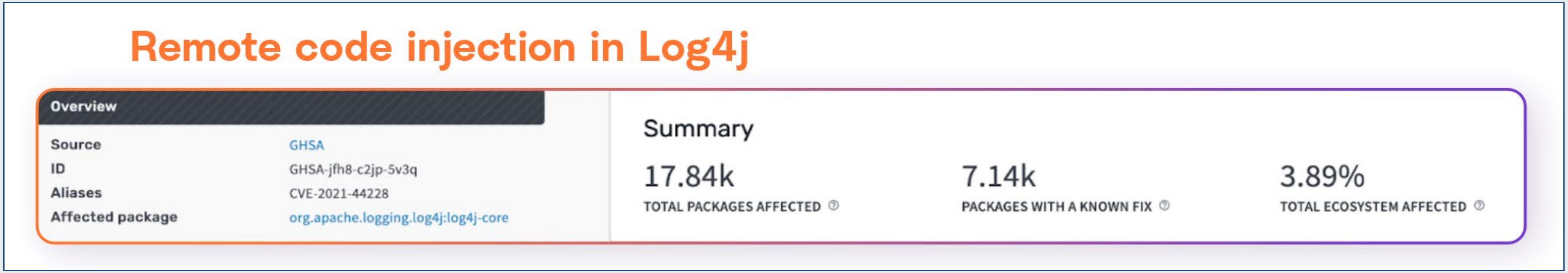
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-40r4

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Rezilion Log4J/Log4Shell Research

Rezilion released research on the vulnerabilities in Log4J, including Log4Shell.

- They identified ~90,000 Internet-facing applications that had unpatched Log4Shell instances.
- Four months after Log4Shell was discovered, millions of Java applications remained vulnerable to compromise.
- They found that out of almost 18,000 packages affected by the vulnerability, only about 7,000 were patched, making nearly 60% still vulnerable.



Remote code injection in Log4j

Overview

Source	GHSA
ID	GHSA-jfh8-c2jp-5v3q
Aliases	CVE-2021-44228
Affected package	org.apache.logging.log4j:log4j-core

Summary

17.84k	7.14k	3.89%
TOTAL PACKAGES AFFECTED	PACKAGES WITH A KNOWN FIX	TOTAL ECOSYSTEM AFFECTED

Image source: Rezilion

Sophos: State of Ransomware 2022

Sophos released their State of Ransomware 2022 report.

5,600 IT professionals in mid-sized organizations (100 – 5,000 employees) in 31 countries were surveyed during January and February 2022. Some data points of note from their research:

- The average ransomware payment is now right around $800K, which is a significant increase from the 2020 average, which was around $170K.
- The health sector represented the lowest ransom payments, with the average being under $200K.
- The proportion of victims who pay ransoms greater than $1M increased from 4% to 11%.
- Just under 50% of all ransoms are paid, and 99% of all organizations who paid the ransom received at least some of their data back.
- On average, about 60% of encrypted data is restored after paying the ransom, and 4% of all organizations received access to all their data back when they paid the ransom.

The State of Ransomware 2022

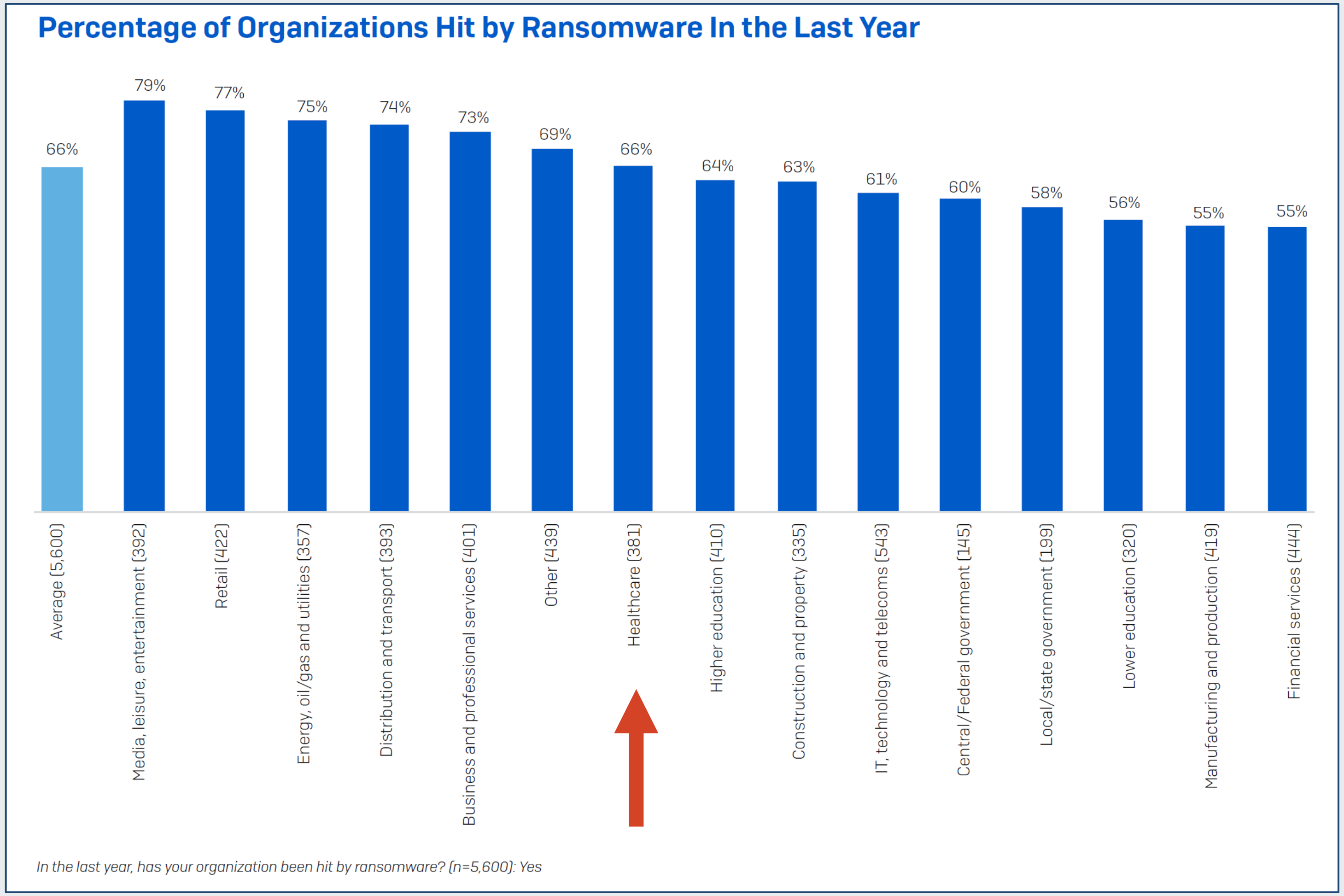
Findings from an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations across 31 countries.

Image source: Sophos

Sophos: State of Ransomware 2022, Part 2

66% of the healthcare organizations surveyed by Sophos reported that they were attacked with ransomware.

This was average across all industry verticals.



Percentage of Organizations Hit by Ransomware In the Last Year

In the last year, has your organization been hit by ransomware? (n=5,600): Yes

Image source: Sophos

Sophos: State of Ransomware 2022, Part 3

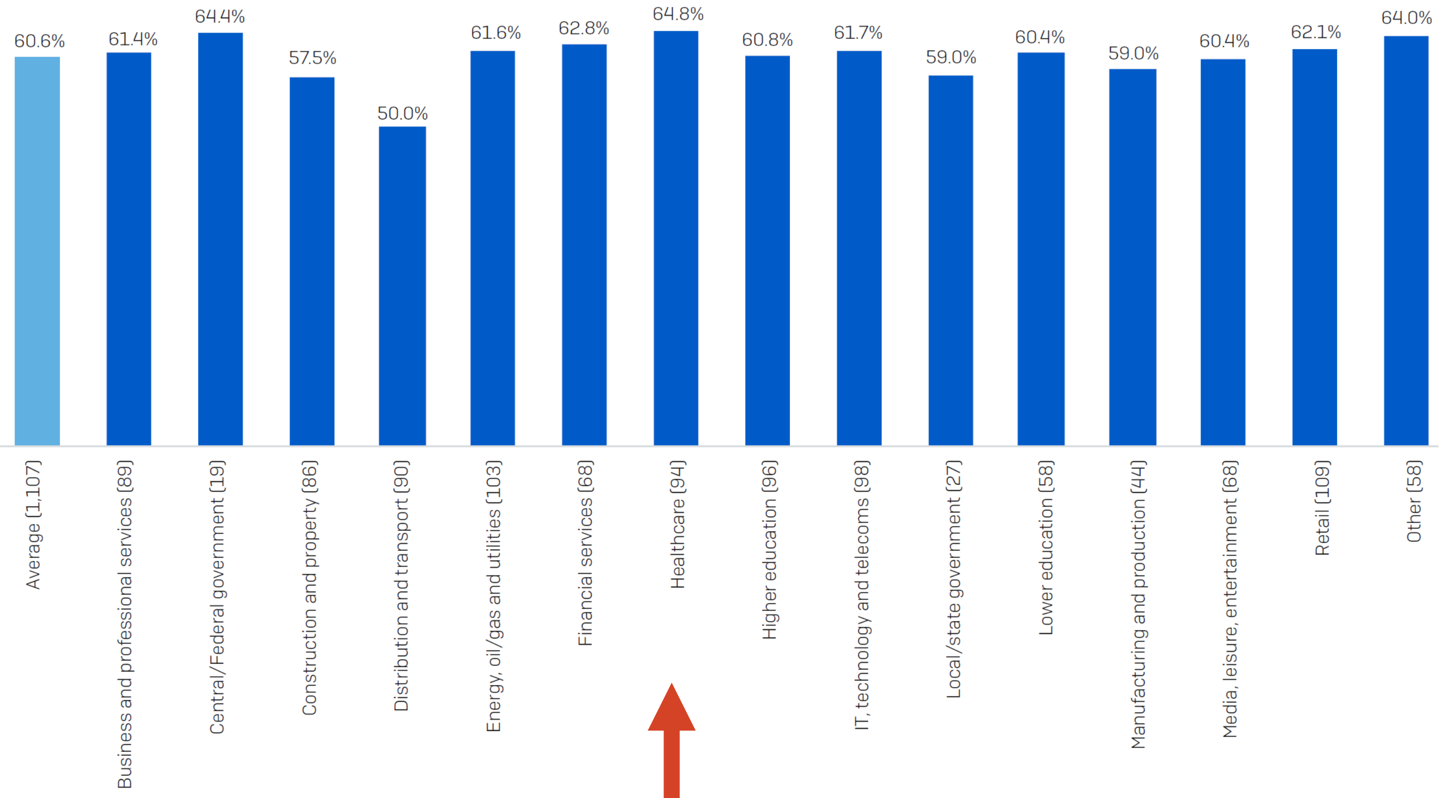
An average of 64.8% of healthcare data was restored after paying the ransom.

This is above the average of 60.6% across all industry verticals.

With regards to ransomware:

- Prevention is significantly optimal.
- Paying ransom does not guarantee all data will be returned.

Percentage of Data Restored After Paying Ransom



How much of your organization's data did you get back in the most significant ransomware attack?
(n=1,107 organizations that paid the ransom and got data back)

Image source: Sophos

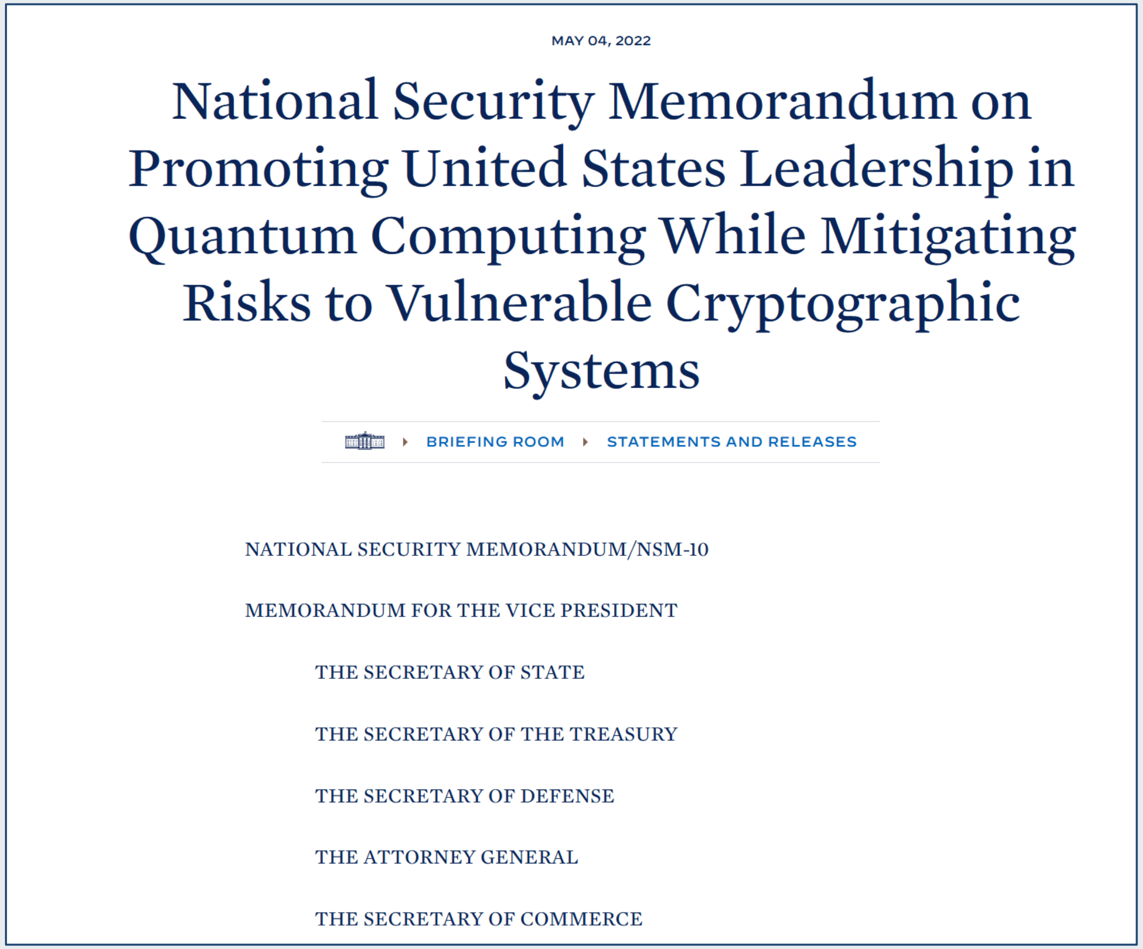
Government Acts on Crypto and Quantum Computing

Securities and Exchange Commission expands Crypto Assets and Cyber Unit:

- Added 20 positions to the unit, which will have 50 dedicated positions after it is fully staffed.
- They assist in collaborating across the federal government in tracking fraud related to ransomware, cryptocurrencies, decentralized finance, NFTs and stablecoins.

White House released a National Security Memorandum on Quantum Computing:

- Requires federal agencies to implement risk mitigation measures to mitigate the risk associated with quantum cryptography.
- Some of those risks are threats to SCADA and ICS systems, which impact healthcare.



MAY 04, 2022

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

NATIONAL SECURITY MEMORANDUM/NSM-10

MEMORANDUM FOR THE VICE PRESIDENT

THE SECRETARY OF STATE

THE SECRETARY OF THE TREASURY

THE SECRETARY OF DEFENSE

THE ATTORNEY GENERAL

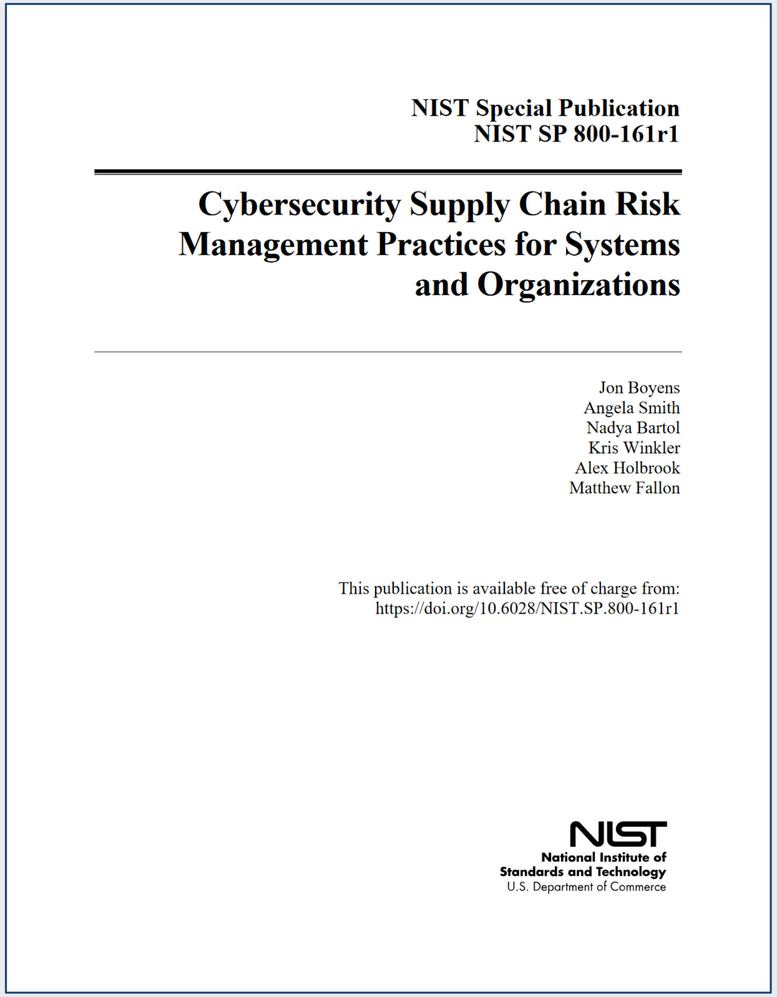
THE SECRETARY OF COMMERCE

Rewards for Justice: Conti & New NIST Publication

The U.S. State Department Rewards for Justice program announced a $10 million bounty for information leading to the identification or location of the Conti ransomware operators. They are also offering $5 million for information that leads to the arrest of a member.

- According to their numbers, the Conti gang has been responsible for successfully targeting over 1000 victim organizations and extorting a total of $150M dollars, making Conti the costliest ransomware gang ever documented.

NIST released a revision of their cybersecurity supply chain risk management publication: SP 800-161 Revision 1.



NIST Special Publication
NIST SP 800-161r1

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Jon Boyens
Angela Smith
Nadya Bartol
Kris Winkler
Alex Holbrook
Matthew Fallon

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-161r1

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Microsoft and Mozilla Research

Microsoft released a report, Special Report: Ukraine.

- They have observed six Russia-attributed APTs launch over 237 cyber operations against Ukraine, including destructive attacks using wipers.
- Russia appeared to be pre-positioning cyber assets for this conflict almost a year early.

Mozilla analyzed mental health and prayer apps:

- They examined 32 applications and labeled 28 of them with a “Privacy not included” warning.
- They noted that many of the companies are non-responsive when they reached out to them.
- There were only two apps which they considered trustworthy.

> “The vast majority of mental health and prayer apps are exceptionally creepy. They track, share, and capitalize on users’ most intimate personal thoughts and feelings.”
>
> – Jen Caltrider, Mozilla

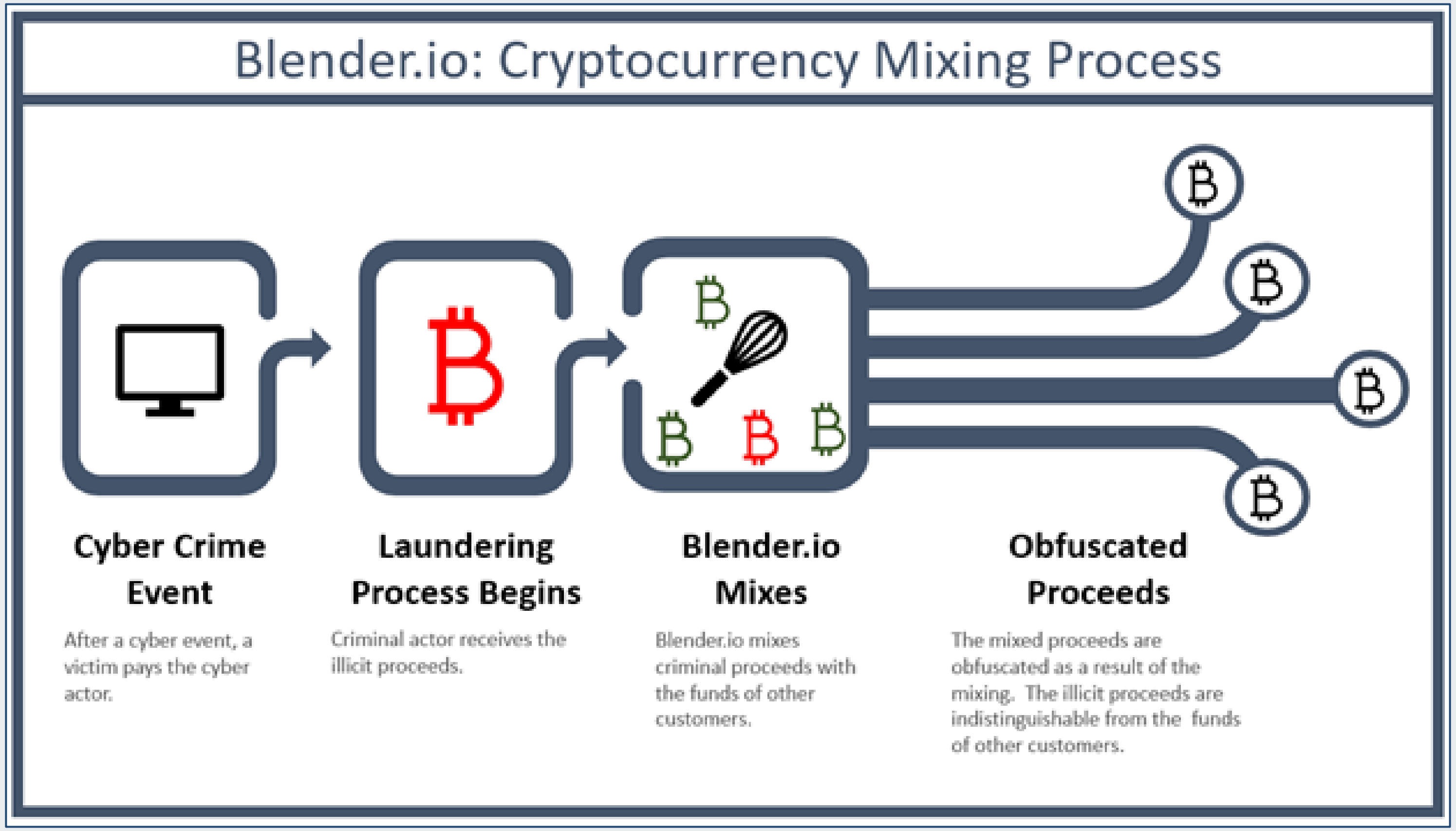
Treasury Sanctions Blender.io

The Department of Treasury sanctioned cryptocurrency mixer Blender.io.

The mixer was used by the North Korea-backed Lazarus hacking group to launder stolen cryptocurrency.

According to the Treasury, Lazarus used Blender.io to launder over $20.5 million of the illicit proceeds.

These same laundering techniques are also used by cybercriminals, especially ransomware operators.



Blender.io: Cryptocurrency Mixing Process

Cyber Crime Event

After a cyber event, a victim pays the cyber actor.

Laundering Process Begins

Criminal actor receives the illicit proceeds.

Blender.io Mixes

Blender.io mixes criminal proceeds with the funds of other customers.

Obfuscated Proceeds

The mixed proceeds are obfuscated as a result of the mixing. The illicit proceeds are indistinguishable from the funds of other customers.

Image source: Treasury Department

Food and Drug Amendments of 2022

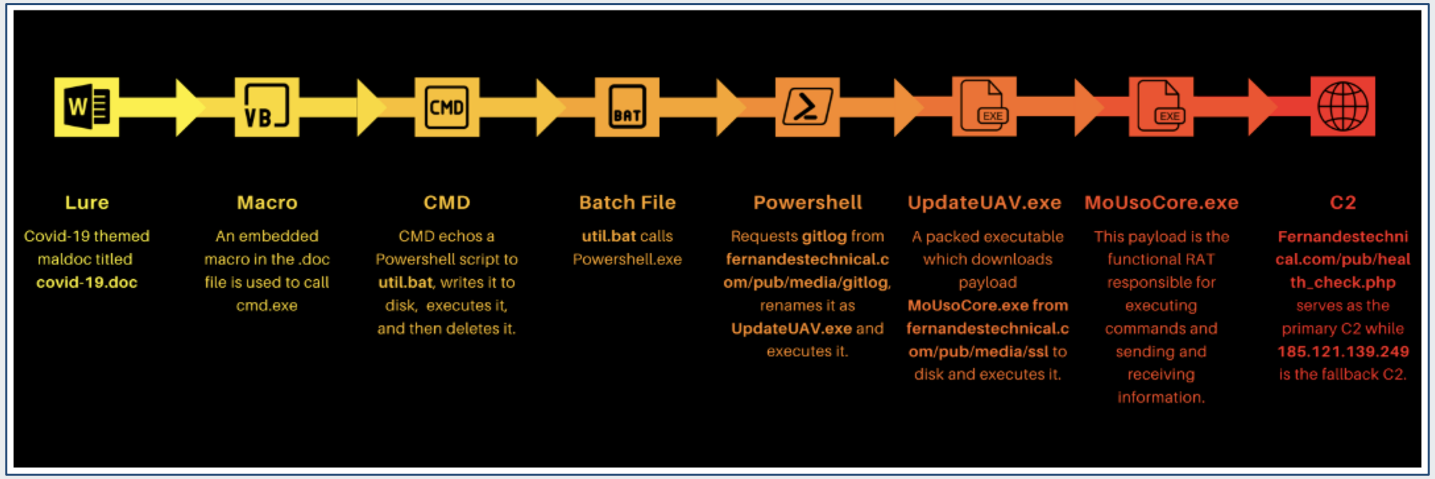
Representative Anna Eshoo (D-CA) proposed the bill, and Representatives Brett Guthrie (R-KY), Frank Pallone (D-NJ), and Cathy McMorris Rogers (R-WA) co-sponsored it.

- Formally titled: H.R. 7667 Food and Drug Amendments of 2022
  - Passed by the House of Representatives on June 8, 2022
  - Last action: Received by the Senate on June 9, 2022
- Has many non-cybersecurity components but also includes provisions to address medical device cybersecurity - SEC. 524C, ensuring cybersecurity of devices.
  - Specifically, calls for medical device manufacturers to monitor, identify, and address post-market cybersecurity vulnerabilities in their devices.
    - “The manufacturer shall design, develop, and maintain processes and procedures to ensure the device and related systems are cybersecure, and shall make available updates and patches to the cyber device and related systems throughout the lifecycle of the cyber device.”
    - “The manufacturer shall provide in the labeling of the cyber device a software bill of materials, including commercial, open-source, and off-the-shelf software components.”

Proofpoint: Nerbian RAT

Proofpoint discovered a new remote access trojan (RAT) called Nerbian.

- It is a 64-bit cross-platform malware variant written in Go, and it has some noteworthy anti-detection capabilities.
- It looks for certain MAC addresses; it examines WMI strings to determine if disk names are legitimate; it looks for smaller hard drives, indicative of a virtualized environment (sandbox); it examines running processes for memory analysis or tampering detection programs.



Lure

Covid-19 themed maldoc titled **covid-19.doc**

Macro

An embedded macro in the .doc file is used to call cmd.exe

CMD

CMD echos a Powershell script to **util.bat**, writes it to disk, executes it, and then deletes it.

Batch File

util.bat calls Powershell.exe

Powershell

Requests **gitlog** from **fernandestechnical.com/pub/media/gitlog**, renames it as **UpdateUAV.exe** and executes it.

UpdateUAV.exe

A packed executable which downloads payload **MoUsoCore.exe from fernandestechnical.com/pub/media/ssl** to disk and executes it.

MoUsoCore.exe

This payload is the functional RAT responsible for executing commands and sending and receiving information.

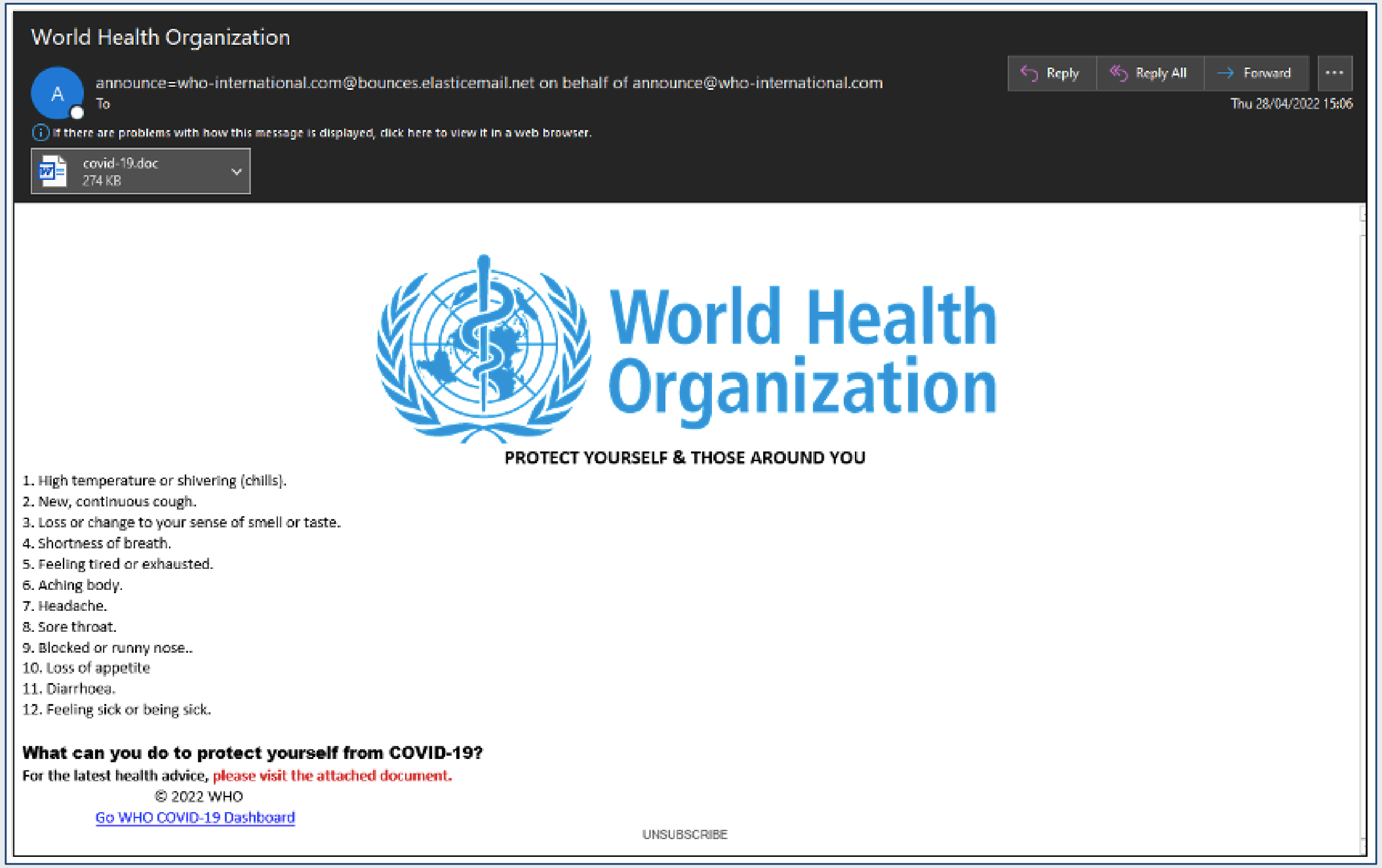
C2

Fernandestechnical.com/pub/health_check.php serves as the primary C2 while **185.121.139.249** is the fallback C2.

Image source: Proofpoint

Proofpoint: Nerbian RAT, Part 2

Nerbian is being dropped in smaller phishing campaigns. It impersonates the World Health Organization and purports to be sending COVID-19 information to the targets.



World Health Organization

announce=who-international.com@bounces.elasticemail.net on behalf of announce@who-international.com

To

Thu 28/04/2022 15:06

If there are problems with how this message is displayed, click here to view it in a web browser.

covid-19.doc
274 KB

PROTECT YOURSELF & THOSE AROUND YOU

1. High temperature or shivering (chills).
2. New, continuous cough.
3. Loss or change to your sense of smell or taste.
4. Shortness of breath.
5. Feeling tired or exhausted.
6. Aching body.
7. Headache.
8. Sore throat.
9. Blocked or runny nose..
10. Loss of appetite
11. Diarrhoea.
12. Feeling sick or being sick.

What can you do to protect yourself from COVID-19?

For the latest health advice, please visit the attached document.

© 2022 WHO

Go WHO COVID-19 Dashboard

UNSUBSCRIBE

Image source: Proofpoint

DOJ Charges Venezuelan Doctor with Ransomware

The Department of Justice announced charges against a Venezuelan doctor – Moises Luis Zagala Gonzalez – with operating ransomware in his free time.

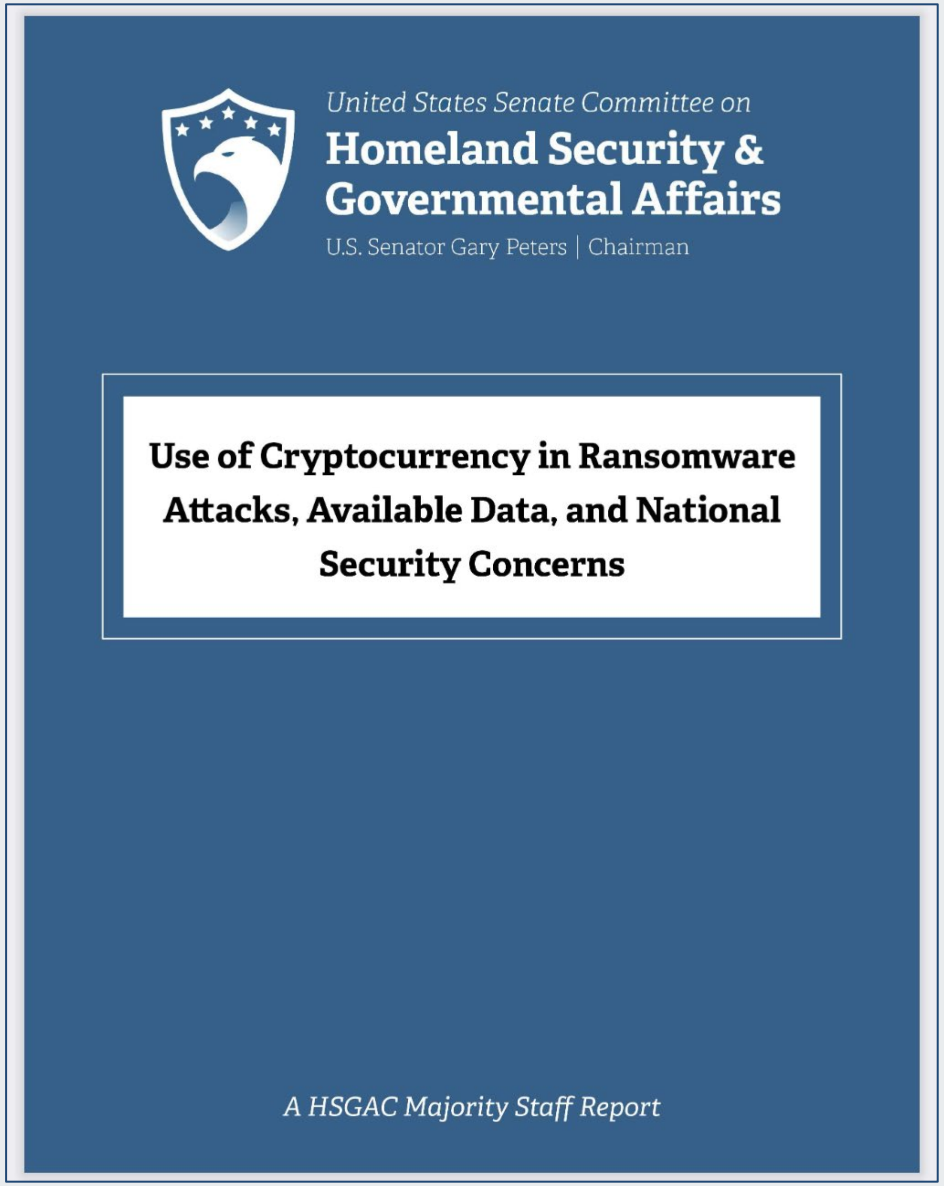
- Gonzalez is a full-time medical doctor who treated patients regularly and is alleged to operate both the Jigsaw and Thanos ransomware variants.
- He is accused of building and maintaining the code, identifying partners on the dark web, training them and operating both variants as ransomware-as-a-service.
- He is facing up to five years in prison for attempted computer intrusion and five years of in prison for conspiracy to commit computer intrusions.

Image source: FBI

Congressional Report: Use of Cryptography in Ransomware Attacks, Available Data and National Security Concerns

U.S. Senator Gary Peters (D-MI), Chairman of the U.S. Senate Committee on Homeland Security & Governmental Affairs, released the report:

- U.S. federal agencies only capture a fraction of the cybercrime threat.
- There is a lack of reliable data on ransomware attacks and ransom payments.
- Currently available data on ransomware attacks and cryptocurrency payments limit private sector and federal government efforts to assist cybercrime victims.



United States Senate Committee on

Homeland Security & Governmental Affairs

U.S. Senator Gary Peters | Chairman

Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns

A HSGAC Majority Staff Report

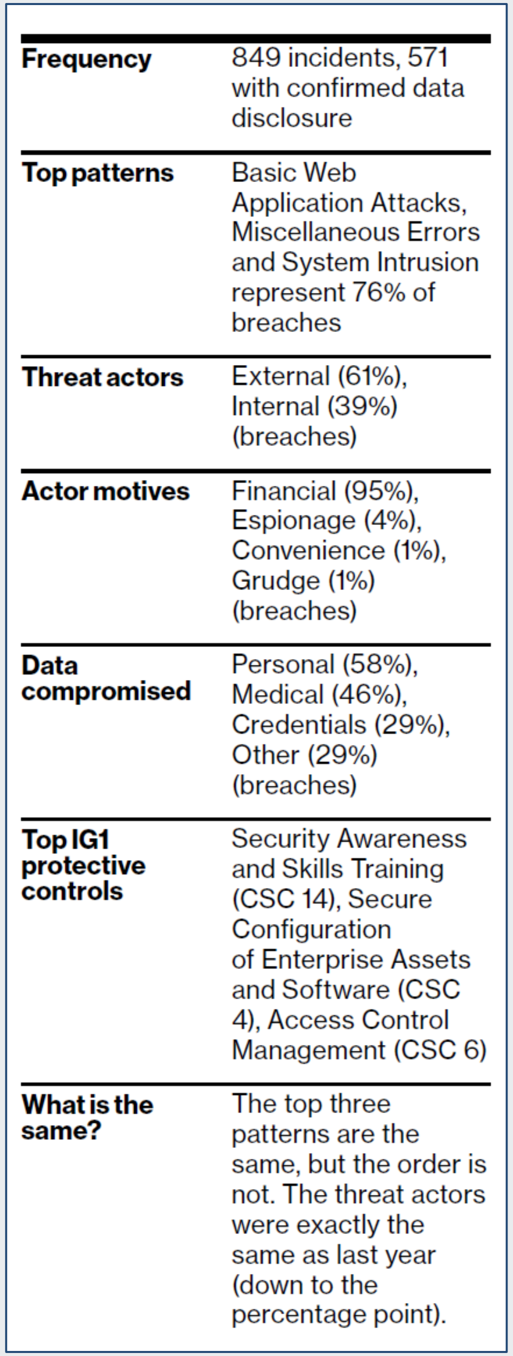
Image source: House of Representatives

2022 Verizon Data Breach Investigation Report

Verizon released its 2022 Data Breach Investigation report:

- Verizon analyzed ~24K security incidents, including over 5,000 data breaches across sectors.
- Healthcare accounted for just under 1,000 of the reported security incidents, over 500 of which had confirmed data disclosures.
- Further healthcare-specific data on the chart to the right.

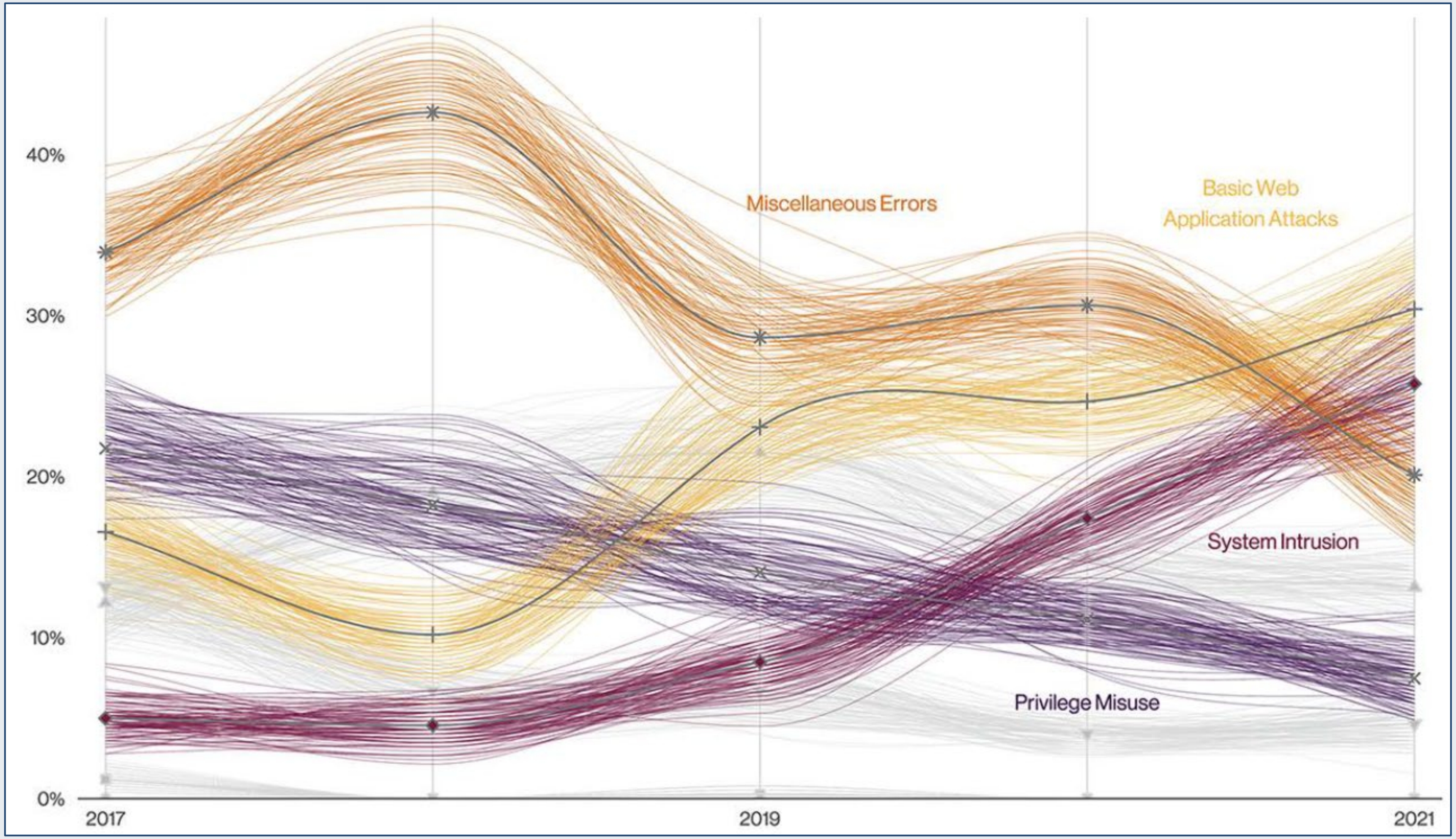
The original report can be found here.



Frequency	849 incidents, 571 with confirmed data disclosure
Top patterns	Basic Web Application Attacks, Miscellaneous Errors and System Intrusion represent 76% of breaches
Threat actors	External (61%), Internal (39%) (breaches)
Actor motives	Financial (95%), Espionage (4%), Convenience (1%), Grudge (1%) (breaches)
Data compromised	Personal (58%), Medical (46%), Credentials (29%), Other (29%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Secure Configuration of Enterprise Assets and Software (CSC 4), Access Control Management (CSC 6)
What is the same?	The top three patterns are the same, but the order is not. The threat actors were exactly the same as last year (down to the percentage point).

Image source: Verizon

Image source: Verizon



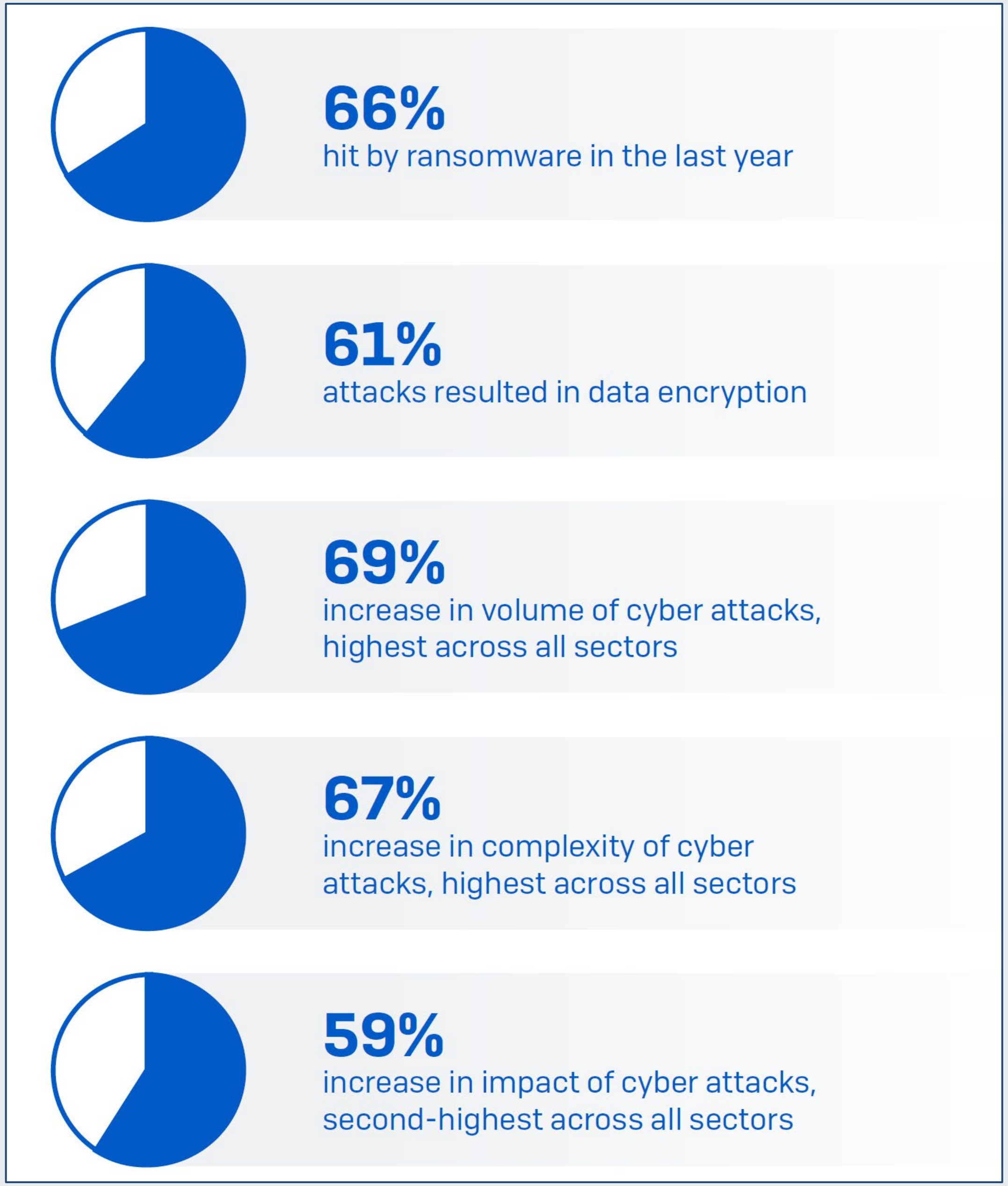
2022 Verizon Data Breach Report: Patterns over time in healthcare industry breaches

Sophos: State of Ransomware in Healthcare 2022

Sophos released their State of Ransomware in Healthcare Report 2022 report.

Healthcare continued to be heavily targeted.

The original report can be found here.



66%
hit by ransomware in the last year

61%
attacks resulted in data encryption

69%
increase in volume of cyber attacks, highest across all sectors

67%
increase in complexity of cyber attacks, highest across all sectors

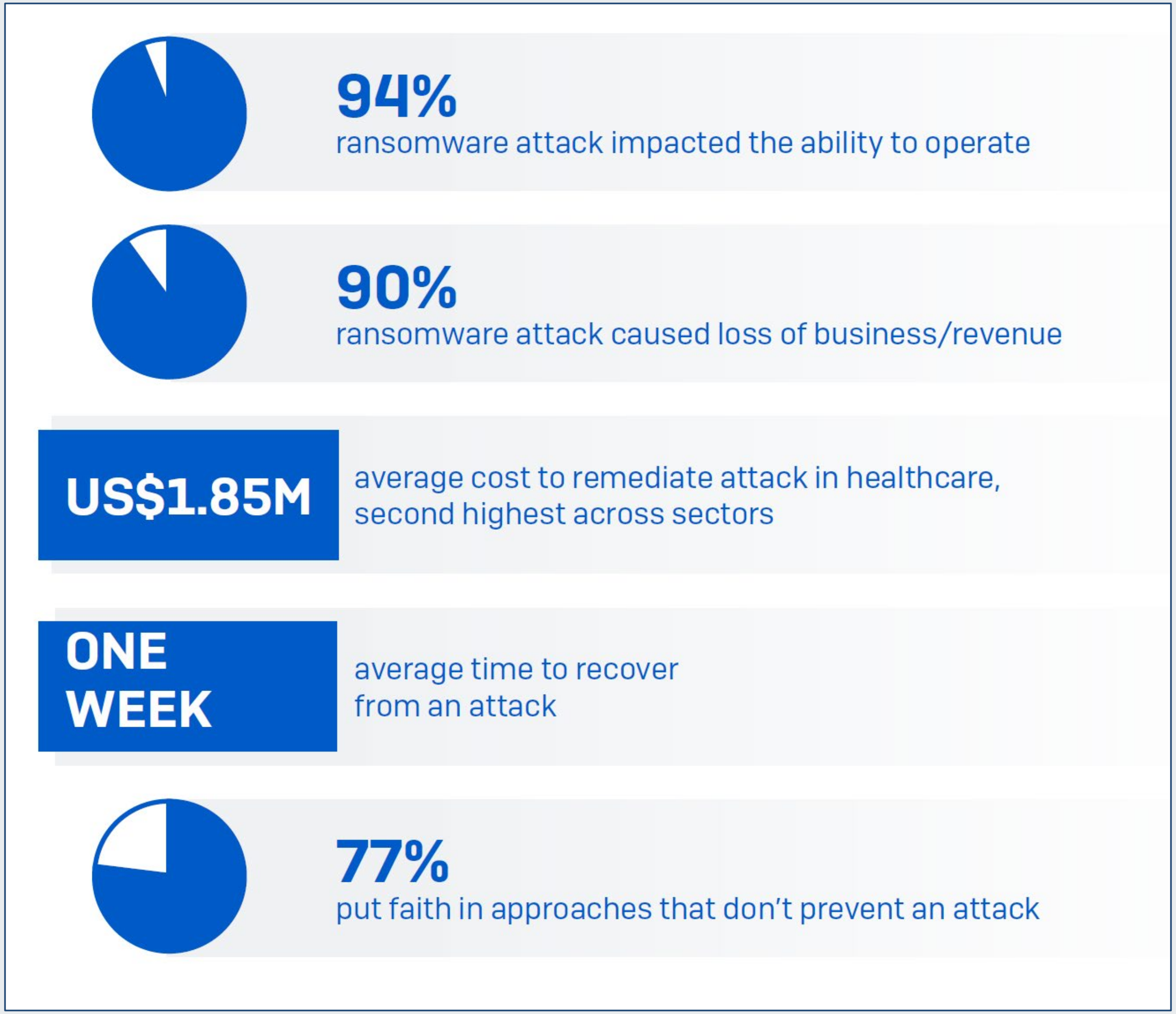
59%
increase in impact of cyber attacks, second-highest across all sectors

Image source: Sophos

Sophos: State of Ransomware in Healthcare 2022, Part 2

The impact of ransomware attacks are particularly egregious on the health sector.

Impacts on the ability to operate and general downtime can be impactful to patient outcomes.



94%
ransomware attack impacted the ability to operate

90%
ransomware attack caused loss of business/revenue

US$1.85M
average cost to remediate attack in healthcare, second highest across sectors

ONE WEEK
average time to recover from an attack

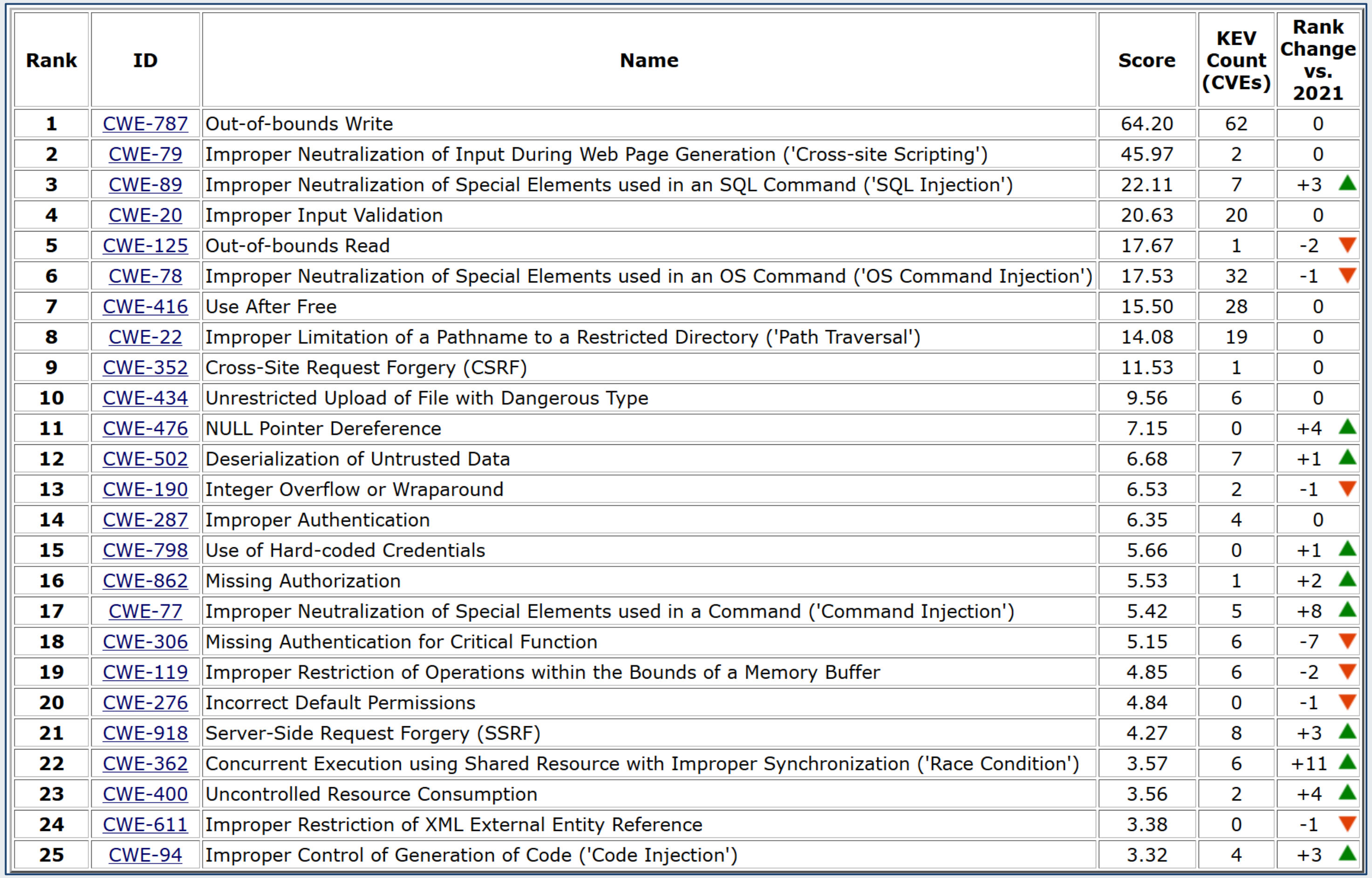
77%
put faith in approaches that don't prevent an attack

Image source: Sophos

2022 CWE Top 25 Most Dangerous Software Weaknesses

MITRE released their top 25 most common and dangerous software weaknesses, which covers the last 48 months.

A lot of these made the list because they are easy for adversaries to discover.



Rank	ID	Name	Score	KEV Count (CVEs)	Rank Change vs. 2021
1	CWE-787	Out-of-bounds Write	64.20	62	0
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.97	2	0
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22.11	7	+3 ▲
4	CWE-20	Improper Input Validation	20.63	20	0
5	CWE-125	Out-of-bounds Read	17.67	1	-2 ▼
6	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17.53	32	-1 ▼
7	CWE-416	Use After Free	15.50	28	0
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.08	19	0
9	CWE-352	Cross-Site Request Forgery (CSRF)	11.53	1	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type	9.56	6	0
11	CWE-476	NULL Pointer Dereference	7.15	0	+4 ▲
12	CWE-502	Deserialization of Untrusted Data	6.68	7	+1 ▲
13	CWE-190	Integer Overflow or Wraparound	6.53	2	-1 ▼
14	CWE-287	Improper Authentication	6.35	4	0
15	CWE-798	Use of Hard-coded Credentials	5.66	0	+1 ▲
16	CWE-862	Missing Authorization	5.53	1	+2 ▲
17	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	5.42	5	+8 ▲
18	CWE-306	Missing Authentication for Critical Function	5.15	6	-7 ▼
19	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	4.85	6	-2 ▼
20	CWE-276	Incorrect Default Permissions	4.84	0	-1 ▼
21	CWE-918	Server-Side Request Forgery (SSRF)	4.27	8	+3 ▲
22	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	3.57	6	+11 ▲
23	CWE-400	Uncontrolled Resource Consumption	3.56	2	+4 ▲
24	CWE-611	Improper Restriction of XML External Entity Reference	3.38	0	-1 ▼
25	CWE-94	Improper Control of Generation of Code ('Code Injection')	3.32	4	+3 ▲

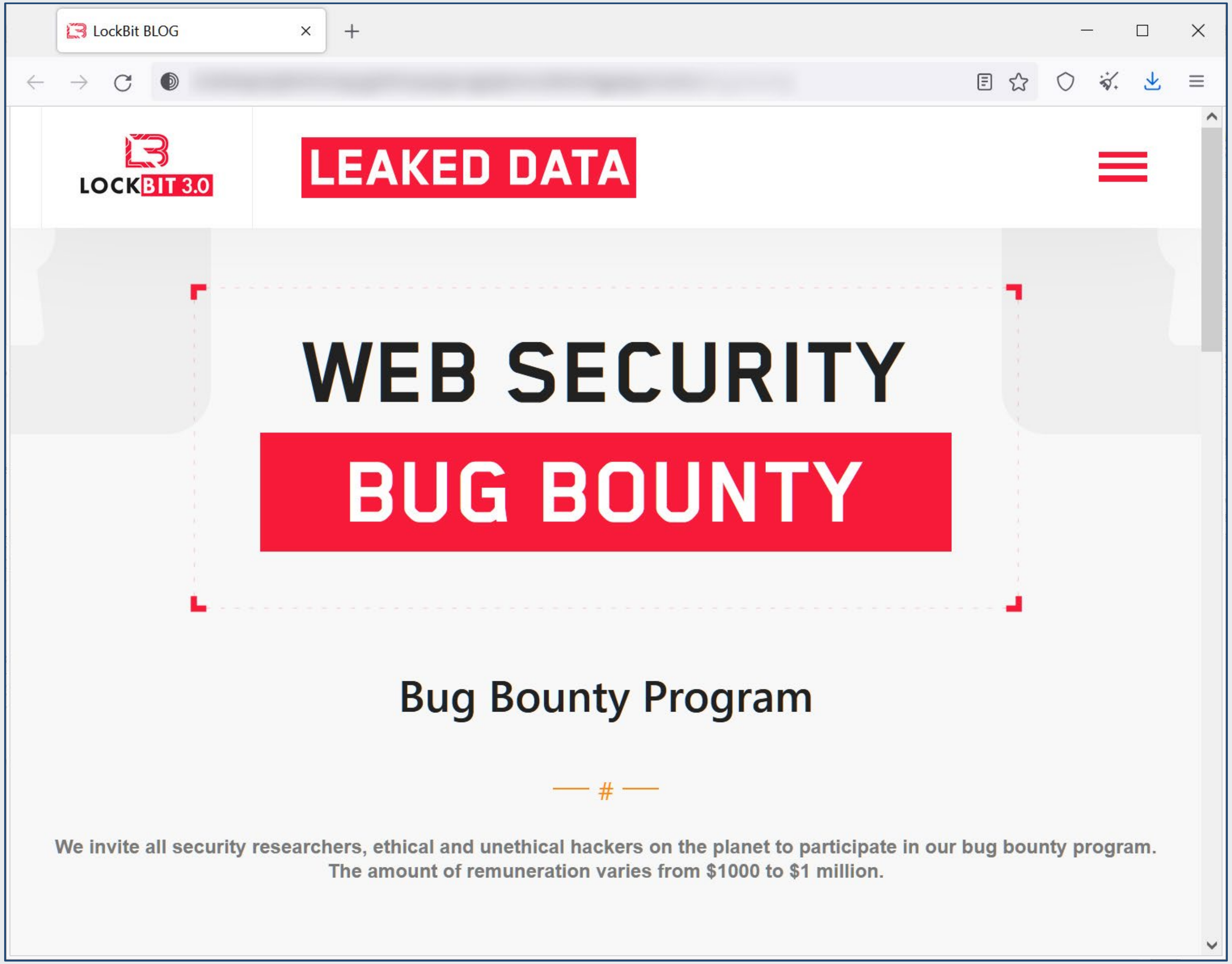
Image source: MITRE

LockBit Bug Bounty Program

LockBit introduced the first ransomware bug bounty program.

Rewards range from $1,000 to $1M.

Payments made in Bitcoin, Monero and Zcash.



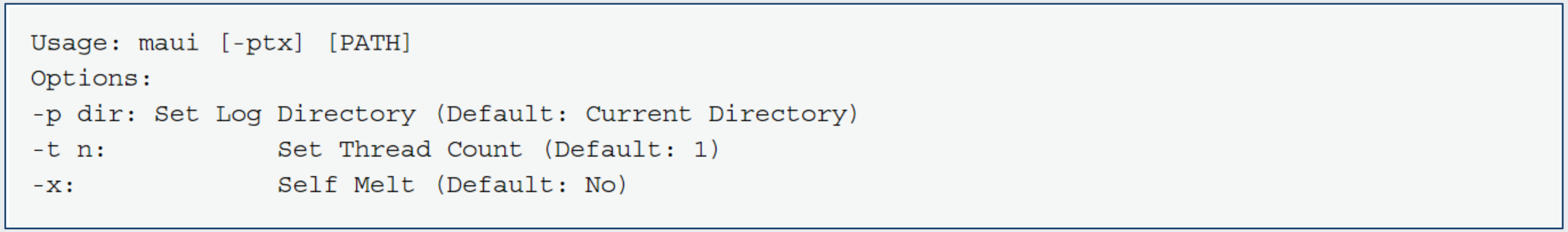
Bug Bounty Program

We invite all security researchers, ethical and unethical hackers on the planet to participate in our bug bounty program. The amount of remuneration varies from $1000 to $1 million.

Image source: Bleeping Computer

Maui Ransomware vs. the Health Sector

- CISA released Alert (AA22-187A) North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector.
- The Department of Justice announced that they seized ransoms that were paid to the Maui ransomware operators by two healthcare organizations in 2021.
- Deputy Attorney General Lisa Monaco said the Justice Department seized and returned about $500,000 in cryptocurrency paid by two American medical organizations in ransom fees.
- Stairwell released a threat report on Maui, including an overview of its encryption and key process, a key extractor, YARA rules and indicators of compromise.



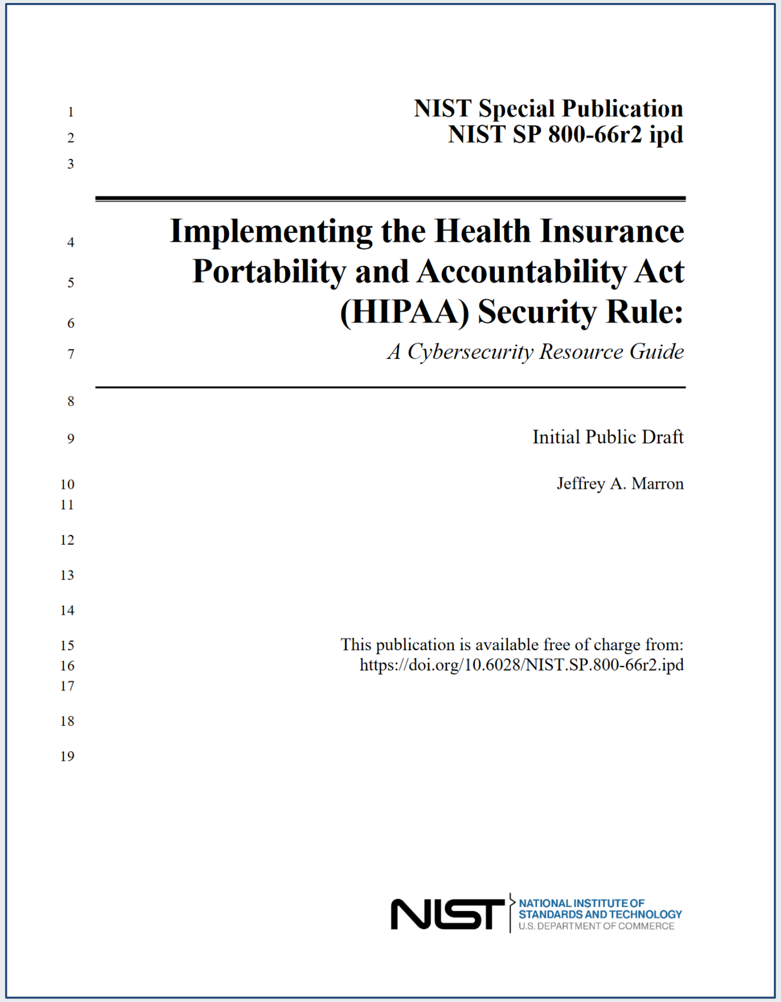
```
Usage: maui [-ptx] [PATH]
Options:
-p dir: Set Log Directory (Default: Current Directory)
-t n:           Set Thread Count (Default: 1)
-x:             Self Melt (Default: No)
```

Image source: Stairwell

NIST: Draft SP 800-66r2: Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide

The National Institutes of Standards and Technology released the draft version of revision 2 of Special Publication 800-66r2: Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide.

- It is designed primarily to help healthcare organizations protect health-related data.
- In this version, they have also integrated their cybersecurity framework and mapped their recommendations to their latest list of security and privacy controls.
- The previous version – revision 1 – was released in 2008.



NIST Special Publication
NIST SP 800-66r2 ipd

Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule:

A Cybersecurity Resource Guide

Initial Public Draft

Jeffrey A. Marron

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-66r2.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Image source: NIST

IBM Cost of a Data Breach Report 2022

IBM released their Cost of a Data Breach 2022 report – one of the more prominent and influential cyber reports released each year.

For the 12th year in a row, the health sector had the highest costs for a data breach.

The average breach in healthcare increased by nearly $1M and is now $10.1M.

Costs have also increased over 40% in the last two years, according to the data.

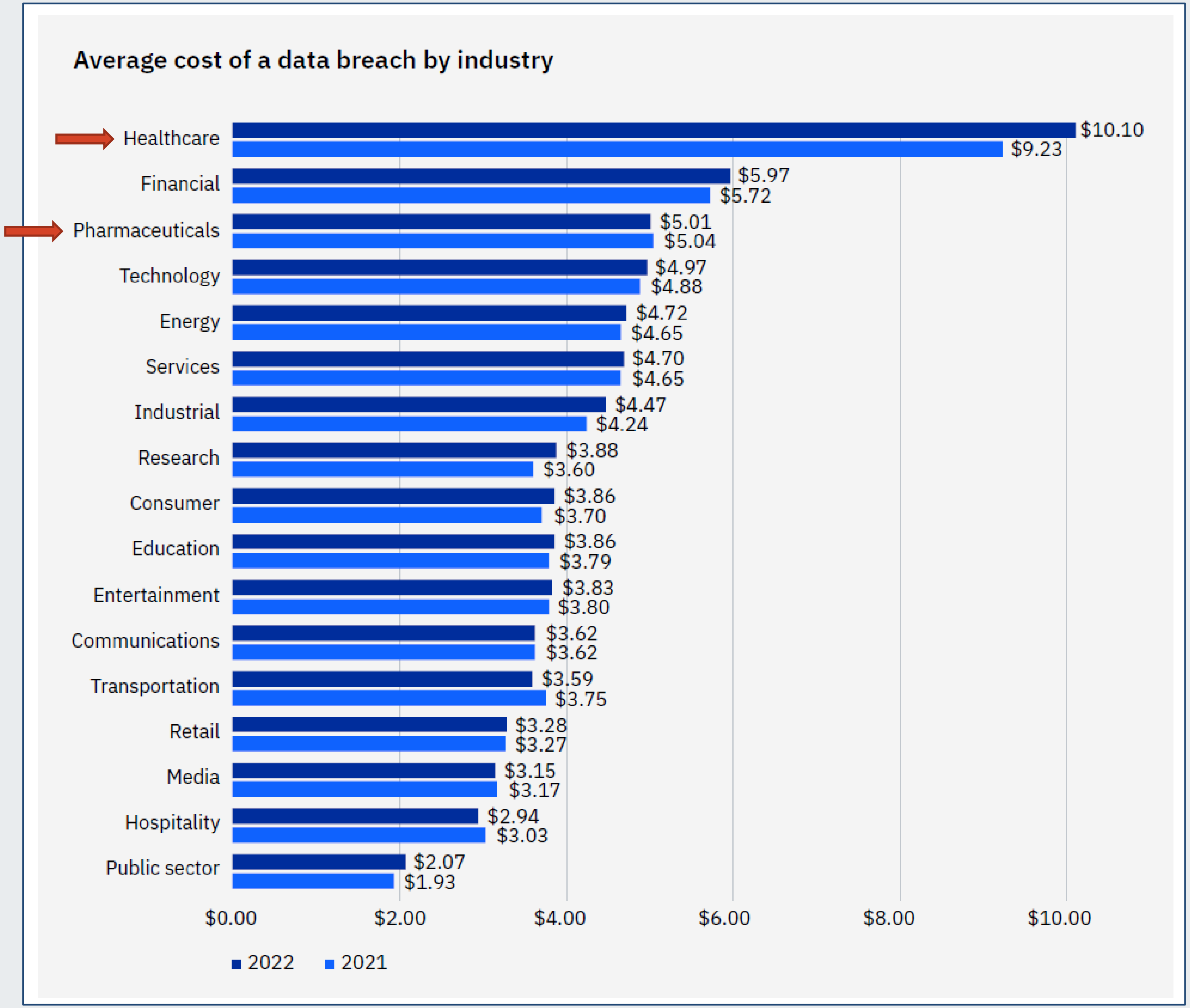


Image source: IBM

Palo Alto: Black Basta Ransomware Analysis

- Researchers at Palo Alto's Unit 42 released an analysis of Black Basta ransomware.
- First discovered in April 2022. (Likely in development since February.)
- Operates as Ransomware-as-a-service.
- Successfully compromised 75 organizations; 20 victims in first two weeks of operation.
- Black Basta is possibly a rebrand of an old group.
- Black Basta has been leveraged in attacks along with Qbot.
- Targets included the U.S., Germany, Switzerland, Italy, France and the Netherlands.

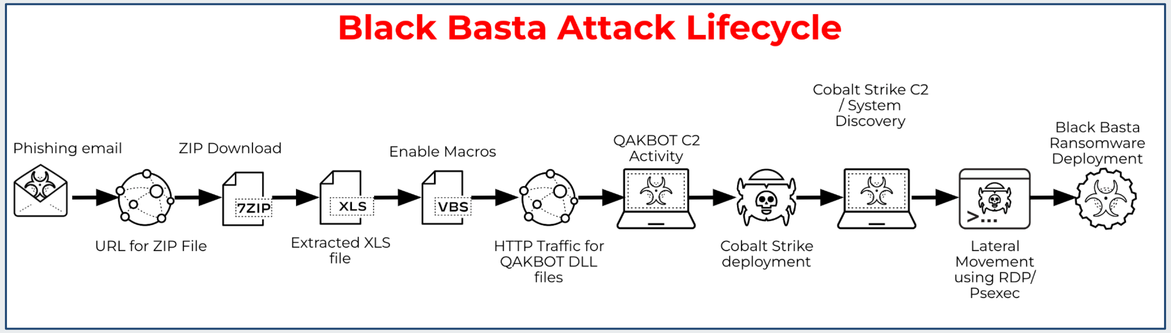

Black Basta Attack Lifecycle
Phishing email
URL for ZIP File
ZIP Download
7ZIP
Extracted XLS file
XLS
Enable Macros
VBS
HTTP Traffic for QAKBOT DLL files
QAKBOT C2 Activity
Cobalt Strike deployment
Cobalt Strike C2 / System Discovery
Lateral Movement using RDP/ Psexec
Black Basta Ransomware Deployment

Image source: Palo Alto

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

FBI: Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities

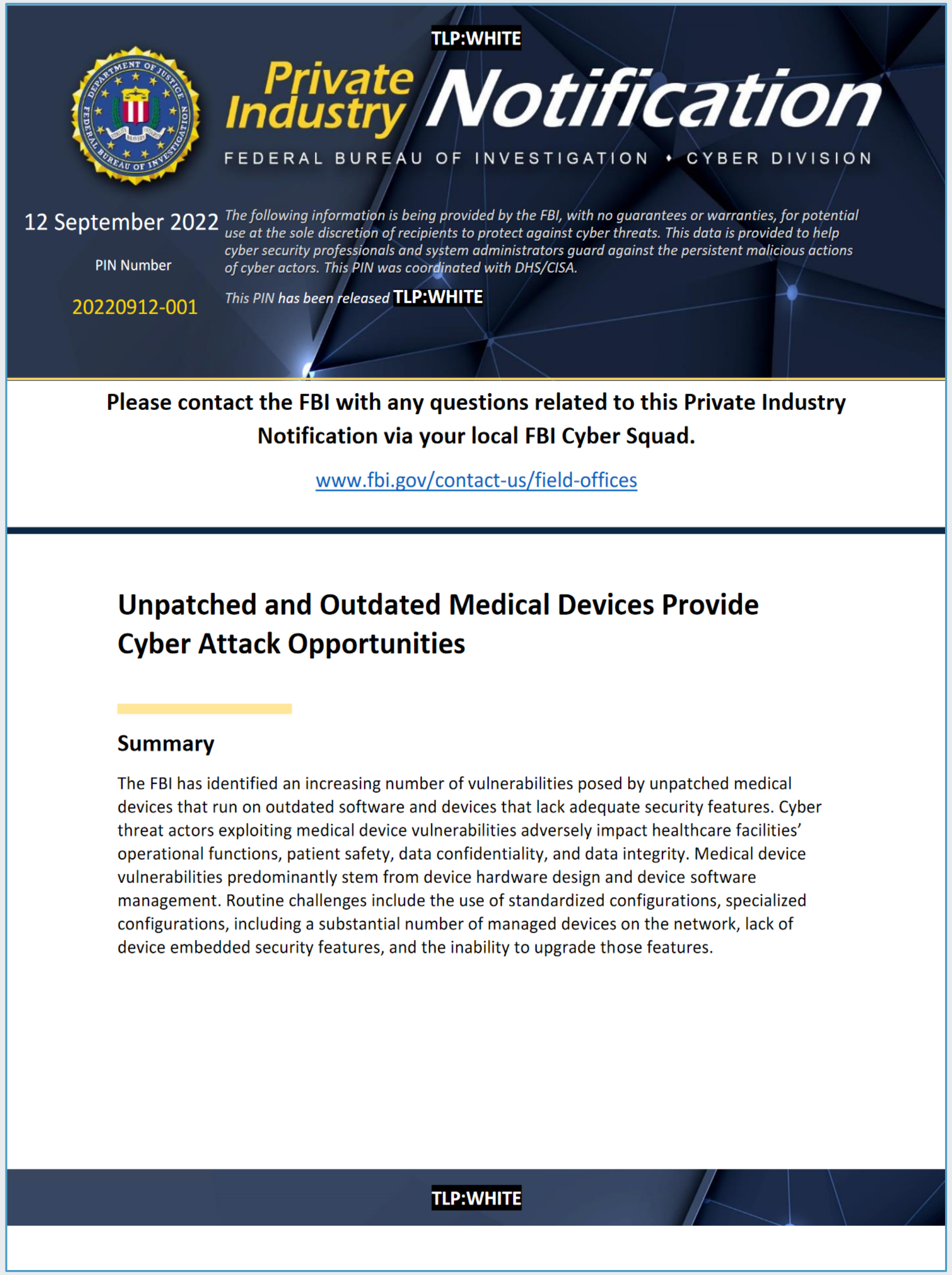
The FBI Internet Crime Complaint Center released a private industry notification titled: *Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities.*

They noted the prevalence of medical device vulnerabilities.

Proposed security recommendations:

- Endpoint protection
- Identity and access management
- Asset management
- Vulnerability management
- Training

The original report can be found here.



TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

12 September 2022

PIN Number

20220912-001

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS/CISA.

This PIN has been released **TLP:WHITE**

Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.

www.fbi.gov/contact-us/field-offices

Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities

Summary

The FBI has identified an increasing number of vulnerabilities posed by unpatched medical devices that run on outdated software and devices that lack adequate security features. Cyber threat actors exploiting medical device vulnerabilities adversely impact healthcare facilities' operational functions, patient safety, data confidentiality, and data integrity. Medical device vulnerabilities predominantly stem from device hardware design and device software management. Routine challenges include the use of standardized configurations, specialized configurations, including a substantial number of managed devices on the network, lack of device embedded security features, and the inability to upgrade those features.

TLP:WHITE

Image source: FBI

AdvIntel: Emotet Persists

- Advanced Intel recently released research showing that the Emotet operators are back in full force.
- Emotet returned to highly operational in the spring of 2022, took a break for a few months, and returned to operations again in the summer.
- They observed almost 1.3M instances of Emotet infections worldwide since the beginning of 2022.
- They have seen Emotet being used to drop both Quantum and Black Cat ransomware since June.

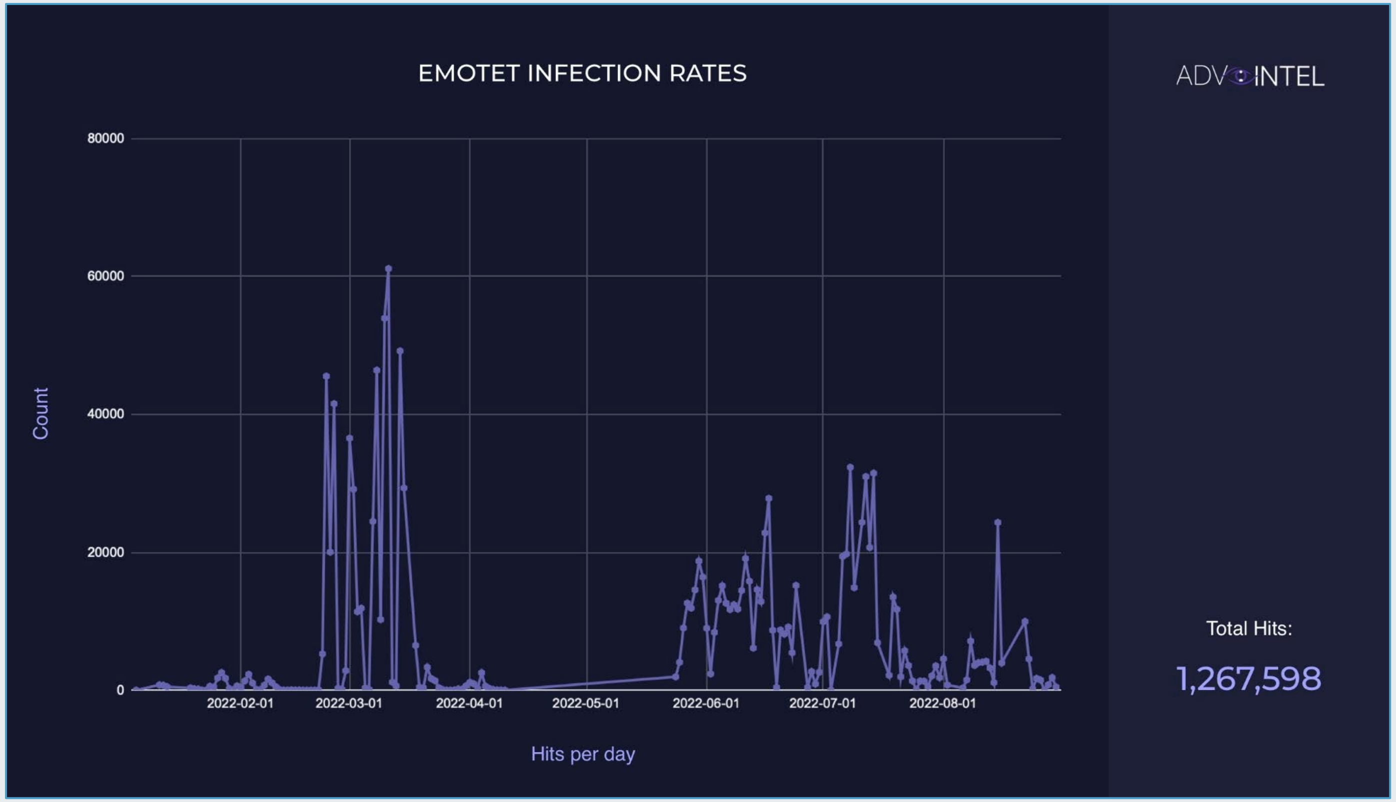


Image source: AdvIntel

Securing Open Source Software Act

Senators Gary Peters (D-MI) and Rob Portman (R-OH) introduced S4913, the Securing Open Source Software Act.

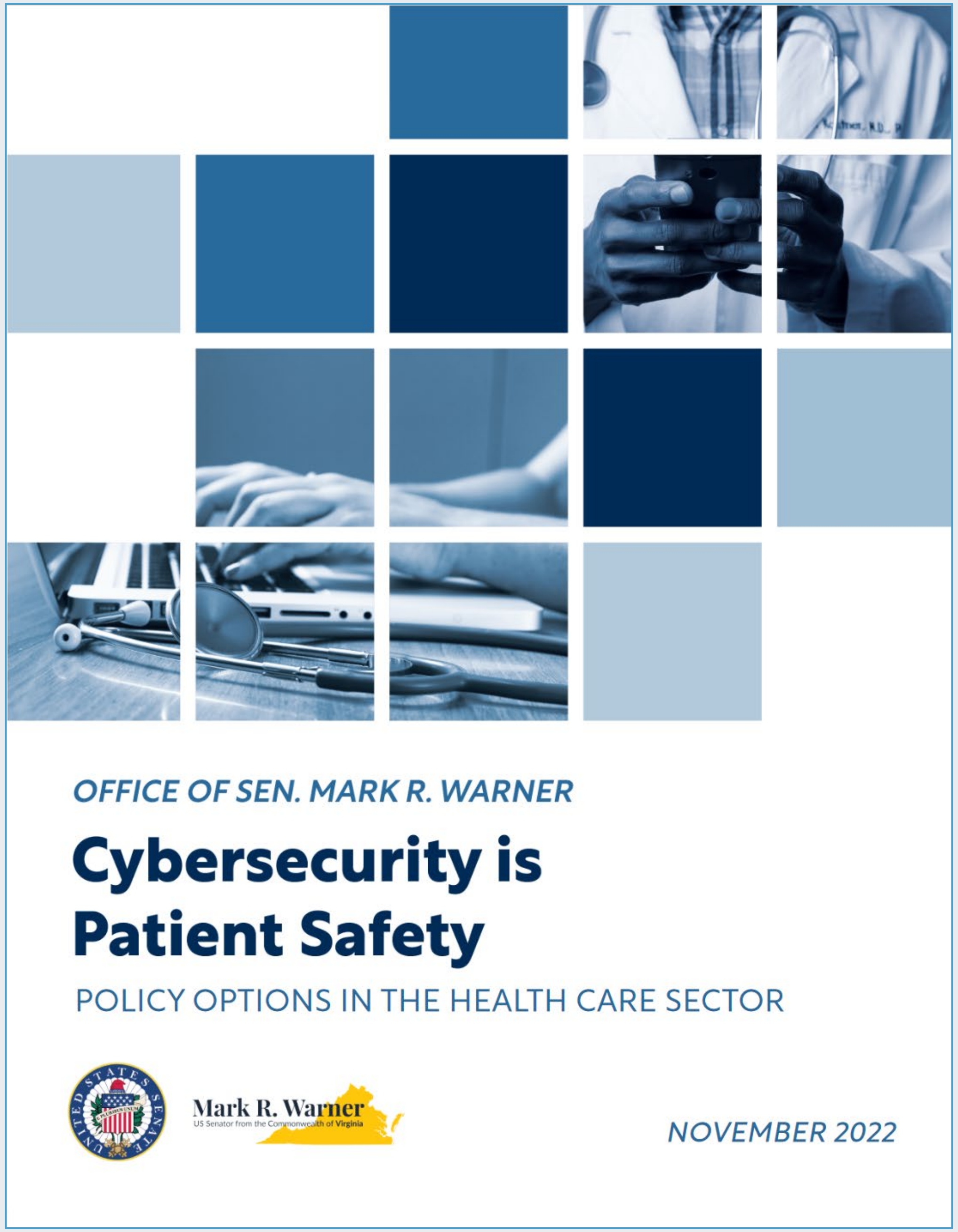
- The bill was intended to address security risks of open source software in government and critical infrastructure.
- If passed in its current form:
  - It will require CISA to develop a risk framework for open source software for government and critical infrastructure.
  - A software security subcommittee would be created within CISA's Cybersecurity Advisory Committee.
- Both Senators identified the Log4J vulnerabilities as drivers for the creation of the bill.
- Last action: The bill was reported to the Senate on December 19, 2022.

Senator Mark Warner’s Healthcare Cybersecurity White Paper

Senator Mark Warner (D-VA) released a white paper soliciting input from the private sector and the research community on healthcare cybersecurity issues.

It asks questions about the federal government’s performance, NIST standards, and the effectiveness of he 405(d) program, among other things.

The original report can be found here.



OFFICE OF SEN. MARK R. WARNER

Cybersecurity is Patient Safety

POLICY OPTIONS IN THE HEALTH CARE SECTOR

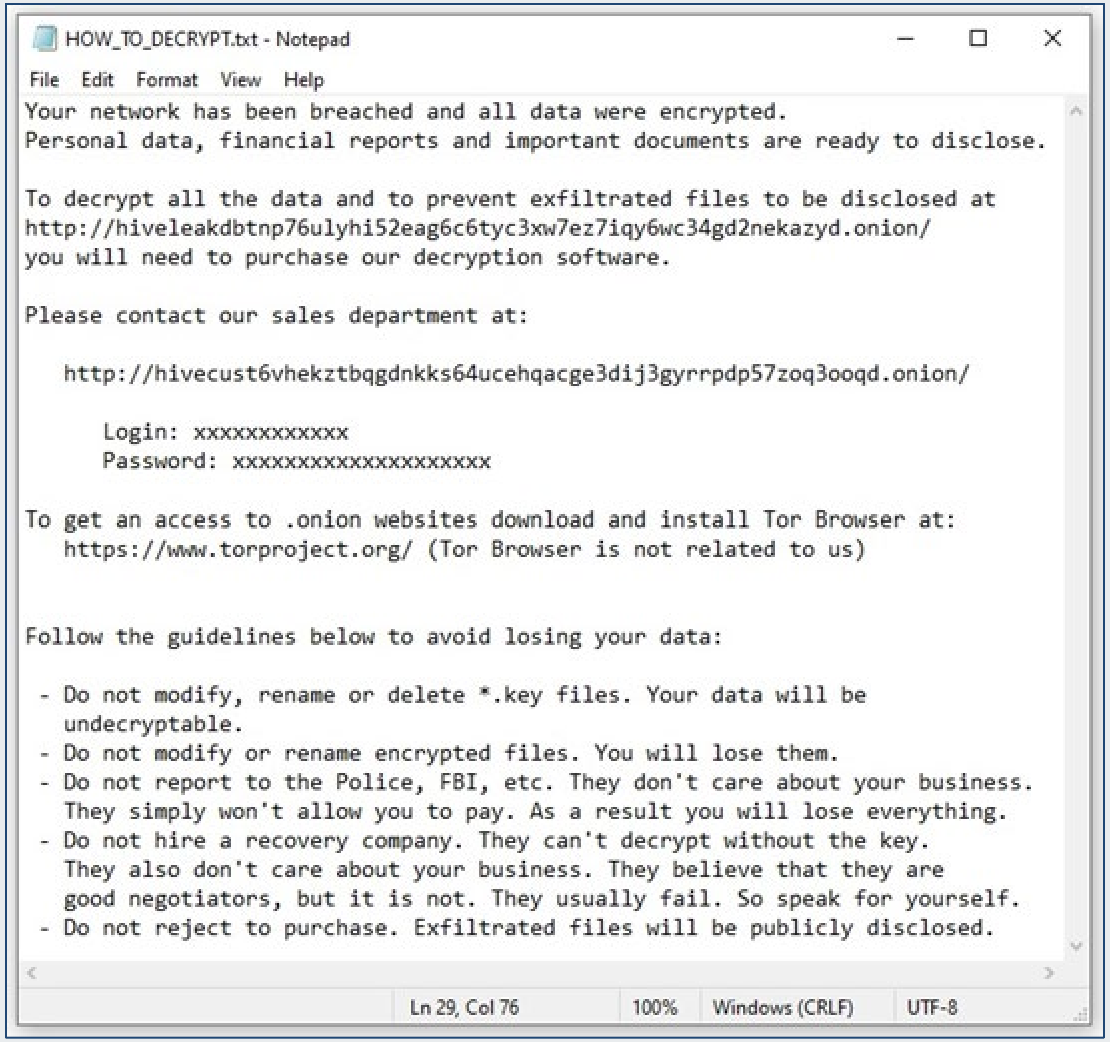
Mark R. Warner
US Senator from the Commonwealth of Virginia

NOVEMBER 2022

Image source: U.S. Senate

CISA/FBI Alert on Hive Ransomware

- CISA and the FBI released a joint alert – (AA22-321A) #StopRansomware: Hive Ransomware
- The alert noted that Hive has compromised over 1,300 organizations and extorted approximately $100M, as of November 2022.
  - This includes government, communications, manufacturing, technology and "especially healthcare."



```
Your network has been breached and all data were encrypted.
Personal data, financial reports and important documents are ready to disclose.

To decrypt all the data and to prevent exfiltrated files to be disclosed at
http://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion/
you will need to purchase our decryption software.

Please contact our sales department at:

   http://hivecust6vhekztbqgdnkks64ucehqacge3dij3gyrrpdp57zoq3ooqd.onion/

      Login: xxxxxxxxxxxx
      Password: xxxxxxxxxxxxxxxxxxxx

To get an access to .onion websites download and install Tor Browser at:
   https://www.torproject.org/ (Tor Browser is not related to us)


Follow the guidelines below to avoid losing your data:

 - Do not modify, rename or delete *.key files. Your data will be
   undecryptable.
 - Do not modify or rename encrypted files. You will lose them.
 - Do not report to the Police, FBI, etc. They don't care about your business.
   They simply won't allow you to pay. As a result you will lose everything.
 - Do not hire a recovery company. They can't decrypt without the key.
   They also don't care about your business. They believe that they are
   good negotiators, but it is not. They usually fail. So speak for yourself.
 - Do not reject to purchase. Exfiltrated files will be publicly disclosed.
```

Image source: CISA

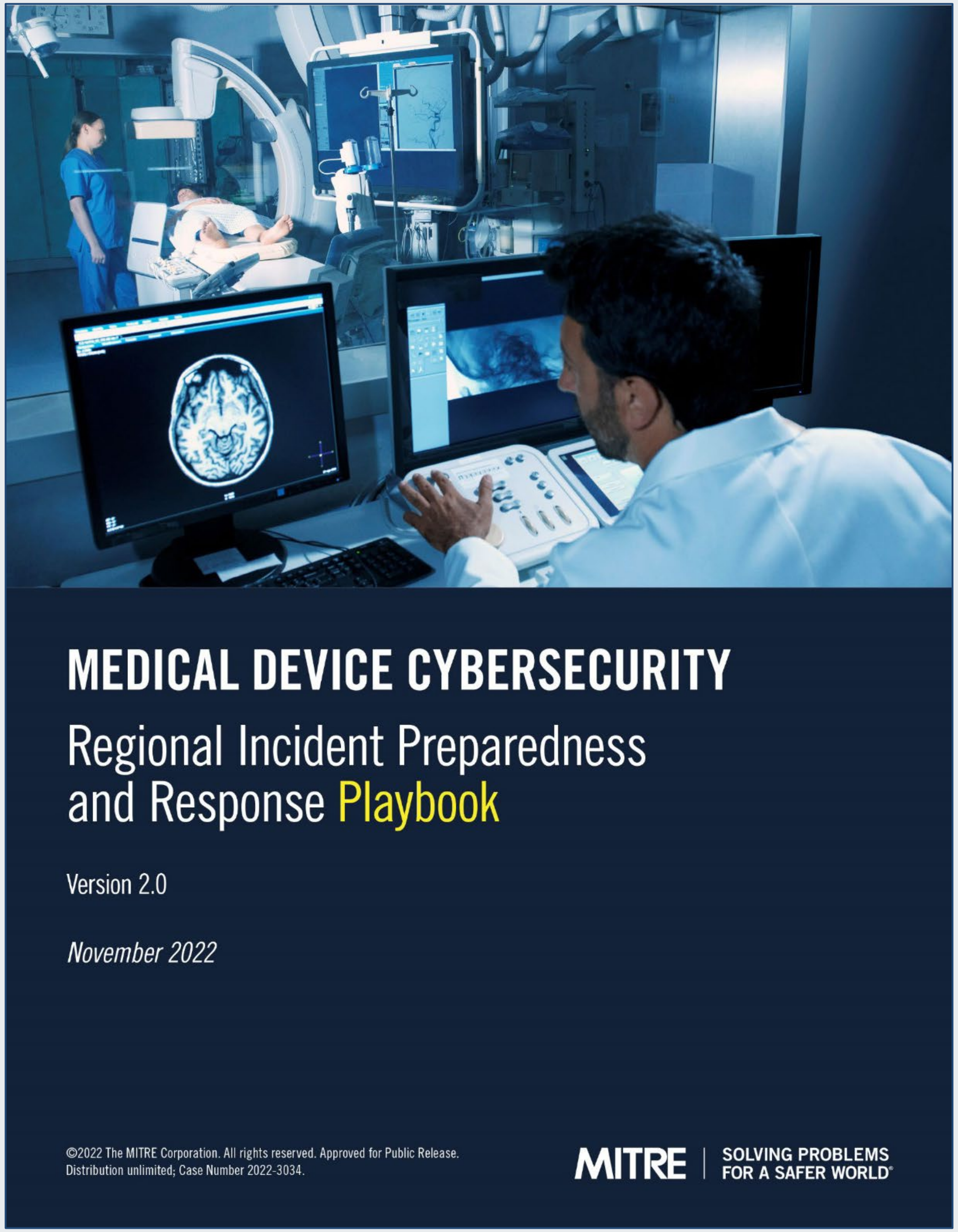
FDA/MITRE: Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook

The FDA and MITRE updated their Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook.

Purpose: To help hospitals and healthcare delivery organizations (HDOs) develop a cybersecurity preparedness and response framework.

The updated playbook can be found here.

The Quick Start Companion Guide can be found here.



MEDICAL DEVICE CYBERSECURITY

Regional Incident Preparedness and Response Playbook

Version 2.0

November 2022

©2022 The MITRE Corporation. All rights reserved. Approved for Public Release. Distribution unlimited; Case Number 2022-3034.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Image source: FDA & MITRE

CISA/FBI: Cuba Ransomware Alert

CISA and the FBI released an (updated) joint alert on Cuba Ransomware: Alert (AA22-335A) #StopRansomware: Cuba Ransomware.

This an updated alert – the original one was released about a year ago.

Some of the noteworthy data points that came out of it were:

- The Cuba ransomware operators have compromised over 100 targets to date and have received over $60 million in ransoms, following a total of $145M in demands.
- They have been observed targeting five critical U.S. infrastructures, including financial services, government, manufacturing, and information technology, and of course healthcare.
- They also noted that the Cuba operators have expanded the infection vectors and malware that they leverage – they currently leverage remote-access Trojans, the Hancitor dropper, Qbot and other malware variants.

Quantum Computing Cybersecurity Preparedness Act

The President recently signed into law HR 7535, which is titled the Quantum Computing Cybersecurity Preparedness Act.

- It encourages the federal government to adopt technology that is protected from decryption, and more specifically, attacks from quantum computing systems.
- The Act doesn't contain any mandates or standards.
  - It requires high-level reporting and requires guidance and reports by OMB, CISA and NIST.
  - It serves as a reminder that the federal government should be planning long-term for the upgrading of systems that rely on modern cryptography.
- The private health sector would be well-advised to ensure their organizations are preparing for quantum computing and its potential impact on classical cryptography.

Image source: Sophos

Consolidated Appropriations Act of 2023

- On December 29, 2022, the White House signed H.R. 2617, the Consolidated Appropriations Act 2023, which included several cybersecurity provisions.
- This bill includes new requirements for medical device manufacturers to ensure that their devices meet certain minimum cybersecurity standards.
  - Those requirements will take effect 90 days after the bill is enacted.
  - These provisions include:
    - Monitoring, identifying, and addressing postmarket cybersecurity vulnerabilities and exploits, which includes coordinated vulnerability disclosure, and requiring the release of postmarket software and firmware updates and patches.
    - It also includes requiring medical device manufacturers to provide a Software Bill of Materials (SBOM) to the Secretary of the FDA that includes all off-the-shelf, open source, and critical components used by the devices.
  - Many of these provisions were introduced as part of the PATCH Act in the spring.

What Happened to the Conti Members?

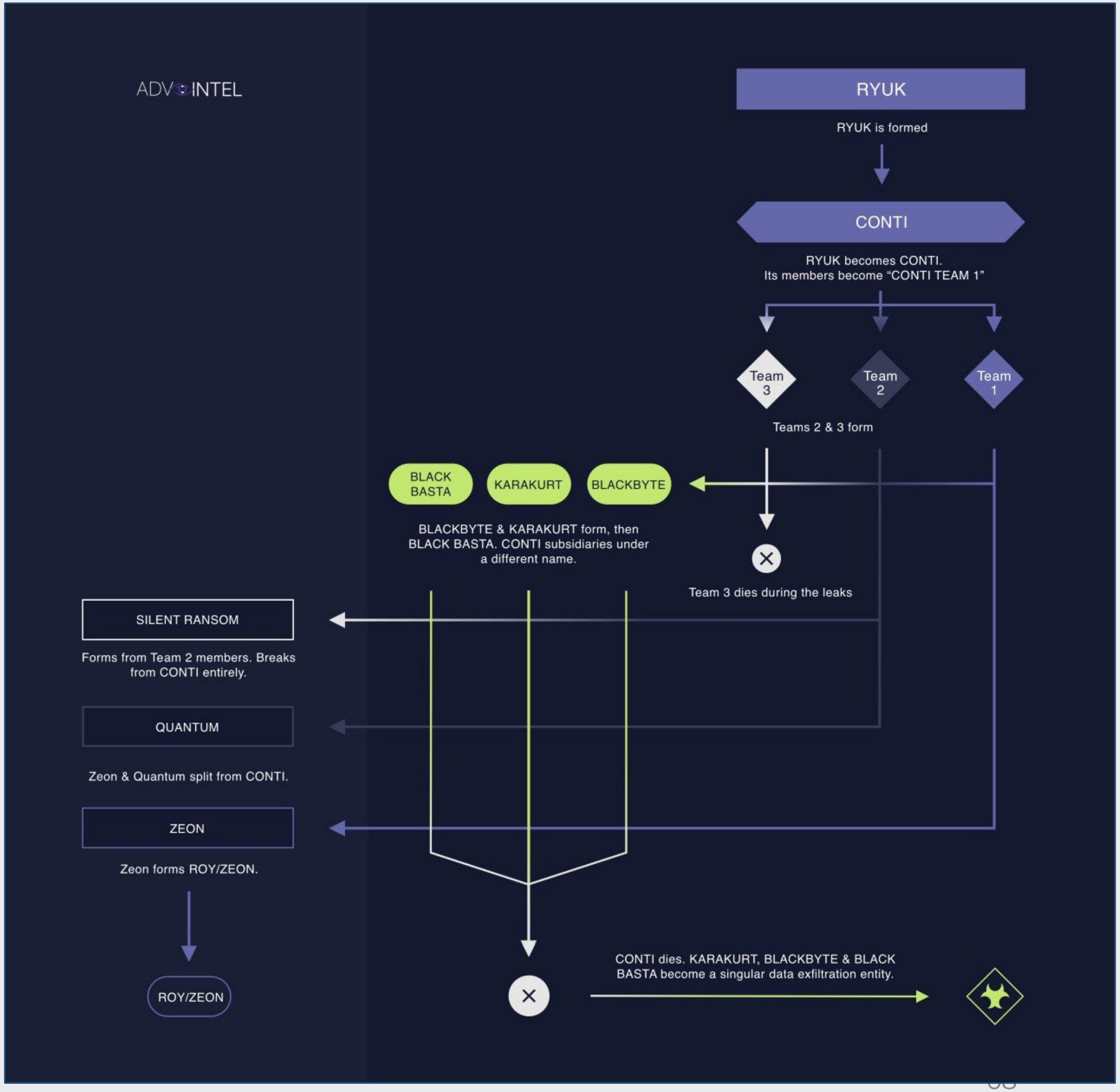
After Conti disbanded, what became of the individual members?

The diagram on the left, provided by Vitali Kremez, CEO of AdvIntel, shows their possible decisions.

Many joined other existing cybercriminal groups.

We even have reason to believe that several of them joined the Royal Ransomware gang.

The saga continues, and the individual criminals continue to commit crimes regardless of their affiliations…



RYUK is formed

RYUK becomes CONTI.
Its members become "CONTI TEAM 1"

Teams 2 & 3 form

BLACKBYTE & KARAKURT form, then BLACK BASTA. CONTI subsidiaries under a different name.

Team 3 dies during the leaks

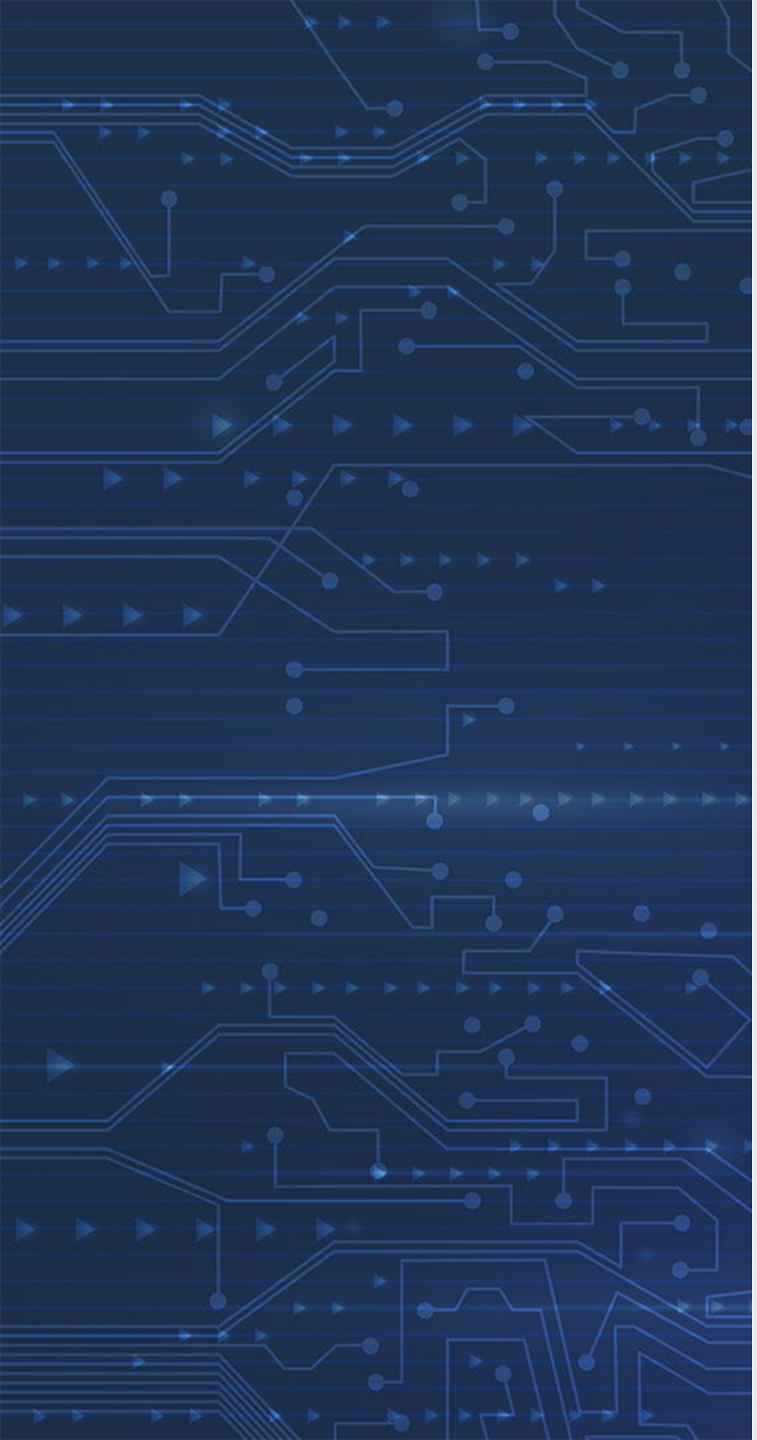
Forms from Team 2 members. Breaks from CONTI entirely.

Zeon & Quantum split from CONTI.

Zeon forms ROY/ZEON.

CONTI dies. KARAKURT, BLACKBYTE & BLACK BASTA become a singular data exfiltration entity.

Image source: Vitali Kremez (Twitter)



2022 Summary

A brief review of summary data from the year

Emsisoft – The State of Ransomware in the U.S. 2022

- Annual total of ransomware attacks across industries and specifically impacting healthcare

The reports can be accessed by clicking here:

2020 2021 2022

YEAR	Total	HPH	PHI	Notes
2020	2,354	560	12	Maze was the only ransomware gang conducting double extortion at the beginning of the year; no less than 17 other gangs had adopted the tactic by the end of 2020.
2021	2,323	1,203	Unk.	One single attack targeted a provider that maintains over 600 locations; one single HPH compromise cost over $110 million.
2022	2,421	290	17	Only hospitals tracked this year (as opposed to other HPH organizations); one attack impacted a computer system that calculated doses of medication, and as a result, a 3-year-old patient was reported to have received a massive overdose of pain medicine.

Coveware Trends for 2022: Ransom Fees

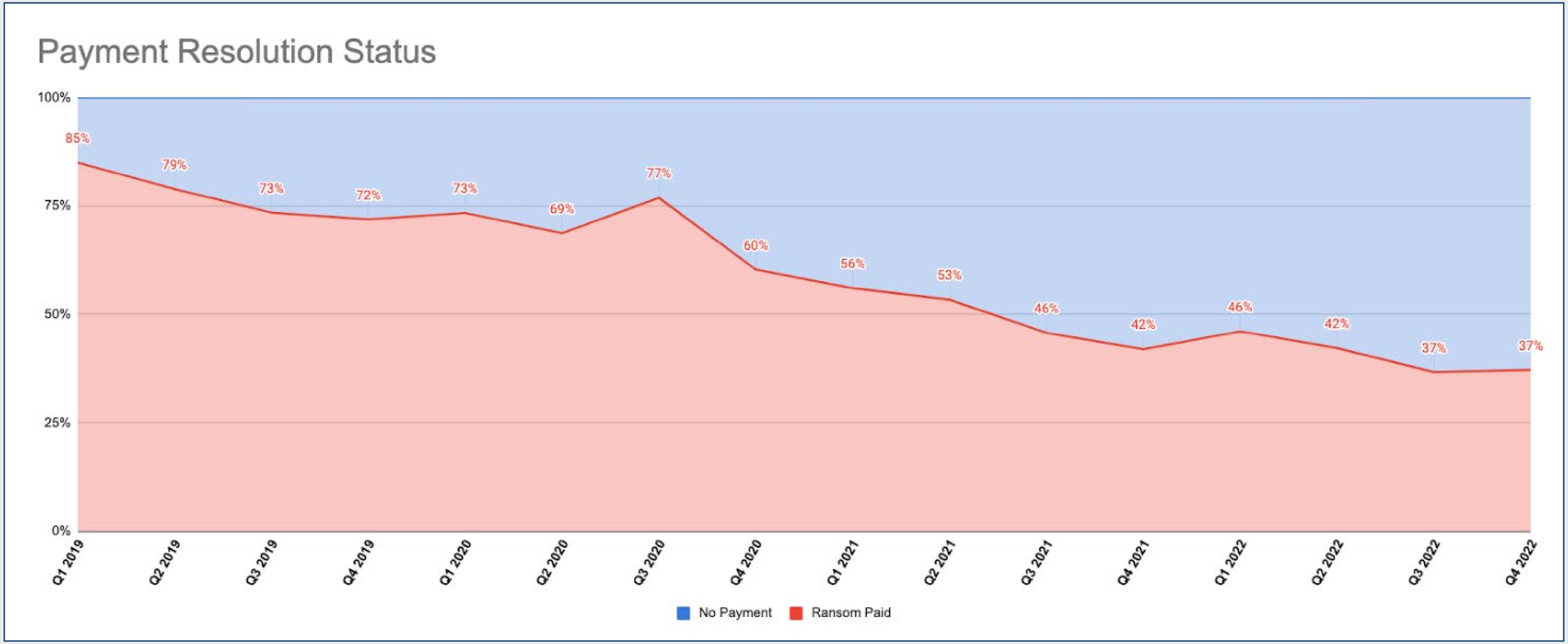


Image source: Coveware

Coveware Trends for 2022: Ransom Fees (Part 2)

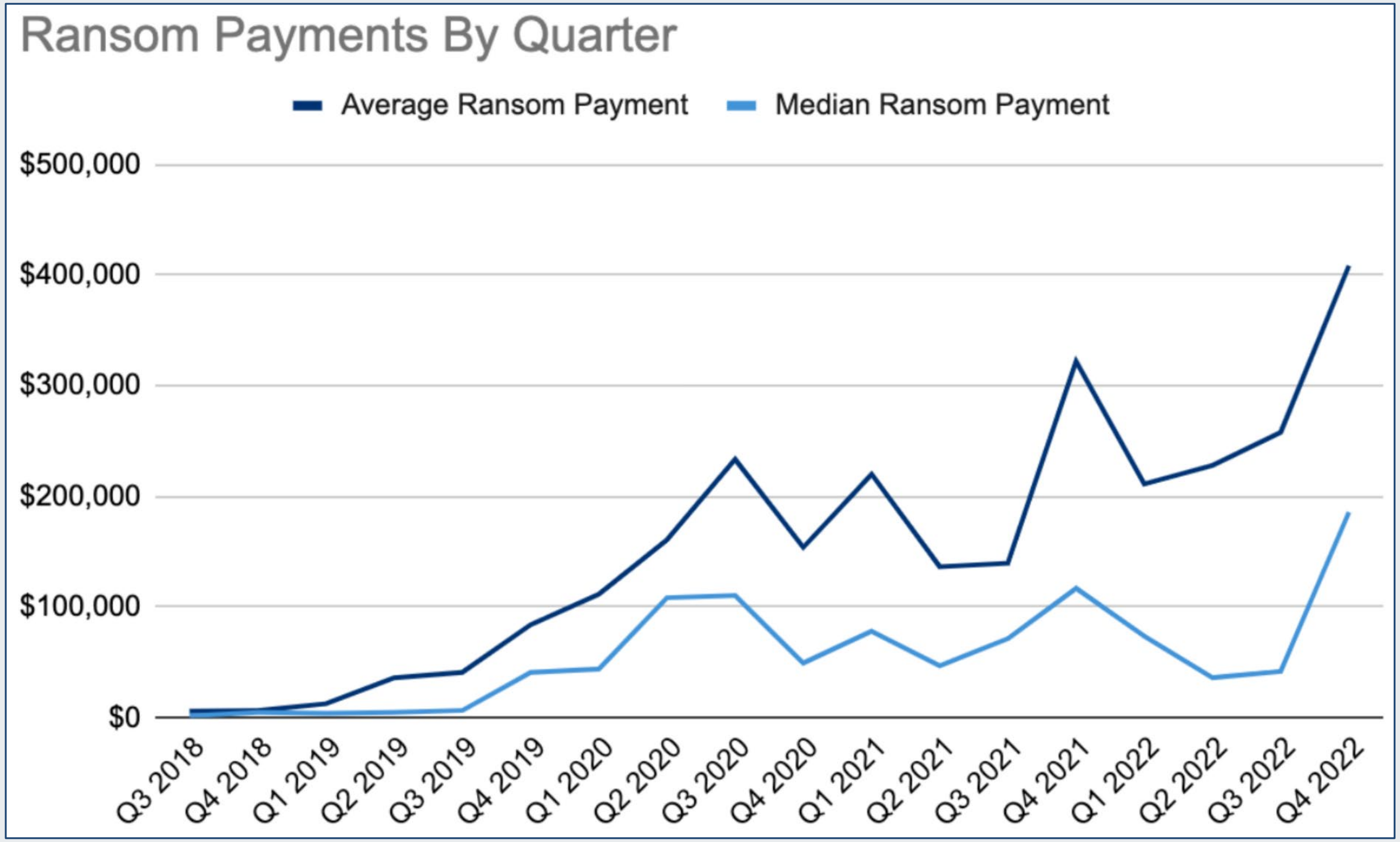


Image source: Coveware

Coveware Trends for 2022: Attack Vectors

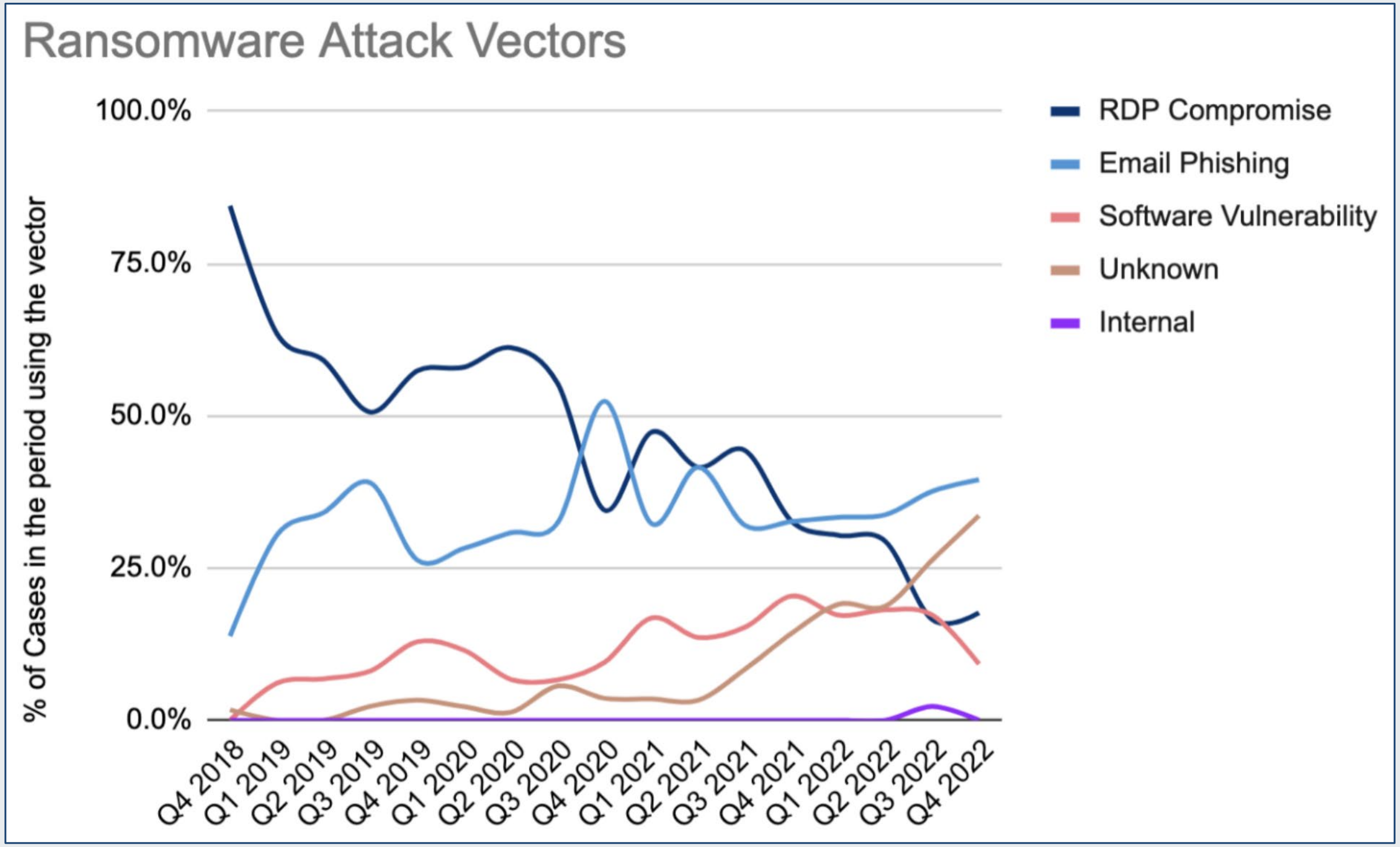


Image source: Coveware

Coveware Trends for 2022: Industries

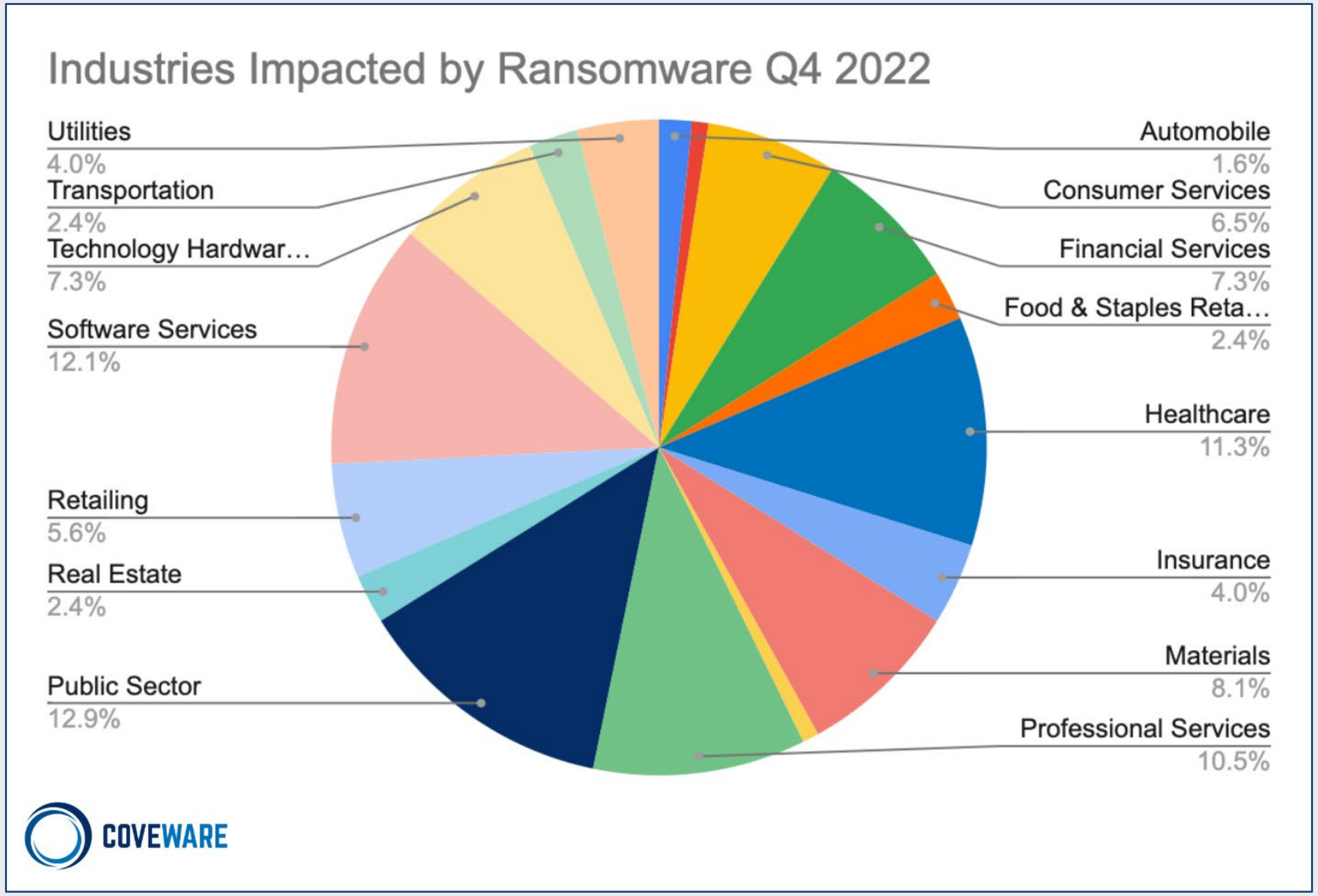


Image source: Coveware

Healthcare Data Breaches (Organizations)

- This data was compiled by BankInfoSecurity.com from OCR portal data.
- Same data we saw earlier but including 2022 data.
- Decreases in breached healthcare records in 2022.

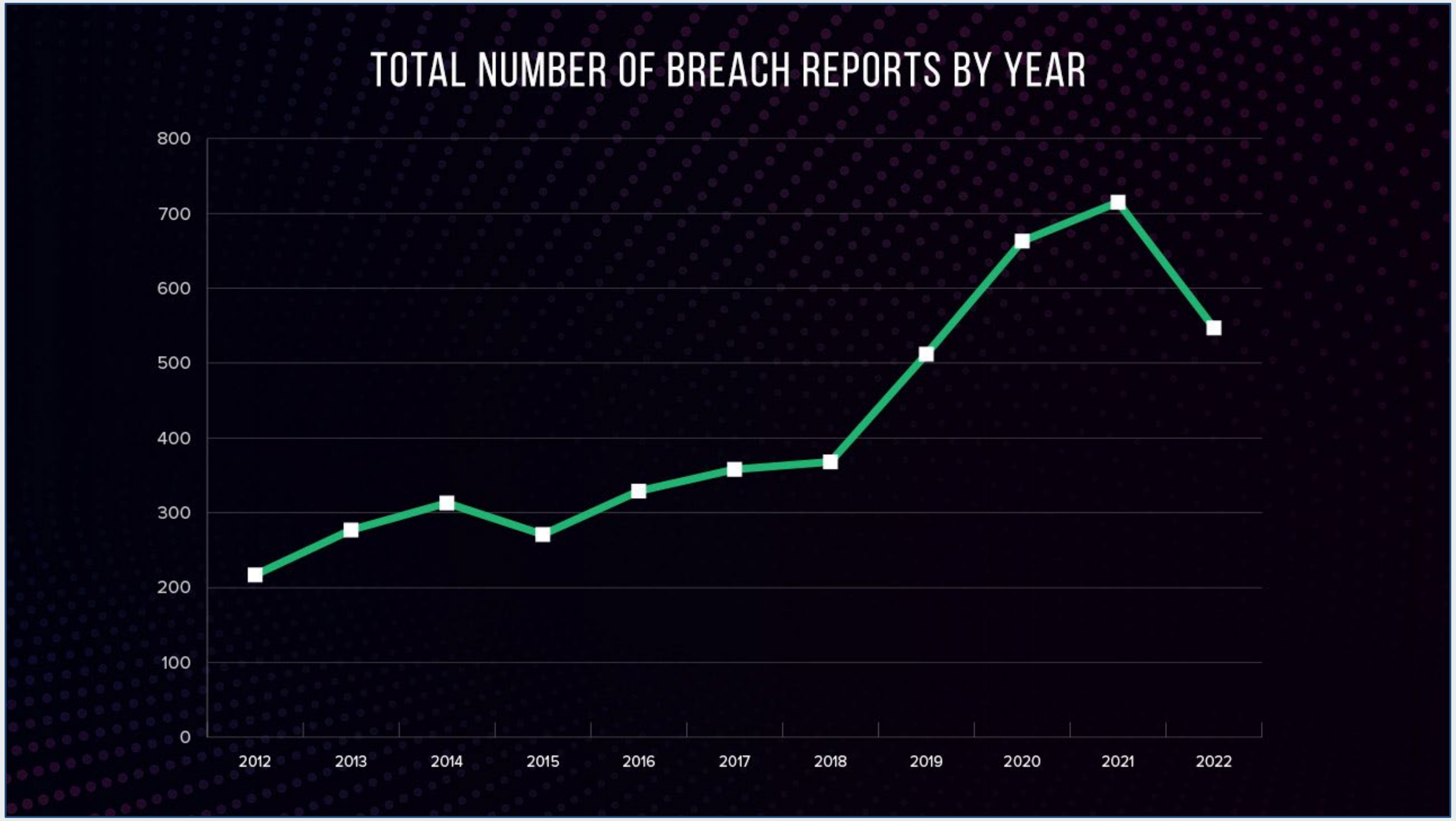


Image source: BankInfoSecurity.com

Monthly Data Breaches – 2022

Number of U.S. healthcare organizations breached by month, data from HIPAA Journal:

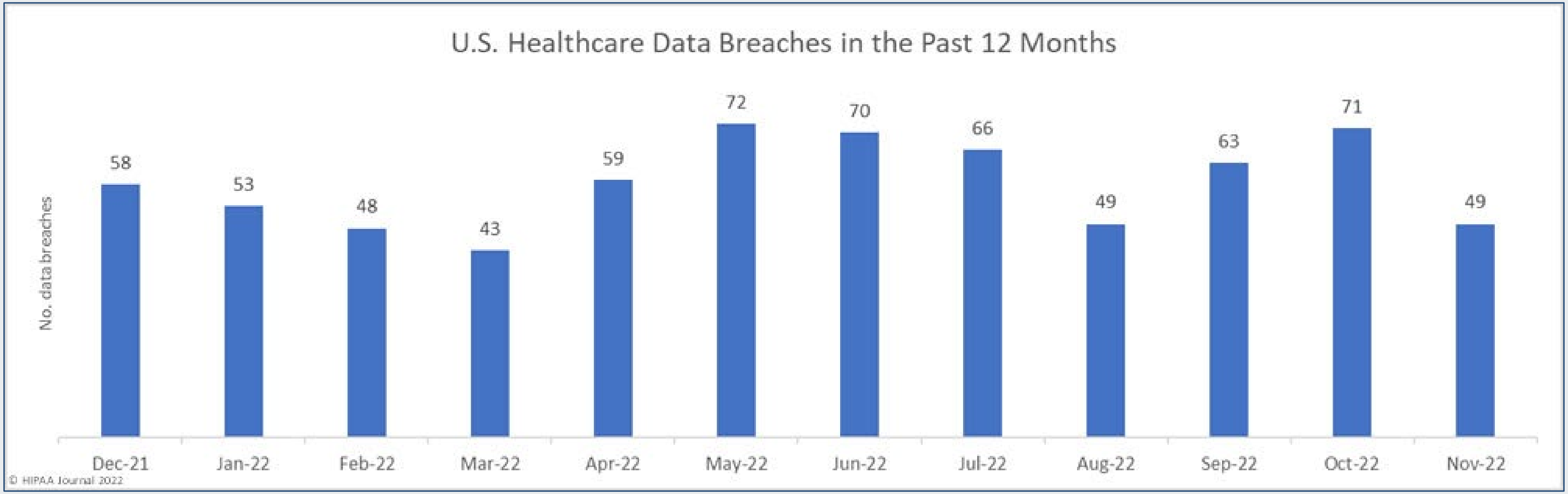


Image source: HIPAA Journal

Annual Data Breaches

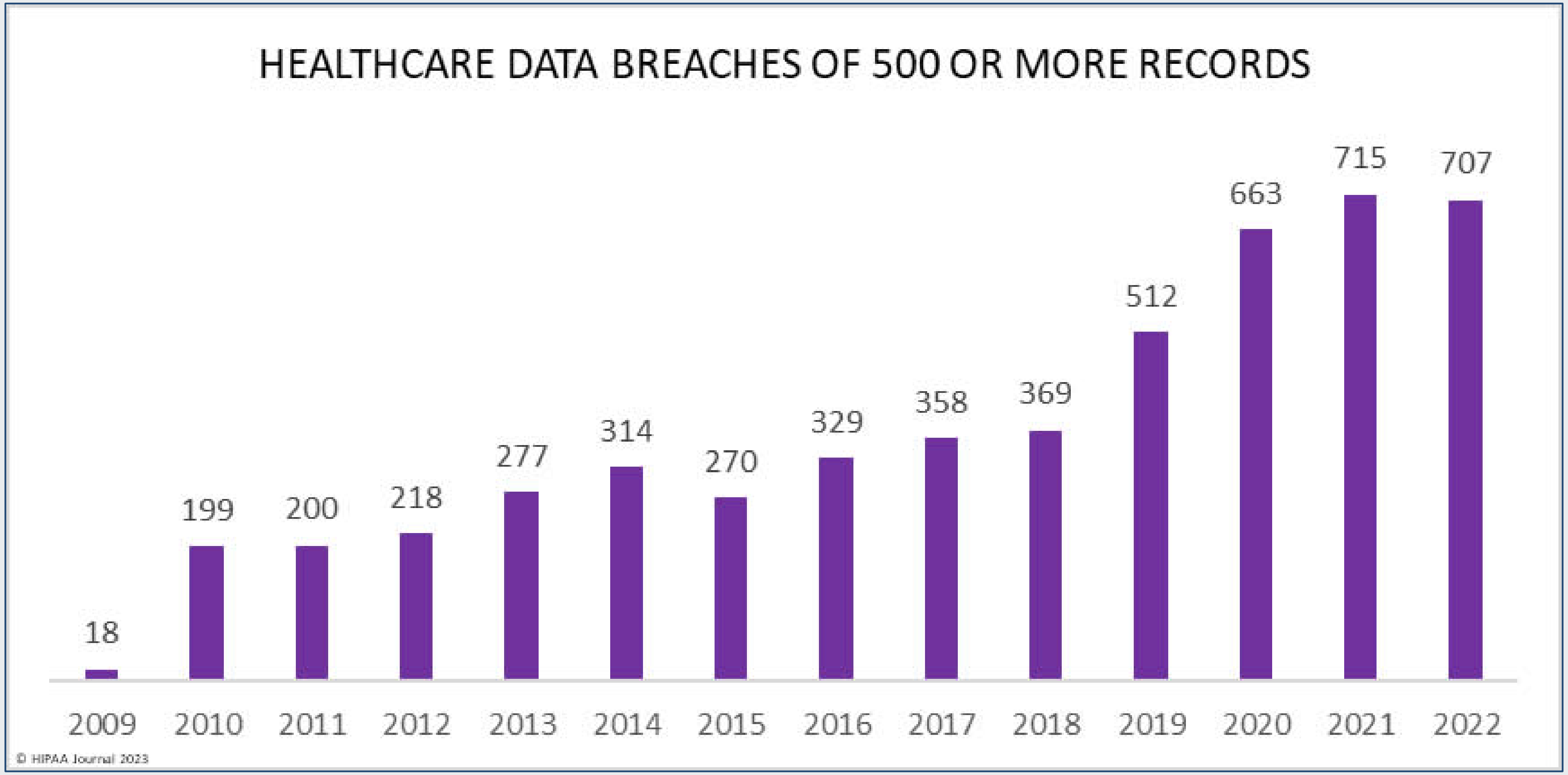


Image source: HIPAA Journal

Individuals Impacted by U.S. Healthcare Breaches

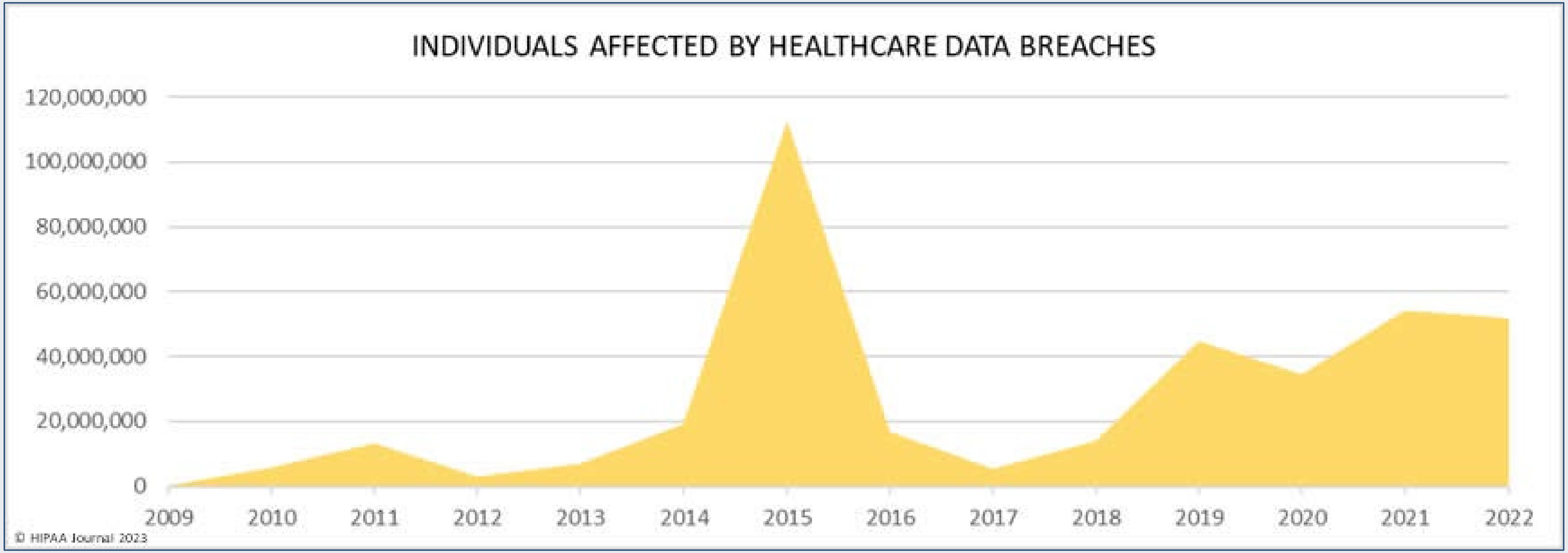


Image source: HIPAA Journal

The Cause of U.S. HPH Data Breaches in 2022

What caused U.S. healthcare data breaches in 2022?

Deliberate cyberattacks were once again at the top of the list.

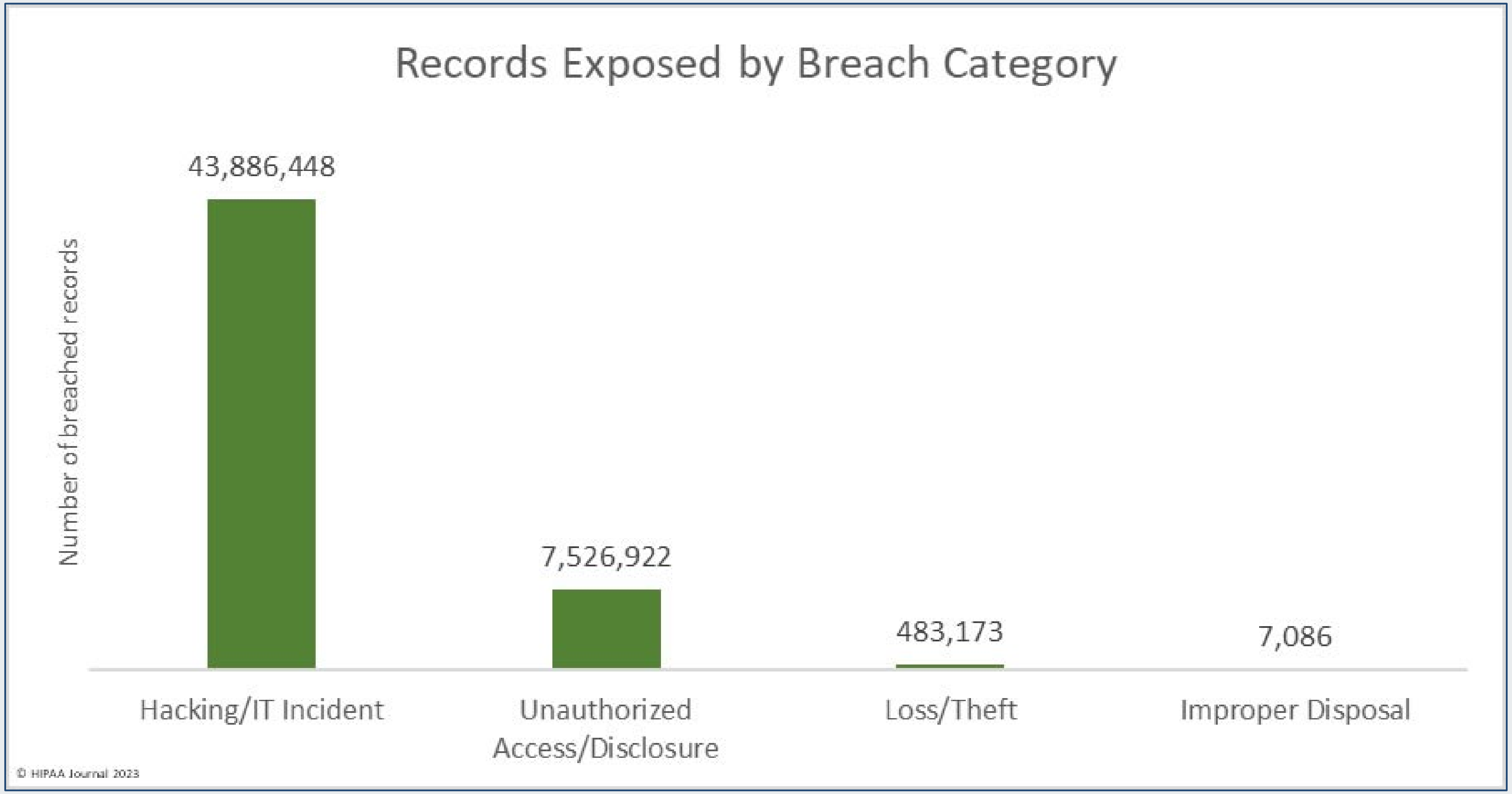


Image source: HIPAA Journal

What Systems Are the Breached Data Coming From?

Servers, databases and email continue to be heavily targeted for sensitive data.

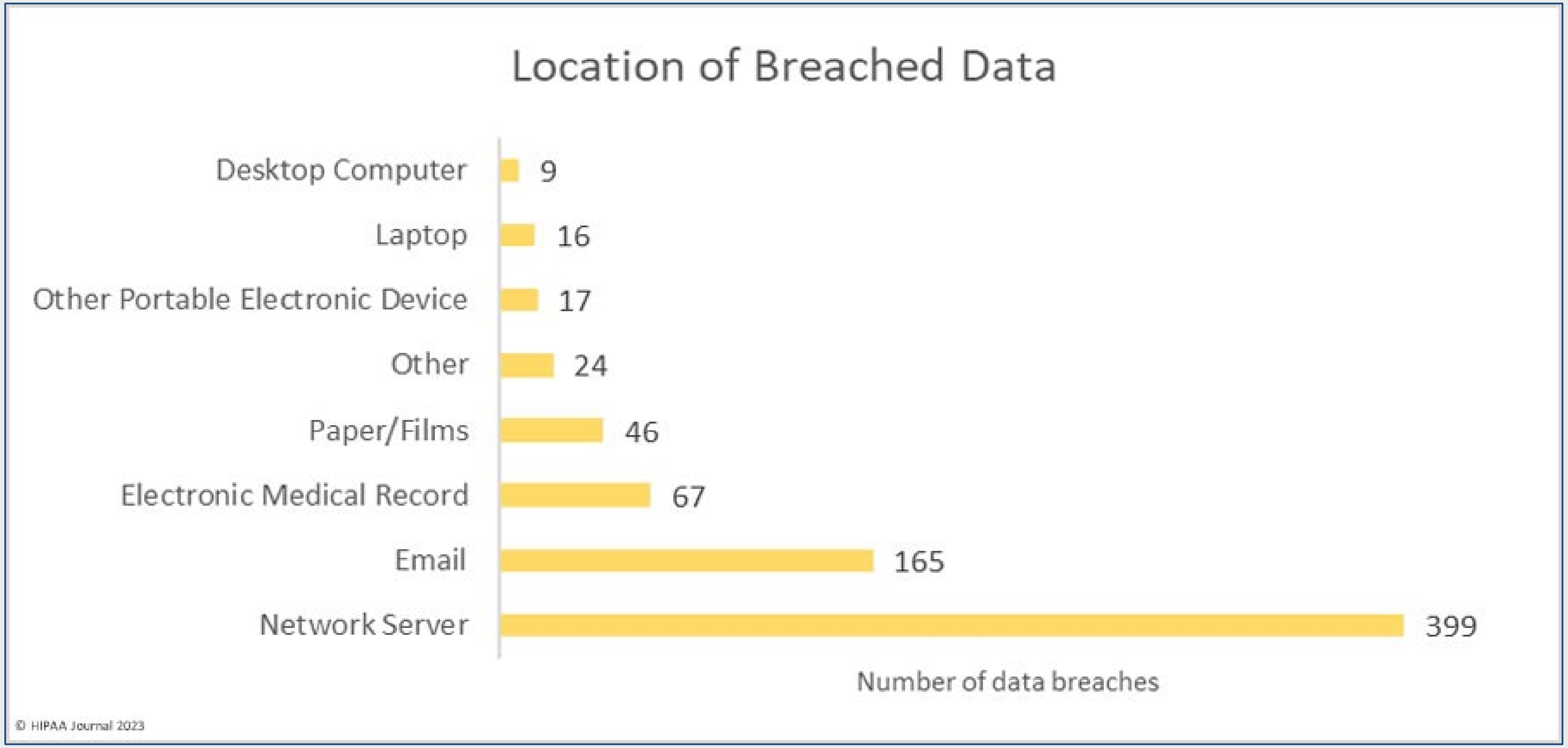


Image source: HIPAA Journal

What Types of HPH Organizations Were Breached?

Insurers, healthcare providers and third-party business associates represent all data breaches for 2022 – this is fairly standard across time.

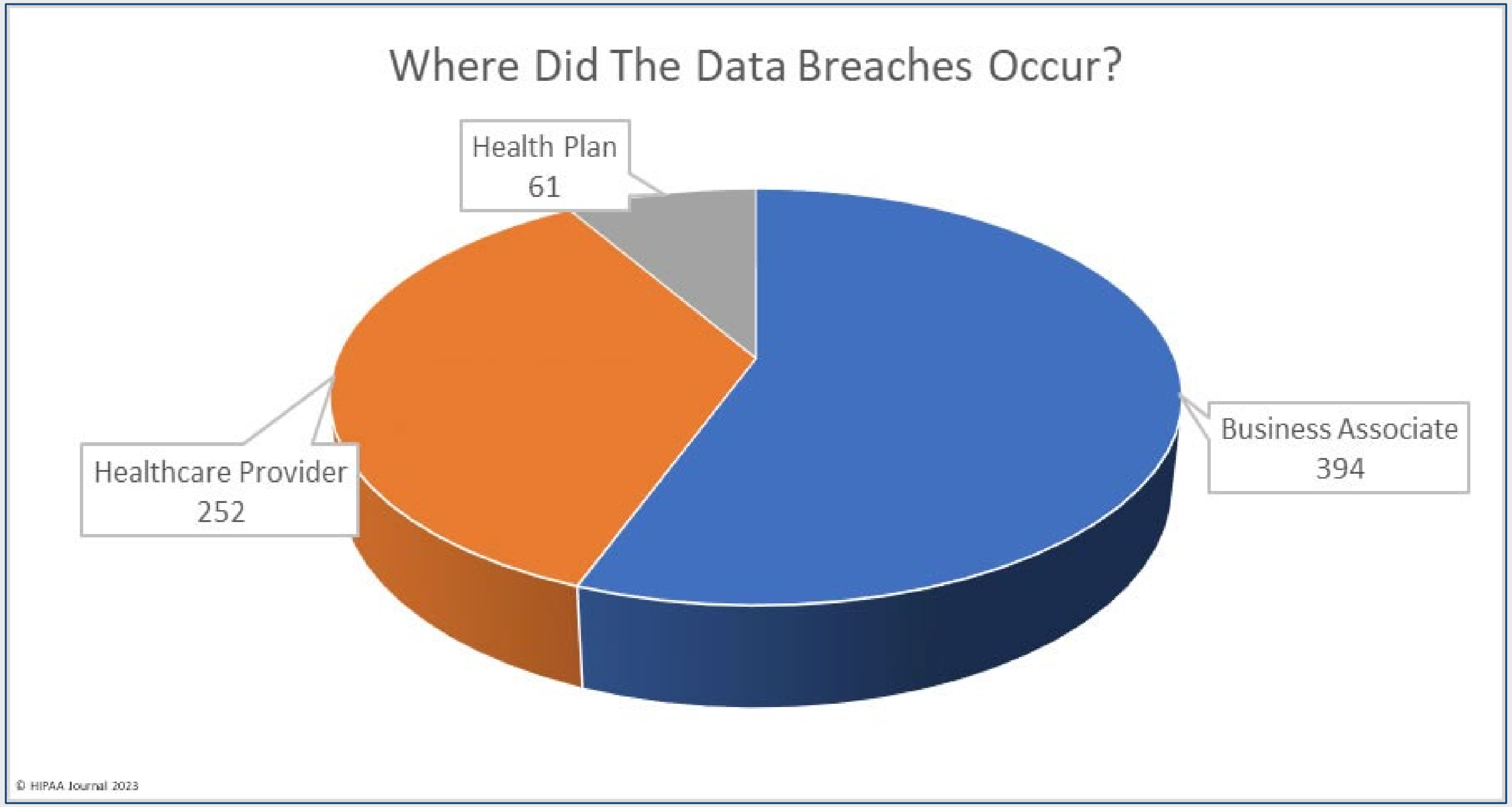


Image source: HIPAA Journal

How Much Has Each Organization Been Breached?

2022 was a year when attackers compromised health sector organizations both directly and indirectly (through third party support) while insurance plans were relatively less impacted.

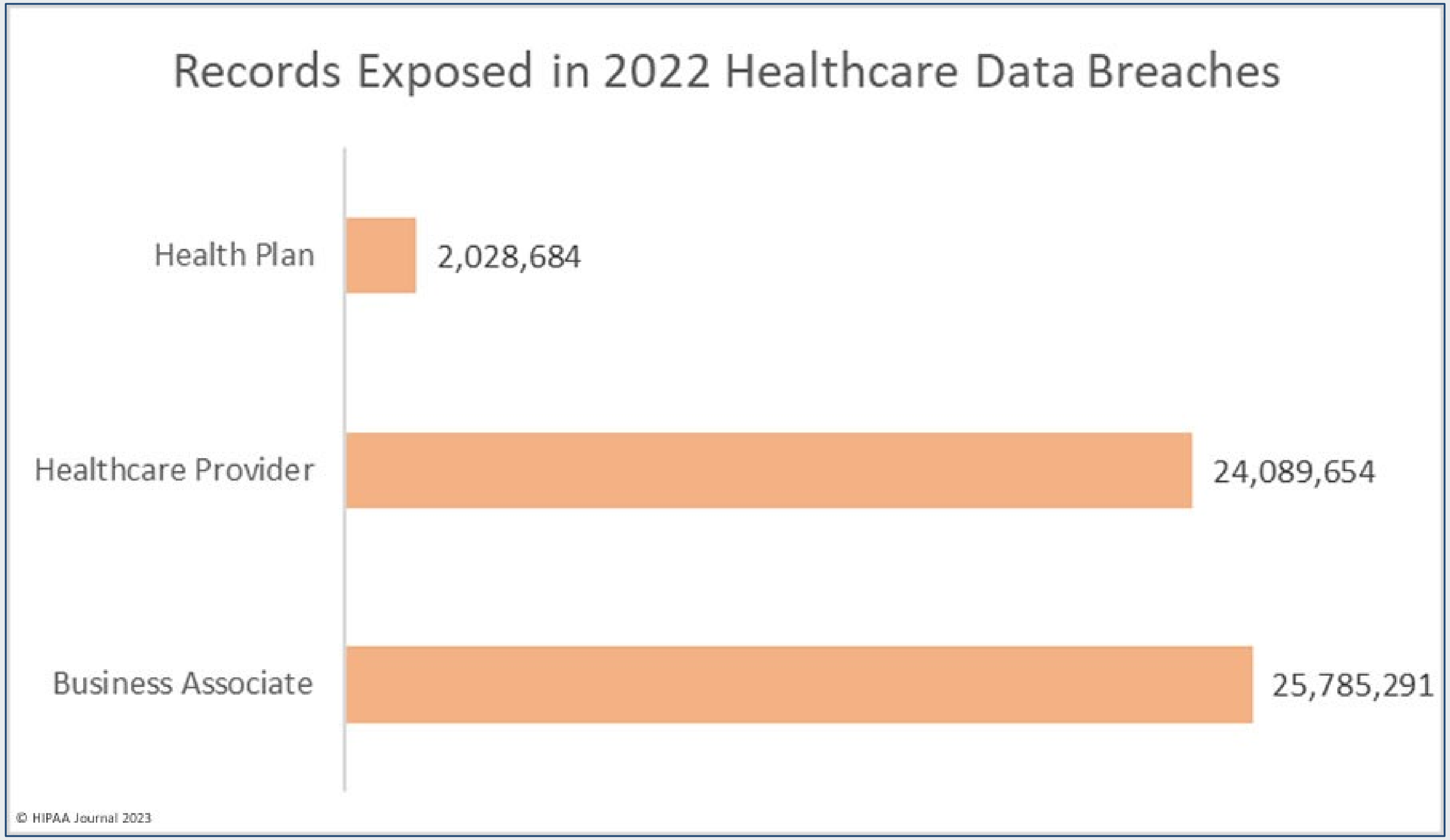


Image source: HIPAA Journal

Number of Data Breaches at U.S. HPH Entities

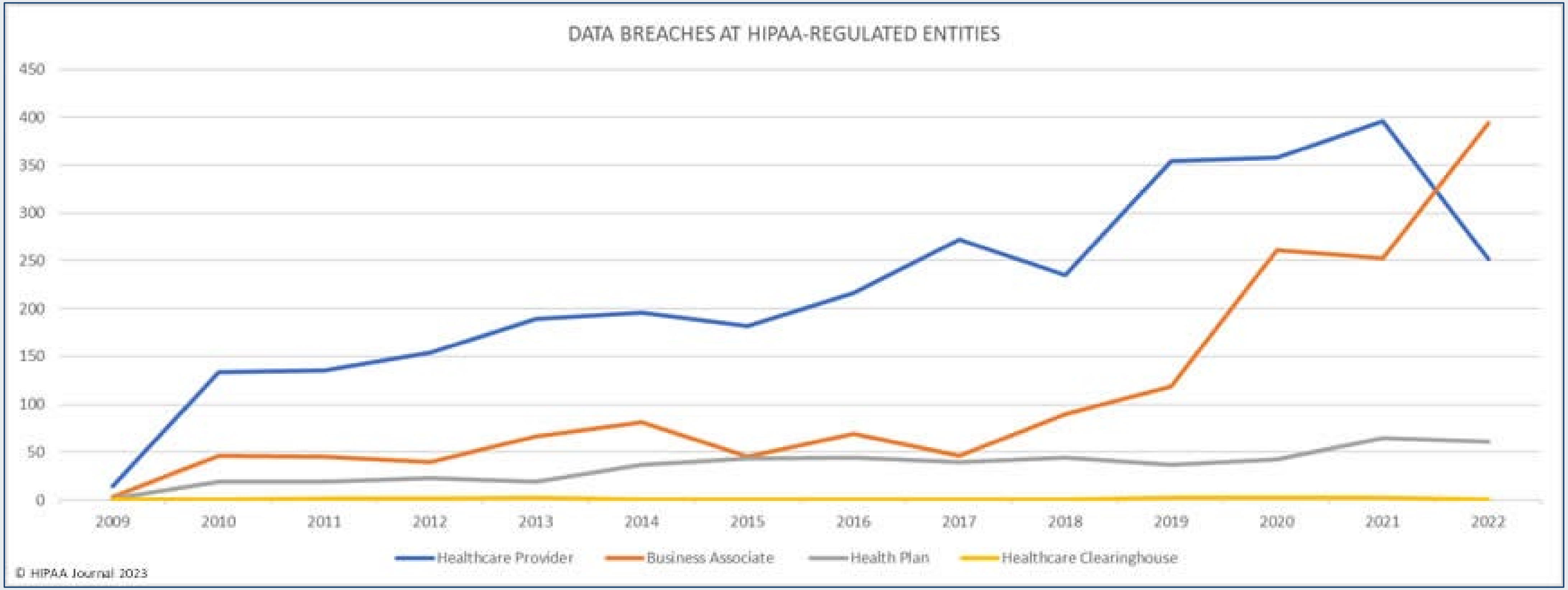
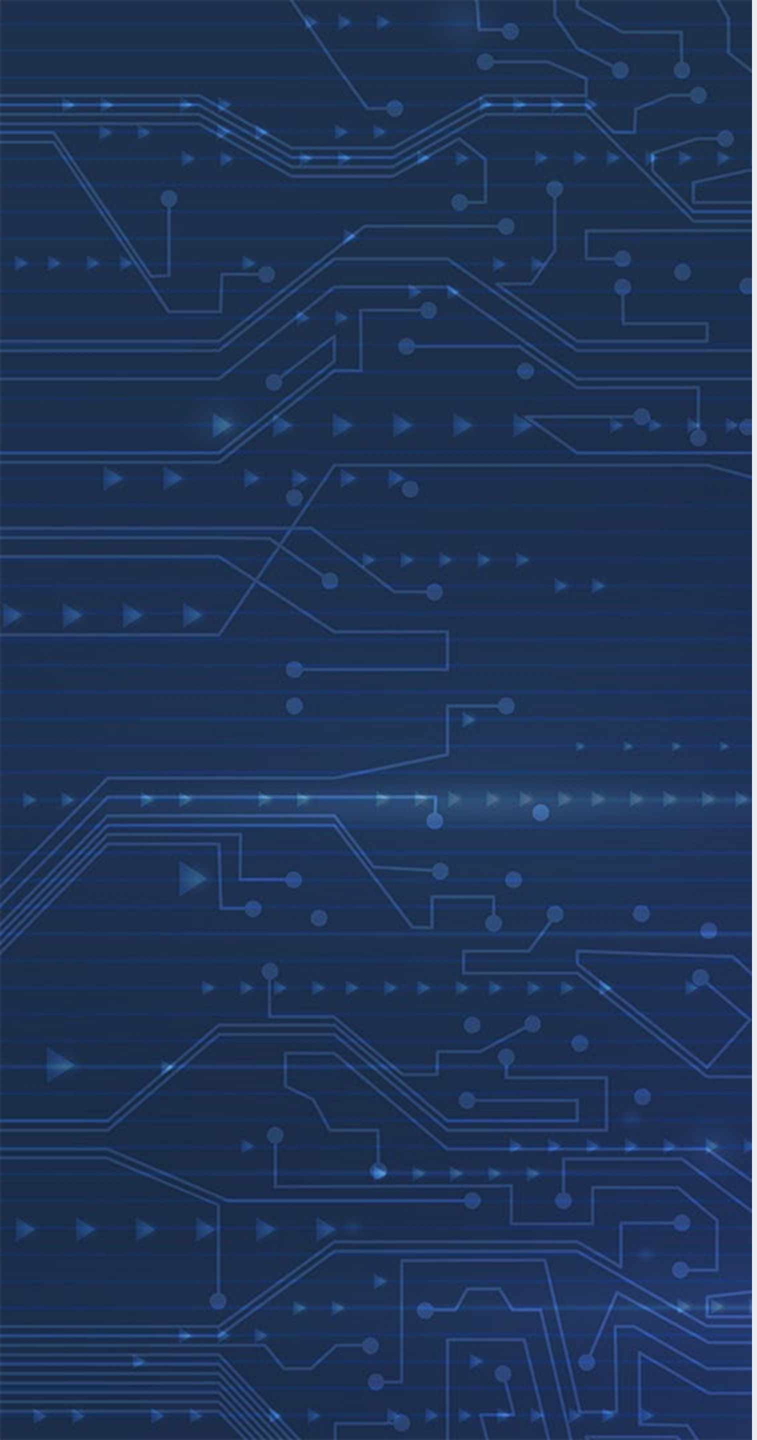


Image source: HIPAA Journal



2023 and Beyond

What does all this mean for today and tomorrow?
How do HPH organizations protect themselves?

Questions to Consider

We began the presentation with the following three questions, and the events of 2022 provide us with possible answers to them:

- What technology and threat actor trends exist, and how will they impact HPH security?
- How can geopolitical events impact healthcare cybersecurity?
- What is the U.S. government and its international allies doing about these threats, and what impacts will they have?

Likely Long-Term Trends to Consider

Ransomware and data breaches are and will continue to be a plague to the U.S. health sector

- Financial incentives, effective choices of attack vectors and geopolitical relationships mean these attacks will continue, often together (double extortion).
- The technical details to defend against these attacks may change, so keeping up with technical indicators will be necessary, but these tactics will likely be around for the long term.

Traditional infection vectors still apply, and prevention is the best way to prevent all cyberattacks

- The cybercriminal ecosystem will continue to adjust based on their feedback loop of effectiveness, but traditional infection vectors will continue to be leveraged:
  - Phishing
  - Remote access (RDP-based technologies and VPNs, among others)
  - Exploitation of known vulnerabilities (especially open source)
  - Managed service provider compromise (especially applicable in recent years)

Likely Long-Term Trends to Consider, Part 2

Seemingly unrelated geopolitical events can have a direct/indirect impact on the U.S. health sector

- The Russia-Ukraine conflict has presented important data points for U.S. HPH cybersecurity:
  - A seemingly unrelated geopolitical event can indirectly impact the provided lessons learned.
    - The Russian government is leveraging wipers and DDoS attacks, among other things.
    - Pay attention to the big cyber capabilities – China, Russia, Iran, North Korea, but also lesser powers as well, especially allies.

Law enforcement and other federal entities will continue to help but are not a "silver bullet"

- The federal government, including U.S. Cyber Command, the National Security Agency, the Department of Homeland Security/Cybersecurity and Infrastructure Agency, the Food and Drug Administration, and the Department of Justice/Federal Bureau of Investigation, will continue to act against the threats you see in this brief.
  - None of this is an excuse to drop your guard. Both APTs and the cybercriminal ecosystem are here to stay.

Software supply chain attacks are here to stay

- Log4J is just one example – know what's in your code!

Staying Secure

- Government resources:
  - DHS/CISA Stop Ransomware: https://www.cisa.gov/stopransomware
  - FBI Cybercrime: https://www.fbi.gov/investigate/cyber
  - FBI Internet Crime Complaint Center (IC3): https://www.ic3.gov/Home/ComplaintChoice/default.aspx/
  - FDA: Medical device information: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
  - HC3 Products: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html

"Every industry and every subindustry in healthcare is seeing an increase in attacks. This isn't going away."
– Taylor Lehman, Google Cloud

Ransomware Mitigations and Defense (Source: FBI)

- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Review Task Scheduler for unrecognized scheduled tasks. Additionally, manually review operating system defined or recognized scheduled tasks for unrecognized “actions” (for example: review the steps each scheduled task is expected to perform).
- Review antivirus logs for indications that they were unexpectedly turned off.
- Implement network segmentation.
- Require administrator credentials to install software.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).

Ransomware Mitigations and Defense, Part 2

- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Use multifactor authentication where possible.
- Regularly change passwords to network systems and accounts, and avoid reusing passwords for different accounts.
- Implement the shortest acceptable timeframe for password changes.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a virtual private network (VPN).
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.

Recommendations

In addition to following the mitigations, HC3 recommends organizations review and utilize CISA's Free Cybersecurity Services and Tools, which can be accessed by visiting https://www.cisa.gov/free-cybersecurity-services-and-tools .

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

Reference Materials

References

Conti Ransomware Decryptor, TrickBot Source Code Leaked
https://threatpost.com/conti-ransomware-decryptor-trickbot-source-code-leaked/178727/

Conti Team One Splinter Group Resurfaces as Royal Ransomware with Callback Phishing Attacks
https://www.trendmicro.com/en_us/research/22/l/conti-team-one-splinter-group-resurfaces-as-royal-ransomware-wit.html

2022 Year in Review: APTs Livestream Replay
https://blog.talosintelligence.com/apts-2022-year-in-review-livestream/

October 2022 Healthcare Data Breach Report
https://www.hipaajournal.com/october-2022-healthcare-data-breach-report/

ICS cyberthreats in 2023 – what to expect
https://securelist.com/ics-cyberthreats-in-2023/108011/

The Top Ransomware Trends to Watch Out for in 2023
https://www.reliaquest.com/i/blog/ransomware-trends-2023/

References

How ransomware gangs and malware campaigns are changing
https://www.helpnetsecurity.com/2022/11/10/malware-ransomware-trends/

2022 Adversary Infrastructure Report
https://go.recordedfuture.com/hubfs/reports/cta-2022-1215.pdf

Bitdefender Year in Review: Top Cybersecurity Highlights from 2022
https://businessinsights.bitdefender.com/bitdefender-year-in-review-top-cybersecurity-highlights-from-2022

October's Most Wanted Malware: AgentTesla Knocks Formbook off Top Spot and New Text4Shell Vulnerability Disclosed
https://blog.checkpoint.com/2022/11/08/octobers-most-wanted-malware-agenttesla-knocks-formbook-off-top-spot-and-new-text4shell-vulnerability-disclosed/

Russia arrests 14 alleged members of REvil ransomware gang, including hacker U.S. says conducted Colonial Pipeline attack
https://www.washingtonpost.com/world/2022/01/14/russia-hacker-revil/

References

The cases for using the SBOMs we build
https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-cases-for-using-sboms/

Healthcare Data Breaches Doubled in 3 Years: Here's Why
https://www.bankinfosecurity.com/healthcare-data-breaches-doubled-in-3-years-heres-why-a-20516

If healthcare doesn't strengthen its cybersecurity, it could soon be in critical condition
https://www.weforum.org/agenda/2021/11/healthcare-cybersecurity

Endpoint Best Practices to Block Ransomware
https://news.sophos.com/en-us/2022/12/06/endpoint-best-practices-to-block-ransomware/

Inside the Second White House Ransomware Summit
https://securityintelligence.com/articles/inside-second-white-house-ransomware-summit/

E-mail threats in 2022
https://www.kaspersky.com/blog/email-threats-in-2022/46582/

References

Trellix Predicts Heightened Hacktivism and Geopolitical Cyberattacks in 2023
https://www.trellix.com/en-us/about/newsroom/news/news-detail.html?news_id=4a568aeb-1e2e-4bac-83f4-dc17d168cae0

Academics publish method for recovering data encrypted by the Hive ransomware
https://therecord.media/academics-publish-method-for-recovering-data-encrypted-by-the-hive-ransomware/

Cyberattacks are targeting smaller healthcare companies and specialty clinics. But why?
https://www.tripwire.com/state-of-security/cyberattacks-are-targeting-smaller-healthcare-companies-and-specialty-clinics-why

Beers with Talos Ep. 129: Talos Year in Review 2022 w/ Dave Liebenberg
https://blog.talosintelligence.com/beers-with-talos-ep-129/

14 lessons CISOs learned in 2022
https://www.csoonline.com/article/3682748/14-lessons-cisos-learned-in-2022.html

References

Most of the 10 largest healthcare data breaches in 2022 are tied to vendors
https://www.scmagazine.com/feature/breach/most-of-the-10-largest-healthcare-data-breaches-in-2022-are-tied-to-vendors

Forging Ahead in 2023: Insights From Trend Micro’s 2023 Security Predictions
https://www.trendmicro.com/en_us/research/22/l/forging-ahead-in-2023--insights-from-trend-micro-s-2023-security.html

2022 In Review: An Eventful Cybersecurity Year
https://www.forbes.com/sites/emilsayegh/2022/12/13/2022-in-review-an-eventful-cybersecurity-year/

From Babuk Source Code to Darkside Custom Listings — Exposing a Thriving Ransomware Marketplace on the Dark Web
https://www.venafi.com/blog/babuk-source-code-darkside-custom-listings-exposing-thriving-ransomware-marketplace-dark-web

References

2022 Adversary Infrastructure Report
https://www.recordedfuture.com/2022-adversary-infrastructure-report

Digital Health Unplugged: 2022 Year in Review
https://www.digitalhealth.net/2022/12/digital-health-unplugged-2022-year-in-review/

The Near and Far Future of Ransomware Business Models
https://documents.trendmicro.com/assets/white_papers/wp-the-near-and-far-future-of-ransomware.pdf

The Top Ransomware Trends to Watch Out for in 2023
https://www.reliaquest.com/blog/ransomware-trends-2023/

Ransomware predictions for 2023
https://www.helpnetsecurity.com/2022/12/20/ransomware-predictions-for-2023-video/

Reassessing cyberwarfare. Lessons learned in 2022
https://securelist.com/reassessing-cyberwarfare-lessons-learned-in-2022/108328/

References

NSA Publishes 2022 Cybersecurity Year in Review
https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3247606/nsa-publishes-2022-cybersecurity-year-in-review/

Cyberattacks in 2022 and what hospitals, health systems can learn going into 2023
https://www.beckershospitalreview.com/cybersecurity/cyberattacks-in-2022-and-what-hospitals-health-systems-can-learn-going-into-2023.html

Forging Ahead in 2023: Insights From Trend Micro’s 2023 Security Predictions
https://www.trendmicro.com/en_us/research/22/l/forging-ahead-in-2023--insights-from-trend-micro-s-2023-security.html

Reassessing cyberwarfare. Lessons learned in 2022
https://securelist.com/reassessing-cyberwarfare-lessons-learned-in-2022/108328/

4 Most Common Cyberattack Patterns from 2022
https://securityintelligence.com/articles/most-common-cyberattack-patterns-2022/

? Questions

FAQ

Upcoming Briefing

- March 9 – Data Exfiltration Trends in Healthcare

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes

Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings

Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Contacts

HHS.GOV/HC3

HC3@HHS.GOV