LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

2020: A Retrospective Look at Healthcare Cybersecurity

02/18/2021

Report #: 202102181030

Agenda

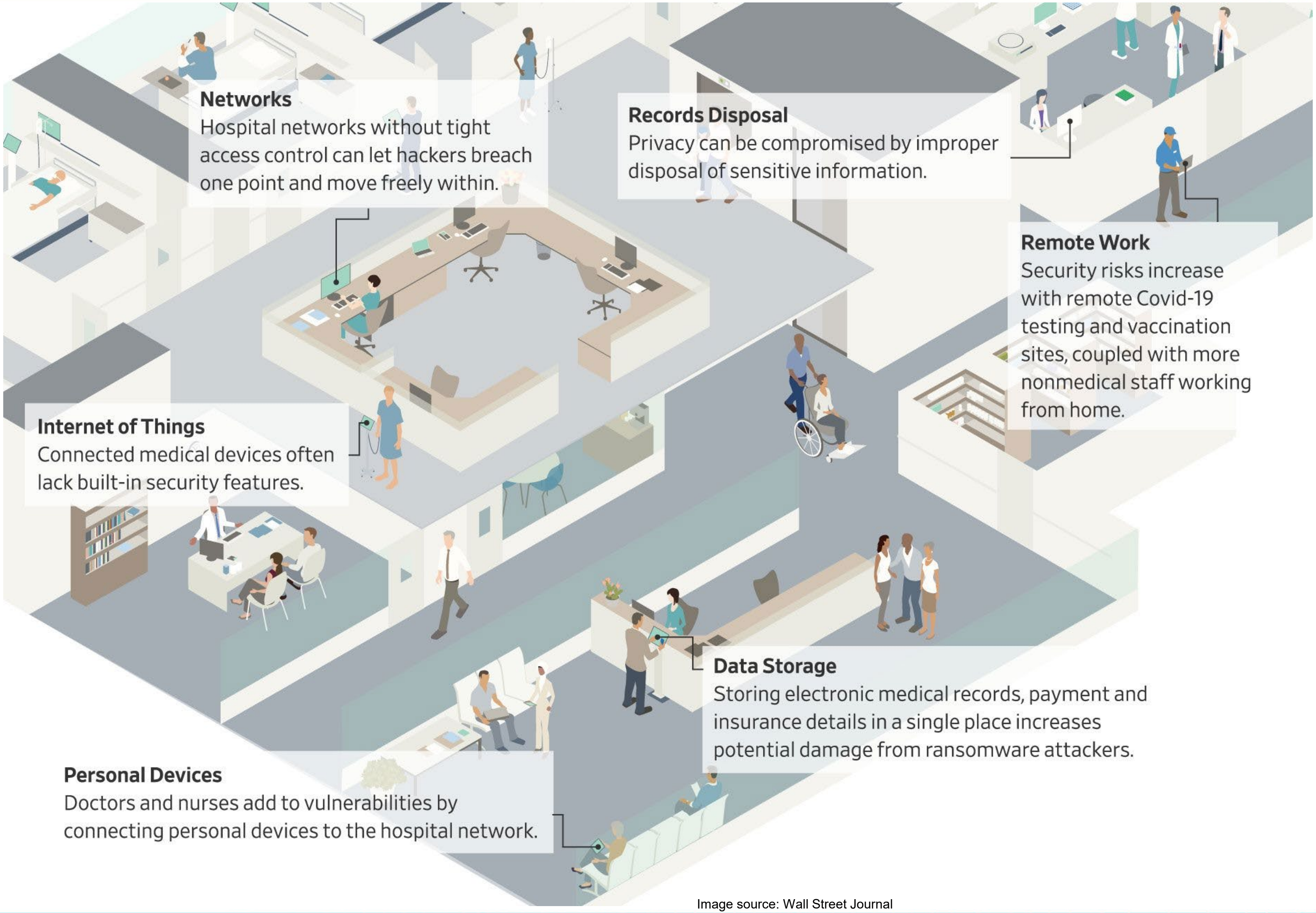
- Vulnerability points in hospitals
- 2020 Healthcare overview – a snapshot
- Ransomware
- Data Breaches
- Blackbaud
- COVID-19 and its implications for healthcare cybersecurity
- Other fraudulent activity
- References
- Questions

Image source: CSO Online

Slides Key:

👤	Non-Technical: Managerial, strategic and high-level (general audience)
⚙	Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Vulnerability points in hospitals



Networks
Hospital networks without tight access control can let hackers breach one point and move freely within.

Records Disposal
Privacy can be compromised by improper disposal of sensitive information.

Remote Work
Security risks increase with remote Covid-19 testing and vaccination sites, coupled with more nonmedical staff working from home.

Internet of Things
Connected medical devices often lack built-in security features.

Data Storage
Storing electronic medical records, payment and insurance details in a single place increases potential damage from ransomware attackers.

Personal Devices
Doctors and nurses add to vulnerabilities by connecting personal devices to the hospital network.

Image source: Wall Street Journal

A Snapshot of Healthcare in 2020

Image source: Times Higher Education

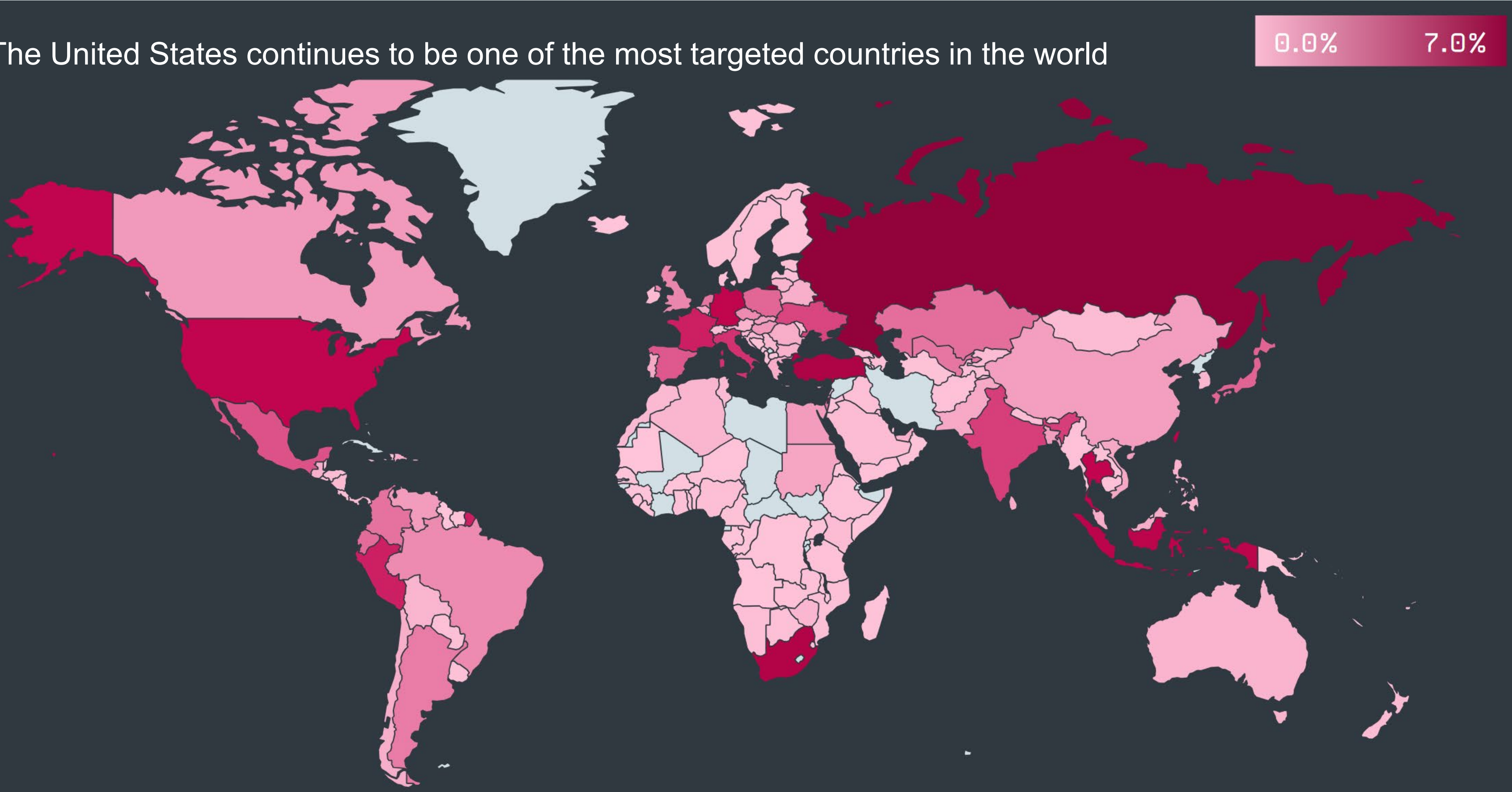
What did 2020 look like for healthcare cybersecurity?

- VMWare/Carbon Black:
  - 239.4 million cyberattacks attempted in 2020
- Average of 816 attempted attacks per healthcare endpoint
  - 9,851% increase from 2019
  - Between January and February: 51% increase
  - Increased throughout year
    - Peaked September/October at 87% increase
- Emsisoft Ransomware statistics for 2020
  - 560 healthcare organizations impacted
- Wall Street Journal (HHS): ~1M healthcare records breached each month last year
  - One breached service provider is estimated to be responsible for ~10M breached records
- Patient in Germany died when being re-routed to another healthcare facility during ransomware attack
- Ransomware-as-a-service became standardized; Double extortion became popular
- COVID-19 themed cyberattacks began along with the pandemic

> "Another banner year for cybercriminals" - Emsisoft

Ransomware vs. Healthcare in 2020

The United States continues to be one of the most targeted countries in the world



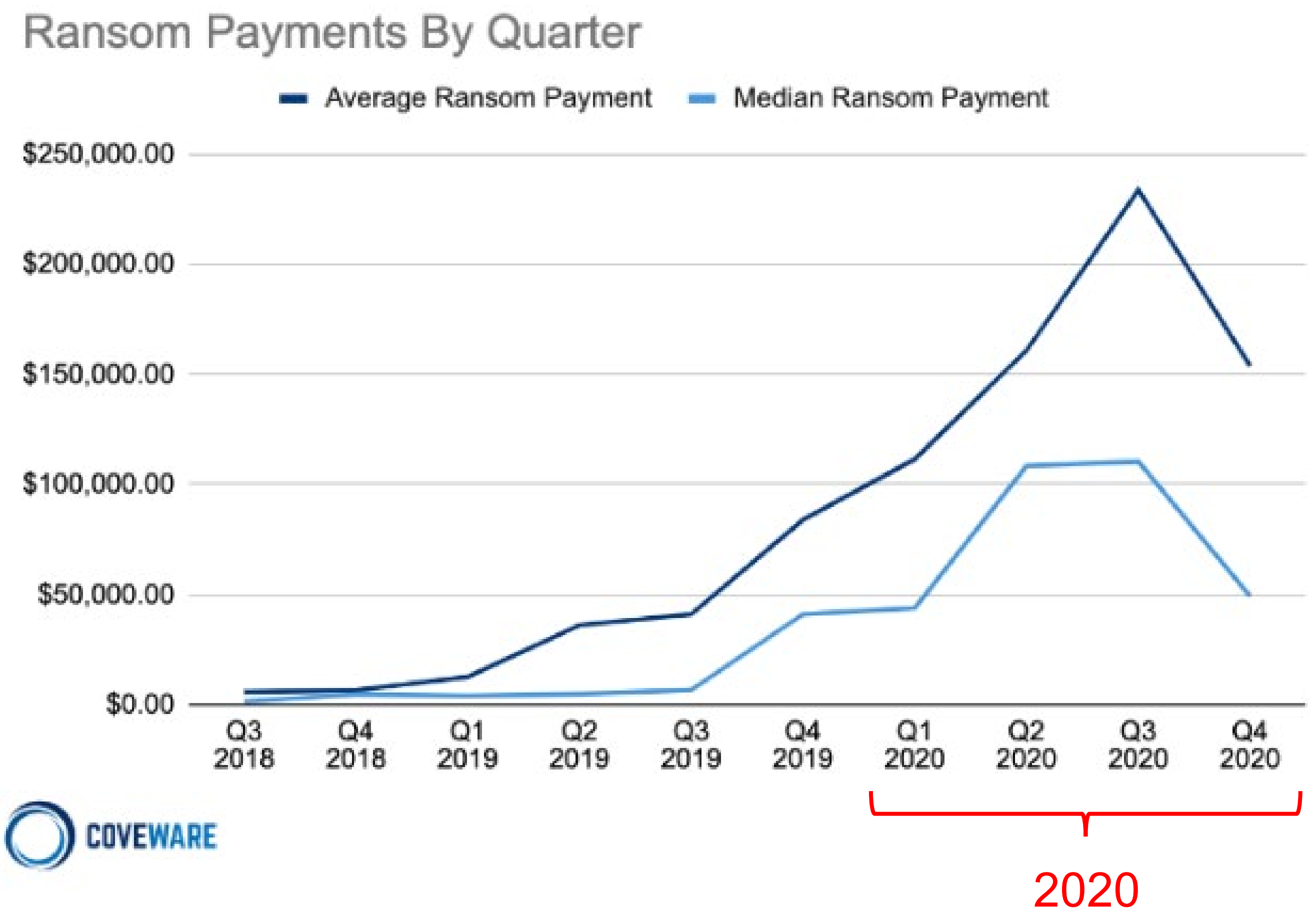
Rate of ransomware detections in 2020

Ransomware vs. Healthcare in 2020, Part 2

Noteworthy HPH ransomware targets:

- Fortune 500 Healthcare provider based out of Pennsylvania
  - 250 US hospitals lost use of their systems for 3 weeks
- Health network in Vermont
  - 5,000 systems disrupted
  - Furloughed 300 staff
  - Estimated costs at $1.5M/day
- May 2020: Coveware finds that ransomware causes an average of 15 days of downtime for EHRs
- Double-extortion expanded from exclusively Maze to 18 ransomware operators in 2020
- Ransomware statistics for 2020
  - 80 incidents (560 healthcare organizations impacted)
  - Ambulances were rerouted
  - Radiation treatments for cancer patients were delayed
  - Medical records were rendered temporarily inaccessible and, in some cases, permanently lost
  - Hundreds of staff were furloughed
  - On healthcare organization in Vermont furloughed 300 staff, estimated the cost at $1.5M/day
  - PHI and other sensitive data was stolen and published online in at least 12 incidents

Ransomware vs. Healthcare in 2020, Part 3



Average Ransom Payment

$154,108

-34% from Q3 2020

Median Ransom Payment

$49,450

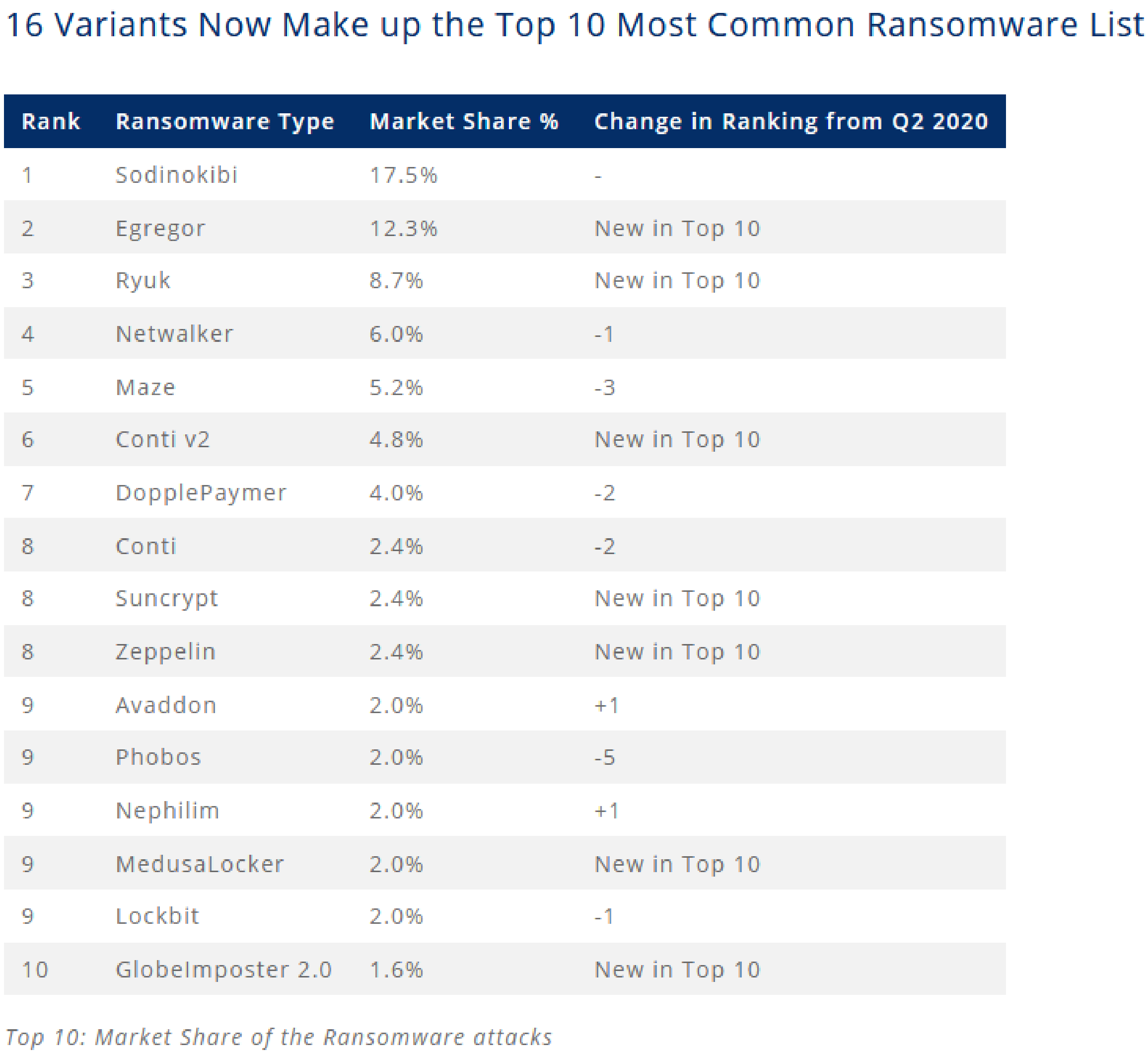
-55% from Q3 2020

COVEWARE

Ransomware vs. Healthcare in 2020, Part 4

The usual healthcare suspects:

- Sodinokibi/Revil
- Egregor (formerly Maze)
- Ryuk
- Netwalker
- Conti
- Dopplepaymer

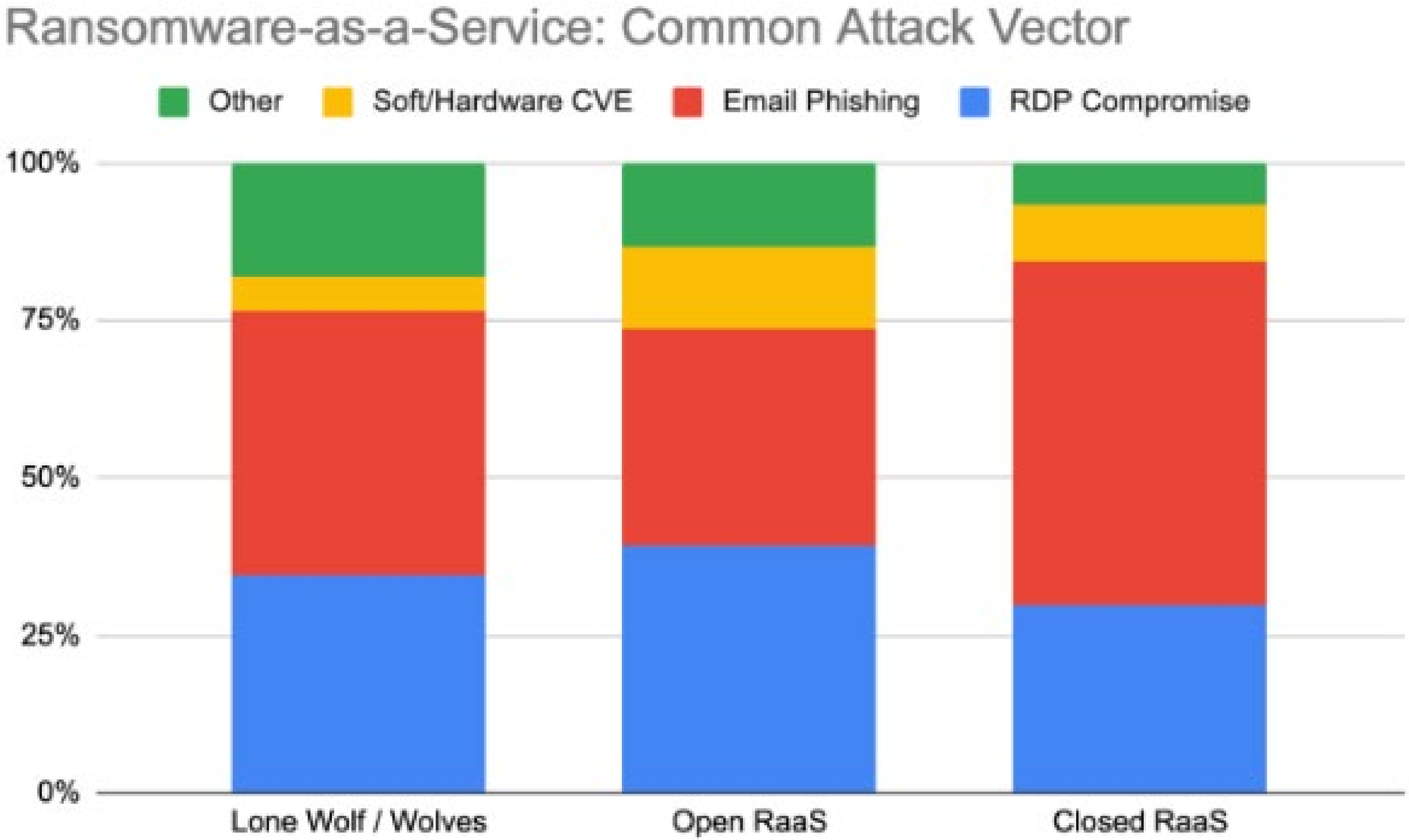


16 Variants Now Make up the Top 10 Most Common Ransomware List

Rank	Ransomware Type	Market Share %	Change in Ranking from Q2 2020
1	Sodinokibi	17.5%	-
2	Egregor	12.3%	New in Top 10
3	Ryuk	8.7%	New in Top 10
4	Netwalker	6.0%	-1
5	Maze	5.2%	-3
6	Conti v2	4.8%	New in Top 10
7	DopplePaymer	4.0%	-2
8	Conti	2.4%	-2
8	Suncrypt	2.4%	New in Top 10
8	Zeppelin	2.4%	New in Top 10
9	Avaddon	2.0%	+1
9	Phobos	2.0%	-5
9	Nephilim	2.0%	+1
9	MedusaLocker	2.0%	New in Top 10
9	Lockbit	2.0%	-1
10	GlobeImposter 2.0	1.6%	New in Top 10

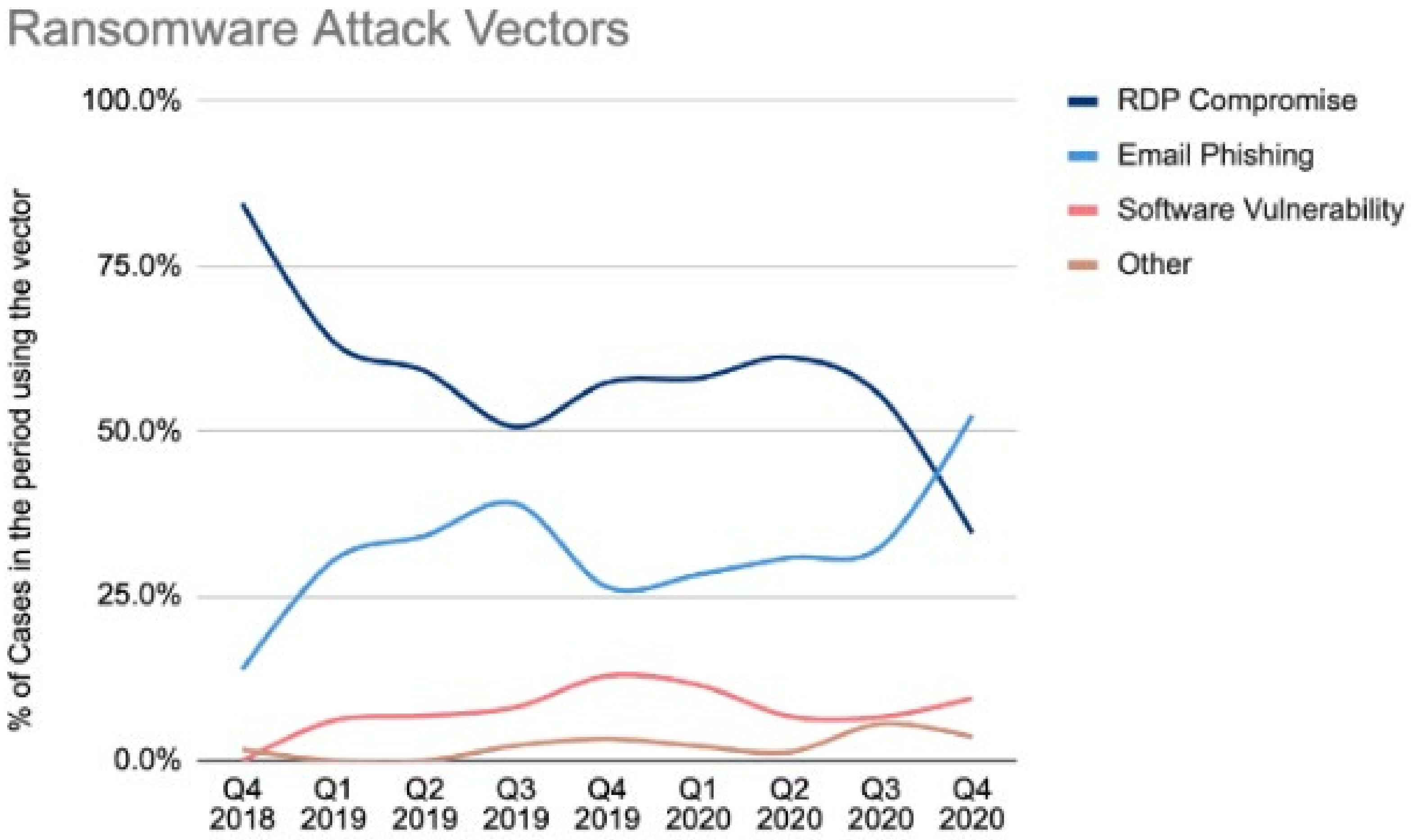
Top 10: Market Share of the Ransomware attacks

Ransomware vs. Healthcare in 2020, Part 5

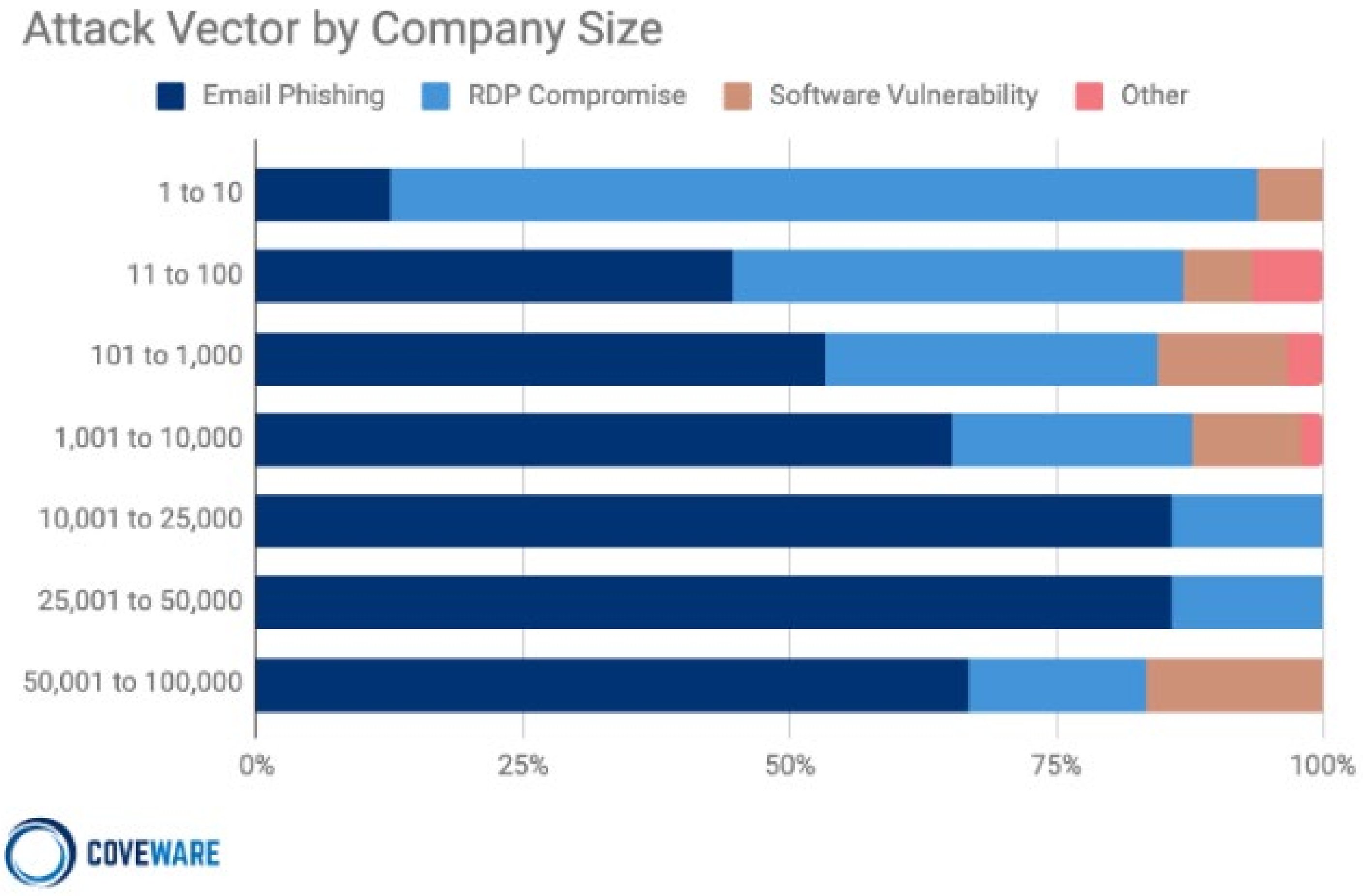


COVEWARE

Ransomware vs. Healthcare in 2020, Part 6

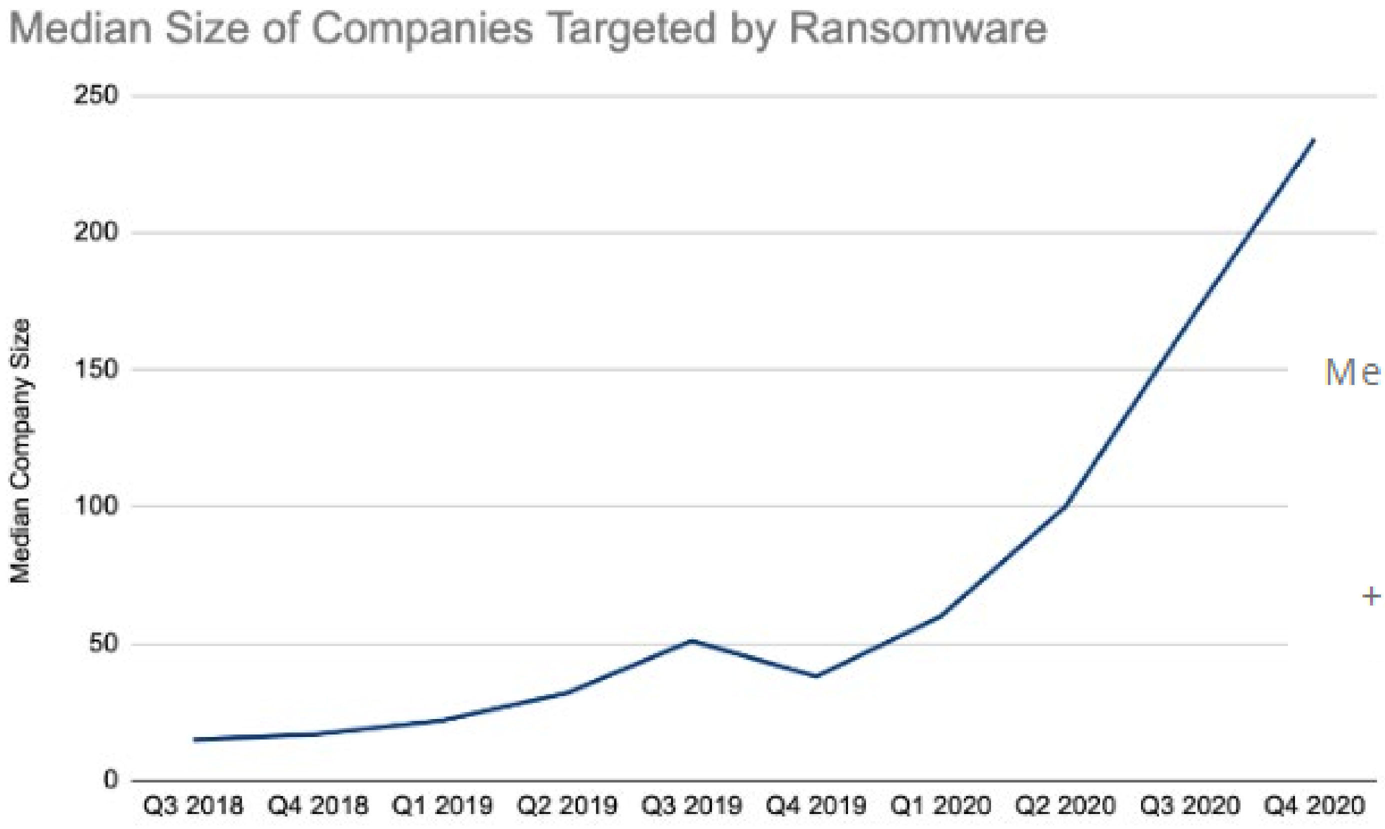


COVEWARE



Attack Vector by Company Size Q4,2020

Big game hunting:



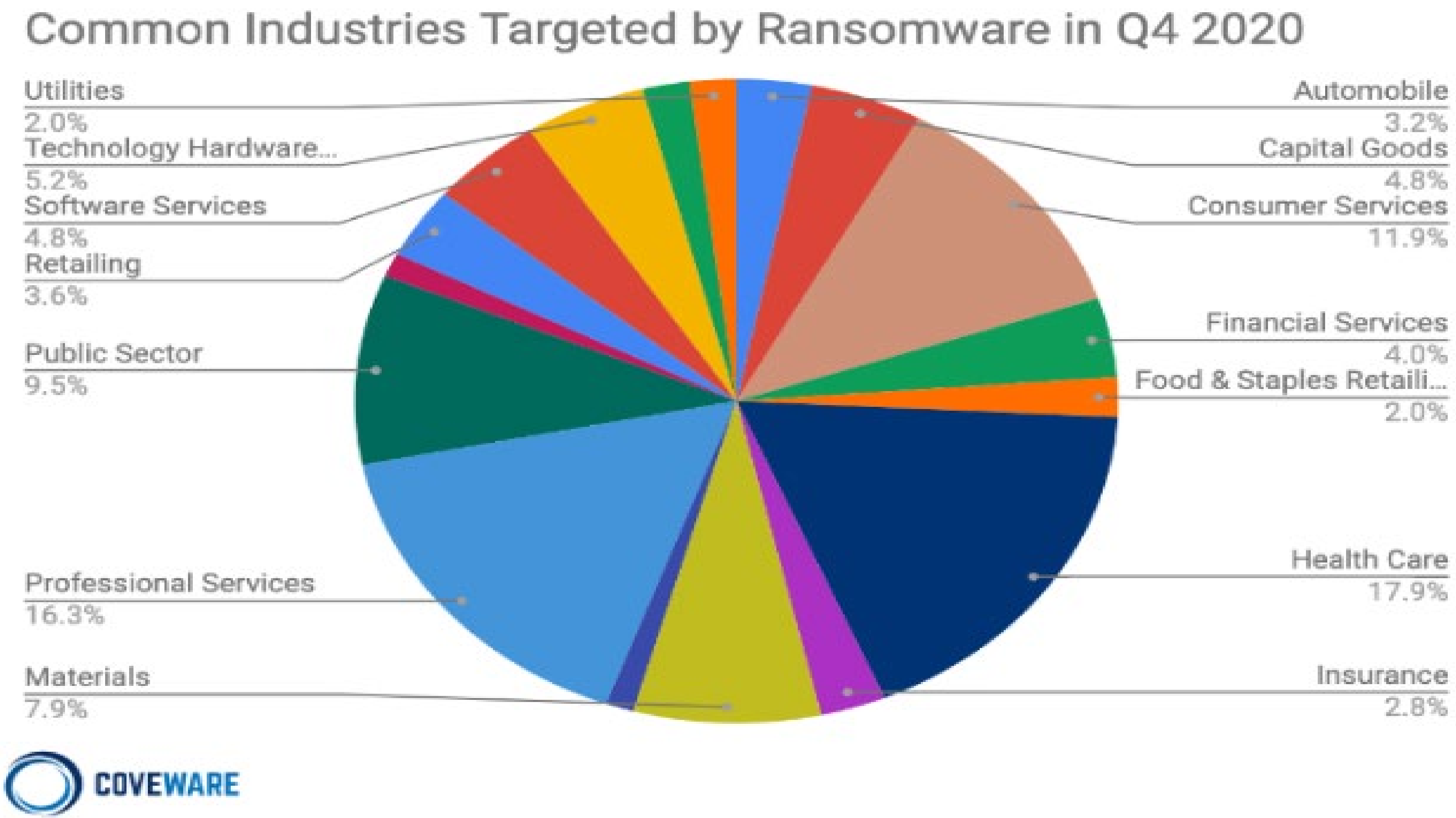
Median # of Employees

234

+39% from Q3 2020

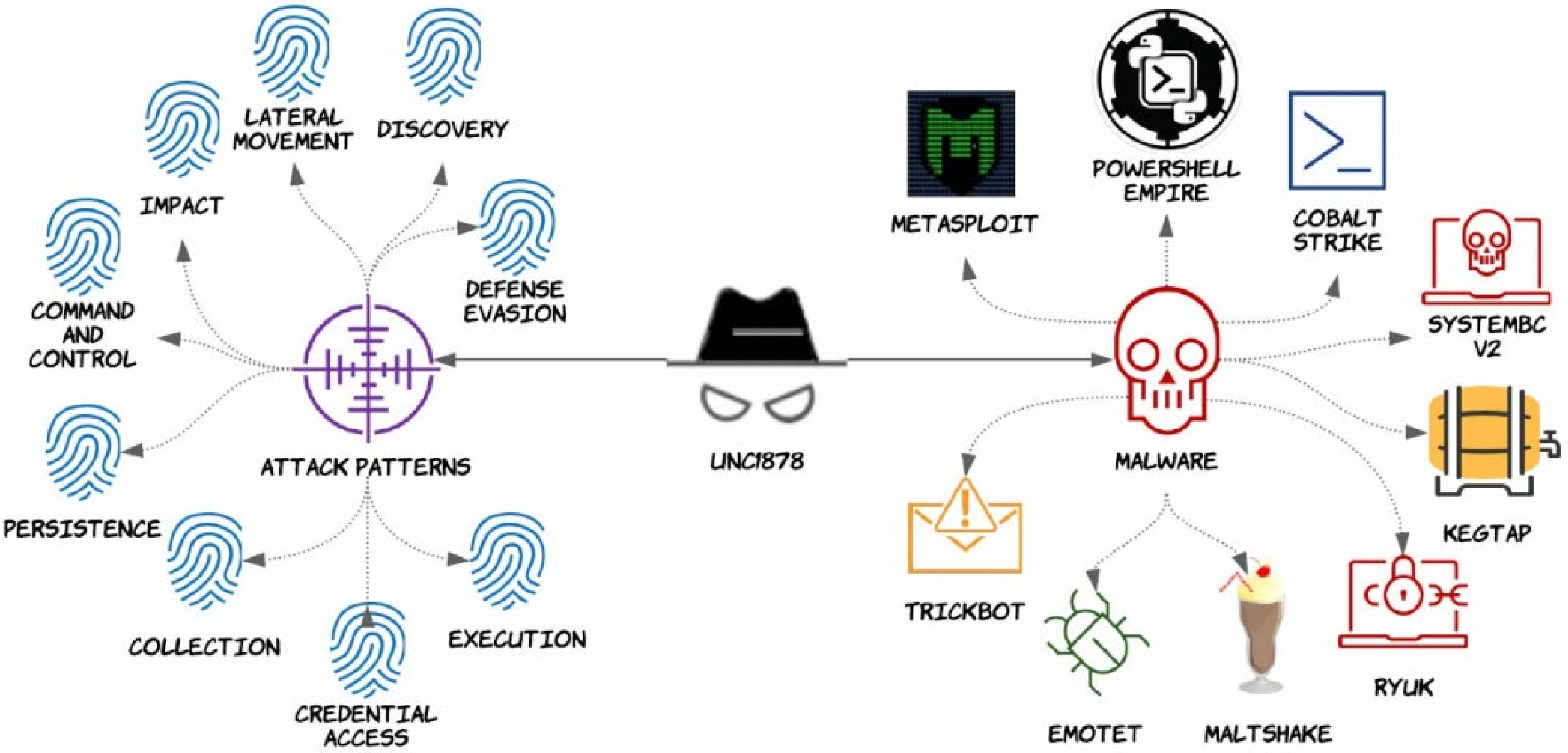
COVEWARE

Ransomware vs. Healthcare in 2020, Part 9


Common Industries Targeted by Ransomware in Q4 2020

Source: https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020

Ransomware vs. Healthcare in 2020, Part 10

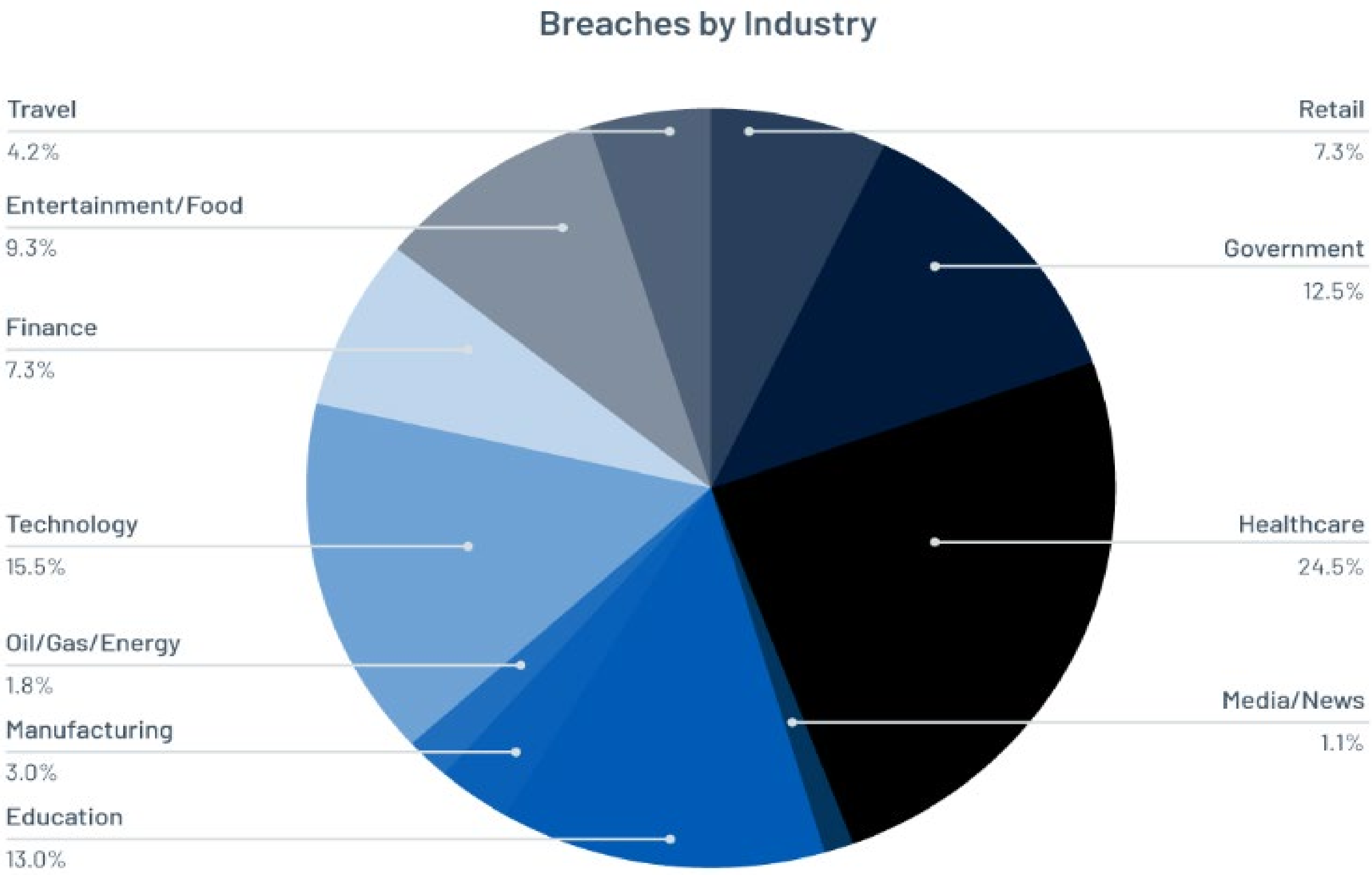


Carbon Black report: https://www.carbonblack.com/blog/tau-threat-advisory-imminent-ransomware-threat-to-u-s-healthcare-and-public-health-sector/

Data Breaches vs. Healthcare in 2020

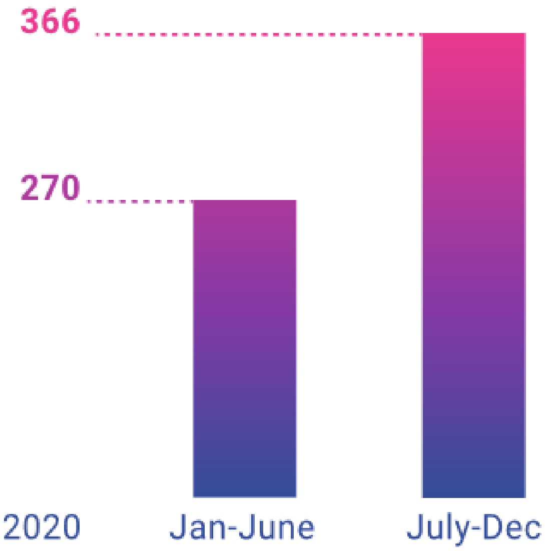
- In addition to ransomware attacks, data breaches are the other major plague to healthcare in cyberspace
  - These two attacks are often combined
- Ransomware attacks were responsible for almost 50% of all healthcare data breaches in 2020
  - 19 leakers/sites double extortion
- Healthcare is the most targeted sector for data breaches.
- CI Security 2020 data:
  - 630+ total healthcare organizational breaches
  - 29 million healthcare records breached

Data Breaches vs. Healthcare in 2020, Part 2



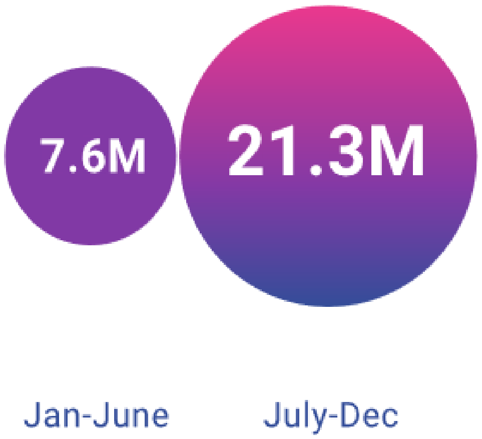
Data breaches vs. Healthcare in 2020, Part 3

Breach Reports



The total number of reported breaches among healthcare organizations increased by 36% from 270 in the first half of 2020 to 366 in the second half of the year.

Records Breached



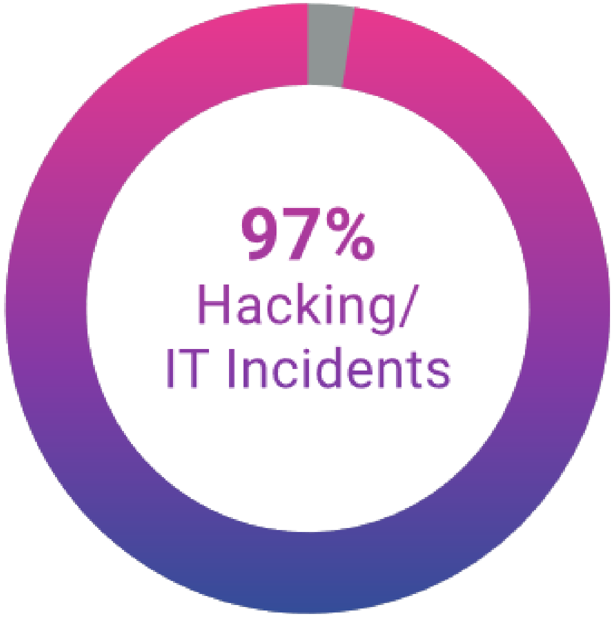
The number of individual patient records that were breached in the second half of 2020 nearly tripled compared to the first half of the year from 7,691,199 to 21,358,070.

Data Breaches vs. Healthcare in 2020, Part 4

Breaches: Cause and size

- The top eight breaches reported to the Department of Health and Human Services involved 500,000 records or more
  - Over 6.5 million records total were reported
- 75% of all records exposed in the second half of 2020 were due to compromised business associates.
- Specific types of healthcare organizations targeted:
  - Life science labs
  - Research labs
  - Rehabilitation facilities
  - Hospital systems
  - Generic healthcare organizations

Type of Breach



Of the 21.3 million records breached in the second half of 2020, 97% were attributed to malicious hacking incidents, rather than other causes such as unauthorized disclosure, improper disposal, theft, or loss.

Blackbaud: What Happened?

Who is Blackbaud?

- Managed IT services provider that serves nonprofits
- Based in South Carolina and is publicly traded
- Claims 25,000+ clients in 60+ countries
- Awards:
  - Forbes: Leading Employer for Diversity
  - Fortune: 56 Companies Changing the World
  - IDC: Top 40 Global Cloud Software Service Providers

What are the details of the attack?

- It was disclosed on July 16, 2020 that they were the victim of an unnamed ransomware attack, and they had paid the ransom.
- Confirmed attackers were able to gain access to some customers' unencrypted banking information, login credentials, and social security numbers.
- In November 2020, they confirmed they had been named as a defendant in 23 putative class suits.
- They have received over 160 claims related to the attack.
- 200 organizations (many in the healthcare sector) and millions of individuals have been impacted.

Healthcare Organizations Impacted by Blackbaud

- A sample set of compromised healthcare organizations is on the right. This list does not represent every healthcare organization impacted by Blackbaud.
- It is believed that about 10 million records were breached.
- Some of these are subject to change as updated information becomes available.
- Blackbaud had to spend over $3 million to deal with the attack's aftermath between July and September 2020, and it also recorded almost $3 million in accrued insurance recoveries during the same time period.

Organization Name	Records breached
Medical center in Kansas	315,811
Hospital in Michigan	52,711
Hospital in Michigan	95,000
Hospital in North Carolina	Unknown
Hospital in California	39,881
Healthcare provider in Ohio	118,874
Health center in Pennsylvania	3,320,726
Healthcare network in Virginia	1,045,270
Health service provider in Maine	657,392
Health service provider in Washington State	300,000
Health service provider in Pennsylvania	60,595
Healthcare providers in Illinois	55,983

COVID-19 as a Cyberattack Theme

"…the COVID-19 pandemic provides criminal opportunities on a scale likely to dwarf anything seen before. The speed at which criminals are devising and executing their schemes is truly breathtaking."

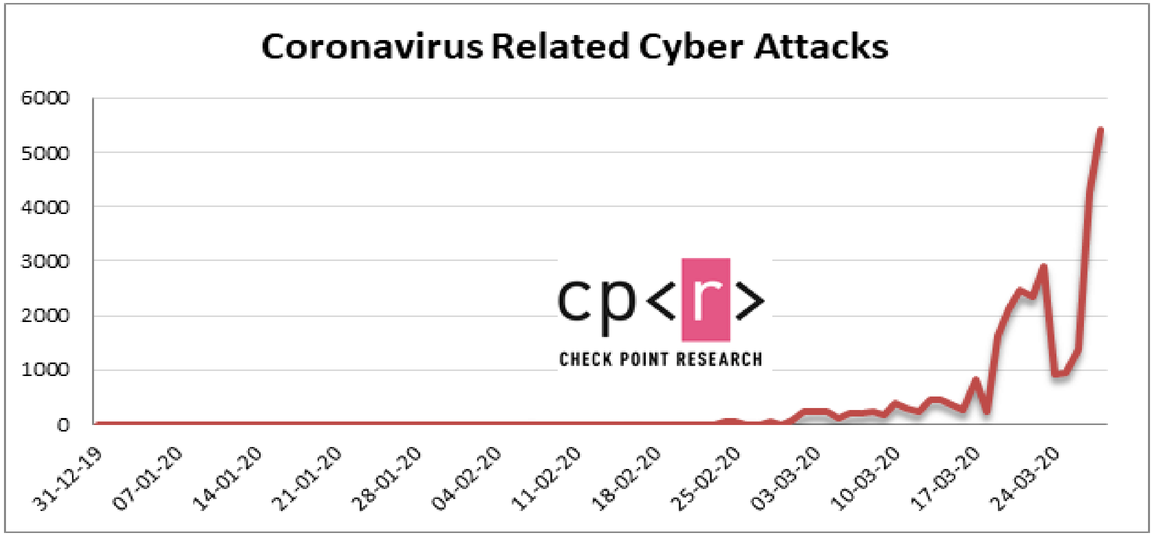
- Michael D'Ambrosio, Head of the U.S. Secret Service Office of Investigations

Terry Wade, lead of the Federal Bureau of Investigation Criminal, Cyber, Response and Services Branch.

WashingtonPost.com, April 14, 2020

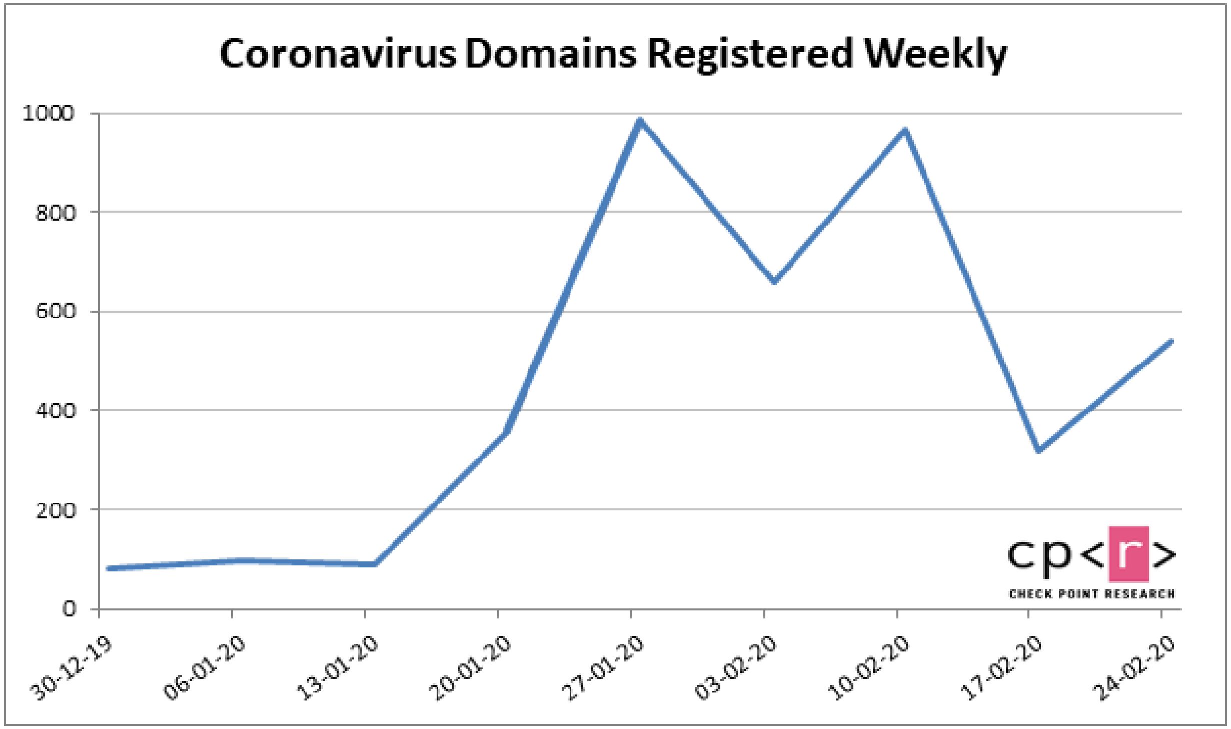
"...the risk to this sector will be elevated throughout this crisis."

- FireEye, as part of an analysis of cyber threats to the healthcare industry during the coronavirus pandemic



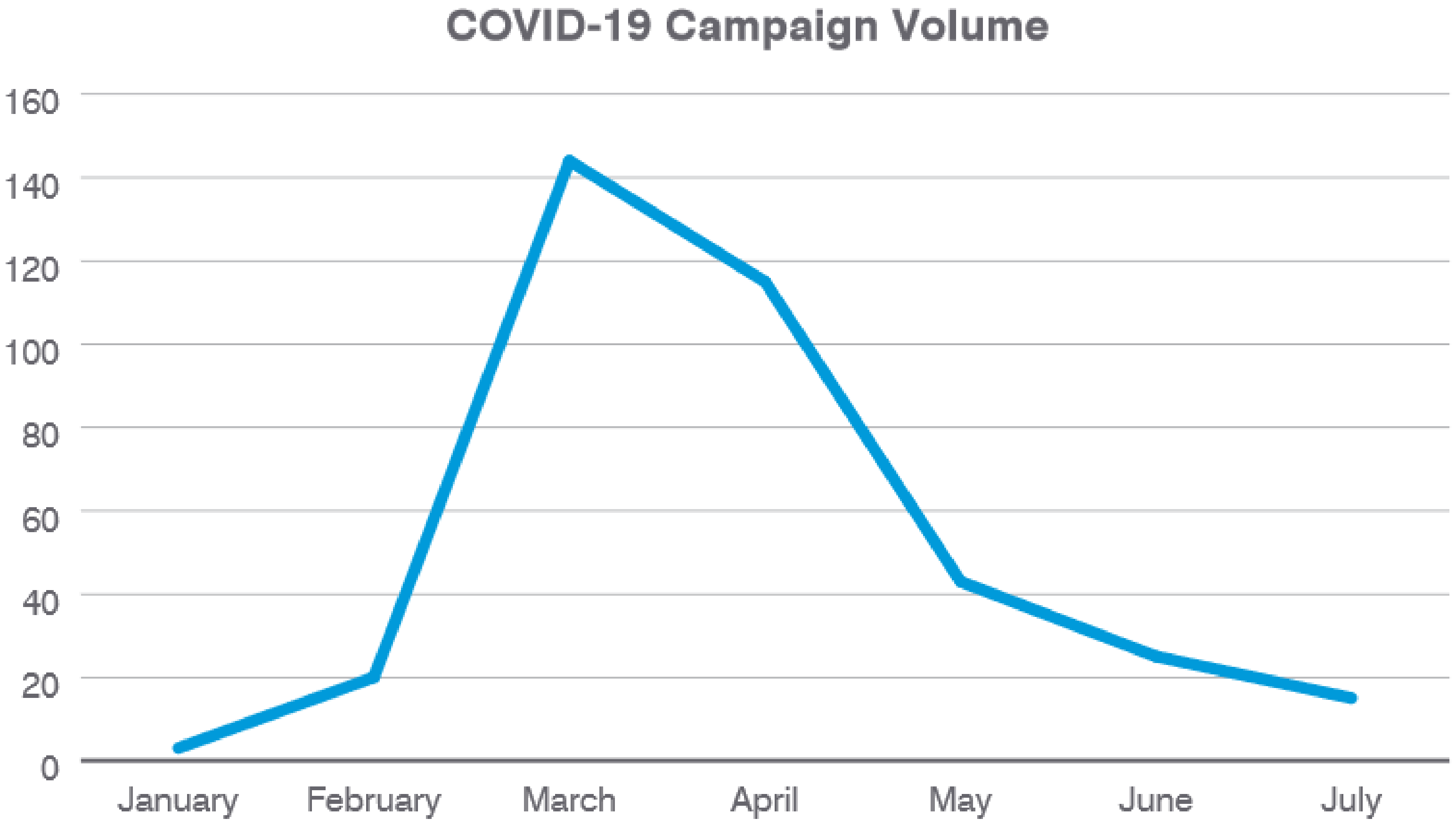
COVID-19 as a Cyberattack Theme, Part 2

- In many cases, these domains will host malware. The attack vector can be any number of options, such as phishing, watering-hole attacks and typosquatting.
- According to Checkpoint, new coronavirus-related domains are being registered at very high rates, and many of them are malicious.
  - Over 4,000 coronavirus-related domains registered in January and February 2020.
  - Coronavirus-themed domains are 50% more likely to be malicious compared to other domains.
  - Over 6,000 coronavirus-related domains were registered in the third week of March 2020.



SolarWinds – Who Was Impacted?

Coronavirus-themed campaign volume (Jan – July 2020):

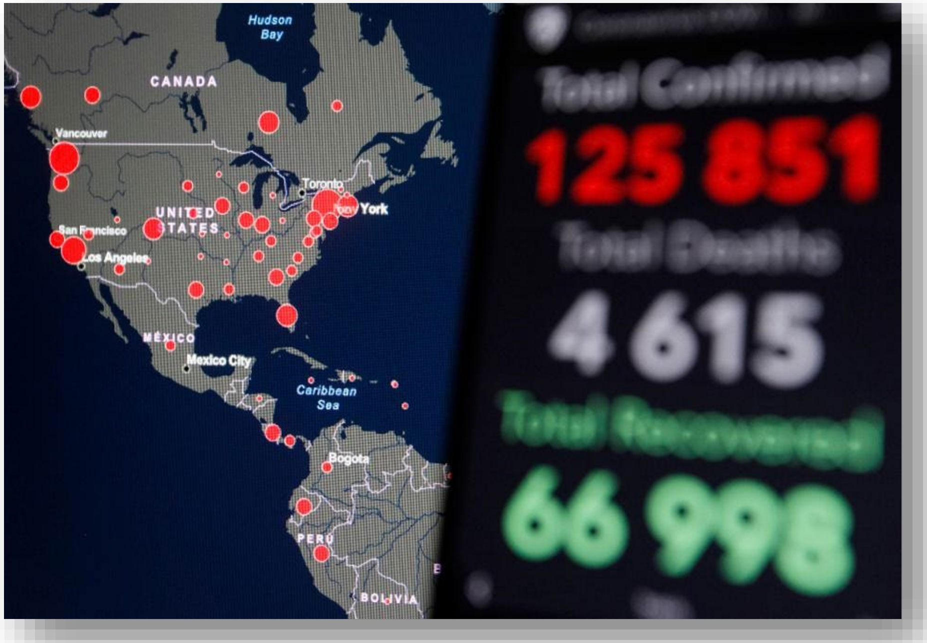


Proof Point report: https://www.proofpoint.com/sites/default/files/e-books/pfpt-us-tr-healthcare-report.pdf

COVID-19 as a Cyberattack Theme, Part 3

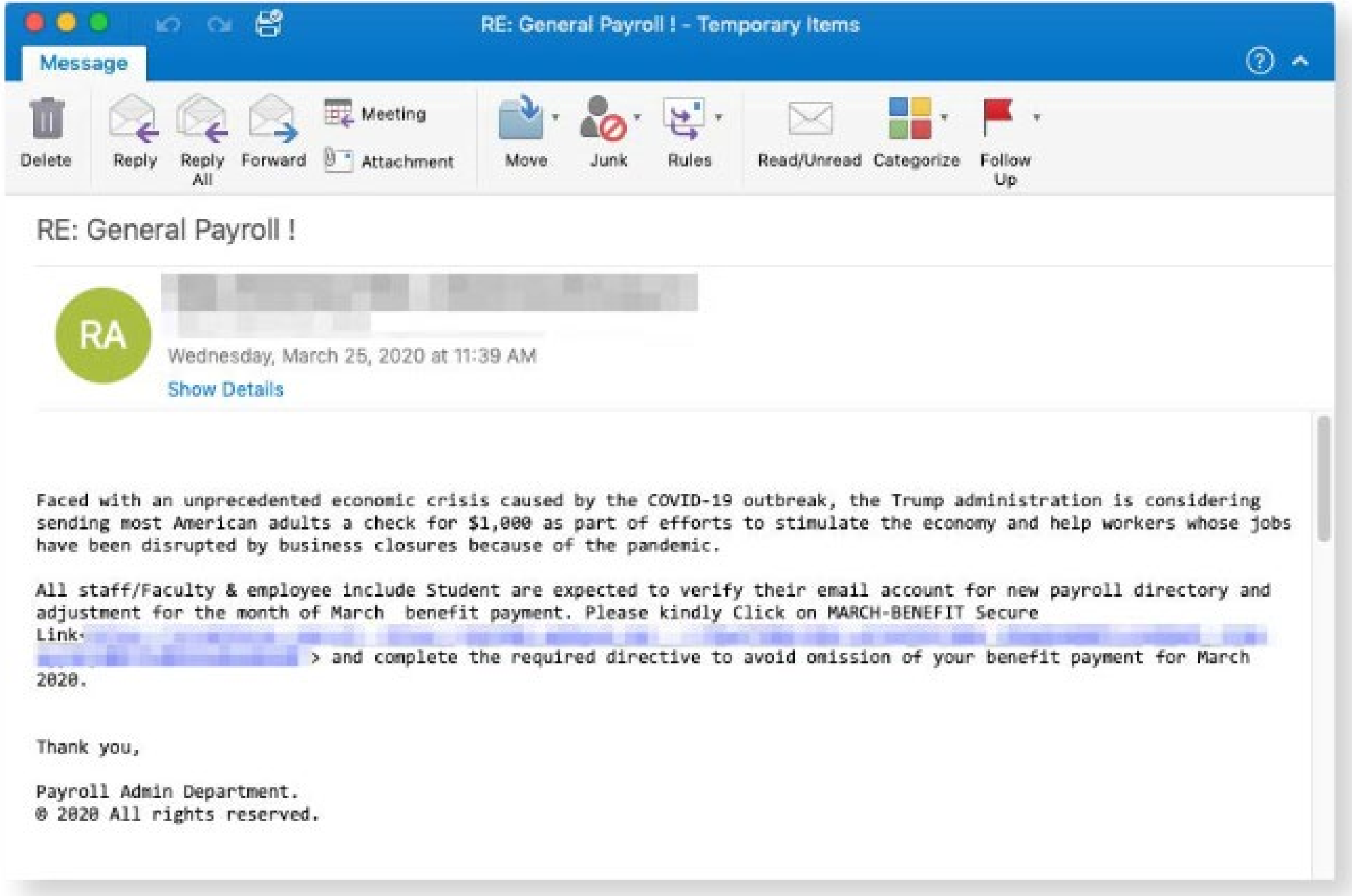
As the coronavirus/COVID-19 pandemic spread, several real-time infection maps were created:

- Johns Hopkins University
  - https://coronavirus.jhu.edu/map.html
- World Health Organization
  - https://who.sprinklr.com/
- Kaiser Family Foundation
  - https://www.kff.org/global-health-policy/fact-sheet/coronavirus-tracker/
- HealthMap
  - https://www.healthmap.org/covid-19/
- SharedGe0
  - https://uscovid-19map.org/
- Microsoft Bing:
  - https://www.bing.com/covid
- University of Washington
  - https://hgis.uw.edu/virus/



COVID-19 as a Cyberattack Theme, Part 4

Cares Act (COVID-19 relief bill) payroll lure:



RE: General Payroll !

[redacted]

Wednesday, March 25, 2020 at 11:39 AM

Faced with an unprecedented economic crisis caused by the COVID-19 outbreak, the Trump administration is considering sending most American adults a check for $1,000 as part of efforts to stimulate the economy and help workers whose jobs have been disrupted by business closures because of the pandemic.

All staff/Faculty & employee include Student are expected to verify their email account for new payroll directory and adjustment for the month of March benefit payment. Please kindly Click on MARCH-BENEFIT Secure Link< [redacted] > and complete the required directive to avoid omission of your benefit payment for March 2020.

Thank you,

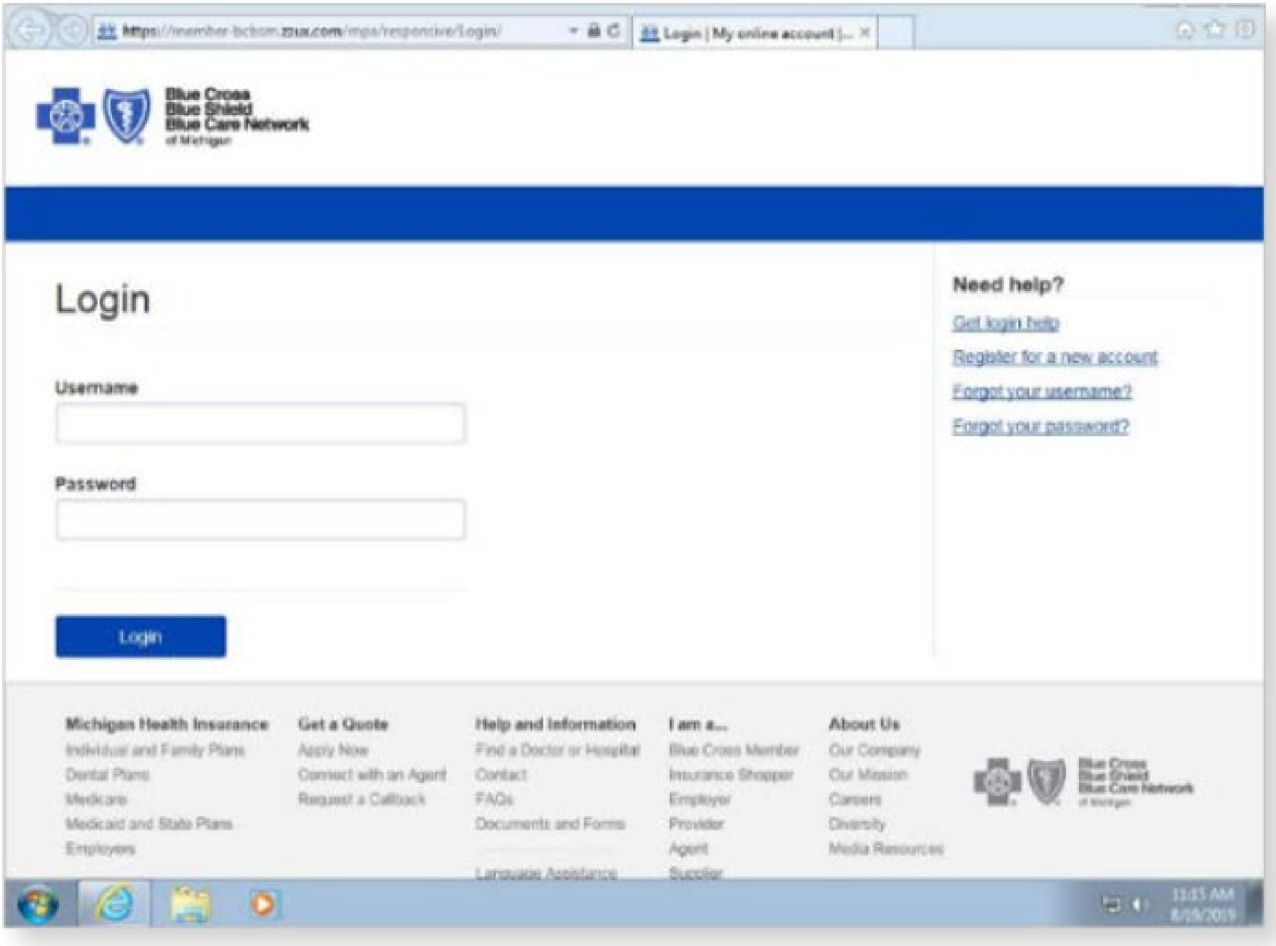
Payroll Admin Department.
© 2020 All rights reserved.

Proof Point report: https://www.proofpoint.com/sites/default/files/e-books/pfpt-us-tr-healthcare-report.pdf

Image source: ProofPoint

Other Healthcare-Related Fraud

Cloned portal mimicking an insurer:



https://member-bcbsm.zuux.com/mpa/responsive/Login/

Login | My online account |...

Blue Cross Blue Shield Blue Care Network of Michigan

Login

Username

Password

Login

Need help?

Get login help

Register for a new account

Forgot your username?

Forgot your password?

Michigan Health Insurance

Individual and Family Plans

Dental Plans

Medicare

Medicaid and State Plans

Employers

Get a Quote

Apply Now

Connect with an Agent

Request a Callback

Help and Information

Find a Doctor or Hospital

Contact

FAQs

Documents and Forms

Language Assistance

I am a...

Blue Cross Member

Insurance Shopper

Employer

Provider

Agent

Supplier

About Us

Our Company

Our Mission

Careers

Diversity

Media Resources

Blue Cross Blue Shield Blue Care Network of Michigan

11:15 AM 8/19/2019

Proof Point report: https://www.proofpoint.com/sites/default/files/e-books/pfpt-us-tr-healthcare-report.pdf

The top 5G capabilities that will apply to healthcare:

- Speed
- Capacity/hyperconnectivity
- Low latency
- Massive device connectivity
- Data-driven insights

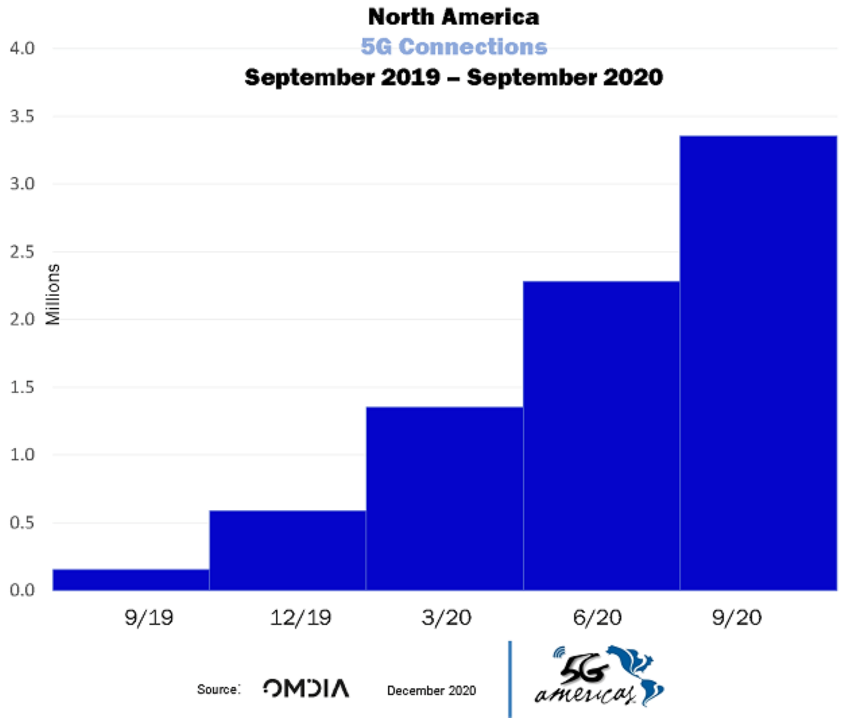
“Healthcare will benefit from 5G technology from countless aspects; it is basically the field that might experience the most changes.” - The Medical Futurist

Healthcare benefits from 5G:

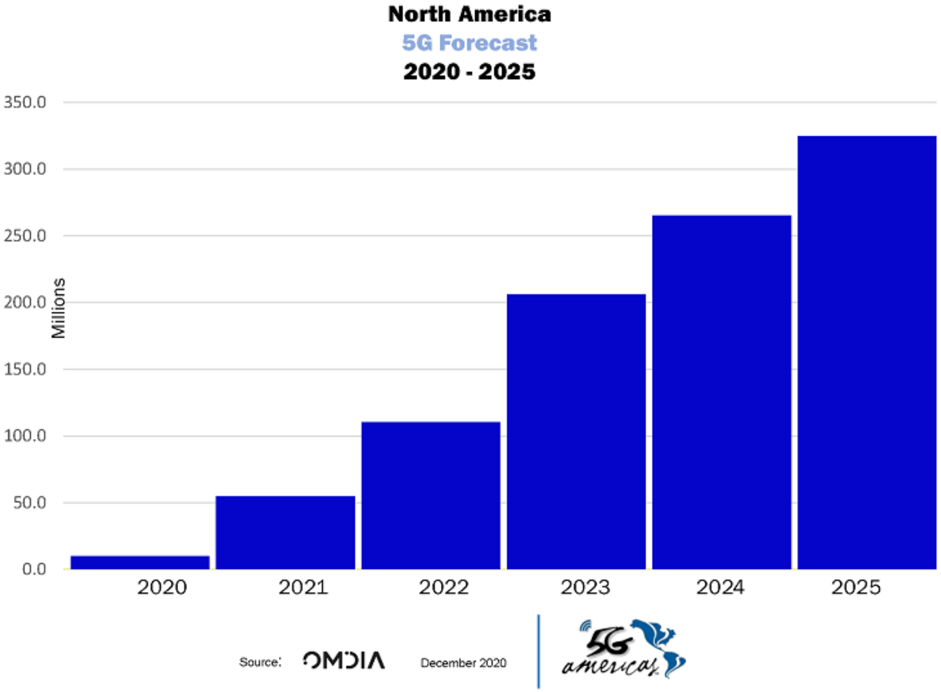
- Telehealth/telemedicine
- Remote patient monitoring
- Augmented/virtual reality
- Large file transfers
- Data analysis

5G and Healthcare Security in 2020, cont.

5G Implementation in 2020 (and Beyond)



Source: OMDIA December 2020 | 5G americas



Source: OMDIA December 2020 | 5G americas

Internet of Medical Things and Healthcare Security in 2020

- Wearables and Internet of Medical Things (IoMT):
  - Transmit real-time patient health data to doctors (remote patient monitoring)
  - According to Anthem, 86% of doctors say they increase patient engagement with their own health
  - Predicted to decrease hospital costs by 16% in the next five years
  - The market for IoMT generally, and wearables specifically, is expected to increase significantly – it's already happening!
- U.S. IoMT market:
  - $70B in 2020
  - Predicted to be $190B by 2025

What to Do About These Threats

Where you can go for guidance on these issues:

- **Health Care Industry Cybersecurity Task Force Resource Catalog**
  https://www.phe.gov/Preparedness/planning/CyberTF/Documents/hccs-tf-resource-catalog.pdf
- **Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM)**
  https://healthsectorcouncil.org/hic-scrim-v2/
- **Health Industry Cybersecurity Protection of Innovation Capital (HIC-PIC)**
  https://healthsectorcouncil.org/hic-pic/
- **Medical Device and Health IT Joint Security Plan**
  https://healthsectorcouncil.org/wp-content/uploads/2019/01/HSCC-MEDTECH-JSP-v1.pdf
- **Joint Cybersecurity Advisory - Ransomware Activity Targeting the Healthcare and Public Health Sector**
  https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf
- **Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients**
  https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf
- **FBI – Ransomware**
  https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware
- **HHS: FAQs on Telehealth and HIPAA during theC OVID-19 nationwide public health emergency**
  https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf
- **Must-Have Telehealth, Remote Work Privacy and Security for COVID-19**
  https://healthitsecurity.com/news/must-have-telehealth-remote-work-privacy-and-security-for-covid-19

Reference Materials

References

- ProofPoint 2020 Healthcare Threat Landscape report https://www.proofpoint.com/sites/default/files/e-books/pfpt-us-tr-healthcare-report.pdf
- 2020 MID-YEAR Horizon Report The State of Cybersecurity in Healthcare https://fortifiedhealthsecurity.com/wp-content/uploads/2020/07/Fortified-2020-Mid-Year-Horizon-Report-Digital.pdf
- The State of Healthcare Cybersecurity: VMware Carbon Black Explores the Surge in Cyber Threats https://www.carbonblack.com/blog/the-state-of-healthcare-cybersecurity/
- Hospitals Suffer New Wave of Hacking Attempts https://www.wsj.com/articles/hospitals-suffer-new-wave-of-hacking-attempts-11612261802 v
- VMWare Carbon Black Explores the State of Healthcare Cybersecurity in 2020 https://www.hipaajournal.com/vmware-carbon-black-explores-the-state-of-healthcare-cybersecurity-in-2020/
- The State of Ransomware in the US: Report and Statistics 2020 https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/
- 70% Ransomware Attacks Cause Data Exfiltration; Phishing Top Entry Point https://healthitsecurity.com/news/70-ransomware-attacks-cause-data-exfiltration-phishing-top-entry-point
- Top Healthcare Cybersecurity Resources from NIST, HHS, OCR, HSCC https://healthitsecurity.com/news/top-healthcare-cybersecurity-resources-from-nist-hhs-ocr-hscc
- ESET Threat Report Q4 2020 https://www.welivesecurity.com/wp-content/uploads/2021/02/ESET_Threat_Report_Q42020.pdf
- Fueled by Profits, Ransomware Persists in New Year https://www.bankinfosecurity.com/fueled-by-profits-ransomware-persists-in-new-year-a-15818

References

- Tenable 2020 Threat Landscape Retrospective https://static.tenable.com/marketing/research-reports/Research-%20Report-Threat_Landscape_2020.pdf
- Ransomware tactics are changing up a gear in 2021 https://techhq.com/2021/01/ransomware-tactics-are-changing-up-a-gear-in-2021/
- Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report
- Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020

Questions

Upcoming Briefs

- Securing SSL/TLS 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 HC3@HHS.GOV.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday between 9am-5pm (EST) at **202-691-2110.**

Health Sector Cybersecurity Coordination Center (HC3) Background

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directs communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, and general notifications to the HPH about currently impacting threats via the HHS OIG.

White Papers

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

Threat Briefings & Webinar

Briefing document and presentation that provides 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.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV, or call us Monday-Friday between 9am-5pm (EST) at **202-691-2110.**

Questions

Contact

Health Sector Cybersecurity Coordination Center (HC3)

202-691-2110

HC3@HHS.GOV