LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Cyberthreats to Biotechnology

03/18/2021

Report #: 202003181030

Agenda

Image source: CSO Online

- HC3 Mission and Core Functions
- Vulnerability points in healthcare organizations
- Cyberattacks – Attack vectors and phishing
- Cyberattacks – Ransomware
- Cyberattacks – Data Breaches
- Healthcare Cybersecurity Data from 2020
- Access Control
- Physical Security for Covid-19 Vaccines
- Case Studies
- Resources
- References
- Questions

Slides Key:

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

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

Common Attack Points for a Healthcare Organization

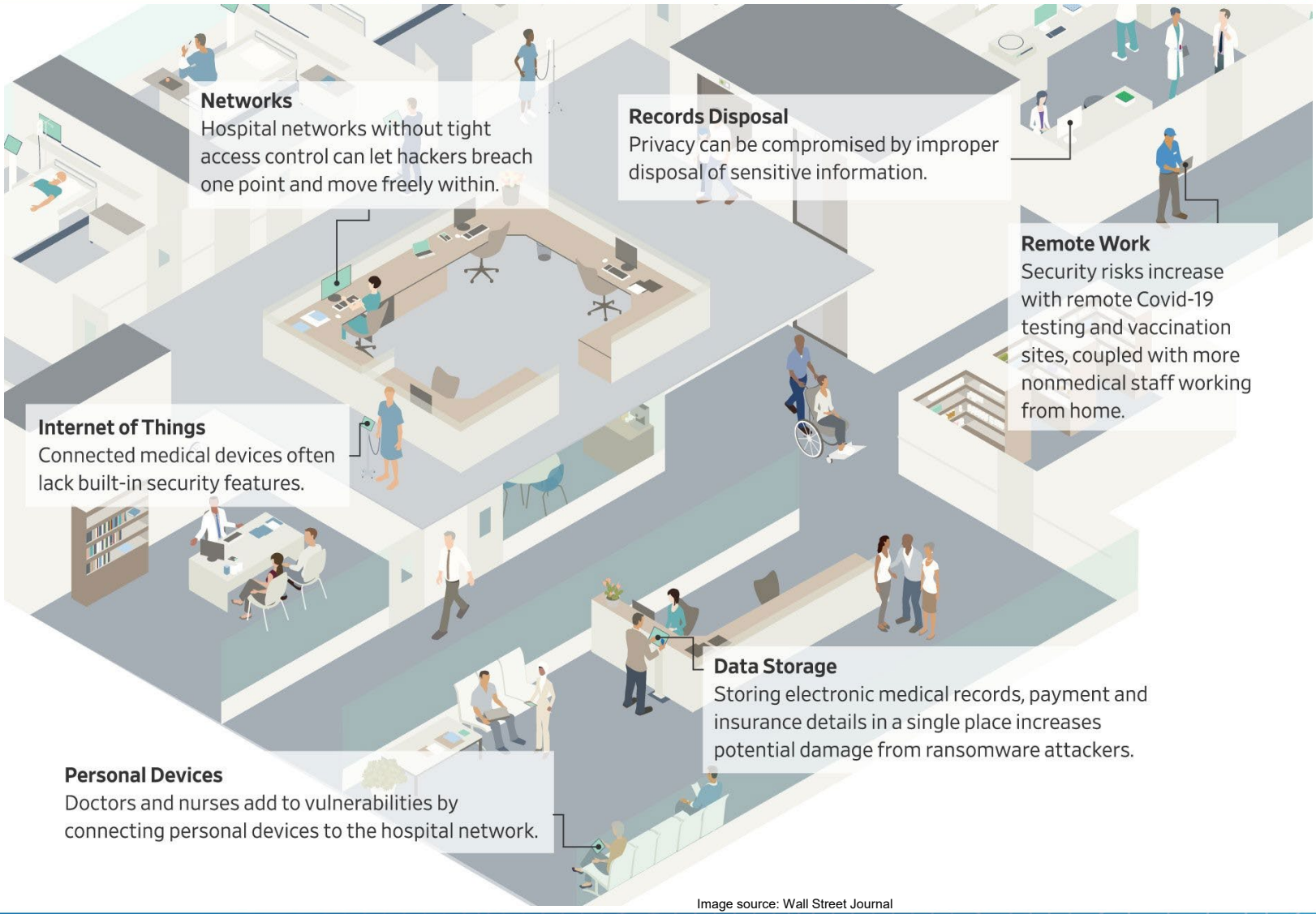


Image source: Wall Street Journal

How does a cyberattack begin? How is infrastructure initially penetrated?

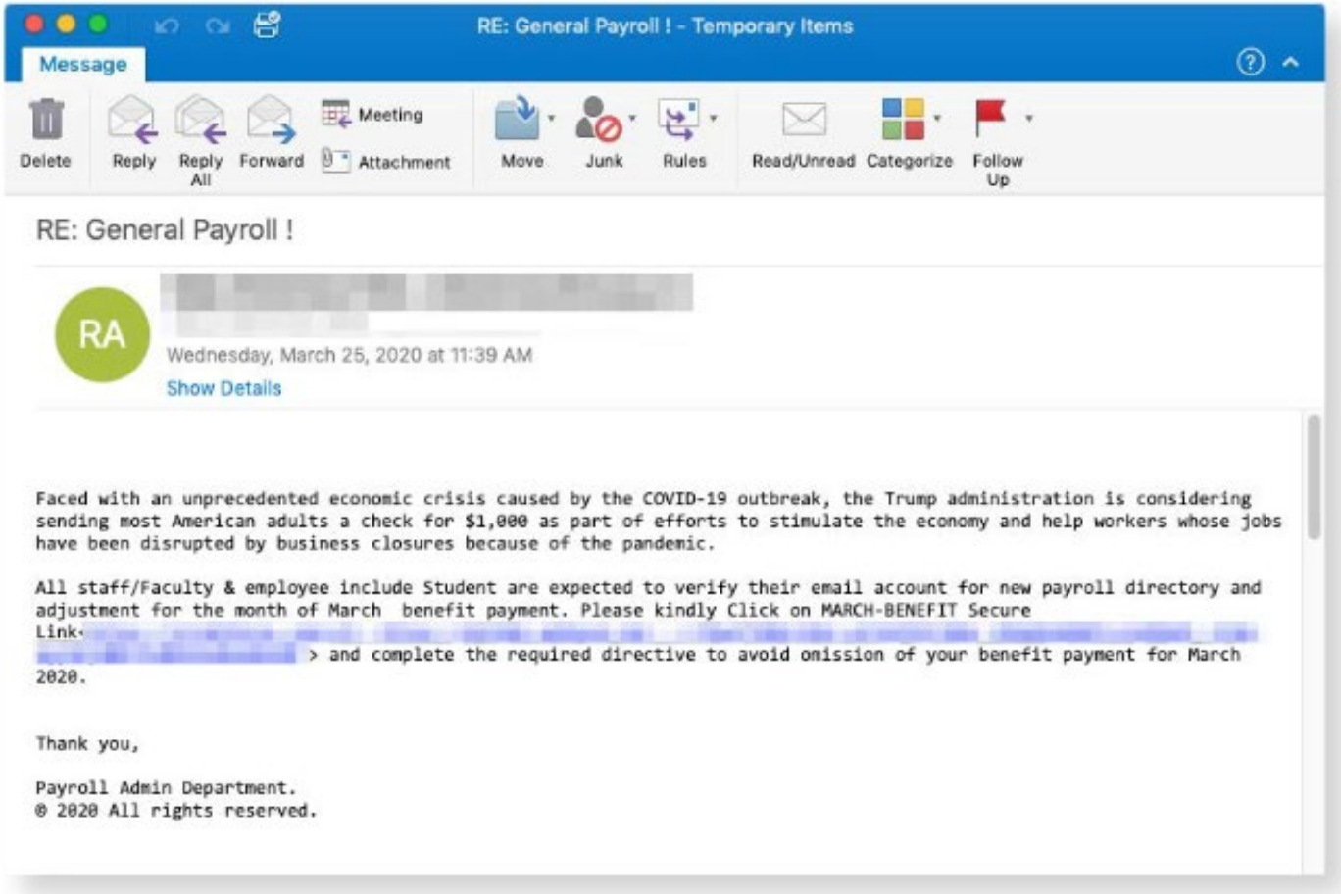
- The attack vector

What are the more common types of attack vectors?

- **Phishing** – A social engineering attack using a fake e-mail, *often with a theme*, to elicit interaction (clicking a link or opening an attachment) to deposit malware on the target system.
- **Remote Desktop Protocol (RDP)** – RDP is a protocol that is used for legitimate administrative access to a network. It is often exploited by cyberattackers.
- **Software/application/hardware vulnerabilities** – New vulnerabilities are constantly being discovered and patched. They are also exploited before they are patched.
- **Watering hole attacks (poisoned websites)** – Malicious websites can contain malware which is deposited on the system of anyone who surfs to the website.

Phishing example: COVID-19 theme

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



Phishing example: COVID-19 theme, Part 2

Re:SAFTY CORONA VIRUS AWARENESS WHO

WO World Health Organization

World Health Organization

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

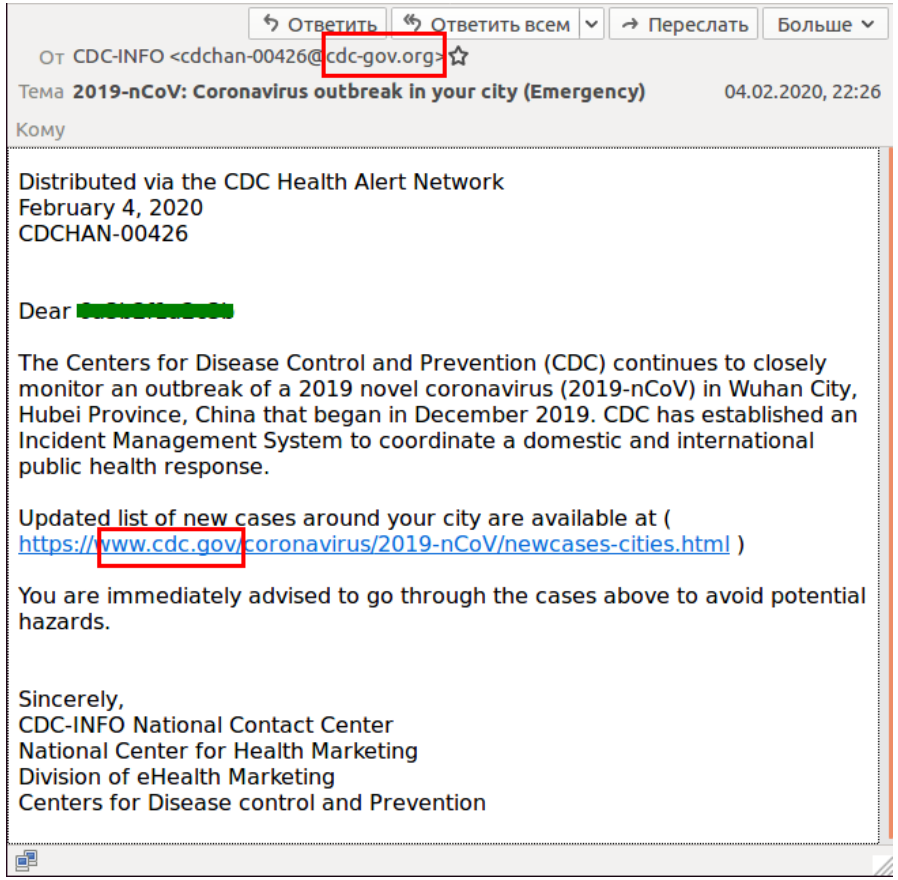
Safety measures

Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong
Specialist wuhan-virus-advisory

FAKE



Ответить | Ответить всем | Переслать | Больше

От CDC-INFO <cdchan-00426@cdc-gov.org>

Тема **2019-nCoV: Coronavirus outbreak in your city (Emergency)** 04.02.2020, 22:26

Кому

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

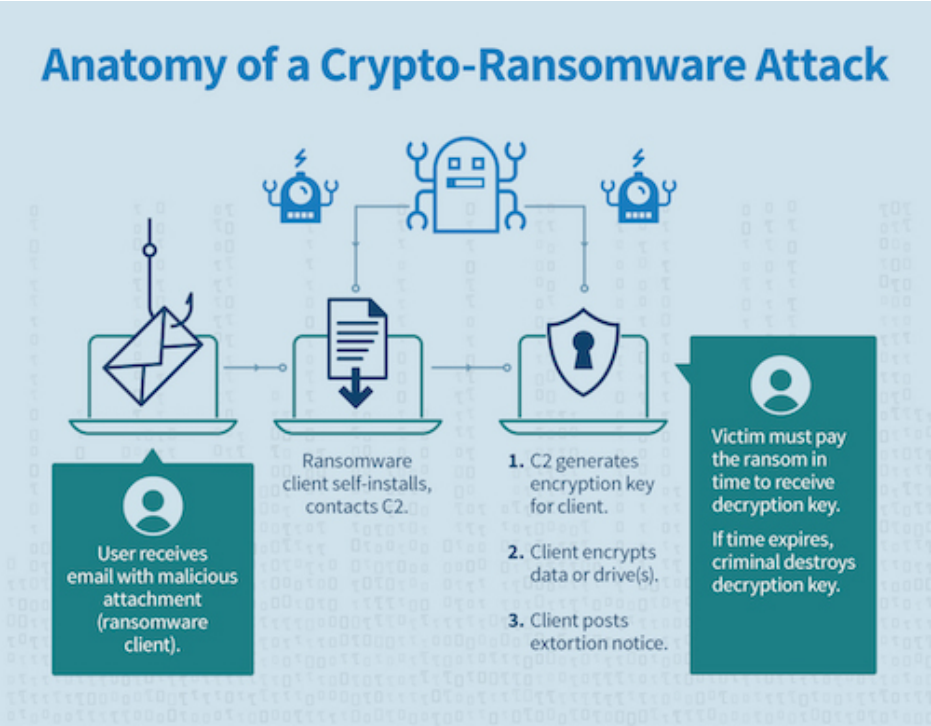
Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

What is the purpose of ransomware?

- Used by cybercriminals as a form of a denial-of-service attack
- Demands cryptocurrency payment in return for restoration of access

How does ransomware work?

1. Attack vector (usually phishing or Remote Desktop Protocol compromise)
2. Victim system reaches out to command-and-control server to download ransomware
3. Ransomware is executed on victim system(s)
4. Ransom note is left on victim system

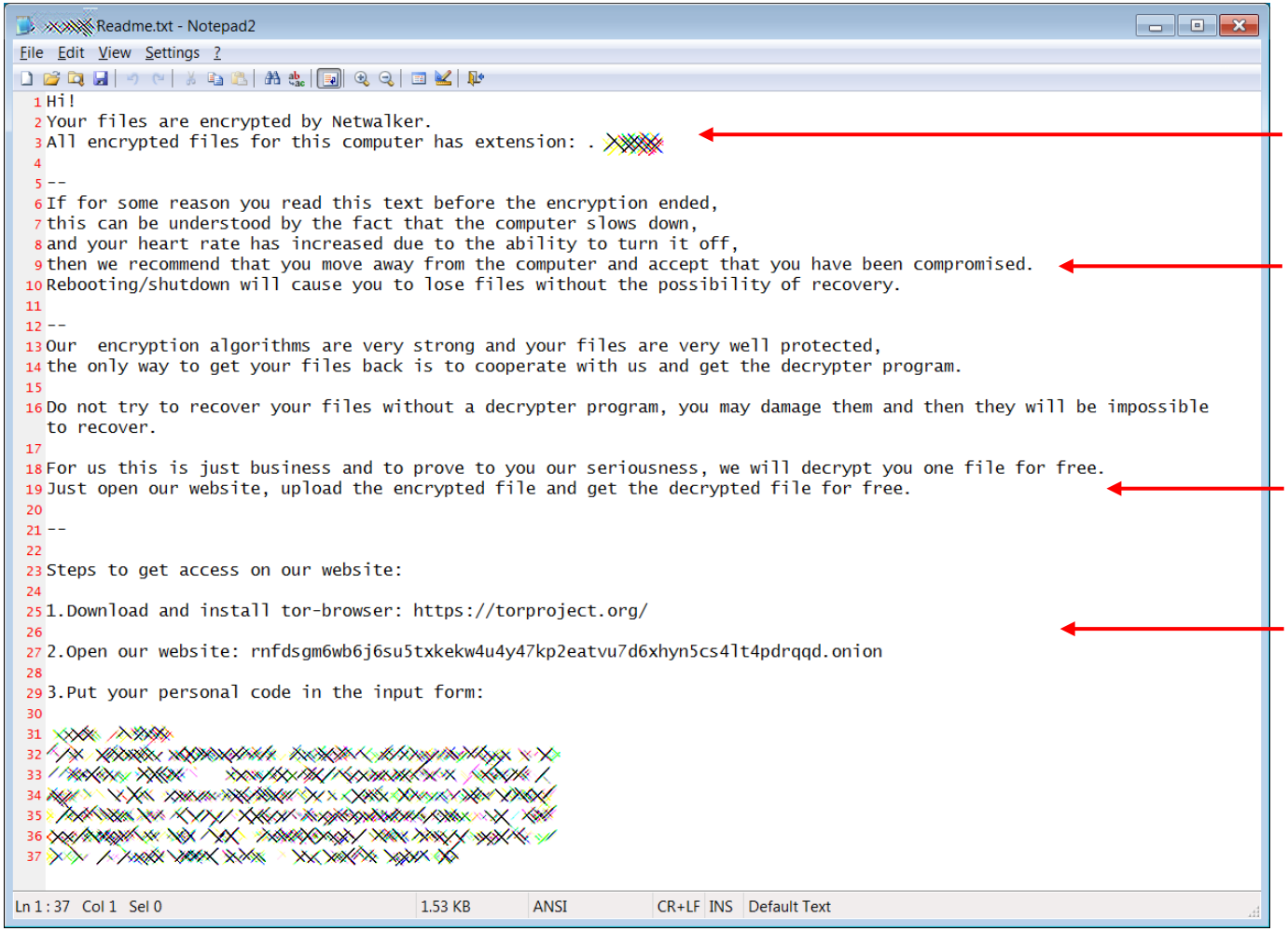


Some ransomware operators will conduct reconnaissance and move laterally to other systems to maximize the number of targets they can encrypt

Double extortion has become common

Example Ransom Note

Ransom note with standard elements found in most ransomware notes:



Notification of attack

Futility of non-cooperation

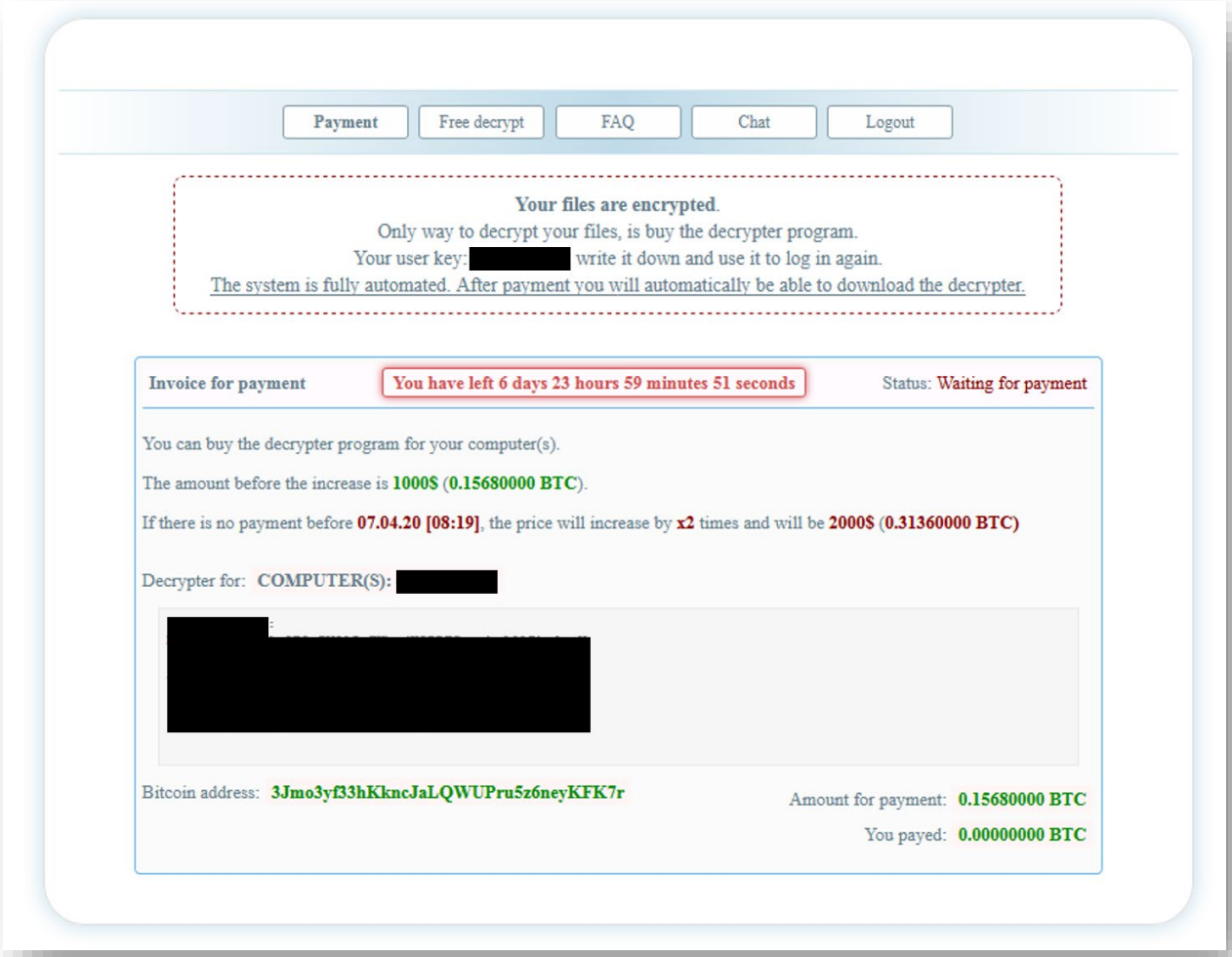
Justification for trust

Instructions

Ransom portal login

Portal to upload files to test decryption

Ransom portal landing page



Communications between victim and ransomware operators, part 4

Negotiation

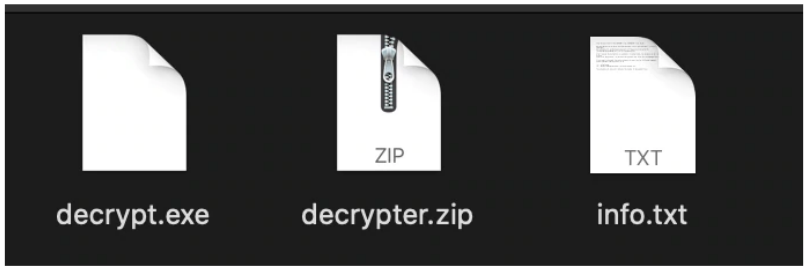
Operator: I can see from log you decrypted 2 files, the txt will be decrypted too
07.05.20 [13:22]

I don't know. $14,500 is really our limit. It's probably a little more than what the rebuilding costs are but I think decryption will be faster. We're open to going with either option, but if you can accept $14,500 then we have a deal. **You** 07.05.20 [16:16]

Operator: ok, 14.500
07.05.20 [17:14]

Operator: we can make you a a 10% discount if you pay in 7 days time
07.05.20 [10:50]

Delivery of decryptor



info.txt

```
This decrypt file for ALL NETWORK / ALL COMPUTERS / ALL FILES

Run decrypt.exe on PC which you want decrypt. Click "Auto decrypt" -> click "delete
crypter note file" -> click "decrypt".
The program will automatically decrypt all files on an encrypted PC.
The decryption program will fit all encrypted PCs.

After running the decryption in automatic or manual mode, the program can be closed only
when the close button becomes active,
never kill the process, if you kill the process your files will be damaged and they will
not be able to recover.

If you want to decrypt the entire network at once, use the following command:
psexec <params> "decrypt.exe" /S /D

/s – silent mode.
/d – delete lending(optional, not work without /s).

The program exit code will indicate the number of decrypted files.
```

Payment and invoice

Invoice for payment | **You have left 5 days 19 hours 39 minutes 31 seconds** | Status: Waiting for payment

You can buy the decrypter program for your computer(s).

The amount before the increase is

If there is no payment before **15.06.20 [03:33]**, the price will increase by **x2** times and will be

Decrypter for: **COMPUTER(S):**

```
lP3/zSq8ezm64Fx3SZDiizxE+kGjXuGmOK5M66fyZ9GPtG41Zj
AoeHPjSiZd5TrKfrVlWrcJIL0d9AIvAhLl3BtTr3kKjouPs8UZ
```

Bitcoin address:

Amount for payment:

You payed: **0.00000000 BTC**

Invoice for payment | Status: **Payed**

Payment received. You can download the decrypter program

Decrypter for: **ALL NETWORK / ALL COMPUTERS / ALL FILES**

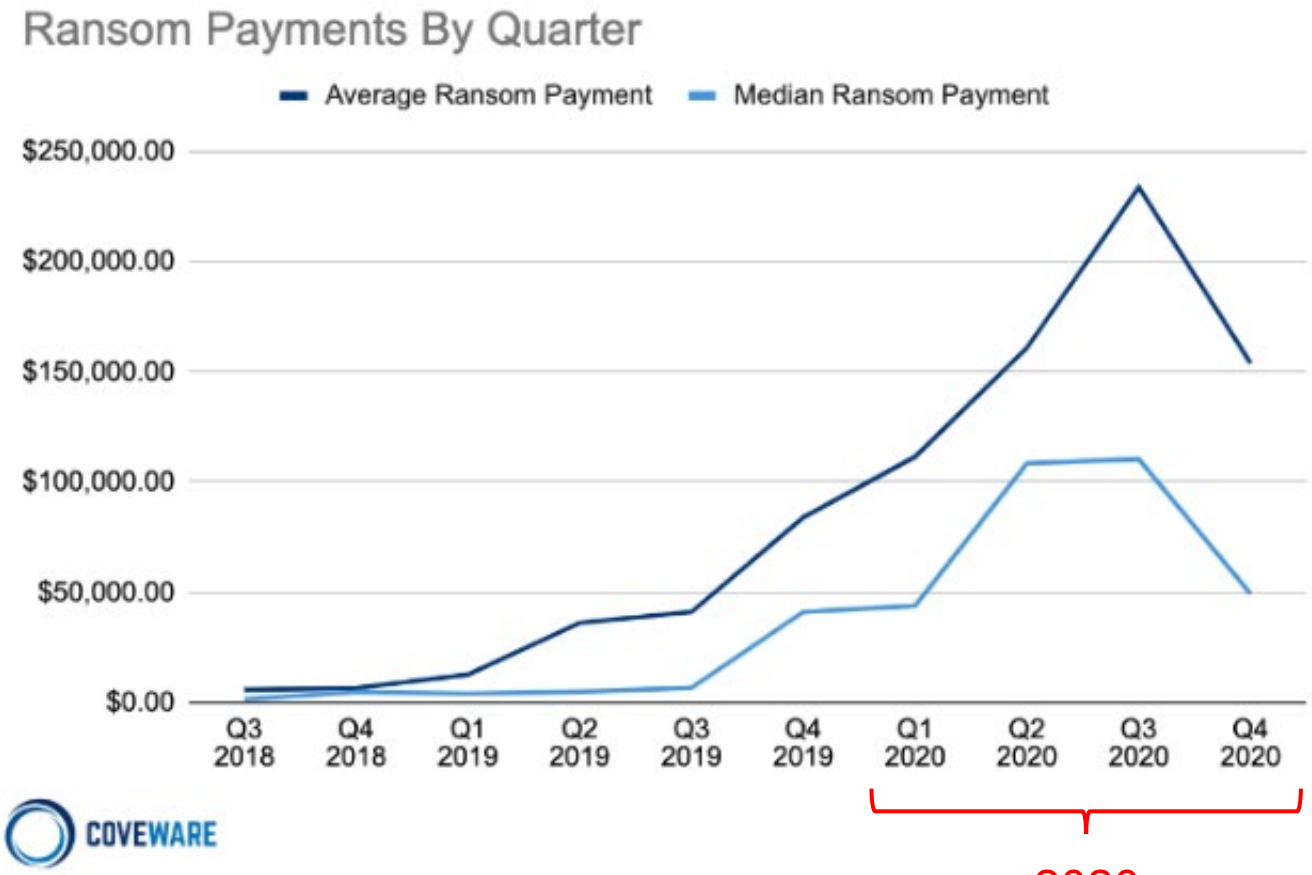
Download decrypter

A Snapshot of Healthcare Cybersecurity in 2020

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
- Tenable: 102 million healthcare records breached last year
- 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
- Comparitech: Ransomware cost healthcare $21 billion last year
- COVID-19 themed cyberattacks began along with the pandemic

"Another banner year for cybercriminals" - Emsisoft



Average Ransom Payment

$154,108

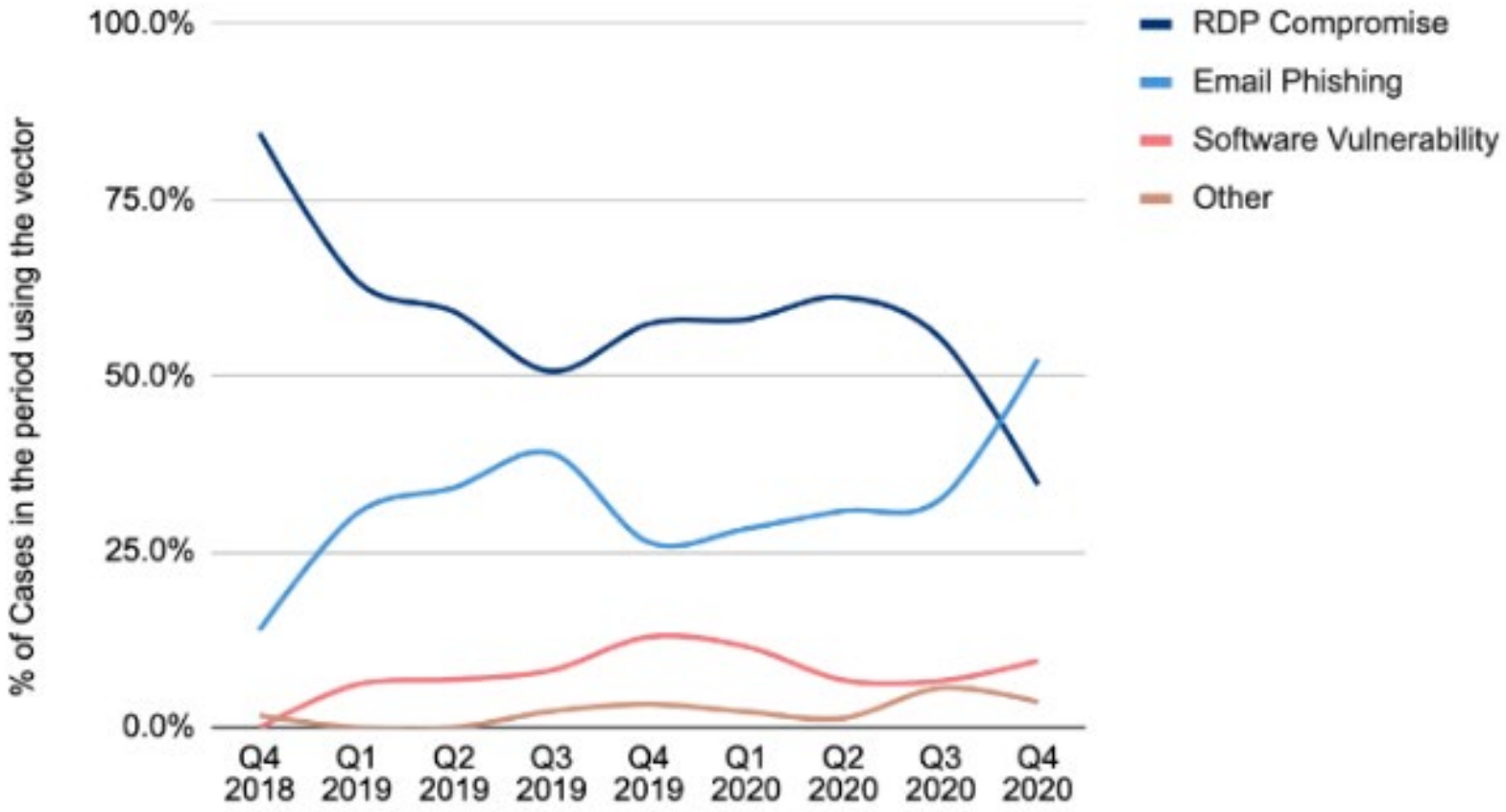
-34% from Q3 2020

Median Ransom Payment

$49,450

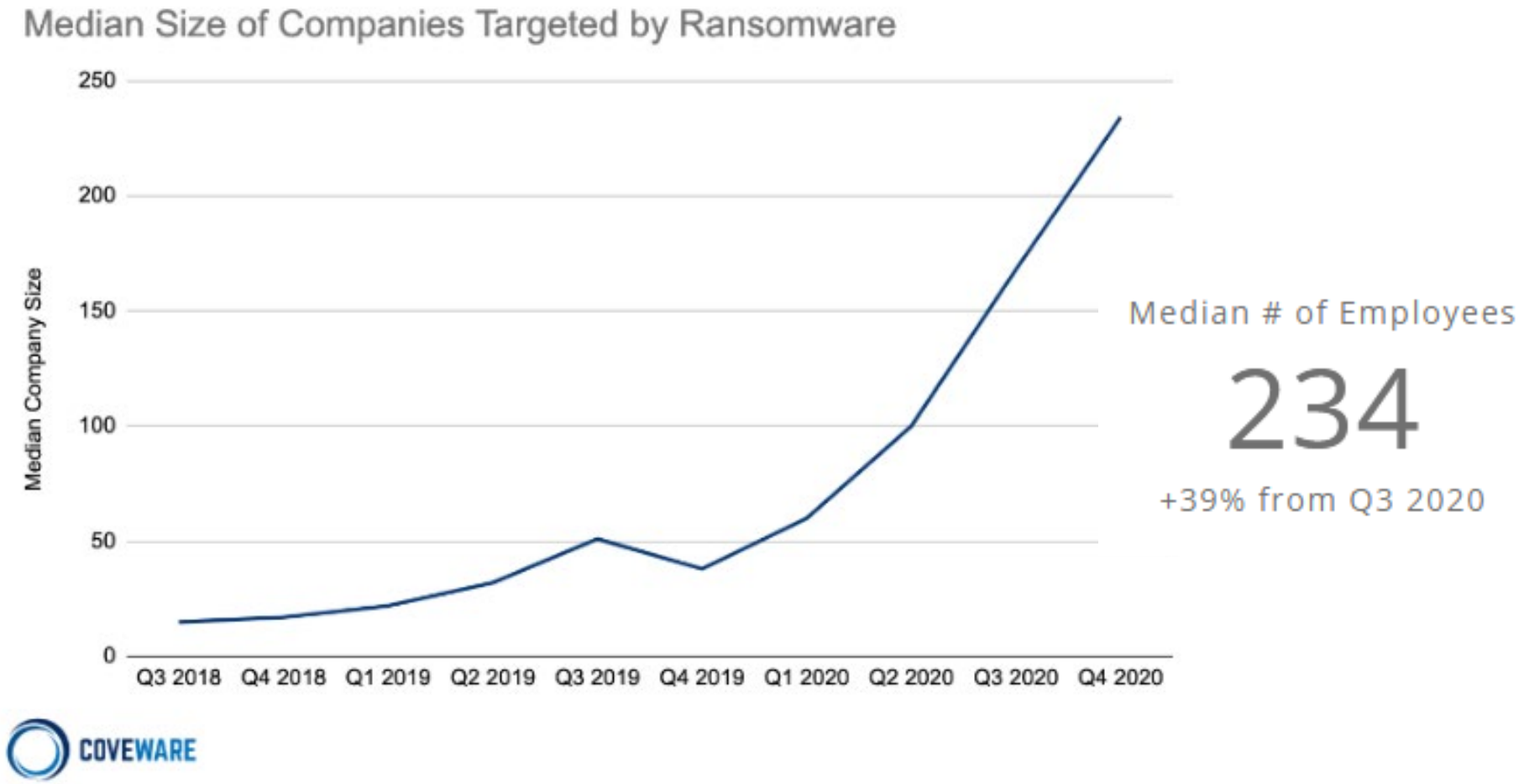
-55% from Q3 2020

Ransomware Attack Vectors

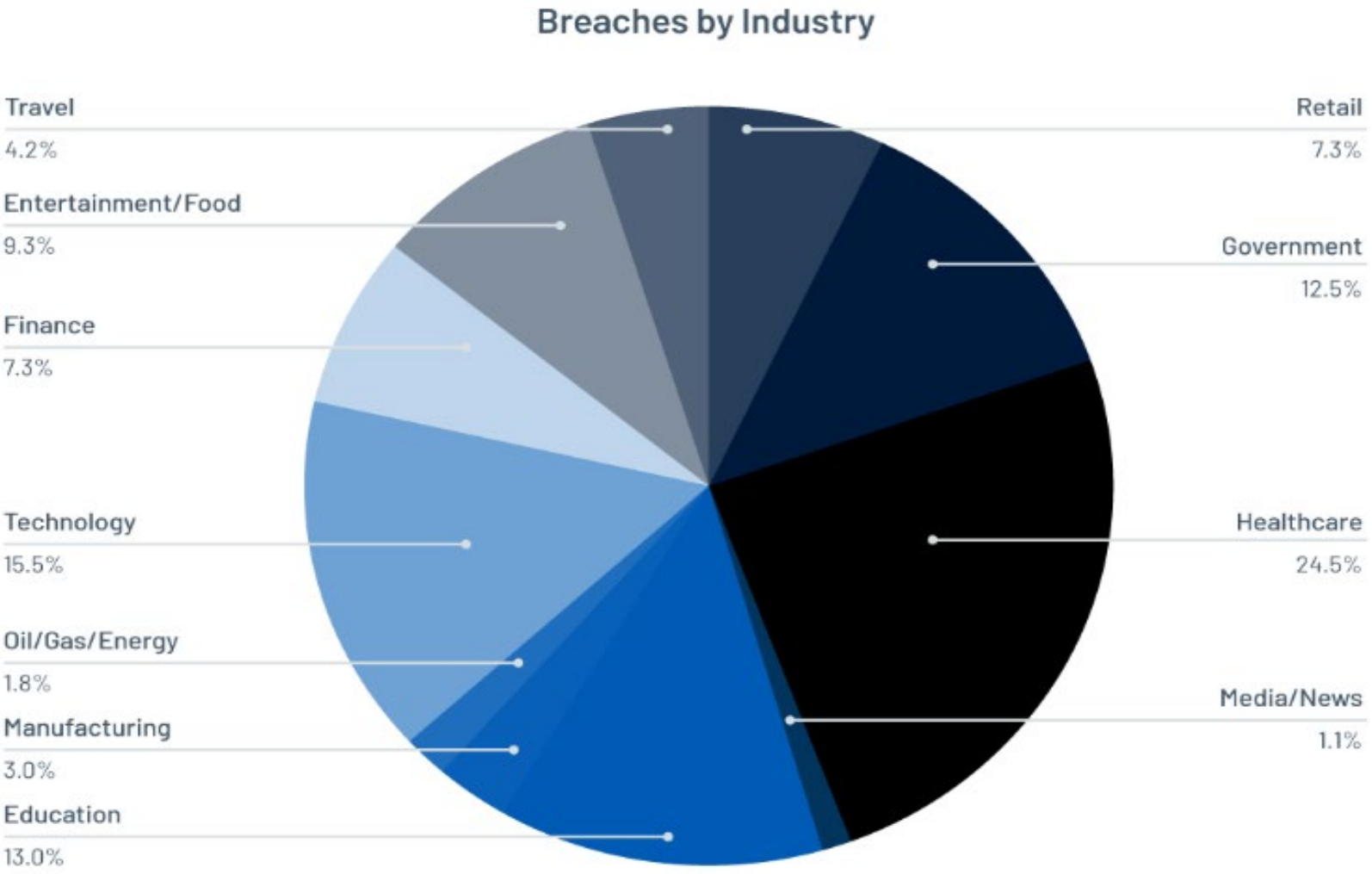


COVEWARE

Big game hunting:



- 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


Breaches by Industry
Travel
4.2%
Entertainment/Food
9.3%
Finance
7.3%
Technology
15.5%
Oil/Gas/Energy
1.8%
Manufacturing
3.0%
Education
13.0%
Retail
7.3%
Government
12.5%
Healthcare
24.5%
Media/News
1.1%

"…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."

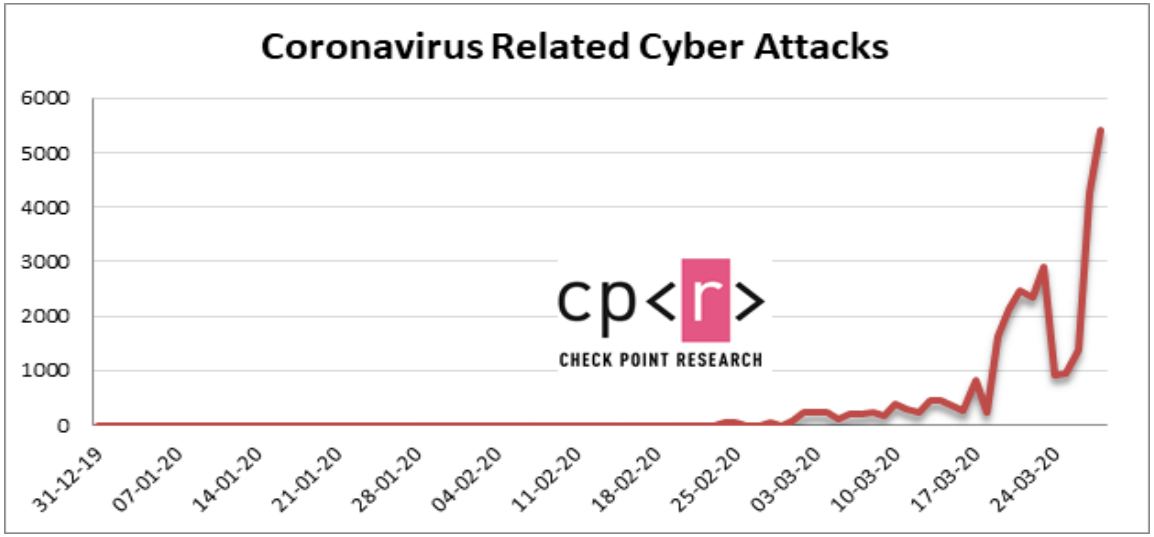
- Michael D'Ambrosio, Head of the U.S. Secret Service Office of Investigations

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

WashingtonPost.com, April 14, 2020

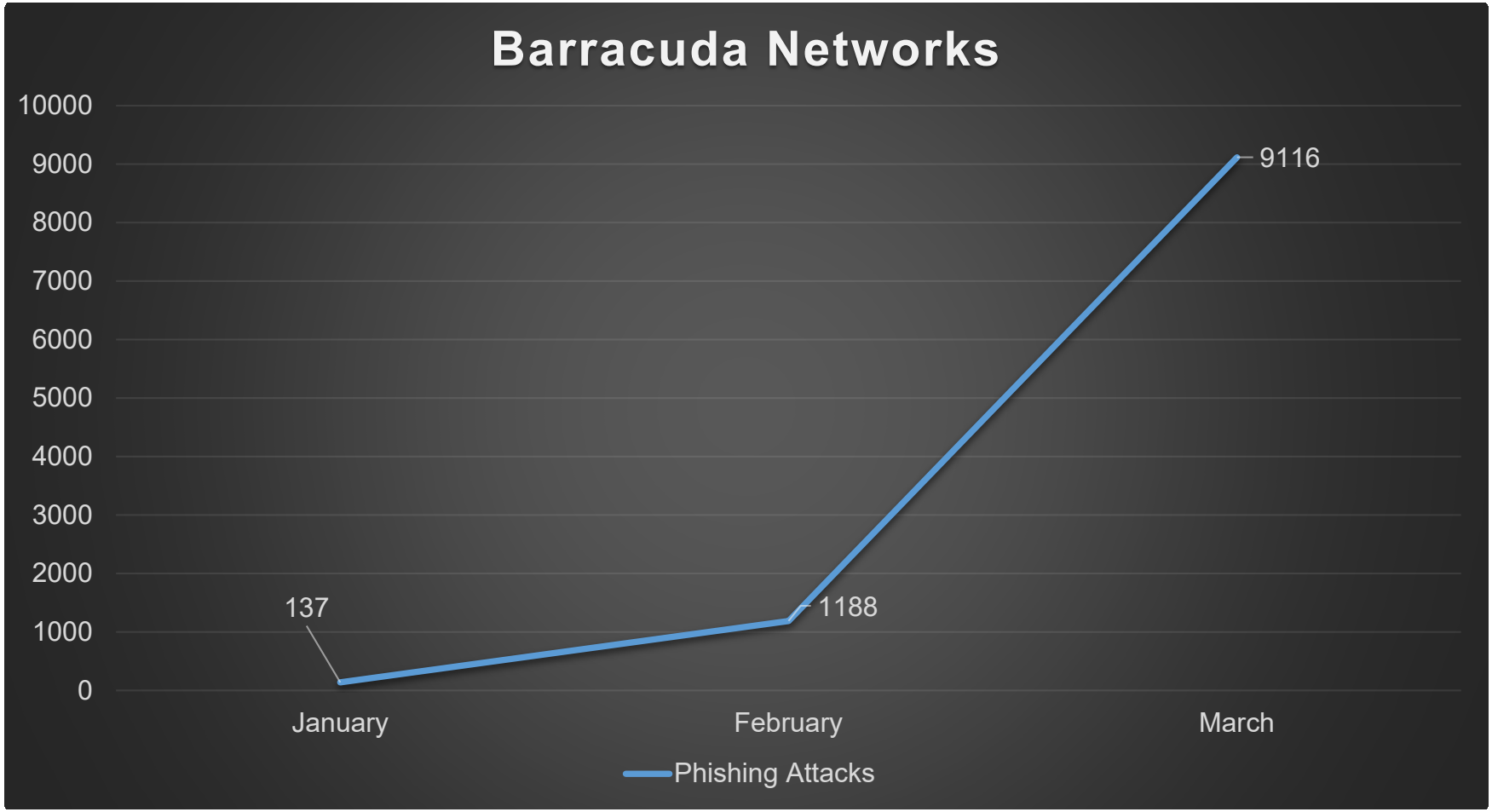
"...the risk to this sector will be elevated throughout this crisis."

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

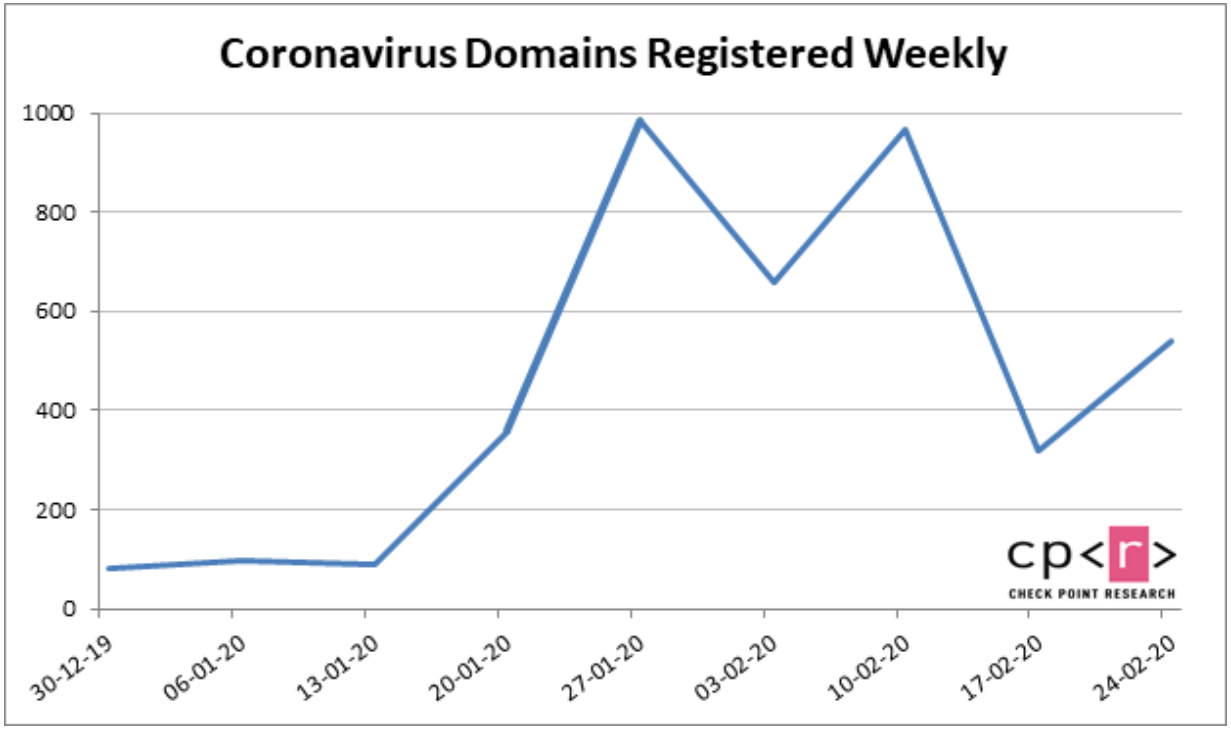


Coronavirus-themed phishing trends:

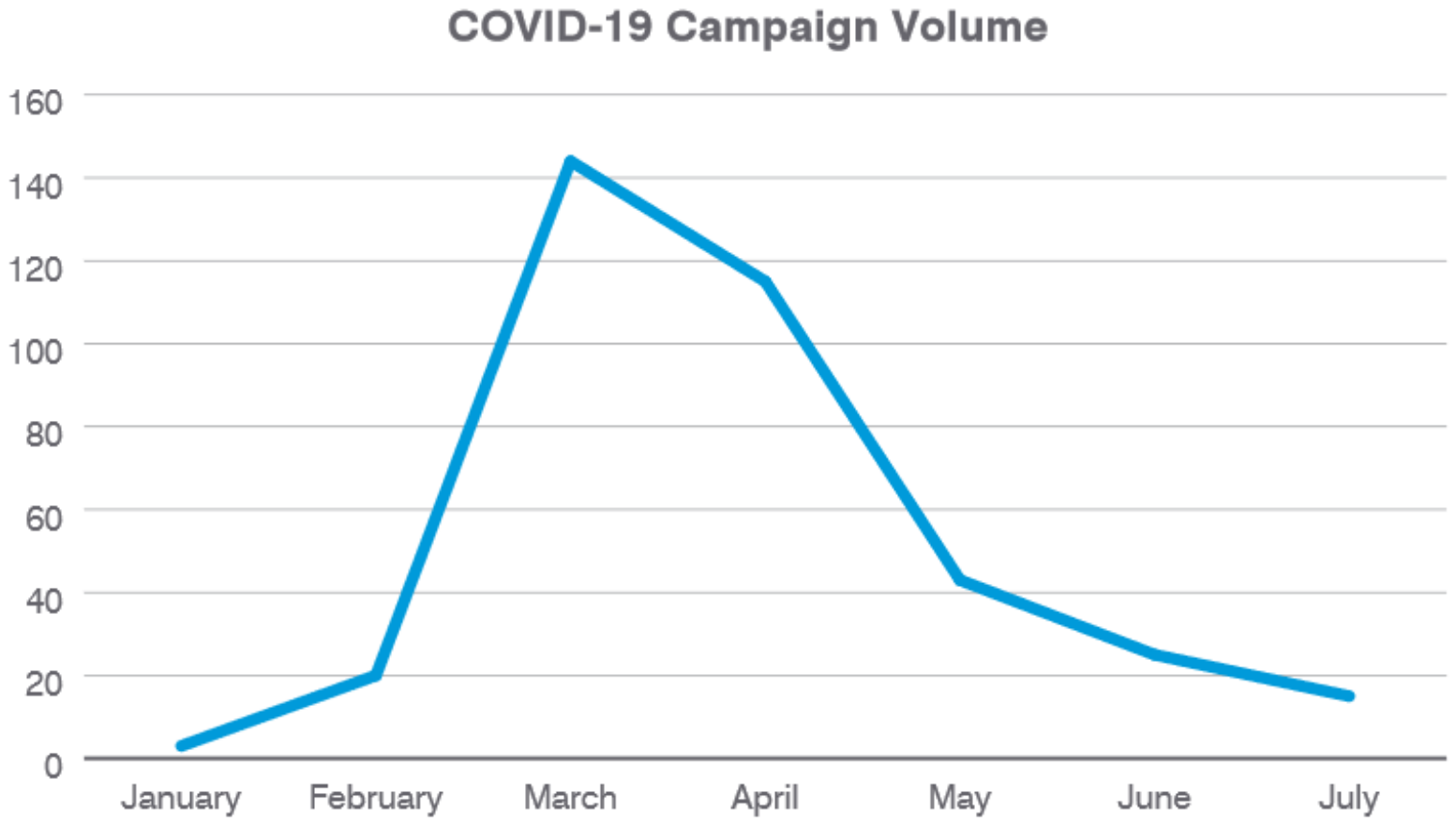
8X increase in Coronavirus related phishing from Jan. to Feb., and again from Feb. to Mar.



- 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.



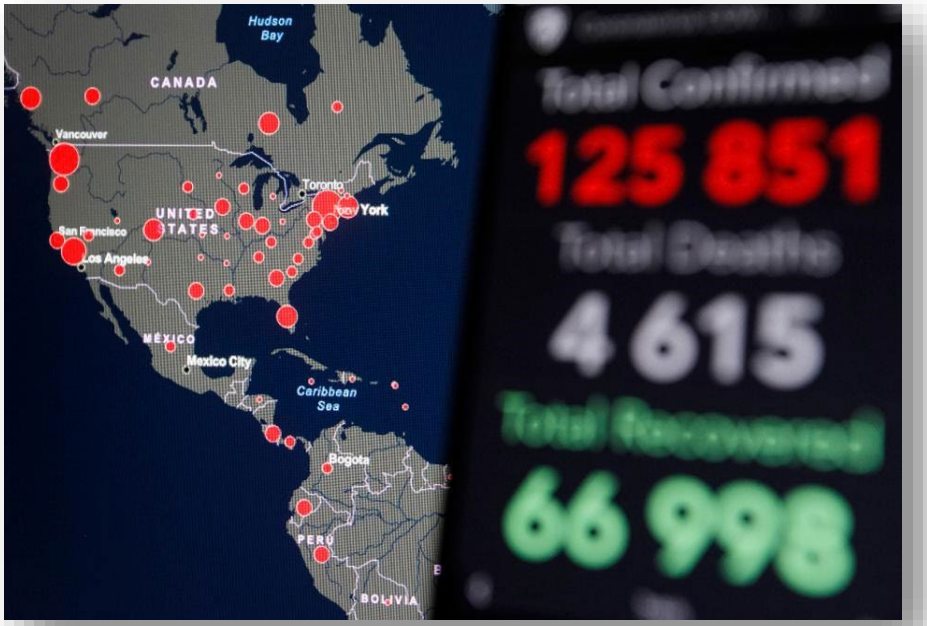
Coronavirus-themed campaign volume (Jan – July 2020):



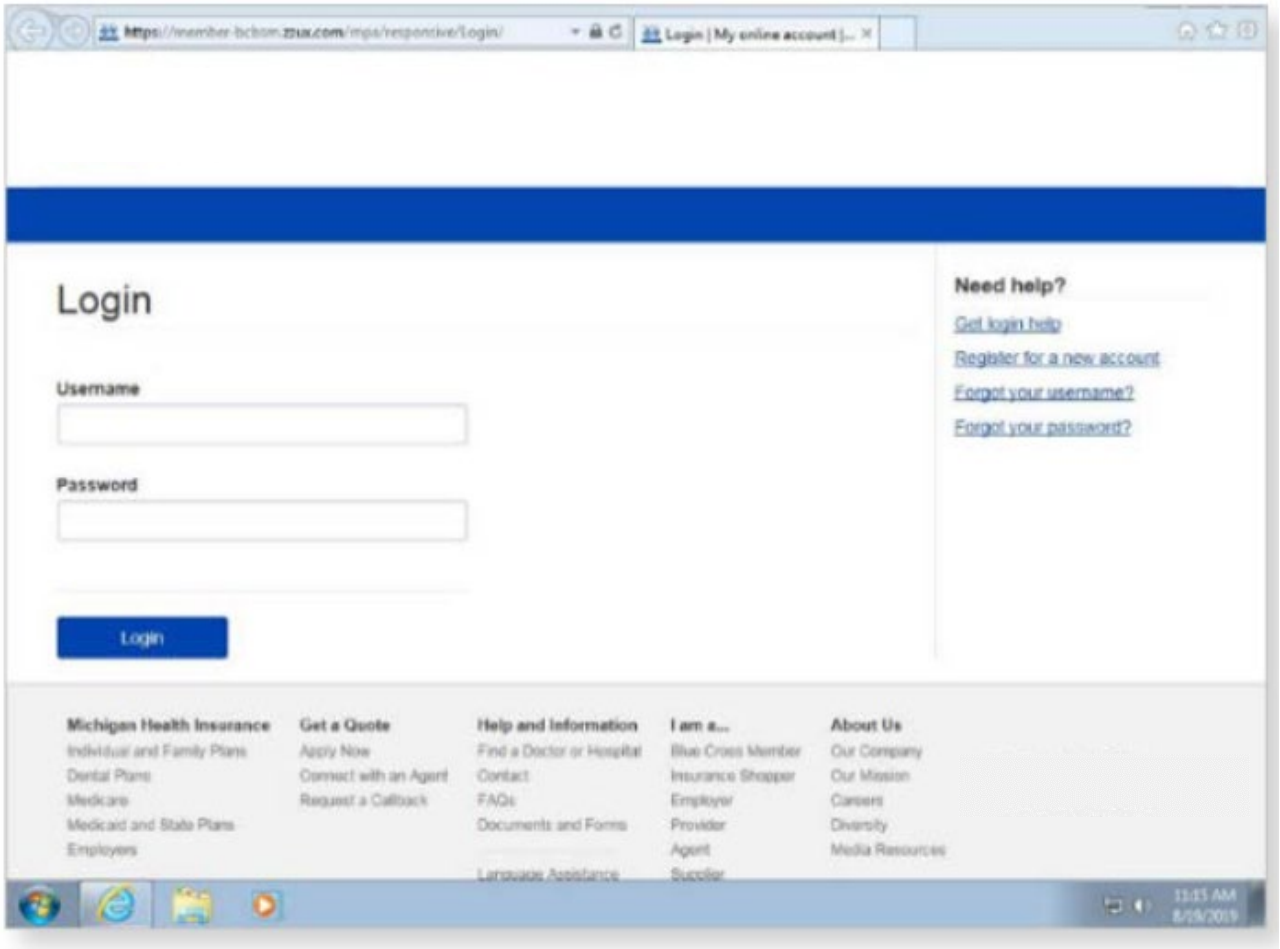
Proof Point report: https://www.proofpoint.com/sites/default/files/e-books/pfpt-us-tr-healthcare-report.pdf

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/



Cloned portal mimicking an insurer:



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

Access control: Security features that govern how users, applications and processes access information or a resource

Three security principles for any type of security control:

- Confidentiality – Ensuring information is not disclosed to unauthorized individuals, applications or processes
- Availability – Ensuring information and resources are available to authorized users, applications or processes in a timely manner
- Integrity – Ensuring that information is accurate and complete and not modified in any unauthorized manner

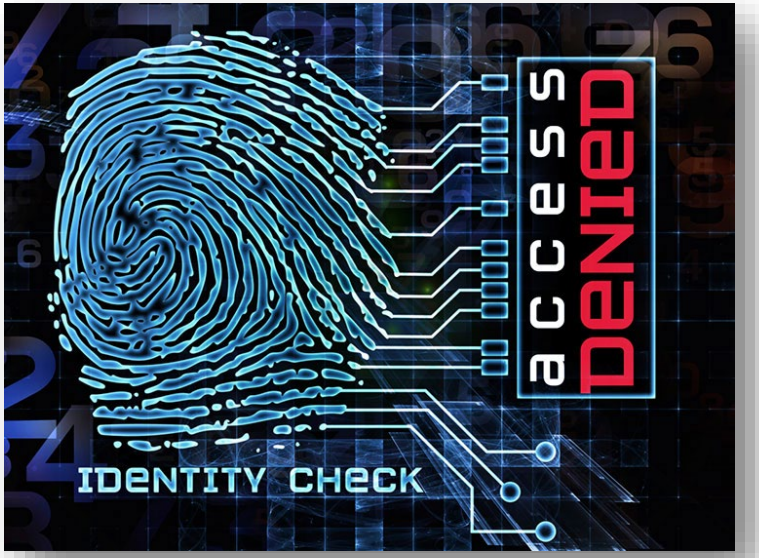
Conceptual components:

- Subject – An entity that requests access to an object
- Object – A passive entity that contains either information or functionality
- Access – the flow of information or the granting of functionality from an object to a subject

Access Control Models

Five types of access control:

- Discretionary Access Control (DAC) – Resource owner can decide who has access to the resource
  - Example: Access granted to SharePoint site granted by project manager
- Mandatory Access Control (MAC) – Access is granted based on sensitivity-based labeling system
  - Example: Access to classified Information is limited based on clearance and need-to-know
- Role-Based Access Control (RBAC) – Access granted based on defined role within organization.
  - Example: All accountants have access to financial database
- Rule-Based Access Control (RB-RBAC) – Built on RBAC, pre-defined rules grant access to a resource
  - Example: You must be a doctor and only during 9AM to 5PM can you access patient records
- Attribute-Based Access Control (ABAC) – Attributes (subject, objects, actions, context, etc…) determine access
  - Example: If a visitor wants to enter the building from 10PM to 6AM, they must first check in at the front desk to get a visitor badge and then they may only be allowed in if they have an employee escort them in



What is to be protected?

- People
  - Employees
  - Infants
  - Elderly
  - Patients
- Medicine/drugs
  - Controlled medications
- Technology
  - Networks
  - Systems
- Data
  - Patient records
  - Employee records
  - Intellectual property

What physical access controls protect these assets?

- Physical barriers/protection
  - Fences, gates, ports
  - Guards/security
  - Secure doors
  - Digital locks
  - Vaults/safes
- Surveillance
  - Live video cameras
- Alarm systems
  - Detecting people in unauthorized areas and/or at unauthorized times

Telehealth and telemedicine can not be covered by most of these? Why?

Limitations on technology and authority.

Most important takeaway: While physical access control is critically important to healthcare, the greatest cyberthreats to healthcare are not mitigated by physical solutions

COVID-19 Vaccine Distribution Physical Security Measures

COVID-19 vaccine distribution efforts are underway, and the Cybersecurity and Infrastructure Security Agency (CISA) encourages organizations involved in the distribution process to assess potential security vulnerabilities and implement corresponding risk mitigation solutions to reduce the probability of disruptions. Although there are currently no credible or imminent threats, the distribution process could potentially be disrupted by anti-vaccination protesters, insiders, criminals or organized crime, or terrorists. As such, organizations involved in the manufacturing, transportation, and distribution of the vaccine should apply cost-effective protective measures to their operations. Vulnerability assessments, planning, and training are key steps to mitigating potential threats and identifying necessary protective measures. This infographic broadly illustrates four stages of vaccination distribution activity, possible physical threats at these stages, and some potential mitigations. For more hands-on assistance, please engage local law enforcement, or contact CISA Central.

DISTRIBUTION STAGES

M Manufacturing Sites → T Transporters → C Clinics, Pharmacies & Healthcare Facilities → P Points of Distribution (PODs)

THREAT VECTORS, MITIGATIONS, AND RESOURCES

Active Shooter

M C P

- Liaise with local police and emergency responders for rapid response to an incident
- Establish and practice emergency response plan (ERP)
- Maintain strict access control protocols
- Implement facility-wide notification system
- Pre-position first responder kits
- Ensure employees and staff are trained and ready to implement **Run, Hide, Fight** protocol

* CISA's Active Shooter Preparedness resources
* Federal Emergency Management Agency's ERP – Ready.gov

Insider Threat

M T C P

- Limit access to sensitive areas, transportation planning information, and security sites
- Establish a multi-disciplinary team to plan for mitigating an insider threat incident
- Conduct pre- and post-employment screening
- Employ user activity monitoring software on all devices
- Maintain comprehensive data back-up on secure remote server

* CISA's Insider Threat Mitigation resources

Hijacking

T

- Ensure drivers do not deviate from designated routes without clearance or make unapproved stops
- Train drivers how to identify and report suspicious behavior during transit and at rest stops
- Notify local law enforcement of time and vehicle type for planned shipments
- Provide visible security personnel for all vehicles transporting valuable cargo

* Transportation Security Administration's (TSA) First Observer Plus Program
* TSA's Surface Transportation Resources for Industry
* Department of Transportation's Emergency Response Guidebook

Theft

T C P

- Maintain alarm systems with panic buttons and remote triggers for staff
- Train staff to identify and report suspicious behavior
- Position Closed-Circuit Television (CCTV) systems to actively monitor vaccine storage and other sensitive areas
- Maintain strict access controls for vaccine storage and dispensing environments
- Notify local law enforcement of the vaccine locations

* "If You See Something, Say Something®" Recognize the Signs
* Department of Homeland Security's Nationwide Suspicious Activity Reporting Initiative

Vehicular Assault

T C P

- Ensure that lines and crowds are diverted away from busy roads; if possible, close roads where satellite clinics occupy space
- Train staff to recognize indicators of a possible assault, including an individual repeatedly revving the vehicle's engine, practicing heavy-vehicle manual shifting, or verbalizing threats
- Lay out a serpentine pathway for queuing vehicles so that drivers cannot accumulate significant speed
- Establish clear standoff zones, ensuring a solid passive barrier between workers on foot and vehicle lines

* CISA's Vehicle Ramming action guide
* CISA's Vehicle Ramming Attack Mitigation video

Improvised Explosive Device (IED) and Improvised Incendiary Device (IID)

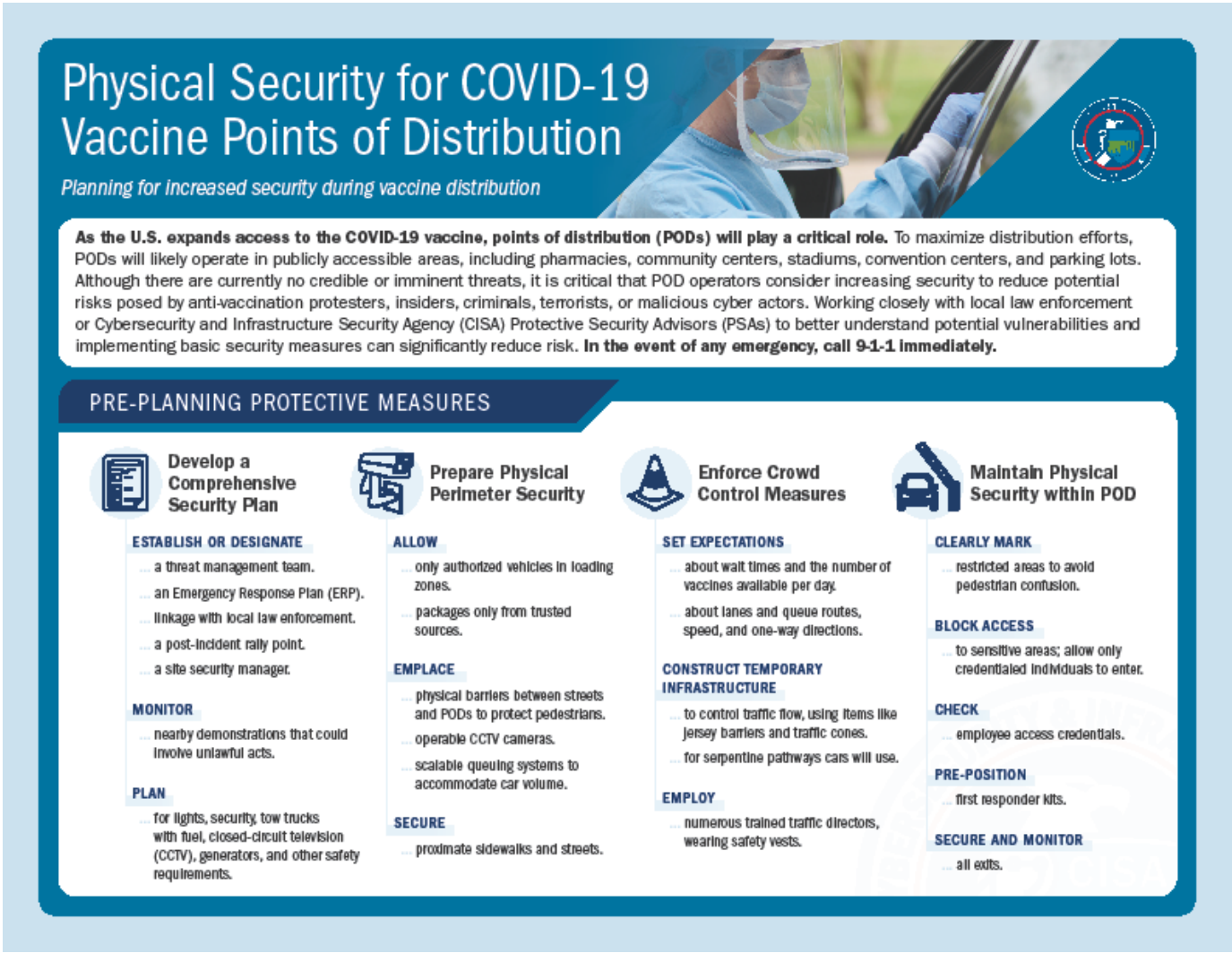
M T C P

- Develop, update, and exercise Bomb Threat Management Plans
- Conduct a periodic visual security sweep of the facility
- Remove nearby trash receptacles
- Notify management, security, or law enforcement immediately of unattended bags or packages
- Establish rally points for personnel accountability

* CISA's Office for Bombing Prevention resources
* CISA's Fire as a Weapon action guide

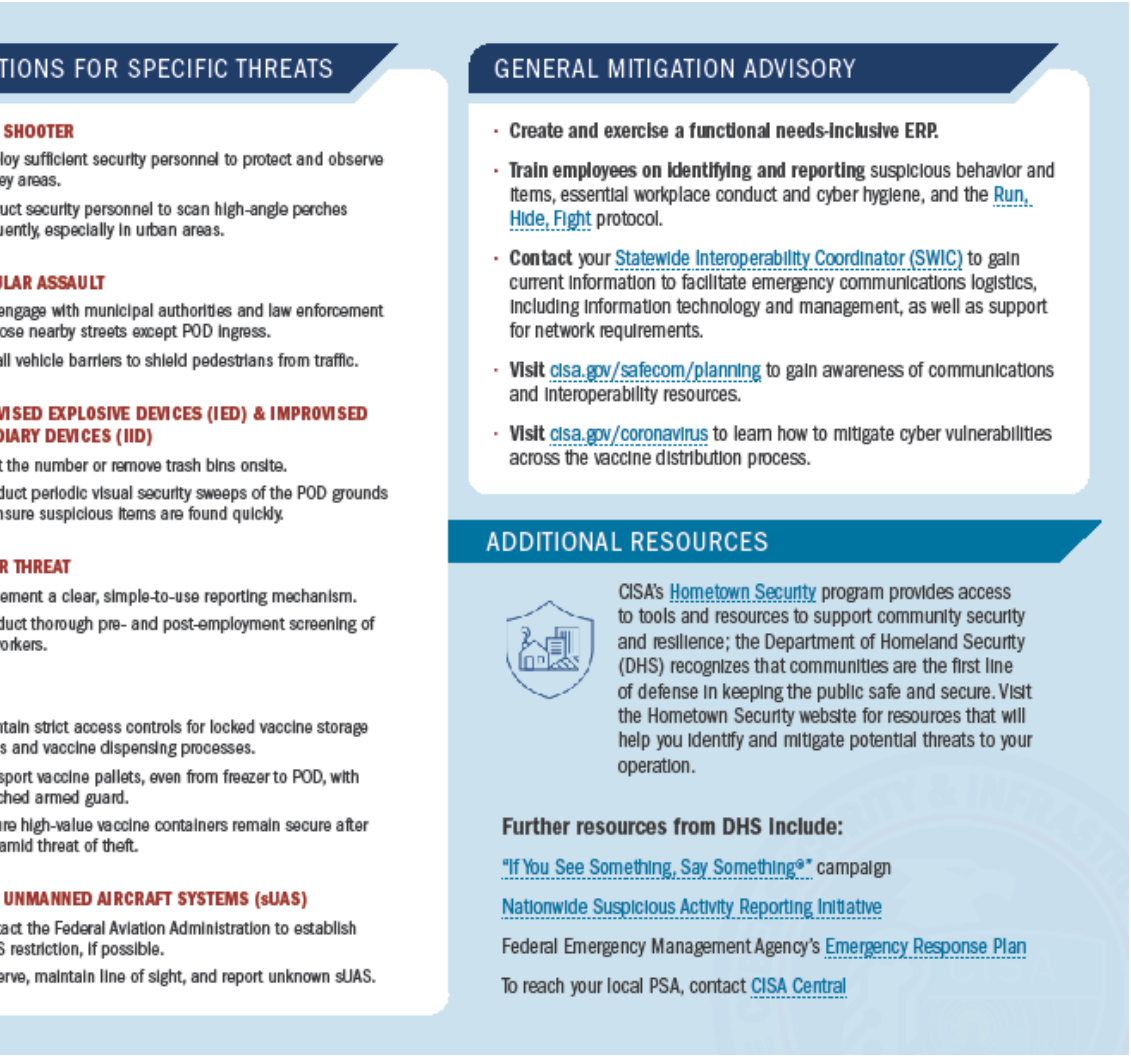
For more information and resources, please visit cisa.gov or email Central@cisa.gov. **Call 9-1-1 immediately in the event of an emergency.**

Source: https://www.cisa.gov/sites/default/files/publications/COVID-19_Vaccine_Distribution_Physical_Security_Measures_508.pdf



Source: https://www.cisa.gov/sites/default/files/publications/POD%20Physical%20Security%20Action%20Guide_508.pdf

CISA: Physical Security for Covid-19 Vaccine Points of Distribution Guidance (2 of 2)



MITIGATION OPTIONS FOR SPECIFIC THREATS

ACTIVE SHOOTER
- Employ sufficient security personnel to protect and observe all key areas.
- Instruct security personnel to scan high-angle perches frequently, especially in urban areas.

VEHICULAR ASSAULT
- Pre-engage with municipal authorities and law enforcement to close nearby streets except POD ingress.
- Install vehicle barriers to shield pedestrians from traffic.

IMPROVISED EXPLOSIVE DEVICES (IED) & IMPROVISED INCENDIARY DEVICES (IID)
- Limit the number or remove trash bins onsite.
- Conduct periodic visual security sweeps of the POD grounds to ensure suspicious items are found quickly.

INSIDER THREAT
- Implement a clear, simple-to-use reporting mechanism.
- Conduct thorough pre- and post-employment screening of all workers.

THEFT
- Maintain strict access controls for locked vaccine storage areas and vaccine dispensing processes.
- Transport vaccine pallets, even from freezer to POD, with attached armed guard.
- Ensure high-value vaccine containers remain secure after use amid threat of theft.

SMALL UNMANNED AIRCRAFT SYSTEMS (sUAS)
- Contact the Federal Aviation Administration to establish sUAS restriction, if possible.
- Observe, maintain line of sight, and report unknown sUAS.

GENERAL MITIGATION ADVISORY

- **Create and exercise a functional needs-inclusive ERP.**
- **Train employees on identifying and reporting** suspicious behavior and items, essential workplace conduct and cyber hygiene, and the Run, Hide, Fight protocol.
- **Contact** your Statewide Interoperability Coordinator (SWIC) to gain current information to facilitate emergency communications logistics, including information technology and management, as well as support for network requirements.
- **Visit** cisa.gov/safecom/planning to gain awareness of communications and interoperability resources.
- **Visit** cisa.gov/coronavirus to learn how to mitigate cyber vulnerabilities across the vaccine distribution process.

ADDITIONAL RESOURCES

CISA's Hometown Security program provides access to tools and resources to support community security and resilience; the Department of Homeland Security (DHS) recognizes that communities are the first line of defense in keeping the public safe and secure. Visit the Hometown Security website for resources that will help you identify and mitigate potential threats to your operation.

Further resources from DHS include:

"If You See Something, Say Something®" campaign

Nationwide Suspicious Activity Reporting Initiative

Federal Emergency Management Agency's Emergency Response Plan

To reach your local PSA, contact CISA Central

Source: https://www.cisa.gov/sites/default/files/publications/POD%20Physical%20Security%20Action%20Guide_508.pdf

Case Study: Miltenyi Biotech attacked with ransomware

Miltenyi Biotec, a global biotechnology and clinical research company headquartered in Cologne, Germany, was attacked with ransomware in October 2020

- They provide products and services that support scientists, clinical researchers, and physicians across basic and translational research, and clinical applications
- They offer solutions covering techniques of sample preparation, cell separation, cell sorting, flow cytometry, cell culture, molecular analysis, clinical applications and small animal imaging
- They employee 2500 people across 28 countries and offer over 17,000 products
- Working on the development of covid vaccine research among other things
- IT infrastructure spans 73 countries
- Breach was discovered to have began back in July 2020
- Confirmed data was leaked
- Mount Locker claims they stole 150GB of data, they posted 5% online in early November
- Operational disruption: “there have been isolated cases where order processing was impaired by malware in parts of our global IT infrastructure,”
- E-mail and phones down for several weeks

Miltenyi Biotec

Case Study: Biotech firm attacked with ransomware

American biotech firm, whose cold-storage capabilities are integral to Covid-19 vaccine distribution, was attacked with ransomware in November 2020

- 100-year old company that manages 183 warehouses worldwide and has approximately 13,000 employees
- Operations were impacted including phone systems, email, inventory management, and order fulfillment
- They shut down systems to prevent the spread of the attack
- The company filed an 8-K report with the Securities and Exchange Commission on November 16, 2020
  - "determined that its computer network was affected by a cybersecurity incident" an " took immediate steps to help contain the incident and implemented business continuity plans, where appropriate, to continue ongoing operations“

HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA

Hackers Hit COVID-19 Biotech Firm, Cold Storage Giant with Cyberattacks

Case Study: Biotech firm attacked with ransomware

American biotech firm that designs and manufactures gene sequencing technology was attacked with ransomware in March of 2020

- The company is part of an international alliance that is sequencing cells from recovered COVID-19 patients to understand possible treatments
- The ransomware group that attacked them was Revil/Sodinokibi
- Company usernames, an employee database, internal password policies and domain information were posted on a leak site as proof of compromise
- The company filed an 8-K report with the Securities and Exchange Commission on November 16, 2020
  - They reported no material day-to-day impact on operations

Compromise of Video Security Company

Cyberattack on American video surveillance company provides hackers with access to live feeds from schools, personal residences, workplaces, prisons and hospitals for two days in March of 2021

- The company sells cameras and AI-driven face and object recognition technology
- Hackers tracked down to Switzerland, not financially motivated or associated with any state
  - Justified attacks: "lots of curiosity, fighting for freedom of information and against intellectual property, a huge dose of anti-capitalism, a hint of anarchism — and it's also just too much fun not to do it.“
- The compromise was caused by credentials posted on the public Internet

Resources:

- **MIT Sloan: Cybersecurity Management in Pharmaceutical ad Biotechnology Industries**
  https://jalali.mit.edu/sites/default/files/documents/Cybersecurity_Management_Pharma_Biotech.pdf
- **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 the COVID-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

Ransomware attacks on healthcare organizations cost nearly $21B last year, study finds
https://www.beckershospitalreview.com/cybersecurity/ransomware-attacks-on-healthcare-organizations-cost-nearly-21b-last-year-study-finds.html

Over 102 million healthcare records exposed by cyber attacks In 2020
https://gulfnews.com/business/company-releases/over-102-million-healthcare-records-exposed-by-cyber-attacks-in-2020-1.1615747723170

Biotech research firm Miltenyi Biotec hit by ransomware, data leaked
https://www.bleepingcomputer.com/news/security/biotech-research-firm-miltenyi-biotec-hit-by-ransomware-data-leaked/

Hackers Hit COVID-19 Biotech Firm, Cold Storage Giant with Cyberattacks
https://healthitsecurity.com/news/hackers-hit-covid-19-biotech-firm-cold-storage-giant-with-cyberattacks

Food-Supply Giant Americold Admits Cyberattack
https://threatpost.com/food-supply-americold-cyberattack/161402/

References

UNITED STATES SECURITIES AND EXCHANGE COMMISSION 8-K - November 16, 2020
https://www.sec.gov/ix?doc=/Archives/edgar/data/1455863/000119312520294943/d62059d8k.htm

Ransomware strikes biotech firm researching possible COVID-19 treatments
https://www.cyberscoop.com/covid-19-ransomware-10x-genomics-data-breach/

UNITED STATES SECURITIES AND EXCHANGE COMMISSION 8-K: April 1, 2020
https://www.sec.gov/Archives/edgar/data/1770787/000119312520094606/d913176d8k.htm

Another COVID-19 Research Firm Targeted by Ransomware Attack
https://healthitsecurity.com/news/another-covid-19-research-firm-targeted-by-ransomware-attack

Swiss Police Raid Apartment of Verkada Hacker, Seize Devices
https://www.bloomberg.com/news/articles/2021-03-12/swiss-police-raid-apartment-of-verkada-hacker-seize-devices?sref=P6Q0mxvj

Security camera hack exposes live feeds from hospitals, workplaces and schools
https://www.localsyr.com/news/security-camera-hack-exposes-live-feeds-from-hospitals-workplaces-and-schools/

'It's too much fun not to': Hacker who exposed US hospitals' security cameras on inspiration behind attack
https://www.beckershospitalreview.com/cybersecurity/it-s-too-much-fun-not-to-hacker-who-exposed-us-hospitals-security-cameras-on-inspiration-behind-attack.html

Verkada Data Breach Exposes Feeds of 150,000 Security Cameras; Targets Include Health Care Facilities, Schools, Police Stations and a Tesla Plant
https://www.cpomagazine.com/cyber-security/verkada-data-breach-exposes-feeds-of-150000-security-cameras-targets-include-health-care-facilities-schools-police-stations-and-a-tesla-plant/

Upcoming Briefs

- North Korean Cyber Espionage Campaigns Targeting the HPH Sector (3/25)
- New briefing structure beginning 4/8
  - **Keep an eye out for the registration invite soon!**

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.**

Product Evaluations

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

HC3 Customer Feedback

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. HHS does not endorse any specific person, entity, product, service, or enterprise.

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