Monthly Cyber Briefing

June 6, 2024

Clearwater

Logistics

- All attendees in “Listen Only Mode”
- Please ask content related questions in Q&A
- Recording, final slides, resources and attendee certificate shared within 24 hours
- Please take a few minutes to provide feedback via survey prompt at the end of this session

Agenda & Speakers

- Cyber update
- Business email compromise and social engineering tactics

Steve Cagle
Chief Executive Officer
Clearwater

Dave Bailey
Vice President, Consulting Services
Clearwater

Steve Akers
CTO Managed Security Services, CISO
Clearwater

Ricoh Danielson
Information Security and Incident Response – VCISO
1st Responder

Cyber Update

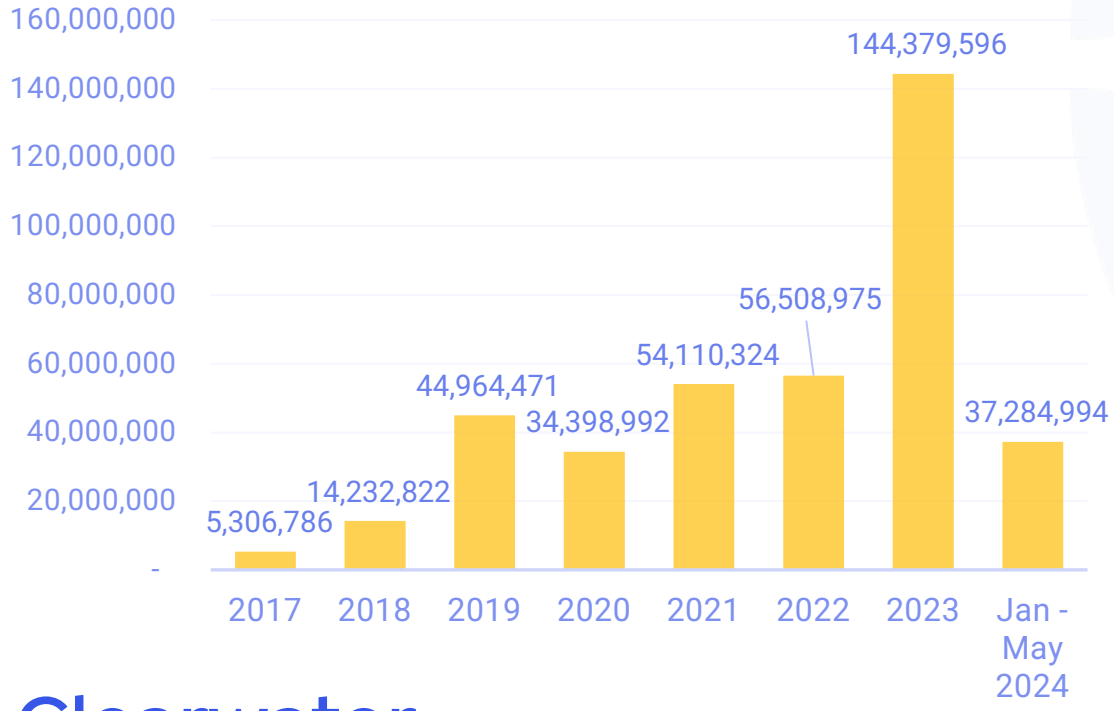
Steve Cagle

Clearwater

Breach Reports via OCR Breach Portal [1] and SEC

- 144.4M records reported breached in 2023, an increase of 61% vs 56.5M records in 2022
- 737 breaches reported in 2023 vs 720 in 2022, a slight increase year over year
- 38.3m records from 315 breaches in 2024; below 2023 pace, but does not include Change Healthcare breach

Records Reported Breached to OCR



Notable in May 2024 breach data

- Relatively “light” month of breaches, with 35 breaches and “only” 4.7m records reported as breached
- Largest breach WebTPA Employer Services, LLC 2.5m individuals affected
- DocGo Telemed – large medical transportation company – disclosed breach through SEC reporting

Clearwater

[1]*HHS Breach Portal (data for 2023 pulled March 21, data for 2024 pulled June 3, 2024).*

Change Healthcare Update

Product updates

● Uninterrupted / Fully Restored ● Partial Service Available ● Restoration in Progress ● Restoration Date Pending

Acuity Revenue Cycle Analytics

Acuity provides revenue cycle analytics for users of Clearance and Assurance

Restored week of **4/1/2024**

Assurance Reimbursement Management

Batch claim submission, remittance management

Restored week of **3/25/2024**

CHC Cardiology PACs

The on-premise management of images, reports, ECG, hemodynamics, waveforms, analytics, charge capture, and inventory management.

CHC Radiology PACs

The integrated, on-premise web-based PACS system for radiologists.

CHC Workflow Intelligence

The on-premise flexible medical imaging workflow rules engine for radiologists.

Clearance Patient Access Suite

Benefits verification, authorization, financial engagement

Restored week of **3/25/2024**

Clinical Exchange

Provider workflow enabling electronic prescribing, ordering and resulting integrated into EHRs

Restored week of **4/15/2024**

Compliance Reporter

Enables NCQA Quality Measure Reporting for HEDIS / CMS Stars Deadlines, Client HEDIS Chart Abstraction Features

Restored week of **4/1/2024**

Coverage Insight

Coverage discovery

Restored week of **3/25/2024** **Vendor Workaround*

Eligibility

Process real-time transactions

Restored **4/3/2024**

HealthQX

Supports retrospective episode-based payment models

Restored week of **4/8/2024**

Hosted Payer Services (HPS)

Payer hosting service for eligibility responses to providers

Restored week of **3/28/2024**

InterQual Customize

Larger plans use this functionality to review and modify the criteria of releases for their own use.

Restored week of **4/1/2024**

Medical Network Exchange

Claims, remittance, eligibility transaction processing

Restored week of **3/25/2024**

MedRX

Pharmacy electronic claims for medical

Restored week of **3/25/2024**

Payer Connectivity Services (PCS)

EDI validation and editing, data routing to different repricers, third parties, end adjudication systems or processing paths

Restored week of **4/25/2024**

Payer Print Communication Multi-Channel Distribution System (MCDS)

Ability for check/remit print production

Restore week of **4/15/2024**

Payments - Electronic Providers

Ability for electronic payment production

Restored week of **3/4/2024**

Pulse Revenue Cycle Benchmarking

Pulse provides RCM KPI benchmarks for institutional claims utilizing Assurance client data

Restored week of **4/1/2024**

Reimbursement Manager

Claim pricing

Restored week of **03/25/2024**

Revenue Performance Advisor (RPA)

Automates E2E revenue cycle processes and provides real-time visibility into eligibility, claims and payment tracking, and denials management

Restored week of **4/1/2024**

Risk Manager

Supports clients in managing value-based payment contracts

Restored week of **4/15/2024*** **date changed*

Risk View

Supports risk-adjusted payment models with advanced analytics

Restored week of **4/29/2024**

Stratus Imaging Analytics

The cloud-native imaging analytics platform.

Stratus Imaging Archive

The fully managed, cloud-native medical imaging archive for providers.

Stratus Imaging PACS

The full-featured, cloud PACS imaging solution.

Stratus Imaging Share

The cloud-based medical-image-sharing platform.

Stratus Imaging Viewer

The cloud-based imaging solution with imaging access.

[Information on the Change Healthcare Cyber Response - UnitedHealth Group]

Clearwater

CEO Testimony on Capitol Hill Takeaways

Andrew Witty
CEO, UnitedHealth Group
at Senate Finance Committee Hearings on
Change Healthcare Breach

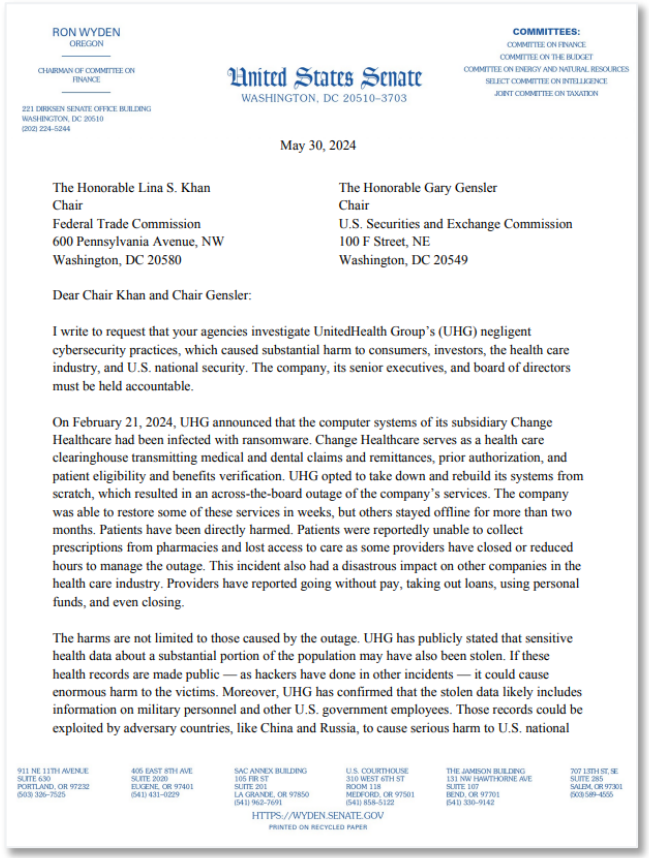
- **Failure to Address Legacy Tech**
- **Lateral Movement for 9 Days Undetected**
- **Access Through Stolen Credentials**
- **Lack of Back-up Separation – No Viable IRP**
- **No MFA on Remote Access Server**
- **Even with 7 Firms Assisting, Months to Recover**

Clearwater

Video Link: UnitedHealth CEO Testifies Before Senate on Cyber Attack Against Change Healthcare | C-SPAN.org

Change Healthcare – SEC & FTC Investigation?

Senator Wyden calls on FTC and SEC to investigate UnitedHealth Group



RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510–3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

May 30, 2024

The Honorable Lina S. Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

The Honorable Gary Gensler
Chair
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Dear Chair Khan and Chair Gensler:

I write to request that your agencies investigate UnitedHealth Group's (UHG) negligent cybersecurity practices, which caused substantial harm to consumers, investors, the health care industry, and U.S. national security. The company, its senior executives, and board of directors must be held accountable.

On February 21, 2024, UHG announced that the computer systems of its subsidiary Change Healthcare had been infected with ransomware. Change Healthcare serves as a health care clearinghouse transmitting medical and dental claims and remittances, prior authorization, and patient eligibility and benefits verification. UHG opted to take down and rebuild its systems from scratch, which resulted in an across-the-board outage of the company's services. The company was able to restore some of these services in weeks, but others stayed offline for more than two months. Patients have been directly harmed. Patients were reportedly unable to collect prescriptions from pharmacies and lost access to care as some providers have closed or reduced hours to manage the outage. This incident also had a disastrous impact on other companies in the health care industry. Providers have reported going without pay, taking out loans, using personal funds, and even closing.

The harms are not limited to those caused by the outage. UHG has publicly stated that sensitive health data about a substantial portion of the population may have also been stolen. If these health records are made public — as hackers have done in other incidents — it could cause enormous harm to the victims. Moreover, UHG has confirmed that the stolen data likely includes information on military personnel and other U.S. government employees. Those records could be exploited by adversary countries, like China and Russia, to cause serious harm to U.S. national

911 NE 11TH AVENUE SUITE 630 PORTLAND, OR 97232 (503) 326-7525
405 EAST 8TH AVE SUITE 2020 EUGENE, OR 97401 (541) 431-0229
SAC ANNEX BUILDING 105 FIR ST SUITE 201 LA GRANDE, OR 97850 (541) 962-7691
U.S. COURTHOUSE 310 WEST 6TH ST ROOM 118 MEDFORD, OR 97501 (541) 858-5122
THE JAMISON BUILDING 131 NW HAWTHORNE AVE SUITE 107 BEND, OR 97701 (541) 330-9142
707 13TH ST, SE SUITE 285 SALEM, OR 97301 (503) 589-4555

HTTPS://WYDEN.SENATE.GOV
PRINTED ON RECYCLED PAPER

- States harm caused to sector, patients, National Security and investors
- Says root cause of attack was that UnitedHealth CISO had no previous CISO experience
- Places negligence on CEO and Board of Directors
- Wants to know if laws were broken? If so, demands to "hold senior officials accountable"

Clearwater

[Wyden Letter to FTC and SEC on UHG Cybersecurity.pdf (senate.gov)]

Change Healthcare – OCR Update

OCR updates FAQs regarding Change Healthcare Investigation and Breach Reporting

- OCR's ransomware guidance provides specific information on the steps covered entities and business associates should take to determine if a ransomware incident is a HIPAA breach
- Reiterates that the covered entity is ultimately responsible for reporting breaches under HIPAA within 60 days of determination (for 500+ individuals affected)
- OCR will not consider the 60-calendar day period from discovery of a breach by a covered entity to start until it has received the information needed from Change Healthcare or UHG
- Business associates are required to notify covered entity of a breach within 60 days
- Covered entity may delegate reporting a breach to individuals to the business associate
- Only one entity needs to make notifications to the affected individuals

Change Healthcare Cybersecurity Incident Frequently Asked Questions | HHS.gov
Fact Sheet: Ransomware and HIPAA | HHS.gov
Breach Notification Rule | HHS.gov

Ascension Ransomware Attack Update

Nurses at Ascension hospital in Michigan raise alarms about safety following ransomware attack

Jonathan Greig, The Record. May 29, 2024

'It's putting patients' lives in danger': Nurses say ransomware attack is stressing hospital operations

Sean Lyngaas, CNN, May 29, 2024

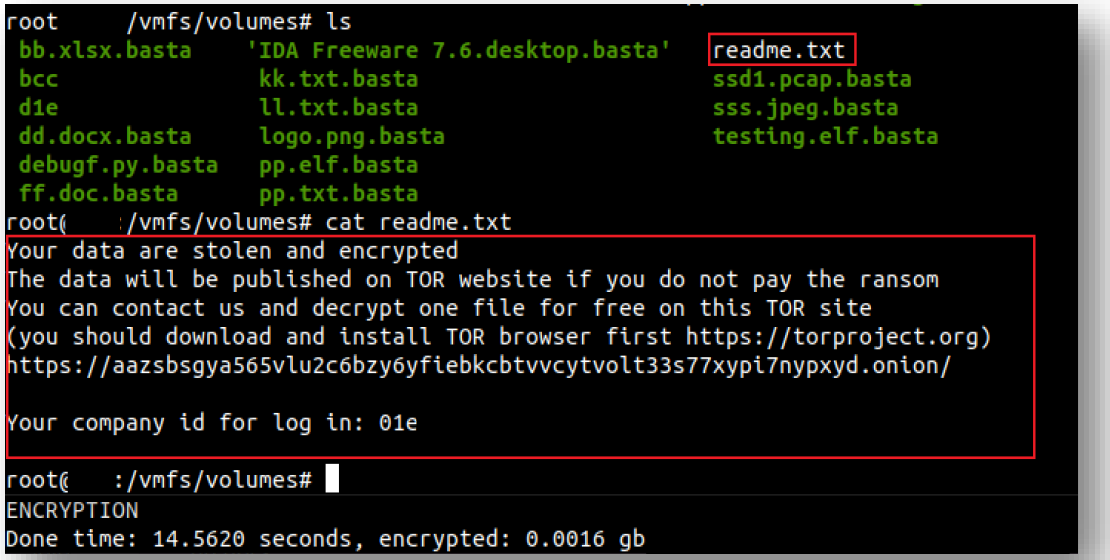
- 140 hospital systems impacted by Black Basta ransomware May 8th
- Reported 3 days later; vendors notified to disconnect systems
- Pharmacy system, EHR, phone, imaging and other systems offline; some ambulance diversions
- Clinicians have reported orders for medication and imaging by hand
- Numerous reports concern of errors and impact to patient safety
- As of 5/31 at least one EHR is back online
- Reporting to have EHR widely available 6/14

Cybersecurity Event Update | Ascension
Nurses at Ascension hospital in Michigan raise alarms about safety following ransomware attack (therecord.media)
'It's putting patients' lives in danger': Nurses say ransomware attack is stressing hospital operations | CNN Business
Ascension restores EHR in 1st market after cyberattack (beckershospitalreview.com)

Clearwater

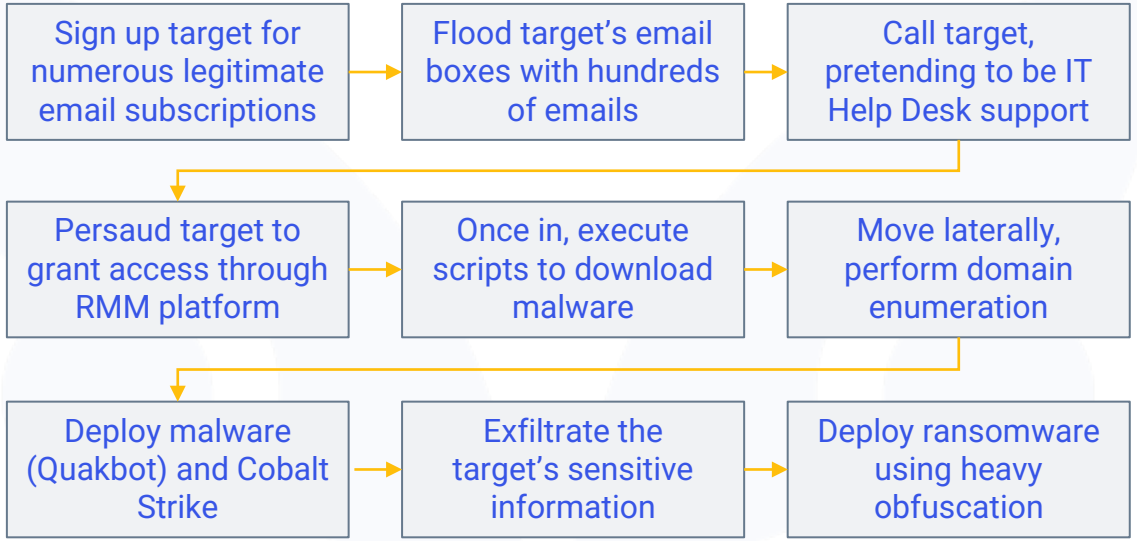
Black Basta Threat Overview and TTPs

Black Basta has targeted over 500 entities including Chilean Government, American Dental Association, Dish Network, and recently Atlas Oil



Black Basta was formed April 2022 (former Conti) and is known for its double extortion attacks and has specifically targeted healthcare since 2023. HC3 published warning in March 2023.[1]

- Historical TTPs include spear-Phishing, Insider Information and buying Network Access
- Most Recent TTPs are “link listing” attacks



Clearwater

1 202303151200_Black Basta Threat Profile_TLPCLEAR (hhs.gov)

Addressing Threat of Black Basta

Recommendations

- Baseline your environment for all installed remote monitoring and management solutions
- Ensure users are aware of established IT channels and communication methods
- Empower users to report suspicious phone calls and texts purporting to be from internal IT staff
- Monitor for IOCs that associated with Black Basta TTPs (and other suspicious activity or other)
- Install updates for operating systems, software, and firmware as soon as they are released
- Identify gaps in multi-factor authentication controls
- Update your Risk Analysis to include all information systems with ePHI and/or that are critical to operations

Review and act on CISA Advisory and H-ISAC Intel

[#StopRansomware: Black Basta (cisa.gov)]

[TLP WHITE - 2c4e32a6 - UPDATE: Black Basta]

TLP WHITE - 2c4e32a6 - UPDATE: Black Basta Threat Actor Emerges as a Major Threat to the Healthcare Industry

Health-ISAC

UPDATE: Black Basta Threat Actor Emerges as a Major Threat to the Healthcare Industry

JOINT CYBERSECURITY ADVISORY

Co-Authored by:

MS-ISAC Multi-State Information Sharing & Analysis Center

TLP:CLEAR

Product ID: AA24-131A

May 10, 2024

#StopRansomware: Black Basta

SUMMARY

***Note**: This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

Actions for critical infrastructure organizations to take today to mitigate cyber threats from ransomware:

- Install updates for operating systems, software, and firmware as soon as they are released.
- Require phishing-resistant MFA for as many services as possible.
- Train users to recognize and report phishing attempts.

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Department of Health and Human Services (HHS), and Multi-State Information Sharing and Analysis Center (MS-ISAC) (hereafter referred to as the authoring organizations) are releasing this joint CSA to provide information on Black Basta, a ransomware variant whose actors have encrypted and stolen data from at least 12 out of 16 critical infrastructure sectors, including the Healthcare and Public Health (HPH) Sector.

This joint CSA provides TTPs and IOCs obtained from FBI investigations and third-party reporting. Black Basta is considered a ransomware-as-a-service (RaaS) variant and was first identified in April 2022. Black Basta affiliates have impacted a wide range of businesses and critical infrastructure in North America, Europe, and Australia. As of May 2024, Black Basta affiliates have impacted over 500 organizations globally.

Black Basta affiliates use common initial access techniques—such as phishing and exploiting known vulnerabilities—and then employ a double-extortion model, both encrypting systems and exfiltrating data. Ransom notes do not generally include an initial ransom demand or payment instructions.

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. SLTT organizations should report incidents to MS-ISAC (866-787-4722 or SOC@cisecurity.org).

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

TLP:CLEAR

Clearwater

Regulatory Update

National Security Memorandum 22

Represents a significant shift towards regulation of owners and operators of critical infrastructure, as it directs federal agencies to set “minimum requirements” and effective “accountability” mechanisms for the security and resilience of critical infrastructure” as well as “enforcement mechanisms”.

The Good

Solidifies Role of CISA, reinforcing Sector Risk Management Agents responsibilities and coordination with DHS for each critical infrastructure sector.

Shortfalls

Does not establish space or cloud as critical infrastructure. No funding to implement the objectives.

8 Objectives of NSM-22

1. Shared Responsibility
2. Risk-Based Approach
3. Minimum Requirements
4. Accountability
5. Information Exchange
4. Expertise & Technical Resources
5. International Engagement
6. Policy Alignment

Clearwater

National Security Memorandum on Critical Infrastructure Security and Resilience | The White House

OCR Increasing Enforcement, Audits – Risk Analysis in Focus

Statements by OCR Director Fontes Rainer during May 7th interview:

A critical area of enforcement focus overall is the HIPAA Security Rule's requirement for conducting risk analysis, which continues to be a significant weakness among many regulated organizations of all sizes, especially for medium- and smaller-sized organizations.

“Poor risk analysis practices persist as a major contributing factor to many significant breaches reported to the agency.”

HHS OCR plans by the end of the year to publish a proposed update to the HIPAA Security Rule.

"We have reopened our HITECH audits. And so, we're proactively doing audits as well right now.”

Clearwater

Listen to the Interview: How HHS OCR Is Boosting HIPAA Enforcement; Here Come Audits (bankinfosecurity.com)

FTC Updates Health Breach Notification Rule ("HBNR")

The final rule will go into effect 60 days after its publication in the Federal Register (4/26/24)

1. Revises definitions to cover all health apps and similar technologies not covered by HIPAA
2. Definition of "breach of security" includes both data security breaches and unauthorized disclosures
3. The revised definition of "PHR-related entity" establishes that the Rule applies to entities that offer products and services through online services of vendors of personal health records, including mobile apps
4. "Personal health record" includes drawing information from multiple sources matters
5. Expands the use of electronic notice to consumers
6. Notices to consumers must be "clear and conspicuous" and "reasonably understandable
7. Covered entities must move quickly to notify consumers – and the FTC – about breaches involving 500 or more people
8. The Final Rule adds cross-references, citations, and more information about penalties for non-compliance

- FTC Health Breach Notification Rule moves reporting more in line with HIPAA requirements
- FTC has already enforced the rule and states it will continue to do so
- FTC is further doubling down on its stance on breaches related to website or other tracking technologies

Clearwater

Health Breach Notification Rule (ftc.gov)

Compliance Recommendations

1. Complete Gap Assessments of HIPAA Rules following the OCR Audit Protocol & and FTC HPNR
2. Ensure OCR-Quality Risk Analysis is up to date
3. Assess your implementation of 405(d) HICP
4. Make updates to policies and procedures to address FTC Health Breach Notification Rule
5. Evaluate use of online tracking technologies

Business Email Compromise & Social Engineering Tactics

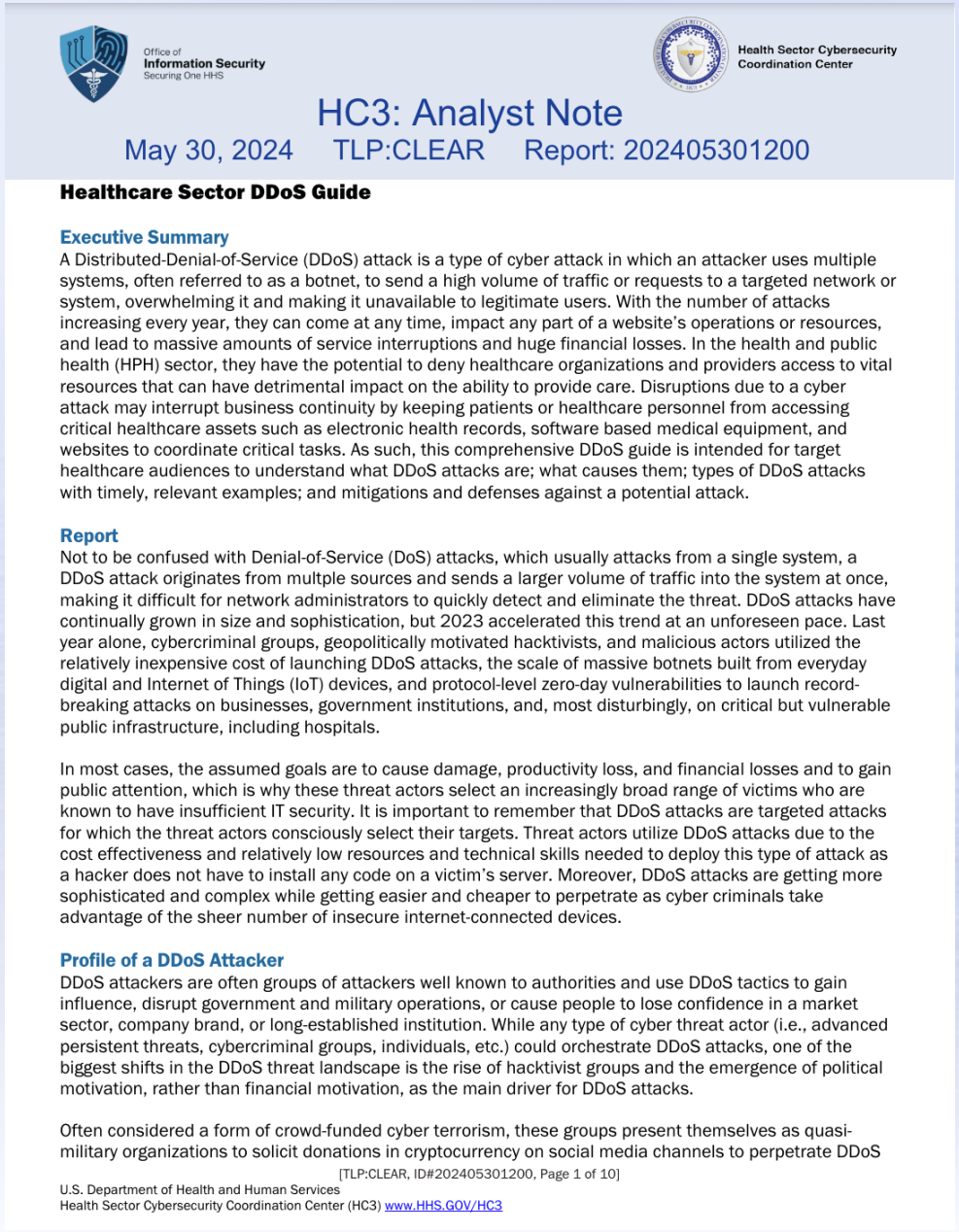
Dave Bailey
Steve Akers
Ricoh Danielson

Clearwater

Distributed Denial of Service

- May 30, 2024, TLP: CLEAR
  - Healthcare Sector DDoS Guide
  - An attacker uses multiple systems (botnet) to send a high volume of traffic or requests to a targeted network (long term or burst)
- DDoS Resources: CISA, NIST, & Health-ISAC

https://www.cisa.gov/news-events/news/understanding-denial-service-attacks
https://www.nist.gov/programs-projects/advanced-ddos-mitigation-techniques
https://h-isac.org/distributed-denial-of-service-ddos-attacks/



Office of Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Analyst Note
May 30, 2024 TLP:CLEAR Report: 202405301200

Healthcare Sector DDoS Guide

Executive Summary

A Distributed-Denial-of-Service (DDoS) attack is a type of cyber attack in which an attacker uses multiple systems, often referred to as a botnet, to send a high volume of traffic or requests to a targeted network or system, overwhelming it and making it unavailable to legitimate users. With the number of attacks increasing every year, they can come at any time, impact any part of a website's operations or resources, and lead to massive amounts of service interruptions and huge financial losses. In the health and public health (HPH) sector, they have the potential to deny healthcare organizations and providers access to vital resources that can have detrimental impact on the ability to provide care. Disruptions due to a cyber attack may interrupt business continuity by keeping patients or healthcare personnel from accessing critical healthcare assets such as electronic health records, software based medical equipment, and websites to coordinate critical tasks. As such, this comprehensive DDoS guide is intended for target healthcare audiences to understand what DDoS attacks are; what causes them; types of DDoS attacks with timely, relevant examples; and mitigations and defenses against a potential attack.

Report

Not to be confused with Denial-of-Service (DoS) attacks, which usually attacks from a single system, a DDoS attack originates from multple sources and sends a larger volume of traffic into the system at once, making it difficult for network administrators to quickly detect and eliminate the threat. DDoS attacks have continually grown in size and sophistication, but 2023 accelerated this trend at an unforeseen pace. Last year alone, cybercriminal groups, geopolitically motivated hacktivists, and malicious actors utilized the relatively inexpensive cost of launching DDoS attacks, the scale of massive botnets built from everyday digital and Internet of Things (IoT) devices, and protocol-level zero-day vulnerabilities to launch record-breaking attacks on businesses, government institutions, and, most disturbingly, on critical but vulnerable public infrastructure, including hospitals.

In most cases, the assumed goals are to cause damage, productivity loss, and financial losses and to gain public attention, which is why these threat actors select an increasingly broad range of victims who are known to have insufficient IT security. It is important to remember that DDoS attacks are targeted attacks for which the threat actors consciously select their targets. Threat actors utilize DDoS attacks due to the cost effectiveness and relatively low resources and technical skills needed to deploy this type of attack as a hacker does not have to install any code on a victim's server. Moreover, DDoS attacks are getting more sophisticated and complex while getting easier and cheaper to perpetrate as cyber criminals take advantage of the sheer number of insecure internet-connected devices.

Profile of a DDoS Attacker

DDoS attackers are often groups of attackers well known to authorities and use DDoS tactics to gain influence, disrupt government and military operations, or cause people to lose confidence in a market sector, company brand, or long-established institution. While any type of cyber threat actor (i.e., advanced persistent threats, cybercriminal groups, individuals, etc.) could orchestrate DDoS attacks, one of the biggest shifts in the DDoS threat landscape is the rise of hacktivist groups and the emergence of political motivation, rather than financial motivation, as the main driver for DDoS attacks.

Often considered a form of crowd-funded cyber terrorism, these groups present themselves as quasi-military organizations to solicit donations in cryptocurrency on social media channels to perpetrate DDoS

[TLP:CLEAR, ID#202405301200, Page 1 of 10]

U.S. Department of Health and Human Services
Health Sector Cybersecurity Coordination Center (HC3) www.HHS.GOV/HC3

Clearwater

Relevant Threat Reports: HHS HC3

5/23 Flashpoint is observing that Russian advanced persistent threat (APT) groups are evolving their tactics, techniques, and procedures (TTPs)—while also expanding their targeting. **They are using new spear-phishing campaigns to exfiltrate data and credentials by delivering malware sold on illicit marketplaces**.

4/10 The Department of Health and Human Services' Health Sector Cybersecurity Coordination Center (HC3) April 5 released an advisory on the top 10 ransomware groups targeting the health care sector. **HC3 has tracked over 530 attacks against the U.S. health care sector in the past six months**, nearly half of them ransomware related. **HC3 also recently released an advisory recommending actions to protect against advanced social engineering attacks targeting IT help desks in the health care sector.**

5/25 BEC attacks target human weaknesses, such as the tendency to trust authority figures, act impulsively, and respond emotionally to urgent requests. **These attacks often start with a phishing email and the theft of credentials, although spoofing is also used to impersonate an authority figure without access to their email account.**

https://www.hipaajournal.com/hph-sector-business-email-compromise-attacks/

Clearwater

By the Numbers – Bad Guys

3.4B phish sent daily

of phishing emails get opened

Most Common Words:

Urgent 8%
Important Updates 8%
Important 5%
Attention 2%

of businesses are targeted for spear phishing each year

24% of BEC was about payroll changes

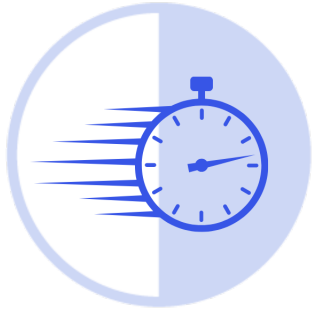
of phish sites use SSL certs

1M attacks using MFA bypass per month

10M TOAD attacks per month

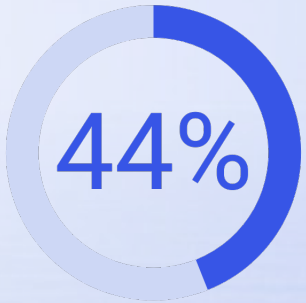
Clearwater

By the Numbers – Good Guys

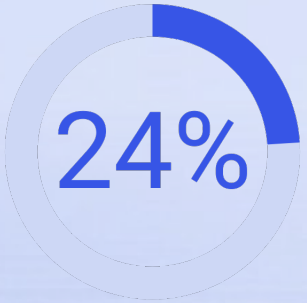


19% make risky decisions to save time

10% make risky decisions to meet a performance objective



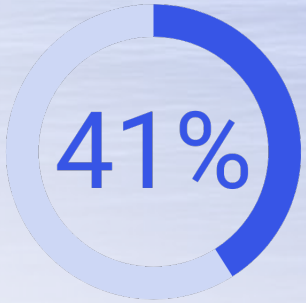
take risky actions for convenience



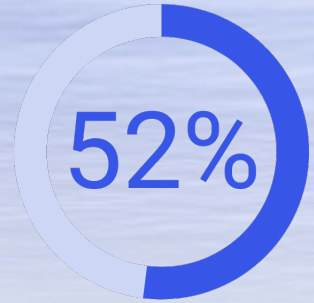
take risky actions for urgent deadlines

of social media users post job status and employer

of social media profiles are public



of staff feel responsible for security



of staff aren't sure if security is their responsibility

How to reduce the risk of BEC and Social Engineering

- Staff Awareness
  - Research is phase one of a BEC attack
    - Social presence of staff can be a significant source of information
      - Post Vacations and Plans before hand - increased plausibility
  - Educate on what is BEC and Social Engineering
    - Samples, Goals, and Tactics
  - Discuss ahead of time how to handle “payment, payroll, or wire” requests
    - Remove the concept of things like this being done in total secrecy
    - Secondary Validation
    - Don’t underestimate the influence of an apparent request from an executive
  - Ensure all staff know part of their responsibility is cybersecurity
    - Highlight examples of their impact and how they can help

How to reduce the risk of BEC and Social Engineering

- Technical Controls
  - Implement, Confirm and Test Email Protocol Protections
    - DomainKeys Identified Mail (DKIM)
    - Sender Policy Framework (SPF)
    - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
  - Enable email access controls
    - MFA for all email access
    - GEO Fence
    - Don’t ignore mobile devices
  - Implement Strong Anti-Phish Protections
    - Two Layers not uncommon – should include URL and attachment scanning
    - Label all external emails as such

How to reduce the risk of BEC and Social Engineering

Technical Controls (cont'd)

Enable proper audit logging within Email Systems

- Don't assume Cloud Defaults are adequate – they are not

Operational Controls

Monitoring of Activities

Incident Response Planning

Regular Security Audits

Business Email Compromise Assessment

Clearwater

Q&A

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Upcoming Events

Incident Response Webinar | June 20

- Partnering with 1st Responder and Jarrad Communications
- Register Here

HCCA Research Compliance Conference | June 10-12 – New Orleans, LA

- Andrew Mahler Speaking on patient's rights in research studies

AHLA Annual Conference | June 24-27 – Washington, DC

Cyber Briefing | July 11

- With Bob Chaput on how to engage your C-suite and board in effective & ongoing Enterprise Cyber Risk Management dialogue.
- Register Here

Clearwater

Clearwater

Healthcare–Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-security-llc/

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.