Legal Disclaimer

Although the information provided by Clearwater Compliance 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 Compliance LLC.

Clearwater

Healthcare – Secure, Compliant, Resilient

Monthly Cyber Briefing

August 2023

Agenda

- Cyber update
- Healthcare Threat Intelligence:
  - Relevant Industry Advisories & Threat Briefings
  - Healthcare Threat Assessment
  - Top Drivers of Risk
  - Managed Security Services and Risk Analysis Themes
  - SOC Trends

August Speakers

Steve Cagle, MBA, HCISSP
Chief Executive Officer

Dave Bailey, CISSP
VP, Consulting Services

Ryan Brown, CEH, GIAC
SOC 3 Analyst

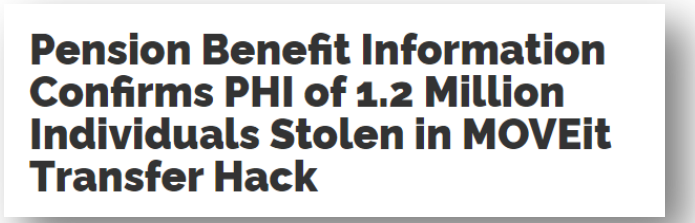
Clearwater

Cyber Update

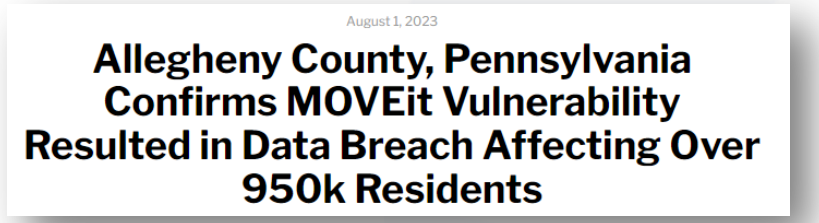
Steve Cagle

Healthcare Breaches in July

- 37 breaches and 3 million records reported to OCR Breach Portal in July
- More breaches reported as a result of MOVEit & Cl0P



Largest breach in healthcare reported on OCR's breach portal in July. (HCA breach of 11 million records not yet reported).



Over 689K+ records in this breach were reported by Allegheny County to OCR as records containing ePHI.

Centers for Medicare & Medicaid Services breached via contractor / business associate.

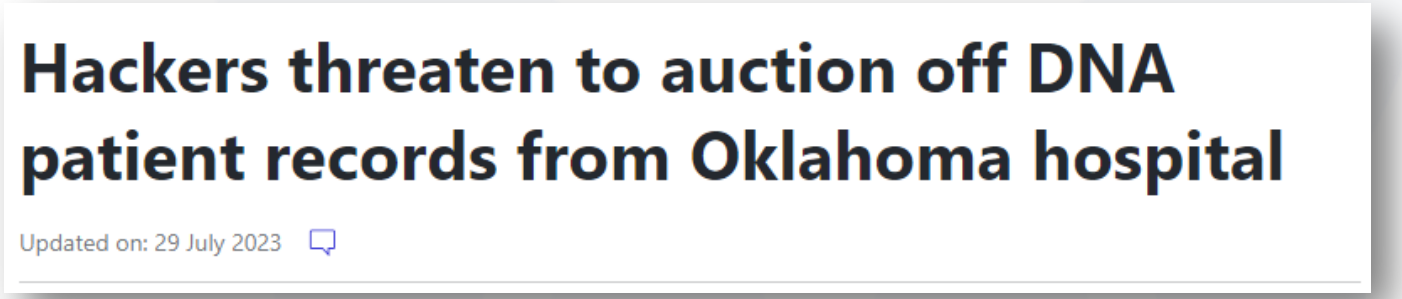
Healthcare Breaches in July (cont.)

Panorama Eyecare's breach caused by LockBit led to exposure of ePHI from 4 separate Healthcare provider customers

Screenshot from Lockbit leak site

[Recent Karakurt ransomware attack on McAlester Regional Health]

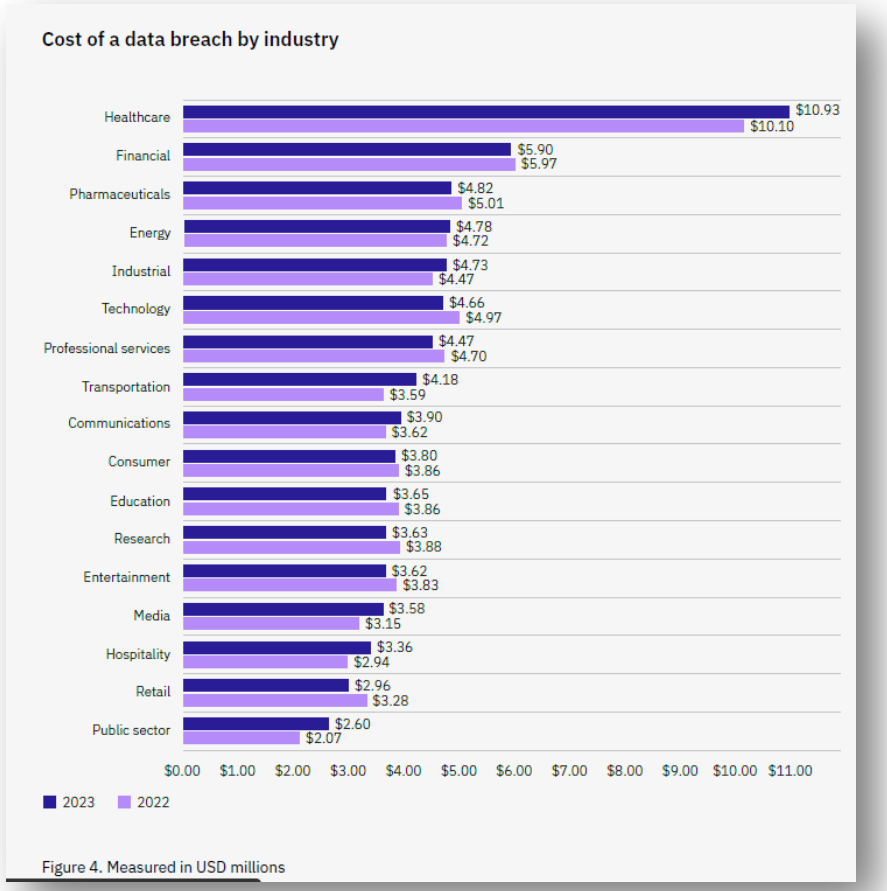
Cybersecurity and Infrastructure Security Agency (CISA) warned about Karakurt in an advisory in June 2022.



Hackers threaten to auction off DNA patient records | Cybernews

Clearwater

Ponemon “Cost of a Data Breach” Report 2023



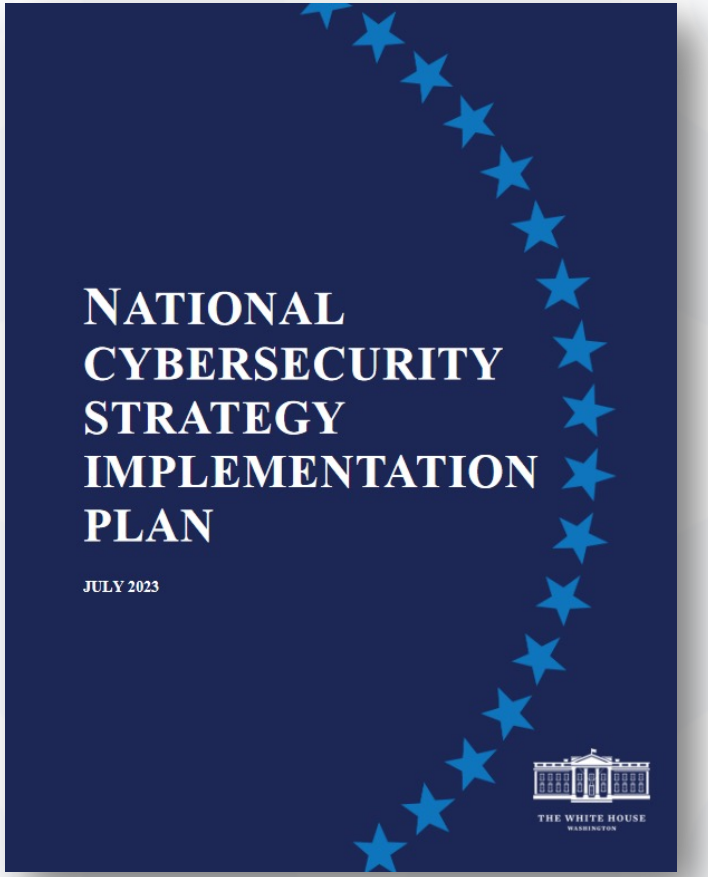
- Average cost of a breach is $4.45 million across all industries
- Breach cost in healthcare is $11m, by far the highest in any industry
- 51% or organizations are increasing spending on cybersecurity

Link to Register to Download the Report

Clearwater

National Cybersecurity Implementation Plan Released

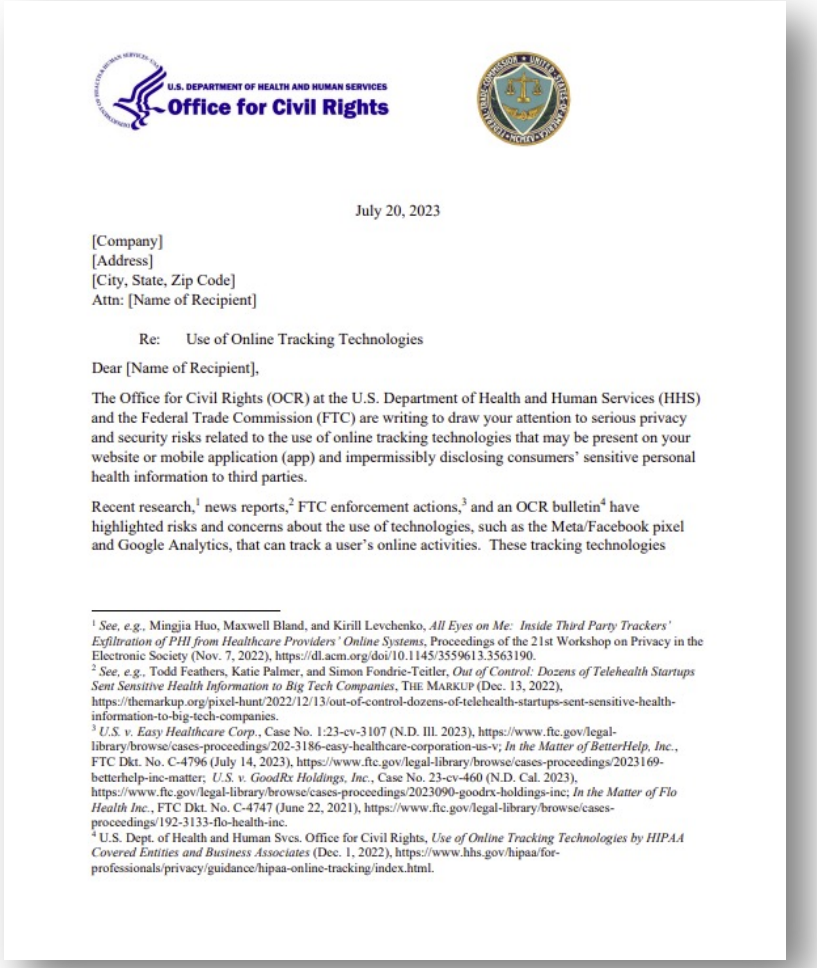
- Follow-up to National Cybersecurity Strategy
- Roadmap for implementation of strategy
- 65 initiatives broken out by strategic pillar
- Assigns agency responsibility
- Focuses on aligning stakeholders and creating “incentives” for investment



Released in July

Clearwater

FTC & OCR Issue Joint Warning on Use of Online Tracking Technologies



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

July 20, 2023

[Company]
[Address]
[City, State, Zip Code]
Attn: [Name of Recipient]

Re: Use of Online Tracking Technologies

Dear [Name of Recipient],

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) are writing to draw your attention to serious privacy and security risks related to the use of online tracking technologies that may be present on your website or mobile application (app) and impermissibly disclosing consumers' sensitive personal health information to third parties.

Recent research,[1] news reports,[2] FTC enforcement actions,[3] and an OCR bulletin[4] have highlighted risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies

[1] *See, e.g.*, Mingjia Huo, Maxwell Bland, and Kirill Levchenko, *All Eyes on Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems*, Proceedings of the 21st Workshop on Privacy in the Electronic Society (Nov. 7, 2022), https://dl.acm.org/doi/10.1145/3559613.3563190.
[2] *See, e.g.*, Todd Feathers, Katie Palmer, and Simon Fondrie-Teitler, *Out of Control: Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, THE MARKUP (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies.
[3] *U.S. v. Easy Healthcare Corp.*, Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; *In the Matter of BetterHelp, Inc.*, FTC Dkt. No. C-4796 (July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; *U.S. v. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; *In the Matter of Flo Health Inc.*, FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc.
[4] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

- Sent to 130 healthcare providers to draw attention to serious privacy and security risks on their web sites or mobile apps
- Reminder of obligations of those subject to under HIPAA, FTC Act and FTC Breach Notification Rule, and OCR Guidance on Tracking Technologies
- Reminder of recent enforcement, with respect to tracking technologies
- "…We strongly encourage you to review the laws cited in this letter and take action to protect the privacy and security of individuals' health information."

Clearwater

Link to Model Letter: Use of Online Tracking Technologies (ftc.gov)

Recommendations About Online Tracking Technologies

- Map your data, and understand what is tracked on your site, and where the data goes
- Determine regulations you are subject to
- Update policies and procedures
- Make sure any statements you are making about privacy and security practices are accurate
- Review third party agreements, and if they are impermissibly acquiring data
- If you have had a breach under the recent guidance by OCR, FTC's health Breach Notification Rule, or other (e.g., state) regulation

Re-iterating Recommendations For Mature Organizations to Address Current Threat Environment

- Know where your data is! Ensure Risk Analysis is up to date and has analyzed specific risks and controls at the information systems level
- Respond to high risks through diligent risk treatment and risk management processes
- Conduct on-going vulnerability management – not just periodic scans – and patch critical or high vulnerabilities
- Monitor and act on-going threat intelligence and alerts from H-ISAC, CISA, and other agencies
- Ensure that the security controls you have in place are working as you expect
- Assess high impact third parties for risk, including asking questions about their vulnerability management programs and risk analysis
- Develop and test incident response plans
- Consider increasing security awareness training and social engineering tests

Healthcare Threat Intelligence

Dave Bailey

Ryan Brown

Purpose

- Provide relevant industry updates and threat briefings
- Present a healthcare assessment of the adversary
- Provide an overview of risk drivers; a Clearwater perspective

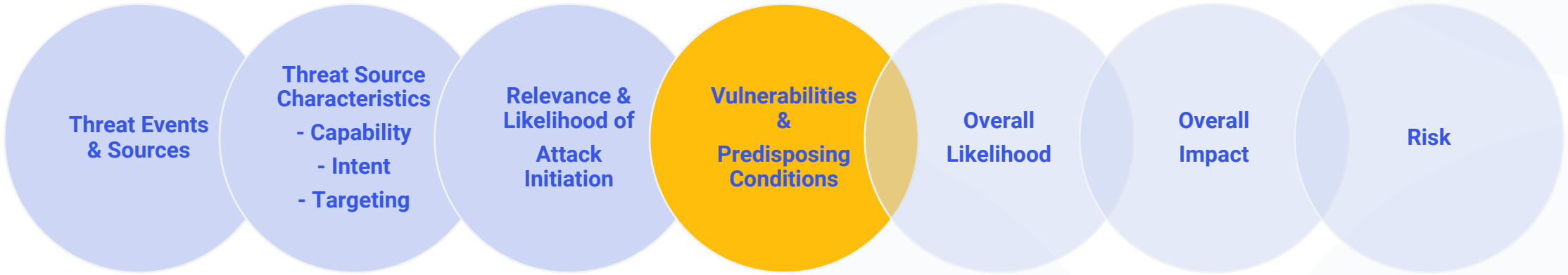
Perspective

- Turn information into action;
- Improve the effectiveness of risk determination
- Improve relevance

The first step in the risk management process is to acknowledge the reality of risk. Denial is a common tactic that substitutes deliberate ignorance for thoughtful planning

Effective Risk Management: Know Your Adversary

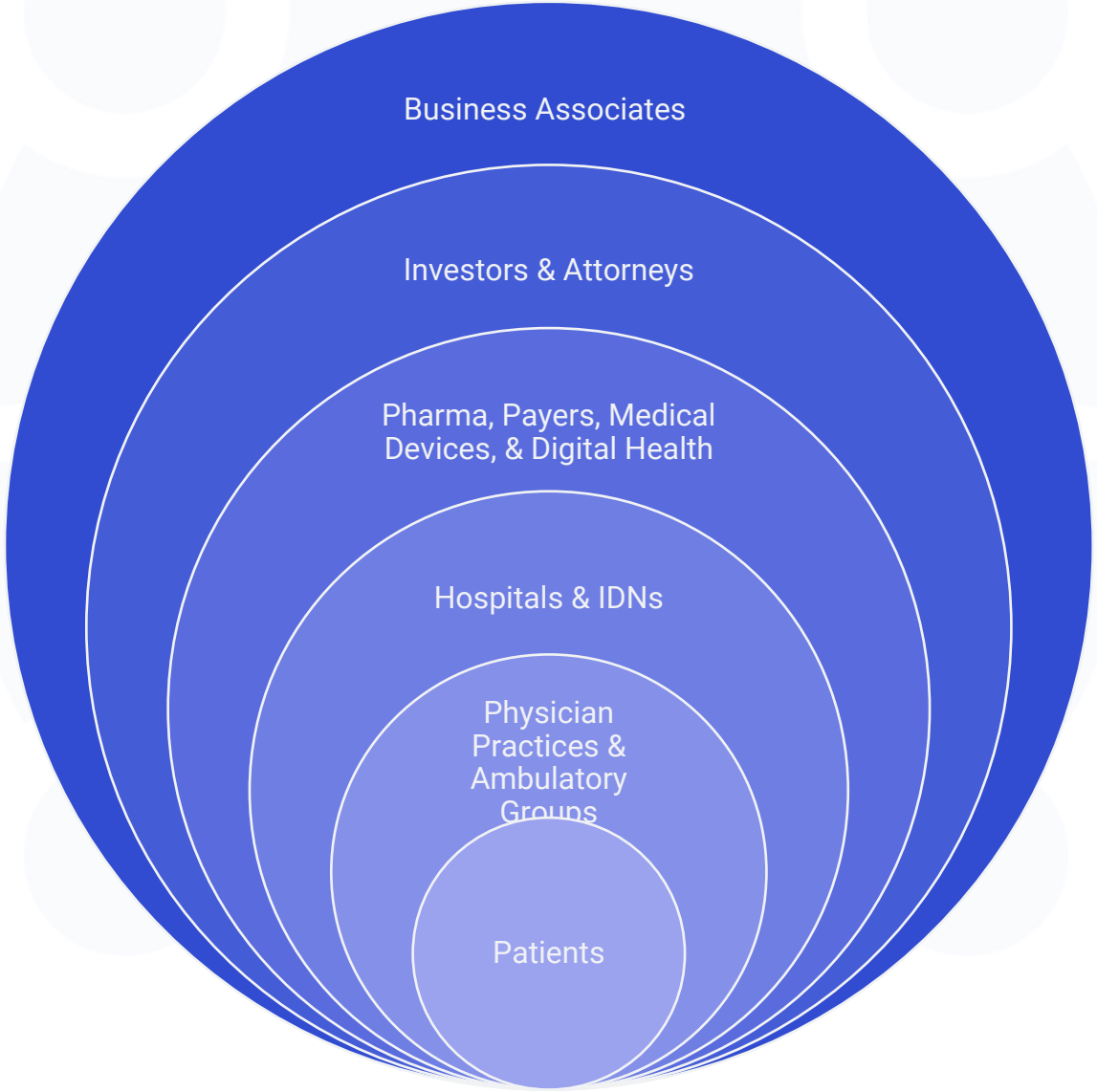
Risk defined by NIST 800-30



Know your Adversary | Know your Security Program | Know your Risk & Know your Opportunity

Target Landscape: Healthcare

- Large connected ecosystem and attack surface
- Third-party dominance; cloud, analytics, automation, & point of care systems



Clearwater

Relevant Industry Advisories & Threat Briefings

Relevant Industry Advisories and Threat Briefings

Cybersecurity Advisory: Threat Actors Citrix CVE-2023-3519 to Implant Webshells

- CISA has issued a cybersecurity advisory to alert network defenders about the exploitation of CVE-2023-3519, an unauthenticated remote code execution (RCE) vulnerability in NetScaler ADC and NetScaler Gateway
- **June 2023**, threat actors used this zero-day vulnerability to place a webshell on a critical infrastructure organization's NetScaler ADC appliance in a non-production environment
- This allowed the actors to conduct discovery on the victim's active directory (AD) and gather and exfiltrate AD data

HC3: Sector Alerts

- **July 20, 2023**: Citrix ADC and Gateway Vulnerabilities Sector Alert
- **June 16, 2023**: Critical Vulnerability in MOVEit Transfer Software Sector Alert
- **Jun 2, 2023**: MOVEit Transfer Software Sector Alert

HC3: Threat Briefs

- **July 13**, 2023: AI Cybersecurity and the Health Sector
- **June 8, 2023:** Types of Threat Actors That Threaten Healthcare
- **April 6, 2023**: EMRs A Top Target for Cyber Threat Actors

The Impacts of Artificial Intelligence

- How AI is impacting Cyberthreats: Threat Actors are using AI for both designing and executing attacks
  - Development of phishing emails
  - Impersonation attacks
  - Rapid exploitation of vulnerabilities
  - Development of complex malware code
  - Deeper target reconnaissance
  - Automation of attacks
  - Overwhelming human defenses
  - Ransomware; wider spread and more evasive

Clearwater

Time to act: Artificial Intelligence

- Integrate AI into existing governance practices; what are the use cases?
- Determine and implement reasonable and appropriate controls to safeguard your data from AI based threats
- Assess AI technology as part of overall risk management strategy

Relevant Industry Threat Briefings

- Top Attacks Utilized by Cyber Threat Actors
  - Social Engineering
  - Phishing; Business Email Compromise
  - Distributed Denial of Service (DDoS)
  - Botnet
  - Zero-day Vulnerability/Exploit
  - Person-in-the-Middle (PTM)
  - Malware
  - Adware
  - Ransomware

Clearwater

Healthcare Threat Assessment

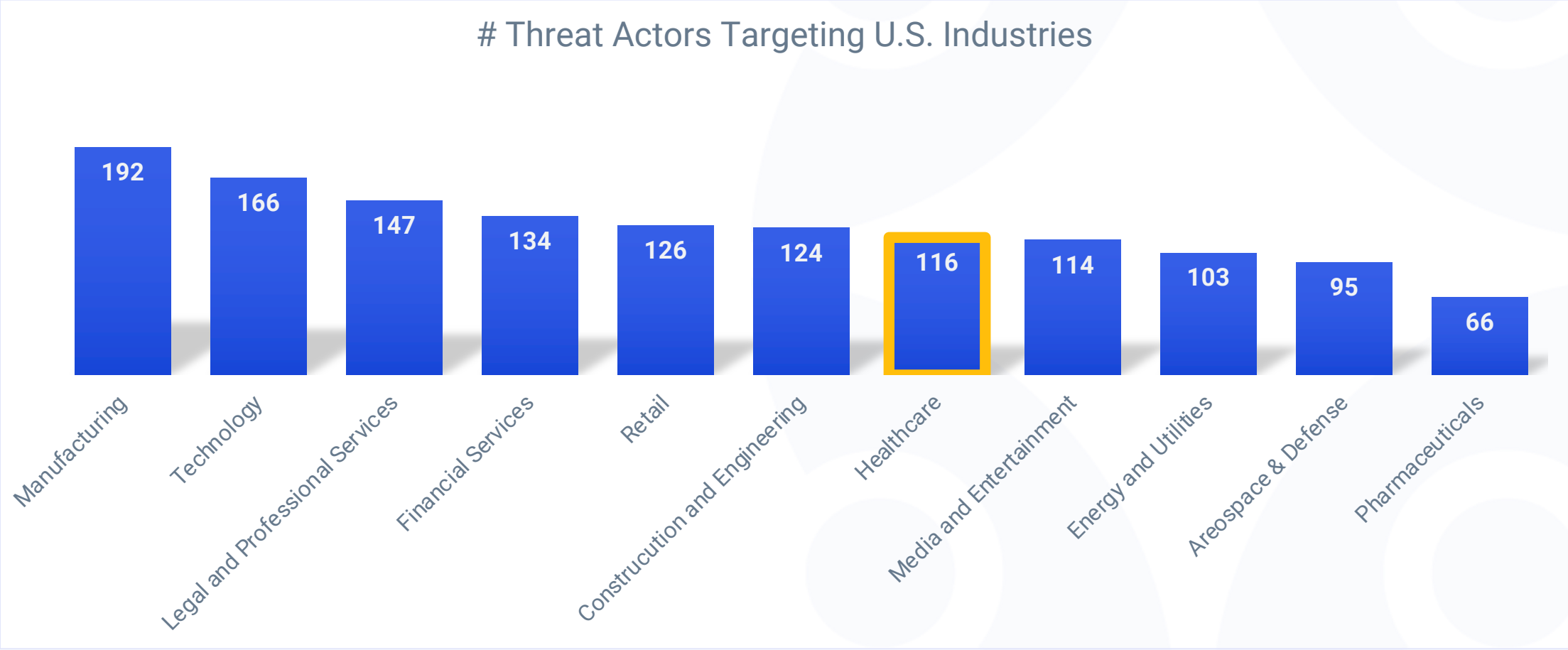
Adversarial Threat

Healthcare Threat Assessment: Characteristics of the Adversary

CAPABILITY	Very Low	Low	Moderate	High	**Very High**	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
INTENT	Very Low	Low	Moderate	**High**	Very High	The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.
TARGETING	Very Low	Low	Moderate	**High**	Very High	The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.
RELEVANCE	Possible	Predicted	Anticipated	**Expected**	Confirmed	The threat event or TTP has been seen by the organization's peers or partners.
LIKELIHOOD	Very Low	Low	Moderate	**High**	Very High	Adversary is almost certain to initiate the threat event.

Threat Actor Overview

As of Aug 2023, 116 threat actors target the US healthcare industry



Clearwater

Source: Mandiant Threat Intelligence

Threat Intelligence Report – As of July 2023

- 246 Actors targeting US Industries; +9
- 116 Actors targeting US Healthcare Industry; +7
- Europe and Asia are primary known target source regions

Source Region	# Actors
Europe	22 (+2)
Asia	49 (+1)
Unknown	45 (+4)
Total Targeting US Healthcare	**116**

Source: Mandiant Threat Intelligence

Clearwater

Typical Ransomware: How They Attack

MITRE ATT&CK Enterprise Tactics

Clearwater

Assumptions and Takeaways From an Attack

- A threat actor was present on your network
- Data may be exfiltrated; assume it was and prove otherwise
- At least one account was compromised; most likely many
- Network may still be compromised; assume it was and prove otherwise

Top Drivers of Risk

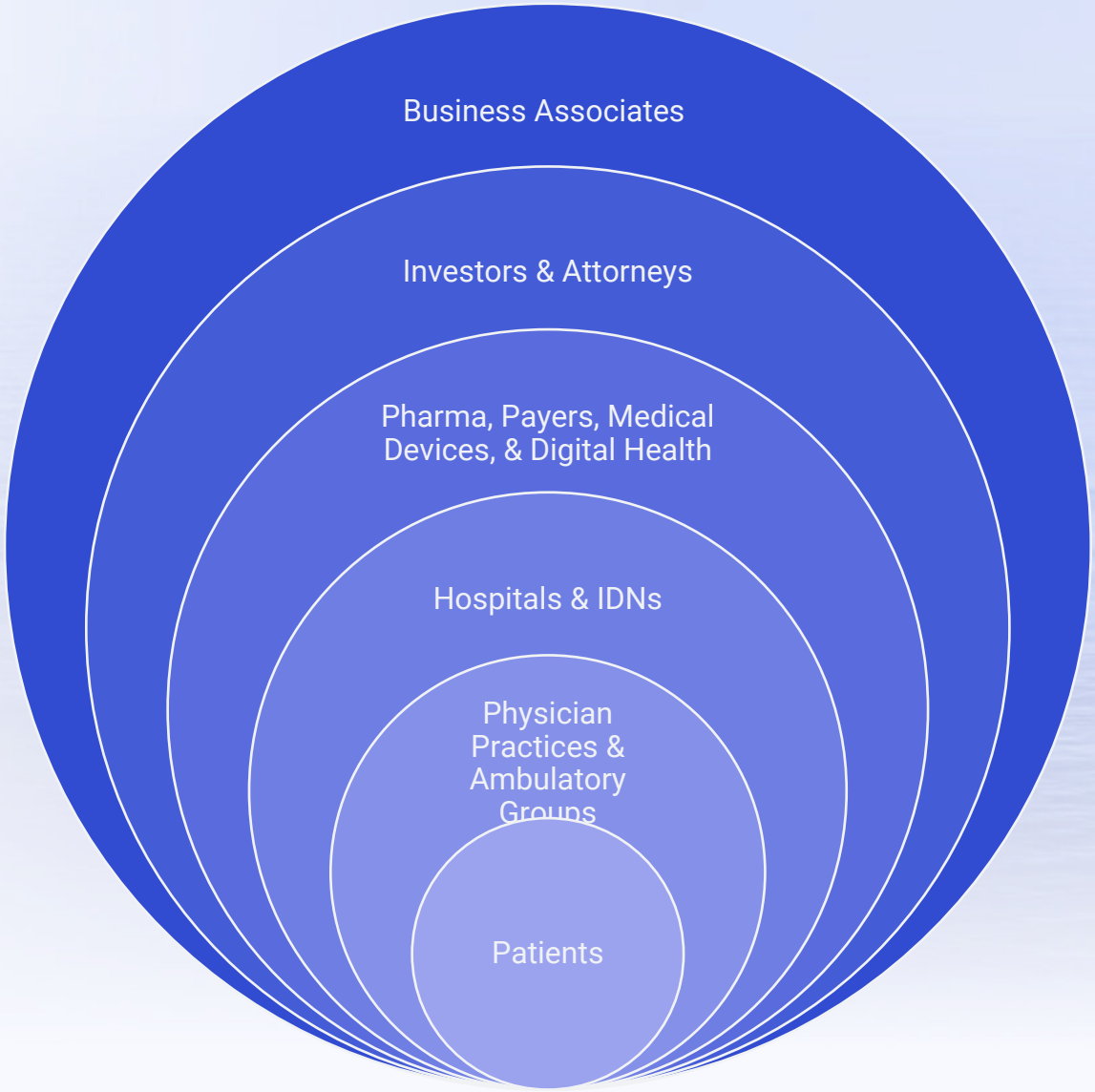
A Clearwater Perspective

Listen to the Full Episode

https://clearwatersecurity.com/monthly-cyber-briefing/

Target Landscape: Clearwater Perspective Q3 2023

- Weaknesses identified as part of:
  - Managed Security Services and Security Operations Center
  - Asset Based Risk Analysis using IRM Analysis
  - NIST CSF Performance Program Assessments



Clearwater

Clearwater Managed Security Services and Risk Analysis

Common Themes Identified by Clearwater During Risk Analysis and Assessment

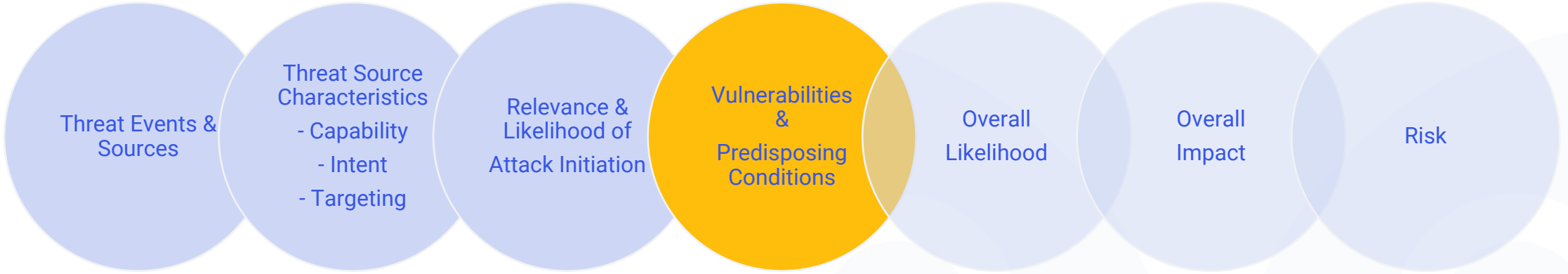
- Organizations lack adequate controls to protect user identities
  - Dormant Accounts, Privileged Access Management, MFA, User Provisioning
- Not all network connected assets are formally managed, have adequate safeguards implemented, and secured
- Not all assets are continually monitored to detect and respond to cyber attacks
- Networks are not adequately segmented
- Organizations are operating known unpatched, legacy, and unsupported systems
- A formal and complete Business Impact Analysis is not performed

Top Drivers of Risk Categorized by NIST CSF

Function	Description	Category
Identify (ID)	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	• **Asset Management ID.AM** • **Business Environment ID.BE** • Governance ID.GV • Risk Assessment ID.RA • **Risk Management ID.RM** • **Supply Chain Risk ID.SC**
Protect (PR)	Develop and implement appropriate safeguards to ensure delivery of critical services	• **Identify Management, Authentication, and Access Control PR.AC** • **Awareness & Training PR.AT** • **Data Security PR.DS** • **Information Protection Processes and Procedures PR.IP** • Maintenance PR.MA • **Protective Technology PR.PT**
Detect (DE)	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.	• Anomalies and Events DE.AE • **Security Continuous Monitoring DE.CM** • Detection Processes and Procedures DE.DP
Respond (RS)	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.	• Response Planning RS.RP • Communications RS.CO • Analysis RS.AN • Mitigation RS.MI • Improvements RA.IM
Recover (RC)	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.	• Recovery Planning RC.RP • Improvements RC.IM • Communications RC.CO

Time to Act: Remediate and Reduce your Risk Profile

- The adversary has a higher likelihood of conducting successful attacks based on these common themes
- Immediately put plans in place to address these weaknesses



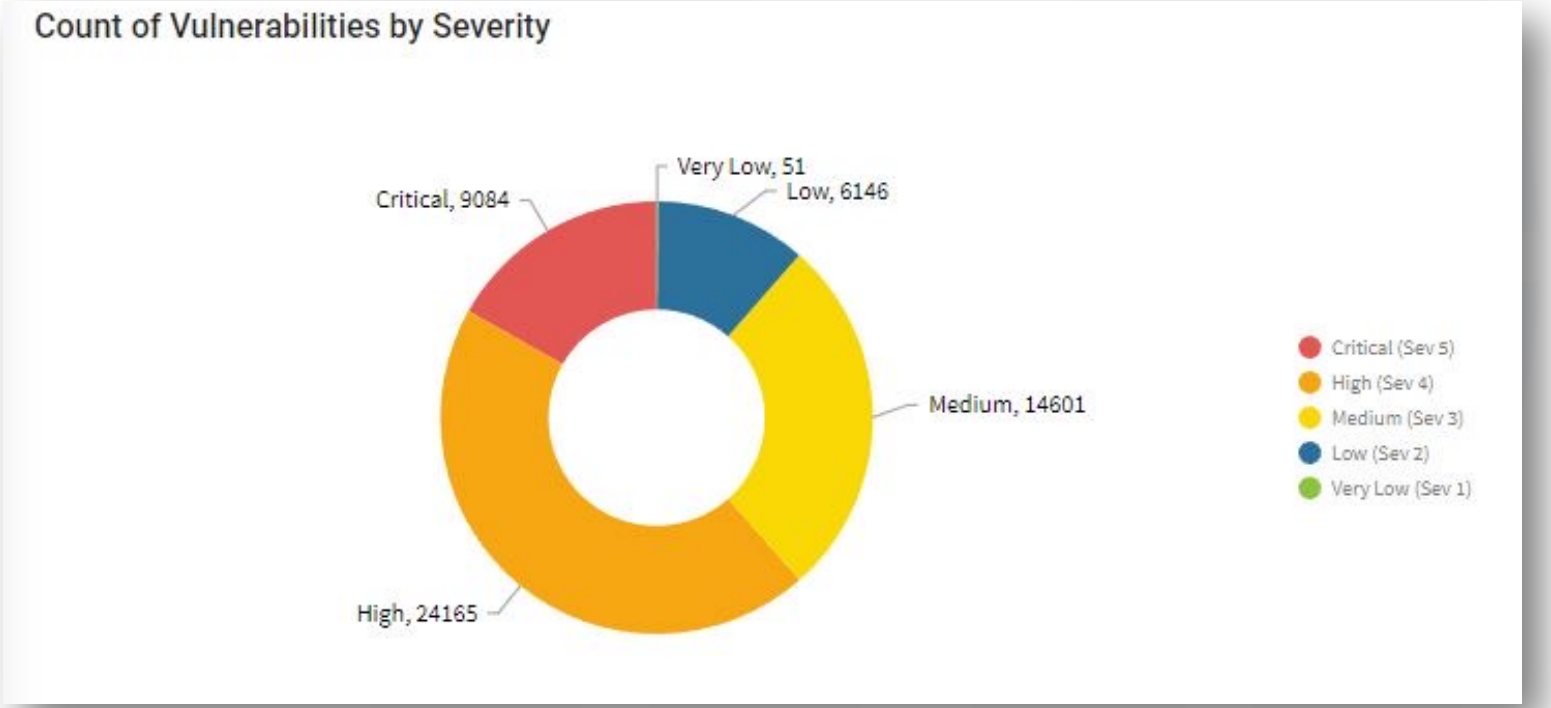
Clearwater

Clearwater Security Operations Center

Threat Perspective

Un-Patched Systems – Increases Attack Surface

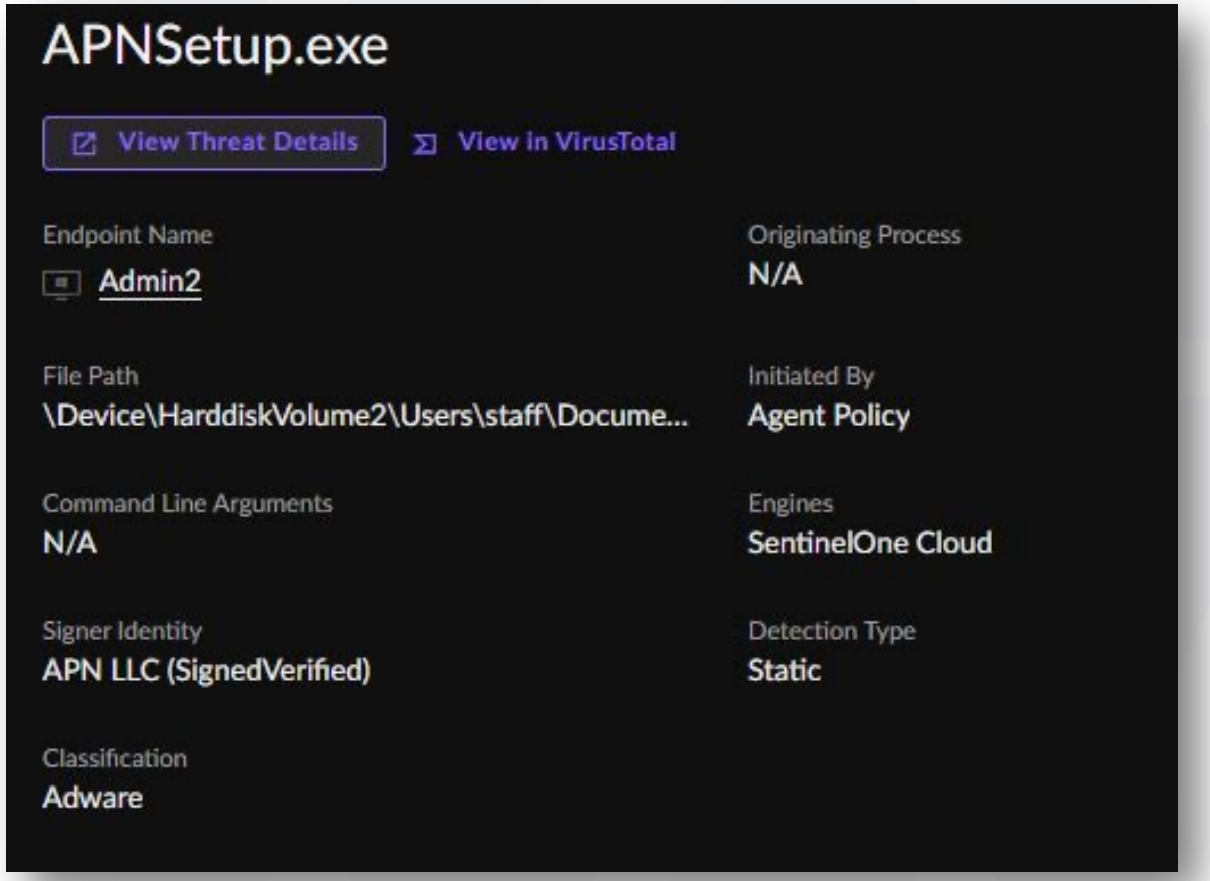
- Protected systems with out-of-date patching/updates
- Critical CVE's missing
- 3rd party software missing updates



Clearwater

Effects of Not Patching/Updating Systems

- Increases attack surface
- Easier for an adversary to maintain a persistent stronghold on the network
- Enables installation of malware
- Increases the risk of successful data exfiltration



True Positive Alerts Last Quarter

- A majority of the True Positive alerts in EDR were suspicious adware and 3rd party add-ons

- Peer Relevance: The Clearwater SOC detected and responded to:

4%	4%	4%	4%
Hacktools	Trojans	Viruses	Ransomware Attempts

Clearwater

Time to Act: Patch Your Systems

- The alerts validate threat actors are actively targeting and attacking healthcare organizations and business associates
- Implement an effective timeframe to patch critical vulnerabilities: you have a greater risk exposure immediately following an advisory
- Upgrade legacy and unsupported systems

Q&A

Steve Cagle
Dave Bailey
Ryan Brown

We are here to help.

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

Clearwater

Healthcare – Secure, Compliant, Resilient

Contact us

info@clearwatersecurity.com

www.clearwatersecurity.com

1.800.704.3394