Monthly Cyber Briefing

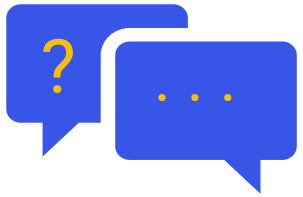
December 5, 2024

Clearwater

Meeting Logistics

Microphones

All attendees are on mute.



Questions

Type your questions in the Q&A chat box.

Materials

Briefing materials and recording will be provided after event.

Survey

Survey will prompt at the end of webinar.

Clearwater

Agenda & Speakers

- Cyber & Regulatory Update
- The State of Vulnerability Management in Healthcare
- Q+A
- Upcoming Events

Steve Akers

Chief Technology Officer, Managed Security Services, & Corporate CISO
Clearwater

Steve Cagle

Chief Executive Officer
Clearwater

Clearwater

Cyber & Regulatory Update

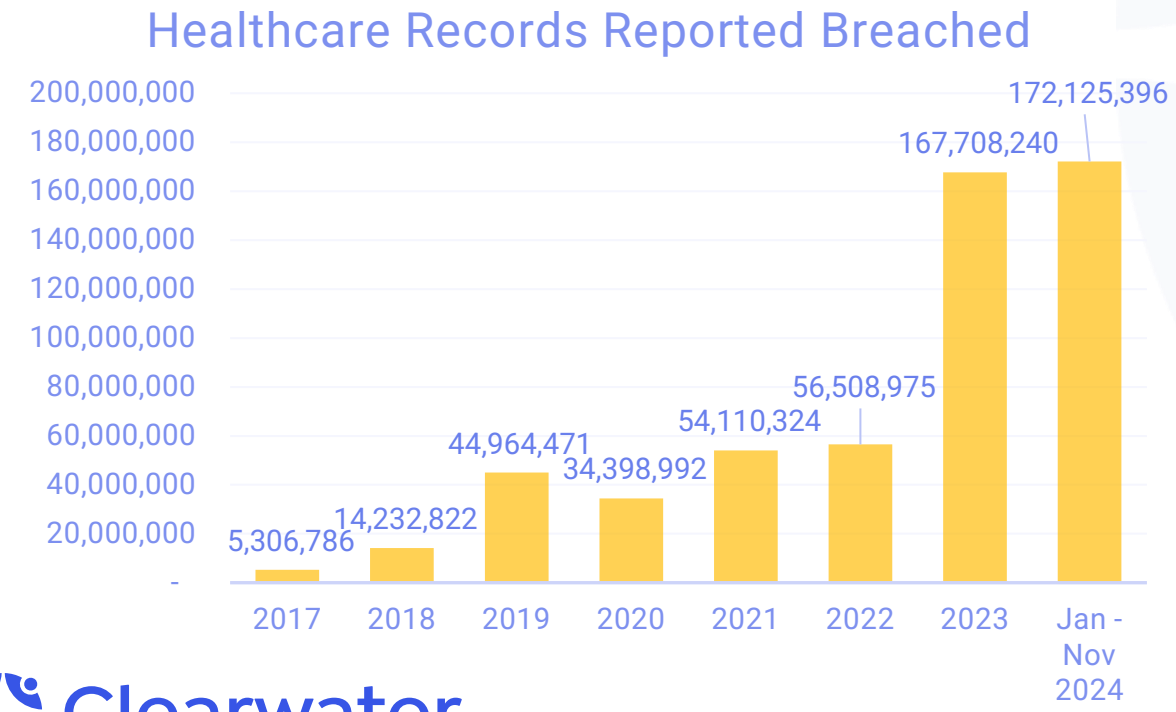
Steve Cagle

Clearwater

Breach Reports via OCR Breach Portal

OCR Breach Portal Data[1]

- In 2023 167.7M records reported as breached vs previously reported 144.4M records reported breached in 2023, an increase of 196% vs 56.5M in 2022
- YTD = 172M records from 642 breaches in 2024; 91% of records due to Hacking/IT Incident



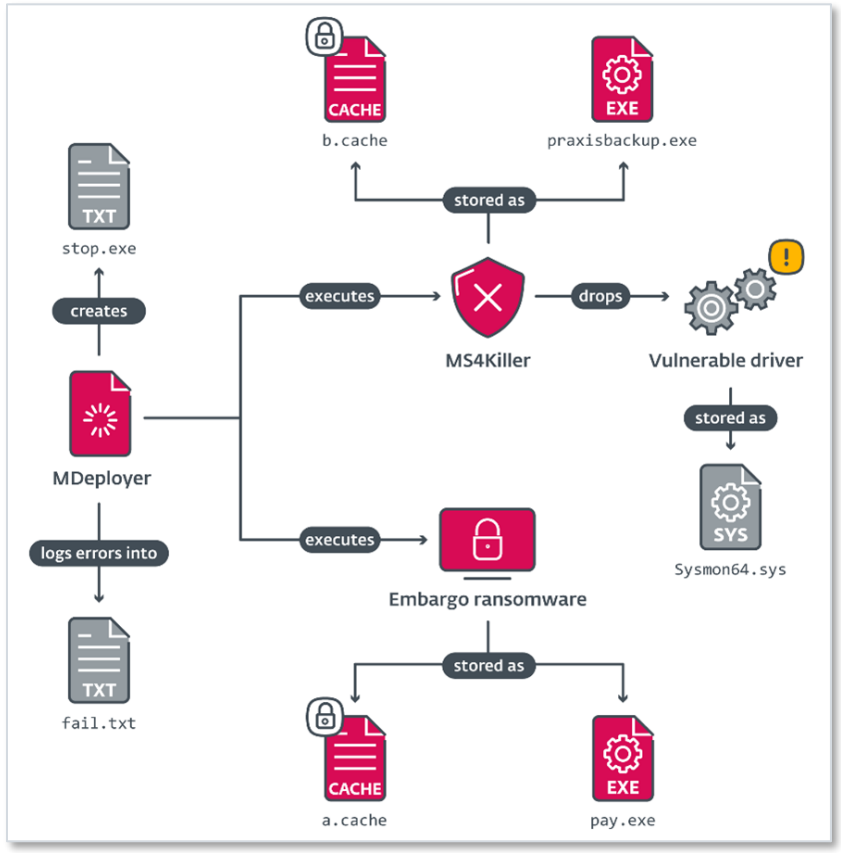
- 85% of all reported breaches in November (82% YTD) were from Healthcare providers vs. business associates or health plans
- Majority or provider reported breaches are from physician practices / specialty providers (vs hospitals)
- 366K records reported by Rocky Mountain Gastroenterology Associates PLLC, is the largest gastroenterology group in the Rocky Mountain region following a triple ransomware attack by RansomHub, Meow and Trinity[2]

Clearwater

1 The HHS Breach Portal (2024 data through 11/30/24, pulled on 12/1/24; 2023 data pulled 11/3/24)
2 Rocky Mountain Gastroenterology Reportedly Experiences Triple Cyberattack, Resulting in Data Breach Affecting Up to 169k | Console and Associates, P.C. - JDSupra

New Threat Actor of Note: Embargo Ransomware

Relatively new threat actor is targeting successfully healthcare using new class of EDR Killer software.



Source: ESET Threat Research

Victims

- Attacked Memorial Hospital and Manor an 80-bed hospital and 107-bed long-term care facility in Bainbridge, GA November 3rd , delaying patient care and claimed theft of 1TB of data[1]
- Ransomware attack on American Associated Pharmacies who allegedly paid the cyber criminals $1.3 million for decryption and now faces another $1.3 million demand to prevent exposure of its data[2]

TTPs[3]

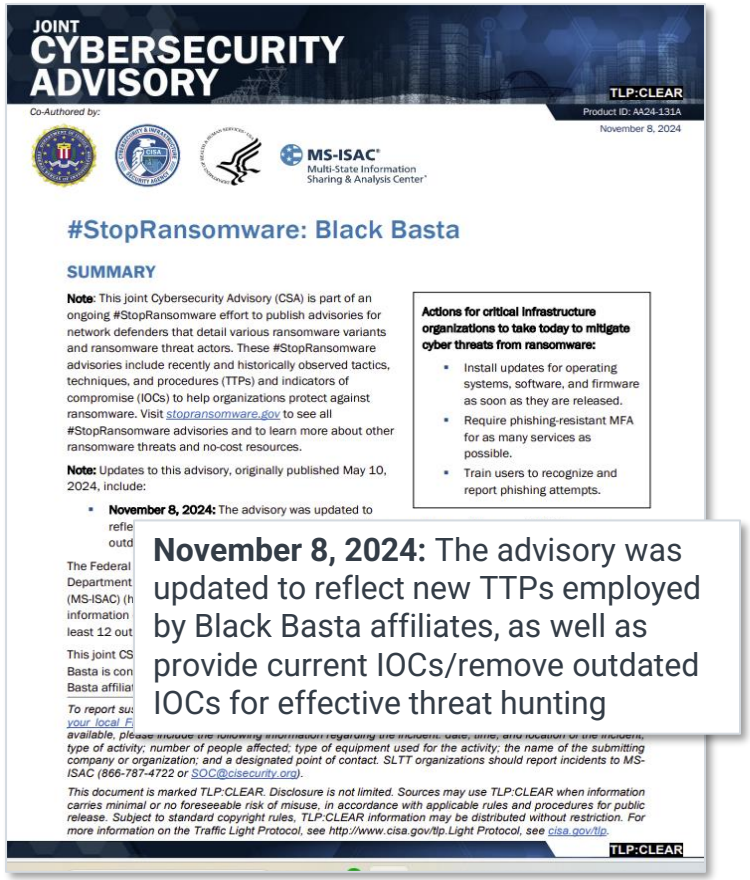
- New toolkit consists of a loader and an endpoint detection and response killer (EDR) MDeployer and MS4Killer
- Abuses Safe Mode and a vulnerable driver (Using BYVOD) to disable the security products running on the victim's machine
- Custom-compiled for each victim's environment, targeting specific security solutions
- Leverages double extortion technique, with payment required for decrypter key, and separate payment to not publish data

Clearwater

1 Ransomware Attack Disrupts Georgia Hospital's Access to Health Records – SecurityWeek
2 American Associated Pharmacies allegedly breached by Embargo ransomware | SC Media
3 New ransomware group Embargo uses toolkit that disables security solutions, ESET Research discovers | ESET

BlackBasta Escalating its Attack Techniques

The Black Basta ransomware group who has been a frequent focus of our cyber briefings has escalated its attack strategy to include email Bombing combined with social engineering Via MS Teams[1,2]



JOINT CYBERSECURITY ADVISORY

TLP:CLEAR

Co-Authored by:

Product ID: AA24-131A

November 8, 2024

MS-ISAC® Multi-State Information Sharing & Analysis Center®

#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.

Note: Updates to this advisory, originally published May 10, 2024, include:

- **November 8, 2024:** The advisory was updated to reflect new TTPs employed by Black Basta affiliates, as well as provide current IOCs/remove outdated IOCs for effective threat hunting

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 Department (MS-ISAC) (h information least 12 out

This joint CS Basta is con Basta affiliat

To report su your local F

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 http://www.cisa.gov/tlp. Light Protocol, see cisa.gov/tlp.

TLP:CLEAR

- CISA updated its Cybersecurity Advisory #Stop Ransomware: Black Basta on November 8th With new TTPS and IOCs
- Email bombing used to spam user's email box, followed by threat actor contacting victim by Microsoft Teams
- Display name included the string "Help Desk," often surrounded by whitespace characters, which is likely to center the name within the chat.
- Poses as help desk in Teams Chat. Sends QR Code and/or initiates MS Quick Assist to deploy loader and malware payload

Entra ID tenants observed:

- securityadminhelper.onmicrosoft[.]com
- supportserviceadmin.onmicrosoft[.]com
- supportadministrator.onmicrosoft[.]com
- cybersecurityadmin.onmicrosoft[.]com

Malicious files observed

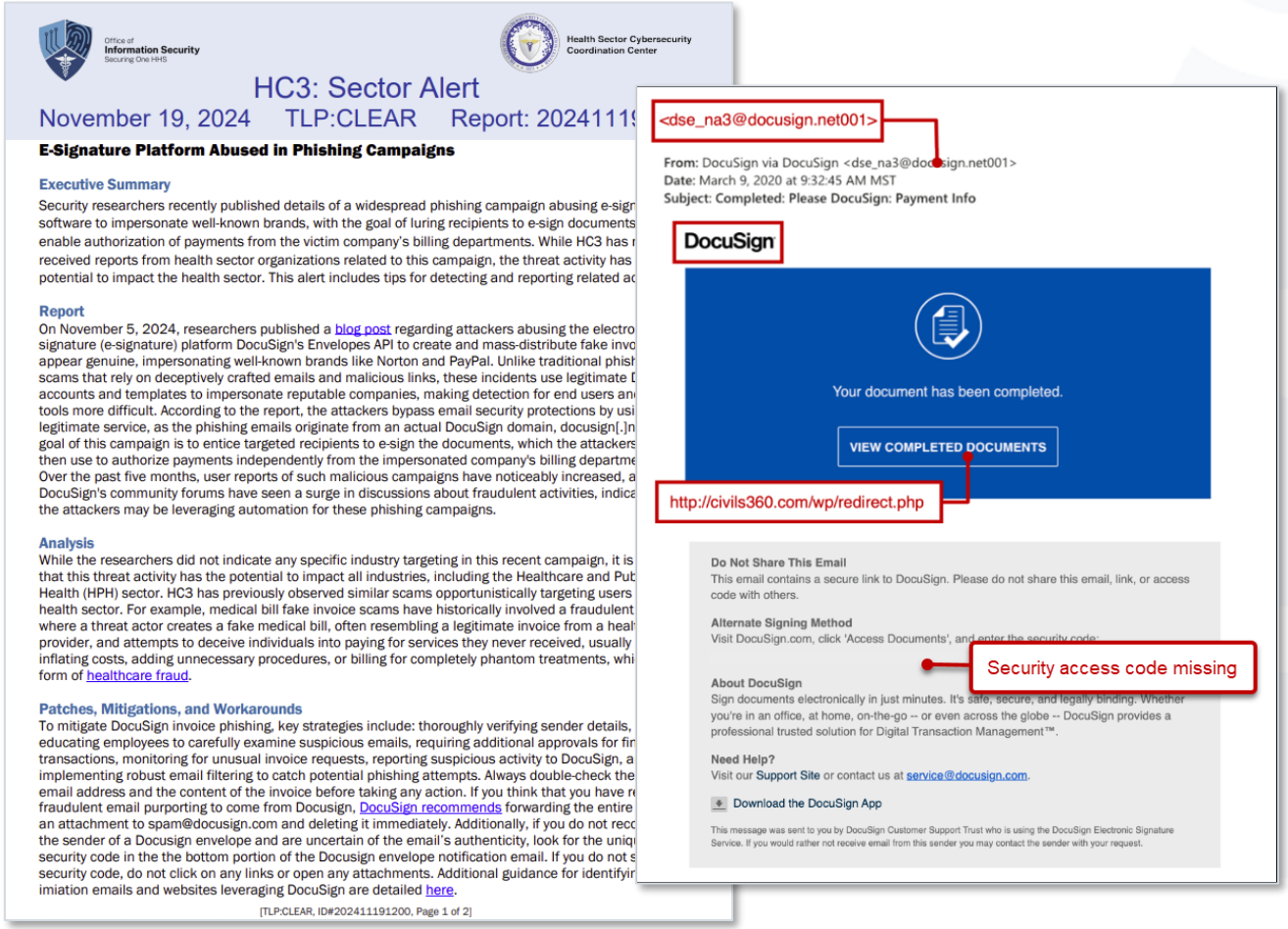
- AntispamAccount.exe
- AntispamUpdate.exe
- AntispamConnectUS.exe

Clearwater

1 ReliaQuest Uncovers New Black Basta Social Engineering Technique – ReliaQuest 10/25/24
2 #StopRansomware: Black Basta | CISA

E-Signature Platform Abused in Phishing Campaigns

Cybercriminals are leveraging DocuSign's APIs to send fake invoices that appear strikingly authentic.



Office of Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Sector Alert

November 19, 2024 TLP:CLEAR Report: 20241119

E-Signature Platform Abused in Phishing Campaigns

Executive Summary

Security researchers recently published details of a widespread phishing campaign abusing e-sign software to impersonate well-known brands, with the goal of luring recipients to e-sign documents enable authorization of payments from the victim company's billing departments. While HC3 has r received reports from health sector organizations related to this campaign, the threat activity has potential to impact the health sector. This alert includes tips for detecting and reporting related ac

Report

On November 5, 2024, researchers published a blog post regarding attackers abusing the electro signature (e-signature) platform DocuSign's Envelopes API to create and mass-distribute fake invo appear genuine, impersonating well-known brands like Norton and PayPal. Unlike traditional phish scams that rely on deceptively crafted emails and malicious links, these incidents use legitimate D accounts and templates to impersonate reputable companies, making detection for end users an tools more difficult. According to the report, the attackers bypass email security protections by usi legitimate service, as the phishing emails originate from an actual DocuSign domain, docusign[.]n goal of this campaign is to entice targeted recipients to e-sign the documents, which the attackers then use to authorize payments independently from the impersonated company's billing departme Over the past five months, user reports of such malicious campaigns have noticeably increased, a DocuSign's community forums have seen a surge in discussions about fraudulent activities, indica the attackers may be leveraging automation for these phishing campaigns.

Analysis

While the researchers did not indicate any specific industry targeting in this recent campaign, it is that this threat activity has the potential to impact all industries, including the Healthcare and Pub Health (HPH) sector. HC3 has previously observed similar scams opportunistically targeting users health sector. For example, medical bill fake invoice scams have historically involved a fraudulent where a threat actor creates a fake medical bill, often resembling a legitimate invoice from a heal provider, and attempts to deceive individuals into paying for services they never received, usually inflating costs, adding unnecessary procedures, or billing for completely phantom treatments, whi form of healthcare fraud.

Patches, Mitigations, and Workarounds

To mitigate DocuSign invoice phishing, key strategies include: thoroughly verifying sender details, educating employees to carefully examine suspicious emails, requiring additional approvals for fir transactions, monitoring for unusual invoice requests, reporting suspicious activity to DocuSign, a implementing robust email filtering to catch potential phishing attempts. Always double-check the email address and the content of the invoice before taking any action. If you think that you have r fraudulent email purporting to come from Docusign, DocuSign recommends forwarding the entire an attachment to spam@docusign.com and deleting it immediately. Additionally, if you do not rec the sender of a Docusign envelope and are uncertain of the email's authenticity, look for the uniq security code in the the bottom portion of the Docusign envelope notification email. If you do not s security code, do not click on any links or open any attachments. Additional guidance for identifyir imiation emails and websites leveraging DocuSign are detailed here.

[TLP:CLEAR, ID#202411191200, Page 1 of 2]

<dse_na3@docusign.net001>

From: DocuSign via DocuSign <dse_na3@docusign.net001>
Date: March 9, 2020 at 9:32:45 AM MST
Subject: Completed: Please DocuSign: Payment Info

DocuSign

Your document has been completed.

VIEW COMPLETED DOCUMENTS

http://civils360.com/wp/redirect.php

Do Not Share This Email
This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.

Alternate Signing Method
Visit DocuSign.com, click 'Access Documents', and enter the security code:

Security access code missing

About DocuSign
Sign documents electronically in just minutes. It's safe, secure, and legally binding. Whether you're in an office, at home, on-the-go -- or even across the globe -- DocuSign provides a professional trusted solution for Digital Transaction Management™.

Need Help?
Visit our Support Site or contact us at service@docusign.com.

Download the DocuSign App

This message was sent to you by DocuSign Customer Support Trust who is using the DocuSign Electronic Signature Service. If you would rather not receive email from this sender you may contact the sender with your request.

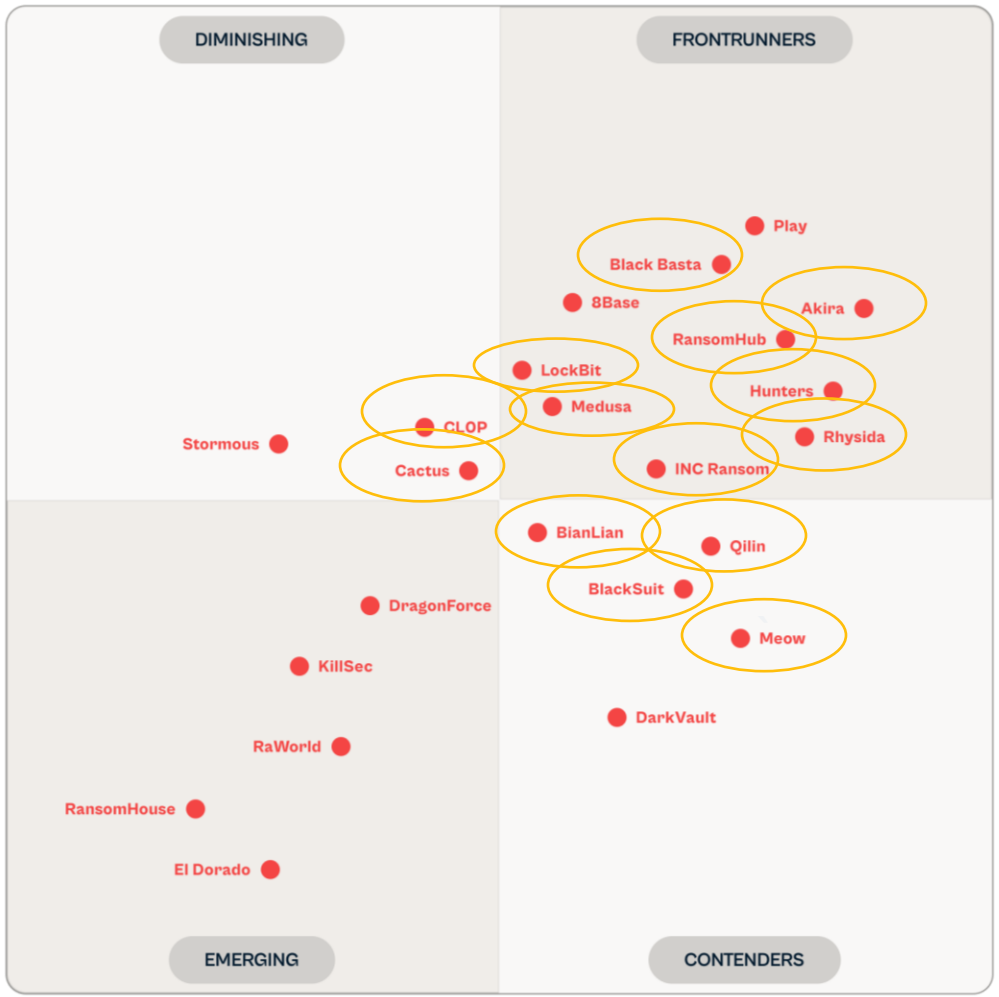
- Attacker creates a legitimate, paid DocuSign account that allows them to change templates and use APIs to generate invoices
- Invoices appear to be from legitimate companies, e.g., renewal notice from Norton Anti-Virus subscription
- Users may e-sign the document, which is then used by the attacker to request payment from accounts payable or finance, or authorize payments from bank accounts
- HC3 issued a sector alert on November 19th

Clearwater

202411191200_DocuSign Abuse Sector Alert_TLPCLEAR
Docusign API Abused in Widescale, Novel Invoice Attack

Other Notable Attacks in Healthcare From Threat Actors

Halycon RaaS "Power Rankings"[1]



= Ransomware Threat actors targeting healthcare that we have discussed at previous cyber briefings

Notable Recent Attacks

- Everest has been focused heavily on dental clinics, with targeted efforts against Value Dental Center, Asaro Dental Aesthetics, and Artistic Family Dental.[2]
- RansomHub attacked medical Health Services and Northwest Porter Hospital
- Blacksuit attacked Kapur and Associates
- BianLian attacked Healthcare Management Services and Immuno Laboratories
- In September 2024, Great Plains Regional Medical Center, a 62-bed not-for-profit hospital in Elk City, Oklahoma, fell victim to a ransomware attack that encrypted files and exfiltrated sensitive data, some of which was not recoverable. Threat Actor unknown.[3]
- Watsonville (Calif.) Community Hospital reported an IT disruption Nov. 29, forcing the hospital into downtime procedures[4]

1 Holycon Top Ransomware Groups
2 Ransomware on the Move: BlackSuit, Everest, Akira, Meow
3 Ransomware Attack on Oklahoma Medical Center Impacts 133,000 – SecurityWeek
4 Watsonville hospital investigates multi-day network outage

Clearwater

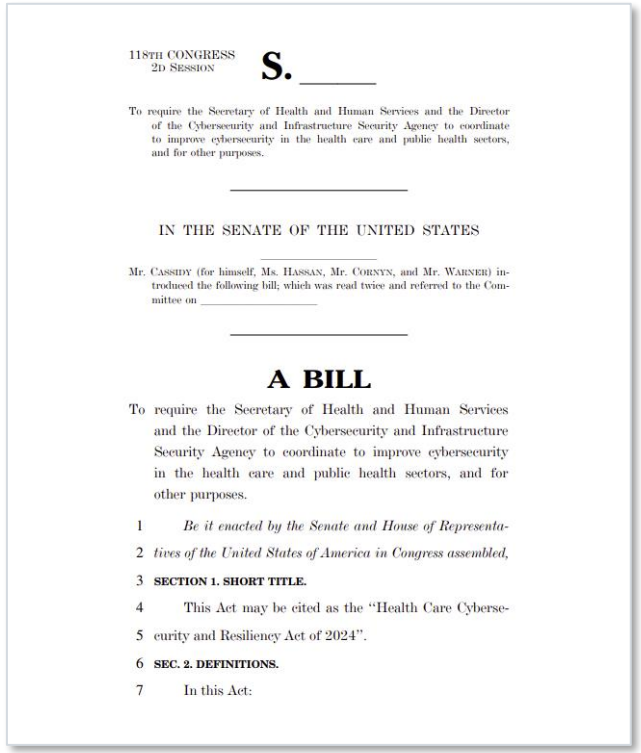
Recommendations for Addressing Current Threat Environment

Specific recommendations related to content in this briefing:

- Restrict communication to trusted external users within Teams to prevent unwanted chat messages from reaching end users
- Enable logging for Teams, and search for Teams display names that contain “Help Desk”
- Set up aggressive anti-spam policies within email security tools
- Disable use of MS Quick Assist and AnyDesk
- Update Security awareness training to incorporate the latest social engineering TTPs
- Ensure your monitoring, detection and response capabilities are sufficient relative to the adversary
- Remind users to double-check the sender's email address and any associated accounts for legitimacy
- Implement strict internal procedures for approving purchases and financial transactions, involving multiple team members where possible.

Regulatory Update: Health Care Cybersecurity and Resiliency Act of 2024

Unlike the HISAA, HCCRA is a bi-partisan bill proposed by the members of a healthcare cybersecurity working group created over a year ago and includes provisions that were derived from that effort.



118TH CONGRESS
2D SESSION

S. _____

To require the Secretary of Health and Human Services and the Director of the Cybersecurity and Infrastructure Security Agency to coordinate to improve cybersecurity in the health care and public health sectors, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. CASSIDY (for himself, Ms. HASSAN, Mr. CORNYN, and Mr. WARNER) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To require the Secretary of Health and Human Services and the Director of the Cybersecurity and Infrastructure Security Agency to coordinate to improve cybersecurity in the health care and public health sectors, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Health Care Cybersecurity and Resiliency Act of 2024".

SEC. 2. DEFINITIONS.

In this Act:

Key Provisions in the Bill

- Coordination between HHS and CISA
- Oversight of cybersecurity activities
- Cybersecurity response plan
- Breach portal reporting update
- Clarification of breach reporting obligations
- Required cybersecurity standards
- Guidance on rural cybersecurity readiness
- Grants to enhance cybersecurity in the health sector (rural)
- Healthcare cybersecurity workforce (education)

Click here to read my blog which describe each section of the bill and provides commentary.

Clearwater

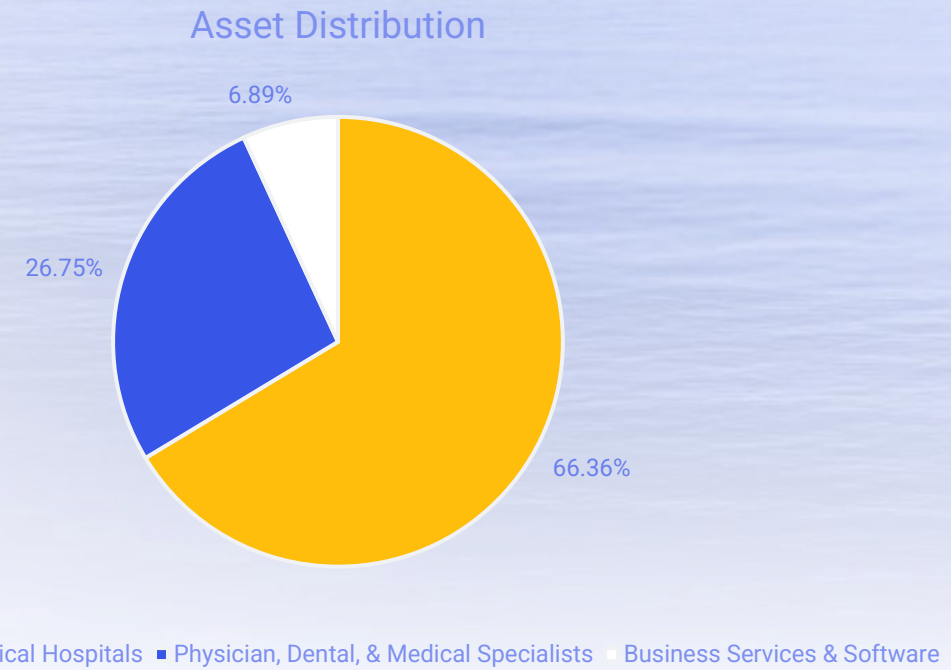
The State of Vulnerability Management in Healthcare

Steve Akers

Clearwater

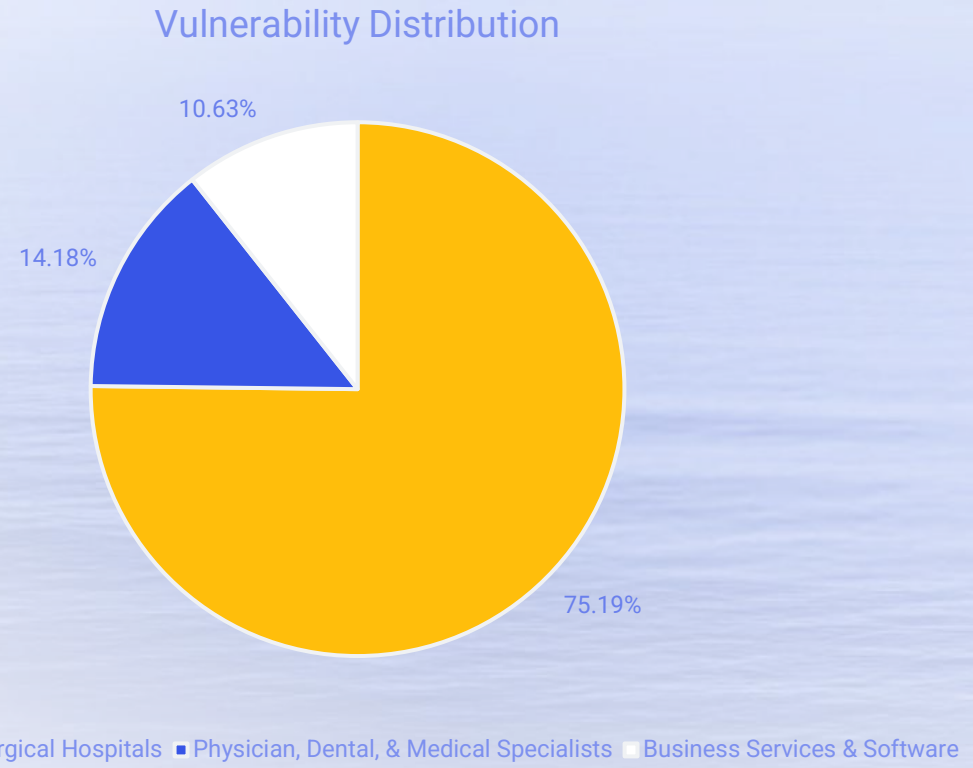
About the Data

- All source information is derived from Clearwater's vulnerability management and scanning services
- All Healthcare clients have been categorized into one of the following Market Segments:
  - Health Centers & Surgical Hospitals
  - Physician, Dental, and Medical Specialists
  - Healthcare Business Services and Software
- Timeframes are either:
  - Point in time ~11/25/24 - 11/30/24
  - Trended over Aug - Nov 2024
- Hospitals, with the diverse environments, are the largest asset group by percentage at ~66%

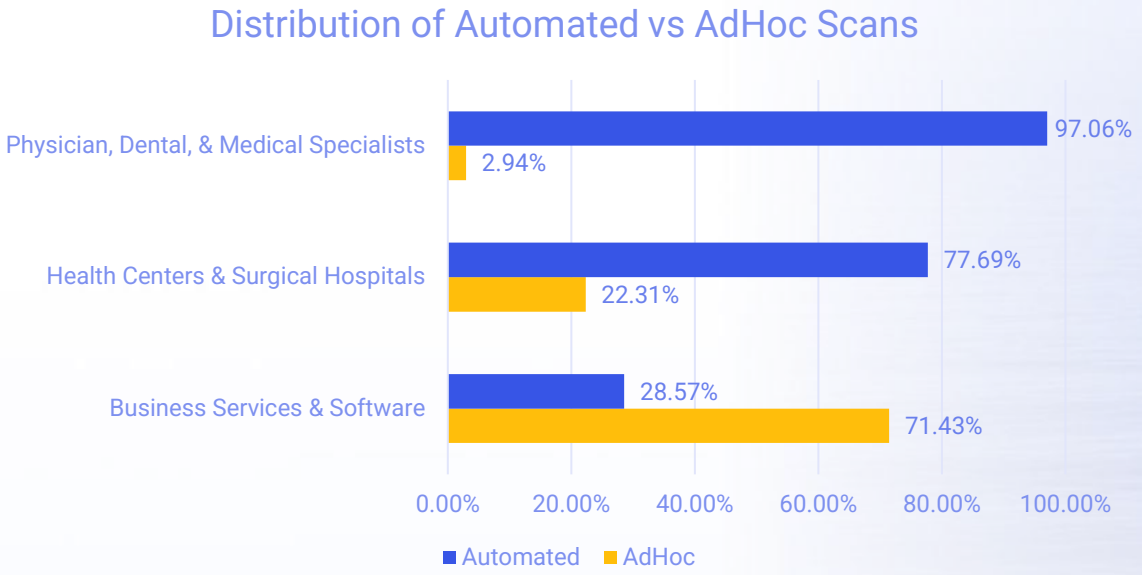


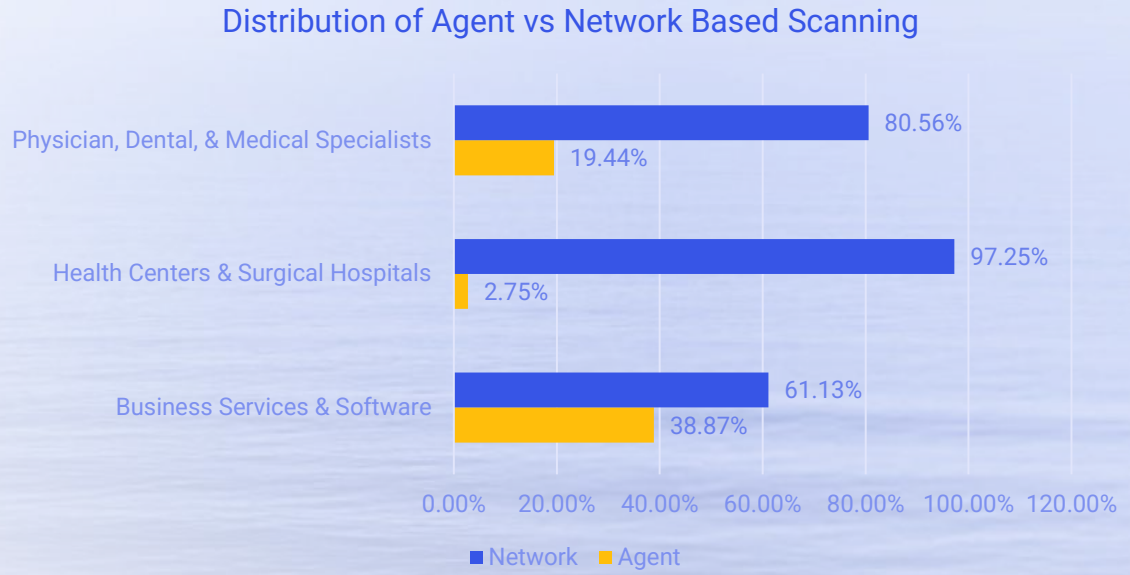
Vulnerability Attribution Across Verticals

- Despite being the second largest asset group representing about 27% of all assets, Physician, Dental, and Medical Specialists represent just over 14% of all current vulnerabilities
- Other segments represent between 4-9% more vulnerabilities than their respective asset distribution
- This distribution has stayed within ~1-2% over the trending period



Scanning Usage and Methods



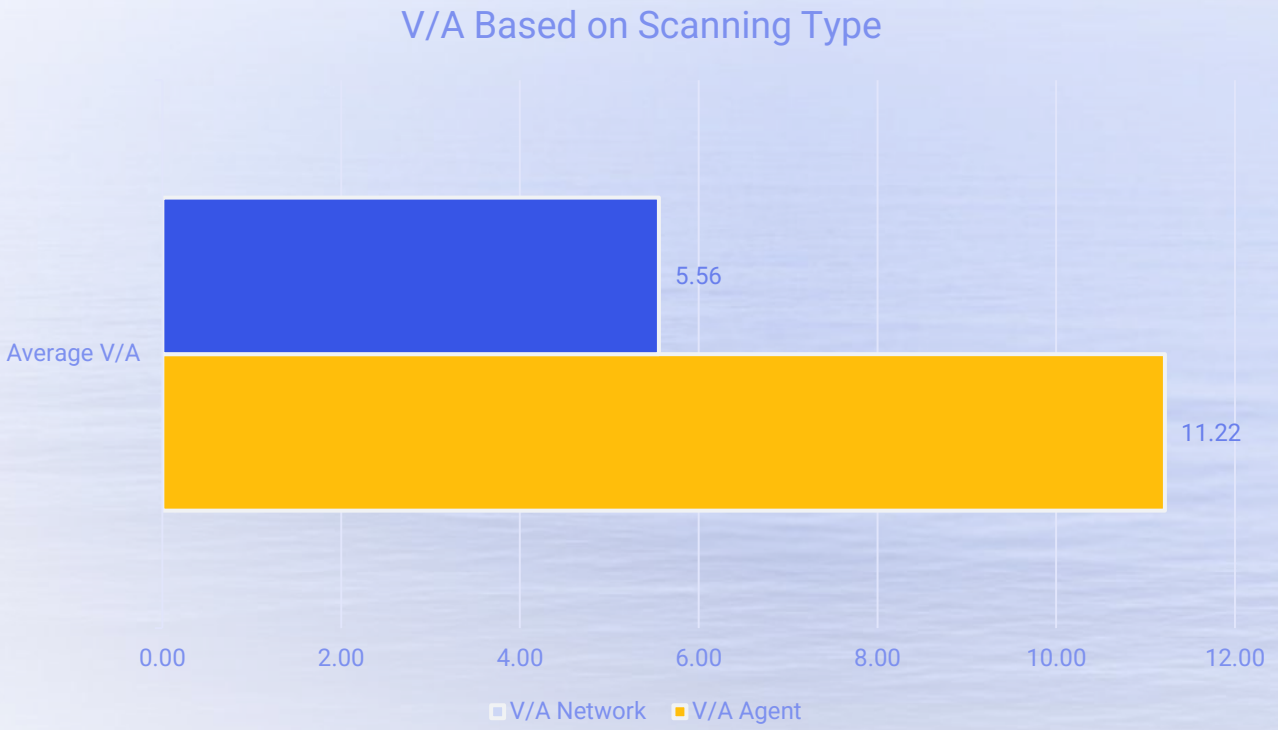


- Organizations that have a separation between remediation efforts and those responsible for scanning often do not use a lot of ad hoc
- Hospitals are overwhelmingly Network based or passive, and therefore aren't getting as near a real-time view of vulnerabilities across the org.

Clearwater

Agent vs Network Scanning

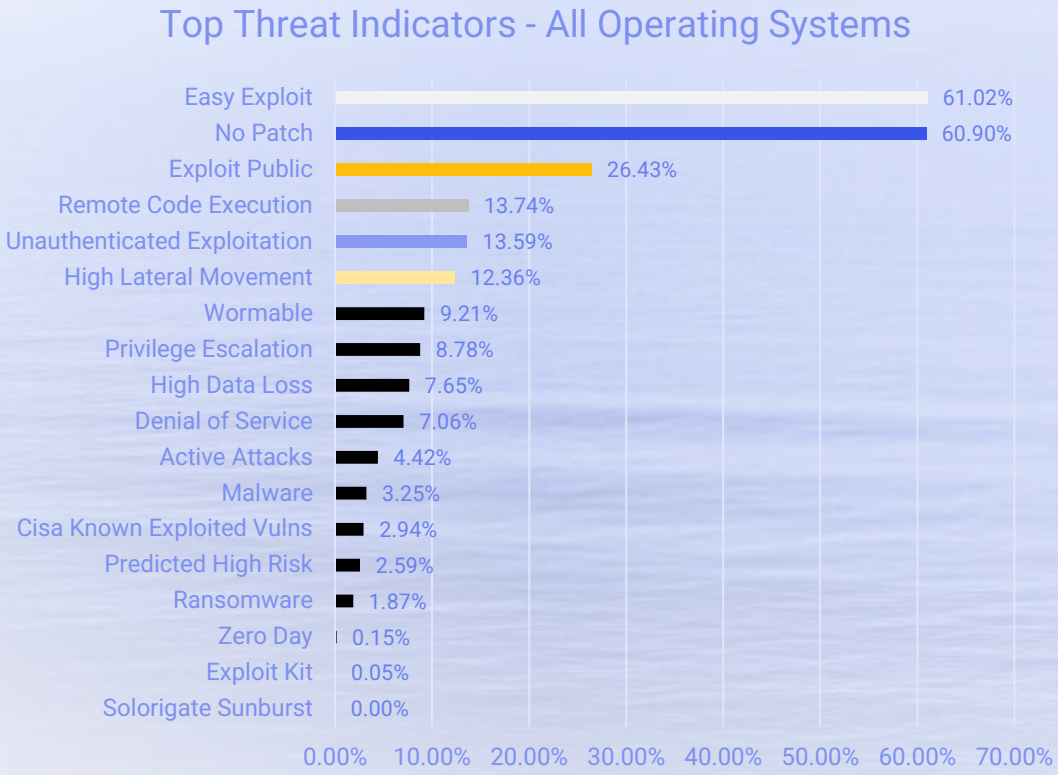
- Logical “Scoring” or tracking metric of Vulnerabilities per Asset or V/A
- Agent based scanning finds ~2x the number of vulnerabilities
- Network scanning can mask about half of the real findings
  - Authenticated scans help some
- Network scanning still has its place:
  - External
  - Non Agent Based Assets



Clearwater

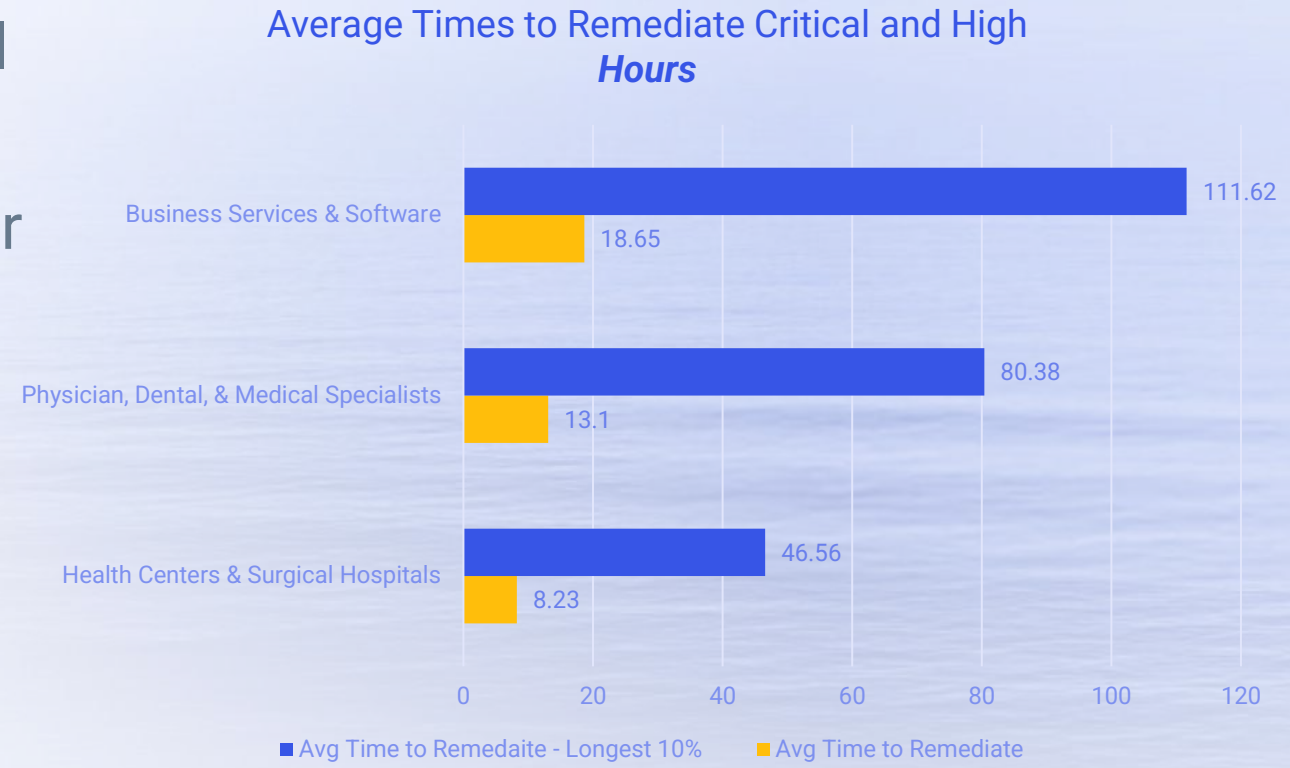
Threat Indicators

- Real Time Threat Indicators (RTI) represent different kinds of threats a vulnerability could be subject to.
  - RTIs are a great additional metric for prioritization
- All Operating Systems shared 5 of the top 6
- 64% of Easy Exploit also have no patch
- 28% of Easy Exploit also have a public exploit
- 13% of No Patch also have a public exploit
- Zero Day and Ransomware – Lower Tier



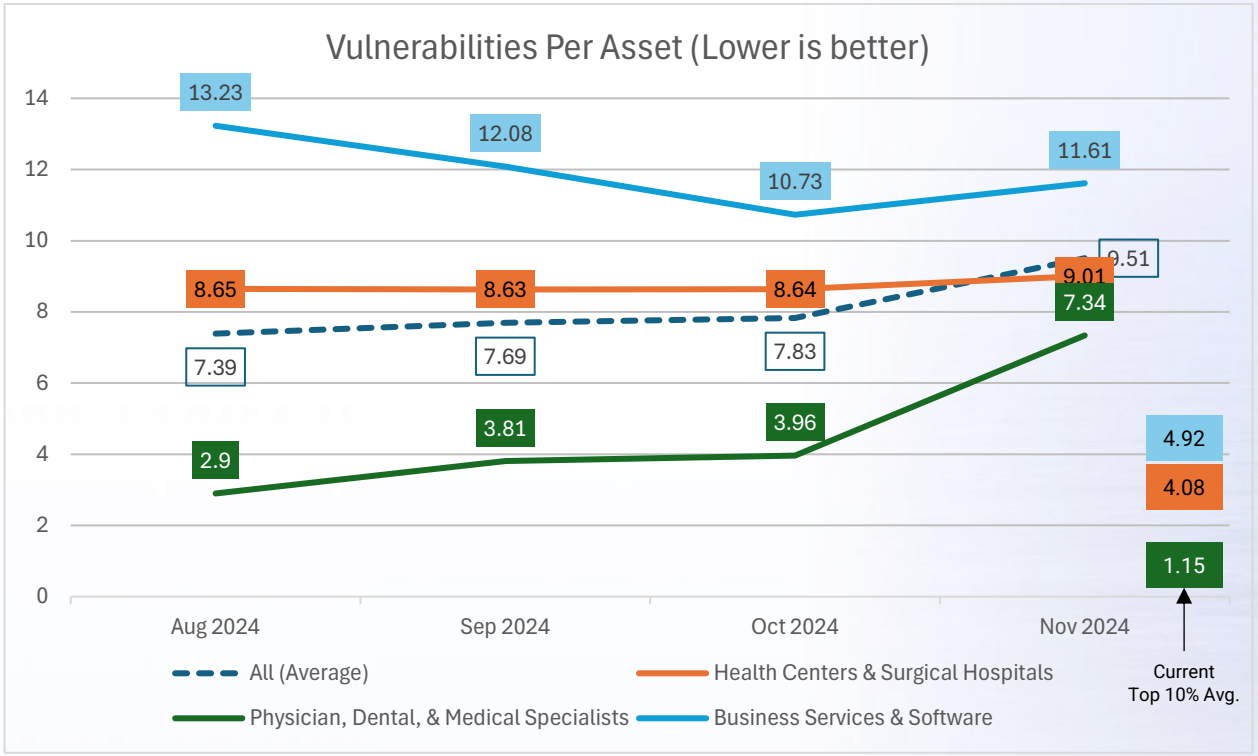
Time to Remediate

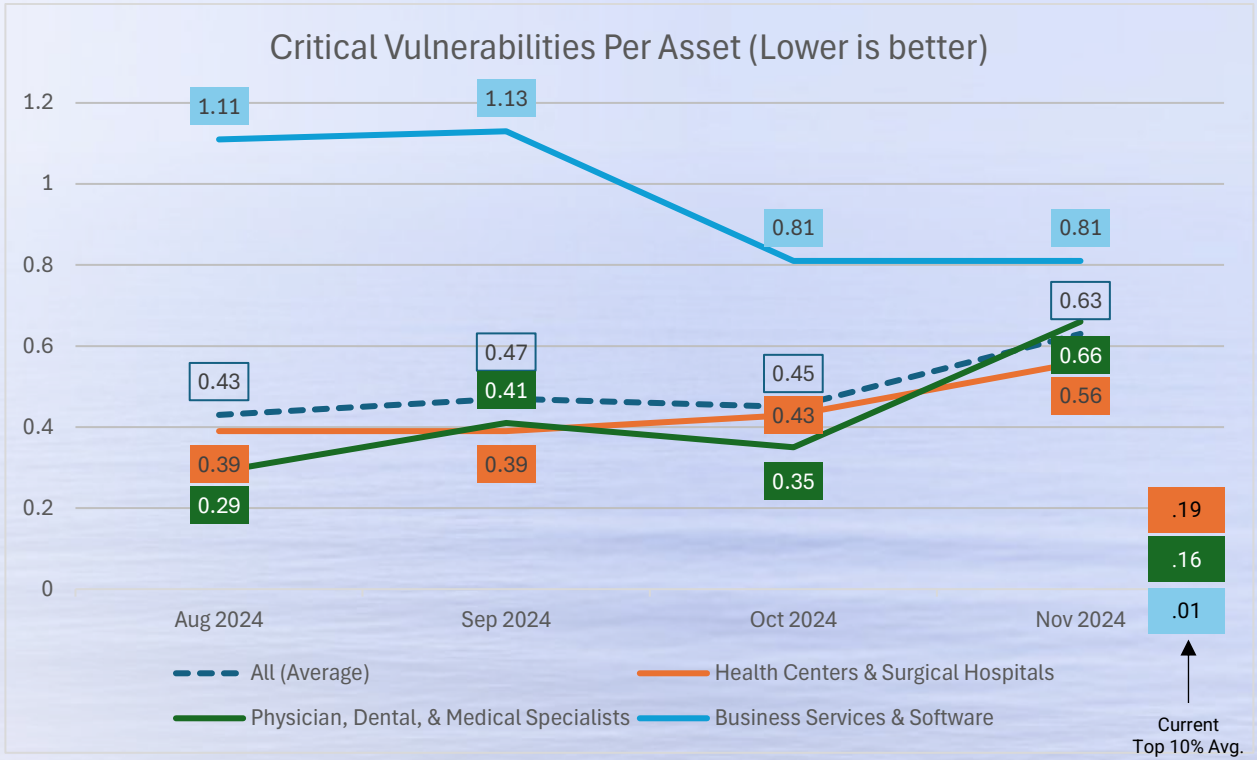
- All three segments are averaging less than 24 hours for remediating critical and high vulnerabilities
- All also are averaging about 2 days or more for remediating the top 10% of their longest Critical and High Vulnerabilities
  - Most often – these are configuration related vs. patches
  - May require more manual effort



Clearwater

Vulnerabilities per Asset



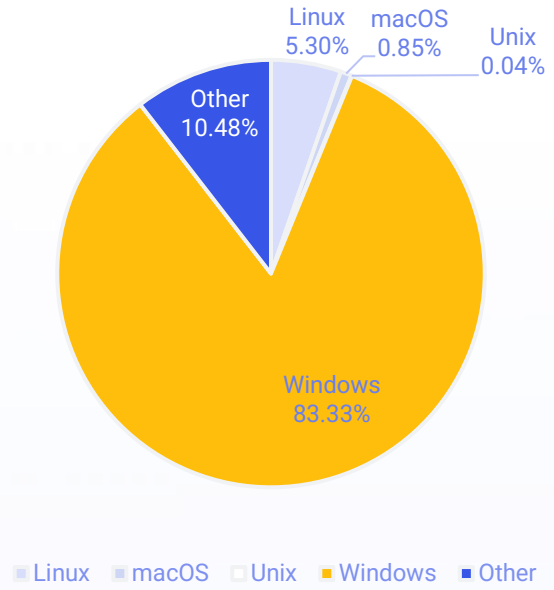


- Outside of Business Services – general trend is up
- Spikes – new release of vulns that impact all segments
- All segments well outside the top performers within their segement

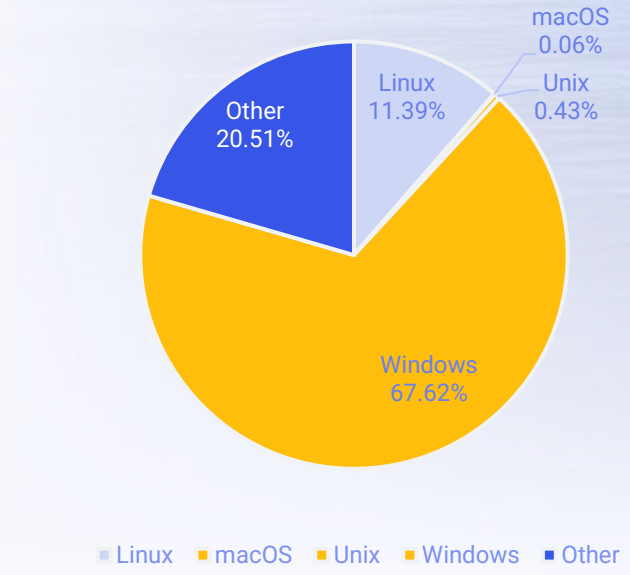
Clearwater

Vulnerability Drill Down – Operating System

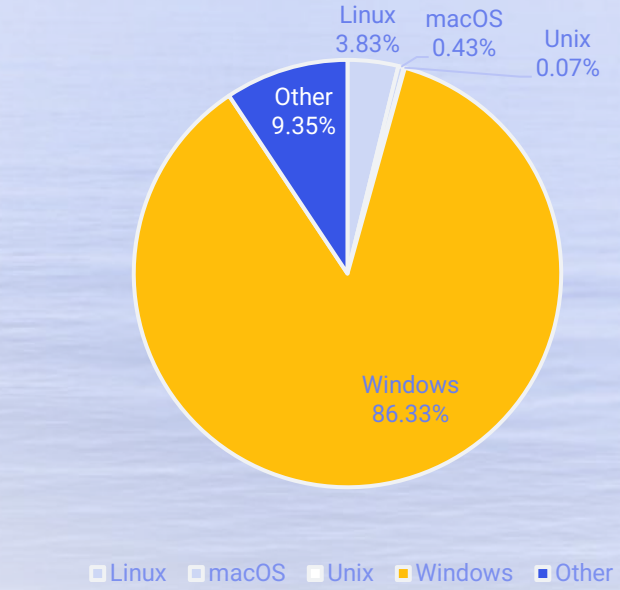
Critical and High Vulnerability Distribution
Business Services & Software



Critical and High Vulnerability Distribution
Health Centers & Surgical Hospitals



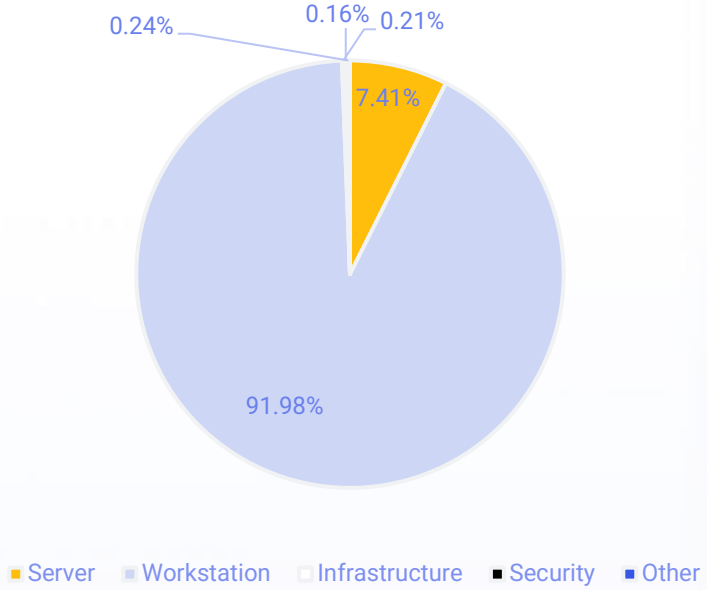
Critical and High Vulnerability Distribution
Physician, Dental, and Medical Specialists



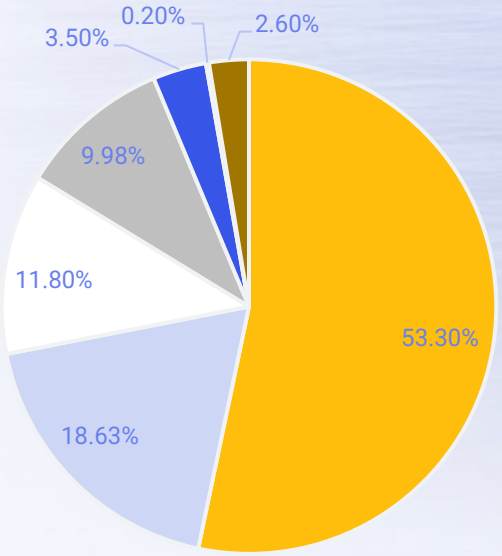
Clearwater

Vulnerability Drill Down – Role

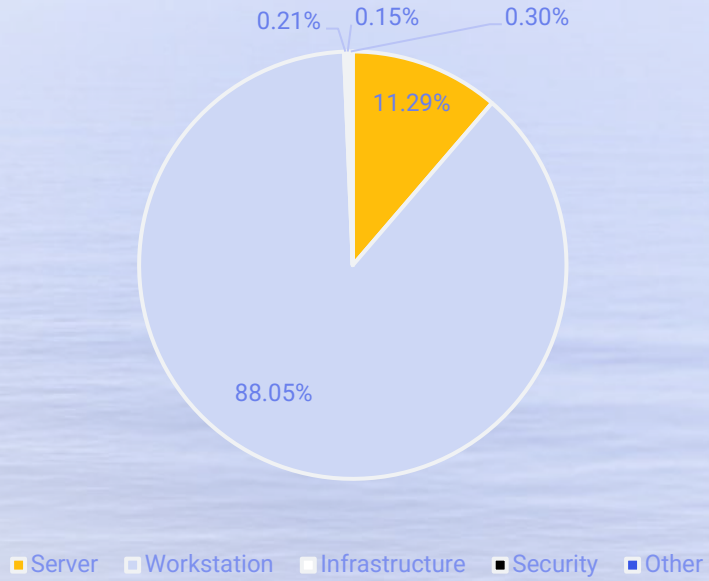
Critical and High Vulnerability Distribution
Business Services & Software



Critical and High Vulnerability Distribution
Health Centers & Surgical Hospitals



Critical and High Vulnerability Distribution
Physician, Dental, and Medical Specialists



Vulnerability Management Take Aways

- Fixing all critical vulns. is too long at about 2 days or more
- The trend for Vulns. per Asset (V/A) is up
  - Rate of new vulns. being released is faster than remediation efforts (in most cases)
- Network scanning has its place, but should not be the only method used
  - Agents identify about 2x the vulns.
- Significant numbers of vulnerabilities don’t have a patch, are easy to exploit and have an exploit in the wild
- Vulnerability Management needs to be a critical component to your overall cybersecurity program and strategy

Q&A

Upcoming Industry Events

ViVE | February 16-19, 2025 – Nashville, TN

- Clearwater is excited to again serve as title sponsor of the Cybersecurity Pavilion as the ViVE conference returns to Nashville in early 2025
- We are teaming up with Holland & Knight and 25m Health for a networking night on Sunday to Kickoff the week.

- Click here for more information and to register

HIMSS Global Conference | March 3-6, 2025 – Las Vegas, NV

- Clearwater Chief Risk Officer and Head of Consulting Services & Client Success Jon Moore is teaming with Michal Gross, Manager of Cybersecurity Intelligence for the Cleveland Clinic, to deliver the presentation "Mastering Cyber Threat Intelligence to Protect Patient Safety" at HIMSS25 in Las Vegas. Be sure to catch Jon and Michael's session on Tuesday, March 4, at 10:15am PT.

- Click here for more information and to register

Clearwater

Upcoming Webinars

Our 2025 Cyber Briefing Series is coming up!

All attendees will be automatically enrolled into our series for next year, so no action is needed on your part to register again.

Monthly Cyber Briefing on January 9 @ 12:00 CST

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

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.