Ransomware & Healthcare

January 18, 2024

TLP:CLEAR, ID# *202401181300*

Agenda

- Ransomware: An Overview
- A Look at the Impact of Ransomware on the HPH
- Top Initial Access Vectors
- Mitigations
- Education and Awareness

Slides Key:

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

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

Ransomware: An Overview

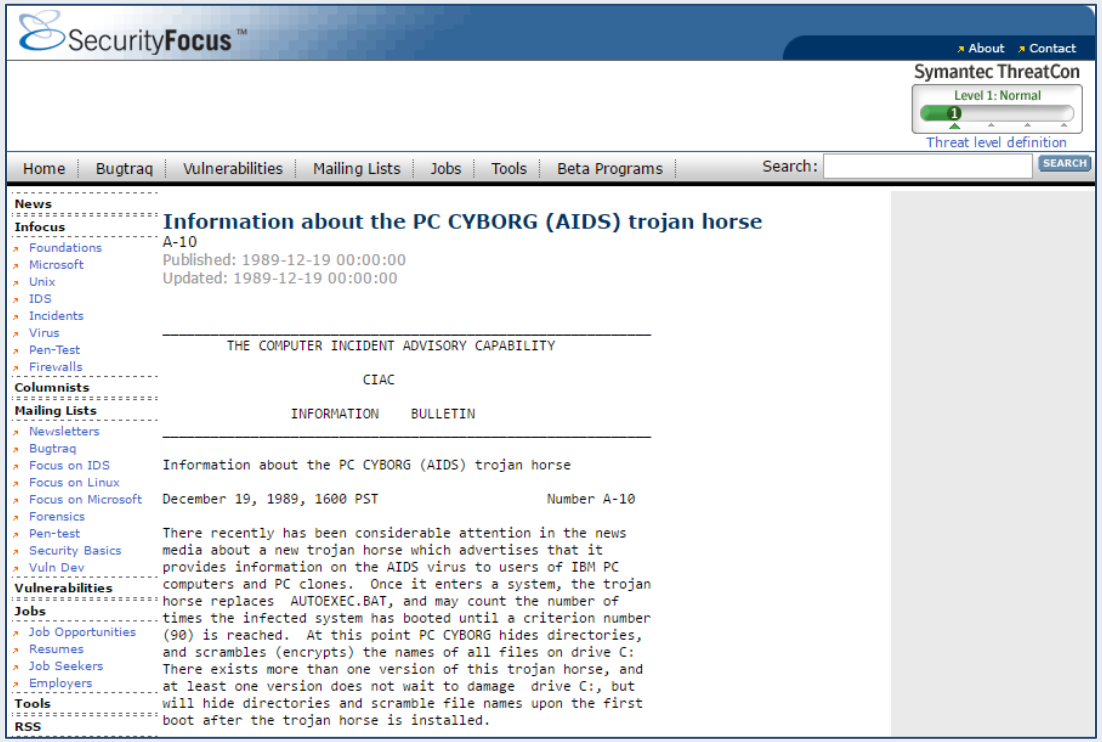
What is Ransomware?

- A type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files.

Source: Kaspersky

The Dawn of Ransomware

- First known ransomware attack occurred in 1989, and coincidentally targeted the healthcare industry.
- Involved Harvard-trained evolutionary biologist and AIDS researcher Joseph L. Popp, who distributed 20,000 floppy disks labelled “AIDS Information – Introductory Diskettes” to attendees of the World Health Organization’s international AIDS conference.
- Disk contained a malware program that initially remained dormant in computers, only activating after a computer was powered on 90 times, at which point the Trojan, known as AIDS Trojan or PS Cyborg, hid directories and encrypted the names of the files on the recipient’s computer.
- After the 90-start threshold was reached, the malware displayed a message demanding a payment of $189.



PC CYBORG advisory from 1989. *Source: Security Focus*

Welcome to the Internet and Monetization

- **eCrime:** A broad category of malicious activity that includes all types of cybercrime attacks, including malware, banking Trojans, ransomware, cryptojacking, and more.
- Ransomware efforts are aided by criminal organizations using more effective asymmetric RSA (Rivest—Shamir—Adleman) encryption.
- Notable attacks:
  - Archiveus Trojan: A virus that encrypted everything in the My Documents directory and required victims to purchase items from an online pharmacy to receive the 30-digit password.
  - Gpcode: An encryption Trojan that initially spread via an email attachment purporting to be a job application, and which used a 660-bit RSA public key.
- The creation and popularity of cryptocurrencies, such as Bitcoin, provides adversaries with the means to receive instant payments while maintaining anonymity, all transacted outside the limits of traditional financial institutions.

The Persistent Threat of CryptoLocker

- **CryptoLocker:** One of the most profitable ransomware strains of this time; first versions appear to have been posted September 2013; usually entered the company by email.
  - Not only harnessed the power of Bitcoin transactions but combined it with more advanced forms of encryption.
  - Infected more than 250,000 systems between September and December 2013.

A CryptoLocker ransom message. *Source: Computer World*

CryptorBit & CryptoWall

- **CryptorBit:** Discovered in December 2013; corrupts the first 1,024 bytes of any data file it finds; could bypass Group Policy settings put in place to defend against this type of ransomware infection.
  - Social engineering used to get end users to install the ransomware using such methods as a fake flash update, or a rogue antivirus product.
  - Tor and Bitcoin used for ransom payment; also installed crypto-coin mining software that uses the victim's computer to mine digital currency.
- **CryptoWall:** Rebranded from CryptoDefense in April 2014; exploits a Java vulnerability; malicious advertisements on real domains led people to sites were CryptoWall infected and encrypted their drives.
  - 2.0 appeared January 2015; delivered via email attachments, malicious PDF files, and various exploit kits; encrypted the user's data; used TOR to obfuscate the C&C (Command & Control) channel; incorporated anti-VM and anti-emulation checks to hamper identification via sandboxes.
  - 3.0 appeared March 2015; used exploit kits to gain privilege escalation on the system; disabled many security features on a target system.
  - 4.0 appeared September 2015; biggest change from previous iteration was that it re-encrypted the file names of the encrypted files, making it more difficult to decipher which files needed to be recovered.

Modern Ransomware

- **Big Game Hunting (BGH):** A type of cyberattack that usually leverages Ransomware-as-a-Service (RaaS) or ransomware with the tactics, techniques and procedures (TTPs) common in targeted attacks aimed at larger, high-value organizations or high-profile entities.
- The goal of BGH is to focus efforts on fewer victims that can yield a greater financial payoff. Victims are chosen based on their ability to pay a ransom, as well as the likelihood that they will do so to resume business operations or avoid public scrutiny. Common targets may include:
  - Large corporations
  - Banks and other financial institutions
  - Utilities
  - Hospitals and other healthcare institutions
  - Government agencies
  - High net worth individuals, such as celebrities and prominent business leaders
  - Any organization that holds sensitive data, including intellectual property, trade secrets, personal data or medical records

Modern Ransomware, cont.

- 2020 witnessed a widespread adoption of ransomware, with data-leak extortion tactics among multiple eCrime groups. This method involves both encrypting a victim organization's environment, and exfiltrating data with the threat to leak it if the extortion demand is not paid.
- Threat actors have also become more sophisticated in their methods of leaking the data. In general, they will leak exfiltrated data slowly, saving what they perceive to be the most sensitive data for last to increase pressure on the victim organization to pay the extortion, rather than posting all the exfiltrated data at once.
- Big Game Hunters are sophisticated cyber threat actors, often working as part of an organized group to take down significant targets. In many cases, these groups operate as highly structured and organized networks, not unlike corporate enterprises. They are often state-sponsored and are suspected to have ties to government agencies or prominent public figures.

How Does Ransomware Work?

- **Access:**
  - Attackers gain access to your network. They establish control and plant malicious encryption software. They may also take copies of your data and threaten to leak it. There are several ways for systems to be corrupted and subsequently ransomed; an attack or infection vector is how ransomware obtains access.
- **Initiation:**
  - The malware goes to work, locking devices and causing the data across the network to be encrypted, meaning that you can no longer access it.
- **Ransom:**
  - This usually happens in the form of an on-screen notification from the cyber-criminal, demanding a ransom in exchange for decryption. The computer itself may become locked, or the data on it might be encrypted, stolen or deleted. The attackers may also threaten to leak the data they steal. Payment is usually demanded via an anonymous web page and usually in a cryptocurrency, such as Bitcoin.

Types of Ransomware

Crypto Ransomware/Encryptors

- Most well-known and damaging variant
- Encrypts the files and data within a system, making the content inaccessible without a decryption key

Scareware

- Fake software that claims to have detected a virus or other issue on your computer and directs you to pay to resolve the problem; some types lock the computer, while others simply flood the screen with pop-up alerts without damaging files

Lockers

- Completely lock you out of your system, so your files and applications are inaccessible; a lock screen displays the ransom demand, possibly with a countdown clock to increase urgency and drive victims to act

Doxware or Leakware

- Threatens to distribute sensitive personal or company information online; many people panic and pay the ransom to prevent private data from falling into the wrong hands or entering the public domain

Types of Ransomware, cont.

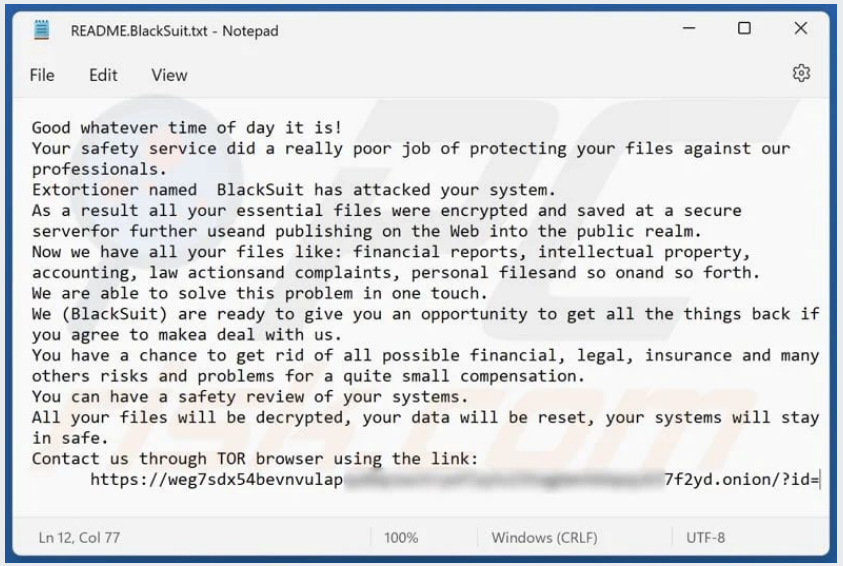
Ransomware-as-a-Service (RaaS)

- A business model between ransomware operators and affiliates, in which affiliates pay to launch ransomware attacks developed by operators.
- There are four common RaaS revenue models:
  - Monthly subscription for a flat fee
  - Affiliate programs, which are the same as a monthly fee model, but with a percent of the profits (typically 20-30%) going to the ransomware developer
  - One-time license fee with no profit sharing
  - Pure profit sharing

RaaS Operators	RaaS Affiliates
✓ Recruits affiliates on forums	✓ Pays to use the ransomware ✓ Agrees on a service fee per collected ransom
✓ Gives affiliates access to a "build your own ransomware package" panel ✓ Creates a dedicated "Command and Control" dashboard for the affiliate to track the package	✓ Targets victims ✓ Sets ransom demands ✓ Configures post-compromise user messages
	✓ Compromises the victim's assets ✓ Maximizes the infection using "living off the land" techniques ✓ Executes ransomware
✓ Sets up a victim payment portal ✓ "Assists" affiliates with victim negotiations	✓ Communicates with the victim via chat portals or other communication channels
✓ Manages a dedicated leak site	✓ Manages decryption keys

BlackSuit

- A relatively new ransomware group with significant similarities to the Royal ransomware family; an increasing threat to the Healthcare and Public Health (HPH) sector.
- Discovered in early May 2023, BlackSuit's striking parallels with Royal—the direct successor of the former notorious Russian-linked Conti operation—potentially places the group with one of the most active ransomware groups in operation today.
- BlackSuit primarily targets Linux systems and Windows and prevents victims from accessing their files by encrypting them.
- BlackSuit appends the file extension (".blacksuit") to the files it encrypts, changes the desktop wallpaper, creates and drops its ransom note ("README.BlackSuit.txt") into the directory, renames files, and lists its TOR chat site in the ransom note along with a unique ID for each of its victims. Its operators also set up a data leak site as part of their double extortion strategy to coerce victims into paying the ransom demand.
- Cybercriminals may distribute BlackSuit ransomware through e-mail attachments that contain infected links or macros, torrent websites, malicious ads, and Trojans.
- Target industries appear to be indiscriminate, but include the healthcare, manufacturing, business technology, business retail, and government sectors.
- **HC3 Resource:** [BlackSuit Ransomware]



Screenshot of BlackSuit's text file "README.BlackSuit.txt". *Source: PCRisk*

Rhysida

- First observed on May 17, 2023, following the emergence of their victim support chat portal, hosted via TOR. Rhysida describes itself as a “cybersecurity team” that aims to help victims highlight potential security issues and secure their networks.
- Rhysida is a 64-bit Portable Executable (PE) Windows cryptographic ransomware application compiled using MINGW/GCC.
- Deployed in multiple ways; primary methods include breaching targets’ networks via phishing attacks, and by dropping payloads across compromised systems after first deploying Cobalt Strike or similar command-and-control frameworks.
- For the encryption phase, Rhysida uses a 4096-bit RSA key with the ChaCha20 algorithm. After the encryption details are established, Rhysida enumerates files and folders connected to the system. The main function ends by calling PowerShell to delete the binary after encryption has completed. The group then threatens victims in a ransom note with public distribution of the exfiltrated data, bringing them in line with modern-day double-extortion groups. Victims are instructed to contact the attackers via their TOR-based portal, utilizing their unique identifier providers in the ransom note.
- Typically targets the United States, Italy, Spain, and the United Kingdom more than other countries.
- **HC3 Resource:** Rhysida

Ryhsida logo. *Source: SentinelOne*

A Look at the Impact of Ransomware on the HPH

Ransomware & the HPH

- The long-time perceptions of domestic, rogue, individual hackers as primary perpetrators do not match the current reality in the healthcare and life sciences sector. Institutions are routinely targeted by full-time professional cyber actors that are well-trained, well-equipped, well-funded, and often supported and sheltered by adversarial nation states.
- These cyber criminals are remotely launching ransomware attacks against U.S. hospitals, medical research laboratories, and other critical infrastructure—creating a direct threat to public health and safety; an example of how cyber criminals have become more sophisticated that is extremely troubling for hospitals, is that hackers now specifically target medical devices, not only networks, servers, PCs, databases, and medical records.
- A further point of concern for healthcare organizations that has developed is regarding the supply chain. While supply chain attacks are not new, these incidents have come under the spotlight in recent years, due to the realization that organizations outsource specific tasks and software to other companies.

The Data Doesn’t Lie

- Over 630 ransomware incidents impacting healthcare worldwide in 2023; over 460 of these affected the U.S. HPH.
- The top ransomware groups witnessed targeting the HPH:
  - LockBit
  - Cl0p
  - ALPHV
  - BianLian
- Followed by:
  - Royal or BlackSuit
  - Karakurt
  - Medusa
  - Akira
  - 8BASE
  - NoEscape

FBI Cyber Incident Reporting

Report to CISA

Notable Ransomware Incidents:

Petya

WannaCry

GandCrab

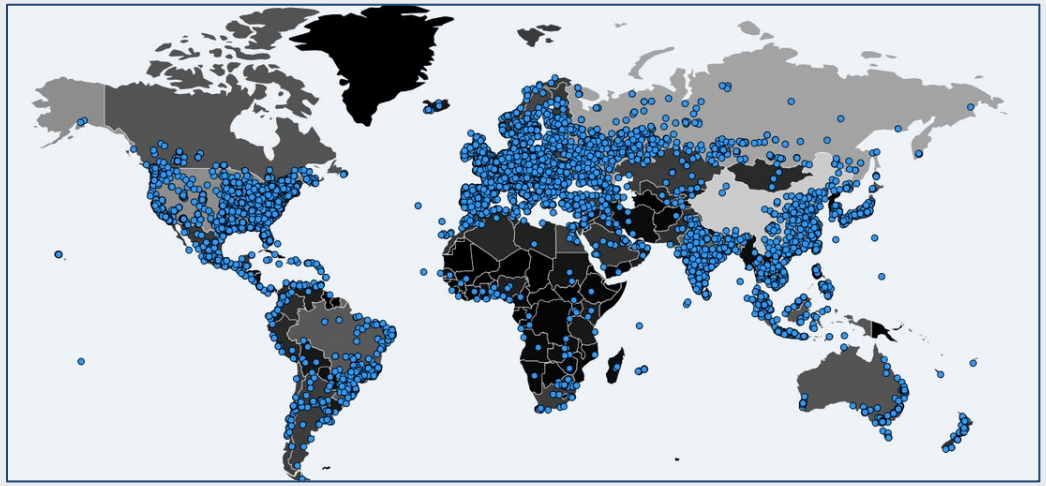
Locky

Ryuk

Source: Marcum

WannaCry Ransomware Attack in 2017

- WannaCry (Wcry or WannaCryptor)
- Vulnerability in the SMB Protocol
- ".WCRY" extension was added to encrypted files
- A two-component ransomware:
  - Encrypted files, self-propagating



Source: NPR

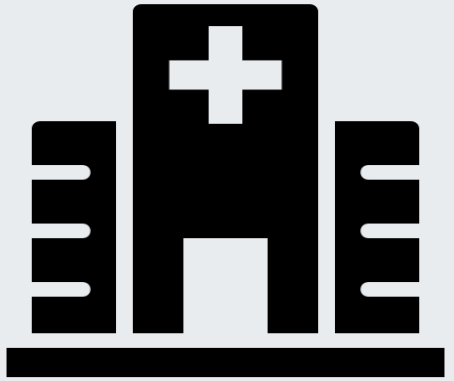
Source: TechCrunch

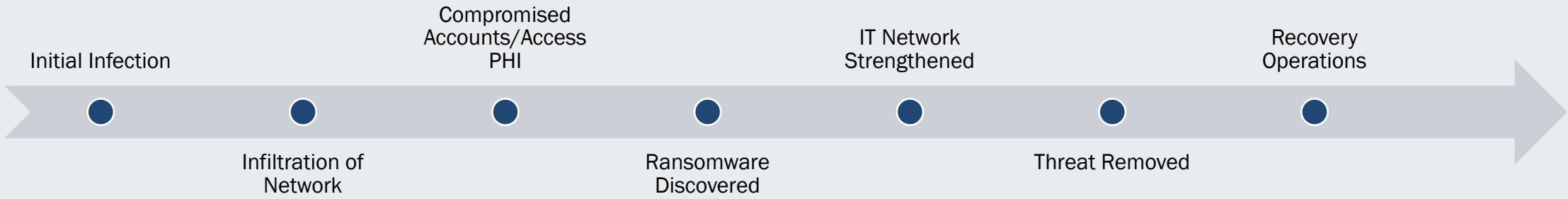
- Leveraged an exploit known as "EternalBlue"
- Estimated USD $4 billion in damage
- Impacted organizations worldwide

Notable Ransomware Incident

In 2022, a large hospital network was impacted by ransomware, which resulted in multiple sites being impacted and sensitive patient data being acquired.

- Large hospital network experienced a ransomware incident, and multiple sites within the network were impacted.
- The initial attack vector was not publicly reported, but phishing was suspected.
- It took almost six months to fully investigate impacted data.





Incident Response

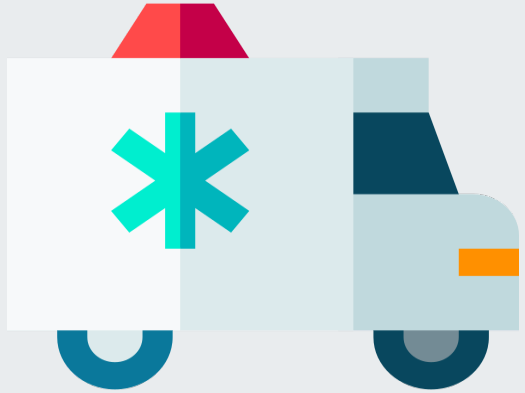
The IT staff worked to contain the incident and made proactive efforts to minimize the damage.

- Mobilized the IT/security team
- IT staff worked to contain the threat
- Bolstered network security
- Took systems offline to contain the threat
  - Actor(s) already had access for nearly 20 days
- Activated third-party cybersecurity specialist
- Notified law enforcement
- Once secured, systems returned to normal operations, along with enhanced features

Damage to the Network

Despite efforts to minimize and contain the malware, the threat actors were already in the victim's environment for nearly 20 days and were able to cause significant damage. Some of the notable impacts:

- Copies of patient data were stolen
- Over half a million patients were impacted
- Disruption to payroll and portals
- Delays in patient care
- Ambulances diverted
- Switching to paper records
- IT outages, EHR downtime
- Cancelations occurred
- Temporary switch to paper records
- Estimated over USD $100 million in damages



Top Initial Access Vectors for Ransomware

Ransomware Initial Access Vectors

Attackers have numerous ways to obtain initial access to a victim's environment, and one of the reasons healthcare is targeted is due to the multiple possible entry points.

- Phishing Emails
  - Malicious links, documents
- Software Vulnerabilities
  - Unpatched systems, zero-days
- Remote Desktop Protocol Attacks
  - Brute force, etc.
- Drive-By Downloads
  - Malicious websites
- Malvertising
  - Malicious advertisements
- Watering Hole Attacks
  - Compromised websites
- USB Drives and External Devices
- Supply Chain Attacks
- Insider Threats
- Other

Ransomware and Phishing

Phishing plays a significant role in the spread of successful ransomware attacks.

- **Delivery Mechanism:** Phishing emails are a common delivery mechanism for ransomware.
- **Social Engineering:** Phishing relies heavily on social engineering tactics to trick individuals.
- **Exploiting Human Vulnerabilities:** Phishing preys on human vulnerabilities such as curiosity, fear, or urgency.
- **Impersonation:** Phishing emails can impersonate trusted entities.
- **Credential Theft:** Some phishing attacks are designed to steal login credentials. Once compromised, attackers can gain unauthorized access.

Ransomware and Software Vulnerabilities

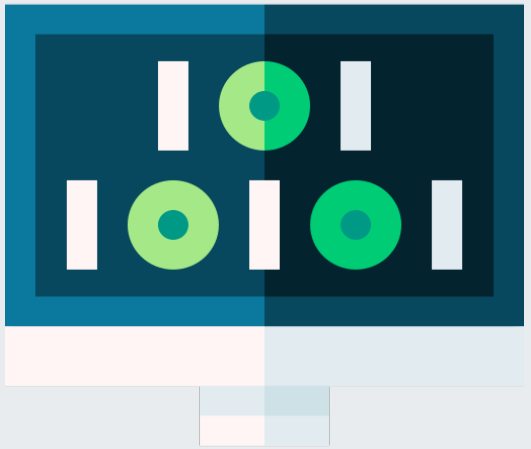
Software vulnerabilities play a significant role in ransomware because threat actors can leverage known and unknown weaknesses in a victim's environment.

- **Exploitation of Weaknesses:** Ransomware authors often exploit vulnerabilities in software to gain access.
- **Delivery Mechanism:** Exploiting vulnerabilities is a common method for delivering ransomware.
- **Zero-Day Attacks:** Vulnerabilities that are not yet known by the vendor or public.
- **Avoidance of Detection:** Exploiting vulnerabilities allows ransomware to avoid detection in security measures.

Ransomware and Remote Desktop Protocol

Remote Desktop Protocol (RDP) is a legitimate access tool, which a threat actor can compromise to obtain the same level of access as the authorized user.

- **Weak Passwords:** Weak or easy passwords may enable unauthorized access.
- **Brute Force Attacks:** Attackers may use brute force techniques to guess RDP credentials.
- **Unsecure Ports:** If RDP is exposed to the internet without security measures, it can become a target for attackers.
- **No MFA:** Enabling MFA will add an additional layer of protection from RDP attacks.
- **Network Security:** Networks lacking proper configuration can give attackers access to RDP sessions (Person-in-the-Middle attacks).



Ransomware Mitigations

Backups

Backing up your data

Data Recovery

Avoiding Ransom Payments

Redundancy

Continuity

Backup Considerations

Backing up your data can be an effective defense against ransomware attacks, but there a few considerations to be mindful of:

- **Integrity Verification:** Verifying that backups are free from malware or other types of corruption are vital to ensure backups serve their purpose during recovery.
- **Security Isolation:** Backups are encouraged to be stored on a separate network to prevent ransomware from spreading to the backup copies.
- **Regular Testing:** Periodic testing of the restoration process ensures backup copies are accessible and that your recovery plan is effective.

Network Segmentation

Network segmentation can help contain ransomware on a network. Since ransomware typically moves laterally, segmentation can limit that movement.

- **Containment of Spread:** With network segmentation, the damage of the ransomware attack can be contained within a certain segment.
- **Isolation of Critical Systems:** Segmentation can enable the isolation of sensitive or critical information.
- **Reduced Attack Surface:** Network segmentation can make it more challenging for ransomware to move laterally, and it limits entry points.
- **Enhanced Access Control:** Increases granular access control. Each segment can have their own set of rules and permissions.

- **Improved Monitoring and Detection:** Anomalous behavior in one segment can be more easily detected and allow for quicker response times.
- **Backup Integrity:** Network segmentation can isolate backups and make it more challenging for attackers to compromise backup data.
- **Increased Recovery:** Increased recovery and restoration, with the impact of ransomware being limited to certain segments, other parts of the network can continue to function.

Endpoint Security

- **First Line of Defense:** Individual devices (computers, laptops, etc.) are frequently the initial target of ransomware. Endpoint security can help prevent unauthorized software.
- **Automatic Updates & Patch Management:** Regular updates and patching can address security flaws that may be exploited by ransomware.
- **Policy Enforcement:** Endpoint security allows organizations to enforce policies across devices.
- **Incident Response:** In the event of a ransomware attack, endpoint security can provide information about the attack and improve response and containment measures.

Source: syncromsp

Education & Awareness

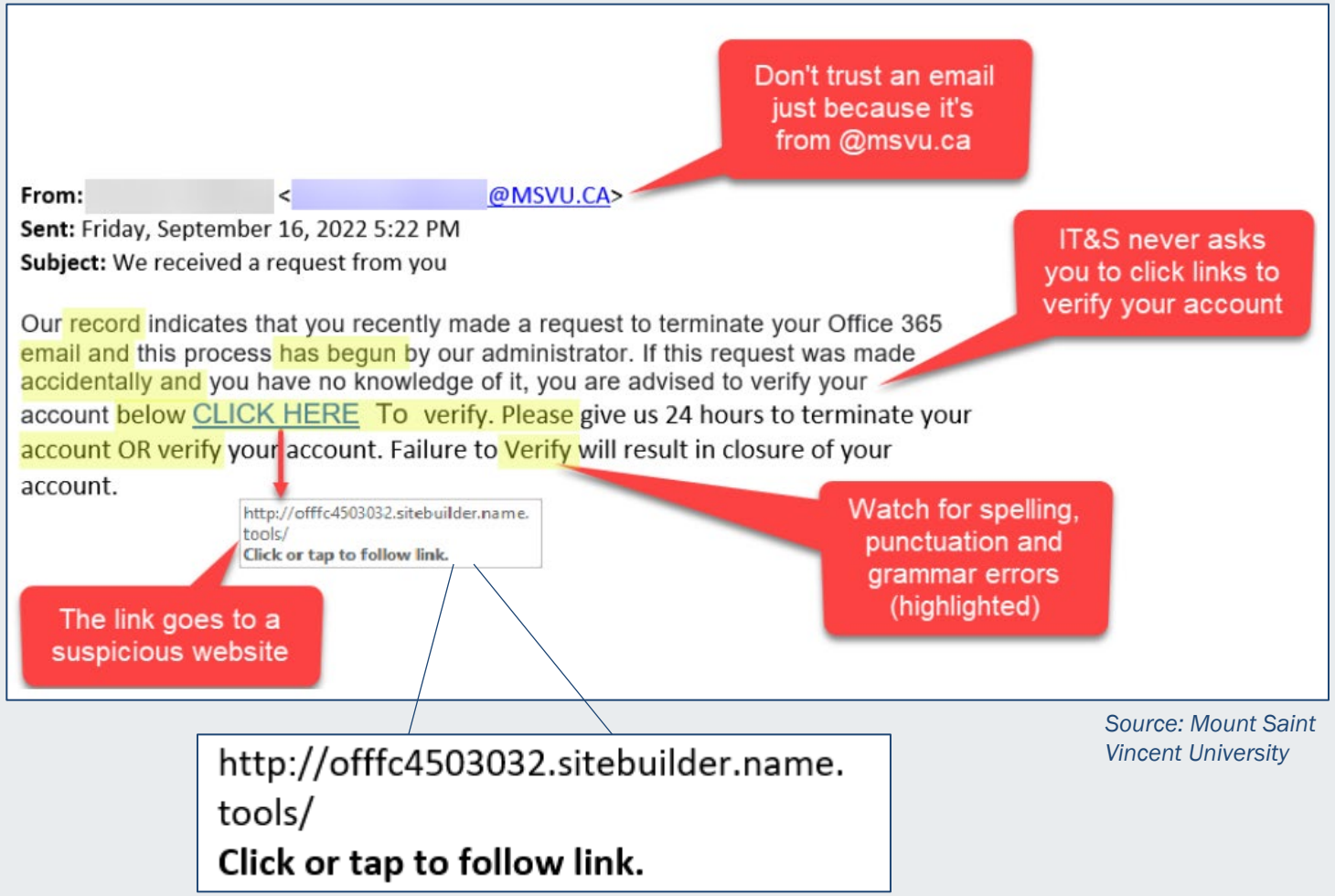
Phishing

Phishing is a form of social engineering where attackers try to deceive people into either installing malware or revealing sensitive information.

- Suspicious-looking source address
- Generic greetings
  - “Dear Customer”
- Spoofed hyperlinks
- Poor spelling
- Suspicious attachments
  - All attachments and links should be treated with caution.

Example of a Phishing Email

- Call to action
- Suspicious link
- Grammatical errors



Source: Mount Saint Vincent University

Password Hygiene

Creating strong passwords can help users limit the actions from an attacker.

- Complex passwords
- Avoid recycling passwords
- Change default credentials
- Recommended at least 12 characters
- Password manager

Source: thecyberexpress

Multi-Factor Authentication (MFA)

Incorporating multi-factor authentication can help add an additional layer of security for accounts, beyond traditional usernames and passwords.

Reference Materials

References

- Baker, Kurt. “5 TYPES OF RANSOMWARE”. CrowdStrike. 30 Jan 2023. 5 Most Common Types of Ransomware - CrowdStrike
- Baker, Kurt. “HISTORY OF RANSOMWARE”. CrowdStrike. 10 Oct 2022. https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/
- Baker, Kurt. “RANSOMWARE AS A SERVICE (RAAS) EXPLAINED - HOW IT WORKS & EXAMPLES”. CrowdStrike. 30 Jan 2023. https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/
- “Best Password Hygiene Practices to Protect Your Data”. The Cyber Express. 08 Aug 2022. https://thecyberexpress.com/password-hygiene-simple-steps-to-prevent-data-breach/
- CISA. “#StopRansomware Guide”. https://www.cisa.gov/stopransomware/ransomware-guide
- CISA. “Recognize and Report Phishing”. https://www.cisa.gov/secure-our-world/recognize-and-report-phishing

References

- CISA. “More Than A Password”. https://www.cisa.gov/MFA
- Chappell, Bill. “WannaCry Ransomware: What We Know Monday”. Npr. 15 May 2017. https://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday
- “Critical Ransomware Threat to Public Hospital/Health Systems”. Marcum. 29 Oct 2020. https://www.marcumllp.com/insights/critical-ransomware-threat-to-public-hospital-health-systems
- “Cyber Hygiene: Ransomware is Causing Critical Care Disruption in Hospitals”. Securin. 15 Oct 2020. https://www.securin.io/articles/cyber-hygiene-ransomware-is-causing-critical-care-disruption-in-hospitals/
- CISA. “Securing Network Infrastructure Devices”. https://www.cisa.gov/news-events/news/securing-network-infrastructure-devices

References

- Chin, Kyle. “How to Prevent Ransomware Attacks: Top 10 Best Practices in 2023”. UpGuard. 15 Nov 2023. https://www.upguard.com/blog/best-practices-to-prevent-ransomware-attacks
- De Groot, Juliana. “A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time”. Digital Guardian. 28 Dec 2022. https://www.digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time
- Good, Caitlin. “Patch Management vs. Vulnerability Management”. Syncro. 25 May 2022. https://syncromsp.com/blog/patch-management-vs-vulnerability-management/
- Hacquebord, Feike, Hilt, Stephen, Sancho, David. “THE FUTURE OF RANSOMWARE”. TrendMicro. 15 Dec 2022. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-future-of-ransomware
- “How Network Segregation, Segmentation Can Stop Ransomware Attacks”. Hitinfrastructure. 08 Feb 2019. https://hitinfrastructure.com/features/how-network-segregation-and-segmentation-can-stop-ransomware-attacks
- Kelley, Diana. “Top 6 password hygiene tips and best practices”, Tech Target. 11 Oct 2023. https://www.techtarget.com/searchsecurity/tip/Top-5-password-hygiene-tips-and-best-practices

References

- Kelley, Diana. “Top 3 ransomware attack vectors and how to avoid them”. Tech Target. 14 Aug 2023. https://www.techtarget.com/searchsecurity/tip/Top-3-ransomware-attack-vectors-and-how-to-avoid-them
- Kaspersky. “What is Ransomware?”. https://www.kaspersky.com/resource-center/threats/ransomware
- Laffan, Kieran. “A Brief History of Ransomware”. Varonis. 09 Jun 2023. A Brief History of Ransomware (varonis.com)
- Lenaerts-Bergmans, Bart. “CYBER BIG GAME HUNTING”. CrowdStrike, 24 Oct 2023. https://www.crowdstrike.com/cybersecurity-101/cyber-big-game-hunting/

References

- Meskauskas, Tomas. “BlackSuit (.blacksuit) ransomware virus - removal and decryption options”. Pcrisk. 25 May 2023. https://www.pcrisk.com/removal-guides/26646-blacksuit-ransomware
- National Security Cyber Centre. “A guide to ransomware”. https://www.ncsc.gov.uk/ransomware/home#:~:text=What%20is%20ransomware%3F-,Ransomware%20is%20a%20type%20of%20malware%20which%20prevents%20you%20from,ransom%20in%20exchange%20for%20decryption
- NIST. “Ransomware”. https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware
- “Phishing Email Examples”. Mount Saint Vincent University. https://www.msvu.ca/campus-life/campus-services/it-services/it-security/phishing/phishing-email-examples/
- “R/C Midrange Ambulance”. DRIVEN. https://drivenbybattat.com/product/r-c-midrange-ambulance/
- SentielOne. “What Is Rhysida Ransomware?”. https://www.sentinelone.com/anthology/rhysida/

References

- Watts, Ben. “How to prevent ransomware attacks with good email security”. Cyber Security Hub. 08 Aug 2023. https://www.cshub.com/security-strategy/articles/prevent-advanced-ransomware-attacks-with-good-email-security
- “What Is Endpoint Management?”. Sentinel One. https://www.sentinelone.com/cybersecurity-101/endpoint-management/
- “What Is Ransomware? Attack Types, Examples, Detection, and Prevention”. Perception Point. https://perception-point.io/guides/ransomware/what-is-ransomware-attack-types-examples-detection-and-prevention/
- Whittaker, Zack. “Two years after WannaCry, a million computers remain at risk”. TechCrunch. 12 May 2019. https://techcrunch.com/2019/05/12/wannacry-two-years-on/
- “7 Steps to Help Prevent & Limit the Impact of Ransomware”. Center for Internet Security.
- https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware
- “9 Steps to Mitigate Ransomware Attacks for Your Business”. SecurityScorecard. https://securityscorecard.com/blog/steps-to-mitigate-ransomware-attacks/

Questions

FAQ

Upcoming Briefing

- February 15 – Russian Threat Actors Targeting the HPH Sector

Product Evaluations

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

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

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

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes

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

Threat Briefings

Presentations that provide 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.

CPE Credits

This 1-hour presentation by HHS HC3 provides you with 1 hour of CPE credits based on your Certification needs.

The areas that qualify for CPE credits are Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Typically, you will earn 1 CPE credit per 1 hour time spent in an activity. You can report CPE credits in 0.25, 0.50 and 0.75 increments.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Contacts

WWW.HHS.GOV/HC3

HC3@HHS.GOV