HC3: Healthcare Cybersecurity Bulletin

Q1 2023 TLP:CLEAR Report: 202304061200

Executive Summary

In Q1 of 2023, HC3 observed a continuation of many ongoing trends with regards to cyber threats to the Healthcare and Public Health community. Ransomware attacks, data breaches and often both together continued to be prevalent in attacks against the health sector. Ransomware operators continued to evolve their techniques and weapons for increasing extortion pressure and maximizing their payday. Vulnerabilities in software and hardware platforms, some ubiquitous and some specific to healthcare, continued to keep the attack surface of healthcare organizations open. Managed service provider compromise continued to be a significant threat to the health sector, as did supply chain compromise.

News and Industry Reports of Interest

Emotet back online and operational

https://www.trendmicro.com/en_us/research/23/c/emotet-returns-now-adopts-binary-padding-for-evasion.html

Emotet – historically a prolific threat to the health sector – went operational again in early March after being offline for three months. The operators began to reconstitute their command-and-control infrastructure in late January. Their epochs began going back online on January 25, and on March 8, four epochs resumed delivery of phishing e-mails, which is their standard practice for distributing malicious office documents in ZIP archives. One new technique they are using now is binary padding. They are inflating both the dropper and the dynamic link library to avoid detection by exceeding size limitations by anti-malware software. After the payload is successfully downloaded, Emotet does a check to ensure the file is either ZIP or a PE (portable executable). This seems to suggest they may be preparing to leverage other file formats outside of zipped archives in the future. They have also been spotted using fake W-9 tax forms purported to be from the IRS.

Microsoft Exchange Server 2013 to reach EoS in April

https://www.bleepingcomputer.com/news/security/microsoft-exchange-server-2013-reaches-end-of-support-in-april/

Microsoft released a public notification that Exchange Server 2013 will reach its extended end-of-support date on April 11, 2023. It reached its mainstream end date in April 2018. Once this extended EOS date is reached this coming April, Microsoft will stop providing technical support and bug fixes for it.

Microsoft Announces End of Support for Windows Server 2012

https://learn.microsoft.com/en-US/lifecycle/announcements/windows-server-2012-r2-end-of-support

Microsoft announced end of support for Windows Server 2012 and 2012 R2. The official date is October 10, 2023, so the good news is that there is still some time. The bad news is that server migrations and upgrades are major projects and can take a lot of time. As part of this, they are providing three options: migrate to Azure, which is their cloud solution, upgrade on-prem to Server 2022, or subscribe to extended security updates which will provide three more years of updates.

Multiple vulnerabilities in OpenEMR

https://www.sonarsource.com/blog/openemr-remote-code-execution-in-your-healthcare-system/

Vulnerabilities were made public for OpenEMR, which is a popular open-source electronic health record and medical practice management application. They can be used to fully compromise a system running a vulnerable version. There is a patched version available.

HC3 Products

HC3: Healthcare Cybersecurity Bulletin

Q1 2023 TLP:CLEAR Report: 202304061200

In the fourth quarter of 2021, HC3 released alerts, briefs and other guidance on vulnerabilities, threat groups and technical data of interest to the Healthcare and Public Health community. Our products can be found at this link: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html. The below table highlights those products.

DATE	TITLE	SUMMARY
1/4	Clop Ransomware Analyst Note	Clop operates under the Ransomware-as-service (RaaS) model, and it was first observed in 2019. Clop was a highly used ransomware in the market and typically targeted organizations with a revenue of $5 million U.S. Dollars (USD) or higher. The HPH sector has been recognized as being a highly targeted industry for the Clop ransomware.
1/12	Threat Brief: Royal & BlackCat Ransomware	Two relatively new ransomware variants, Royal and BlackCat, that both pose a significant threat to the Healthcare and Public Health (HPH) sector.
1/17	AI for Malware Development Analyst Note	Artificial intelligence (AI) has now evolved to a point where it can be effectively used by threat actors to develop malware and phishing lures. While the use of AI is still very limited and requires a sophisticated user to make it effective, once this technology becomes more user-friendly, there will be a major paradigm shift in the development of malware. One of the key factors making AI particularly dangerous for the healthcare sector is the ability of a threat actor to use AI to customize attacks easily and quickly against the healthcare sector.
1/18	2022 Q4 Healthcare Cybersecurity Bulletin	A list and summary of the Q4 products for HC3 as well as news updates of interest to the Healthcare and Public Health (HPH) sector.
1/19	December 2022 Vulnerability Bulletin	Summary of vulnerabilities patched in December 2022 pertinent to the HPH, including those released during Patch Tuesday.
2/6	January 2023 Vulnerability Bulletin	Summary of vulnerabilities patched in January pertinent to the HPH, including those released during Patch Tuesday.
2/9	Threat Brief: Healthcare Cybersecurity - 2022 Retrospective & 2023 Look Ahead	A retrospective look back at some of the events of 2022 that are significant to the Health and Public Health (HPH) sector including cyberattacks, vulnerabilities, new regulations and legislation, research and well as geopolitical events of significance.
2/13	Healthcare Sector DDoS Guide	Distributed Denial of Service (DDoS) attacks have the potential to deny healthcare organizations and providers access to vital resources that can have detrimental impact on the ability to provide care. In healthcare, disruptions due to a cyberattack 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.
2/22	Clop Allegedly Targets Healthcare Industry in Data Breach	Russia-linked ransomware group Clop reportedly took responsibility for a mass attack on more than 130 organizations, including those in the healthcare industry, using a zero-day vulnerability in secure file transfer software GoAnywhere MFT. The Cybersecurity & Infrastructure Security Agency (CISA) added the GoAnywhere flaw (CVE-2023-0669) to its public catalog of Known Exploited Vulnerabilities. This Sector Alert follows previous HC3 Analyst Notes on Clop (CLOP Poses Ongoing Risk to HPH Organizations and CLOP Ransomware) and provides an update

		on its recent attack, potential new tactics, techniques and procedures (TTPs), and recommendations to detect and protect against ransomware attacks.
2/24	MedusaLocker Ransomware Analyst Note	Ransomware variants used to target the healthcare sector, from relatively well-known cyber threat groups, continue to be a source of concern and attention. (See HC3 reports on Royal Ransomware and Clop Ransomware). Likewise, the threats from lesser known but potent ransomware variants, such as the MedusaLocker, should also be a source of concern and attention by healthcare security decision makers and defenders.
3/8	The HPH Sector Cybersecurity Framework Implementation Guide	This guide is intended to help public and private healthcare sectors prevent cybersecurity incidents.
3/9	Threat Briefing: Data Exfiltration Trends in Healthcare	The health sector is highly susceptible to data exfiltration attacks and this brief includes a review of recent trends by threat actors on carrying out such attacks.
3/13	February 2023 Vulnerability Bulletin	Summary of vulnerabilities patched in February pertinent to the HPH including those released during Patch Tuesday.
3/15	Black Basta Threat Profile	Black Basta was initially spotted in early 2022. Known for its double extortion attacks, the Russian-speaking group not only executes ransomware, but also exfiltrates sensitive data, operating a cybercrime marketplace to publicly release it, should a victim fail to pay a ransom. The threat group's prolific targeting of at least 20 victims in its first two weeks of operation indicates that it is experienced in ransomware and has a steady source of initial access. The level of sophistication by its proficient ransomware operators, and reluctance to recruit or advertise on dark web forums, supports why many suspect the nascent Black Basta may even be a rebrand of the Russian-speaking RaaS threat group Conti, or also linked to other Russian-speaking cyber threat groups. Previous HC3 Analyst Notes on Conti and BlackMatter even reinforce the similar tactics, techniques, and procedures (TTPs) shared with Black Basta. As ransomware attacks continue to increase, this Threat Profile highlights the emerging group and and provides best practices to lower risks of being victimized.
3/23	HPH Mobile Device Security Checklist	Mobile devices are prevalent in the health sector, and due to their storage and processing of private health information (PHI) and other sensitive data, these devices can be a critical part of healthcare operations. This document represents a basic checklist of recommended items for health sector mobile devices to maintain security, including data in motion and at rest, as well as the capabilities of the device itself.

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback