HC3: Healthcare Cybersecurity Bulletin

Q4 2022 TLP:CLEAR Report: 202301181700

Executive Summary

In Q4 of 2022, 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 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 wide 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

Dutch National Police and Respomnders.NU trick ransomware gang into handing over decyption keys

The Dutch National Police worked with the cybersecurity company Responders.NU to trick a ransomware gang – DeadBolt – into handing over decryption keys. The DeadBolt gang have aggressively attacked network-attached storage devices. They were able to acquire 155 decryption keys before the group determined what had occurred. According to the Dutch authorities, Deadbolt has launched successful ransomware attacks against 20,000 NAS devices worldwide and 1,000 of those in the Netherlands.
https://www.bleepingcomputer.com/news/security/police-tricks-deadbolt-ransomware-out-of-155-decryption-keys/

Meta Pixel security issues lead to healthcare data leaks

Meta Pixel is Facebook's JavaScript tracker that can be added to a website to track how people interact with ads, and it can track interactions with current and prospective customers. Ultimately, it allows for targeted improvements. Pixel was found to have security issues causing leaked PHI for a number of hospitals.
https://www.bleepingcomputer.com/news/security/health-system-data-breach-due-to-meta-pixel-hits-3-million-

World leaders and corporate executives meet in Washington DC to discuss global cybercrime

In late October, the White House hosted leaders from over 30 countries, as well as individuals from the private sector, to reinforce and double down on international efforts to combat ransomware and various other kinds of cybercrime. Companies who were represented included Microsoft, Palo Alto, SAP, Crowdstrike, and this year they've invited 13 countries from around the world. The first session was held at FBI headquarters and attended by Director Chris Wray, and there was a briefing by representatives from the FBI, ODNI and CISA. The following day they met at the Treasury Department.
https://therecord.media/white-house-aims-to-redouble-global-push-against-ransomware/

Senator Warner releases white paper soliciting feedback on healthcare cybersecurity

In early November, Senator Mark Warner (D-VA) released a white paper soliciting input from the private sector as well as the research community on healthcare cybersecurity issues. HIPAA was called out as a piece of legislation that needs to be modernized. The white paper requested feedback on NIST standards and their utility for the health sector as well as feedback on federal government collaboration and the effectiveness of the 405(d) program, on cyber hygiene and feedback on the possible requirement that healthcare practitioners train on legacy systems in the event of a catastrophic event.
https://therecord.media/senior-dem-solicits-input-for-health-care-cybersecurity-legislation/

HC3: Healthcare Cybersecurity Bulletin

Q4 2022 TLP:CLEAR Report: 202301181700

HC3 Products

In the fourth quarter of 2021, HC3 released alerts, briefs and other guidance on vulnerabilities, threat groups and technical data of interest to the health sector and public health community. Our products can be found at this link: https://www.hhs.gov/HC3. Those products are also highlighted below.

- Abuse of Legitimate Security Tools and Health Sector Cybersecurity – October 6 – https://www.hhs.gov/sites/default/files/abuse-of-legitimate-security-tools-hph.pdf
  - Overview of legitimate security and penetration testing tools used to protect HOH systems which are often used in cyberattacks against the same systems; Includes mitigations and defense recommendations
- September 2022 Vulnerability Bulletin – October 25 – https://www.hhs.gov/sites/default/files/september-2022-vulnerability-bulletin.pdf
  - Summary of vulnerabilities patched in September pertinent to the HPH including those released during Patch Tuesday
- Joint HHS, CISA, FBI Alert: Daixin Team – October 24
  - The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Department of Health and Human Services (HHS) are releasing this joint CSA to provide information on the "Daixin Team," a cybercrime group that is actively targeting U.S. businesses, predominantly in the Healthcare and Public Health (HPH) Sector, with ransomware and data extortion operations. The Daixin Team is a ransomware and data extortion group that has targeted the HPH Sector with ransomware and data extortion operations since at least June 2022. Since then, Daixin Team cybercrime actors have caused ransomware incidents at multiple HPH Sector organizations. This joint CSA provides TTPs and IOCs of Daixin actors obtained from FBI threat response activities and third-party reporting.
- Sector Alert: Critical OpenSSL Vulnerability Will Require Action by Healthcare Organizations – October 28 – https://www.hhs.gov/sites/default/files/openssl-critical-patch.pdf
  - A software library called OpenSSL which is deployed across the health sector is going to receive an important update on November 1, 2022. This sector alert notifies the HPH of this upgrade and describes the steps needed to identify applicable systems and appropriately upgrade them.
- Brief: Iranian Threat Actors & Healthcare – November 3 – https://www.hhs.gov/sites/default/files/iranian-threat-actors-and-healthcare.pdf
  - Overview of the Iranian state-sponsored cyber threat landscape and how it applies to the HPH
- Analyst Note: Venus Ransomware Targets Publicly Exposed Remote Desktop Services – November 9 – https://www.hhs.gov/sites/default/files/venus-ransomware-analyst-note.pdf
  - Overview of the Venus ransomware operators who are known to target the U.S. health sector. This includes an overview of their operations as well as indicators of compromise and a MITRE ATT&CK mapping along with defense and mitigation recommendations.

- October 2022 Vulnerability Bulletin – November 14 – https://www.hhs.gov/sites/default/files/hc3-october-2022-vulnerability-bulletin.pdf
    - Summary of vulnerabilities patched in October pertinent to the HPH including those released during Patch Tuesday.
- Analyst Note: Lorenz Ransomware – November 21 – https://www.hhs.gov/sites/default/files/lorenz-analyst-note.pdf
    - Overview of the Lorenz Ransomware gang who, in the short time they have been operating have targeted the U.S. health sector. This includes an overview of their operations as well as indicators of compromise.
- Amplification Alert: Cuba Ransomware – December 2 – https://www.hhs.gov/sites/default/files/cuba-ransomware-alert-tlpclear.pdf
    - Notification to the HPH that the FBI and CISA released a joint alert on Cuba Ransomware including indicators of compromise as we
- Analyst Note: Royal Ransomware – December 7 – https://www.hhs.gov/sites/default/files/royal-ransomware-analyst-note.pdf
    - Overview of the Royal ransomware gang who, in the short time they have been operating have targeted the U.S. health sector. This includes an overview of their operations as well as indicators of compromise.
- November 2022 Vulnerability Bulletin – December 8 – https://www.hhs.gov/sites/default/files/november-2022-vulnerability-bulletin-tlpclear.pdf
    - Summary of vulnerabilities patched in November pertinent to the HPH including those released during Patch Tuesday.
- Automation & Hacking: Potential Impacts on Healthcare – December 8 – https://www.hhs.gov/sites/default/files/automation-hacking-healthcare.pdf
    - The use of Automated tools in cybersecurity operations and hacking, as it pertains to the health sector. This includes examples of tools as well as use cases.
- Analyst Note: LockBit 3.0 – December 12 – https://www.hhs.gov/sites/default/files/lockbit-3-analyst-note.pdf
    - Overview of the LockBit 3.0 ransomware variant and operators who have been operating have targeted the U.S. health sector. This includes an overview of their operations as well as indicators of compromise.
- Analyst Note: BlackCat – December 12 – https://www.hhs.gov/sites/default/files/blackcat-analyst-note.pdf
    - Overview of the BlackCat ransomware gang who has targeted the U.S. health sector. This includes an overview of their operations, defense and mitigations recommendations as well as indicators of compromise.
- Sector Alert: Citrix ADC and Gateway Vulnerabilities. – December 16 – https://www.hhs.gov/sites/default/files/citrix-adc-gateway-sector-alert.pdf
    - Citrix released patches for a vulnerability that impacts both their Application Delivery Controller and Gateway platforms. This vulnerability allows a remote attacker to completely compromise a target system. These vulnerabilities are known to be actively exploited by a

highly capable state-sponsored adversary. Healthcare entities that have been compromised by the exploitation of this vulnerability.

- **Analyst Note: Killnet – December 22 –** https://www.hhs.gov/sites/default/files/killnet-analyst-note-tlpclear.pdf
    - Overview of the Russian hacktivist gang who has targeted the U.S. health sector. This includes an overview of their operations, defense and mitigations recommendations, as well as indicators of compromise.

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