Urgent Cybersecurity Alert: Imminent Ransomware Threat in the Healthcare Sector

ARTICLE 10.29.20 DEAN DORTON

An advisory has been released by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS). **This advisory describes the tactics, techniques, and procedures (TTPs) used by cybercriminals against targets in the Healthcare and Public Health Sector (HPH) to infect systems with Ryuk ransomware for financial gain. CISA, FBI, and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers.** CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats.

Dean Dorton recommends the implementation of a strong information security program that includes ongoing security risk assessment to assess and remediate any weaknesses that might be exploited by threat actors and to minimize the risk of Ransomware and other cyber threats. Preparedness is critical and incident response playbooks specific to Ransomware should be developed, tested, and updated on a regular basis.

Dean Dorton strongly recommends all Healthcare organizations to review the recommendations included in the link below and to contact us if you need any assistance.

These recommendations include:

- Patch operating systems, software, and firmware as soon as manufacturers release updates.
- Check configurations for every operating system version for organization-owned assets to prevent issues from arising that local users are unable to fix due to having local administration disabled.
- Regularly change passwords to network systems and accounts and avoid reusing passwords for different accounts.
- Use multi-factor authentication where possible.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Implement application and remote access allow listing to only allow systems to execute programs known and permitted by the established security policy.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind. Audit logs to ensure new accounts are legitimate
- Identify critical assets; create backups of these systems and house the backups offline from the network.

- Implement network segmentation. Sensitive data should not reside on the same server and network segment as the email environment.
- Set antivirus and anti-malware solutions to automatically update.
- Conduct ongoing security risk assessments. Scan for open or listening ports and mediate those that are not needed.

Cybersecurity Advisory

Gui Cozzi
Cybersecurity Associate Director
gcozzi@ddaftech.com • 859.425.7649