??????????????

??????????????

???Nitanshu Upadhyay

Healthcare organizations are more vulnerable to data breaches as they increasingly move operations and patient data online and rely on virtual services. The average cost of a security breach in the healthcare industry is $10.1 million, which is 9.4 percent up from $9.2 million in 2021. This is the highest average cost of a breach for the past 12 years. The cost of a security breach in healthcare has increased by 42 percent since 2020, according to IBM. Healthcare presents many challenges unique to the industry:

- Most healthcare providers lack an established framework and don't use an internal hardened build standard to validate their current state. These frameworks include NIST, HITRUST, CIS, DISA, and HIPAA.
- Most of the changes to patient data are done manually, making it difficult to capture changes in scope, processes, and jobs. It's unclear who has access to systems retaining patient data and electronic records.
- Limited resources are allocated to IT security as healthcare is a cost-constrained industry.

Although we are just a month into the new year, numerous cybersecurity events are already making arising in healthcare. This blog focuses on a few recent cybersecurity events that occurred in the healthcare sector.

More Than 250,000 People Were Affected by a Recent Healthcare Data Breach

Third-party insurance administrator Bay Bridge Administrators (BBA) experienced a data security incident affecting nearly 250,000 individuals enrolled in some employment insurance benefits administered by BBA in 2022. A threat actor gained unauthorized access to the BBA network in late August 2022 and used that access to obtain data. The stolen data included names, Social Security Numbers, health insurance information, medical information, driving license numbers, and dates of birth.

Trend Micro Uncovers Gootkit Malware Actively Targeting the Australian Healthcare Sector

The Gootkit loader has resurfaced in a recent campaign, targeting the Australian healthcare sector by exploiting SEO poisoning for its initial access and abusing legitimate tools such as VLC Media Player. The Gootkit malware is capable of stealing data from the browser and performing other malicious actions.

How to Fight Gootkit Malware

The healthcare sector is uniquely vulnerable to cyberattacks, which is a cause of constant concern for top healthcare cybersecurity companies. IT security in healthcare needs to evolve considering the potential cybersecurity threats and develop robust solutions to mitigate risks.

Organizations must prioritize healthcare cyber threat prevention and must take necessary steps to mitigate against such attacks. For instance, below is our recommendation for how healthcare organizations in Australia can fight the Gootkit malware attack:

- The attack vector has used multiple tools to execute the malware and used different ports to connect to the network. Ports 389, 445, 3268 must be blocked in the firewall/IDPS, and if needed, the ports can be allowed for specific source and destination IPs.
- Since this malware is currently targeting the healthcare and legal sectors, we need to notify the appropriate people to be aware and block the IOCs. IOCs such as IPs, domains, and file hash used to spread the infection should be blocked at the perimeter/EDR tools.
- Since the malware searches the internet for WordPress contract sites, the application needs to be updated with patches and plugins/themes should be from trusted sources.
- The network and application layer should be configured with the least privileges and a specific source to restrict access for external users.

We also recommend that providers partner with a service provider who is well-versed with the terrain.

At Centific, we define a comprehensive healthcare cyber strategy with best practices to manage our clients' risks and protect the enterprise. Our digital safety framework mitigates against various security events and prepares organizations to become more vigilant against vulnerabilities.

Using our framework capabilities, we perform an automated security posture analysis that provides us with a risk score based on which we perform a vulnerability assessment. This helps us plan for security breaches and attack simulations, tests security policies, and provides a security architecture recommendation that leads to an optimized total cost of ownership.

Contact us for more information. Learn more about the author of this post, Nitanshu Upadhyay, by visiting his LinkedIn profile.

-
-
-
-
-