BRUNSWICK

US Issues Warning on North Korean Hackers

Takeaways for the Healthcare and Public Health Sector

Brunswick Cybersecurity and Data Privacy Practice

July 2022

Collective Intelligence

US Issues Warning on North Korean Hackers: Takeaways for the Healthcare and Public Health Sector

Overview

On July 6, 2022, the FBI, Cybersecurity and Infrastructure Security Agency (CISA) and the Department of the Treasury jointly issued a Cybersecurity Advisory, which cautioned hospital systems and other organizations operating in the public health sector of an uptick in North Korean state-backed hackers targeting their networks with a strain of ransomware dubbed "Maui."

The advisory outlines concrete, tactical steps that senior leadership can take to buttress cybersecurity preparedness and defenses, such as implementing security controls and conducting phishing exercises for employees. The document also underscores growing governmental scrutiny of the Maui ransomware variant, which is unlike traditional, pre-developed ransomware tools. Maui is manually operated, for example, which allows the threat actor to select which files to encrypt when deploying the malware.

The interagency warning comes amid a surge in healthcare breaches over the last few months, with the US Department of Health and Human Services (HHS) listing more than 240 electronic data breaches of large healthcare organizations this year – a 78% increase from 2021. In addition, the advisory amplifies the US government's broader efforts to discourage ransomware payments, including a September 2021 updated advisory from the Treasury Department that emphasized the sanctions risks tied to ransomware payments and suggested "meaningful steps" to lessen the risk of data-related extortion activities, such as maintaining offline data backups and developing incident response plans.

Healthcare is increasingly in North Korea's crosshairs

The advisory comes amid intensifying political headwinds with the US, EU and other likeminded governments. The US, for example, has stepped up sanctions pressure on Pyongyang over the last three months following a spate of missile launches earlier this year, including one in April that marked North Korea's first full Intercontinental Ballistic Missile test in five years.

Sanctions have exacerbated economic challenges facing North Korea, which closed its borders during the COVID-19 pandemic and experienced a slump with its leading trading partner - China. As a result, North Korea's cybercriminals now face mounting pressure to expand their operations to new targets, including healthcare and public health systems, to help replenish the coffers of the state's elites and fund the government's nuclear weapons program.

Organizations operating in the HPH sector should expect state-backed North Korean hackers to increasingly target their networks for data-related extortion efforts. These intrusions may also lay the groundwork for longer-term cyber-enabled espionage. Cybersecurity researchers reported in February, for example, that North Korean hacking group Lazarus has been delivering malware to unsuspecting users through the use of doctored Microsoft Word files guised as employment opportunities from a leading defense contractor. The phishing documents allowed the threat actor to deliver payloads, subsequently install spyware on the victims' computers and gain access to potentially sensitive and proprietary information.

Advisory recommendations

1. Implement security controls

The advisory includes indicators of compromise for the Maui variant and suggested technical measures that companies can adopt to mitigate the risk of ransomware, including but not limited to the following:

- **Confirm that patching is up to date** against all known vulnerabilities, such as Microsoft Windows LSA Spoofing Vulnerability.

- **Pay careful attention to network activity**. For example, monitor remote access/remote desktop protocol logs and enforce account lockouts after a specified number of attempts to defend against brute force campaigns.
- **Require multi-factor authentication,** especially for webmail, VPNs and accounts that access critical systems, to mitigate credential theft and reuse.

2. Implement user training program and phishing exercises

The advisory also emphasizes the importance of addressing the role of people in managing cyber threats. For example, the document calls for organizations to take steps to raise awareness among users about the risks of clicking on suspicious links and opening attachments from unknown or unusual senders.

Additionally, the advisory highlights the importance of developing and exercising an incident response plan beforehand as well as thorough security stress tests. While these are crucial to bolstering the company's strategic response, prevention is also key. To this end, companies are advised to conduct training to help employees identify and report spear phishing and other common attacks.

3. Confirm backup of key data

The advisory recommends that IT staff should not only test the backup system, but also verify that these backups are offline and beyond the reach of cyber criminals. This is especially true for the "crown jewels," or any data essential to a company's regular business operations that would attract the most attention from highly capable cyber actors. The absence or incomplete nature of a company's backup strategy expands the window of opportunity for cyber criminals and increases the probability of their success.

Next steps to prepare for heightened cyber risk

This advisory recommends that companies have an incident response plan that explicitly addresses ransomware attacks, and that they periodically test the plan, including the senior leadership team. Brunswick can assist companies with all aspects of this preparation and refresh existing materials to reflect the changing threat landscape. Specifically, Brunswick can help with the following:

- **Assess the business risks and reputational impacts** of cyberattacks, including ransomware, that companies face;
- **Plan, exercise, and implement corporate-wide strategy** for cyber crises; and
- **Prepare the company leadership and employees** to lead through such crises, should they occur.

Additionally, our global cyber team has experience working with clients to develop effective internal cyber education campaigns that engage employees and train them to be an informed line of defense against cyber incidents.

To continue the conversation:

Brunswick's global Cybersecurity, Data and Privacy team helps companies in every region and every sector prepare for, respond to and build resilience to existing threats and future risks. For more information, please contact Cyber@BrunswickGroup.com.