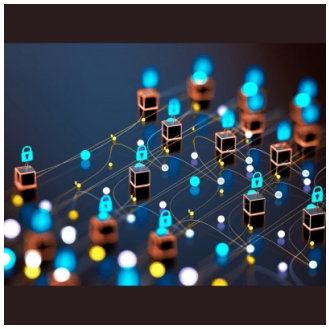
HealthManagement
Promoting Management and Leadership

Twist in the Change Healthcare Cyberattack: New Menace Emerges



Twist in the Change Healthcare Cyberattack: New Menace Emerges

Across the landscape of healthcare cybersecurity this week, a looming specter of a potential double-extortion attack by RansomHub has emerged concerning Change Healthcare in the wake of the February cyberattack by ALPHV. The narrative surrounding the Change Healthcare breach has taken a twist, with the emergence of a new ransomware group named RansomHub claiming possession of 4TB of data stolen from the healthcare tech company back in February.

The ALPHV Attack and RansomHub's Emergence

Change Healthcare, a platform under the ownership of UnitedHealth Group subsidiary Optum, fell victim to a breach by an affiliate of the ALPHV/BlackCat ransomware group in February. This breach resulted in widespread operational disruptions and raised concerns about the potential leak of sensitive patient and client data. It has been reported by multiple sources that a new group, RansomHub, is now claiming ownership of the 4TB of stolen data from Change Healthcare and has threatened to make it public unless a ransom is paid. There are reports suggesting that Optum may have paid a $22 million ransom, as evidenced by blockchain transaction records associated with ALPHV/BlackCat. However, it appears that this payment was allegedly stolen by the ransomware-as-a-service (RaaS) group in an exit scam. The group purportedly published a fake law enforcement takedown notice on their leak site before disappearing with the entire $22 million, leaving the affiliate who conducted the breach, known as "notchy," empty-handed.

RansomHub's Ultimatum: A Deadline for Payment and Data Exposure

Now, a new ransomware group named RansomHub has entered the fray, initiating demands for payment and threatening to expose the stolen data. They have set a deadline of just over 12 days for UnitedHealth to make a ransom payment before proceeding to sell the dataset. According to RansomHub, the 4TB of data includes a wide array of sensitive information, such as medical and dental records, payment and claims data, as well as personal identifiable information (PII) of patients, including social security numbers, and even PII of active U.S. military personnel. Additionally, the group claims to have obtained more than 3,000 source code files for Change Healthcare's software solutions.

Intricacies of Ransomware-as-a-Service: Adding Layers to the Cybersecurity Scenarios

The involvement of middlemen in ransomware attacks, typical in ransomware-as-a-service (RaaS) operations, adds another layer of complexity and risk to negotiations and payment processes. This complexity makes it challenging for affected companies to establish direct lines of communication with threat actors. The potential exposure of such a significant trove of protected health data underscores the urgent need for robust business-continuity planning and the implementation of enhanced security measures. The dynamic and unpredictable nature of the threat landscape emphasises the importance of proactive cybersecurity measures aligned with industry best practices. Furthermore, businesses must carefully consider the implications of paying ransoms to avoid becoming soft targets for repeated attacks. Disaster preparedness planning should encompass considerations of extortion scenarios, insurance coverage, regulatory obligations, and the tactics, techniques, and procedures (TTPs) of threat actors.

The evolving nature of cyber threats demands continuous vigilance and proactive measures to safeguard sensitive data and uphold the integrity of healthcare systems. The recent incidents involving Change Healthcare serve as a stark reminder of the persistent challenges faced by organisations in defending against cyber threats in an increasingly digital world.

Source: SCMedia

Image Credit: iStock

Published on : Tue, 16 Apr 2024