EINPRESSWIRE

Change Healthcare hit with second ransomware attack affecting over 3000 US service members records- Axios Security Group

Change Healthcare received another significant cyber attack just weeks after a major ransomware attack took down its systems and delayed prescription services.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

MITRE ATT&CK TACTICS AND TECHNIQUES

See Table 1 through Table 3 for all referenced threat actor tactics and techniques in this advisory.

Table 1: ALPHV Blackcat/ALPHV Threat Actors ATT&CK Techniques - Reconnaissance

Technique Title	ID	Use
Phishing for Information	T1598	ALPHV Blackcat affiliates pose as company IT and/or helpdesk staff using phone calls or SMS messages to obtain credentials from employees to access the target network.

Table 2: ALPHV Blackcat/ALPHV Threat Actors ATT&CK Techniques – Resource Development

Technique Title	ID	Use
Compromise Accounts	T1586	ALPHV Blackcat affiliates use compromised accounts to gain access to victims' networks.

Table 3: ALPHV Blackcat/ALPHV Threat Actors ATT&CK Techniques – Credential Access

Technique Title	ID	Use
Obtain Credentials from Passwords Stores	T1555	ALPHV Blackcat affiliates obtain passwords from local networks, deleted servers, and domain controllers.
Adversary-in-the-Middle	T1557	ALPHV Blackcat/ALPHV affiliates use the open-source framework Evilginx2 to obtain MFA credentials, login credentials, and session cookies for targeted networks.

CISA, FBI warn critical infrastructure sector of ALPHV Blackcat ransomware, data extortion incidents

WASHINGTON, DISTRICT OF COLUMBIA, UNITED STATES, April 12, 2024 /EINPresswire.com/ -- The news of Change Healthcare facing a second ransomware attack in 2024 highlights the persistent threat posed by ransomware collectives targeting organizations for sensitive data. Change Healthcare has fallen victim to another significant cyber attack just weeks after a major ransomware attack took down its systems and caused delays to prescription services across the US.

This is the company's second cyber incident of 2024. The company has had a rocky start to the year after suffering a significant breach orchestrated by notorious threat collective ALPHV/BlackCat. In response to this incident, Change Healthcare and other organizations can take proactive steps to mitigate the impact of ransomware attacks and protect against future incidents.

The stolen information includes the PII of active US service members and other patients, medical records, insurance records, payment information, and over 3,000 source code files for Change Healthcare Solutions.

Here are some key actions to consider:

Containment and Mitigation:
Immediately isolate affected systems and networks to prevent the spread of ransomware and minimize damage. Disconnect compromised devices from the network, shut down affected systems, and implement containment measures to halt further encryption or data exfiltration.

ALPHV/BlackCat Ransomware

Response and Recovery Planning:
Activate incident response teams and follow established response and recovery procedures to address the ransomware attack effectively. Engage with internal IT security personnel, external cybersecurity experts, and law enforcement agencies to coordinate response efforts and restore operations.

> “As a veteran, I, too, am concerned about the information leaked via this ransomware attack. Hiring a cybersecurity company like Axios Security Group can identify and protect against future attacks.”
>
> *Axios Security Group CEO*

Data Restoration and Backup Verification:
Prioritize data restoration efforts to recover encrypted or compromised data from secure backups. Verify the integrity and reliability of backup copies and conduct thorough testing to ensure that critical systems and data are fully restored and operational.

Communication and Transparency:
Maintain open lines of communication with stakeholders, including customers, partners, employees, and regulatory authorities, to provide timely updates and transparent information about the ransomware incident. Establish clear channels for reporting incidents and responding to inquiries from affected parties.

Enhanced Security Measures:
Implement additional security controls and measures to strengthen defenses against future ransomware attacks. This may include deploying advanced endpoint protection solutions, enhancing network segmentation, and improving user access controls to minimize the risk of unauthorized access.

Employee Training and Awareness:
Reinforce cybersecurity training and awareness programs for employees to educate them about the risks of ransomware attacks and the importance of following security best practices. Emphasize the role of employees in identifying and reporting suspicious activities or potential security threats.

Continuous Monitoring and Threat Intelligence:
Implement continuous monitoring capabilities to detect and respond to emerging threats in real time. Leverage threat intelligence sources and information-sharing partnerships to stay informed about evolving ransomware tactics, techniques, and procedures (TTPs) threat actors use. Hire a professional monitoring service such as Axios Security Group to analyze and protect against these ransomware attacks.

Axios Security Group Logo

Regulatory Compliance and Reporting:

After a ransomware attack, ensure compliance with applicable data protection regulations and reporting requirements. Notify regulatory authorities, law enforcement agencies, and affected individuals as required by law and cooperate fully with investigations.

By taking proactive measures to respond effectively to ransomware attacks and strengthen cybersecurity defenses, organizations like Change Healthcare can minimize the impact of such incidents and protect sensitive data from falling into the hands of cybercriminals. In today's digital landscape, it's essential to remain vigilant, adaptive, and resilient in the face of evolving cyber threats.

Robert Conroy
News Break
+ +1 (800) 485-3983
clientservices@axiossecuritygroup.com
Visit us on social media:
Facebook
Twitter
LinkedIn
Other