Change Healthcare Breach

C-Suite level threat review by applicable business area addressing active threats.

In late February, affiliates of the Blackcat ransomware-as-a-service (RaaS) operation successfully breached Change Healthcare, the largest clearinghouse for medical claims in the United States. The threat actors exfiltrated 6TB of sensitive data, including patient information, insurance records and financial documents. The breach led to Change Healthcare paying the ransom (~$22 million).

The Change Healthcare Breach serves as a cautionary tale for paying the ransom. The payment did not safeguard the exfiltrated data; 22 snapshots of protected patient health information were still leaked online. Moreover, a second RaaS threat actor, known as RansomHub, entered the narrative, claiming to also have the stolen data and demanding payment. Allegedly, Blackcat did not pay its affiliates their fair share of the ransom. As a result, those affiliates brought the data to RansomHub, hoping to utilize RansomHub's infrastructure to extract payment. The ransom payment also underscores the profitability of targeting healthcare systems which, as a result, will likely increase attacks on the industry. All this demonstrates that generally paying the ransom does not mitigate the adverse impacts of a breach.

Blackcat (other aliases include ALPHV):

K logix wrote about Blackcat in its January newsletter, discussing the FBI's seizure of its dark web data site. As predicted, in response, Blackcat elevated its attacks, targeting critical infrastructure systems such as oil and gas and healthcare. However, Blackcat announced it is shutting down operations and selling its ransomware source code following the Change Healthcare Breach in an apparent exit-scam to pocket the portion of the ransomware payment owed to its affiliate. These events have sowed distrust between big RaaS names and affiliates, paving the way for new RaaS actors to emerge, like RansomHub.

RansomHub:

New to the threat landscape, RansomHub has been operating a ransomware-as-a-service (RaaS) model since February 2024. This adversary recruits from Russian-language underground forums and prohibits affiliates from targeting Cuba, North Korea, China, and countries in the Commonwealth of Independent States (areas from the former Soviet Union). Its top 3 targeted industries are retail, software, and construction. RansomHub differentiates itself from other RaaS operations by allowing affiliates to directly collect ransomware payouts. This strategy is advantageous to affiliates and will likely make RansomHub a popular RaaS operation, especially in light of the alleged Blackcat scam.

Blackcat

Threat Level: Medium

Attack:

While much of the details of the Change Healthcare attack are not accessible, how the attackers gained initial access to Change Healthcare's environment has been revealed. The success of the attack hinges on a lack of multi-factor authentication (MFA). Blackcat affiliates used stolen credentials to remotely access a Change Healthcare Citrix portal. Since MFA was not enabled, the hackers were able to gain entry with just the stolen credentials. The malicious actors were in Change Healthcare's environment for nine days before deploying the ransomware.

Remediation:

- Ensure MFA is implemented across key systems such as remote access tools.
- Consider putting in place time-based and location-based conditional access policies.
- Ensure your detection tools are alerting on unusual login activity.

RansomHub

Threat Level: Medium

Attack:

RansomHub's ransomware strain is written in Golang and C++ and is capable of targeting Windows, Linux and ESXi instances. Once installed on a Windows environment, it is capable of deleting Windows volume shadow copies to prevent backup restoration and inhibit system recovery (MITRE T1047 and T1490). To further inhibit recovery, RansomHub uses the "iisreset.exe" binary to stop all the IIS services (MITRE T1489). To evade detection and inhibit post-event analysis, this ransomware strain is capable of clearing applications, systems, and security event logs (MITRE T1070.001). According to RansomHub's advertisements, it offers faster encryption than other ransomware strains on the market (MITRE T1486).

Remediation:

- Acquire an Endpoint, Detection and Response (EDR) solution that uses behavior-based analysis to distinguish between malicious activity and everyday user action.
- Aggregate logs into a SIEM to alleviate harm from a malicious actor manipulating and deleting logs locally.
- Conduct quarterly access reviews to ensure the principle of least privilege is in place. Doing so will reduce the likelihood that a malicious actor can get access to critical services and files.

Blackcat:

- **Information on the Change Healthcare Breach:** https://healthitsecurity.com/news/change-healthcare-disconnects-system-amid-cyberattack#:~:text=Witty%20also%20said%20that%20ALPHV,%2Dfactor%20authentication%20(MFA).
- **Additional analysis on the Change Healthcare Breach:** https://blog.barracuda.com/2024/04/12/change-healthcare-and-ransomhub-redefine-double-extortion

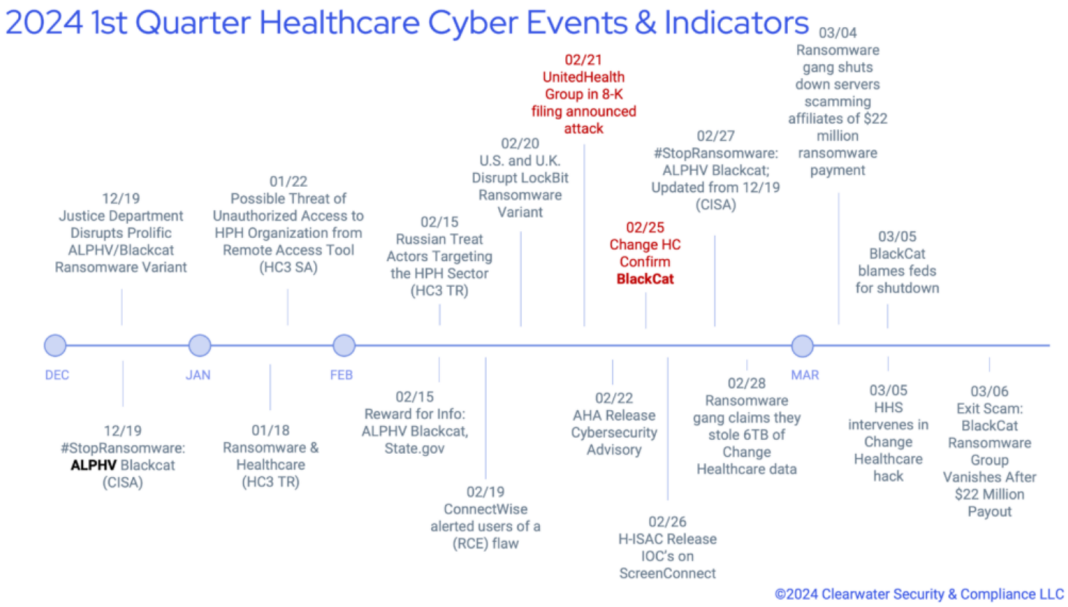
RansomHub:

- **An overview of the threat actor:** https://socradar.io/dark-web-profile-ransomhub/
- **Technical review of the ransomware:** https://community.fortinet.com/t5/FortiEDR/Threat-Coverage-How-FortiEDR-protects-against-RansomHub/ta-p/308376

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Response (EDR)
  - Identity and Access Management (IAM)
  - Managed Security Service Provider (MSSP)
  - Security Information and Event Management (SIEM)
  - Cloud Security Posture Management (CSPM)
  - SaaS Security Posture Management (SaaS)
- Programmatic Advisory
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
  - Cloud Security Maturity
  - Identity and Access Management Program Maturity
- Threat Intelligence
  - Notification to customers of threats
  - On-demand briefings
  - Threat exposure workshops
  - User awareness training seminars
  - Monthly and quarterly threat intelligence reports

Timeline of Change Healthcare Breach



Source: https://clearwatersecurity.com/blog/understanding-the-change-healthcare-breach-and-what-it-means-for-your-healthcare-organization/