**Cyber 644 Project - 1 Documentation**

**Title:** Change Healthcare Ransomware Attack

**Overview of the breach:**

* On Feb. 21, 2024, Change Healthcare publicly disclosed that it had been impacted by a cyberattack.
* BlackCat/ALPHV claimed responsibility for this attack and demanded money to return services online.
* The impact of the Change Healthcare cyberattack has been devastating for the healthcare industry and hundreds of millions of Americans who rely on services powered by victimized providers. In a [message](https://twitter.com/ddd1ms/status/1764639329165406497) posted on X (formerly Twitter) Recorded Future's product management director Dmitry Smilyanets included a transaction link and claimed that a $22 million ransom in the form of 350 [Bitcoins](https://www.techtarget.com/whatis/definition/Bitcoin) was paid on March 1

**Detailed Explanation:**

**Change Healthcare Overview:**

* [Change Healthcare](https://www.techtarget.com/searchhealthit/definition/Change-Healthcare) is a healthcare technology company that is headquartered in Nashville, Tenn., with locations across the U.S., Canada, the United Kingdom, New Zealand, Israel and Taiwan. Change Healthcare was founded in 2007 and was acquired by UnitedHealth Group (UHG) and its Optum Insight business unit in an $8 billion deal that closed in October 2022.
* The Change Healthcare platform provides several different services to healthcare providers including payment and revenue cycle management. The platform helps healthcare providers with claims processing and payments as well as integrating a system for appeals management from claimants for denied claims. The Change Healthcare Platform is one of the largest health information exchange ([HIE](https://www.techtarget.com/searchhealthit/definition/Health-information-exchange-HIE)) platforms in the U.S. The company manages 15 billion claims a year, totaling over $1.5 trillion.
* As part of the overall platform offering Change Healthcare also provides clinical decision support, with technologies to help healthcare providers to make informed decisions about treatments. Change Healthcare also has a suite of patient engagement tools such as patient portals, secure messaging and appointment scheduling that help healthcare providers connect with patients.

**Change Healthcare Attack:**

1. The cyberattack on Change Healthcare was carried out by a ransomware group known as ALPHV or BlackCat. The attack led to significant disruptions in Change Healthcare's operations.
2. Tactics have included gaining access via Microsoft's [remote desktop protocol](https://www.techtarget.com/searchenterprisedesktop/definition/Remote-Desktop-Protocol-RDP) as well as [brute-force attacks](https://www.techtarget.com/searchsecurity/definition/brute-force-cracking) against Active Directory ([AD](https://www.techtarget.com/searchwindowsserver/definition/Active-Directory)). There has also been speculation that vulnerabilities in the [ConnectWise Screen Connect](https://www.techtarget.com/searchsecurity/news/366570996/ConnectWise-ScreenConnect-flaws-under-attack-patch-now) application, which were disclosed on Feb. 19 might have potentially been involved.
3. Once inside the Change Healthcare network, the attackers deployed ransomware. Ransomware attacks are particularly damaging because they can immediately render critical systems and data unavailable, posing immediate risks to patient safety and care delivery. In the case of Change Healthcare, the attack disrupted key operations, forcing healthcare providers and pharmacies to deploy workarounds to continue providing services.
4. Change Healthcare responded to the attack by disconnecting more than 111 different services across its system to prevent further damage. The company also engaged with law enforcement and cybersecurity firms to contain and remediate the ransomware risk.

**Overview of threat actor:**

1. The BlackCat ransomware gang, also known as *ALPHV*, claimed responsibility for the attack against Change Healthcare. BlackCat/ALPHV is the same group that was allegedly [behind the attacks on Caesars Entertainment and MGM Resorts](https://www.techtarget.com/searchsecurity/news/366552775/Okta-Caesars-MGM-hacked-in-social-engineering-campaign) in September 2023.
2. BlackCat/ALPHV operates with a ransomware-as-a-service ([RaaS](https://www.techtarget.com/whatis/definition/ransomware-as-a-service-RaaS)) model. In the RaaS approach, BlackCat/ALPHV enables affiliates to attack victims with its ransomware code, who are then paid a share of any ransomware payment.
3. Law enforcement has not been standing idly by while BlackCat/ALPHV attacks organizations, though the group appears to be very resilient. In December 2023, the U.S. Department of Justice led an international law enforcement operation against the group. Yet despite that action, BlackCat/ALPHV was still able to attack Change Healthcare.
4. On March 5, 2024, the BlackCat/ALPHV leak site was taken offline in what some security experts suspect is a possible exit scam designed to cheat affiliates out of any potential payouts.

**Tactics Used by threat actor:**

1. Initial Access: ALPHV Blackcat affiliates use advanced social engineering techniques and open source research on a company to gain initial access. Actors pose as company IT and/or helpdesk staff and use phone calls or SMS messages [[T1598](https://attack.mitre.org/versions/v14/techniques/T1598/)] to obtain credentials from employees to access the target network (Techniques T1598)
2. After gaining access to a victim network, ALPHV Blackcat affiliates deploy remote access software such as AnyDesk, Mega sync, and Splashtop in preparation of data exfiltration. ALPHV Blackcat affiliates create a user account, “aadmin,” and use Kerberos token generation for domain access [[T1558](https://attack.mitre.org/versions/v14/techniques/T1558/)]. After gaining access to networks, they use legitimate remote access and tunneling tools, such as Plink and Ngrok [[S0508](https://attack.mitre.org/versions/v14/software/S0508/)]. ALPHV Blackcat affiliates claim to use Brute Ratel C4 [[S1063](https://attack.mitre.org/versions/v14/software/S1063/)] and Cobalt Strike [[S1054](https://attack.mitre.org/versions/v14/software/S0154/)] as beacons to command and control servers. ALPHV Blackcat affiliates use the open source adversary-in-the-middle attack [[T1557](https://attack.mitre.org/versions/v14/techniques/T1557/)] framework Evilginx2, which allows them to obtain multifactor authentication (MFA) credentials, login credentials, and session cookies. The actors also obtain passwords from the domain controller, local network, and deleted backup servers to move laterally throughout the network [[T1555](https://attack.mitre.org/versions/v14/techniques/T1555/)].
3. To evade detection, affiliates employ allowlisted applications such as Metasploit. Once installed on the domain controller, the logs are cleared on the exchange server. Then [Mega.nz](http://mega.nz/) or Dropbox are used to move, exfiltrate, and/or download victim data. The ransomware is then deployed, and the ransom note is embedded as a file.txt. According to public reporting, affiliates have additionally used POORTRY and STONESTOP to terminate security processes.
4. Some ALPHV Blackcat affiliates exfiltrate data after gaining access and extort victims without deploying ransomware. After exfiltrating and/or encrypting data, ALPHV Blackcat affiliates communicate with victims via TOR [S0183], Tox, email, or encrypted applications. The threat actors then delete victim data from the victim’s system.
5. ALPHV Blackcat affiliates offer to provide unsolicited cyber remediation advice as an incentive for payment, offering to provide victims with “vulnerability reports” and “security recommendations” detailing how they penetrated the system and how to prevent future re-victimization upon receipt of ransom payment.

**Indicators of Compromise:**

**A screenshot of a computer

Description automatically generated**

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated

**A screenshot of a computer

Description automatically generatedMitre Attack Tactics and Techniques:**

**Mitigation Strategies:**

1. Implementing application controls to manage and control execution of software, including allowlisting remote access programs. Application controls should prevent installation and execution of portable versions of unauthorized remote access and other software. A properly configured application allowlisting solution will block any unlisted application execution. Allowlisting is important because antivirus solutions may fail to detect the execution of malicious portable executables when the files use any combination of compression, encryption, or obfuscation. Implementing FIDO/WebAuthn authentication or Public key Infrastructure (PKI)-based MFA [[CPG 2.H](https://www.cisa.gov/resources-tools/resources/cpg-report)][[HPH CPG – Multifactor Authentication](https://hphcyber.hhs.gov/performance-goals.html)]. These MFA implementations are resistant to phishing and not susceptible to push bombing or SIM swap attacks, which are techniques known be used by ALPHV Blackcat affiliates.
2. Implementing FIDO/WebAuthn authentication or Public key Infrastructure (PKI)-based MFA [CPG 2.H][HPH CPG – Multifactor Authentication]. These MFA implementations are resistant to phishing and not susceptible to push bombing or SIM swap attacks, which are techniques known be used by ALPHV Blackcat affiliates. See CISA’s Fact Sheet Implementing Phishing-Resistant MFA for more information.
3. Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool. To aid in detecting ransomware, implement a tool that logs and reports all network traffic [CPG 5.1][HPH CPG – Detect and Respond to Relevant Threats and Tactics, Techniques and Procedures], including lateral movement activity on a network. Endpoint detection and response (EDR) tools are useful for detecting lateral connections as they have insight into common and uncommon network connections for each host. Implement user training on social engineering and phishing attacks.
4. Implement internal mail and messaging monitoring. Monitoring internal mail and messaging traffic to identify suspicious activity is essential as users may be phished from outside the targeted network or without the knowledge of the organizational security team. Establish a baseline of normal network traffic and scrutinize any deviations. Install and maintain antivirus software.
5. Implement free security tools to prevent cyber threat actors from redirecting users to malicious websites to steal their credentials. For more information see, CISA’s Free Cybersecurity Services and Tools webpage.
6. Install and maintain antivirus software. Antivirus software recognizes malware and protects your computer against it. Installing antivirus software from a reputable vendor is an important step in preventing and detecting infections. Always visit vendor sites directly rather than clicking on advertisements or email links. Because attackers are continually creating new viruses and other forms of malicious code, it is important to keep your antivirus software up to date.