MACRO PRAXIS | Research Institute

Turn Back Time (TBT) – Breach Analysis

CHANGE HEALTHCARE BREACH

ANALYSIS AUTHOR: Bobby Boughton, MacroPraxis Research Institute Fellow

PUBLICATION DATE: November 4th 2024

BREACH: CHANGE HEALTHCARE RANSOMWARE ATTACK – 2024

MITRE ATT&CK FRAMEWORK													
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
			Potential Deception Discovery										Actual Breach Discovery

Breach Information:	
Breach Date:	**2024**
Breach Name:	**Change Healthcare Ransomware Attack (United Healthcare)**
Target Name:	Change Healthcare
Attacker Name:	BlackCat / ALPHV ransomware group
Type of Attack:	Ransomware
Attack Dwell Time:	Undetected for 9 days
Impact of Attack (1):	UHG's CEO, Andrew Witty, disclosed that a ransom payment of **$22 million** in Bitcoin was made to the BlackCat/ALPHV ransomware group responsible for the attack.
Impact of Attack (2):	**Direct Response Costs:** Approximately **$1.7 billion** was allocated for direct response efforts in the first nine months of 2024.
Impact of Attack (3):	**Business Disruption:** The attack led to about **$747 million** in business disruption costs over the same period, encompassing revenue losses and expenses to maintain operational readiness.
Total Impact:	UHG, the parent company of Change Healthcare, reported an estimated **total financial impact of $2.87 billion** for the fiscal year ending December 31, 2024. This figure includes direct response costs and business disruptions.

#	Tactics for MITRE ATT&CK:	Attack Tactics Description:	Security FAILURE:	Deception TECH:
1	Reconnaissance	While it's common for attackers to conduct reconnaissance to identify vulnerabilities and plan their attacks, specific details about any	No direct failure	**Decoys & Baits -** Decoy systems and fake vulnerabilities could have misled

		advance reconnaissance activities in this incident have not been publicly disclosed.		attackers, alerting security teams before real access was attempted.
2	Resource Development	BlackCat / ALPHV developed or acquired tools and infrastructure necessary for the attack, including the zero-day vulnerability in ConnectWise ScreenConnect (CVE-2024-1709), the ransomware payloads and command-and-control servers.	No direct failure	
3	Initial Access	**Technique:** Critical Vulnerability **Description:** The BlackCat / ALPHV group exploited a critical zero day vulnerability in ConnectWise ScreenConnect, specifically CVE-2024-1709. This authentication bypass flaw allowed the attackers to gain unauthorized access to systems running ScreenConnect.	Exposure to Zero-days	
4	Execution	**Technique:** Command and Scripting Interpreter **Description:** Though not publicly disclosed, post-infiltration, the attackers executed malicious scripts and commands to establish control over the compromised systems.	EDR / SIEM	**Baits -** Ransomware canaries and baits (files that trigger alerts upon modification) could have detected encryption activities early.
5	Persistence	**Technique:** Create Accounts **Description:** To maintain access, new user accounts with elevated privileges were created, ensuring continued presence even if initial access points were secured.	IAM / PAM / SIEM	**Honeytoken accounts** (decoy accounts) could have alerted security teams upon unauthorized use.
6	Privilege Escalation	**Technique:** Exploitation for Privilege Escalation **Description:** The attackers exploited system vulnerabilities to gain higher-level permissions, facilitating broader control over the network most liking using the following: 1) Access Token Manipulation: The attackers manipulated access tokens to gain elevated system privileges. By adjusting access tokens, they acquired extensive system rights, enabling system-wide modifications and access to protected resources. This manipulation is crucial for comprehensive encryption and system control, and 2) Utilization of Valid Accounts: The attackers leveraged stolen	IAM / PAM	**Decoy administrative credentials** could have detected unauthorized privilege escalation attempts.

		credentials to authenticate across the network. Storing configuration data in a decrypted JSON format at runtime, the malware contained credentials specific to the victim's environment. These credentials facilitated authentication to network shares and further system compromise.		
7	Defense Evasion	**Technique:** Obfuscated Files or Information **Description:** Techniques such as encrypting payloads and deleting logs were employed to avoid detection by security systems. It has not been disclosed whether or not the attackers disabled the endpoint security tools as a method to avoid detection.	EDR / SIEM	Decoy EDR & SIEM Services
8	Credential Access	**Technique:** Credential Dumping **Description:** Tools were used to extract additional user credentials from compromised systems, enabling further access. It has not been disclosed the exact tools used to harvest user credentials (i.e. keylogging or credential dumping).	IAM / EDR / SIEM	**Honey Tokens & Honey Token Accounts -** Planting fake credentials in accessible locations could have led attackers to reveal themselves when attempting to use them.
9	Discovery	**Technique:** System Network Configuration Discovery **Description:** Attackers mapped the network to identify critical systems and data repositories, most likely using 1) Living off the Land Binaries (LOLBins) or 2) the pen testing tool Cobalt Strike.	EDR / SIEM	**Baits, Breadcrumbs & Decoys -** Deploying decoy systems and services could have diverted attackers away from real assets and triggered alerts upon interaction.
10	Lateral Movement	**Technique:** Remote Services **Description:** Utilizing the harvested credentials, attackers moved laterally across the network to access and compromise additional systems.	IDS / SIEM / Segmentation	**Decoys & Fake RDP Sessions -** Moving within the network to access additional systems and data.
11	Collection	**Technique:** Data from Information Repositories **Description:** Sensitive data, including patient records and financial information, was gathered from various systems.	IAM / MDR / SIEM	**Baits, Breadcrumbs & Decoy Databases** and Fake High Value Data

12	Command & Control	**Technique:** Application Layer Protocol **Description:** Established encrypted channels to communicate with external command and control servers, facilitating data exfiltration and remote commands.	IAM / IR	**Fake C2 Server Decoys & Deceptive Authentication Responses -** Monitoring for connections to known malicious domains and using decoy C2 servers could have identified and disrupted attacker communications.
13	Exfiltration	**Technique:** Exfiltration Over C2 Channel **Description:** Collected data was transmitted out of the network through the established command and control channels.	IDS / SIEM / IR	Fake High-Value **Baits** could have slowed down or stopped data theft.
14	Impact	**Technique:** Data Encrypted for Impact **Description:** Finally, the BlackCat/ALPHV group deployed their proprietary ransomware, known as BlackCat or ALPHV, to encrypt data within the compromised systems. This ransomware is notable for being written in the Rust programming language, which enhances its performance and cross-platform capabilities. The ransomware disrupted services, causing widespread outages across the healthcare industry, which was used to coerce Change Healthcare into paying a ransom.	EDR / SIEM	**Ransomware Baits (fake encrypted files) -** could have helped contain the attack sooner.

Key Takeaways:

1. **Change Healthcare detected the attack way too late (Stage 14 – Impact), by which time attackers had already compromised critical systems and removed sensitive data.**
2. **Deception technology could have detected the attack as early as Stage 4 – Execution.** If Change Healthcare had deployed **baits at this stage**, attackers might have triggered alerts at this early stage of the attack, allowing for proactive containment.
3. **Earlier detection could have significantly reduced the financial impact.** Had the attack been identified at **Stage 4 instead of Stage 14**, it could have prevented or minimized the **$2.87 billion+ in damages**.

4. **Deception technology should be part of a layered security strategy, providing an early-warning system to detect and divert attackers before they cause major damage.**

Disclaimer:

The **Turn Back Time (TBT) Analysis** is a hypothetical evaluation based on publicly available breach information and industry best practices. It illustrates how deception technology could have **improved early detection and response capabilities**. However, **no cybersecurity solution can guarantee complete prevention of cyber threats**.

Deception technology is **one component of a multi-layered security strategy**, and its effectiveness depends on **deployment scope, integration with existing security tools, and evolving attack techniques**. This analysis is **for informational purposes only** and should not be interpreted as a **guarantee of breach prevention**.

The MACROPRAXIS Research Institute is **not liable for any cybersecurity incidents, financial losses, or damages** resulting from the use or implementation of deception technology. Customers are advised to conduct **independent security assessments** and integrate deception tools as part of a **comprehensive cybersecurity strategy**.