2024 Ascension Health Ransomware Attack Threat Intelligence Report

On May 8, 2024, unusual activity was detected within Ascension Health's systems. The following day, it was confirmed that Black Basta, a known ransomware-as-a-service (RaaS) group, had launched a targeted attack. The incident resulted in the shutdown of all 142 facilities for approximately 6 weeks, cutting off access to electronic health records, phone systems, and prescription services, which severely disrupted operations and patient care across the network. The attack caused one of the largest healthcare data breaches to date, exposing the protected health information (PHI) and personally identifiable information (PII) of approximately 5.6 million patients. The financial cost of the attack is unknown, along with whether the ransom was paid or not, but Ascension did end its fiscal year with ~$1.8 bn in losses [1].

Responsible for this disruption was Black Basta, a ransomware group first observed in 2022 that operates under a RaaS model and has consistently focused on critical infrastructure, including the healthcare sector [2]. Its affiliates are financially motivated, and the choice of target reflects a calculated decision to exploit the healthcare industry's reliance on outdated systems, the critical nature of care delivery, and the high sensitivity of patient data. These conditions heighten the chances of ransom payments, making healthcare a strategically attractive target [3]. This was evident in the methods used during the Ascension attack.

Initial access in this case was achieved through spearphishing voice attacks, in which victims were socially engineered into downloading remote access tools such as AnyDesk [4]. This technique was supplemented by Qakbot, a malware strain often used to establish a foothold in the system. Once access was obtained, Black Basta affiliates conducted internal network scans and used masquerading techniques to hide malicious utilities by disguising them as legitimate files in the root drive [5]. Privilege escalation was then performed using Mimikatz to extract credentials, followed by lateral movement via PsExec and BITSAdmin, allowing attackers to traverse the environment with elevated access. In order to avoid detection, PowerShell scripts were used to disable antivirus and endpoint detection tools [6]. This cleared the way for the exfiltration of data using RClone, a command-line utility capable of syncing with cloud storage services. Finally, files were encrypted using the ChaCha20 algorithm, effectively paralyzing digital operations. [7]

Given Black Basta's reliance on widely available tools, credential theft, and social engineering tactics that can bypass standard defenses, the probability of a similar threat actor exploiting a vulnerable organization remains high across all sectors lacking mature cyber hygiene. So, the recommended actions to mitigate the chances of similar attacks include more robust employee phishing training, mandated MFA on all access points and for remote access, network segmentation to limit lateral movement, secure and comprehensive backups to lower down time, and implementing incident response and continuity plans.

References

[1] S. Alder, “Ascension Ransomware Attack: Initial Access Vector and Data Theft Confirmed,” *The HIPAA Journal*, Dec. 20, 2024. https://www.hipaajournal.com/ascension-cyberattack-2024/ (accessed Jul. 20, 2025).
[2] CISA, “#StopRansomware: Black Basta | CISA,” *www.cisa.gov*, May 10, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a (accessed Jul. 20, 2025).
[3] D. Narayanan, “Ascension Health Ransomware Attack Impact, Lessons, and How to Strengthen Cybersecurity,” *VComply*, Mar. 18, 2025. https://www.v-comply.com/blog/ascensiorn-cyber-attack/ (accessed Jul. 20, 2025).
[4] MITRE ATT&CK, “Phishing: Spearphishing Voice, Sub-technique T1566.004 - Enterprise | MITRE ATT&CK®,” *attack.mitre.org*, Sep. 07, 2023. https://attack.mitre.org/techniques/T1566/004/ (accessed Jul. 21, 2025).
[5] MITRE ATT&CK, “Masquerading, Technique T1036 - Enterprise | MITRE ATT&CK®,” *Mitre.org*, 2024. https://attack.mitre.org/versions/v15/techniques/T1036/ (accessed Jul. 21, 2025).
[6] MITRE ATT&CK, “Command and Scripting Interpreter: PowerShell, Sub-technique T1059.001 - Enterprise | MITRE ATT&CK®,” *attack.mitre.org*, Mar. 09, 2020. https://attack.mitre.org/techniques/T1059/001/ (accessed Jul. 21, 2025).
[7] MITRE ATT&CK, “Data Encrypted for Impact, Technique T1486 - Enterprise | MITRE ATT&CK®,” *attack.mitre.org*, Mar. 15, 2019. https://attack.mitre.org/techniques/T1486/ (accessed Jul. 21, 2025).