Blaine Gernandizo

Professor Bowman

CYSE 200T

14 November 2025

Exploring Attacks on Availability: Ransomware

Ransomware attacks represent one of the most severe threats to modern organizations. Ransomware is considered an "attack on availability" as its primary objective is to disrupt, block, or deny legitimate access to data, applications, or systems. According to the Sophos State of Ransomware 2024 survey of 5,000 IT and cybersecurity leaders released in April, 59% of organizations were hit by a ransomware attack in 2023 (Fruhlinger, 2025). These attacks typically begin with an initial intrusion, often achieved through phishing emails containing malicious attachments, exploitation of unpatched software vulnerabilities, or the use of compromised user credentials. Once inside a network, the malware establishes a foothold, disables security software, and spreads laterally to locate and encrypt critical data which includes files, databases, and backups. The final stage is the ransom demand, where attackers extort payment in cryptocurrency in exchange for the decryption key. The 2021 Colonial Pipeline ransomware attack is a prime example of this. A criminal group, DarkSide, used a compromised VPN password to infiltrate the company's corporate IT network. They then deployed ransomware that encrypted critical business data, rendering systems that managed logistics, communications, and billing inaccessible. Fearing the malware could spread to the operational technology controlling the physical pipeline, Colonial Pipeline proactively shut down the entire system. This turned a digital encryption event into a severe physical availability crisis, halting the flow of nearly half the US East Coast's fuel supply for six days, which then triggered a widespread panic buying and fuel shortages. Implementing strict network segmentation between corporate and operation technology (OT) systems could have contained the infection, potentially preventing the need for a full shutdown. Furthermore, maintaining frequent, isolated, and tested backups would have provided a recovery path without negotiating with attackers.

References

Fruhlinger, J., & Muse, D. (2025, May). *Ransomware explained: How it works and how to remove it*. CSO Online. https://www.csoonline.com/article/563507/what-is-ransomware-how-it-works-and-how-to-remove-it.html

Analyst, C. G. (2024, November 21). Executive Summary: COLONIAL PIPELINE RANSOMWARE ATTACK. *CTG*. https://www.counterterrorismgroup.com/post/executive-summary-colonial-pipeline-ransomware-attack