John Heath

November 11, 2025

Exploring Attacks on Availability

An “attack on availability” is a deliberate attempt to make information systems or data unavailable via a cyber attack, leading authorized users to be unable to access information, systems, or networks. A specific type of attack on availability is ransomware, a type of malware that encrypts data/information, which denies authorized users access to it. Ransomware attacks require a source of infection such as phishing, infected websites, or fake hard drives with predownloaded ransomware. Once infected, the ransomware locks authorized users out and demands a ransom for the organization/individual to regain access to their data.

In 2018, a Russian group called Wizard Spider attacked the Universal Health Systems hospital chain in the United States. The group targeted the hospitals with phishing e-mails, which effected ~ 400 hospitals. $67 million dollars were lost due to the attack, as well as putting millions of patients at risk of identity theft/fraud.

Ransomware has a tremendous impact on its victims. Organizations effected by it often have their reputations ruined, as they can no longer be trusted to secure data. Additionally, they lose customers because of their unreliable cybersecurity. Ransomware, if paid - which is ill advised, also comes at a hefty monetary cost, along with the costs of losing customers.

Ransomware can be defended against by utilizing employee training, frequent backups, and incident response planning. By preparing for potential conflict, organizations or individuals can heavily mitigate the risk of falling victim to a ransomware attack.