Write Up: Exploring Attacks on Availability

Devin Matkozich

Old Dominion University

CYSE200T

Professor Christopher Bowman

November 16th, 2025

Introduction

An attack on availability is a cyberattack where the goal is to block access to systems, networks or data so users are not able to access them. Availability is a core principle in cybersecurity, so when it is compromised, organizations can have serious operation and financial repercussions. Some examples of what these attacks do is they overwhelm systems with traffic and encrypt data so they cannot be accessed. With an expanding use of technology, the number of attacks has also risen. Looking at recent examples of attacks, organizations can break down how they happen, how much damage they cause, and how to defend against them.

Distributed Denial of Service (DDOS)

One recent attack on availability, which ended up breaking a record by peaking at 22 tbps and 10 bpps, was a directed attack DDoS attack on European network infrastructure company. The attackers “flooded the target with traffic at a scale never seen before, overwhelming all standard defenses.”. (Kovacs, 2025) How this attack works is by sending huge amounts of data and requests to a network until it slows down and eventually stops responding. In this specific attack, they send a very large amount of traffic which disrupted access to their online services. This forced them to divert traffic through a backup system. To defend against attacks like these, companies can use tools like traffic filtering and load balancing which can help absorb or block malicious traffic before it shuts down a system.

Ransomware

Another big attack which happened recently was against the state of Nevada. It was reported that the attack happened because an employee downloaded malware, and then “the infection quickly spread through state systems, encrypting files and shutting down public services.” (Jones, 2025) Once the files were encrypted, the government was locked out of important systems, which prevented anyone from using their services. Ransomware attacks availability by locking users out of their own data and then gives the victim an ultimatum: pay them to decrypt it or lose all access. This can be very hard for organizations that rely on these systems since losing access, even for a short time, can lead to huge consequences. The ability of employees to recognize suspicious downloads and keep backups is required as a defense against ransomware attacks so they can restore their systems without paying any ransoms.

Conclusion

Since availability attacks can stop critical systems and services, they pose a very serious threat. Both ransomware and DDoS attacks have both demonstrated how quickly important systems can be disrupted and data can be lost. Anybody who depends on an organization's services may experience significant issues and massive financial losses if they lose access to the systems they depend on. Organizations must therefore train staff and have dependable backups to strengthen their defenses. As a result, organizations will be ready for attacks and can react quickly to stop or reduce any losses.

References

Kovacs, E. (2025, September 24). *Record-breaking ddos attack peaks at 22 tbps and 10 BPPS - SecurityWeek*. SecurityWeek. https://www.securityweek.com/record-breaking-ddos-attack-peaks-at-22-tbps-and-10-bpps/

Jones, D. (2025, November 7). *Nevada ransomware attack traced back to malware download by employee*. Cybersecurity Dive. https://www.cybersecuritydive.com/news/nevada-ransomware-attack-traced-back-to-malware-download-by-employee/805011/?utm_source=chatgpt.com