Securing a Popular Online Gaming Server

Problem

A popular online gaming host experienced decreased bandwidth and game quality due to malicious attempts to access the server

Solution

We tested the server for vulnerabilities, then worked with our client to mitigate potential risks and harden the server against future attacks

Results

Increased bandwidth by 40%, mitigated brute-forcing attempts and installed systems to monitor and prevent intrusion attempts

Overview

A popular massive multiplayer online gaming host was experiencing frequent unauthorized SSH and FTP access attempts to their server. These attempts appeared to be part of an orchestrated attempt to gain administrative access to the server to harvest user credentials, personal and financial data. Although these attacks were conspicuous, they were also persistent and used up much of the server's bandwidth, decreasing game quality, player satisfaction and threatening sensitive data.

Challenges

Alacer Group performed a comprehensive vulnerability audit to get a bird's eye view of the situation and test for misconfigurations and security holes. The audits found several unused yet open ports, including those generally used by SSH and FTP protocols. We advised the system administrator to close these unused ports. An intrusion detection system (IDS) was installed on the server, allowing the administrator to view any abnormal activity and to provide automatic alerts if unauthorized or suspicious activity was noticed.

Results

Closing the ports effectively blocked the brute-force hacking attempts by 100% — the targeted ports were no longer an option. Eliminating the malicious traffic gave players better server uptime through 40% increase in bandwidth and a dramatically increased quality of experience. Our solution gave the client's system administrator peace of mind knowing two wide-open attack avenues were closed, sensitive data was protected and the new, very perceptive intrusion detection system will warn of malicious attacks in the future.