AWS re:Start

LAB

# Malware Protection

Malware, short for malicious software, refers to any intrusive software developed by cybercriminals to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan horses, spyware, adware, and ransomware.

Firewalls are like physical security walls situated between an organization's internal network and any external public networks such as the internet. The firewall protects an internal network from access by unauthorized users on an external network.

Users need access to the internet for business reasons, but they can inadvertently download malware, which can impact network and data security.

Malware threats can be present, and organizations can use various techniques and services to mitigate these threats. This lab focuses on countermeasure techniques using a firewall.

In this scenario, a company has hired you as a new security engineer, and the company has tasked you with hardening the company’s security perimeter. There have been reports of users accidentally downloading malware after accessing specific websites. The IT team has provided you with the URLs of the sites hosting the malware. It is your job to find a solution to mitigate access to these malicious actor files.

aws re/start