CYBER THREATS GLOSSARY

Axcient

An at-a-glance guide to some of the most common threats to your data

ADVANCED PERSISTENT THREAT (APT)

Cybercriminals typically use an advanced persistent attack to target larger organizations with the objective of soliciting financial information. This type of attack is executed over a long period of time and is difficult to detect.

BACKDOOR TROJAN

A backdoor Trojan allows cybercriminals to take control of a system without permission. Posing as a legitimate program, a Trojan spreads though phishing campaigns which fool users into accessing malware through everyday activities such as clicking links.

DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)

A DDoS attack is meant to prevent users from accessing specific locations online. In this attack, a cybercriminal will flood a website with large quantities of information requests which essentially renders the site inaccessible to legitimate users.

FLOODING

In this security attack, hackers will send a large amount of information to a server or web location. The result is a break in the system's proper operation due to a block in its processing power.

DID YOU KNOW?

20%

of all security incidents are caused by malware[2]

Changing employee behavior can reduce security breach risk by

25%

BE AWARE. BE CYBERSECURE.

RANSOMWARE

A type of malicious software, Ransomware encrypts all of the data on a PC desktop or mobile device which blocks access by the data's owner. Aptly named, Ransomware requires a ransom be paid, typically in Bitcoins, to the attacker in order to regain access to the files.

SOCIAL ENGINEERING

Social engineering uses psychological manipulation to persuade users to perform specific actions or reveal sensitive information. Lies, bribes, extortion and impersonation are often used in this type of attack.

SQL INJECTION

SQL Injection is an attack wherein an attacker uses malicious SQL code, often moving all data into a central location controlled by the attacker. By doing this attackers can impersonate identities, modify or delete data, or completely take control of an entire database.

WORM

One of the most common types of malware, a worm is an infection that has the ability to spread indefinitely and self-replicate. By exploiting OS vulnerabilities, this replication happens automatically and does not need human activity in order to spread.

CONTACT: Axcient, 707 17th Street, Suite 3900, Denver, CO, 80202 Tel: 720-204-4500 | axcient.com