The Best Defense is a Good Offense:

Is Your Cybersecurity Team Ready to Win?

Business Email Compromise (BEC) attacks are a growing concern, and new "talent" is always being drafted to get a win. These attackers are becoming more sophisticated and regularly update their playbook with new ways to try and sneak past the good guys. Their starting lineup is skilled, patient, and strategic.

Meet the Starting Lineup: The Attackers

ATTACKERS

Open-Source Intelligence (OSINT) and Reconnaissance

Gathering personal information on a target through basic Internet searches, website scraping, and social media outlets

#11

ATTACKERS

Social Engineering

Using deception, manipulation, and information collected through OSINT to get targets to divulge sensitive or confidential information

#14

ATTACKERS

Phishing

Disguising malicious emails in a mask of familiarity to obtain user credentials, infect a device with malware, or gain a point of entry into an entire network

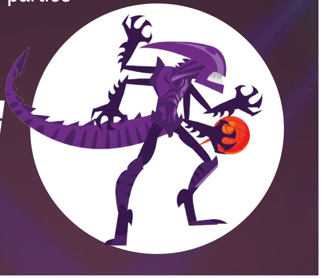
#22

ATTACKERS

Man-in-the-Email

Patiently watching communications between two parties to understand workflows and policies to later exploit them to acquire sensitive data or money; hijacking an email conversation and altering the conversations between two parties

#36

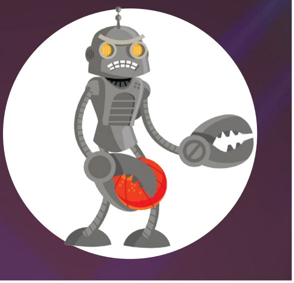


ATTACKERS

Credential Theft

Purchasing stolen credentials on the Dark Web or using brute force to guess weak passwords

#09



DATAPRISE

The matchup between cyber attackers and prevention is always a close game. Just when attackers update their techniques, we swoop in to stop the score using the latest technologies. Our starting lineup is always learning, adapting, and strengthening to combat our opponent.

Meet the Starting Lineup: The Defenders

DEFENDERS

Dark Web Credential Monitoring

Scours the Dark Web for your credentials and alerts you if it detects any of your information, allowing you to mitigate threats before attackers can compromise your system

DEFENDERS

Multi-Factor Authentication

Provides an additional layer of security when accessing company systems by requiring two or more proofs of identification

DEFENDERS

Employee Training

Educates your staff on malicious social engineering tactics so they know how to identify and react to suspicious online behavior

DEFENDERS

24x7 Security Monitoring

Identifies anomalies in your network and alerts trained security analysts so they can isolate and eliminate attacks quickly

DEFENDERS

Mindfulness

Ensures you are always aware of what information you make public through social media; any piece of personal information, regardless of how small, has some value to a cyber criminal

SECURITY BEST PRACTICES

Close security gaps in your environment that attackers could otherwise exploit. Some of these best practices include:

- A centralized patch management system to automatically apply operating system and application patches
- Written security policies to govern organizational behavior regarding cyber security
- An incident response plan to clearly define the appropriate steps to take during a security event

With strong cybersecurity defenses, your organization can thwart attackers and protect its employees, data, and reputation. To draft new players for your starting lineup and learn more about IT security services, visit our website.

DATAPRISE