SOLUTION BRIEF

proofpoint.

PROTECTING AGAINST BUSINESS EMAIL COMPROMISE AND EMAIL ACCOUNT COMPROMISE

BLOCK ATTACKS WITH A LAYERED SOLUTION THAT PROTECTS YOU FROM BEC AND EAC

According to the FBI, business email compromise (BEC) and email account compromise (EAC) have cost businesses more than $26 billion globally between June 2016 and July 2019. The scale of these losses shows that threat actors are switching tactics in how they attack the people who work at the organizations they target. Attackers are using convincing phishing techniques to steal credentials, money, and sensitive documents such as tax or HR information.

It's not easy to stop these complex threats, which use many different channels and techniques. Only a layered approach can be truly effective. Gaps in protection can result in significant losses. And these can be greater than the cost of the protection you implement.

METHODS OF ATTACK

Phishing attacks use identity deception to trick victims. Cyber criminals spoof an identity (BEC) or steal a valid identity (EAC). These threats use email as the main threat vector. But you also need to consider other communication channels. This will help you minimize the potential impact of such attacks.

BUSINESS EMAIL COMPROMISE

To accurately detect BEC, a security solution must integrate controls across the gateway, authentication, and visibility. Automated remediation is also critical to minimize exposure. And security awareness training will help your people identify and report suspicious email.

Threat actors use many different techniques to carry out BEC attacks:

- Domain spoofing
- Display name spoofing
- Look-alike domain spoofing

An effective solution should detect all these techniques. And it should prevent threats from entering your organization.

Attackers can also use your own domains to send messages out to customers and business partners in order to steal money or impact your brand in a negative way. A comprehensive solution needs to have visibility to these threats as well.

ACCOUNT COMPROMISE AND CREDENTIAL THEFT

Another attack the FBI points to is attempted account compromise or credential theft. This can impact your organization in many ways because it allows threat actors to operate in spite of any security controls you have in place. That's why you need to:

- Prevent your people from sharing their credentials on phishing sites
- Identify attempted account compromise across email and cloud applications
- Detect suspicious activity from potentially compromised accounts
- Remove the symptoms of compromised accounts, such as spreading malware and lateral movement
- Remediate compromised accounts through password resets or requiring reauthentication

OTHER THINGS TO CONSIDER

Preventing threats is the top goal of any security solution designed to stop BEC and EAC. It should also provide visibility into who is being attacked. After your Very Attacked People (VAPs) have been identified, you can put in place appropriate adaptive controls. For example, you can enroll users who are at high risk of attack in security awareness training that is directly related to the attacks they are experiencing. This can help decrease the likelihood of a successful attack. Effective training can transform your users into your last line of defense.

How to Effectively Block BEC and EAC Attacks	
Gateway	Block attacks that use spoofed domains
	Tag external email to inform recipients of the origin of the email
	Analyze message headers to identify anomalies
	Analyze all email content with machine learning
	Identify and block display name spoofing
	Enforce email authentication policy
Authentication	Create a global email authentication policy (DMARC) and enforce it on an internet-wide basis
	Block all attempts to send unauthorized emails from your trusted domains
	Report on look-alike domain registrations
Cloud Applications	Identify suspicious cloud account activity
	Detect brute-force attacks
	Build policies to prioritize alerts
Web Access	Isolate access to unknown websites
	Provide read-only access until security analysis is complete
	Control content entering your organization through personal webmail accounts
Visibility	Identify the VAPs in your organization
	View the authentication status of your supply chain
	Provide user-centric visibility into account attacks

How to Effectively Block BEC and EAC Attacks	
Automated Remediation	Identify and remove suspicious emails that have entered the organization
	Remove unwanted email from internal accounts that are compromised
	Force password resets and disable accounts that are compromised
	Use an account authentication solution to reauthenticate sessions
	Investigate account compromise incidents
Education	Assess user vulnerability to BEC and EAC threats
	Train users on how to identify threats and credential theft
	Automate abuse mailbox process

THE PROOFPOINT DIFFERENCE

Proofpoint offers multiple ways to protect you from both BEC and EAC attacks across email and cloud applications. We focus on all areas of concern to help you minimize the potential loss from this costly threat.

LEARN MORE

For more information, visit www.proofpoint.com.