Mimecast Targeted Threat Protection

Impersonation Protect

Instant and comprehensive protection from the latest malware-less social engineering-based email attacks, often called CEO fraud, impersonation, whaling or business email compromise.

Not all email based attacks use malicious URLs or attachments. Business email compromise attacks are designed to trick key users, often in finance, into making wire transfers or other transactions to cyber-criminals by pretending to be the CEO or CFO. Some also target those responsible for sensitive employee data, for example payroll information, which could be used for identity theft. Attackers also pose as supply chain partners or well-known internet brands in an attempt to exploit the relationship or trust of external organizations.

Targeted Threat Protection - Impersonation Protect detects and prevents these types of attacks. Impersonation Protect identifies combinations of key indicators in an email to determine if the content is suspicious, even in the absence of a malicious URL or attachment.

HOW IT WORKS

- As email passes through the Mimecast Secure Email Gateway, Impersonation Protect examines several key aspects of the message.
- Impersonation Protect examines the email's display name, domain name, recency of email from that domain, reply-to information, and the body of the message to determine if the email could be an impersonation attack.
- If the email fails a combination of these tests, administrators can configure Impersonation Protect to discard the message, quarantine it, or warn the receiver that the email is suspicious.

PROTECT EMPLOYEES FROM THE NEW BREED OF EMAIL CYBERATTACKS

According to the U.S. Federal Bureau of Investigation (FBI), since it's Internet Crime Complaint Center (IC3) was established in May 2000, there have been over 4 million complaints of Business Email Compromise with total losses exceeding $5.5 Billion. Cybercriminals are becoming ever more inventive and creative when it comes to compromising organizations.

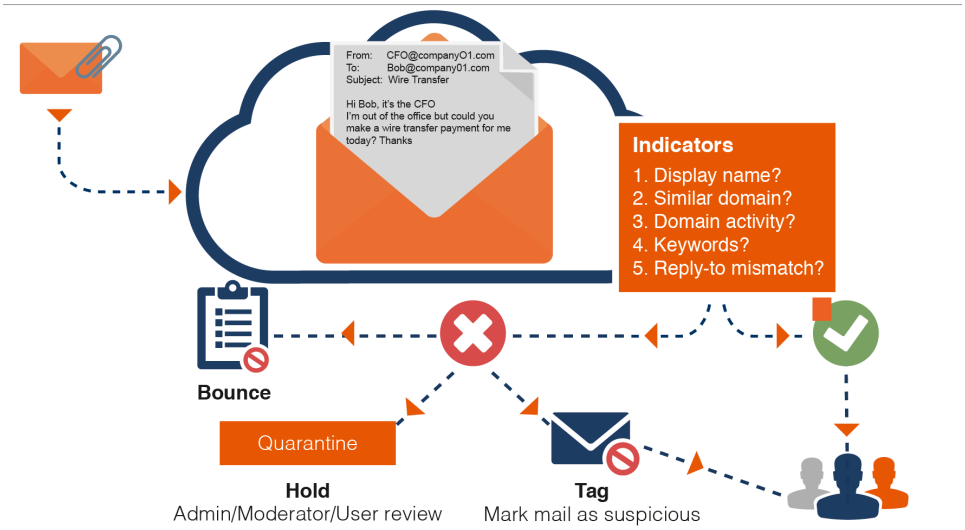
KEY CAPABILITIES:

- Real-time protection against malware-less social engineering attacks like whaling, CEO fraud, business email compromise, impersonation or W-2 fraud.
- Protects against newly observed and newly registered domains used as part of the attack.
- Scans for popular internet domain brand impersonation while Administrators control their own domain list of organizations they work with to monitor for typo-squatting abuse.
- Includes a Targeted Threat Dictionary managed by Mimecast to which custom terms can be added by the customers' administrators.
- Ensures end users are protected by visibly marking suspicious emails.
- Backed by comprehensive protection from Mimecast's threat intelligence infrastructure and the Mimecast Security Operations Center.
- Complete administrative control over handling of emails; quarantine, block or mark emails depending on your organization's preferences.
- Works alongside URL Protect, Attachment Protect, and Internal Email Protect to provide comprehensive protection against the latest attack methods.

The attacks seek to fraudulently trick employees into sending wire transfers, or other sensitive data transfers, to the cybercriminals as a way of generating income for organized crime.

With Mimecast Targeted Threat Protection - Impersonation Protect, organizations can protect their employees, intellectual property, and financial assets from this type of fraud.

Impersonation Protect provides instant and comprehensive protection against this latest type of email-borne cyberattack which are often malware-less and based heavily on social engineering, thereby able to pass through traditional gateway checks.



KEY INDICATORS OF THREAT

Impersonation Protect examines a number of indicators in email such as:

- Display name analysis to determine if the attacker is trying to spoof an internal sender.
- Reply-to mismatch to determine if the sender is trying to hide their true sending email address.
- The sending domain name; to detect if it is similar to your existing corporate domains, well known internet brands, and supply-chain partners of the organization.
- The recency of the sending domain name; newly observed domains are more likely to be malicious.
- Keywords in the message body; attackers will use phrases like 'wire transfer', 'bank transfer' or 'W-2' in this type of attack. Organizations can also enter their own key words into the threat dictionary.
- Impersonation Protect blocks, quarantines or tags the email as suspicious ensuring employees are not tricked into making fraudulent wire-transfers or giving out sensitive data.

ADDITIONAL PROTECTION FROM MALICIOUS URLS AND WEAPONIZED ATTACHMENTS

Impersonation Protect works with URL Protect, Attachment Protect, and Internal Email Protect for comprehensive protection against advanced email-borne threats.