mimecast®

DATASHEET

Mimecast Targeted Threat Protection

Impersonation Protect

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

Not all email based attacks use malicious URLs or weaponized attachments, and are increasingly sophisticated and convincing in their efforts to use social engineering tactics against users. Whaling attacks, business email compromise or CEO fraud are designed to trick key users, often in the finance team, into making wire transfers or other financial transactions to cyber-criminals by pretending to be the CEO or CFO in a spoofed email. Some also target those responsible for sensitive employee data, for example payroll information, which could be used for identity theft.

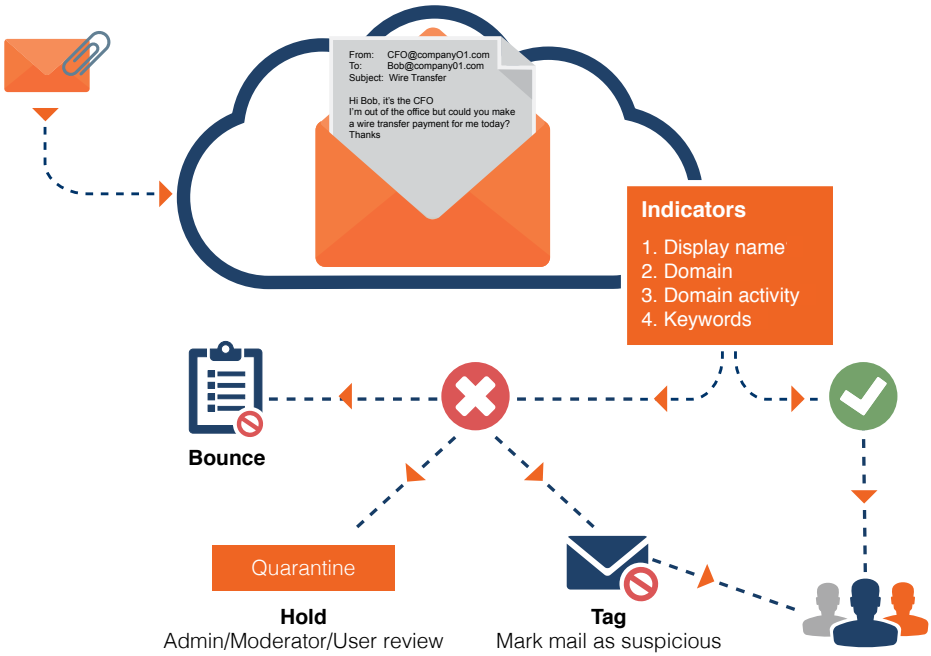
Targeted Threat Protection, with Impersonation Protect detects and prevents these types of attack. Impersonation Protect identifies combinations of key indicators in an email to determine if the content is likely to be suspicious, even in the absence of a URL or attachment.

How it works

- As email passes through the Mimecast Secure Email Gateway, Impersonation Protect examines several key components of the message.
- Impersonation Protect examines the email's display name, domain name, domain age and the body of the message to determine if the email could be a social engineering attack, like whaling or CEO fraud.
- If the email fails a combination of these tests, administrators can configure Impersonation Protect to bounce the message.
- Or, alternatively quarantine or even notify end users the email is suspicious.

KEY FEATURES:

- Real-time protection against malware-less social engineering attacks like whaling, CEO fraud, business email compromise or W-2 fraud.
- Protects against unknown or newly registered domain names used as part of the attack.
- Protects against display name or friendly name spoofing.
- Ensures end users are protected at all times by visibly marking suspicious emails.
- Backed by comprehensive protection from Mimecast's threat intelligence infrastructure and Messaging Security teams.
- Complete administrative control over security of message; quarantine, bounce or mark emails depending on your security posture.
- Works alongside URL Protect and Attachment Protect for comprehensive protection against the latest attack methods.



Protect employees from the new breed of email cyberattack.

According to the U.S. Federal Bureau of Investigation (FBI), whaling email scams alone were up 270 percent from January to August 2015. The FBI also reported business losses due to whaling of more than $1.2 billion in little over two years, and a further $800 million in the six months since August 2015. Cybercriminals are becoming ever more inventive and creative when it comes to compromising organizations and this latest tactic is proving to be very successful.

The attacks seek to fraudulently trick employees into making wire transfers to the cybercriminals as a way of generating income for organized crime.

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

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

Key indicators of threat

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

- Display name or friendly name; to determine if the attacker is trying to spoof an internal email address.
- The sending domain name; to detect how near a match to your existing corporate domain name the sender's domain is.
- The age of the sending domain name; newly registered domain names are more likely to be suspicious in this scenario.
- Keywords in the message body; attackers will use phrases like 'wire transfer' or 'bank transfer' in this type of attack.

Impersonation Protect blocks, bounces or tags the email as suspicious ensuring employees are not tricked into making fraudulent wire-transfers or giving out sensitive employee data

Additional protection from malicious URLs and weaponized attachments

Impersonation Protect works with URL Protect and Attachment Protect for complete protection against advanced threats in email.

Mimecast (NASDAQ: MIME) makes business email and data safer for thousands of customers and millions of employees worldwide. Founded in 2003, the Company's next-generation cloud-based security, archiving and continuity services protect email and deliver comprehensive email risk management.