mimecast

SOLUTION BRIEF

Mimecast Targeted Threat Protection

Comprehensive protection from spear-phishing and advanced attacks

Business Needs

With cyber-attacks and data breaches on the increase, organizations are painfully aware of the potential threats to their valuable data and intellectual property (IP), as well as any customer data they may hold.

Security scanning or gateway services have made it harder for traditional spam or phishing attacks to penetrate enterprise email systems. However, determined attackers are using a combination of sophisticated social engineering and targeted spear-phishing emails to breach their targets.

The unfortunate results of many attacks are highly publicized, but a larger number are unreported or simply go undetected. As spear-phishing attacks evolve to defeat even the most sophisticated security defenses, organizations must seek out more specialized solutions to mitigate these growing threats and protect themselves, their staff and customers.

Business Challenges

The ever-growing data repositories and valuable IP held by organizations are an attractive target and attackers are becoming increasingly sophisticated in their methods.

Organizations may be targeted to be used as a springboard – the attackers use their systems to gain access to trusted third-party companies, damaging the reputation of both organizations in the process.

Spear-phishing attacks in email are amongst the latest breed of tactics. Designed to look authentic and pass freely through traditional email security services, these emails are often created following social engineering reconnaissance that helps to make them look legitimate. When clicked, links to malicious sites can trick employees into giving away sensitive credentials or expose their systems to malware, further compromise or persistent penetration. Zero-hour weaponized attachments are often used instead of a malicious URL and can infect targeted systems if opened.

Technical Challenges

IT teams have successfully deployed secure email gateway services to block traditional malware and other widespread attacks. But spear-phishing attacks are highly targeted and designed to pass through existing security gateways. Often the embedded URLs are initially inactive and therefore clean when scanned. Phishing web content is activated later when the attacker knows all gateways have passed the email and link. Traditional email gateways are not designed to detect zero-hour malware in email attachments either. While most organizations choose to block executable attachments at the gateway by default, they must still allow files such as PDF and Microsoft Office to pass freely. Attackers exploit this by weaponizing files in these common formats.

Several major data breaches and state sponsored hacking attacks have been initiated through the use of spear-phishing or targeted email attacks of this kind. Existing security protection must therefore be augmented to combat this growing threat. An effective solution must protect users no matter what device they use to access business email – desktop or mobile, corporate provided or personally owned.

mimecast®

SOLUTION BRIEF

Mimecast Solution

Mimecast Targeted Threat Protection extends our existing security gateway services to protect organizations against the growing threat posed by spear-phishing and targeted attacks in inbound email.

Targeted Threat Protection - URL Protect rewrites URLs in all inbound email. When clicked, the destination website is scanned in real-time for potential risks before being opened in the employee's browser. If the site is safe, it opens as normal. If not, a warning page is displayed and access to the website is blocked. Links are scanned on every click to help ensure they are safe and to protect against the risk of a legitimate site being compromised at a later date. Wholesale protection of this kind is safer and more effective than attempting to detect a single phishing email and recognizes that links can start safe but be compromised at a later date.

Administrators can also enable a dynamic user awareness capability to help make employees aware of the risks of spear-phishing and targeted attacks - driving a mentality of caution. It helps employees understand their role as your 'human firewall' and enhances their ability to spot dangerous emails and potentially suspicious URLs.

Mimecast Targeted Threat Protection - Attachment Protect reduces the threat from weaponized or malware-laden attachments used in spear-phishing and other advanced attacks. It includes pre-emptive sandboxing to automatically security check email attachments before they are delivered to employees. Attachments are opened in a virtual environment or sandbox, isolated from the corporate email system, security checked and passed on to the employee only if clean.

Attachment Protect also includes the option of an innovative transcription service that automatically converts attachments into a safe file format, neutralizing any malicious code. The attachment is delivered to the employee in read-only format without any delay. As most attachments are read rather than edited, this is often sufficient. Should the employee need to edit the attachment, they can request it is sandboxed on-demand and delivered in the original file format. This approach minimizes email delivery delays inherent in traditional pre-emptive sandbox solutions.

Protection Across All Devices

Targeted Threat Protection provides the same protection whether an employee is accessing a link or attachment in their enterprise email from a work or personal mobile, or desktop device. This is a key benefit for organizations without comprehensive web security or end point protection and those where personally-owned devices are not protected in the same way as corporate provided devices.

KEY BENEFITS:

- Comprehensive protection against spear-phishing attacks – simply managed and without the need for additional infrastructure or IT overhead.
- Instant protection on and off the corporate network, including mobile devices – with no disruption to users.
- Real-time scanning protects each time a link is clicked as today's safe site may not be safe tomorrow.
- Flexible attachment protection options with pre-emptive sandboxing and the option of innovative attachment conversion to a safe file format with on-demand sandboxing.
- Rapid service activation through Mimecast's cloud platform.
- Granular reporting allows for end-to-end, real-time threat analysis

Mimecast makes business email and data safer for more than 13,000 customers and millions of employees worldwide. Founded in 2003, the Company's cloud-based security, archiving and continuity services protect email and deliver comprehensive email risk management.