Spoofed C-level executive emails are the next big threat, and it's costing businesses billions.

Singtel

According to the Federal Bureau of Investigation (FBI), recent report shows that global losses from compromised business email have reached **$5.3 billion**[1], with CEOs being spoofed the most by such attacks.

Businesses are increasingly becoming susceptible to such security attacks because unsuspecting email users are working from mobile devices that may not have the proper security measures in place to filter out such threats.

Chief Information and Security Officers (CISOs)[2] have shared that IT security, especially for mobile devices, can often be overlooked by businesses, particularly by C-level executives, who are often attractive targets for identity and data theft. This has lead to increased incidences of employees unknowingly replying to false emails that they believe are coming from their top executives and revealing sensitive corporate data or downloading malicious attachments which target the business networks.

Proactive email security is therefore needed to mitigate such email-based risks across all devices. Offering zero day email protection, **Microsoft Advanced Threat Protection (ATP)** will be the first defence to scan your business email automatically for threats and unknown attacks.

It's time to safeguard your business data - ATP helps guard against sophisticated threats including unknown malware and viruses. It offers email filtering and real time, time-of-click protection against malicious URLs, protecting your employees and key executives with access to confidential company data from email-based threats, malware and other sophisticated threats which can result in the loss of personal and business data.

Filter out threats with Advanced Threat Protection.

Secure your mailbox and protect against unsafe attachments

Safe Attachments is designed to detect malicious attachments before anti-virus signatures are available, and to provide better zero day email protection to safeguard your messaging system. All messages and attachments without a known virus/malware signature are routed to a special hypervisor environment, where a behavioral analysis is performed using a variety of machine-learning and analysis techniques to detect malicious intent. Safe Attachments then detonates attachments that are common carriers of malicious content, such as Office documents, PDFs, executable (EXE) files, and Flash files. If no suspicious activity is detected, the attachment is released for delivery to the mailbox.

Protect your environment when users click on malicious links

Safe Links is a feature that helps prevent users from going to malicious websites when they click them in email. Attackers sometimes try to hide malicious URLs within seemingly safe links, redirecting users to unsafe sites through a forwarding service after the message has been received. The ATP Safe Links feature proactively protects your users if they click such a link. That protection remains every time they click the link, so malicious links are dynamically blocked while good links remain accessible.

Obtain rich reporting and track links within messages

Safe Attachments has two traffic reports which show aggregated data for a tenant by disposition (blocked, replaced etc.) and the file types. The report also shows detailed data (i.e. date, sender, recipient, ID, subject). Safe Links has advanced reporting features that make it easy to determine who has clicked through a malicious link to support faster remediation. The rich reporting URL trace capabilities provide critical insights into who is getting targeted in the organization and the category of attacks being faced. Addtionally, ATP reporting will expand to provide analysis on why ATP flagged an email as a threat and granular details on scan times for emails with attachments.

Get zero day email protection for your Office 365 subscription with Advanced Threat Protection at just

$3.00 /user/month*

Unsure of your email security risk?
Contact us for a one-to-one consultation today.

1800-SME-1111 (1800-763-1111)

g-segmentict@singtel.com

*Add-on of Advanced Threat Protection is applicable to: Exchange Online Plans (Plan 1, Plan 2, Kiosk, Protection), Office 365 Business Essentials, Business Premium, Office 365 Enterprise E1, E3. Contract term for Advanced Threat Protection (ATP) will be tied to the specified Office 365 basic pack's contract term.

Source:

[1] https://www.zdnet.com/article/trend-micro-finds-ceos-are-spoofed-the-most-by-business-email-compromise/

[2] https://www.computerweekly.com/news/252437107/C-suite-a-cyber-attack-risk-say-security-chiefs