

Trend Micro Custom Defense

STOP TARGETED EMAIL ATTACKS

Critical protection against spear-phishing emails, the most common initiators of targeted attacks

Today's security landscape is scarier than ever due to a dangerous new breed of targeted attacks. Organizations are blind to advanced threats that cloak themselves by using a variety of means and methods to escape detection. Targeted or spear-phishing email attacks have become the preferred method to gain a foothold in your network. In fact, a recent Trend Micro study found that 91% of targeted attacks are initiated by spear-phishing emails.

With attackers becoming more sophisticated and using personalized spear-phishing emails to lure employees, today's enterprises must enhance their traditional gateway security to protect their valuable data, intellectual property, and communications. Trend Micro gives your security team the visibility into email activity to detect suspicious attachments and URLs, confirm the nature of the threat, and block targeted email attacks before they begin.

TARGETED EMAIL ATTACKS: THE FALSE FACE THAT CAN WREAK HAVOC ON YOUR BUSINESS

In a typical spear-phishing attack, specially crafted emails are sent to specific employees, partners, or others with access to your network. Using personal and professional information gleaned from social networks and the Internet to entice their target, attackers convince recipients to unknowingly download a malicious file attachment or to click on a link to a malicious site. And when they do, advanced malware is installed on their machines and the trouble begins. Malware typically contacts a remote command-and-control server to await instructions—and suddenly, your organization's sensitive data and proprietary information are at risk.

Spear-phishing is used to initiate targeted attacks because it is proven to be a path of least resistance for attackers to gain a foothold on your network to launch a targeted attack. And if successful, the average cost of a single targeted attack on a large organization is US\$5.9 million, according to a 2014 Ponemon Institute study.

But trying to detect these sophisticated new threats with standard security processes doesn't work. To counter these attacks, you need a purpose-built solution that works seamlessly with your existing email gateways, using advanced detection methods to detect and block targeted email attacks.



TREND MICRO DEEP DISCOVERY EMAIL INSPECTOR

Deep Discovery Email Inspector detects and blocks spear-phishing emails designed to evade existing security defenses and establish a beachhead to launch targeted attacks and advanced threats.

DETECT TARGETED ATTACK EMAILS BEFORE THEY LAUNCH THEIR PAYLOADS

Trend Micro delivers a proven ability to stop targeted email attacks and protect companies against today's advanced threats. The **Trend Micro Deep Discovery Email Inspector** exposes spear-phishing emails that are specifically designed to evade traditional IT security.

This single-appliance solution seamlessly interoperates with your existing secure email gateways to create an integrated defense against attacks that would otherwise evade your defenses.

- **Protects** sensitive data, intellectual property, and privileged communications from theft and spying
- **Defends** organizations and executives against unwanted exposure and damage to their reputation
- **Minimizes** the risk of major financial impacts associated with litigation, fines, cleanup, and investigation costs

ENHANCE EXISTING SECURITY TO DETECT AND BLOCK TARGETED EMAIL ATTACKS

Advanced detection exposes invisible threats

Attackers intend to exploit your on-premises email system as a delivery mechanism to infiltrate your network. Once inside, they'll use advanced malware to steal your data and intellectual property. Trend Micro helps you thwart their plans.

By adding advanced detection capabilities, Trend Micro helps you discover malicious content that would otherwise pass through unnoticed by your secure email gateway. Our specialized detection techniques include IP address and email address reputation; URL reputation; custom sandboxing of suspicious attachments, content, and URL links; and more, all correlated and kept up to date with the Trend Micro™ Smart Protection Network™ global threat intelligence system.

Cost-effective appliance easy to install and integrate

It's easy to protect your email system against targeted attacks with a single appliance that works with your existing secure email gateways. It seamlessly interoperates as a transparent enhancement—no policy, management, or configuration changes are required.

No other email threat protection system available today is more effective than the Trend Micro Custom Defense—including solutions that cost more, are more complex to configure and deploy, and require multiple appliances to be installed.

Contact Trend Micro or your preferred reseller to learn more about the Trend Micro Custom Defense and how to enhance your email security with capabilities to detect advanced threats and targeted attacks.

Top-Scoring Detection Technology

In recent testing by NSS Labs, Trend Micro Deep Discovery Inspector scored 100% in detecting malware delivered by email, using capabilities and detection engines that are also built into Deep Discovery Email Inspector.



Securing Your Journey to the Cloud

©2014 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [SB01_CD_Stop_Targeted_Email_140711US]