Social Engineering Attack Protection

Stops social engineering and targeted attack emails before they reach your endpoint

Trend Micro™ Social Engineering Attack Protection actively identifies social engineering and targeted attack emails. The technology uses social engineering correlation to analyze email content such as the header, body, and network traffic. Powered by the Trend Micro™ Smart Protection Network™, Social Engineering Attack Protection stops targeted email attacks before they reach your endpoint.

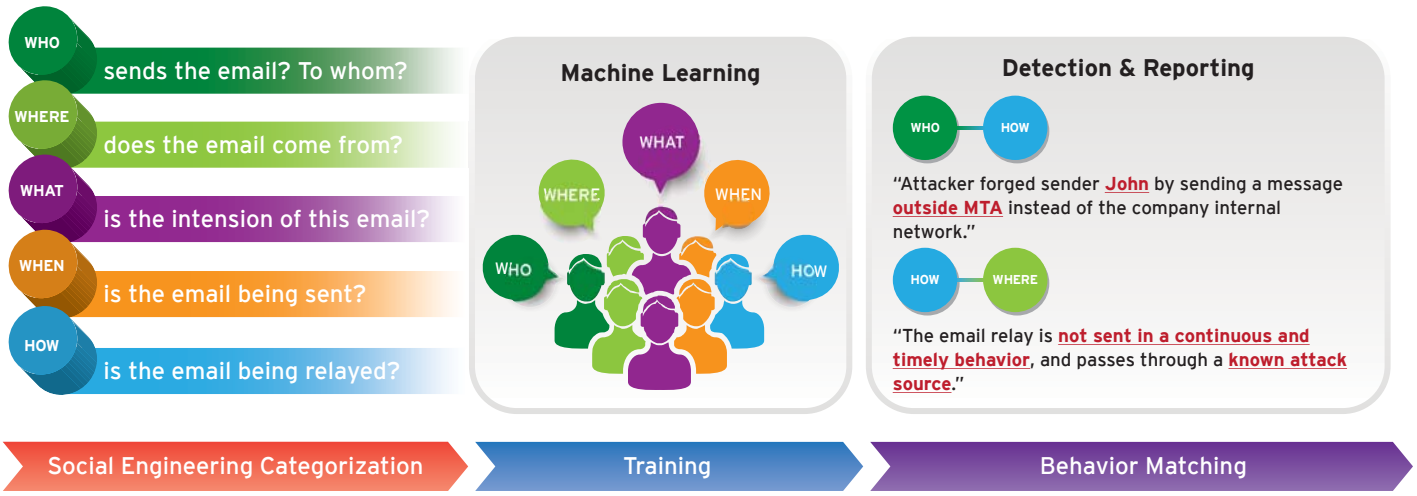
Cybercriminals and Spear Phishing

Cybercrime is already an established trade. Cybercriminals profit from selling stolen data and from offering various services, such as web development and hacking. Gaining recognition for a malware attack is no longer enough. These days, cybercriminals choose specific targets with valuable assets. These targets are usually government offices and multinational companies in critical industries such as aviation, finance, transportation, and electronics.

Given the increased awareness on malware attacks, cybercriminals need to use more sophisticated techniques to be able to infiltrate a target network. After establishing an initial infiltration strategy, attackers go after the 'weakest link' in the network to gain entry to a target organization.

Trend Micro research reveals that more than 90% of targeted attacks begin with a spear-phishing email containing a malicious attachment or link that is undetectable using standard email or endpoint security. Unlike ordinary phishing attacks, spear phishing is more target-specific, customized, and personal. Attackers use contextually relevant messages, up-to-date and attractive headers, and targeted keywords. These techniques increase the chances of a target falling into a spear phishing trap.

How Social Engineering Attack Protection Works



Trend Micro™ Social Engineering Attack Protection technology inspects the behavior of social engineering emails using five components that disclose the end-to-end lifecycle of targeted attack emails. By answering the questions Who, Where, What, When, and How Social Engineering Attack Protection detects targeted attack emails and prevents them from reaching your endpoint.

Phase 1: Social Engineering Categorization

Research on social engineering behaviors used in targeted attack emails help differentiate ordinary phishing attacks from spear phishing attacks. The distinct social engineering behaviors are categorized into a list called ***Features***, which is used to identify targeted attack emails.

Phase 2: Training

The **Features** list will be trained into a set of ***Correlation Combinations***. Each combination represents a social engineering scenario, and each social engineering scenario represents an attack method. For example,

An email message from a person claiming to be from abc.gov.com, but who is actually sending the message using a consumer MTA (e.g. ISP). The email message contains relevant content and includes a suspicious attachment.

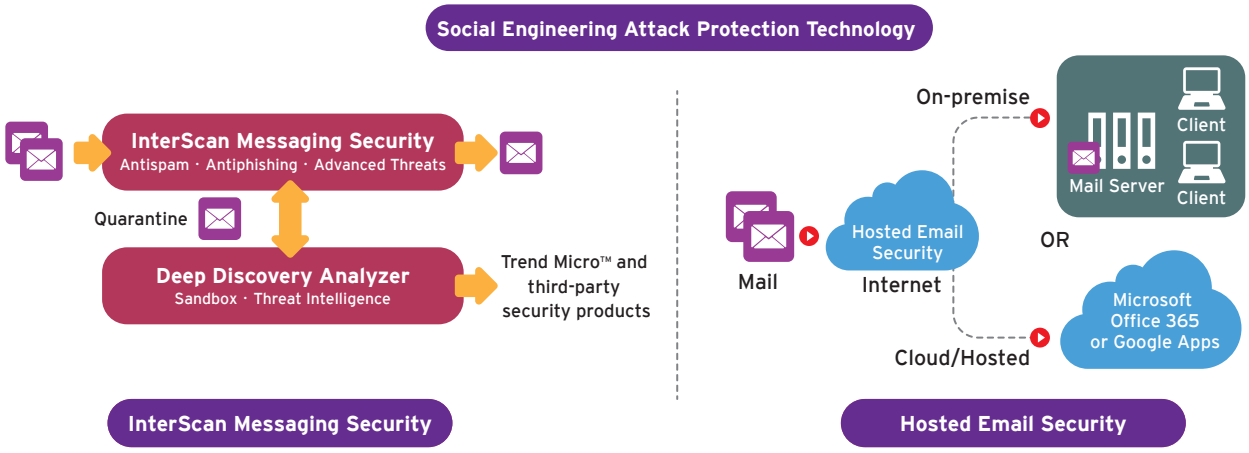
Phase 3: Behavior Matching

The ***Correlation Combinations*** is the core technology for identifying social engineering and targeted attack emails. After an email is detected as a possible spear phishing attack, an analysis report is generated why an email is detected based on the five social engineering behaviors of Who, Where, What, When, and How.

Solution

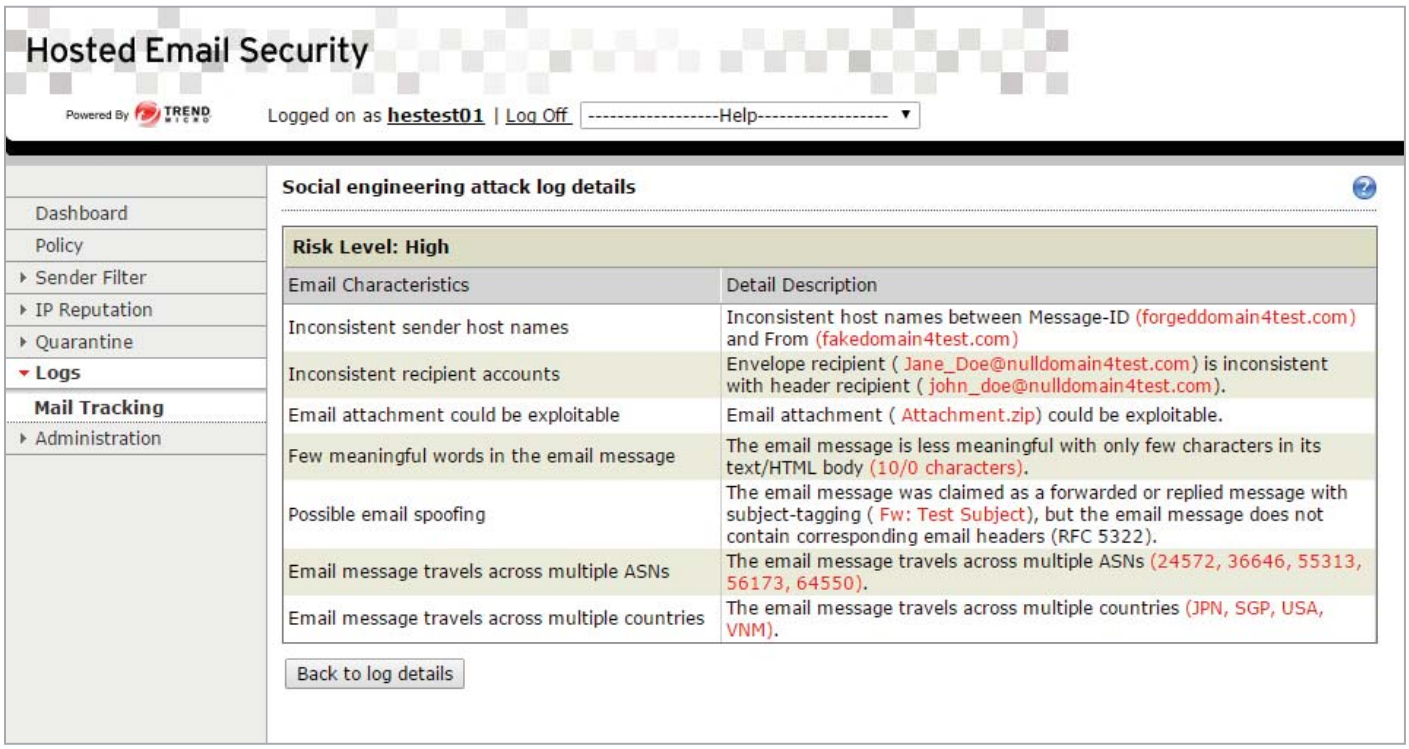
Integration with Messaging Security

Trend Micro™ Social Engineering Attack Protection technology is integrated with Trend Micro™ InterScan™ Messaging Security and Hosted Email Security, where it acts as an additional layer of protection by using social engineering correlations to analyze email contents, including email headers, body, and corresponding histories of network traffic.



Analysis Report

After an email is detected as a possible spear phishing attack by Trend Micro™ Social Engineering Attack Protection, an analysis report is generated to explain the reason of detection based on an attack scenario using the social engineering correlations of Who, Where, What, When, and How.



Advantages

- **Increased Protection:** Effectively identifies targeted attacks by looking into the social engineering behaviors of each email on top of URL, SPAM, and file-based detection technology.
- **Protection without Compromise:** Detects social engineering and targeted attack emails in real-time without compromising performance.
- **Social Engineering Characteristics Analysis:** Generates analysis reports that provide information on matched correlation combinations with specific details of the identified social engineering characteristics.

Get Enhanced Overall Protection with Social Engineering Attack Protection

Trend Micro™ Social Engineering Attack Protection complements other email filtering technologies by addressing the gaps to provide an enhanced overall protection.

- **Signature-based Technology**

  Signature-based scanning technologies may not immediately detect a new attack sample that has unique characteristics. Social Engineering Attack Protection identifies new targeted attack emails based on the social engineering behaviors to increase your protection against the latest email threats.
- **Sandbox-based Technology**

  Sandbox-based filtering technologies require time to analyze possibly malicious email attachments. Social Engineering Attack Protection asks the questions Who, Where, What, When, and How to identify targeted attack emails and reveal the end-to-end attack scenario without time-consuming sandbox analysis.
- **Email Reputation-based Technology**

  Email Reputation-based technologies stop email threats by blocking the IP addresses of malicious email servers. Social Engineering Attack Protection identifies email attacks from legitimate servers by analyzing not only the email source but also the email correlation combinations.