Trend Micro™

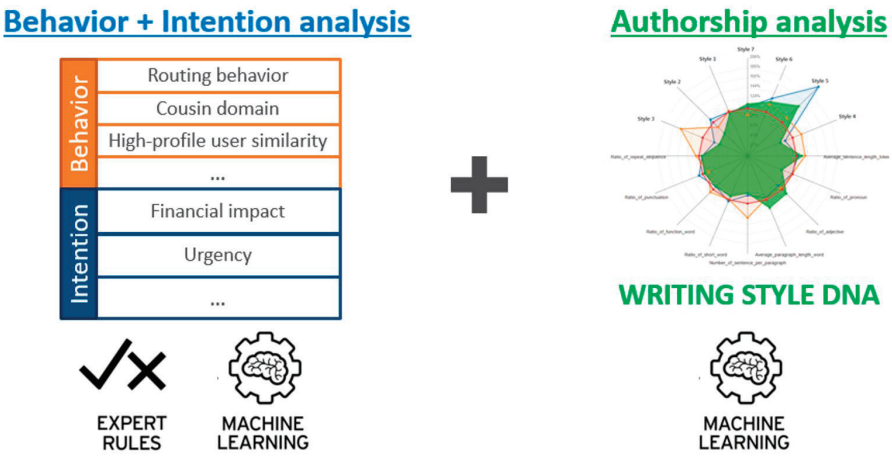
PROTECT YOUR ORGANIZATION FROM BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) attacks have increased rapidly in recent years, with the cost to businesses now over $12 billion in 2018[1]. The average loss per incident is $160,000, according to the FBI.

BEC attacks usually don't contain attachments or URLs, and the content closely mirrors the look of a legitimate email, which is why traditional email security solutions struggle with these attacks. Email authentication standards (SPF, DKIM, DMARC) can prevent domain/sender spoofing, but don't prevent other email forging techniques, like using a look-alike email domain name or using a compromised account to attack internally. That is why additional BEC prevention technologies are required in order to fully protect email users.

Trend Micro email security solutions offer multi-layered protection to prevent BEC attacks. From employee awareness training and domain spoofing protection, to artificial intelligence (AI) based BEC protection, our modern security approach can help you combat this fast growing and potentially damaging threat.

BEC DETECTION ANALYZING EMAIL HEADER, CONTENT, AND AUTHORSHIP



Trend Micro uses AI that combines the knowledge of a security expert, with a self-learning mathematical model to identify fake emails. We can mimic the decision-making process of the security researcher, using a form of AI called an **expert system**. The rules of the researcher would examine both the email's **behavior** and **intention**.

We then use a second form of AI called **machine learning**, which takes the results of the expert system and uses a computer-generated algorithm to determine if the email is real, fake, or suspicious. The machine learning algorithm is based on millions of real and fake emails and is constantly learning and improving. It weighs the results of the expert rules and more accurately detects the fraudulent email as fake.

WHAT IS BEC?

According to the FBI, BEC is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments.

The most common type of BEC attack is "CEO Fraud". These attackers will pose as an executive of the company and send an email to employees–usually to those in finance–requesting a money transfer to the accounts they control. The emails are usually designed to be "urgent" in order to throw their targets off-guard. These attacks are achieved by spoofing the sender address through the creation of a domain that looks similar to that of the target company, or by creating a free webmail address that would closely resemble an email address the impersonated executive would use.

BEC scams have been reported in over 150 countries and have a marked increase of 136 percent in identified exposed losses, between December 2016 and May 2018[1]

[1] Source: FBI July, 2018

EMAIL BEHAVIOR, INTENTION, AND AUTHORSHIP EXPLAINED

Email Behavior Analysis

Examines the email header for indications of an attack, such as: an insecure email provider, a sender domain similar to the target organization, the sender is using the name of an executive at the recipient's organization but the email address is from a free email domain, and many other factors.

Email Intention Analysis

The content of the email is examined for a sense of urgency, a request for action, or a financial implication. None of these factors are suspicious on their own, but they paint a more complete picture when combined with the other behavioral factors.

Email Authorship Analysis

Uses AI to determine if the email is impersonating a high-profile user by examining the writing style.

In addition, we examine the **authorship** of the email to determine the true author. Our Writing Style DNA technology first trains a machine learning model on the executive's writing style based on previously sent email. To protect privacy, only the metadata for the writing style is captured, rather than the actual text of the email. When an external email arrives with the same name as the executive, we compare the writing style to the trained model, and if they do not match we warn the recipient of a possible impersonation.

By combining multiple layers of AI to examine email behavior, intention, and authorship, Trend Micro's email security solution can effectively prevent damaging BEC attacks.

BEC protection is included in most Trend Micro email security products. Writing Style DNA is available in Cloud App Security™ and ScanMail™ for Microsoft® Exchange™.

DOMAIN SPOOFING PROTECTION (DMARC, SPF, DKIM)

A popular way to conduct a forged email attack is by faking the "Mail From" address. This will give the illusion that the email is coming from an internal sender (same domain as the recipient) or a well-known service provider or internet domain. Simple Mail Transfer Protocol (SMTP) authentication or email validation techniques such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC) were developed over the years to detect and prevent email spoofing.

Domain spoofing protection is included in Hosted Email Security™, InterScan™ Messaging Security Virtual Appliance, and Deep Discovery™ Email Inspector.

EMPLOYEES TRAINING

Your users are an important defense against email threats. BEC scams can be better deflected if employee training is in place, as it is reliant on social engineering. Trend Micro™ Phish Insight™ is a free phishing simulation and awareness service. You can use it to send realistic-looking phishing emails to your users, monitor the results, and offer training to those who need it most.

We are committed to making our connected world a safer place, and are offering this tool for free to ensure your organization is equipped to handle cyber threats. Learn More about Phish Insight.

As BEC attacks evolve, businesses need to keep up with the threats. Partner with Trend Micro, and get email security solutions to prevent the attacks.

DOMAIN SPOOFING PROTECTION EXPLAINED

- **Sender Policy Framework (SPF)** enables an organization to specify what IP addresses are allowed to send emails to the internet on their behalf. This prevents their domain from being used in forged and spoofed emails.
- **DomainKeys Identified Mail (DKIM)** stamps an outgoing email with a digital signature that the receiving mail server can use to verify if the email actually came from the specified source email address. This also prevents forged email addresses in the "Mail From."
- **Domain-based Message Authentication, Reporting, and Conformance (DMARC)** is an email validation system designed to detect and prevent email spoofing. It leverages SPF and/or DKIM to authenticate email messages for specific domains, sends feedback to senders, and conforms to a published policy.
- Domain spoofing protection is only designed to protect against direct domain spoofing (e.g. company.com, but not otherdomain.com or company.net). While impersonating a given domain is a common method used for phishing and other malicious activities, there are other attack vectors that DMARC does not address.

TREND MICRO EMAIL SECURITY SOLUTIONS

Trend Micro uses XGen™ security, the most advanced blend of cross-generational threat defense techniques, with proven methods to find more phishing emails and malware.
Learn More

TREND MICRO™
Securing Your Connected World