Trend Micro | Newsroom

Trend Micro Unveils Industry’s First AI-Powered Writing Style Analysis to Halt Email Fraud

Innovative new capability helps detect BEC attacks that impersonate execs

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today announced a new capability designed to enhance protection against Business Email Compromise (BEC) attacks. Powered by artificial intelligence (AI), this innovation will be integrated into multiple products to raise the alarm when emails are suspected of impersonating an executive or other high-profile user.

“This is the first time I’ve seen email writing style analysis launched in our industry,” said Michael Osterman at Osterman Research. “This is a compelling demonstration of AI being used for essential cybersecurity protection against today’s most financially impactful attack vector – email.”

Trend Micro Writing Style DNA is a new layer of protection against BEC attacks, which uses AI to “blueprint” a user’s style of writing, employing more than 7,000 writing characteristics. When an email is suspected of impersonating a high-profile user, the style is compared to this trained AI model and a warning is sent to the implied sender, the recipient and the IT department.

“The future threat landscape requires AI-powered protection that leverages expert rules and machine learning,” said Eva Chen, CEO of Trend Micro. “We are proud to add another industry first in this area.”

Chen continued: “This new capability is the perfect complement to our existing email security as well as the free phishing simulation and awareness service we’re making available to businesses. In a world of increasingly sophisticated and financially damaging email fraud, multiple layers are needed to put organizations back on the offensive.”

In 2017, 94 percent of all ransomware blocked by Trend Micro was distributed via email. In addition, total global losses from BEC scams are predicted to reach $9 billion in 2018, with an average loss of $132,000 per BEC incident. Businesses need to be able to thwart phishing – both through training and technology.

BEC attacks impersonate the CEO, president or managing director of a company nearly 70 percent of the time, with urgent requests for an employee to make a wire transfer or reply with sensitive data. These are hard to detect because the emails usually do not have an attachment or URL link, which are more commonly recognized as suspicious.

Writing Style DNA provides authorship analysis to complement existing AI inspection layers that focus on email intent and attacker behaviors by checking info in the email header and the email content. In doing so, it’s able to spot attackers who hijack legitimate domains/accounts to circumvent traditional filters. Executives can also provide feedback on the flagged emails to improve detection and reduce false positives.

Writing Style DNA will be released in June 2018 on Cloud App Security (CAS) for Microsoft Office 365 and ScanMail for Microsoft Exchange (SMEX), and will be included with existing BEC protections at no extra cost. The beta period started mid-March (for SMEX) and the beginning of April (for CAS).

However, Business Email Compromise is just one of many email-borne threats. Another serious risk to organizations comes from phishing, where spoofed messages are used to trick users into downloading malware or divulging personal details and log-ins.

That’s why Trend Micro has introduced a free phishing simulation platform, Phish Insight, which enables businesses of all sizes and budgets to test their employees' understanding of scam emails. Organizations can then tailor an education program based on the simulation results using material provided through the platform.

Click here to read more.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and investigation, enabling better, faster protection. With almost 6,000 employees in more than 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their connected world. For more information, visit www.trendmicro.com.

Contact:

Trend Micro Incorporated
Kateri Daniels, 817-522-7911
media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY