Preventing Business Email Compromise Requires a Human Touch

By Josh Lefkowitz on March 19, 2018

Human-powered Intelligence Plays a Critical Role in Defending Against Socially Engineered Attacks

The FBI's Internet Crime Complaint Center (IC3) declared Business Email Compromise (BEC) the "**3.1 billion dollar scam**" in 2016, an amount which then grew in the span of one year into a "5 billion dollar scam." Trend Micro now projects those losses in excess of 9 billion dollars.

It's an understatement to say BEC scams and the resulting damages are on the rise. But with cybersecurity spending across all sectors at an **all-time high**, how is such an unsophisticated threat still costing otherwise well-secured organizations billions of dollars?

Unlike the numerous types of attacks that incorporate malware, most BEC scams rely solely on social engineering. In fact, its use of trickery, deception, and psychological manipulation rather than malware is largely why BEC continually inflicts such substantial damages. Since most network defense solutions are designed to detect emails containing malware and malicious links, BEC emails often land directly in users' inboxes. And when this happens, the fate of an attempted BEC scam is in the hands of its recipient.

Indeed, BEC underscores why even the most technically sophisticated cyber defenses aren't always a match for low-tech threats. Combating BEC requires more than just advanced technologies and robust perimeter security—it requires humans to understand the threat. Here's why:

Human-Powered Intelligence Trumps Automation

Since socially engineered attacks such as BEC are designed to exploit human instincts and emotions, human-powered intelligence naturally plays a critical role in defending against these attacks. I've written previously about the limitations of so-called **automated intelligence** and why human expertise and analysis are irreplaceable. BEC epitomizes this notion.

After all, intelligence offerings that rely solely on automation tend to comprise little more than technical indicators of compromise (IoCs). BEC campaigns can have IoCs—but they tend to be less technical and more nuanced, often pertaining to an attacker's syntax, dialect, or other behavioral characteristics. While an IoC for a phishing campaign, for example, might be an email address, an IoC for a BEC campaign could be the phrase an attacker uses to open or sign off the email. Automated intelligence offerings and traditional network security solutions are generally not designed to identify these types of IoCs, which is why human-powered intelligence and subject matter expertise are crucial.

User Awareness and Education Prevail

Since traditional network defense solutions alone typically aren't sufficient countermeasures for BEC, **user education**—especially when shaped and informed by human-powered intelligence—is crucial. Implementing enterprise-wide efforts to raise awareness of BEC TTPs can help employees more accurately detect and report malicious emails and other socially engineered attacks.

It's also important to consider that many users may be unaware that BEC is not only a legitimate but also very common threat capable of inflicting significant monetary damages. After all, cybersecurity-related news coverage tends to focus on state-sponsored activity and large-scale cyber attacks such as Mirai or WannaCry. It should come as no surprise that unsophisticated scams such as BEC—though widespread and damaging—are often considered far less newsworthy outside the security community.

Ultimately, the simple yet far-reaching consequences of BEC should serve as a reminder for organizations across all sectors to re-examine the role of human expertise within their security strategies. Remember that even organizations with the most robust defense solutions and advanced automated technologies cannot effectively combat threats such as BEC without the adequate support and nuanced expertise of humans.