Cybercriminals and other threat actors continuously evolve their tools and techniques to ensure success. One area in which they continue to improve their techniques is in spammed messages and spear phishing emails. Another example is Business Email Compromise (BEC), an attack against businesses worldwide, for which the FBI issued an alert in 2015 and 2016.

SPEAR PHISHING AND SOCIAL ENGINEERING

Trend Micro research reveals that more than 76 percent of targeted attacks begin with a spear phishing email containing a malicious attachment or link using techniques which are difficult to detect 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.

Spear phishing continues to be a favored means for attackers to infiltrate target networks. The emails used in Operation Pawn Storm were aimed at very specific targets—they were only sent to three employees in the legal department of a billion-dollar multinational firm.\(^2\)

In a typical spear phishing attack, a specially crafted email is sent to specific individuals within a target organization. The recipients are convinced through clever and relevant social engineering tactics to either download a malicious file attachment or to click a link to a compromised site, which downloads malware onto the victim’s system.

Below is a typical infection chain for spear phishing attacks.

---

Based on data from our year-end 2014 security roundup, the volume of phishing sites increased by nearly 90 percent in the course of the year, with the bulk creation of new domains and easy one-year registration for new ones.

As with any form of social engineering, one important way to reduce the effectiveness of spear phishing attacks is to implement robust employee-awareness programs. Well-trained employees will be less likely to download attachments or click on links in suspicious emails.

At the same time, it must be acknowledged that sophisticated spear phishing attacks will always be able to successfully trick at least a small number of employees, no matter how well they may be trained. For this reason, advanced detection capabilities are also required to block spear phishing emails before they reach their victims, and to detect malware once it has infiltrated the network.

BUSINESS EMAIL COMPROMISE

The FBI defines Business Email Compromise (BEC) as a sophisticated scam targeting businesses working with foreign suppliers and businesses that regularly perform wire transfer payments. Formerly known as Man-in-the-Email scams, these schemes compromise official business email accounts to conduct unauthorized fund transfers. According to the FBI, BEC scams have already costed victims around the world nearly $2.3 billion dollars and have affected more than 7,000 U.S. companies between October 2013 and August 2015. The average loss of BEC victims is $130,000.

BEC scams often begin with an attacker compromising or forging a business executive's email account or any publicly listed email. This is usually done using keylogger malware or phishing methods, where attackers create a domain that's similar to the company they're targeting, or a spoofed email that tricks the target into providing account details. Upon monitoring the compromised email account, the fraudster will try to determine who initiates wires and who requests them. The perpetrators often perform a fair amount of research, looking for a company that has had a change in leadership in the C-suite of the finance function, or companies where executives are travelling, or by leading an investor conference call and using this as an opportunity to execute the scheme. One key item to note is that these emails do not contain any malicious attachments or code to help identify them as fraudulent. As such, new technology is needed to address detection of these emails.

As cybercrime and hacking is already an established trade from which cybercriminals profit, focusing on the malware element on an attack is no longer enough.
NEWLY-BORN SPAM DOMAINS

Spammers have been working on ways to evade one of the current anti-spam defenses which identifies spam based on the reputation of domains used in spam message runs. This technology is very effective when the time between the registration of the new domain and an email coming from this domain is long, as it allows many reputation systems to build a bad reputation of the new domain. Spammers have recently begun to shorten this timeframe to the point where newly registered domains are used within minutes of the registration—before they’ve had any time to earn a negative reputation. When these URLs appear within spam email, purely reputation-based detection doesn’t work. The table below shows some recent examples we found.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Time Lapse Between Registration and Spam Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>bu____b.com</td>
<td>0:02:44</td>
</tr>
<tr>
<td>fu__k.com</td>
<td>0:02:45</td>
</tr>
<tr>
<td>van____f.net</td>
<td>0:04:36</td>
</tr>
<tr>
<td>bo__z.net</td>
<td>0:04:57</td>
</tr>
<tr>
<td>to____b.net</td>
<td>0:05:03</td>
</tr>
<tr>
<td>ya__g.net</td>
<td>0:05:05</td>
</tr>
<tr>
<td>ab____s.net</td>
<td>0:05:10</td>
</tr>
<tr>
<td>ag__b.net</td>
<td>0:05:14</td>
</tr>
<tr>
<td>ro__y.net</td>
<td>0:05:14</td>
</tr>
<tr>
<td>fa_____s.com</td>
<td>0:05:29</td>
</tr>
<tr>
<td>op_____w.com</td>
<td>0:07:12</td>
</tr>
<tr>
<td>to____g.com</td>
<td>0:13:35</td>
</tr>
</tbody>
</table>

The results of this new technique required a new approach in combating this type of spam activity.
EFFECTIVE STRATEGIES FOR DETECTION

As cybercrime and hacking is already an established and profitable trade, focusing on the malware element of an attack is no longer enough. Because newly-born spam domains and IPs are already in use within minutes of registering, reputation-based technologies are not enough to address this ongoing issue.

Given the increased awareness of such attacks, cybercriminals will keep adopting newer, more sophisticated techniques to infiltrate their target network after going after the network’s weakest link.

Enhanced Spam Filtering with Newly-born Host Inspection

Trend Micro Newly-born Host Inspection is an additional layer of protection on top of the state-of-art Trend Micro email filtering technology, which effectively identifies spam, phishing, advanced threats, and social engineering attacks. By using a combination of fast real-time domain lookups with big data correlation techniques, we are able to identify newly-born malicious domains and block messages that contain links to them. With the addition of Newly-born Host Inspection, the Trend Micro email filtering technology now provides enhanced overall protection from email-based threats.

Email filtering technology with Newly-born Host Inspection is integrated with several Trend Micro products, including InterScan™ Messaging Security Software and Virtual Appliance, Hosted Email Security, and ScanMail™ for Microsoft® Exchange™.

SOCIAL ENGINEERING ATTACK PROTECTION

Trend Micro Social Engineering Attack Protection technology inspects the behavior of socially engineered emails using five components that disclose the end-to-end life cycle 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 endpoints.

![Figure 3. How Social Engineering Attack Protection Works](image-url)
Trend Micro Social Engineering Attack Protection works in three phases:

- **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 and BEC 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.

- **Phase 3: Behavior Matching** - The set of 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 that details why an email is considered suspect—based on the five social engineering behaviors of Who, Where, What, When, and How.

The Social Engineering Attack Protection technology is integrated with the on-site Trend Micro™ InterScan™ Messaging Security Virtual Appliance, and with software as a service Trend Micro Hosted Email Security.

*NEW* Social Engineering Attack Protection for Business Email Compromise

Recently Trend Micro added new capabilities into this protection method to address the BEC threat. Focusing on the Who, Where, and What features within an email message, seven new correlation combination rules have been included in the training component to help identify new BEC emails targeting victims.

![Email Example](image.png)
Organizations receive a log associated with any detection to give details of what was identified through the analysis of the message. Trend Micro™ InterScan™ Messaging Security Virtual Appliance supports this, and software as a service Trend Micro Hosted Email Security will support this in July 2016.

Trend Micro Social Engineering Attack Protection complements other email filtering technologies by addressing the gaps to provide an enhanced overall protection. No single technology can fully protect you against today’s threats. By enabling and using these other technologies, you can improve your detection by providing a layered defense strategy.

- **Heuristic-based Technology**: Heuristic-based scanning technologies may detect a new attack sample that has unique characteristics based on rules designed to identify the behavior of the malware when executed. Social Engineering Attack Protection compliments this by identifying 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 can analyze possible malicious email attachments or embedded URLs used in these attacks. 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 outside of attachments and URLs.

- **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.

**CONCLUSION**

Threat actors will regularly change their tools, tactics, and procedures to ensure they are able to infect the greatest amount of victims, which in turn earns them money. This requires constant and fast innovation in order to address these changes. Trend Micro’s history of innovation assures our customers we will continue to deliver unique and timely solutions.

Trend Micro Incorporated, a global leader in security software and solutions, strives to make the world safe for exchanging digital information. For more information, visit [www.trendmicro.com](http://www.trendmicro.com).

©2016 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro logo, OfficeScan, TippingPoint and Trend Micro Control Manager 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. [TB02_Combating_Social_Eng_and_BEC_Attacks_160621US]