TECHNICAL BRIEF

Trustwave SEG Cloud BEC Fraud Detection Basics

Table of Contents

About This Document **1**

1 Background **2**

2 Configuring Trustwave SEG Cloud for BEC Fraud Detection **5**

2.1 Enable the Block Business Email Compromise Mails Rule 5

2.2 Enable Anti-Spoofing Settings 6

2.2.1 Set Up Spoofing Exclusions 6

2.2.2 Other Domain Authentication Features in SEG Cloud 7

2.3 Configure the Executive Name List 8

2.4 Other Anti-Fraud Features in SEG Cloud 9

About Trustwave **10**

About This Document

This document provides:

- Brief background information about Business Email Compromise (BEC) email fraud.
- Details of basic steps that Trustwave SEG Cloud customers should follow to set up basic protection against BEC Fraud.
- Notes about other features of Trustwave SEG Cloud that can also be used to protect against BEC Fraud.

1 Background

Business Email Compromise (BEC) email fraud, also known as “CEO Fraud” or “whaling”, has become a major financial cyber threat, affecting businesses of all sizes globally. In such attacks a fraudster poses as an executive of an organization to trick individuals in the organization into sending money or sensitive information. According to the FBI, such scams have cost their victims over USD $5 billion since 2013.

In contrast to most cyber-attacks, BEC fraud attacks do not require the sophistication to exploit any technical vulnerabilities or use any malware. Instead, they target individuals working in an organization, exploiting human trust to further their malicious purposes.

Although attackers are constantly evolving their approach towards BEC attacks, wire fraud is still the most common form of BEC scam. These messages are typically short and require a response without providing much detail, and convey urgency to avoid suspicion, as shown in Figures 1 and 2.

Figure 1: Typical short BEC fraud message, demanding urgency and a wire transfer

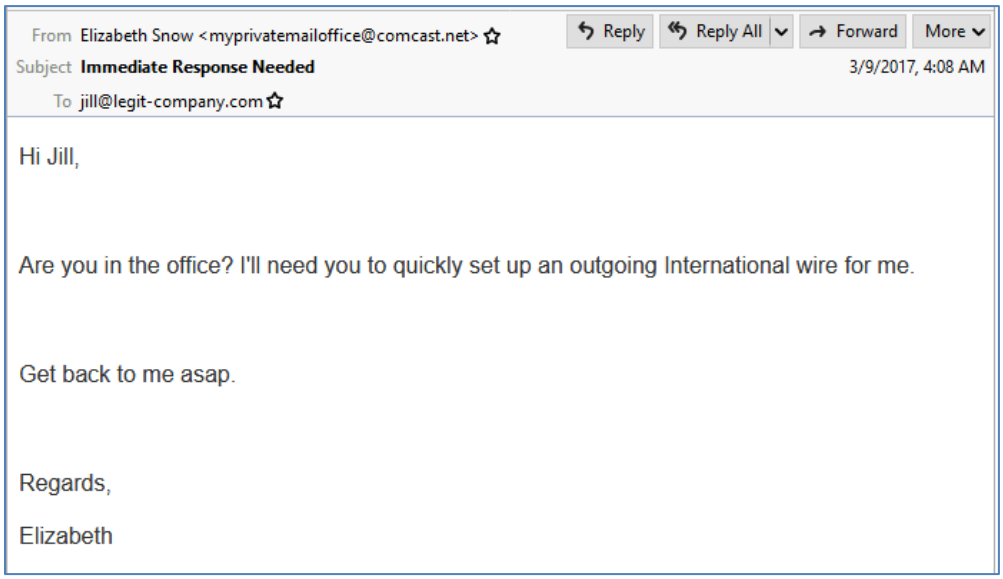
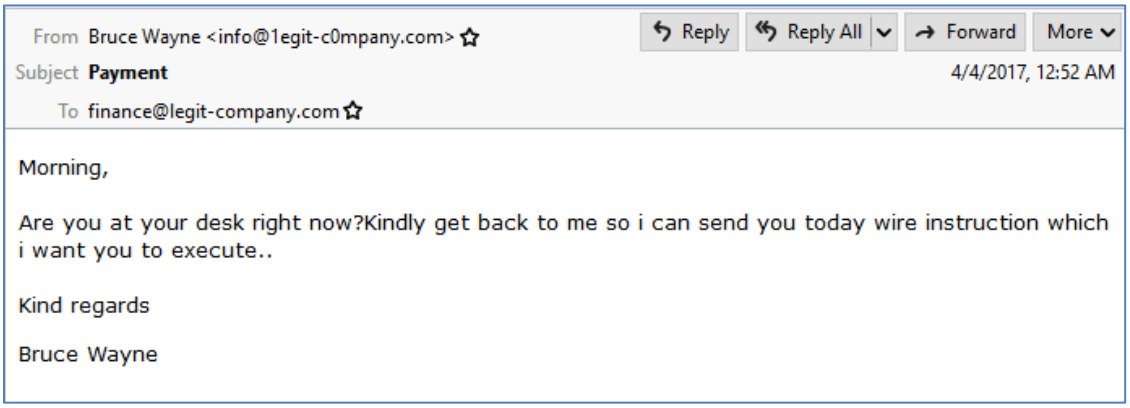


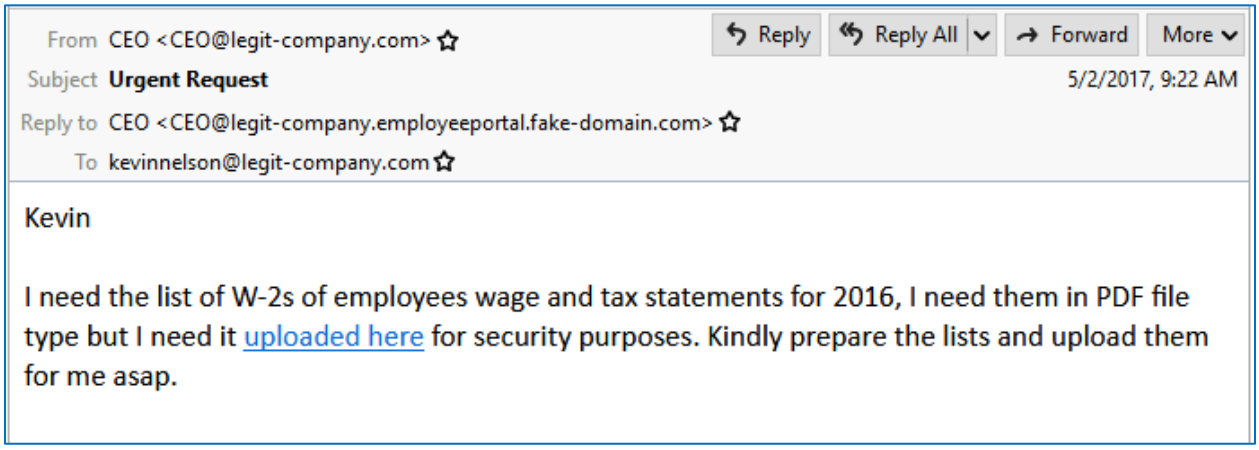
Figure 2: BEC fraud message, sent to the Finance department from a look-alike domain.



Many BEC Fraud emails contain headers that falsify the origin of the mail using spoofed details of the target organization (masquerading the sender address of an email message so that it appears that it is from another person). This technique makes the BEC Fraud email appear to be coming from within the organization.

Some BEC Fraud emails will use the organization's real domain in the From: address, but a different Reply-To address and domain as shown in Figure 3.

Figure 3: The new W-2 scam message usually surfaces near end of financial year, with an upload link to an attacker controlled FTP server.



Also common in BEC Fraud email is ID spoofing, in which the attacker uses an executive name (such as "Bill Gates") in the email header "From" field. Note the name is shown in the "Real Name" part of the From: field and not necessarily the email address part. This sort of title-spoofing traditionally uses titles of CEOs and CFOs in the email "From" field. However, attackers are now adding more executives and influencers in an organization, targeting employees across multiple departments, indicating deeper background study on the target, as shown in Figure 4, 5 and 6.

Figure 4: BEC message sent from free email account

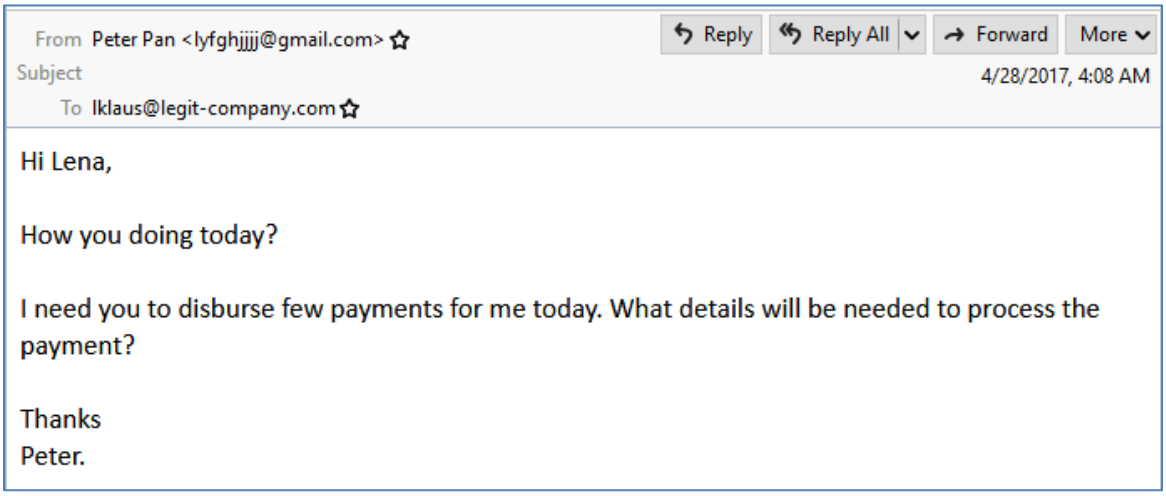


Figure 5: BEC email from free email account, with a spoofed name and title of managing director

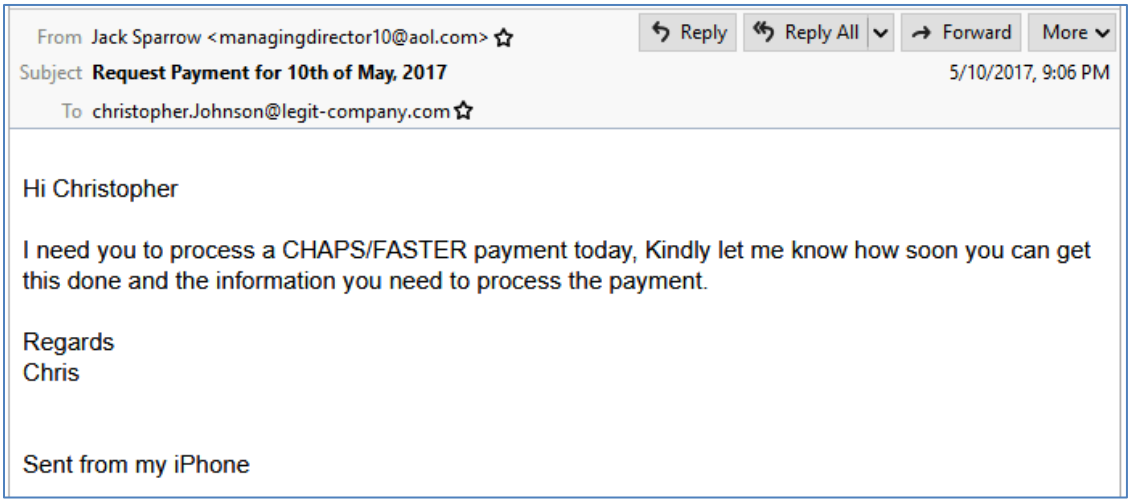


Figure 6: BEC scam email sent with a legitimate appearing spoofed address of the CEO in the From field, but a scammer-controlled email in the Reply-To header.

2 Configuring Trustwave SEG Cloud for BEC Fraud Detection

This section presents three basic steps that customers should follow to set up basic BEC Fraud protection on Trustwave SEG Cloud. More advanced options are available, but these steps should be considered the minimum.

1. Enable the rule **Block BEC – BEC Fraud Filter**
2. Enable anti-spoofing
3. Configure the Executive Names List

2.1 Enable the Block Business Email Compromise Mails Rule

All customers should confirm that they have enabled the “Block BEC – BEC Fraud Filter” rule in the Business Email Compromise (Inbound) policy. This rule is enabled by default. There are numerous subtleties and differences in BEC scam emails. To detect these attacks, Trustwave created a special filter, maintained by Trustwave SpiderLabs, that targets many traits found in BEC fraud emails. The filter is called the BEC Fraud filter and consists of hundreds of heuristic checks and thousands of signatures of known BEC Fraud actors. The filter also includes checks for use of Executive Names and domain mis-spellings. To protect against BEC Fraud with Trustwave SEG, if you do nothing else, ensure this rule is enabled. The rule appears as shown below.

Rule: Block BEC – BEC Fraud Filter
This rule blocks messages with multiple traits associated with BEC fraud.

When a message arrives
And the message is incoming
Where message is categorized as 'BECFraud v8'
Then
Send a 'Business Email Compromise - In' system notification message
And write log message with 'Spam - Scam'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.2 Enable Anti-Spoofing Settings

In email security, "spoofing" generally means forging the email header to disguise the source, usually for malicious reasons. Scammers may use (spoof) your real domain in the From: header of a BEC email. Most often the spoofed From: address is accompanied by a different Reply-To address, the address where the attacker will receive their responses, as illustrated here:

```
From: "CEO Name" <ceo.email.address@example.com>
Reply-To: "CEO Name" <email.address@attackerdomain.com>
```

The built-in anti-spoofing features in SEG Cloud, if implemented correctly, will block this type of email. SEG Cloud considers email "spoofed" if the From: address appears to be in a local domain but the source IP address is not permitted to send mail from that domain. SEG Cloud checks the From: domain to see if it is configured in the 'Local Domains' table, and then gets the IP address of the sending server. SEG Cloud then checks:

- Whether that IP address is associated with a configured local domain (a mail server where incoming email is delivered)
- Whether that IP address is allowed to relay a local domain. The list of computers allowed to relay is determined by the IP address ranges manually configured in the Trustwave SEG cloud interface (by request to SEG Cloud support).
- Whether the IP address is included in SPF records for the domain

If none of these conditions are met, the email is considered spoofed.

2.2.1 Set Up Spoofing Exclusions

For many customers, a concern when implementing the anti-spoofing rule is to allow "valid spoofed email." This is email sent by trusted third parties that use your domain in the From: address. These may include, for example, mailing list managers or cloud service providers.

Tip: Trustwave recommends that you first enable the built in rule to copy and deliver messages detected as "spoofed," instead of blocking or quarantining the messages. This will allow you to review the messages and find the message sources that should be excluded from the anti-spoofing rule. Once you have updated settings to exclude these sources from detection as spoofed, you can enable the rule to quarantine spoofed messages.

To find the sources that you want to allow:

1. Enable the rule “Monitor Spoofed Messages” in the Message Content (Inbound) policy. The rule appears as shown below:

   Rule: Monitor Spoofed Messages
   This rule monitors inbound messages sent from one of your domains, which were sourced from an unknown IP address, from a client that has not authenticated with the SEG Cloud service, or from a host not designated in your SPF records. The rule doesn't block any messages.
   When a message arrives
   And the message is incoming
   Where message spoofing analysis is based on anti-relay
   Then
   Copy the message to 'Archive (Incoming) - 2 weeks' with release action “continue processing”
   And write log message with 'Message - Spoofed Message'

2. After using this rule for a few days, review the messages and determine which ones should be excluded from spoofing rules.
3. Make changes to SPF records or request additional relay settings as required to exclude these messages. Verify the messages are excluded.
4. Disable the monitoring rule, and enable the rule “Block Spoofed Messages” in the Message Content (Inbound) policy. The rule appears as shown below:

   Rule: Block Spoofed Messages
   This rule blocks inbound messages sent from one of your domains, which were sourced from an unknown IP address, from a client that has not authenticated with the SEG Cloud service, or from a host not designated in your SPF record.
   When a message arrives
   And the message is incoming
   Where message spoofing analysis is based on anti-relay
   Then
   Write log message with 'Message - Spoofed Message'
   And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

2.2.2 Other Domain Authentication Features in SEG Cloud

In addition to anti-spoofing, SEG supports major email domain authentication technologies, including SPF. Full DKIM and DMARC integration will be supported in a forthcoming update. These technologies can also help to detect spoofed email. Implementation of any of these standards requires detailed planning, implementation and testing and is beyond the scope of this document.

- **Sender Policy Framework (SPF):** Provides a standard for validation of the source of an email message, based on the MAIL FROM: (SMTP envelope) domain.
- **Domain-Keys Identified Mail (DKIM):** Provides a method of digitally signing an email message. Public keys used to verify the signature are retrieved from special DNS records. SEG Cloud can validate DKIM signed incoming messages. DKIM signing will be supported in a forthcoming update.
- **Domain-based Message Authentication, Reporting & Conformance (DMARC):** Defines an email validation standard and system based on both SPF and DKIM checks. The owner of a sending domain sets a policy that defines validation methods used by their domain, and suggests how recipients should deal with messages that fail validation. The recipient returns reports about messages and actions to the sending domain.

2.3 Configure the Executive Name List

A common strategy used by BEC Fraud scammers is to send an email to the target, using the name of the CEO in the “real name” part of the From line (perhaps also with the CEO’s email address), but setting the From: email address to an unrelated address. The “real name” is the part of the line preceding the email address, and usually, but not always, surrounded by quotes.

```
From: "CEO Name" <address@unrelated-domain.com>
```

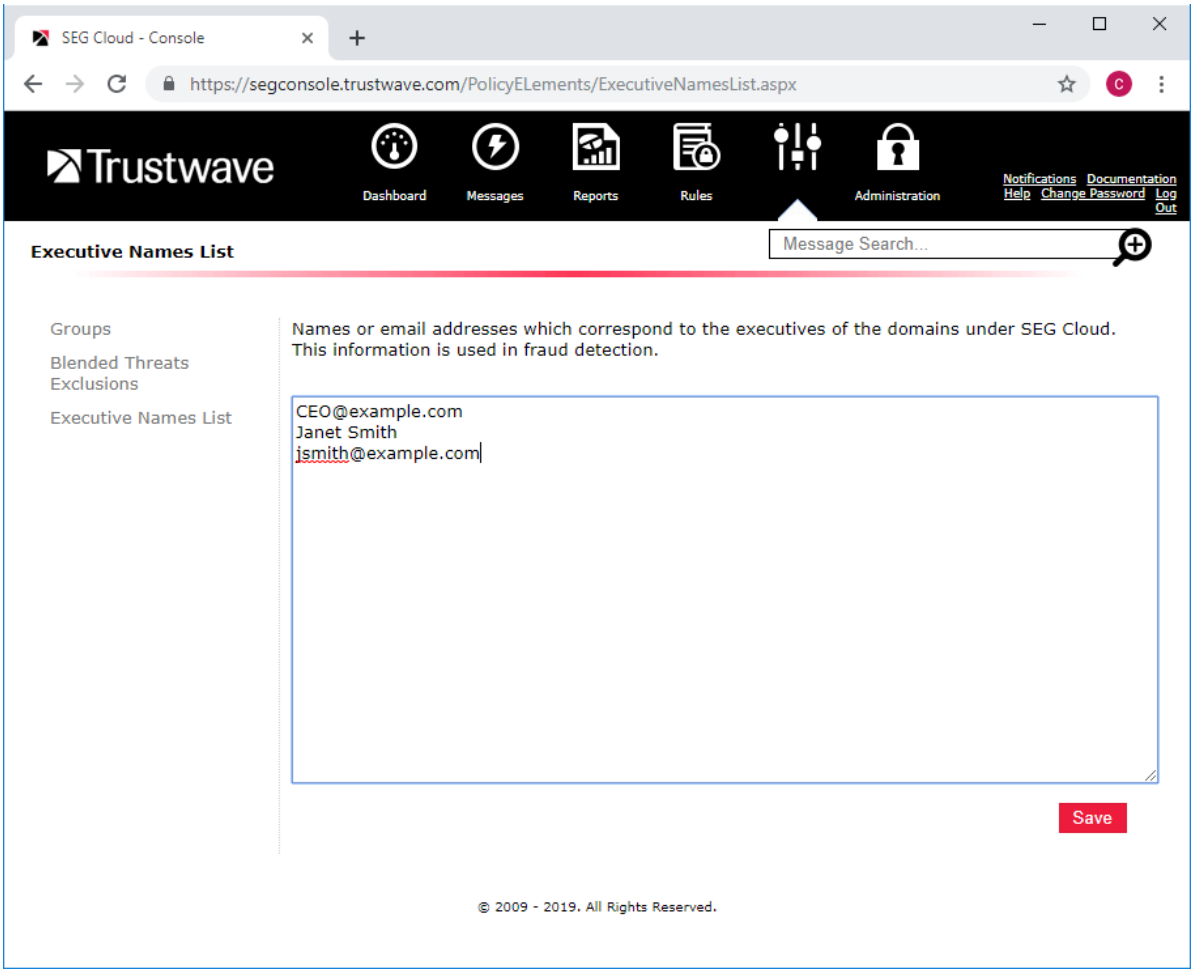
Or

```
From: "ceo.email.address@example.com" <address@unrelated-domain.com>
```

To help detect use of this strategy, SEG Cloud customers can add a list of the personal names or email addresses of their business executives and staff into the SEG Cloud **Executive Name List**.

The Executive Name List is used as one part of the BEC Fraud filter in the default “Block BEC – BEC Fraud Filter” rule. If a matching name is found in a message, the message is more likely to be blocked as suspicious.

The Executive Names List can be edited in the Customer Console under **Policy Elements > Executive Names List**:



2.4 Other Anti-Fraud Features in SEG Cloud

The Business Email Compromise (Inbound) policy contains several other rules that can help to protect against fraud attacks. You can use any of these rules by simply enabling it.

- **Block – Executive Name Match:** This rule checks the From: header for names or addresses that match the Executive Names List. The executive name match is one of the checks used by the BEC Fraud Filter rule, but testing for this check alone may trigger with greater sensitivity.
- **Block – Domain Similarity Match:** This rule blocks messages where the domain in the From: address is a “look-alike” or “typo” for one of your managed domains, based on a proprietary algorithm (for example, substituting zero for O or with minor mis-spelling). Registering a similar domain is a common technique to misdirect responses and get private information.
- **Warn – From Reply-To Mismatch:** This rule adds a warning to the message where the From and Reply-To email addresses (headers) are different. Legitimate messages such as newsletters or marketing email are known to use this technique legitimately, but it can also be used for fraud because replies can go to an unexpected recipient.
- **Warn – External Email:** This rule adds a warning to the message indicating that it was received from an external source.

About Trustwave

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit https://www.trustwave.com.