AGARI

Business Email Compromise (BEC) Attack Trends Report

Executive Summary

In the second half of 2017, BEC attacks continued to accelerate with 96% of organizations analyzed by Agari being attacked at least one time, and with the average business experiencing 45 BEC attacks from June through December 2017. Because BEC attacks have no payload (such as a malicious attachment or URL) to detect and block, they are able to slip past most of the conventional security technology used to protect organizations. To build the security controls and resources needed to protect organizations and their employees, it is critical to gain a better understanding of the nature of BEC attacks. Until now, relatively little research has been done on this topic.

As part of this research paper, Agari analyzed over 1 billion real-world emails that were considered safe by conventional security technologies: Secure Email Gateways (SEG), Advanced Threat Protection (ATP), and Targeted Attack Protection (TAP). In doing this, Agari established which security technologies incorrectly classified emails as safe, and the nature of these malicious emails. Agari's unique perspective enables Agari to measure the identity deception techniques that are most commonly used by attackers, measure the effectiveness of different security controls and understand variations in attacks by the size of the organization and the Secure Email Gateway in use.

BEC Attack Snapshot From Agari Research, June 2017 – January 2018:

- 96% of organizations experienced at least one BEC attack.
- On average, 45 BEC attacks evaded each organization's existing defenses.
- 82% of BEC attackers used display name deception to impersonate a trusted party, and without the SEGs, ATP and TAP detecting it.

Q3/Q4 2017

Average Number of BEC Attacks Bypassing SEG Per Organization

45

Percentage of Organizations Experiencing BEC Attacks

96%

Most BEC Attacks for a Single Organization

369

Introduction to Business Email Compromise (BEC) Attacks

Business Email Compromise (BEC) is a type of advanced email attack that inherently relies on the use of identity deception and evades detection by avoiding the use of a detectable payload such as a URL or attachment. Commonly, the criminal will pose as a colleague of the intended victim or as a vendor of the organization of the intended victim, and either ask the intended victim to perform a payment or to send some sensitive data. There are three different types of identity deception that criminals use to execute a BEC attack: spoofing, look-alike domains and display name deception.

In a display name attack, the criminal uses a display name – also referred to as the "friendly from" – that is the same or very similar to that of the impersonated party. Since most people determine the identity of the sender simply by looking at the display name, this attack is very successful. The most common type of display name attack uses free webmail accounts, but some criminals go further and register their own domains, too.

Whereas, in the past, criminals have typically registered domain names similar to the domain of the impersonated party (referred to as a look-alike domain or a cousin-name domain), it is becoming more common for them to use domains that are more generic. For example, a criminal may register a domain such as "secure-email-112.com" or "executive-accountive.com", and then create multiple accounts and associated display names for these. Generic domains are less likely to be automatically identified as deceptive than look-alike domains are, and can also be reused for attacks on many different organizations.

Related to the BEC attack, a spear phishing attack is aimed at tricking the intended victim to give out a credential. Most spear phishing attacks try to steal passwords, but recently, some have instead been constructed to steal password reset codes or to deceive the victim to grant the attacker OAuth access to the victim's account. Like BEC attacks, spear phishing attacks use identity deception, wherein the attacker poses as a trusted brand. Traditionally, this was done using spoofing, but increasingly, display name attacks are used for this purpose, just as for BEC attacks.

BEC Types and Classification

BEC comprises a very small portion of all emails transmitted – fewer than 0.7 parts per million of all delivered emails. Here, BEC is defined as a targeted email with a deceptive sender identity – an impostor – and that uses social engineering methods aimed at coercing the intended victim to perform an action benefitting the attacker. The most common actions are to transfer funds, e.g., for paying a vendor or supposed vendor, or to disclose sensitive data, such as tax data of employees.

Importantly, BEC is also defined by what it is not: other than the text used to con the intended victim to perform an action, there is no payload. In contrast, a message with a malware attachment or link does not fall under the traditional definition of a BEC attack. For the same reason, a phishing attack – or its targeted cousin, the spear phishing attack – is not a BEC attack. The reason is that the phishing attack is associated with a URL payload, leading to an attacker-controlled webpage for the intended victim to enter his or her credentials on.

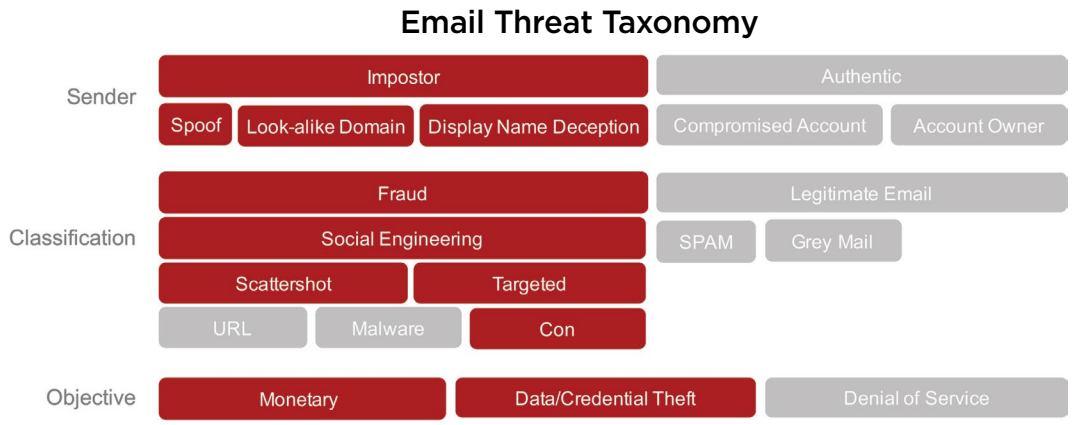
That said, it is clear that there are attacks that exhibit strong similarity with BEC attacks, as defined above. For example, the infamous email that an attacker used to gain access to John Podesta's emails used impersonation (of Google); was targeted; and used social engineering – and used these techniques to breach the security of an organization (in this case, the DNC). But this was a spear phishing email, because it used a malicious URL. Whereas spear phishing emails can also be used to attack enterprises, we do not call them BEC attacks.

The definition of what constitutes a BEC attack corresponds to which defense mechanisms are meaningful. Phishing emails can be detected based on having malicious URLs – whether these are blacklisted, or are simply found to correspond to web pages with content determined to mimic authoritative web pages (such as your bank's website, or your email service provider's web page). Similarly, emails with malware can be detected based on having an attachment with malicious content – or links to webpages with malicious content – where content is determined to be malicious based either on matching a signature or by exhibiting unwanted behavior. BEC attacks cannot be detected in this way; instead, security technologies typically detect BEC attacks because they come from untrusted sources, while looking like emails from trusted sources.

Email Threat Taxonomy

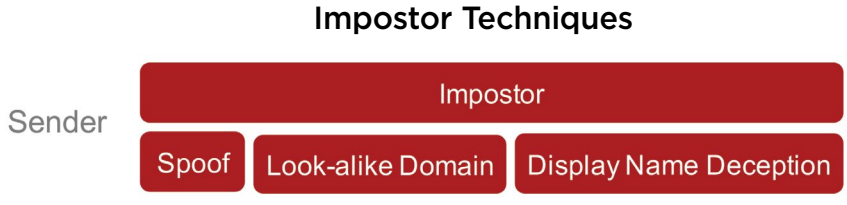
The rapid evolution of cyber attack techniques has outpaced development of a widely shared language for describing the threats. It limits the ability to identify proper countermeasures, and frustrates meaningful comparison between potential approaches.

To establish a common way of talking about the problem, Agari in 2017 published a classification system for cyber threats - a threat taxonomy - that breaks down common Internet attacks in terms of how they are carried out, and what the attackers wish to achieve.

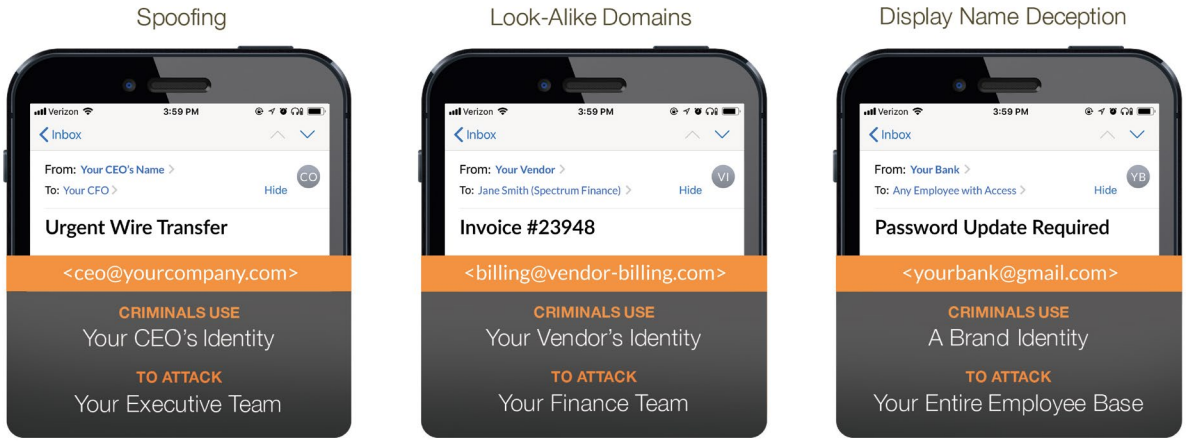


The chart above shows a portion of the email fraud taxonomy, highlighting in red the aspects associated with BEC. A BEC attack is sent using an impostor identity that impersonates a party the intended victim trusts. It is a fraud email – as opposed to typical spam, for example – and uses social engineering to make the intended victim perform a risky action. It is, furthermore, a con: it is based solely on convincing the intended victim to send money or data; it does not have a payload. For more details, please see **https://www.agari.com/threat-taxonomy-framework-cyber-attacks/**

BEC Attack Impostor Techniques

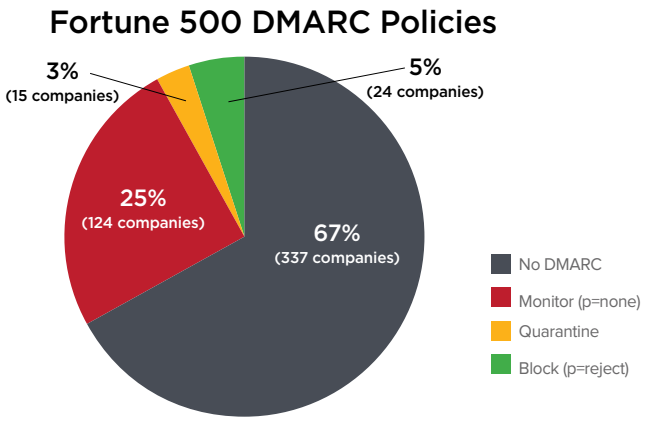


Agari's research shows that 12% of BEC attacks use spoofing; 7% a combination of look-alike domains and display name deception; and 81% pure display name deception. The portion of pure display name deception has been on a steady rise for the last twelve months. Understanding these three identity deception techniques and their definitions is critical to understanding the conclusions of this research paper and planning security controls to stop BEC attacks.



Spoofing

In a spoofing attack, an attacker operates a router set up as a mail server, but instead of simply forwarding emails, the attacker inserts forged emails in the mail stream – complete with forged delivery paths. Alternatively, the scammer simply uses a free or paid service that does this for him: the barrier to entry is almost non-existent.



If the impersonated domain has a published DMARC policy, spoofed emails can be blocked or quarantined. However, most organizations do not have a DMARC policy on their own domain and even fewer filter inbound email to block email based on DMARC authentication; for example only 5% of the Fortune 500 have a Reject (or "blocking") policy on their corporate domain.[2]

Some BEC scammers use spoofing to either impersonate users of the targeted organization or users of organizations trusted by the targeted organization. It is important to note that DMARC will only protect BEC against attacks that spoof protected domains: if a company protects its domains using DMARC, those domains cannot be spoofed. However, attackers can still spoof other trusted entities such as the company's law firm, a supplier or brand.

[2] https://www.agari.com/wp-content/uploads/2017/08/Agari_DMARC_Adoption_Report_PR1.pdf

Look-Alike Domains

A look-alike domain is a deceptive-looking domain under the control of an attacker. There are two principal types of look-alike domains. The “traditional” type looks like the domain of the impersonated organization – for example, “agarii.com” (with two i’s) might be used to impersonate a user with the domain “agari.com” (with only one ‘i’.) The second and more common type is generic, such as “admin-messg-mail.com”, which is a real-world domain used by cyber criminals. Whereas one may argue that does not strictly look like the domain of the impersonated party, one can also see it as a domain that is “consistent” with the role of the impersonated party, meaning that an intended victim may not notice a discrepancy.

All attacks involving look-alike domains also use display name deception to add a display name matching the impersonated user. However, for the purposes of this research we will categorize all domains that use both look-alike domains and display name deception into the look-alike domain category.

Display Name Deception Attacks

In a typical display name attack, the attacker registers a free webmail account and sets the display name to match that of the impersonated party. Typically, a BEC attacker sets the display name of an email impersonating a user or an organization to match the impersonated entity. For example, the attacker may set the display name to “Ravi Khatod” to impersonate Agari’s CEO; or “Wells Fargo” to consider an example display name attack focusing on an organization rather than a person.

The figure above shows another type of display name deception that is becoming more common. The display name in this case corresponds to the entire text within the quotation marks, including the apparent email address, no-reply@dropbox.com. A typical recipient may think this apparent email address correspond to the sender of the email; however, the real sender corresponds to the email address in blue, namely <aokeefe@xxxx.com>.

The Role of the Username

In addition to selecting display names matching those of the impersonated users, criminals also sometimes choose usernames to help perpetrate their impersonation attempts. The username of the registered account is sometimes chosen to allude to the impersonated organization and/or user, e.g., <Ravi.Khatod.Agari.com@gmail.com> being used to impersonate <Ravi.Khatod@agari.com>. Note that this is not the display name, which in this example case might be set to be either “Ravi Khatod” or “Ravi Khatod <ravi.khatod@agari.com>”. On the other extreme, the username is sometimes simply any name, and is not related to the display name. The username in the figure above is an example of this. The most common situation, though, is for the user name to correspond to the role of the impersonated user – for example, <executiveexco252@gmail.com> was a real-world account used by a scammer. The benefit of this latter approach, from the perspective of the criminal, is that this name remains consistent with the role of the impersonated user as the criminal cycles through a large number of users he wishes to impersonate – as long as these users have similar roles.

The Effectiveness of BEC Attacks and Recent Examples

The most recently published statistics estimate the exposed losses of BEC attacks at $5.3 billion[3] between October 2013 and December 2016, a sharp increase from similar time intervals of previous years. In 2017, BEC scams continued to accelerate. Based on our research, BEC scams are not discriminating based on industry, company size or security controls in place. While cyber criminals attack organizations of all shapes and sizes, they also have a wide range of sophistication from simple display name attacks using free webmail accounts to sophisticated multi-level and globally distributed cyber criminal organizations using everything from cleverly selected look-alike display names to masquerade their identities, to proxies hiding their actual locations.

Here are a few of the BEC attacks that made the headlines in the past year that illustrate the range, variety and success of attackers:

Google/Facebook $100M Partner Invoice Scam

In April 2017, the United States Justice Department made public[4] that Google and Facebook lost a combined $100 million to BEC attacks impersonating their server hardware supplier Quanta. The perpetrator was a Lithuanian named Evaldas Rimasauskas, who went as far as creating real corporate entities and associated bank accounts, to convince the accounting departments of both firms to make wire transfers to bank accounts in Eastern Europe.[5]

MacEwan University $11.8M Wire Transfer Fraud

In August 2017, MacEwan University in Alberta, Canada was defrauded of $11.8 million in a BEC attack impersonating a vendor of the university. Fortunately, the attack was detected quickly, and most of the funds were tracked down and frozen. The university is working with law enforcement to recover the stolen money.

New York Judge Loses Over $1M in Real Estate Scam

A New York State Supreme Court judge lost over $1 million in a BEC attack that impersonated her lawyer, conning her into wiring the closing costs for an apartment she was buying to a criminal's bank account in China.[6]

These are just three example out of tens of thousands. Fortune 500 organizations, small businesses, universities and individuals continue to be plagued by BEC attacks.

[3] https://www.ic3.gov/media/2017/170504.aspx

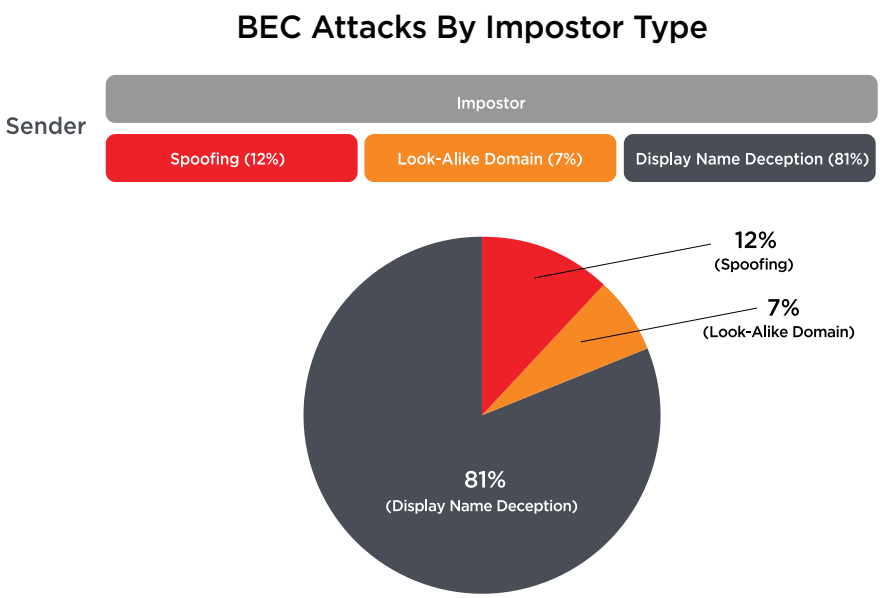
[4] https://www.justice.gov/usao-sdny/pr/lithuanian-man-arrested-theft-over-100-million-fraudulent-email-compromise-scheme

[5] http://fortune.com/2017/04/27/facebook-google-rimasauskas/

[6] https://www.bleepingcomputer.com/news/security/ny-supreme-court-judge-loses-over-1-million-in-email-scam/

How Cyber Criminals Impersonate You and Those You Trust: Results & Analysis

BEC Attacks By Impostor Techniques



BEC attacks, by definition, have no payload such as a malicious attachment or URL to detect and block. This limits the applicability of common security technologies to address this rising problem. As a result, understanding the prevalence of different types of impostors used in targeted email attacks is critical to planning the security controls and resources required to protect organizations.

As part of this research report, we classified more than 1,000 real-world BEC attacks. The result showed that 81% of BEC attacks use display name deception as the technique to deceive the target victim into taking action. Initiating a display name deception requires no skill to execute. It is as simple as signing up for a free cloud email account and changing the name in the account profile. These attacks also have the advantage of coming from trusted infrastructure, which eliminates the possibility of them being blocked based on the reputation of the sending server.

Spoofing a domain of a company accounted for only 12% of the observed BEC attacks. This includes both spoofing of the domain of the targeted company and spoofing of the domain of a trusted partner, such as a law firm or a vendor working with the targeted company. While technically straightforward, spoofing a domain requires slightly more skill than display name deception does. Moreover, this technique will not work for any domain that has DMARC email authentication deployed, with a policy of reject or quarantine. While this still describes a minority of existing domains, it eliminates the ability for criminals to impersonate many banks, government organizations, technology and retail organizations, which commonly use DMARC. The additional effort required to execute an attack with a domain spoof is often not worth the yield.

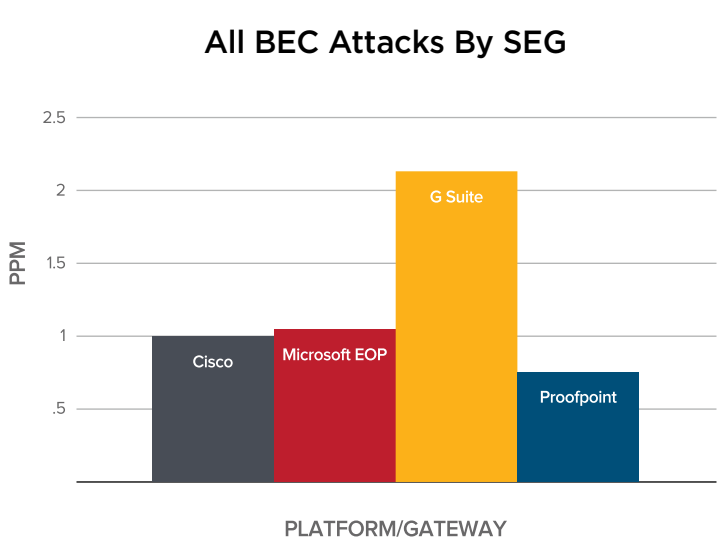
Look-alike domain based attacks represent the least common impostor technique, with only 7% of attacks. The reason for this is that look-alike attacks require both effort to set up the domain and money to register it. To make it worse – for the attacker, that is – look-alike domains mimicking a particular organization often have a short life, as the owner of the brand often executes a take-down of the offending domain soon after the initial wave of attacks is detected.

Frequency of BEC Attacks Bypassing Secure Email Gateways

The data in this report was collected from Agari Enterprise Protect, an advanced email threat solution that filters email traffic after it has been sent to the inbox by a Secure Email Gateway (SEG). Typically, SEGs apply spam filtering, anti-virus, URL and malware analysis prior to sending the email along to the end user's inbox. Some SEGs also include basic impostor detection capabilities or the ability to enforce email authentication for domains that publish a DMARC record.

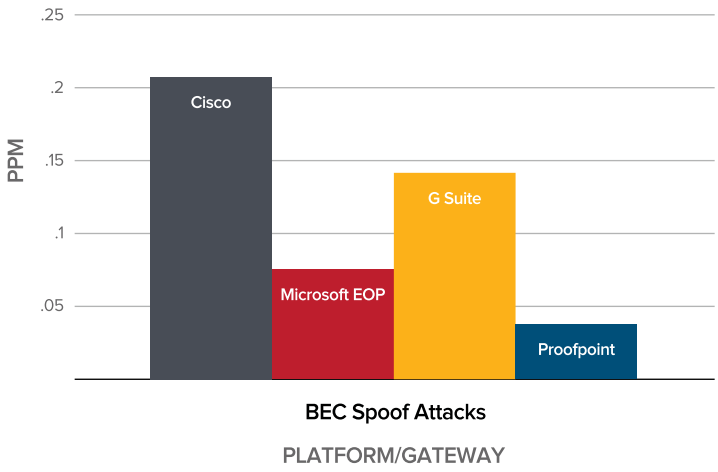
As a result, this data can be used to analyze how many BEC attacks bypass all of the pre-Agari security controls for these organizations, including SEGs, Targeted Attack Protection (TAP), Advanced Threat Protection (ATP) and DMARC enforcement. In the analysis below, Agari has normalized the data using "parts per million" (PPM) to represent the number of attacks that go through security controls by percentage of email volume so that sample sizes do not impact the effectiveness measurements. One part per million means that one BEC attack was detected getting through the SEG out of an email volume of 1 billion emails sent to the inbox of the user after applying all security controls (SEG, ATP, TAP, DMARC).

Agari measured BEC attacks that bypassed Cisco, Microsoft EOP, Google G Suite, Proofpoint and Symantec Secure Email Gateways. Because the sample size of the traffic through Symantec's SEG was too small to be statistically significant, Symantec was removed from the charts in this section.



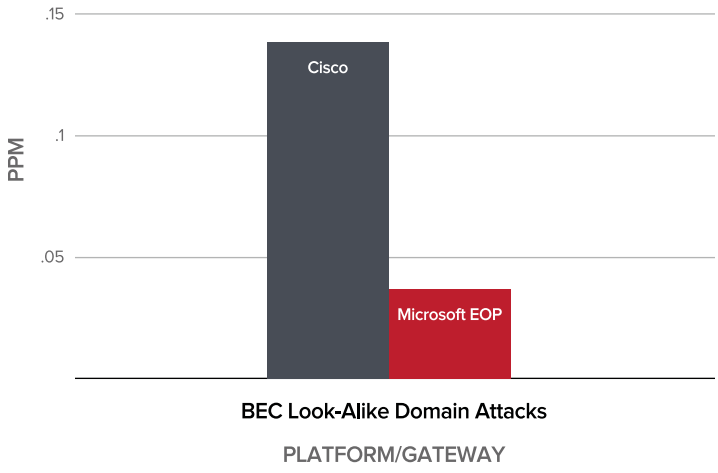
For all BEC attack types, Google G Suite saw more than twice the number of BEC attacks get through per million email messages compared to the other SEGs. All of the organizations using G Suite were small, based on both employees and revenue. None of the organizations considered in this data set that relied on G Suite used additional security controls beyond the integrated Secure Email Gateway, nor did any of them enforce DMARC email authentication on inbound email. Cisco and Microsoft EOP were roughly equivalent at approximately 1 BEC attack per million emails. Proofpoint fared best with 3/4 BEC attacks per million. Two thirds of the organizations using Proofpoint are large organizations (more than 10,000 employees) which tend to have several additional security controls in the mail flow.

Spoofing BEC Attacks By SEG

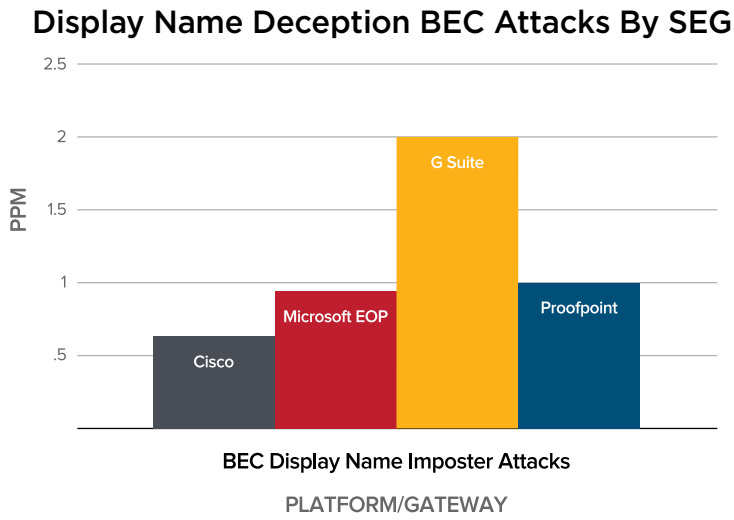


For BEC attacks using spoofing, Cisco saw the most attacks getting through, at 1/5 PPM. Google G Suite users also suffered a relatively high incidence of spoofing, at roughly 1/7 PPM. Both Microsoft EOP and Proofpoint were below 1/10 PPM. Some of the Proofpoint customers used Agari Customer Protect to publish a DMARC reject policy on their primary domain and used Proofpoint to enforce DMARC authentication on inbound traffic, making it impossible for a domain spoof of their own domain to get through.

BEC Attacks Using Look-Alike Domains, By SEG

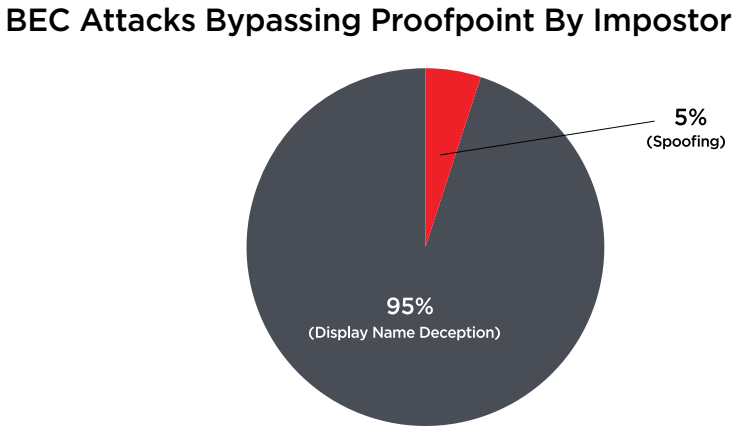


For BEC attacks using look-alike domains, the reported data only contained attacks that bypassed Cisco and Microsoft EOP. There were no attacks of this type seen to evade G Suite or Proofpoint. Given the low occurrence of BEC attacks using look-alike domains, the sample size may be too small to draw any definitive conclusions from this data. Even for Cisco, which had by far the most look-alike attacks, the number is still only 1/7 PPM.



For BEC attacks using display name deception, which were the most common BEC attack type, Google G Suite again saw the most attacks get through their controls. However, in this scenario, Cisco and Microsoft EOP outperformed Proofpoint. This makes sense as the additional security controls such as DMARC authentication and TAP that are supported by Proofpoint are not effective at stopping display name deception.

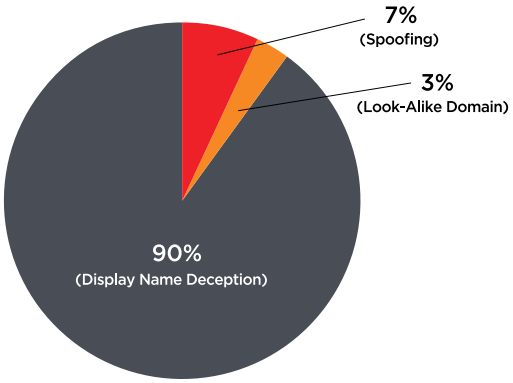
BEC Attacks By Impostor Techniques Bypassing ProofPoint



For organizations that use Proofpoint, 95% of attacks that went undetected used display name deception and 5% domain spoofing. There were no look-alike domain-based BEC attacks. As previously mentioned, this is likely because the Proofpoint customers tended to be larger and to enforce DMARC protection, which would prevent spoofing or look-alike domains (DMARC) or look-alike domains, but ineffective protection against display name deception.

BEC Attacks By Impostor Techniques Bypassing Office 365 Exchange Online Protection (EOP)

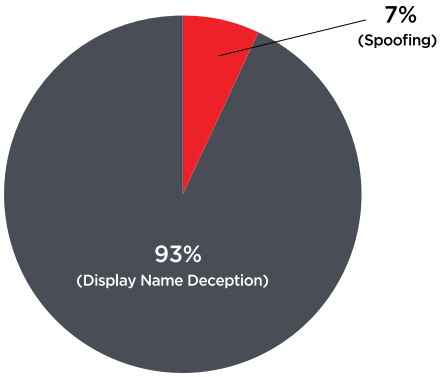
BEC Attacks Bypassing Microsoft EOP By Impostor Technique



For organizations that used Microsoft EOP with no third-party SEG, 90% of attacks were display name deception, 7% domain spoofs and 3% look-alike domain-based BEC Attacks. The distribution of attacks circumventing Microsoft EOP matches the overall percentages across all SEGs fairly closely.

BEC Attacks By Impostor Techniques Bypassing G-Suite

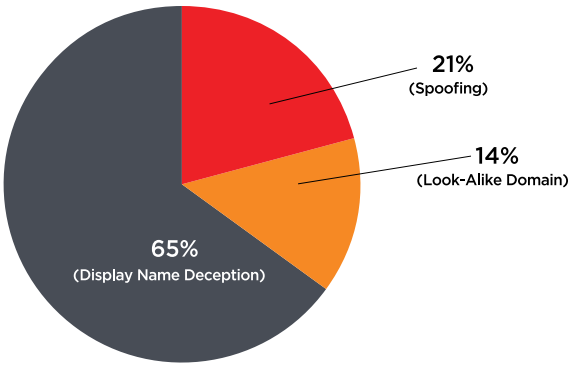
BEC Attacks Bypassing Google G Suite By Impostor Technique



For organizations that use Google G Suite with no third-party SEG, 93% of the attacks that were not blocked used display name deception and 7% domain spoofing. There were no look-alike domain-based BEC attacks that were not blocked. The lack of look-alike domains may have been due to the small sample size, although Google may have controls in place to detect such attacks.

BEC Attacks By Impostor Techniques Bypassing Cisco SEG

BEC Attacks Bypassing Cisco by Impostor Technique



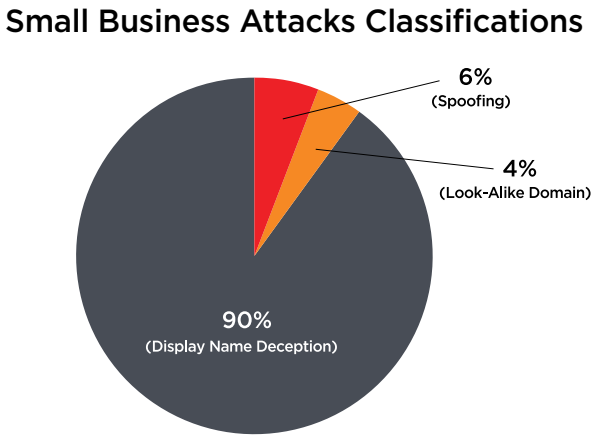
For organizations that use the CISCO SEG, 65% of attacks used display name deception, 21% domain spoofing and 14% were based on look-alike domains. This data shows a significantly higher occurrence of both domain spoofs and look-alike domain-based attacks with Cisco than other SEGs. Two thirds of the organizations that used a Cisco SEG were large and the remaining third were medium size organizations. However, none of the Cisco customers had a DMARC reject policy published for their primary email domain and enforced by the Cisco gateway. This explains the greater prevalence of domain spoofing. With regards to the high use of look-alike domains, we were not able to determine a cause and didn't have access to information about alternative security controls such as defensive domains registered, brand spoofing monitoring or take down activity by Cisco SEG organizations.

BEC Attacks By Impostor Techniques By Company Size

When analyzing the attacks, we wanted to see if certain types of attacks occur more often based on the size of the company. The following section breaks down the variation based on company size according to the following employee count:

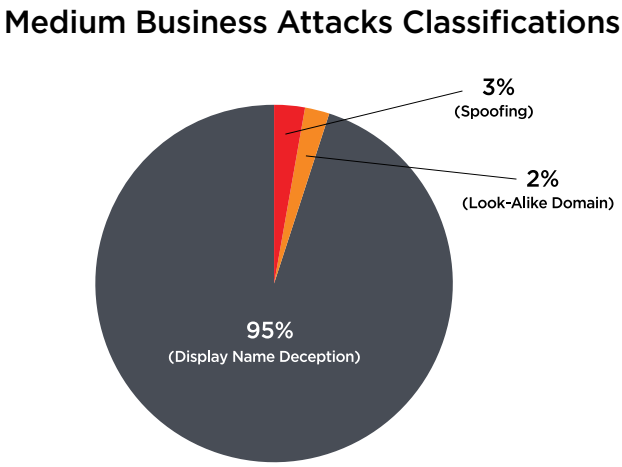
- Small: under 2000 employees
- Medium: 2,000-10,000 employees
- Large: 10,000+ employees

BEC Attacks By Impostor Technique, Targeting Small Businesses



For small businesses, 90% of BEC attacks observed used display name deception, 6% used domain spoofing and 4% used look-alike domains. Small businesses tended to use either Google G Suite or Microsoft EOP in conjunction with Office 365 as the SEG. None of the small organizations used DMARC email authentication on inbound email traffic. However, the occurrence of domain spoofing was relatively low. This may be because the additional payoff of investing time to spoof the domain of small organizations is not worth the potential reward, given how effective display name deception is.

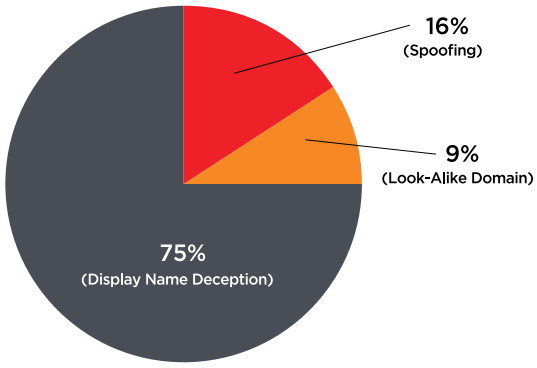
BEC Attacks By Impostor Technique, Targeting Medium Businesses



For medium businesses, 95% of BEC attacks used display name deception, 3% used domain spoofing and 2% used look-alike Domains. Again, the occurrence of domain spoofing and look-alike domains was relatively low.

BEC Attacks By Impostor Technique, Targeting Large Businesses

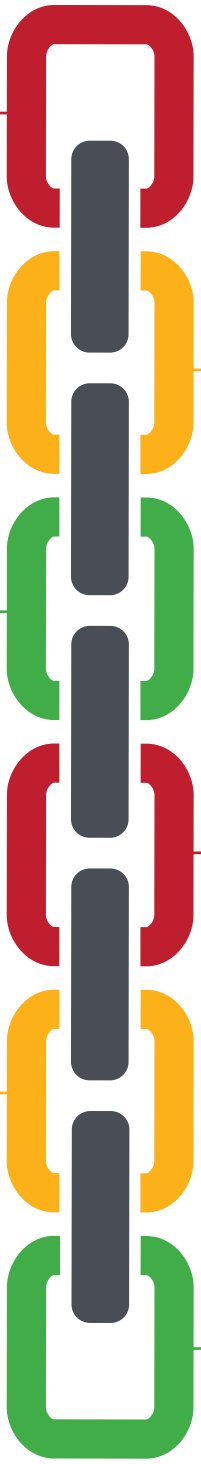
Large Business Attacks Classifications



For large businesses, 75% of BEC attacks used display name deception, 16% domain spoofing and 9% look-alike domains. The occurrence of domain spoofing and look-alike domains is relatively high compared to small and medium organizations.

What does the typical BEC process entail?

A typical BEC scam involves the following stages:



1 Hit Lists

The attacker performs reconnaissance and generates lists comprising the name of a sender (to be impersonated) and the name and email address of the recipient. These are typically are collected in batches of fifty to a hundred entries, each entry corresponding to the same type of relationship between the two entities – e.g., the impersonated sender is the CEO and the intended victim is the CFO. Sometimes, the person generating the list is not the person using it, and the list gets mailed around inside the organization.

2 Launch

The attacker launches the attack by transmitting initial requests to the users on the hit list. This rarely involves any customization beyond changing the display name. In particular, customized domains are hardly ever used, and the user name of the sender is almost always a generic name, such as execs@admin-messg-mail.com

3 Request

As intended victims respond, the criminal engages in a small number of exchanges, after which he makes a request – typically to perform a wire transfer to a supposed vendor. The median amount is $24,750, based on 61 observations made between October 25, 2017 and January 16, 2018.

4 Exfiltration

The wire transfers are not made to accounts belonging to the criminal, but typically, to mule accounts. Some of these accounts may have been compromised by the criminal (e.g., using a phishing attack) or otherwise be accessible by the attacker; for other accounts, the criminal has to involve the mule to have the money transferred out. The step of getting the money is fraught with peril to the criminal, as many banks detect anomalous transfers and block outgoing transfers. Not all banks are equally commonly used for mule accounts: Those banks that the criminals consider less risky will be favored, as will those with branch locations within reach of the mules.

5 Requesting Receipts

Without fail criminals request receipts for transfers they asked for – potentially as a way to prove to their colleagues that the money was transferred, or simply as a confirmation indicating that it is worth the effort to attempt to extract the funds.

6 Repeat

Whether the criminal manages to receive the requested funds or not, he is likely to try requesting another transfer. After all, a victim who did send money was certain of the identity of the party requesting the transfer, so why not? In some cases, successful criminals manage to receive transfers – often for gradually increasing amounts – for months, if not years.

About Agari

Agari, a leading cybersecurity company, is trusted by leading Fortune 1000 companies to protect their enterprise, partners and customers from advanced email phishing attacks. The Agari Email Trust Platform is the industry's only solution that 'understands' the true sender of emails, leveraging the company's proprietary, global email telemetry network and patent-pending, predictive Agari Trust Analytics to identify and stop phishing attacks. The platform powers Agari Enterprise Protect, which help organizations protect themselves from advanced spear phishing attacks, and Agari Customer Protect, which protects consumers from email attacks that spoof enterprise brands. Agari, a recipient of the JPMorgan Chase Hall of Innovation Award and recognized as a Gartner Cool Vendor in Security, is backed by Alloy Ventures, Battery Ventures, First Round Capital, Greylock Partners, Norwest Venture Partners and Scale Venture Partners. Learn more at http://www.agari.com and follow us on Twitter @AgariInc.

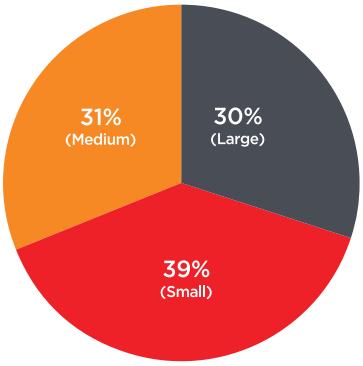
Acknowledgments

While the data in the report was sourced exclusively from Agari, several academic institutions, students and faculty contributed to the analysis and visualization of the data. We would like to acknowledge their contribution to this research:

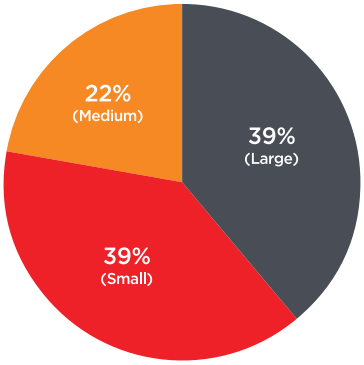
Enrico Bertini, Cristian Felix, Manfredi Roesler Franz, Jay Koven and Hossein Siadati of New York University; David Maimon of University of Maryland; Ana Ferreira of University of Porto, Portugal; and Yifan Tian of Embry-Riddle Aeronautical University.

Appendix: BEC Attack Sample Demographics

Company Size

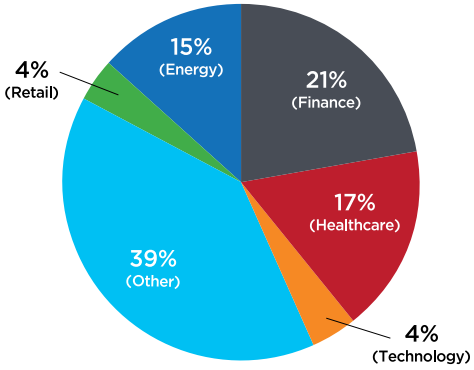


Small: under 2000 employees
Medium: 2,000-10,000 employees
Large: 10,000+ employees

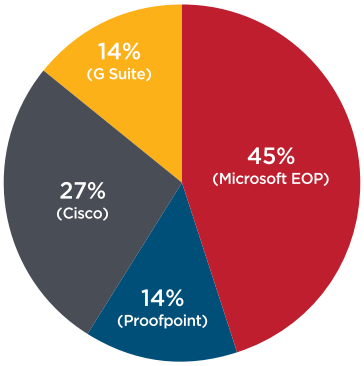


Small: Under $1B revenue
Medium: $1-5B revenue
Large: $5B+

Industry Vertical



SEG Demographics



Email Volume and Number of Attacks Analyzed

Mail Volume: 1,021,199,280
Attacks Analyzed: 1045

Note: The sample is sourced entirely from Agari Enterprise Protect customers and therefore has some bias towards organizations that have been previously attacked and purchased advanced email security controls to stop BEC attacks.