NCFTA®

The National Cyber-Forensics and Training Alliance

ONE TEAM, ONE GOAL. COMPANIES, GOVERNMENT, AND ACADEMIA WORKING TOGETHER TO NEUTRALIZE CYBER CRIME.

Business Email Compromise (BEC)

ABSTRACT

Business email compromise (BEC) causes billions of dollars in economic loss annually. In 2020, it was the costliest form of cybercrime reported by United States consumers.[1]To minimize the further enabling of this cybercriminal activity, individual organizations should assume responsibility and be cognizant of IT security and business relationship practices. The purpose of this white paper is to educate individuals and organizations on the evolution and impact of BEC and offer an accompanying guide on best practices in business and information technology to mitigate this threat.

ASSESSMENT

As the costliest type of cybercrime in 2020, BEC caused billions of dollars in economic loss.[2] The economic loss to victims has increased year-over-year since 2013, increasing 150% from 2018 to 2020, reaching $1.8 billion in 2020.[3] These statistics and amounts are only what is reported. The actual numbers are much higher. Cybercriminals capitalized on the COVID-19 global pandemic in 2020, and BEC has remained an effective means by which to divert funds from organizations.[4] Until organizations increase their overall awareness of evolving threats like BEC and proactively develop and implement basic countermeasures (like those outlined in this white paper and accompanying guide), BEC will, based on its current trajectory, continue its exponential growth with cybercriminals stealing hundreds of millions of dollars from businesses, many of which will be unable to recover from the financial loss.

Background, Definition, and Economic Impact of BEC

BEC is the use of a spoofed email address or a compromised email account to convince an individual or a business to send funds from their account to one owned or controlled by a cybercriminal. Cybercriminals perpetrating BEC are essentially social engineers who take advantage of a person's nature to address urgent requests promptly, especially when coming from the c-suite. They also take advantage of most employees' lack of basic security knowledge when it comes to email (i.e. recognizing a phishing message), how to evaluate a suspicious email's header, or how to identify domain spoofing. BEC emerged significantly in the United States in 2013, based on reports to the IC3 and the NCFTA. In the early days of BEC, the most common version was for scammers to impersonate individuals at the c-suite level and attempt to convince rank-and-file employees to transfer funds to an account belonging to an illegitimate party, many of whom were in China or Hong Kong. The next BEC version emerging in 2016 was vendor or invoice impersonation, which has risen significantly in popularity. Beginning in 2018, this version of BEC overtook executive impersonations in terms of both frequency and financial loss. BEC can be leveraged to redirect fund transfers across virtually any business relationship, making attractive targets of those who conduct high-value or frequent transfers, such as real estate brokers, corporate payroll departments, and vendor invoicing. BEC actors have adapted to early detection

[1] hxxps://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
[2] Ibid.
[3] hxxps://www.ic3.gov/Media/PDF/AnnualReport/2018_IC3Report.pdf; hxxps://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
[4] hxxps://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

methods and now typically first route payments to domestic bank accounts before sending funds abroad, making detection more difficult with multiple bank account "hops". These domestic beneficiaries, often unknowingly, launder proceeds from BEC via personal and business demand deposit accounts (DDAs) (e.g. checking, savings, etc.), gift cards, or cryptocurrency (primarily bitcoin).

Examples of BEC Emails

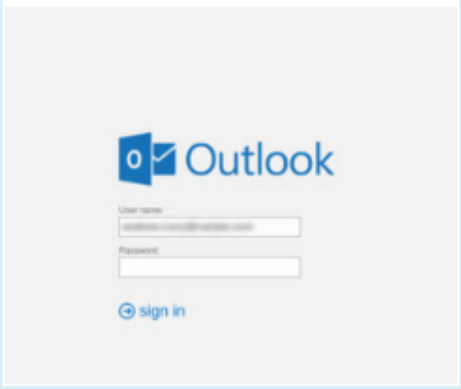
BEC indiscriminately affects businesses of all sizes, industries, and sectors. Many BEC actors strategically select victims (spear phishing) and carefully craft email language to lure victims into transferring funds to illegitimate parties. Others will target key employees (again, via spear phishing), seeking to capture login credentials that will enable the actor to gain access to the employee's email account. Untrained but "well-intentioned" employees will habitually answer emails quickly without pausing to evaluate the sender and/or without possessing the authority to question the change to established payment instructions.

> Please transfer $270,000 from the money market [redacted] to the wire transfer instructions attached. Give me a call at [redacted] for verbal authorization.

> Please be advised that we can't receive a check payment because our accounting department is currently working from home due to the COVID-19 pandemic across the globe. Will you be able to initiate a wire transfer to our operating bank account attached to this email? Your swift response is well appreciated.

Phishing remains the primary method of intrusion for most BEC attacks.[5] In the US, many BEC phishing emails contain poor English vocabulary, grammar, punctuation, and formatting, although cybercriminals are increasingly using translation and business correspondence services solicited from native English speakers, resulting in higher quality messages. These emails often include a direct request for *urgency* and *secrecy* in completing transactions, contain language imitating previous messages, and exploit existing trusted relationships or organization hierarchy.

The method of compromise for a more complex incident is often a phishing email containing a link directing the recipient to provide credentials in a spoofed login landing page. The use of malware, specifically Emotet, is a force multiplier because it can intercept an email thread and generate a reply within the thread, thereby making the phishing email appear legitimate.



In May 2020, NCFTA intelligence analysts analyzed numerous COVID-19-related BEC emails provided by the enterprise email security firm Agari. In some cases, cybercriminals posed as executives and urgently instructed administrative assistants and other support staff to purchase gift cards to give away to other employees or to use for donations.[6] In other incidents, fraudsters asked employees immediately to wire tens of thousands of dollars to illegitimate parties, claiming the funds were needed for COVID-19 medical support.

> I trust you are having a great day, I need you to cut a check for Covid-19 medical support today, The total amount is $37,420.35 Advise if i should forward the details now to get it done?

[5] hxxps://www.proofpoint.com/us/blog/cybersecurity-essentials/what-do-fight-business-email-compromise-bec-and-email-account
[6] hxxps://www.agari.com/email-security-blog/bec-gift-card-scams-covid-19/

Tactics, Techniques, and Procedures (TTPs)

Generally, every BEC incident involves email social engineering, or the use of deception, to convince a person to divulge information or commit an act to enable fraud. Cybercriminals often target organizations that are regularly processing high-value payments, but anyone can fall victim if they have not taken minimum efforts to recognize and mitigate this threat. These incidents can differ in terms of tradecraft and complexity, with some consisting of a social engineering email with poor grammar and others that use criminal proxy services that supply sophisticated malware enabling long-term illegitimate access to a computer network, or network intrusion. The latter can include the deployment of malware, zero-day exploits, phishing kits, keyloggers, and remote access trojans (RATs). In a simple incident, an email sender convinces an email recipient to transfer funds to an illegitimate party. In a complex incident, an email sender using a spoofed domain convinces an email recipient to open an attachment or a link, which infects the recipient's corporate computer network and/or steals user login credentials in order to establish persistent email account access. This persistent email access enables the criminal to monitor all future emails, looking for those that involve payments, invoices, settlements, deposits, or other payment-related communications.

Those using more sophisticated tactics, techniques, and procedures (TTPs) to conduct BEC have greatly benefited from access to commercialized cybercrime services and crime-as-a-service (CaaS) networks, enabling them to buy and use botnets, proxy services, RATs, and high-quality money laundering services. These resources have likely increased the ease, speed, and profitability of BEC. It has also enabled BEC criminals to gain access to a broader range of quality malware, hacked accounts, and stolen personally identifiable information (PII) from around the world. Malware allows actors to automate tasks ranging from account creation and domain registration to money laundering via cryptocurrency trading. It also enables criminals to gain access to high-value targets via phishing kits and crypters, and conduct email intrusion through thread hijacking.[7, 8]

Those conducting BEC attempt to hide their identities largely through legitimate privacy services, such as private email providers, encrypted or private messaging platforms, voice-over-internet-protocol (VoIP) phone numbers, cryptocurrency exchange platforms, privacy protection services for domain and business registration, and registrar's interpretation of the General Data Protection Regulation (GDPR) on non-disclosure of domain registrant information. Moderately competent BEC actors are increasingly able to conduct sophisticated impersonations using spoofed phone numbers, deepfake audio or video content, spoofed or typo-squatted domains, and digital fingerprint matching services, such as those offered by the underground marketplace Genesis Market, to perfectly imitate a legitimate business and social engineer their targets.[9]

BEC actors take advantage of systemic vulnerabilities, including the steady supply of stolen PII from breached organizations, common login credential reuse by employees, lack of adequate telecommunications security controls, and use of third-party services. Both legal and illegal services offer PII for sale, with the legal versions ranging from marketing/business lead generation to background check services, and the illicit services constituting a broad arena of underground marketplaces offering breached information for sale. Regardless of its source, such data can provide the private information needed for advanced social engineering.[10] Practices including mobile phone subscriber identity module (SIM) swapping and phone number porting has created additional vulnerabilities that enable BEC, such as the ability to circumvent two-factor authentication. Finally, actors can leverage popular third-party services to try to gain access to prospective victims and target entities ranging from tax accountants to IT service providers. From January 2014 to October 2019, the IC3 received complaints detailing more than $2.1 billion in actual losses targeting users of popular third-party service providers, such as Microsoft Office and Google G Suite.[11]

[7] A crypter is a software tool that encrypts or manipulates malicious payloads to make them difficult for security programs to detect.
[8] Email thread hijacking uses emails stolen from infected mail clients to spoof legitimate users and impersonates them in malspam email responses sent to email addresses from the original stolen email.
[9] Fingerprint matching services allow victims' stolen digital profiles and unique digital fingerprints to be purchased and used to exactly imitate a user's device.
[10] Lead Generation Services are a legitimate service typically used by sales departments to identify and qualify potential customers for their business, who often trade in leaked or breached information.
[11] hxxps://www.ic3.gov/media/news/2020/200707-4.pdf

Malware Used in BEC

The best-known types of malware used in BEC attacks are remote access trojans (RATs) and information stealers; the most common are:

AgentTesla

AgentTesla is a RAT, primarily spread through malicious attachments in phishing emails, with keylogging capabilities allowing malicious actors to steal credentials from browsers, mail clients, and file transfer protocols. The trojan captures screenshots and steals clipboard data from victim computers, exfiltrating data to its C2 servers using SMTP and FTP protocols.

AZORult

AZORult is an information stealer that obtains a user's browsing history, cookies, passwords, cryptocurrency wallets, and other credentials. The malware is primarily distributed using spear-phishing emails or as a secondary payload in succession of an exploit kit.

Nanocore

NanoCore is a modular RAT that was first developed in 2013. The RAT is primarily distributed via malspam and phishing emails. NanoCore typically gathers user credentials including ones stored in browsers, file transfers, and email clients. These credentials along with other stolen data are sent to the attacker's command and control server. A COVID-19 spam email campaign launched by threat actors in early 2020 lured victims, via COVID-19 updates, to open a malicious ZIP file that delivered the malware to the victim computer.[13]

Raccoon Stealer

Raccoon Stealer steals login credentials, credit card numbers, cryptocurrency wallets, and browser data, and is typically delivered using exploit kits or phishing campaigns. In April 2019, according to the phishing defense and mitigation company, Cofense, Raccoon Stealer was used in a BEC attack where malicious actors sent a phishing email containing a malicious IMG file to a financial institution, which dropped Raccoon Stealer into the victim's network.[14]

NetWire

The NetWire RAT emerged in 2012 and is a commercially available malware, typically spread via phishing emails. The RAT is able to log user keystrokes, steal credentials, and download additional payloads. Around January 2020, threat actors launched a campaign in which businesses received sales-themed emails with IMG attachments that dropped the NetWire RAT onto the victim computer.[12]

DarkComet

DarkComet is a free tool developed in 2011. The malware is typically distributed using malspam or drive-by downloads. It includes features that allow it to remotely control any webcams or microphones, access the full file directory, evade antivirus, lock the computer, hide the desktop, log keystrokes, and fully control the mouse and keyboard.

njRAT

njRAT, or Bladabindi trojan, was first discovered in 2013. The RAT is able to lock the victim's screen, steal saved credentials and passwords, log keystrokes, and grab saved cryptocurrency addresses. Threat actors also commonly use this malware to conduct Distributed Denial of Service (DDoS) attacks against their victims. njRAT is commonly distributed using malspam and drive-by downloads.

Lokibot

Lokibot is an information stealer used to obtain credentials, such as usernames, passwords, and cryptocurrency wallets. It affects Windows and Android operating systems, typically infecting a machine through malspam attachments, malicious third party mobile applications, or malicious websites. Once the user interacts with these malicious entities, the malware calls out to its C2 domains to deliver the final PHP payload.

[12] hxxps://securityintelligence.com/posts/new-netwire-rat-campaigns-use-img-attachments-to-deliver-malware-targeting-enterprise-users/; hxxps://exchange.xforce.ibmcloud.com/collection/NetWire-RAT-Delivered-via-IMG-Attachment-ceefd03401f5c38489b0b363db20c7c7
[13] hxxps://blog.talosintelligence.com/2020/02/coronavirus-themed-malware.html; Coronavirus (COVID-19) Cyber Threats, TLP AMBER
[14] hxxps://cofense.com/raccoon-stealer-found-rummaging-past-symantec-microsoft-gateways/

Know Your Customer (KYC) and Customer Due Diligence (CDD)

The Currency and Foreign Transactions Reporting Act of 1970, also referred to as the Bank Secrecy Act (BSA), requires US financial institutions to assist government agencies to identify and avert money laundering.[15] The Financial Crimes Enforcement Network (FinCEN) of the US Department of the Treasury (USDT) requires financial institutions to practice effective know-your-customer (KYC) or customer due diligence (CDD) solutions. Financial institutions must adhere to the following requirements in establishing a relationship with a customer: "(1) customer identification and verification, (2) beneficial ownership identification and verification, (3) understanding the nature and purpose of customer relationships to develop a customer risk profile, and (4) ongoing monitoring for reporting suspicious transactions and, on a risk-basis, maintaining and updating customer information."[16]

Although unique to the financial sector, these specific regulatory requirements represent best practices in terms of KYC or CDD procedures that, if voluntarily adopted, even minimally, could help any business mitigate the risk of future BEC events. A secondary benefit of a strong CDD policy is avoiding potential violations of other regulations unfamiliar to the business. For example, if a person or an organization financially or materially transacts with an entity listed in the Specially Designated Nationals and Blocked Persons List (SDN), maintained by the Office of Foreign Assets Control (OFAC) of the USDT, they may face penalties, such as fines, sanctions, or other criminal proceedings.[17] Another example is the Export Administration Regulations (EAR), administered by The Bureau of Industry and Security of the United States Department of Commerce, whereby a person or an organization may need to secure a license to export products or services listed in the Commerce Control List and verify the destination, recipient, and end-use/purpose.[18]

The collection and verification of business relationship or CDD information can be challenging, but the benefits should outweigh the effort required. In Q1 2021, the highest amount of funds that were at risk of loss at a single BEC victim was $3,000,000. A CDD compliant organization should develop, implement, and refine standard operating procedures (SOPs) as they relate to invoices and payments, ***especially those that involve a change to previously established payment routing***. They then must educate and train employees to follow the SOPs, hold employees accountable, and detect and counter actions by customers attempting to elude these measures. A BEC incident involves at least two parties (e.g. a business and a vendor) but could also involve a third party that services the transacting parties such as an attorney or closing agent. Even one party pursuing measures to collect or verify more information about a change to a transaction process received via email can help prevent significant economic losses from such an incident.

Closing

Standards across industries exist for many reasons to include ensuring safety, maintaining consistency, meeting regulatory requirements, and facilitating interactions between organizations. Standards are especially important when they can help businesses improve processes to overcome new risks, such as mitigating BEC.

The accompanying guide contains practices in both business and information technology, sourced from NCFTA partners in private industry and law enforcement, to help mitigate the threat of BEC. The data gathered indicates that standard business and IT security practices should be adopted to help significantly reduce risk of the costliest form of cybercrime reported by US consumers, including, but not limited to, multi-layered authentication and transaction verification procedures; regular education, training, and testing of employees; incident response planning, practice, and refinement; and sound information security standards.

[15] hxxps://www.fincen.gov/resources/fincens-mandate-congress
[16] Ibid.
[17] hxxps://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists
[18] hxxps://www.trade.gov/us-export-regulations-0