Microsoft

The Confidence Game

Shifting Tactics Fuel Surge in Business Email Compromise

Microsoft Threat Intelligence

Cyber Signals

May 2023

Microsoft's Digital Crimes Unit has observed a **38 percent increase** in Cybercrime-as-a-Service targeting business email between 2019 and 2022.

Introduction

Business email fraud continues to rise, with the Federal Bureau of Investigation (FBI) reporting more than 21,000 complaints with adjusted losses over $2.7 billion. Microsoft has observed an increase in sophistication and tactics by threat actors specializing in business email compromise (BEC), including leveraging residential internet protocol (IP) addresses to make attack campaigns appear locally generated.

This new tactic is helping criminals further monetize Cybercrime-as-a-Service (CaaS) and has caught federal law enforcement's attention because it allows cybercriminals to evade "impossible travel" alerts used to identify and block anomalous login attempts and other suspicious activity.

We are all cybersecurity defenders.

Security Snapshot

Snapshot data represents **BEC attempts detected and investigated** by Microsoft Threat Intelligence Digital Crimes Unit (DCU) April 2022 to April 2023. Unique phishing URL takedowns directed by DCU are between May 2022 to April 2023.[1]

35 Million
Annual

156,000
Daily

417,678
Phishing URL Takedowns

Inside the rise of BulletProftLink's industrial-scale BEC service

Cybercriminal activity around business email compromise is accelerating. Microsoft observes a significant trend in attackers' use of platforms like BulletProftLink, a popular service for creating industrial-scale malicious email campaigns. BulletProftlink sells an end-to-end service including templates, hosting and automated services for BEC. Adversaries using this CaaS receive credentials and the IP address of the victim.

BEC threat actors then purchase IP addresses from residential IP services matching the victim's location creating residential IP proxies which empower cybercriminals to mask their origin. Now, armed with localized address space to support their malicious activities in addition to usernames and passwords, BEC attackers can obscure movements, circumvent "impossible travel" flags, and open a gateway to conduct further attacks. Microsoft has observed threat actors in Asia and an Eastern European nation most frequently deploying this tactic.

Impossible travel is a detection used to indicate that a user account might be compromised. These alerts flag physical restrictions that indicate a task is being performed in two locations, without the appropriate amount of time to travel from one location to the other.

The specialization and consolidation of this sector of the cybercrime economy could escalate the use of residential IP addresses to evade detection. Residential IP addresses mapped to victim locations at scale provide the ability and opportunity for cybercriminals to gather large volumes of compromised credentials and access accounts. Threat actors are using IP/proxy services that marketers and others may use for research to scale these attacks.

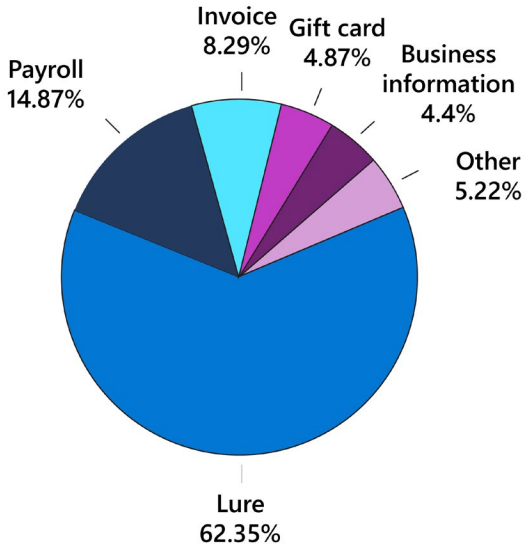
One IP service provider, for example, has 100 million IP address that can be rotated or changed every second.

While threat actors use phishing-as-a-service like Evil Proxy, Naked Pages, and Caffeine to deploy phishing campaigns and obtain compromised credentials, BulletProftLink offers a decentralized gateway design, which includes Internet Computer public blockchain nodes to host phishing and BEC sites, creating an even more sophisticated decentralized web offering that's much harder to disrupt. Distributing these sites' infrastructure across the complexity and evolving growth of public blockchains makes identifying them, and aligning takedown actions, more complex. While you can remove a phishing link, the content remains online, and cybercriminals return to create a new link to existing CaaS content.

Successful BEC attacks cost organizations hundreds of millions of dollars annually. In 2022, the FBI's Recovery Asset Team initiated the Financial Fraud Kill Chain on 2,838 BEC complaints involving domestic transactions with potential losses of over $590 million.

Business Email Compromise Phishing Mail by Type

Data represents a snapshot of BEC phishing by type January 2023 through April 2023



Threat briefing

Although the financial implications are significant, wider long-term damages can include identity theft if personally identifiable information (PII) is compromised, or loss of confidential data if sensitive correspondence or intellectual property are exposed in malicious email and message traffic.

Top targets for BEC are executives and other senior leaders, finance managers, human resources staff with access to employee records like Social Security numbers, tax statements, or other PII. New employees perhaps less likely to verify unfamiliar email requests are also targeted. Nearly all forms of BEC attacks are on the rise. Top trends for targeted BEC attacks include lure, payroll, invoice, gift card, and business information.

BEC attacks stand apart in the cybercrime industry for their emphasis on social engineering and the art of deception. Instead of exploiting vulnerabilities in unpatched devices, BEC operators seek to exploit the daily sea of email traffic and other messages to lure victims into providing financial information, or taking a direct action like unknowingly sending funds to money mule accounts, which help criminals perform fraudulent money transfers.

Unlike a "noisy" ransomware attack featuring disruptive extortion messages, BEC operators play a quiet confidence game using contrived deadlines and urgency to spur recipients, who may be distracted or accustomed to these types of urgent requests. Instead of novel malware, BEC adversaries align their tactics to focus on tools improving the scale, plausibility, and inbox success rate of malicious messages.

Although there have been several high-profile attacks that leverage residential IP addresses, Microsoft shares federal law enforcement and other organizations' concern that this trend can be rapidly scaled, making it difficult in more cases to detect activity with traditional alarms or notifications.

Variances in login locations are not inherently malicious. For example, a user might access business applications with a laptop via local Wi-Fi, and simultaneously be signed into the same work apps on their smartphone via a cellular network. For this reason, organizations can tailor impossible travel flag thresholds based on their risk tolerance. However, the industrial scale of localized IP address space for BEC attacks creates new risks for enterprises, as adaptive BEC and other attackers increasingly take the option of routing malicious mail and other activity through address space near their targets.

Recommendations:

Maximize security settings protecting your inbox: Enterprises can configure their email systems to flag messages sent from external parties. Enable notifications for unverified email senders. Block senders with identities you cannot independently confirm and report their mails as phishing or spam in email apps.

Set up strong authentication: Make email harder to compromise by turning on multifactor authentication, which requires a code, PIN, or fingerprint to log in as well as a password. MFA-enabled accounts are more resistant to the risk of compromised credentials and brute-force login attempts, regardless of address space attackers use. Passwordless technology further strengthens security by verifying identities on the device, rather than passing user credentials through a vulnerable online connection.

Train employees to spot warning signs: Educate employees to spot fraudulent and other malicious emails, such as a mismatch in domain and email addresses, and the risk and cost associated with successful BEC attacks.

Defending against attacks

Fighting business email compromise requires vigilance and awareness

Although threat actors have created specialized tools to facilitate BEC, including phishing kits and lists of verified email addresses targeting C-suite leaders, accounts payable leads, and other specific roles, enterprises can employ methods to preempt attacks and mitigate risk.

For example, a domain-based message authentication, reporting, and conformance (DMARC) policy of "reject" provides the strongest protection against spoofed email, ensuring that unauthenticated messages are rejected at the mail server, before delivery. Additionally, DMARC reports provide a mechanism for an organization to be made aware of the source of an apparent forgery, information that they would not normally receive.

Although organizations are a few years into managing fully remote or hybrid workforces, rethinking security awareness in the hybrid work era is still needed. Because employees are working with more vendors and contractors, thereby receiving more "first seen" emails, it's imperative to be conscious of what these changes in work rhythms and correspondence mean for your attack surface.

Threat actors' BEC attempts can take many forms—including phone calls, text messages, e-mails, or social media messages. Spoofing authentication request messages and impersonating individuals and companies are also common tactics.

A good first defensive step is strengthening policies for accounting, internal controls, payroll, or human resource departments on how to respond when requests or notification of changes regarding payment instruments, banking, or wire transfers are received. Taking a step back to sideline requests that suspiciously do not follow policies, or contacting a requesting entity through its legitimate site and representatives, can save organizations from staggering losses.

BEC attacks offer a great example of why cyber risk needs to be addressed in a cross-functional way with executives and leaders, finance employees, human resource managers, and others with access to employee records like Social Security numbers, tax statements, contact information, and schedules, alongside IT, compliance, and cyber risk officers.

Microsoft's DCU works to disrupt cybercriminal networks and infrastructure using technology, forensics, civil actions, criminal referrals, and public and private partnerships.

Recommendations:

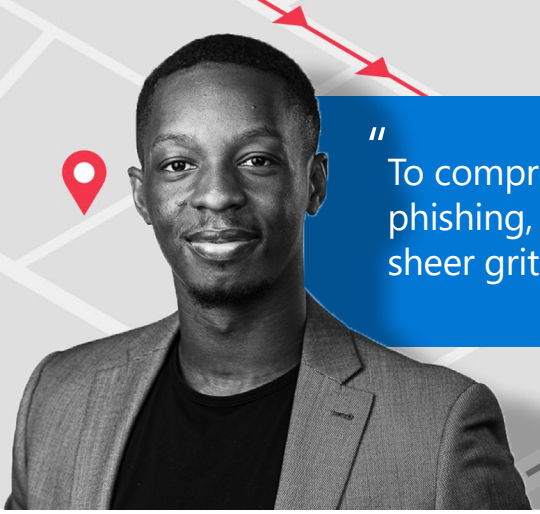
Use a secure email solution: Today's email cloud platforms use AI capabilities like machine learning to enhance defenses, adding advanced phishing protection and suspicious forwarding detection. Cloud apps for email and productivity also offer the advantages of continuous, automatic software updates and centralized management of security policies.

Secure identities to prohibit lateral movement: Protecting identities is a key pillar to combating BEC. Control access to apps and data with Zero Trust and automated identity governance.

Adopt a secure payment platform: Consider switching from emailed invoices to a system designed to authenticate payments.

Hit pause and use a phone call to verify financial transactions: A quick phone conversation to confirm something is legitimate is well worth the time, instead of assuming with a quick reply or click, which could lead to theft. Establish policies and expectations reminding employees it's important to contact organizations or individuals directly—and not use information supplied in suspect messages—to double-check financial and other requests.

Expert Profile



> "To compromise email, credential phishing, social engineering, and sheer grit is all that's required."

Simeon Kakpovi

Senior Threat Intelligence Analyst, Microsoft Threat Intelligence

Simeon Kakpovi initially wanted to be a doctor but soon realized that wasn't his calling. "I switched my major a few times and ended up in information systems. I landed on cybersecurity because my mentors were in the field."

As a sophomore at Howard University, he took additional cybersecurity classes at a local community college, ultimately leading him to the Lockheed Martin Cyber Analyst Challenge. "They mailed us a thumb drive with 80 gigabytes of data. What happened next is some of the most fun I've ever had."

The challenge required participants to analyze a full cyberintrusion using packet capture and memory files. "Through that process, I realized the big picture of cybersecurity and thought, 'I would love to do this for a living.'"

That led to an internship at Lockheed Martin and to co-creating the cyberskilling game KC7. "A lot of cybersecurity classes are taught with acronyms and vague concepts because they don't have access to actual data. That creates circular problem because you can't get the skills until you get the job, but you can't get the jobs unless you have the skills."

Today, Simeon leads Microsoft's team of analysts tracking more than 30 Iranian groups. Though distinct in motivation and activity, Simeon notes all Iranian actors share a common trait: tenacity.

"We've consistently found that Iran is persistent and patient, willing to spend effort, time, and resources to compromise their targets. Iranian-linked actors offer a good reminder that you don't have to use zero-day software exploits or novel offensive techniques to be successful. To compromise email, credential phishing, social engineering, and sheer grit is all that's required."

"Social engineering isn't always as simple as it might appear. We've seen threat actors leverage the personal information revealed on social media to lure victims during social engineering campaigns."

For example, Crimson Sandstorm uses fake social media profiles (honey pots) targeting individuals based on jobs listed on their LinkedIn profile. Then over a period of a few months, they attempt to establish romantic relationships using intelligence gathered from public profiles to build trust and rapport, eventually sending BEC targets malicious files disguised as videos or surveys. However, because these relationships were developed over a long period of time, targets were more likely to ignore security alerts when they executed these files.

Simeon observes that Iranian threat actors are motivated by a wide scope of reasons. "When tracking Mint Sandstorm and attacks on agencies working with governments, sometimes nuclear policy is the driver. With think tanks or academic institutions, publishing information critical of the Iranian government can raise the ire of a threat actor group. That suggests that they may know how the US or other Western countries will position themselves in terms of policy and target individuals with information that's useful to their government."

[1] Methodology: For snapshot data, Microsoft platforms including Microsoft Defender for Office, Microsoft Threat Intelligence, and Microsoft Digital Crimes Unit (DCU) provided anonymized data on device vulnerabilities and data on threat actor activity and trends. In addition, researchers used data from public sources, such as the Federal Bureau of Investigation (FBI) 2022 Internet Crime Report and Cybersecurity & Infrastructure Security Agency (CISA). The cover stat is based on Microsoft DCU business email Cybercrime-as-a-Service engagements 2019 through 2022.