



| Flash |

New BEC Campaign Set to Target Western Countries

F-2024-01-23a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Ransomware, Deep and Dark Web

January 23, 2024

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EST) on January 23, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | New BEC Campaign Set to Target Western Countries

> Key Findings

- ZeroFox has recently observed the announcement of a new Business Email Compromise (BEC) campaign set to target Western states that promises affiliates substantial monetary profit.
- Despite advertisements seeking BEC associates being relatively rare in dark web forums, this is the second to be observed by ZeroFox in 2024.
- There is a roughly even chance that organizations face a heightened threat from BEC attacks in 2024 due to an increase in attacks and the continual diversification of techniques, tactics and procedures (TTPs).

| Details

On January 22, 2024, ZeroFox observed the announcement of a potential new BEC campaign in the dark web forum exploit[.]in. The declaration was made by well-regarded English-speaking threat actor “general7”, who is seeking partners that have “first hand” access to email accounts belonging to corporate entities based in Canada, the United States, the United Kingdom, and specific European Union countries.

- BEC is a type of cyberattack that enables the threat actor to gain unauthorized access to a personal or organizational email account before socially engineering victims. Threat actors—who are usually financially-motivated—leverage threat vectors such as account compromise and CEO or vendor impersonation to elicit fraudulent payment or data theft from unsuspecting victims.

General7 claimed to have significant experience in conducting BEC attacks and also alluded to their extensive network of contacts that assist in attack facilitation.

- An established network of affiliates very likely confirms general7's consolidated ability to conduct successful BEC campaigns. The role of affiliates very likely differs depending upon the campaign specifics but could include specialists proficient in ransomware deployment, data encryption, or various social engineering methods.

**Partnership with Business Email compromise - Professional work - Proof**
By general7, 7 hours ago in [Spam] - mailings, databases, responses, mail-dumps, software

**general7**
megabyte
● ● ●
Paid registration
7
86 posts
Joined
10/27/20 (ID: 110072)
Activity
вирусология / malware

Posted 7 hours ago

I need people who have first hand corporate email access, from networks/spam etc does not matter. Countries: ca/usa/some eu/gb - and we can look at anything else you have as long as it meets our criteria.

I have been doing this for a very long time. I have success because i have a good network that i can trust.

Amounts that are done will start from 100k and go to amounts that are over 5kk and much higher.

I can show proof if i think you are serious. You can pm me your please TG if you want to discuss.

i can buy boxes as well from 1\$

Exploit[.]in post advertising new BEC campaign

Source: ZeroFox Intelligence

The announcement claims that the campaign is set to generate substantial monetary profit, starting at "100k" and reaching as high as "5kk" (very likely USD 100,000 – 5,000,000). It is not made clear how such profit would be divided amongst associates.

- These figures are likely unrealistic and an attempt to attract attention from credible potential affiliates. However, the threat actor's forum reputation (and their claim that proof of previous successes can be shown privately) indicate a small probability that such financial success is possible.
- BEC attacks are very likely becoming an increasingly lucrative attack vector for threat actors, with the median transaction observed during attacks reported to have almost tripled over the past five years to approximately USD 50,000.¹
- Attacks are also becoming increasingly common, reportedly making up the vast majority of cyberattacks.²

In the absence of the mention of malware, it is likely that the campaign will leverage traditional BEC TTPs such as using credential recycling and account takeovers to gain initial access to corporate email accounts. The threat actor can then proceed with numerous social engineering methods to accomplish predetermined, financially-motivated ends.

- During 2023, BEC attackers almost certainly adopted progressively more diverse TTPs. Threat actors increasingly used spoofed email addresses or stolen credentials to target supply chain entities associated with their primary target. This enables them to leverage sensitive information to enhance credibility prior to conducting an impersonation attack, such as seeking payment for an outstanding legitimate invoice.

Despite advertisements seeking BEC associates being relatively rare in dark web forums, this is the second instance ZeroFox has observed in 2024. On January 8, untested threat actor "ke56" posted in three languages (English, Russian, and Chinese) in the RAMP forum seeking an associate with malware experience for a BEC campaign.

- This is not typical for such advertisements but coincides with ke56's claim that the campaign will involve infecting victims' networks with malware.

¹ <https://www.tripwire.com/state-of-security/business-email-compromise-statistics>

² <https://www.verizon.com/business/resources/Te34/reports/2023-data-breach-investigations-report-dbir.pdf>

There is a roughly even chance that organizations will face an increased threat from BEC attacks in 2024, reflected by the upward trajectory in the number of attacks and financial impacts. Threat actors will very likely continue to enhance and diversify their social engineering TTPs, leveraging topical lures to target unsuspected aspects of an organization or its supply chain.

| Recommendations

- Disable the use of legacy email protocol that may enable the bypassing of multi-factor authentication (MFA) security.
- Enable the use of domain-based message authentication, reducing the likelihood of your organization's domain being used to dispatch phishing communications.
- Adopt a secure payment platform able to authenticate and legitimize invoices and payments.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Implement secure password policies with phishing-resistant MFA, complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform detection of malicious activity and associated TTPs and Indicators of Compromise (IOCs).
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site or cloud servers at least once per year—and ideally more frequently.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management system and ensure all business IT assets are updated with the latest software as quickly as possible.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Configure ongoing monitoring for Compromised Account Credentials.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%