The Computer & Internet Lawyer

Volume 37 ▲ Number 8 ▲ SEPTEMBER 2020

Ronald L. Johnston, Arnold & Porter, LLP, Editor-in-Chief

FBI Warns Companies to Be Vigilant as COVID-19-Themed BEC Scams Continue to Grow

By Jeffrey N. Rosenthal and David J. Oberly

As the COVID-19 pandemic continues to cause chaos across the globe, cyber attacks seeking to exploit the crisis on the rise as well. In particular, the frequency of COVID-19 business email compromise ("BEC") schemes – a particularly low-tech, but highly damaging, type of cyber scam – has risen significantly since the onset of the global health emergency, so much so it prompted the Federal Bureau of Investigation ("FBI") to issue two alerts warning businesses of the growing threat. As such, businesses must take appropriate measures to effectively mitigate the enhanced risk posed by BEC fraud, which is expected to increase even further in the coming weeks and months.

BEC Scams: Low-Tech Fraud with Devastating Consequences

BEC scams, also known as "CEO fraud" and "man-in-the-email scams," involve tricking victims – often those who perform legitimate funds transfers – to make unauthorized wire transfers or send funds directly to the coffers of cyber criminals. The typical BEC scheme originates with the theft of a corporate executive's credentials by phishing or other means. With those credentials in hand, cyber criminals will then impersonate the executive, sending urgent messages to lower level employees with requests to transfer or wire funds to bank accounts.

According to the FBI's Internet Crime Report,[1] the bureau received approximately 24,000 complaints concerning BEC fraud last year, with losses totaling $1.7 billion – accounting for nearly half of all cybercrime-related losses in 2019. While ransomware frequently garners headlines due to the operational disruption caused by these attacks, cyber criminals have had much more financial success with BEC scams, netting at least 17 times more per incident ($75,000) than ransomware ($4,400).

It should not come as a surprise, then, that BEC was far and away the top source of cyber-related financial loss in 2019. Moreover, BEC fraud is a relatively low-tech and low-cost scam that provides criminals with the ability to focus on high-value targets and high returns, all with minimal risk. This conflux of factors makes BEC scams particularly popular with cyber criminals.

Jeffrey N. Rosenthal, a partner in the Philadelphia office of Blank Rome LLP, may be contacted at *rosenthal-j@blankrome.com*. **David J. Oberly**, an associate in the firm's Cincinnati office, may be contacted at *doberly@blankrome.com*.

Recent Proliferation of BEC Scams Tied to COVID-19

Over the years, cyber criminals have become more advanced and sophisticated in their attack techniques and methods, leading them to consider the psychological aspect of their scams.

In particular, fraudsters have become extremely adept at exploiting current events – such as terrorist attacks and natural disasters – and the impact on the targets of their scams. As the COVID-19 crisis has continued to deepen, cyber criminals have adjusted their BEC scams to place a greater emphasis on COVID-19 and enhance the social engineering aspect of their attacks. For example, BEC fraudsters are impersonating vendors and requesting payment outside the normal course of business, citing reasons relating to COVID-19 for the request. Similarly, cyber criminals claiming to be company executives are emailing lower-level employees requesting urgent, confidential wire transfers to cover costs due to unexpected issues arising from COVID-19.

FBI Sounds the Alarm on Anticipated Rise in COVID-19 BEC Schemes

Recently, the FBI issued an alert[2] warning that cyber criminals are actively exploiting the uncertainty surrounding the COVID-19 pandemic to further the effectiveness of their BEC scams. In particular, the FBI reports it recently observed a significant spike in BEC fraud targeting organizations purchasing personal protective equipment or other supplies needed in the fight against COVID-19. The FBI further cautions businesses to anticipate an even greater rise in BEC schemes tied to the COVID-19 pandemic moving forward.

To guard against this heightened risk of BEC scams, the FBI advises businesses and their personnel to be on the lookout for the following red flags:

- Unexplained urgency;
- Last-minute changes in wire instructions or recipient account information;
- Last-minute changes in established communication platforms or email account addresses;
- Communications done only through email and a refusal to communicate over the telephone or through online voice/video platforms;
- Requests for advanced payment of services when not previously required; and
- Requests from employees to change direct deposit information.

In addition, the FBI recommends the following tips to help companies further mitigate the risk of falling victim to BEC scams:

- Be skeptical of any last-minute changes in wiring instructions or recipient account information;
- Verify any changes and information via the contact the company has on file, and do not contact the vendor through the number provided via email;
- Ensure the URL in emails is associated with the business it claims to be from;
- Be alert to hyperlinks that may contain misspellings of the actual domain name; and
- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's email address appears to match who it is coming from.

FBI Issues Additional Warning on Cloud-Based BEC Attacks

The FBI also issued a second alert[3] to advise that cyber criminals are targeting organizations that use popular cloud-based email services – i.e., hosted subscription services that enable users to conduct business via tools such as email, shared calendars, online file storage, and instant messaging – with an increasing number of BEC scams. The FBI notes that in doing so, cyber criminals are using tailored phishing kits designed to mimic and impersonate cloud-based email services, making these scams extremely hard to detect as fraudulent. Moreover, the FBI also reports a troubling trend of cyber criminals accessing the address books of compromised accounts to identify new targets and send phishing emails, allowing a single successful email account compromise at one business to be pivoted to multiple victims within an industry.

To mitigate the risk of cloud-based BEC scams, the FBI recommends businesses implement the following practices for employees and other end users:

- Enable multi-factor authentication for all email accounts;
- Verify all payment changes and transactions in person or via a known telephone number; and

- Educate employees about BEC scams, including preventative strategies such as how to identify phishing emails and how to respond to suspected compromises.

The FBI also recommends that businesses work with their IT administrators to implement the following practices to further mitigate the threat of cloud-based BEC fraud:

- Prohibit automatic forwarding of email to external addresses;
- Add an email banner to messages coming from outside your organization;
- Prohibit legacy email protocols, such as POP, IMAP, and SMTP, that can be used to circumvent multi-factor authentication;
- Ensure changes to mailbox login and settings are logged and retained for at least 90 days;
- Enable alerts for suspicious activity, such as foreign logins; and
- Enable security features that block malicious email, such as anti-phishing and anti-spoofing policies.

Conclusion

BEC fraud has continued to grow, evolve, and become significantly more sophisticated and deceptive in recent years. As such, BEC scams now represent one of the most destructive types of security threats faced by companies across all industries. And like many other types of security threats, the prevalence of BEC scams has risen precipitously as the COVID-19 pandemic has progressed, with fraudsters aiming to exploit the expanding scope of the crisis. Moving forward, these same groups will continue to target businesses and individuals with new BEC schemes for the foreseeable future.

Companies must therefore remain vigilant and take active steps to mitigate the burgeoning security threat posed by BEC scams. At the same time, as cyber threats continue to develop and evolve at a rapid pace, companies must also stay current on the latest trends and developments to stay ahead of the curve and effectively defend against these risks, which will remain active and substantial for the duration of the current public health crisis.

Notes

1. Federal Bureau of Investigation, Internet Crime Complaint Center, "2019 Internet Crime Report," *available at https://pdf.ic3.gov/2019_IC3Report.pdf.*
2. Federal Bureau of Investigation, "FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic," April 6, 2020, *available at https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic.*
3. Federal Bureau of Investigation, Internet Crime Complaint Center, "Cyber Criminals Conduct Business Email Compromise Through Exploitation of Cloud-Based Email Services, Costing US Businesses More Than $2 Billion," April 6, 2020, *available at https://www.ic3.gov/media/2020/200406.aspx*.