RrSG Approaches to BEC Scams/CEO Fraud

What is the problem?

Business Email Compromise (BEC) is a type of fraud which occurs when an employee or civil servant authorized to make payments is tricked into paying a fake invoice or making an unauthorized transfer out of the business or governmental organization account.

What is the damage?

The United States Federal Bureau of Investigation (FBI) found that BEC scams cost victims a combined total of USD$26 billion in losses over three years. Those damages occurred across 166,349 separate incidents reported to the FBI between June 2016 and July 2019.[1]

With the sudden move to remote working and reliance on digital means of communication imposed by the worldwide pandemic, BEC attacks have surged since early 2020.

Medium

In the majority of BEC fraud cases, criminals rely on emails. They may also place phone calls in lieu of emails but those are clearly out of the scope of the ICANN RrSG.

Another distinction needs to be made between fraud emails using an address of a service provider (such as gmail.com, outlook.com, fastmail.fm) and those using a custom domain name.

In the first case, registrars will be unable to assist, as the relevant party is the email platform operator. When the criminals use a custom domain name, registrars may be of assistance.

Reporting

Domain names used for BEC typically either do not resolve or forward to the legitimate website of the impersonated party. At first glance, those domain names do not appear to be used illegally. It is only their usage in connection with an email service that is illegal, which is why it is important for reporters to present the registrar with all available evidence that the reported domain name is used as part of a BEC fraud.

The fact that the domain name may resemble a third party's domain name is not enough for a registrar to act. In cases where the issue is related to an intellectual property dispute, UDRP and/or URS is the appropriate method to address the issue. Registrars are not qualified to settle such disputes.

[1] Business Email Compromise The $26 Billion Scam, PSA Alert Number I-091019-PSA, 10 September 2019.

In parallel with the reporting to the registrar, targets of BEC should also contact the email service provider. A DIG[2] lookup tool will allow reporters to find the details of the email service provider easily.

Registrar Actions

While BEC does not fall under the definition of DNS Abuse used by the RrSG[3], fraud of this type is certainly an example of "illegal activity", defined in the RAA[4] as "conduct involving use of a Registered Name sponsored by Registrar that is prohibited by applicable law and/or exploitation of Registrar's domain name resolution or registration services in furtherance of conduct involving the use of a Registered Name sponsored by Registrar that is prohibited by applicable law." As such, registrars have a contractual obligation to investigate and respond to reports of abuse and illegal activity, including reports of BEC using domains registered with them.

Registrars have only one available measure to take: the full suspension of the reported domain name. From a technical standpoint, the registrar is able to modify the DNS servers on which the domain name is hosted to suspend any further use by the registrant. Although the action available to registrars occurs after the fact, it will prevent the criminals from using that domain to send further fraudulent emails.

What can victim companies do?

There is no single foolproof method to protect against this kind of fraud but there are several measures which can be taken by every company to avoid becoming a victim:

1. Implement policies that teach members of your organisation how to vet emails. A mere phone call can make a million dollars difference.
2. Verify your business partners' emails to confirm they are legitimate.
3. Have double-verification requirements in place for payments over certain amounts.
4. Every person authorised to approve or request payment should use an SMIME certificate for their emails.
5. Use a custom domain name and do not rely on an email provider's generic address. If you fail to do so, you will have no control over the domain name used for your email address and any other user may register an address close to your organisation's (e.g. you may use ceo@email.tld but anyone can register president@email.tld).
6. Review information on your company website and show caution in your use of social media.

The above is far from an exhaustive list but should constitute a reasonable basis for your protection against BEC fraud attempts.

---

[2] Domain Information Groper: typically available as a command-line utility but also available publically, including at https://toolbox.googleapps.com/apps/dig/.
[3] CPH Definition of DNS Abuse: DNS Abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for the other forms of DNS Abuse).
[4] https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#raa §1.13

Information for Registrars wanting to go further

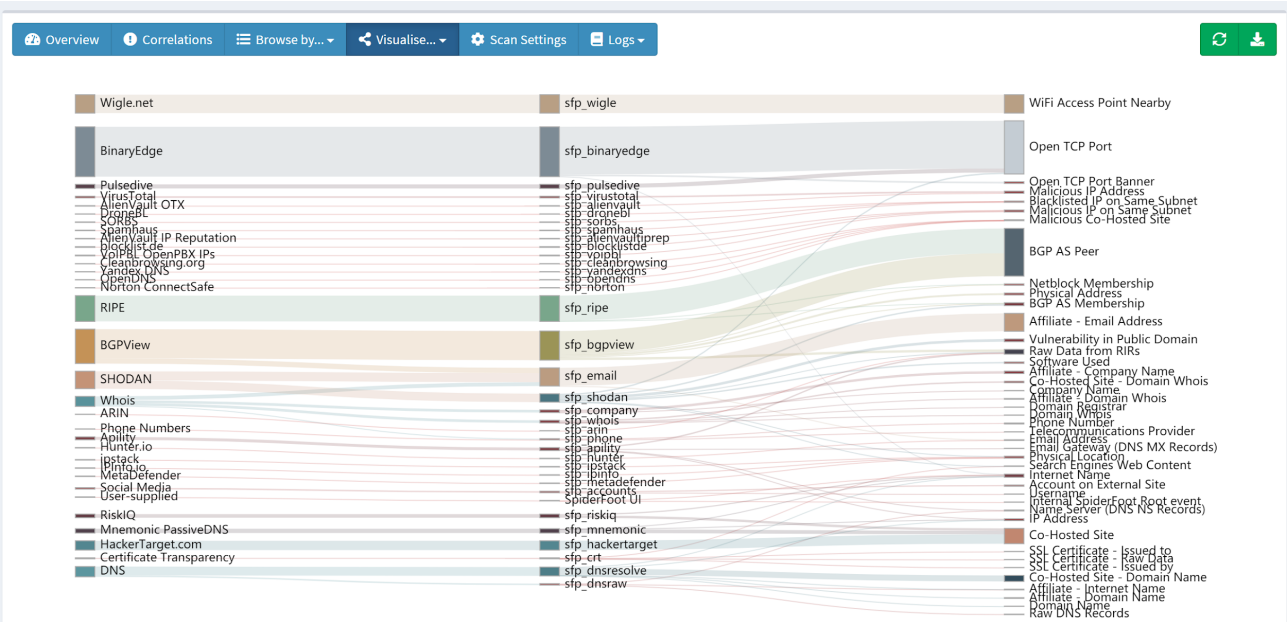
There are a few guidelines that registrars can use to detect BEC attacks. When a registrar receives a possible BEC abuse report, it is advised to switch to an incident response team-based approach.

The Five Steps of Incident Response (Registrar)

1. Be Ready. Never assume that an abuse report is an isolated incident. Be prepared and make sure you have tooling. Here is a list of many useful tools.
2. Report and Document Everything. This includes the reseller, domain name, registrant, IP address of the A record, name servers used, and any other relevant information.
3. Analysis. Tools like pulsedive.com help in reporting and analysis and are able to pivot through information very quickly.
4. Containment and Neutralisation of the Threat. Usually suspension or escalation to the reseller.
5. Lessons Learned. Take time after the report and remediation to examine the situation to help you in future incidents.

Tooling is essential in further discovery. Cybercriminals engaged in BEC fraud usually register domain names with a unique set of fake registration data created by professional fake identification generators, making detection based on registration data almost impossible.

A registrar can use tools like Maltego, Spiderfoot.net, or Pulsedive.com; these types of tools have a steep learning curve and require a hefty investment of time to set up but can be well worth the investment. Tools that scan the technical infrastructure of BEC operators can reveal more domain names engaged in BEC fraud. These tools also allow a registrar to spot mistakes or clues.



Registration data patterns

Look for patterns in the registration data. Does the registration data match the business model of the reseller? A hosting company with primarily EU-based customers suddenly having registrants from Russia should be a red flag for a registrar.

Check for suspicious subdomain names that match company names or organisations.

While everyone is entitled to privacy, zero-knowledge email providers are also used by cybercriminals as a forensic countermeasure and may be a cause for further investigation.