AREA 1

BUSINESS, COMPROMISED?

How Area 1 Stops BEC Phishing

One of today's most damaging phishing attack types is Business Email Compromise (BEC). In fact, nearly 50 percent of cybersecurity-related financial loss in 2018 was due to these attacks, according to a recent FBI report. Also, a recent advisory from the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN), reports that U.S. businesses have been hit with nearly $9 billion in attempted BEC phishing theft since 2016. It's clear from these statistics that tackling BEC requires a new approach to cyber defense—traditional defenses are failing to defend against these attacks.

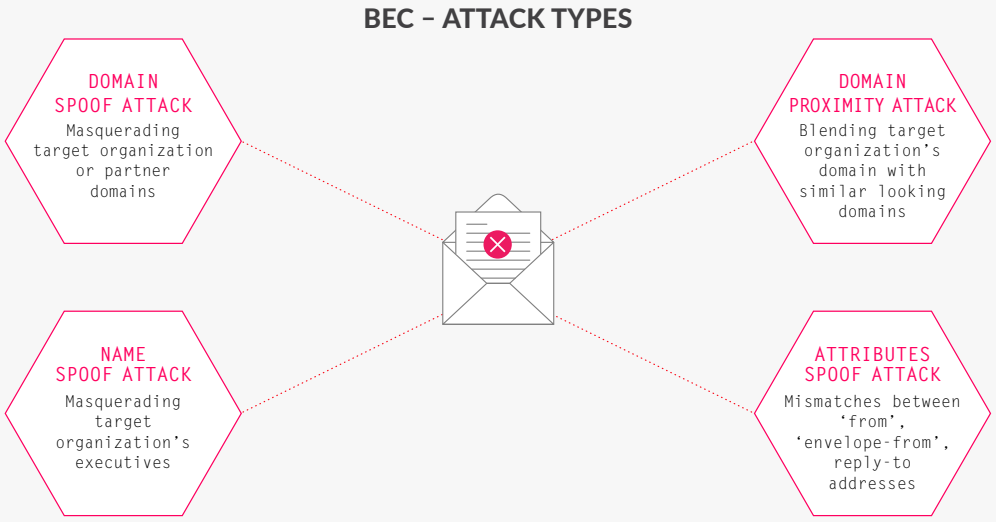
BEC phishing messages are simple, with no links or attachments. They are socially engineered to trick their victims into taking digital or physical action.

The absence of URL and attachments to analyze creates a difficult challenge for traditional detection engines as these messages now look like any other normal business message.

The key to detecting BEC phishing requires using an array of advanced email analysis techniques that can evaluate both the **origin** and the **context** of the email in ways that can reliably detect an imposter email.

HACKERS USE SEVERAL TECHNIQUES TO CRAFT FAKE BEC ATTACKS.

- **Display name spoof attacks:** Hackers can easily spoof the display name or "From" email field to make it appear that an email comes from an executive or other trusted party.
- **Domain spoof attacks:** Hackers can also easily spoof a sender email domain to make it appear that a trusted organization or partner sent an email.
- **Lookalike domain or domain proximity attacks:** In some cases, hackers establish a domain with a name similar to a trusted organization or a trusted partner's domain name. This fools recipient into believing that an email comes from a trusted source.
- **Attributes spoof attacks:** Mismatches between 'from', 'envelope-from', reply-to addresses



THE FIRST CHALLENGE

In order to protect from BEC, the first challenge is automating detection of inbound email that appears to be from an exec, employee, supplier, or customer, and then analyzing that email to determine if the sender is who they claim to be.

Area 1 uses sophisticated exact and fuzzy matching techniques to identify email that purports to be from an exec, employee, or domain that is at risk for impersonation. (Fuzzy matching is an improved method of processing word-based queries to find matching phrases or sentences from a database.)

For example, here's a screenshot of an email, detected by our matching algorithms, that appears to be sent from our VP of Engineering, requesting a change to his direct deposit account information from a Finance Manager.

EMAIL AUTHENTICATION – IMPORTANT YET INEFFECTIVE

Once an email is identified that appears to be from a protected sender, the next challenge is to determine if the sender is truly who they appear to be. Most defenses use email authentication checks, including SPF, DKIM, and DMARC, to validate the sender.

The fact is, these checks are not effective. Hackers can easily register a lookalike or typo squatted domain and properly configure SPF, DKIM, and DMARC to pass recipient email authentication checks. They can also compromise reputable sites to send BEC that will pass sender validation checks. And most simply, they merely create spoofed accounts with public email services, such as gmail or yahoo, that pass sender validation. In many cases, domain registration records aren't complete or kept up-to-date. As a result, email authentication alone can't be relied on to validate that a sender is who they claim to be.

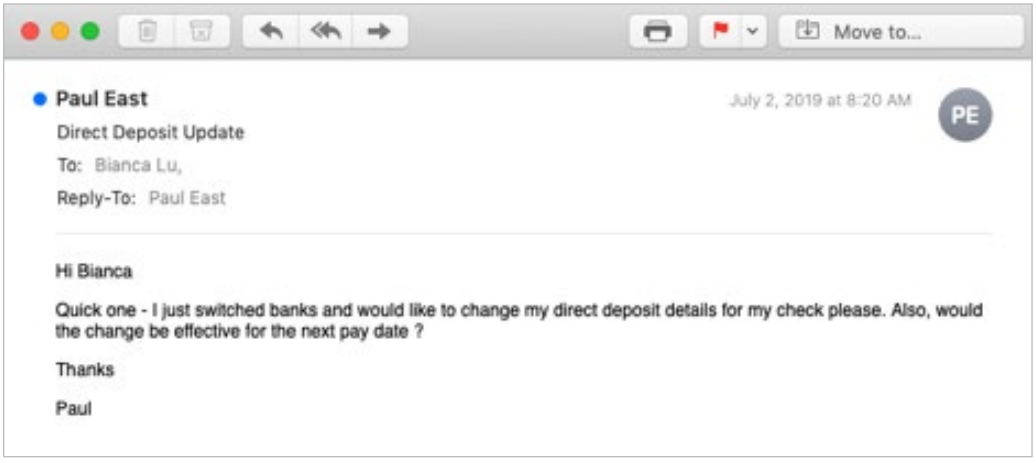


FIG 1: BEC EMAIL DETECTED AND BLOCKED BY AREA 1

In the case of the direct deposit email request referenced above, the detection results noted below here indicate that email authentication is not configured for the sending domain, so the sender validation check is inconclusive. A recent Global DMARC Adoption 2019 report indicates that over 80% of domains aren't configured with DMARC email authentication policies. That means that using email authentication checks to validate the sender is useless for email originating from 80% of domains.

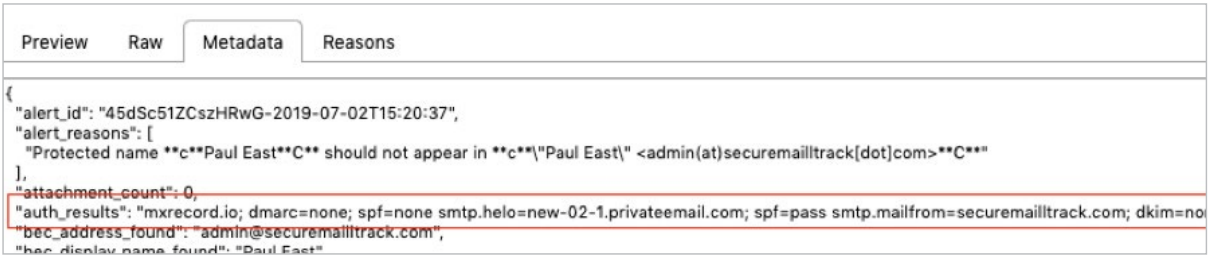


FIG 2: EMAIL ANALYSIS RESULTS

Another technique to uncover imposter email is header analysis. Header analysis can uncover clues, such as "from" and "reply-to" addresses that don't match, which may indicate a sender deception attempt. In this example, the email analysis results above show a mismatch of the display name "from" address, Paul East, and the envelope and reply-to "from" addresses, admin(at)securemailltrack(dot)com, indicating a clue that this is likely a BEC.

BEYOND SENDER VALIDATION ANALYSIS

At Area 1, in addition to sender validation, reputation, and header analysis, we look for more advanced patterns to understand the source of an email.

For example, we look at sender domain and IP address attributes such as age, history, and other associated data using super-fast lookups. We correlate that information with threat data uncovered from Area 1's proactive, continuous threat-hunting. This method uncovers additional clues. For example, what is the domain age? Are known threat actors or malicious infrastructure associated with the sending domain or IP? Is the IP configured appropriately to meet RFC standards?

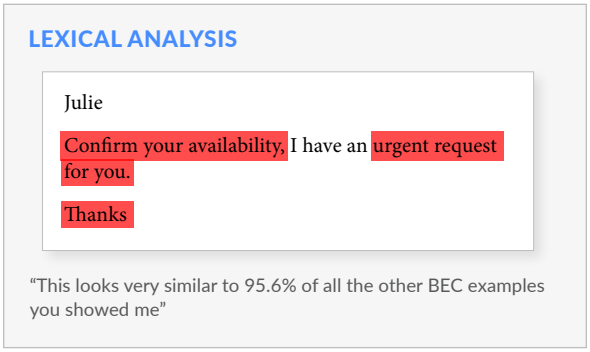
Area 1 proactively discovers the sites that hackers are compromising, as well as the IPs and domain infrastructure they're establishing to execute new phishing campaigns -- before these campaigns are launched. This massive-scale phish indexing creates the industry's largest attack data warehouse, providing early insight into new and emerging phishing infrastructure. The result? Superior capability to detect the BEC attacks that traditional defenses miss.

SPF, DKIM and DMARC checks are not effective for blocking Business Email Compromise.

MESSAGE CONTEXT IS KEY

In addition to Area 1's unique methods of evaluating the trustworthiness and authenticity of an email source, understanding the context of a message is key to detecting BEC phishing.

BEC emails are targeted and socially engineered to achieve their objective. However, using sophisticated matching techniques, the subject and body of a message can be analyzed to uncover small patterns that reveal similarities with other BEC attacks. For example, matching models identified that the body of the message in the figure below is similar to over 95 percent of BEC email detections, indicating a high likelihood that the message is a BEC.



Area 1's techniques for understanding the origin and context of an email yield clues that, in combination with proprietary BEC detection algorithms, calculate an essential verdict. That verdict determines whether an email that appears to be from a trusted sender is benign or a BEC.

One clue on its own may contribute to a verdict; however, Area 1 evaluates the combination of many clues about the origin and the context, using our proprietary BEC detection algorithms, to determine a verdict with certainty.

Area 1 proactively discovers the sites that hackers are compromising, as well as the IPs and domain infrastructure they're establishing to execute new phishing campaigns — before these campaigns are launched.

Correctly identifying BEC attacks requires computationally intensive algorithms and techniques. A task that many appliance based SEGs cannot handled due the required processing horsepower. Area 1's cloud native architecture enables fast, elastic, scalable performance and dynamic updating of databases, detection models, and algorithms. That means it's capable of detecting BEC at scale, and staying ahead of threat actors, without impacting email performance or reliability.

THE THREAT LANDSCAPE IS CONTINUALLY EVOLVING

Because of that shifting environment, the Area 1 service continuously and dynamically updates the detection models, algorithms, and threat data as new and emerging phishing campaigns are discovered to stay ahead of threat actors and effectively detect and stop BEC threats. If you're concerned about BEC email bypassing your defenses, you've already taken the first step to secure your organization. Contact Area 1 to learn more about how we can protect against BEC phishing and to setup a product trial.

About Area 1 Security

Area 1 Security is the first to bring accountability to cybersecurity. Backed by top-tier investors, Area 1 Security is led by security, Artificial Intelligence, and data analytics experts who created a preemptive solution to stop phishing, the number one cause of cyber attacks.

Area 1 Security works with organizations worldwide, including Fortune 500 banks, insurance, and tech companies, and healthcare providers to realign their cybersecurity posture for combating the most significant risks, protecting customer data, and stopping attacks before they happen. Area 1 Security is a recipient of Inc. Magazine's "2018 Inc.'s Best Workplaces" in America. To learn more about Area 1 Security, visit **www.area1security.com**, join the conversation at **@area1security** or follow the **blog** for the latest industry news and insights on how to stop phishing.

▸ **Learn More** INFO@AREA1SECURITY.COM