

# BUSINESS EMAIL COMPROMISE

**According to the FBI's Internet Crime Complaint Center, business email compromises accounted for 40% of total cybercrime losses in 2019.**

## WHAT IS BUSINESS EMAIL COMPROMISE?

Business Email Compromise (BEC) is an attack that involves a bad actor sending an email that appears to be legitimate in order to fraudulently request funds. These attacks, or scams, may be accomplished through a variety of vectors including: spoofing an email address so that it appears to be legitimate; sending spear phishing emails to trick employees into revealing confidential information or account credentials; or using malware to gain access to a corporate email environment. The bad actor then builds a target profile that includes: financial data; sample emails for content and formatting; point of contact information; and other information that will allow them to send a convincing email. Once the bad actor gathers enough information to send a spoofed or fraudulent email from a compromised account, carefully crafted emails are then sent to identified targets requesting fund transfers to new bank accounts.

## THE ARETE PROCESS

Once engaged on a BEC matter, Arete immediately begins collection of logs and artifacts. Once the relevant evidence has been collected and preserved, analysis begins, using Arete's Forensically sound methodology to determine the who, what, where, when, and how of the attack. Arete will produce a report of preliminary findings to the client within 24-72 hours.



If notification list creation is necessary, Arete's internal data breach analysis team can apply process automation and artificial intelligence to data sets. Arete's process zeroes in on the affected documents, producing findings to meet legal and regulatory requirements, at a fixed fee per document being reviewed.

## THE ARETE ADVANTAGE

- Arete's team of experts, with years of experience in the military, government and the private sector, handle hundreds of BEC cases every year.
- Arete can liaise with law enforcement, as Arete superheroes regularly work side-by-side with law enforcement on a variety of matters.
- Arete has the knowledge and expertise to assist with the securing and hardening of the client's infrastructure to help protect the client against future cyber attacks.