THE
NATIONAL LAW REVIEW

Inside a Business Email Compromise Operation

Sunday, June 23, 2019

A new report from cybersecurity company Agari's Cyber Intelligence Division outlines the operations of a business email compromise (BEC) gang in West Africa, showing that criminals who engage in BEC online theft can have a diverse portfolio of online criminal activity that they use to build their capabilities, and use sophisticated methods to scam their victims, including businesses and government agencies.

BEC is a cyberfraud tactic in which a scammer will contact a target using phishing emails imitating a fellow employee of the target (often someone in the finance department or management) usually seeking to convince the victim to conduct a business transaction, most likely a money transfer to an account run by the scammer. The scammers may also try to trick their victims into clicking a link in an email or visiting a scam website, which could provide the scammers with the victim's online credentials or download malware onto the victim's computer and gain access to their company's network.

RISK MANAGEMENT
RISK MONITOR

Article By
Adam Jacobson
Risk and Insurance Management Society, Inc. (RIMS)
Risk Management Monitor
Communications, Media & Internet
Global
All Federal

As *Risk Management* previously reported, Beazley Breach Response Services found that BEC-related attacks cost victims an average of $70,960, but the FBI's Internet Crime Complaint Center has estimated that the total "revenues" of BEC attacks doubled in 2018 to $1.3 billion. BEC attacks are also extremely common—approximately two-thirds of IT executives are reportedly dealing with them.

Agari's report, titled "Scattered Canary: The Evolution of a West African Cybercriminal Startup," shows that cybercriminal gangs diversify their criminal schemes, using their established infrastructure from one type of scam to facilitate others. Agari researchers named the group Scattered Canary and compared it to a tech startup because of its recruitment and expansion strategy. Scattered Canary has pursued a variety of different criminal social engineering efforts, including:

- Romance scams: Creating a fake online romantic relationship with a victim and requesting gifts, access to their bank or retirement accounts, or services related to other scams.
- Check fraud: A scammer offers to purchase an item for more than its advertised price with a check (which is fraudulent), then requests that the seller send the extra amount to a third party (a fictional shipping company, for example).
- Credential harvesting: Tricking victims into providing their online credentials, including log-in information for online financial services.

Agari says that Scattered Canary built up a network of members and the skills to easily transfer from one scheme to another. The group has used multiple BEC tactics over time, transitioning from tricking employees into carrying out wire transfers from their companies' bank accounts to convincing victims to buy gift cards that scammers would then cash out via cryptocurrency exchanges. More recently, the group has targeted human resource departments to change the direct deposit information for a company's executive, then cashed out the deposits using prepaid debit cards.

Businesses should train their staff at all levels on how to spot BEC and other types of online scams. If employees

can recognize phishing emails and websites, and know not to click links or provide information in response to either, this can protect companies from fraud and significant financial loss. In addition to training staff, the FBI suggests always verifying requests to send money, even if the email requesting the transfer is urgent, by speaking directly to the person who seems to be requesting the money on the phone (using the previously known number, not the one provided in the email) or in person. The FBI also suggests setting up filters that flag email addresses that are similar to the company's email, and creating an email rule that notes emails coming from outside the company, among other technical steps.

Source URL: https://www.natlawreview.com/article/inside-business-email-compromise-operation