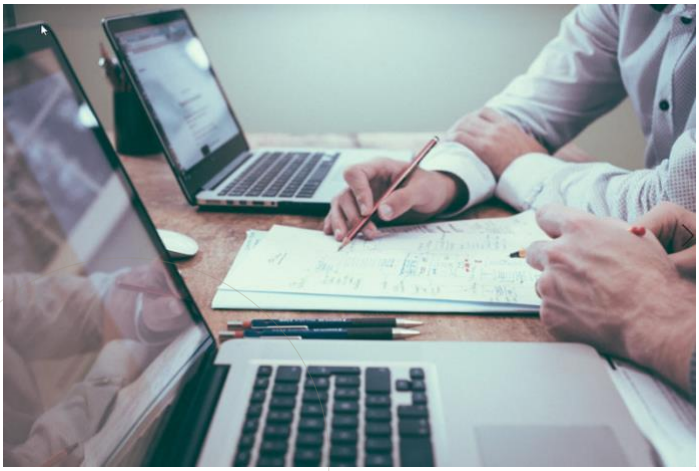
FAMILY OFFICE FALLS VICTIM TO A BUSINESS EMAIL COMPROMISE RESULTING IN MISDIRECTED CLIENT FUNDS

Family offices are huge targets for business email compromise ("BEC") at the hands of cybercriminals worldwide. It only takes a mouse click to expose the entire office and all of their clients to malware and possible breach of confidential information. For family offices and investment firms that operate based in large part on reputation, and this kind of event could be devasting.



BlackCloak was contacted by a family office that was not yet a BlackCloak client after falling victim to a BEC scam. An employee received a phishing email, clicked on the link, and subsequently entered their login credentials on a fake email login page. Cybercriminals used the credentials to create email forwarding rules and adjust existing email rules to intercept any emails containing "wiring instructions". The criminals would read the email messages and send replies with erroneous wiring instructions to third parties so that funds were routed to the criminals' accounts rather than the family office. The family office lost hundreds of thousands of client dollars in this scam and suffered reputational loss by needing to contact their clients and explain what happened.

BlackCloak was engaged and was able to successfully conduct forensics, remediate the online email rules, route out the control that the cybercriminals had installed, and protect the executives of the family office from further malfeasance. Furthermore, the education and training provided by BlackCloak to the family office employees provided huge benefits and enhanced security of the family office that all clients will enjoy going forward.