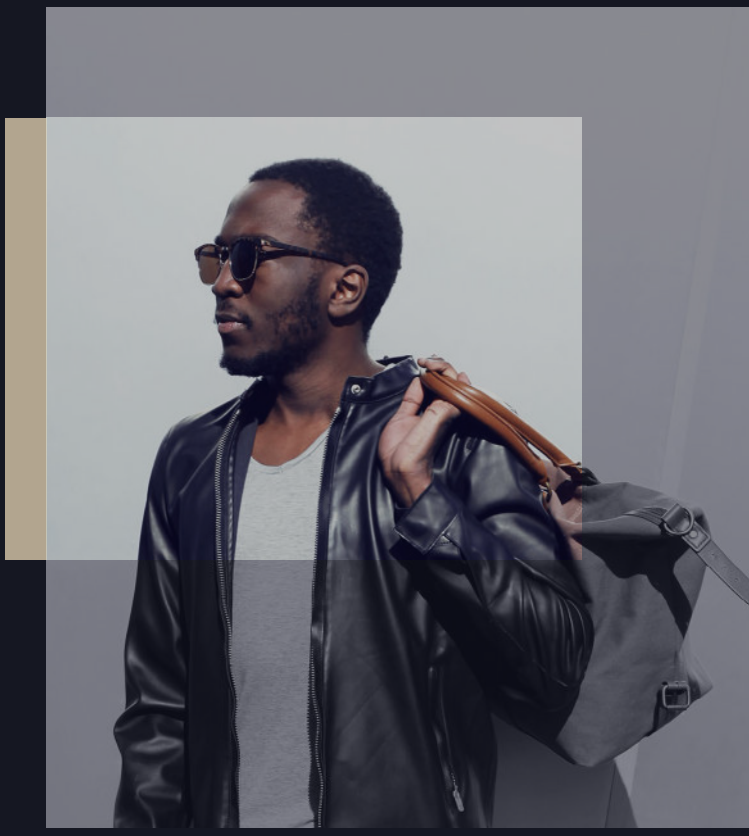
BLACKCLOAK®

Company Recovers Executive's Corporate Email Account from Hackers



Description:

- Company CxO
- Electronics manufacturing services company
- Microsoft Outlook account breached

The Problem:

Compromised Email Account

An executive at an electronics manufacturing services company began to receive undeliverable emails from addresses he had not sent messages to, causing him to become suspicious. It was found that his Microsoft Office Outlook account had been breached without his knowledge.

The bad actors that took over his account sent up to 800 spam emails in the executive's name, putting the recipients at risk of identity and credit theft.

It wasn't just the executive who was at risk. **A compromised Outlook account puts everyone connected to the account at risk, including the corporate network and email recipients.**

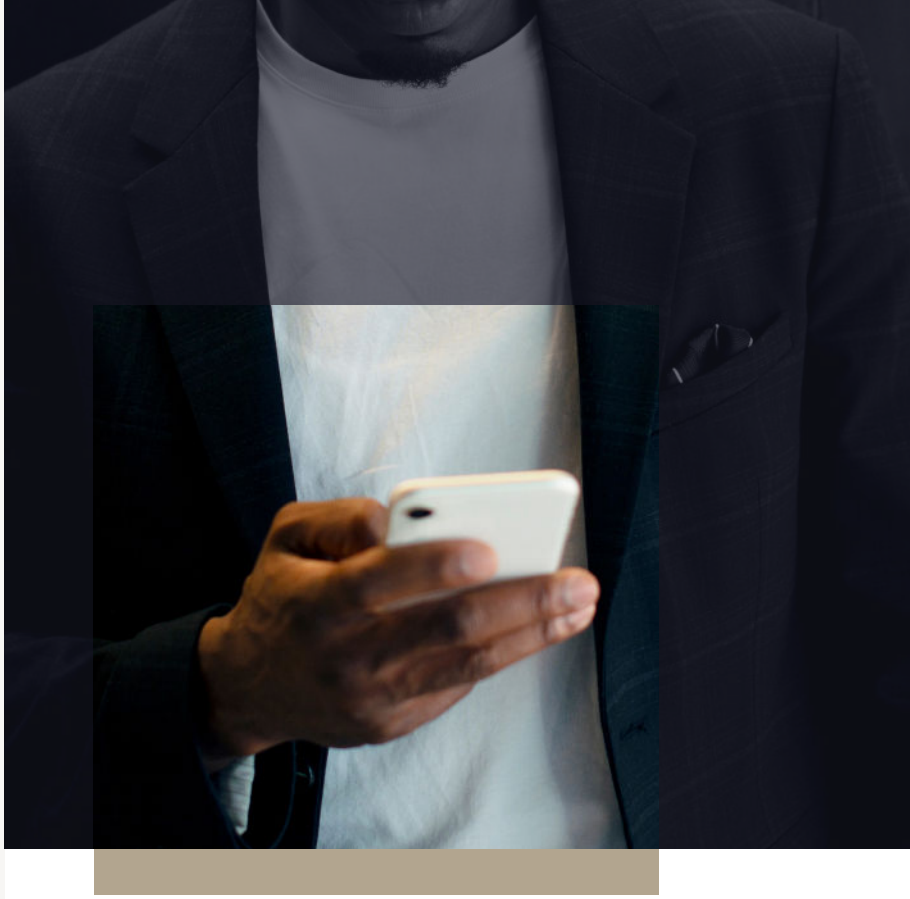
BlackCloak Steps In

After terminating the executive's access to the corporate Outlook account, his company's IT team contacted BlackCloak to help with remediation. BlackCloak initiated a comprehensive discovery analysis of the executive's devices and network access to determine the full level of risk.

It was found that the attack originated from a previously breached Azure virtual machine, which the bad actors used to access the executive's email. BlackCloak also discovered that the executive was using va variation of breached passwords that had been leaked on the dark web.

To remedy the situation, BlackCloak implemented multi-factor authentication (MFA) on all accounts, changed all account passwords, documented the damage, and removed any threats to the executive's digital footprint.

Because the passwords used by the executive had been leaked, BlackCloak scanned the dark web for additional exposed passwords and removed all existing credentials from data broker sites.



The Result

By addressing the breach swiftly and thoroughly, the executive's Microsoft Outlook account and digital footprint were fully secured, preventing further exploitation by bad actors. Through comprehensive remediation, all compromised passwords were changed, and multi-factor authentication was implemented across all accounts for enhanced security.

The proactive removal of exposed credentials from data broker sites eliminated additional risks, while ongoing dark web monitoring ensures continuous protection. The executive's home and corporate networks were safeguarded, stopping the spread of malware or fraudulent activity.