How To Respond to Business Email Compromise Threats

PONDURANCE

When your organization experiences a business email compromise (BEC), it's important to stop the threat actors access quickly and remove them from the environment. Below are our tips for responding to BEC threats and conducting a review afterward:

☐ **Review unified audit logs (UAL)**

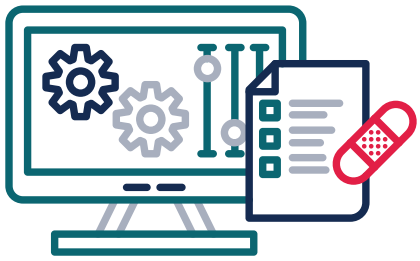
- Microsoft allows you to search for activities performed across the different Microsoft 365 products in one unified audit log. This can help you to identify suspicious activity down to the user and administrator levels. Learn more about this feature in the Microsoft compliance center.
- In UAL, you may want to look for inbox rule changes such as moving emails to a specific folder or forwarding emails to another email address. Both of these tactics are used during BEC to avoid being caught and also exfiltrate email during BEC operations.
- In UAL, you may want to review newly created files and shared files. Sometimes, threat actors may create and share files for their BEC operations or to do additional phishing. In some cases, we've seen threat actors share files containing phishing links with other users in the organization and users outside of the organization.

☐ **Review message trace logs to identify who sent/ received emails**

- You can detect outside influence based on set criteria through the message trace feature in the Microsoft 365 Defender portal. This feature allows you to follow an email message to see if it was received, rejected, deferred, or delivered and if any actions were taken on the message once it reached its final destination.

☐ **Use content search to find data**

- You can search and export data like mailboxes, documents, and Skype for business conversations using content search. This tool can act as an eDiscovery tool if you do experience a BEC attack.



☐ **Create procedures to respond to compromised accounts to reduce impact**

- In the event of a compromise, simply disabling the infected account is not sufficient. We recommend initiating password resets, killing all active sessions, and reviewing authorized applications (and possibly revoking some malicious authorized apps) to prevent any further activity. Learn about investigating apps and how to kill active user sessions in O365.

☐ **Review alerts in the Cloud App Security portal**

- Within Cloud App Security, you can prevent data exfiltration, require authentication context, protect downloads, prevent uploads of unlabeled files, block potential malware, block access, and more. Learn more about how this tool works and how to integrate.

BEC could lead cybercriminals into your network with the opportunity to move laterally. If they do get in, it's important to squash their activity quickly and completely to ensure no further damage can be done. There is an international cybercriminal organization that successfully conducts cyber financial fraud, and BEC is one of the main tools it uses. Watch an on-demand webinar with our Manager of Incident Response, Max Henderson, where he dives into a case study on this cybercriminal activity including the organization's motivations and target victims, its unique scheme to access data, and our recommendations to reduce the cybercriminal organization's success rate.

REGISTER HERE

pondurance.com
500 N. Meridian St., Suite 500, Indianapolis, IN 46204