

The Scale of the Problem

Business Email Compromise (BEC) is one of the most dangerous email-based attack types. Defence technologies struggle to detect BEC attacks as they typically do not involve malware or malicious links. Rather, these attacks leverage well-staged manipulation of human judgment and trust, making even the cyber awareness of employees and executives insufficient.

Most Business Email Compromise (BEC) attacks are motivated by the prospect of large scale financial gain. The extent of the issue can be understood through the statistics provided by the FBI in the US and Enisa in the EU, which are presented in the next column.

Cynode Managed Business Email Compromise (BEC)

Detection & Response Service

Cynode's "Business Email Compromise" (BEC) Detection and Response is a comprehensive service designed to monitor, detect, and respond to BEC related activities in our customers' networks. The service identifies potential BEC threats such as impersonation, fraud, false invoices, data theft, and the spread of malicious code in real time. It responds to any signals or unusual activities that need validation, while also externally monitoring compromised account intelligence.

The Mechanics of BEC Attacks

Business Email Compromise starts with an "Email Account Take Over". Using techniques and data for password exploitation such as brute force, password spraying, combo lists harvested from various data breaches, previous credential theft phishing campaigns, compromised devices by malware attacks, third-party data leaks the threat actor takes over a corporate email account.

Once the account has been compromised, the threat actor can perform actions such as:

- Investigating financial subjects and content that can be manipulated.
- Sending manipulating emails for contacting a third party, sending an invoice, requesting payment, or asking for sensitive data.
- Impersonating key participants in financial matters by registering similar-looking domains, using information gathered from compromised email accounts.
- Carrying out somewhat discreet discovery and data leak actions such as;
 - Creating rules to forward emails to an unusual mailbox folder
 - Forwarding emails externally
 - Deleting impersonated emails from the sent box
 - Reviewing (i.e. on Sharepoint) or exporting a massive number of documents.
- If the compromised account does not contain financially relevant information, it may be used to spread phishing emails to the subject matter individuals or within the enterprise ecosystem.

Key Statistics

European Union's Enisa indicates in its 2023 cyber threat report that BEC is attackers' favourite means for extracting financial gain from their victims.



In 2023, the IC3 of FBI received 21,489 BEC complaints with adjusted losses over \$2.9 billion.

FEDERAL BUREAU of INVESTIGATION
Internet Crime Report
2023

Key Benefits

- Stay proactive in detecting and responding to Business Email Compromise (BEC) threats to minimise the risk of financial loss, fraud, and reputation damage.
- Classify and prioritise potential target users and scenarios.
- Prevent the use of corporate accounts for initial access in the attack kill chain.
- Implement a BEC specific monitoring, detection, and response framework without overburdening the cybersecurity teams.
- Empower cybersecurity teams and save significant time by safeguarding the email accounts of employees and executives.

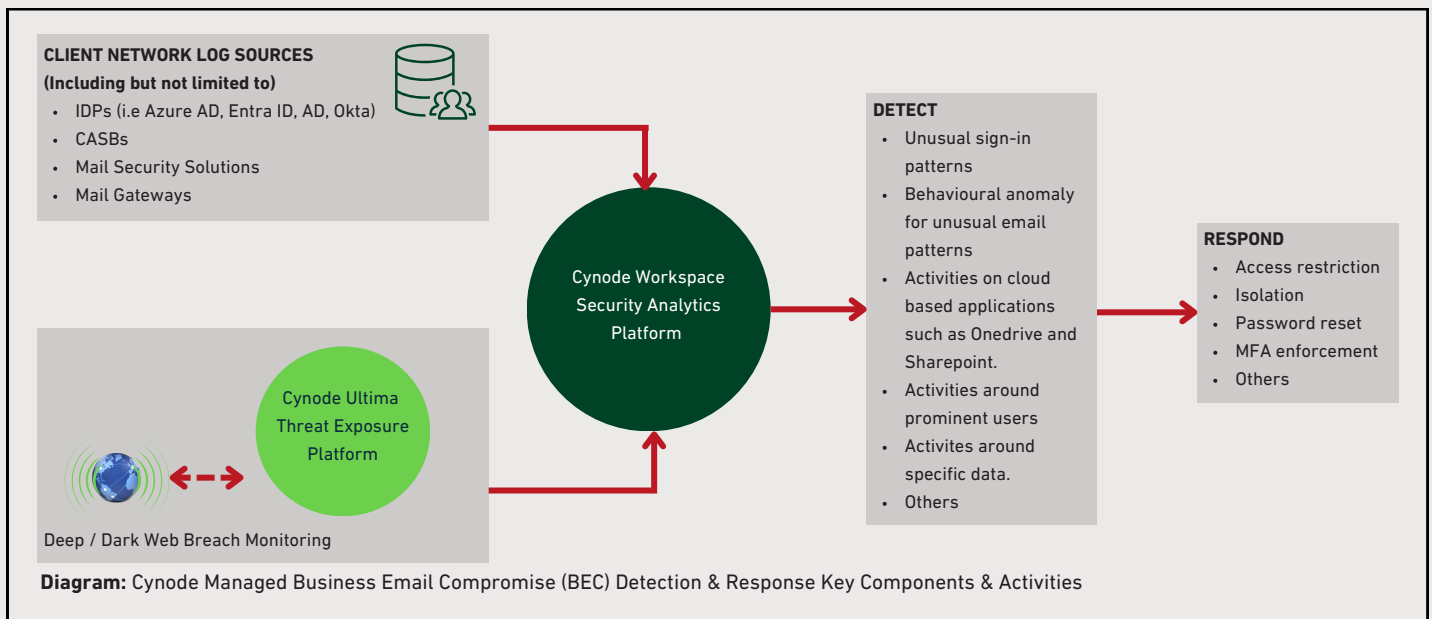
How We Detect

Empowered by Cynode's Workspace Security Analytics and Ultima Threat Exposure Platforms, Cynode's security analysts implement targeted detection capabilities to identify possible BEC activities. These capabilities include but are not limited to:


- Monitoring low signal activities based on various criteria like locations, times, source IPs, OS, applications, and activities to detect unusual sign-in patterns and other indicators.
- Tracking behavioural anomalies for unusual email patterns and activities on cloud-based applications such as Onedrive and Sharepoint.
- Focusing on prominent users with specific data.
- Identifying phishing attempts initiated from the impersonated account.
- Enhancing alerts of suspicious activity by incorporating external intelligence (from dark/deep web breach monitoring).


How We Respond


- Validating the compromised account and notifying the account owner.
- Interrupting the impersonated access to the account by revoking the sessions and tokens.
- Prevent reaccess by enforcing password reset and Multi-Factor Authentication (MFA).
- Implement measures such as access limitations and isolation.
- Investigating the deep and dark web for any mention of sensitive data.
- Identifying any domain registrations that resemble the original.




OTHER CYNODE MDR SERVICES


 Managed Detection and Response for Endpoint


 Managed Detection and Response for Microsoft Defender

 Managed WebApp Exposure Monitoring

 Managed Detection and Response for Cloud

 Managed Phishing Detection and Response

 Managed Detection and Response for Identity Protection

 Managed Shadow IT Monitoring