IstroSec

Data Sheet

BEC Response

Business email compromise (BEC) is a type of attack compromising one or more accounts to send fraudulent emails or to further compromise target organization. Attackers are sending malicious emails using compromised accounts to spread malware, send deceptive requests for financial gain or to further compromise the target.

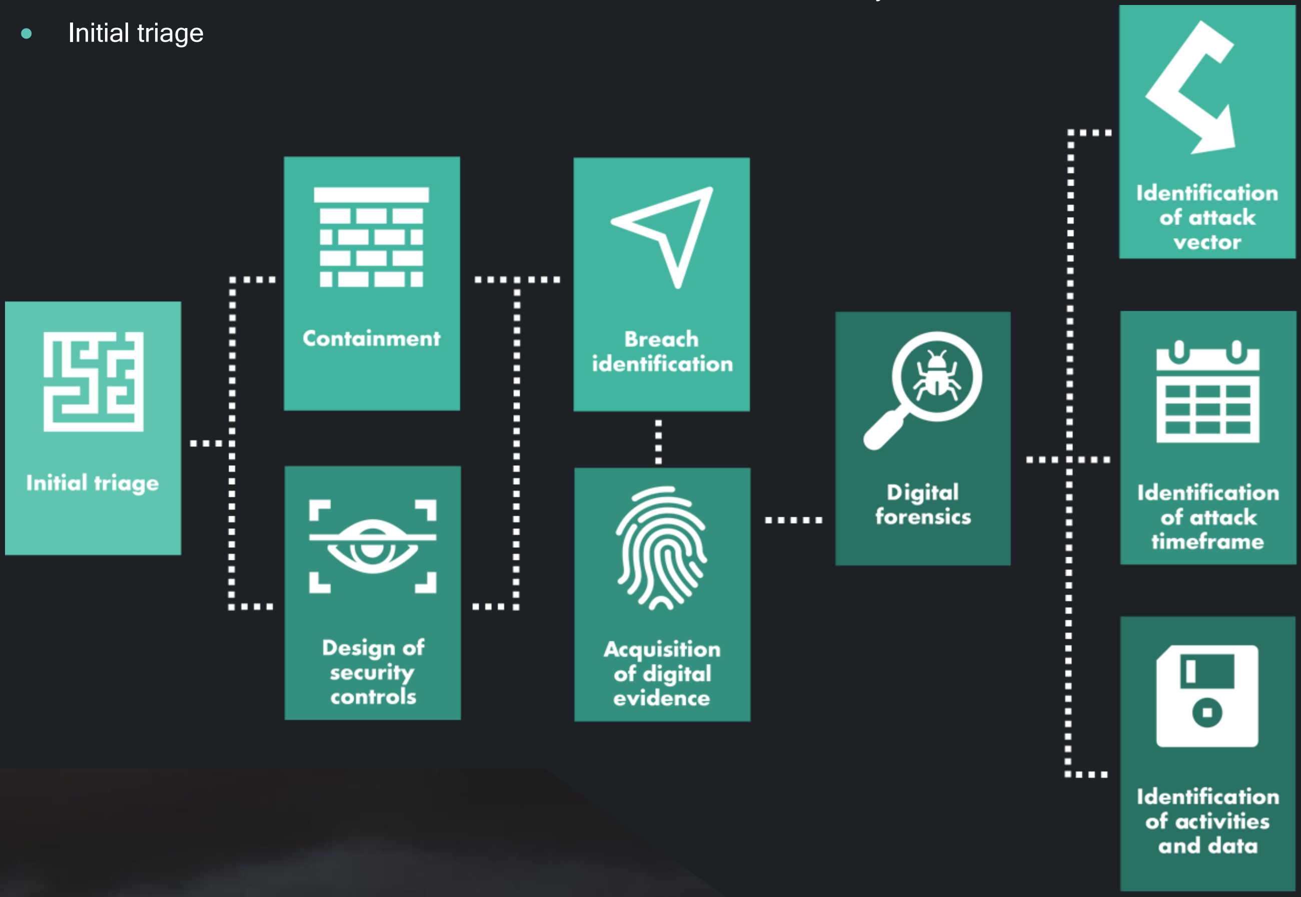
This Service Includes

These types of attacks can be carried out on-prem or using cloud service providers. In both situations, if relevant security controls are lacking, the whole account or even tenant can be compromised.

In case you have been targeted by BEC, contact us 24/7 on phone number +421 917 699 002 or by sending an email to incident@istrosec.com.

ISTROSEC experts will ensure fast and effective remediation consisting of:

- Initial triage
- Containment to prevent further spread of the attack
- Design and implementation of security controls to prevent this type of attack
- Breach identification, acquisition of digital evidence and digital forensics
- Identification of attack vector, attack timeframe and activities performed by the adversary in the system
- Identification of data accessed, exfiltrated or modified by the attacker


Initial triage
Containment
Design of security controls
Breach identification
Acquisition of digital evidence
Digital forensics
Identification of attack vector
Identification of attack timeframe
Identification of activities and data

European Cybersecurity Company.
Threat Intelligence. Incident Response. Cyber Advisory.

www.istrosec.com

Why Choose Us?

IstroSec specialists are experienced in dealing with BEC incidents both within client’s on-premise infrastructure and cloud (Office 365, Gmail, webmail accounts). They know the tactics, techniques and procedures employed by attackers and have the knowledge necessary to perform a quick, effective, and complex reaction.

Effective Reaction

In the case of a cyber-attack, especially targeted or performed by an advanced attacker (APT), it is necessary to respond within hours of detection, identify the current priority tasks and perform the necessary activities immediately. **Istro**Sec specialists have experience in crisis management in such situations and, according to the client's requirements, they coordinate incident response activities or directly manage this process.

Why **Istro**Sec?

Combined experience of more than 70 years

Access to experts in all domains of information security, including penetration testers, forensic analysts, malware analysts, trainers and more

Systematic improvement of information security according to frameworks enriched with the experience of IstroSec experts with advanced security incidents

Certified experts to ensure compliance with security standards and legislation - IstroSec experts have been operating in public administration (NIS Directive, GDPR and others) as well as in the private sector (ISO 27001, NIST, HIPAA and others)

IstroSec has proprietary tools at its disposal, which it implements within the organization, thus enabling effective isolation (containment) of the attack and its analysis.

Target Organization Support

IstroSec specialists have expertise in world-class incident response, forensic and malware analysis, which they have repeatedly demonstrated while responding to state-sponsored cyber-attacks, attacks against FORTUNE 500 organizations, as well as the participation of four **Istro**Sec experts in the winning team of LockedShields 2016 exercise.

Expertise in DFIR and Malware Analysis

IstroSec experts hold internationally recognized certificates in many areas. We hold certificates such as Certified Information Systems Security Professional (CISSP), Certified Information System Auditor (CISA), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE), Certified Reverse Engineering Analyst (CREA) and more.