IstroSec

Arkusz danych

Reakcja na ataki BEC

Business email compromise (BEC) to rodzaj ataku polegający na przejęciu jednego lub większej liczby kont w celu wysłania fałszywych wiadomości e-mail lub dalszego narażenia na atak organizacji docelowej. Atakujący wysyłają złośliwe wiadomości e-mail za pomocą zhakowanych kont w celu rozprzestrzeniania złośliwego oprogramowania, przedstawienia oszukańczych żądań uzyskania korzyści finansowych lub dalszego narażenia organizacji.

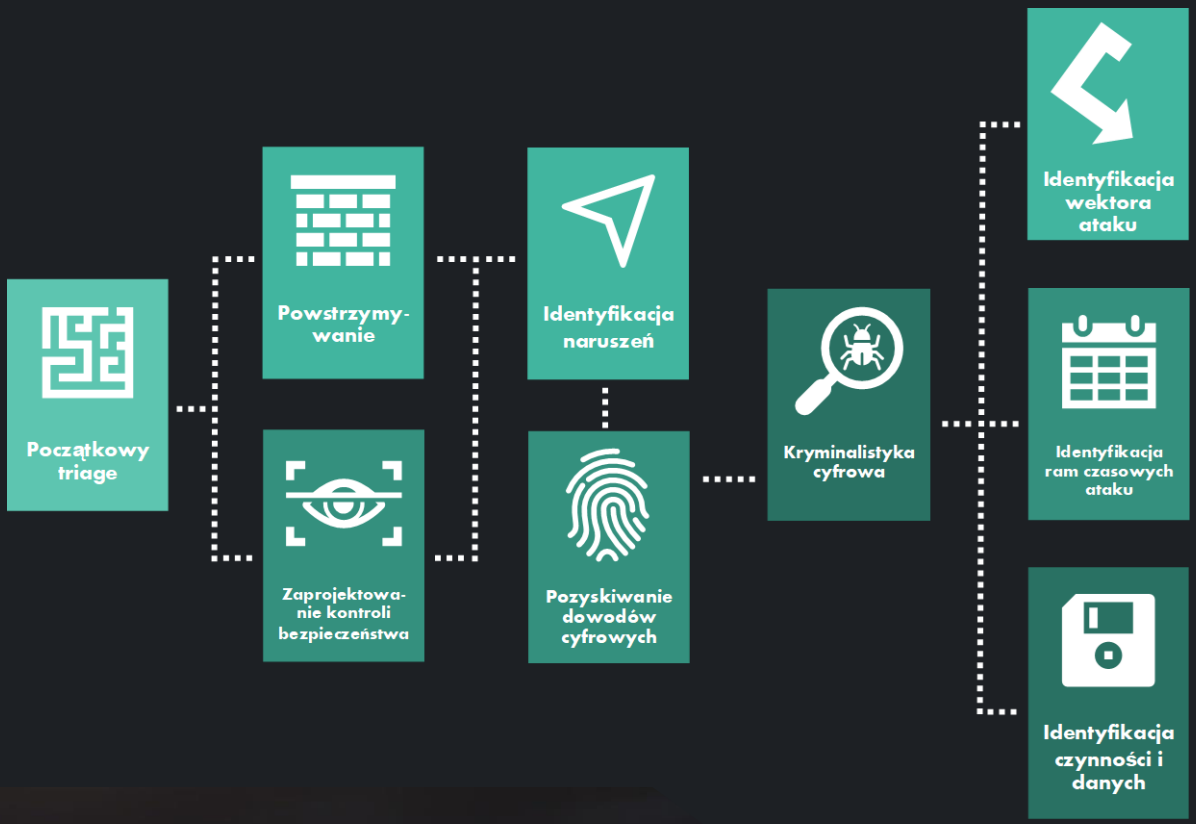
Usługa ta obejmuje:

Tego typu ataki mogą być przeprowadzane lokalnie lub przy użyciu dostawców usług w chmurze. W obu sytuacjach, jeśli brakuje odpowiednich kontroli bezpieczeństwa, przechwycone może być całe konto, a nawet infrastruktura dostawcy.

Jeśli padłeś ofiarą ataku BEC, skontaktuj się z nami poprzez całodobowy numer telefonu +421 917 699 002 lub wysyłając wiadomość e-mail na adres incident@istrosec.com.

Eksperci IstroSec zapewnią szybkie i skuteczne rozwiązanie, na które składa się:

- Początkowy triage
- Powstrzymanie dalszego rozprzestrzeniania się ataku
- Zaprojektowanie i wdrożenie kontroli bezpieczeństwa, aby zapobiec tego typu atakom
- Identyfikacja naruszeń, pozyskiwanie dowodów cyfrowych i kryminalistyka cyfrowa
- Identyfikacja wektora ataku, ram czasowych oraz czynności wykonywanych przez atakującego w systemie
- Identyfikacja danych, do których uzyskał dostęp lub które zostały eksfiltrowane i zmodyfikowane przez atakującego



IstroSec

Arkusz danych

Dlaczego akurat my?

Specjaliści **Istro**Sec mają doświadczenie w radzeniu sobie z incydentami BEC zarówno w infrastrukturze lokalnej klienta, jak i w chmurze (Office 365, Gmail, konta poczty internetowej). Znają taktykę, techniki i procedury stosowane przez atakujących oraz posiadają wiedzę niezbędną do przeprowadzenia szybkiej, skutecznej i złożonej reakcji

Skuteczna reakcja

W przypadku cyberataku, w szczególności ukierunkowanego lub dokonanego przez zaawansowanego atakującego (APT), konieczne jest zareagowanie w ciągu kilku godzin od wykrycia, zidentyfikowanie bieżących zadań priorytetowych i natychmiastowe wykonanie niezbędnych czynności. Specjaliści **Istro**Sec posiadają doświadczenie w zarządzaniu kryzysowym w takich sytuacjach i zgodnie z wymaganiami klienta koordynują działania reagowania na incydenty lub bezpośrednio zarządzają tym procesem.

Dlaczego IstroSec?

- Łącznie ponad 70 lat doświadczenia
- Dostęp do ekspertów ze wszystkich dziedzinach bezpieczeństwa informacji, w tym testerów penetracyjnych, analityków kryminalistycznych, analityków złośliwego oprogramowania, trenerów i nie tylko
- Systematyczna poprawa bezpieczeństwa informacji według frameworków wzbogaconych doświadczeniem ekspertów IstroSec z zaawansowanymi incydentami bezpieczeństwa
- Certyfikowani eksperci w celu zapewnienia zgodności z normami i przepisami bezpieczeństwa - eksperci IstroSec działają zarówno w administracji publicznej (dyrektywa NIS, RODO i inne) jak i w sektorze prywatnym (ISO 27001, NIST, HIPAA i inne)

IstroSec dysponuje autorskimi narzędziami, które wdraża wewnątrz organizacji, umożliwiając tym samym skuteczną izolację (powstrzymanie) ataku i jego analizę.

Wsparcie organizacji docelowej

Specjaliści **Istro**Sec posiadają doświadczenie w światowej klasy reagowaniu na incydenty, analizie kryminalistycznej i złośliwego oprogramowania, co wielokrotnie wykazali podczas reagowania na państwowe cyberataki, ataki na organizacje z listy FORTUNE 500, a także poprzez udział czterech ekspertów **Istro**Sec w zwycięskim zespole ćwiczenia LockedShields 2016.

Specjalistyczna wiedza DFIR i w analizie złośliwego oprogramowania

Eksperci **Istro**Sec posiadają międzynarodowe certyfikaty w wielu dziedzinach. Posiadamy certyfikaty takie jak 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) i inne.

IstroSec | Černyševského 10 | 851 01 Bratysława | Słowacja| +421 917 699 002 | info@istrosec.com | www.istrosec.com