IstroSec

Arkusz danych

Reagowanie na ransomware

Aby zminimalizować wpływ trwającego ataku oprogramowania ransomware w twojej organizacji, bardzo ważne jest szybkie reagowanie. Jeśli padłeś ofiarą oprogramowania ransomware, skontaktuj się z nami przez całodobowy numer telefonu +421 917 699 002 lub wysyłając wiadomość e-mail na adres incident@istrosec.com. Eksperci **Istro**Sec zapewnią szybki i skuteczny sposób na zaistniały incydent w zakresie cyberbezpieczeństwa.

Usługa ta obejmuje:

- Początkowy triage
- Powstrzymanie dalszego rozprzestrzeniania się ransomware
- Identyfikację szczepu ransomware, stojącą za nim grupę atakujących, zakres ataku oraz analizę konieczności komunikacji z atakującym lub zapłacenia okupu
- Pozyskiwanie cyfrowych dowodów do analizy kryminalistycznej, organów ścigania lub firm ubezpieczeniowych
- Monitorowanie DarkWeb pod kątem wycieku danych
- Wdrożenie narzędzi bezpieczeństwa w celu zapewnienia monitoringu bezpieczeństwa sieci klienta na czas trwania incydentu
- Wzmocnienie czystych segmentów sieci, aby zapobiec dalszym atakom
- Jeśli klient zdecyduje się na komunikację z atakującymi:
  - Prowadzenie negocjacji w celu obniżenia okupu i uniknięcia potencjalnych błędów komunikacyjnych prowadzących do nieudanej wymiany z atakującym
  - Pomoc w walidacji i korzystaniu z deszyfratora ransomware
  - Analizę deszyfratora dostarczonego przez atakującego
- Identyfikację wektora kompromitacji, w tym kryminalistykę cyfrową na potrzeby cyberubezpieczeń i organów ścigania
- Identyfikację infekcji wtórnych w organizacji
- Budowanie odporności, aby zapobiec ponownemu pojawieniu się tego ataku oprogramowania ransomware

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 **Istro**Sec działają zarówno w administracji publicznej (dyrektywa NIS, RODO i inne) jak i w sektorze prywatnym (ISO 27001, NIST, HIPAA i inne)

Dlaczego akurat my?

Eksperci IstroSec mają wieloletnie doświadczenie z atakami ransomware, identyfikacją problemu i jego skutecznym rozwiązywaniem. Wykorzystują zastrzeżoną metodologię potwierdzoną przez niezliczone działania związane z reagowaniem na incydenty i narzędzia do skutecznej reakcji na oprogramowanie ransomware (w tym reakcję na zagrożenia związane z oprogramowaniem ransomware), minimalizując jego wpływ i szkody wyrządzane aktywom klienta oraz pozyskiwanie i przechowywanie dowodów cyfrowych dla organów ścigania, organów regulacyjnych lub firm ubezpieczeniowych.

Ułatwianie płatności okupu za pomocą kryptowalut

Jeśli nie ma innej opcji niż zapłacenie okupu, IstroSec może ułatwić komunikację z atakującym, powierzając zadanie profesjonalnym negocjatorom przeszkolonym psychologicznie, aby zapewnić:

- Wykluczenie nieporozumień, które mogłyby potencjalnie doprowadzić do całkowitej utraty danych
- Płynną płatność okupu, aby zmaksymalizować prawdopodobieństwo dostarczenia deszyfratora przez atakującego
- Zminimalizować prawdopodobieństwo opublikowania wyciekających danych

Skuteczna reakcja

Gdy oprogramowanie ransomware zostanie wdrożone w docelowej organizacji, konieczne jest zareagowanie w ciągu kilku godzin. Bardzo ważne jest, aby zidentyfikować działania o wysokim priorytecie i natychmiast je wykonać. Eksperci IstroSec posiadają niezbędne doświadczenie w zarządzaniu kryzysowym w takich sytuacjach i mogą pomóc w koordynacji lub prowadzić działania reagowania.

Zapewnienie wsparcia organizacji docelowej

Nie wszystkie organizacje dysponują niezbędnymi narzędziami do wspierania skutecznej odpowiedzi na ataki ransomware. IstroSec ma do dyspozycji zastrzeżone narzędzia, które można łatwo wdrożyć w twojej infrastrukturze, aby umożliwić skuteczne powstrzymanie ataku i jego analizę.

Ekspertyza w zakresie reagowania na incydenty związane z cyberbezpieczeństwem, analizy złośliwego oprogramowania i kryminalistyki cyfrowej

Eksperci IstroSec wykazali się najlepszą w swojej klasie wiedzą w zakresie reagowania na incydenty, kryminalistyki cyfrowej i analizy złośliwego oprogramowania, potwierdzoną reagowaniem na kilka państwowych ataków APT, reagowaniem na ataki wymierzone w firmy z listy Fortune 500, a czterech specjalistów IstroSec będących członkami zwycięskiego zespołu LockedShields 2016 brało udział w najbardziej zaawansowanych ćwiczeniach reagowania na incydenty cybernetyczne na świecie.

Specjaliści IstroSec ds. reagowania na incydenty posiadają również międzynarodowe certyfikaty, takie jak 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