IstroSec

Data Sheet

Intelligence

Dáta sú v dnešnej dobe najcennejšou komoditou organizácií. Tento fakt si uvedomujú aj útočníci, čo odráža rozmach rôznych ilegálnych trhov a poloverejných diskusných fór, ktoré obchodujú s osobnými a firemnými dátami. Monitorovaním týchto trhov a fór je možné zistiť, na aké útoky sa momentálne sústreďuje väčšina ilegálnej hackerskej komunity, na aké zraniteľnosti sa zameriavajú a aké dáta už útočníkmi boli zneužité (interné dokumenty, používateľské údaje, a podobne).

> *Vďaka zvereniu monitorovania týchto aktivít a údajov o Vašej organizácii do rúk odborníkov zo spoločnosti IstroSec budete informovaní o aktuálnych útokoch relevantným pre Vašu organizáciu, zraniteľnostiach a spôsoboch zmiernenia potenciálneho rizika.*

Typy intelligence

Cielená intelligence o hrozbách. Akčný informačný kanál relevantný pre organizáciu zákazníka. Odborníci z **Istro**Sec poskytujú komplexné služby od analýzy požiadaviek, poskytovania použiteľných informácií o hrozbách a implementácie spotrebiteľov v cieľových organizáciách.

Monitorovanie uniknutých dát. Odborníci z **Istro**Sec budú monitorovať potenciálne úniky dát zo zákazníckych organizácií zverejnené na clear webe, deep webe a dark webe.

Prehľady hrozieb. Odborníci z **Istro**Sec pripravia intelligence reporty pre najvyšší a / alebo stredný manažment, týkajúce sa aktuálnych hrozieb a zneužitých zraniteľností, ktoré sú relevantné pre konkrétnu organizáciu.

Služba obsahuje:

- Monitorovanie uniknutých dát na clear, deep aj dark webe
- Poskytnutie informačného kanálu relevantného pre danú organizáciu, obsahujúceho aktuálne informácie o kybernetických hrozbách pre daný sektor
- Poskytovanie použiteľných informácií o hrozbách
- Pripravenie správy pre vyšší a stredný manažment, obsahujúci zoznam aktuálnych hrozieb a zneužívaných zraniteľností relevantných pre danú organizáciu

Report obsahuje:

- Informácie o zraniteľnosti a spôsobe jej opravy alebo aspoň zmiernenia rizika kompromitácie, pokiaľ oprava ešte nie je k dispozícii
- Dáta organizácie, ktoré boli nájdené uniknuté na webe
- Prehlaď APT skupín zameriavajúcich sa na odvetvie, v ktorom organizácia pôsobí a spôsoby ako zmierniť riziko kompromitácie týmito skupinami
- Indikátory kompromitácie
- Taktiky, techniky a postupy útočníkov
- Odporúčania nástrojov, konfigurácií a iných opatrení na prevenciu voči aktuálnym hrozbám

IstroSec

Data Sheet

Prečo práve my?

Skúsenosti a znalosti

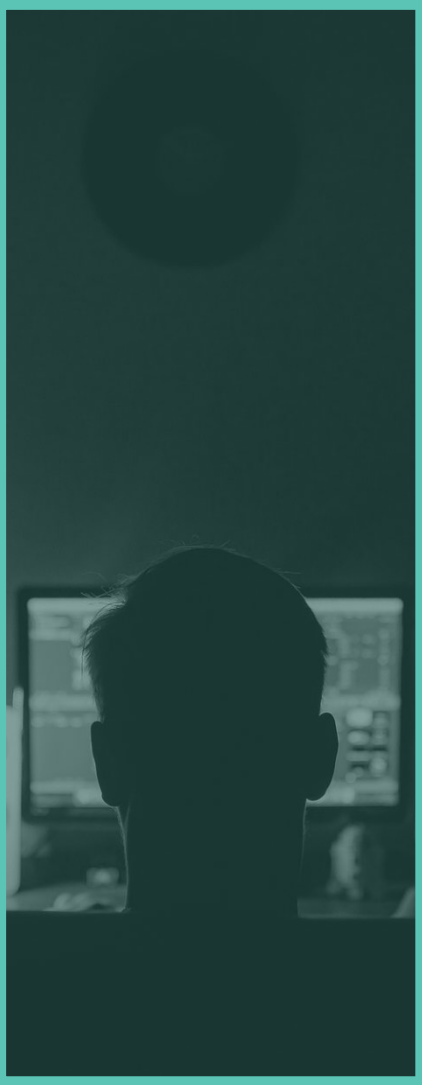
Špecialisti **Istro**Sec majú skúsenosti s vyhľadávaním, spracovávaním a analýzou dát o kybernetických bezpečnostných hrozbách. Poznajú taktiky, techniky a postupy útočníkov a majú znalosti potrebné na to, aby Vám umožnili robiť bezpečnostné rozhodnutia na základe dát o aktuálnych hrozbách.

Expertíza v oblasti intelligence

Expertíza v oblasti intelligence a mnohých ďalších oblastiach, ako napr. reakcia na incidenty, forenzná analýza a analýza malvéru na svetovej úrovni, ktorú viackrát preukázali pri riešení štátmi sponzorovaných kybernetických útokov, útokov vedených voči organizáciám FORTUNE 500 ako aj účasťou 4 expertov spoločnosti **Istro**Sec vo víťaznom tíme cvičenia LockedShields 2016.

Certifikovaní profesionáli

Experti **Istro**Sec sú držiteľmi medzinárodne uznávaných certifikátov v mnohých oblastiach. Držíme certifikáty, ako napríklad 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) a ďalšie.



Prípadová štúdia

Typ organizácie: Výrobca v elektrotechnickom priemysle

Poskytnutá služba: Intelligence

Riešenie: Monitorovanie hackerských fór

Na GitHube sa zverejnila zraniteľnosť, ktorá bola opravená v aktualizácii z predchádzajúceho týždňa. Išlo o zraniteľnosť umožňujúcu získať privilégiá na úrovni systému. Na hackerskom fóre bol zverejnený príspevok, ktorý odkazoval na zraniteľnosť a taktiež na zoznam zariadení, na ktorých je možné túto zraniteľnosť zneužiť. Útočníci si vyberajú obete na základe pomeru náročnosti útoku a potenciálneho zisku. Často začínajú prezretím zoznamu organizácií, ktoré už boli kompromitované a ich údaje sa nachádzajú voľne prístupné na dark webe. Predpokladajú totiž, že ak organizácia bola kompromitovaná raz, tak jej kyberbezpečnostné praktiky nie sú príliš vyvinuté. Následne začnú pripravovať čerstvo zverejnenú zraniteľnosť na použitie voči takejto organizácii.

Tím **Istro**Sec v rámci monitorovania takýchto hackerských fór a ďalších zdrojov spozoroval, že sa zvyšuje početnosť výskytu správ o tejto zraniteľnosti a potenciálnych obetiach. Analytik zo spoločnosti **Istro**Sec porovnal údaje svojich klientov v databáze a zistil, že jeden z jeho zákazníkov používa systémy zraniteľné voči tomuto typu útoku.

Zákazník bude notifikovaný a vypracuje sa report o potencionálnej hrozbe, ktorý obsahuje:

- Informácie o zraniteľnosti a spôsobe jej opravy alebo aspoň zmiernenia rizika kompromitácie, pokiaľ oprava ešte nie je k dispozícii
- Dáta organizácie, ktoré boli nájdené uniknuté na webe
- Prehľad APT skupín zameriavajúcich sa na odvetvie, v ktorom organizácia pôsobí a spôsoby ako zmierniť riziko kompromitácie týmito skupinami