IstroSec

Data Sheet

Threat hunting a posúdenie kompromitácie

Threat hunting je činnosť pri ktorej proaktívne hľadáme v infraštruktúre podozrivú, škodlivú aktivitu prípadne jej pozostatky. V dnešnej dobe sú útočníci a ich snahy preniknúť do cieľovej infraštruktúry čoraz viac sofistikované. Ich činnosť býva často nepovšimnutá komerčnými riešeniami (EDR, AV, atď.) až kým nie je neskoro.

> *Počas „lovu“ sa sústredí na podozrivé aktivity ktoré by mohli znamenať činnosť útočníka, podozrivú činnosť, zraniteľné systémy a taktiež rizikové postupy v IT ako sú ľahko prístupné heslá, zbytočné admin privilégia, atď.*

Predpoklady

- Prístup do SIEM (prípadne EDR a iných logovacích zberačov) klienta
- Možnosť robiť dopyty na dáta koncových zariadení
- Read access a možnosť pracovať s logmi koncových zariadení
- Optional: Predošlé výstupy penetračných testov, auditov, incidentov a podobne

Threat hunting - Basic obsahuje:

- Kontrola IOC v sieťovej komunikácii (ak je to možné).
- Automatizovaná kontrola kľúčových assetov klienta voči IstroSec databáze indikátorov kompromitácie.
- Vypracovanie threat-hunting hypotézy na základe klientovej organizácie. Ako dodatočnú službu vieme poskytnúť vypracovanie “Threat landscape" na špecifickú organizáciu.
- Identifikácia možných zdrojov dát relevantných pre threat-hunting hypotézu a ich analýza.
- Automatizovaná kontrola logov koncových zariadení a vyčlenenie podozrivých eventov.
- Inventarizácia programov, ich verzie a zraniteľností na danú verziu (ak to klientove nástroje umožňujú).
- Prístup k relevantným zdrojom dát (implementácia technológií alebo nástrojov od spoločnosti ISTROSEC).
- Základná identifikácia outlierov v infraštruktúre.

Threat hunting - full obsahuje:

- Analýza možností klienta a navrhnutie vhodných komerčných alebo otvorených nástrojov na monitorovanie infraštruktúry.
- Pomoc z nasadením nástrojov u klienta, jednorazové nastavenie dopytov na mieru pre klientovu infraštruktúru.
- Podrobná manuálna analýza výstupov.

Výstup

- Report obsahujúci manažérske zhrnutie, technické detaily a odporúčané nápravy zistených problémov.
- Dopyty vykonané pri analýze infraštruktúry.

IstroSec

Data Sheet

Prečo práve my?

Skúsenosti a znalosti

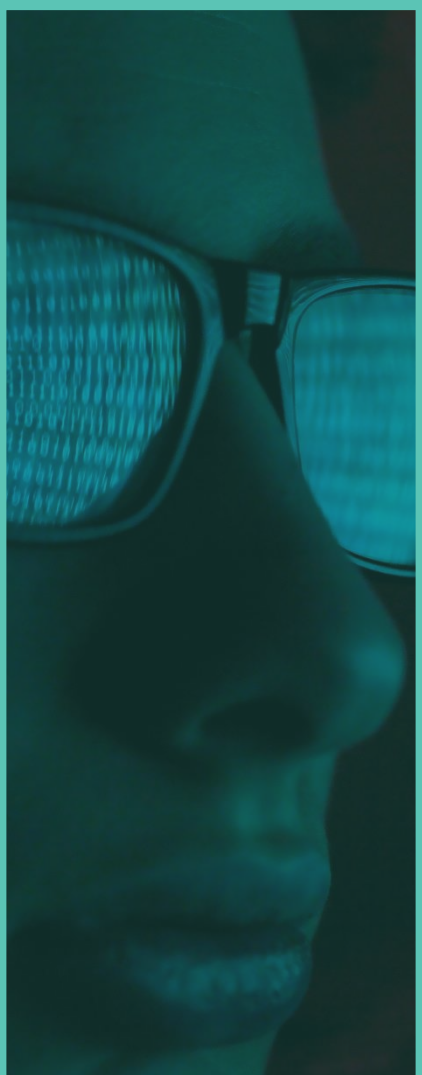
Špecialisti z **Istro**Sec majú skúsenosti s vykonávaním threat huntingu naprieč veľkým množstvom komerčných, verejne dostupných aj natívnych nástrojov. Taktiež majú praktické skúsenosti s útočníkmi od script kiddie úrovne až po štátom sponzorované APT. Poznajú taktiky, techniky a postupy útočníkov a majú znalosti potrebné na to, aby Vám umožnili robiť bezpečnostné rozhodnutia na základe dát o aktuálnych hrozbách.

Expertíza v oblasti intelligence

Expertíza v oblasti threat huntingu 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: Organizácia v sektore, ktorý je lukratívnym cieľom pre útočníkov

Poskytnutá služba: Threat hunting

Riešenie: Posúdenie kompromitácie a threat hunting po zverejnení zero-day zraniteľnosti

Výrobca jedného z nasadených softvérových produktov vydal varovanie o závažnej zero-day zraniteľnosti, o ktorej existujú indikácie o aktuálnom zneužívaní útočníkmi na prienik do infraštruktúry. Threathunting tím **Istro**Sec bol inštruovaný preveriť, či organizácia bola kompromitovaná. Následne tento tím zozbieral dostupné údaje o zraniteľnosti od výrobcu a zo zdrojov v rámci IT bezpečnostnej komunity a na ich základe určil stratégiu threat huntu a indikátorov kompromitácie, ktoré boli počiatočným bodom threat huntu. Tím zmapoval prostredie klienta s dôrazom na identifikáciu dostupných zdrojov informácií o dianí v infraštruktúre - logy zraniteľných aplikácií, logy sieťovej prevádzky, logy z lokálneho DNS servera, systémové logy zariadení a logy nasadeného SIEM riešenia. V logoch zraniteľnej aplikácie boli nájdené záznamy o chybách konzistentné s pokusmi o zneužitie danej zraniteľnosti.

Na základe časovej korelácie boli v logoch sieťovej komunikácie identifikované podozrivé pripojenia. Reputácia zdrojových IP adries bola preverená voči zdrojom IT bezpečnostnej komunity (threat intelligence), avšak zatiaľ nebol žiaden dostupný záznam. Plný záznam sieťovej komunikácie v podobe paketov nebol k dispozícii. Štatistická analýza sieťovej prevádzky zároveň ukázala, že zariadenie začalo vykonávať viac DNS dopytov ako do momentu podozrivej aktivity, čo by mohlo indikovať beaconing a vytvorený C2 kanál útočníkom. Na zariadenie s podozrivou aktivitou bolo operatívne nainštalované EDR riešenie, ktoré pomohlo identifikovať beaconujúci proces a zaistiť vzorky súvisiacich súborov.

Tím odporučil vyhlásenie bezpečnostného incidentu a povolanie forenzných a malvérových analytikov. Threat hunt pokračoval ďalej v podpornej úlohe pri riešení incidentu. Podozrivé IP adresy boli zablokované na perimetrovom firewalle. Malvér analýza identifikovala vzorky ako DNS beacon zo suity CobaltStrike. Forenzná analýza odhalila aktivitu zameranú na krádež prihlasovacích údajov ešte v čase, keď na zariadení nebolo EDR riešenie. V rámci pokračujúceho threat huntingu bola v logoch SIEM preverená aktivita všetkých používateľských účtov nájdených na zaistenom zariadení a ukázalo sa, že jeden administrátorský účet sa v čase po kompromitácii prihlasoval na viacero interných serverov, pričom samotný používateľ takúto aktivitu nepotvrdil. Na základe toho bola v rámci containment fázy incidentu odporučená zmena všetkých používateľských hesiel a reset služby Kerberos.

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