IstroSec

Data Sheet

Digitálna forenzná analýza

Digitálna forenzná analýza je systematické vyšetrovanie zariadenia, systému, sieťovej komunikácie alebo obrazu pamäte. V kontexte riešenia kybernetických bezpečnostných incidentov je jej cieľom odpovedať v závislosti od typu analýzy na otázky.

Digitálna forenzná analýza prebieha vo fázach:

- Zaistenie digitálnych stôp.
- Analýza digitálnych stôp.
- Vypracovanie správy, reportu alebo posudku.

Pri zaistení digitálnych stôp je potrebné zabezpečiť:

- **Korektnosť** - získané stopy sú totožné s dátami z pôvodného média.
- **Autentickosť** - získané stopy pochádzajú z analyzovaného zariadenia/systému/zdroja v danom čase.
- **Integrita** - získané stopy nesmú byť v čase pozmenené, resp. je ich zmenu možné detegovať.
- **Dôvernosť** a dostupnosť.

Prečo IstroSec?

Kombinované skúsenosti expertov viac ako 70 rokov

Prístup k odborníkom na všetky oblasti informačnej bezpečnosti, vrátane audítorov, penetračných testerov, forenzných analytikov, analytikov malvéru, školiteľov a ďalších

Systematické zlepšenie informačnej bezpečnosti v zmysle štandardov a na základe skúseností s riešením pokročilých bezpečnostných incidentov

Certifikovaní odborníci a zaistenie súladu s bezpečnostnými štandardmi a legislatívou - skúsenosti z verejnej správy (zákon o kybernetickej bezpečnosti, zákon o ITVS a iné) ako aj zo súkromného sektora (ISO 27001, NIST, HIPAA a iné)

Metodológia IstroSec:

Aby boli zaistené všetky uvedené atribúty pri zaisťovaní digitálnych stôp, **Istro**Sec má metodológiu pre zaisťovanie digitálnych stôp z pracovných staníc, serverov, sieťových a bezpečnostných technológií, externých médií, mobilných telefónov a cloudu.

Pri zaisťovaní používajú špecialisti **Istro**Sec metodológiu využívajúcu aktuálne best practices a postupy uznávané pred súdmi na Slovensku, v EÚ a USA.

Typy forenznej analýzy:

- Rýchla forenzná analýza - triáž
- Štandardná forenzná analýza
- Špeciálna forenzná analýza

IstroSec

Data Sheet

Rýchla forenzná analýza - triáž

Popis

Pri forenznej triáži sa zameriavame na identifikáciu základných indikátorov kompromitácie. Vykonávame ju spravidla automatizovanými nástrojmi. Forenzná triáž má význam najmä v prípadoch keď je potenciálne kompromitovaných viacero zariadení a je súčasťou incident response. Vtedy je potrebné určiť, ktoré zo zariadení sú v skutočnosti kompromitované, ktoré zariadenie bolo infikované ako prvé, či ktoré bolo útočníkmi použité na kompromitáciu ďalších systémov.

Predpoklady:

- Poskytnutie disku alebo forenzného obrazu disku zo skúmaného zariadenia resp. zaistenie digitálnych stôp
- Poskytnutie lokálnych systémových logov (Windows event logs), webserver access logy
- Poskytnutie logov z centrálneho logovacieho systému v prípade, že logy sú centralizované v systéme na manažment logov (log management solution)

Služba zahŕňa:

- Scan poskytnutých zariadení a dát na prítomnosť známeho malware
- V prípade podozrenia na konkrétnu skupinu útočníkov a pri znalosti ich TTPs (Tactics, Techniques and Procedures), scan zariadení a dát na prítomnosť indikátorov (IOC) špecifických pre danú skupinu
- Vyhľadávanie indikátorov perzistencie (cca viac ako 100 rôznych zdrojov perzistencie)
- Vyhľadávanie stôp indikujúcich spustenie programov
- Vyhľadávanie stôp indikujúcich otvorenie alebo nahliadnutie súborov a priečinkov
- Vyhľadávanie stôp indikujúcich laterálny pohyb (pohyb medzi zariadeniami)
- Vyhľadávanie stôp šifrovania
- Automatizovaná a čiastočná manuálna analýza logov

Výstupy:

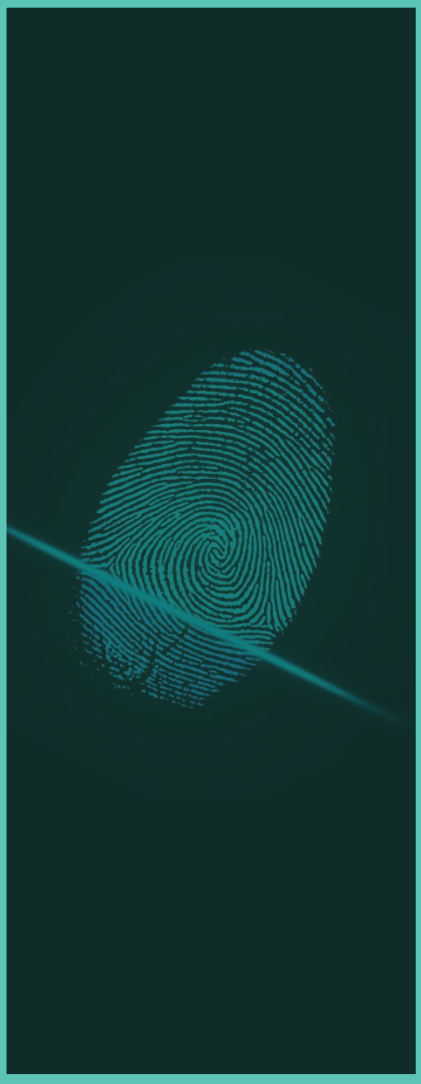
- Súhrn výsledkov analýzy, ktorý je ďalej použiteľný ako podklad pre riešenie bezpečnostného incidentu (vo fázach Containment, Eradication alebo Recovery)

Forenzná triáž štandardne odpovedá napríklad na otázky:

- Je analyzované zariadenie kompromitované?
- Nachádzajú sa na systéme IOC v rámci riešeného prípadu?
- Ktoré ďalšie systémy boli napadnuté z analyzovaného systému?
- Z ktorých zariadení sa pristupovalo na analyzované zariadenie?
- Ktoré účty boli kompromitované?
- Aký spôsob používa útočník na C2 (Command and Control)?
- Aké mechanizmy perzistencie boli použité?
- Boli vykonané pokusy o zametenie stôp?
- Sú bezpečnostné mechanizmy systému nedotknuté?

IstroSec

Data Sheet



Prípadová štúdia 1

Typ organizácie: Súkromný poskytovateľ zdravotníckych služieb

Poskytnutá služba: Digitálna forenzná analýza

Riešenie: Rýchla forenzná analýza - triáž

V organizácií prebieha bezpečnostný incident a šíri sa v nej ransomvér REvil. Forenznému teamu **Istro**Sec bol doručený forezný obraz pracovnej stanice napadnutej ransomvérom. Úlohou teamu je vykonať forenznú triáž a získať indikátory kompromitácie, overiť existenciu perzistencie a identifikovať spôsob šírenia ransomvéru.

Forenzný tím **Istro**Sec vykonal forenznú triáž a identifikoval:

- Malware vzorka s MD5 544900a52XXXXf2e4fe7598985bc688f sa nachádza v adresári C:\Users\Public\ s náhodným názvom.
- Ransomvér je spustený prostredníctvom naplánovanej úlohy v adresári C:\Windows\System32\Tasks s názvom WindowsUpdate.job
- Ransomvér je distribuovaný z doménového Controllera MAINDC01.organizacia.local prostredníctvom doménovej politiky s názvom „ServerHardening“
- Na spustenie úlohy sa používa účet organizacia.local\BackupAdmin
- Na pracovnej stanici sa nachádza aj malware TrickBot v adresári C:\Windows\SysWow64\ s názvom wmicmain.exe
- Perzsistencia malware je zabezpečená prostredníctvom registrového kľúča HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run s názvom WindowsTelemetry.

Informácie získané z forenznej triáže boli použité na zamedzenie šírenia škodlivého kódu prostredníctvom odpojenia doménového radiča MAINDC01.organizacia.local zo siete. Team riešiaci incident napísal rozšírenie pre EDR používané v organizácií, ktoré odstránilo infekciu z organizácie.

Štandardná forenzná analýza

Popis

Pri štandardnej forenznej analýze je predmetom skúmania jeden alebo viac potenciálne kompromitovaných systémov. Analyzujeme forenzné artefakty, ktoré na systéme zostávajú po inštalácií či spustení programov, Windows registre, záznamy udalostí (Event Logy). Zisťujeme, ako používatelia interagovali so systémom, kedy sa prihlasovali a odhlasovali, aké programy použili a kedy, k akým súborom pristupovali a podobne.

Štandardná forenzná analýza pokrýva širokú paletu prípadov, napríklad vyšetrovanie incidentov spojeného so škodlivým kódom alebo ransomvérom, ako aj vyšetrovanie krádeže údajov až po kompletné kompromitácie systémov a identifikácie podozrivých transakcií.

Predpoklady:

- Poskytnutie disku alebo forenzného obrazu disku zo skúmaného zariadenia alebo zaistenie digitálnych stôp expertmi IstroSec
- Poskytnutie dodatočných dát, ako napríklad záloh lokálnych systémových logov obsahujúce dáta nad rámec dát prítomných na disku/v image (Windows event logs), webserver access logy a iné
- Obraz pamäte RAM zariadenia

Služba zahŕňa:

- Zber dát o systéme
- Vyhľadávanie stôp indikujúcich zaisťovanie perzistencie útočníka
- Automatizovaný scan poskytnutých stôp na prítomnosť známych hrozieb (AV, Loki)
- Vyhľadávanie stôp indikujúcich spustenie programov
- Vyhľadávanie stôp indikujúcich otvorenie alebo nahliadnutie súborov a priečinkov
- Vyhľadávanie stôp indikujúcich laterálny pohyb (pohyb medzi zariadeniami)
- Vyhľadávanie stôp šifrovania
- Komplexná analýza logov
- Analýza timeline
- Analýza používateľskej činnosti, história internetovej aktivity
- Automatizovaná a manuálna analýza Microsoft Event Logov a ďalších logov nachádzajúcich sa na zariadení
- Analýzu pamäte RAM

Výstupy:

- Report s podrobnými výsledkami analýzy pre každú poskytnutú digitálnu stopu (disk, image disku, export logov a pod.)
- Manažérske zhrnutie výstupov analýzy v osobitnom dokumente
- Časová os útoku a najvýznamnejších udalostí v priebehu incidentu
- V prípade potreby je možné aj spracovanie znaleckého posudku v odvetviach:
    - Kriminalistická informatika
    - Bezpečnosť a ochrana informačných systémov

Štandardná forenzná analýza odpovedá napríklad na otázky:

- Ktoré zariadenie bolo infikované ako prvé? (Patient 0)
- Ako sa útočník dostal na prvé zariadenie? (Patient 0)
- Akú aktivitu útočník vyvíjal na zariadení?
- Akú zraniteľnosť útočník použil pri kompromitácií prvotného zariadenia?
- Aké súbory útočník otváral alebo prezeral?
- Klikol používateľ na spearphishingový email?
- Boli exfiltrované dáta?
- Pristúpil útočník k nejakej špecifickej databáze?
- Modifikoval útočník dokumenty na zariadení?
- Modifikoval útočník databázu?

IstroSec

Data Sheet

Prípadová štúdia 2

Typ organizácie: Súkromný poskytovateľ zdravotníckych služieb

Poskytnutá služba: Digitálna forenzná analýza

Riešenie: Štandardná forenzná analýza

V organizácií prebieha bezpečnostný incident. V organizácií sa šíri ransomvér REvil. Forenznému teamu IstroSec bol doručený forenzný obraz pracovnej stanice napadnutej ransomvérom. Úlohou teamu je vykonať forenznú analýzu a identifikovať vektor útoku, identifikovať zariadenie, ktoré bolo napadnuté ako prvé. Forenzný tím vykonal forenznú analýzu predloženého obrazu a identifikoval, že ransomvér bol distribuovaný z doménového radiča MAINDC01.organizacia.local ako naplánovaná úloha prostredníctvom doménovej politiky s názvom „ServerHardening“. Rovnako ako REvil bol distribuovaný aj škodlivý kód typu TrickBot. Na zariadení nebol identifikovaný žiadny ďalší prístup útočníka. Analýza malvéru ukázala, že malvér TrickBot na tomto zariadení nedostal od riadiaceho servera žiadne príkazy.

Po zaistení forenzného obrazu pamäte a diskov doménového radiča MAINDC01.organizacia.local bola na tomto zariadení vykonaná forenzná analýza a bolo identifikované:

- Útočník sa na zariadení nachádzal 6 mesiacov pred spustením ransomvéru v organizácií
- Útočník pristupoval na doménový radič z IP adresy 10.10.15.29
- Útočník pristupoval z doménového zariadenia na súborový server File01.organizacia.local a databázový server Database05.organizacia.local, stiahol súbor x.zip a poslal ho prostredníctvom nástroja WinSCP na adresu riadiaceho servera utocnik.example

Na základe uvedených zistení boli zaistené digitálne stopy z pracovnej stanice 10.10.15.29 a serverov File01.organizacia.local a Database05.organizacia.local. Pre zariadenie 10.10.15.29 bude vykonaná štandardná forenzná analýza. Pre zariadenia File01.organizacia.local a Database05.organizacia.local bola odporučená zákazníkovi kompletná analýza exfiltrácie dát z uvedených serverov s cieľom identifikovať uniknuté dokumenty - viď nižšie.

Na zariadení 10.10.15.29 bola vykonaná forenzná analýza a bolo identifikované:

- Zariadenie 10.10.15.29 je Patient 0 infekcie.
- Používateľ john.smith klikol dňa 10.1.2021 na spearphishingový email od anna.bell@partnerOrganisati0n.com s predmetom “Opatrenia pocas pandemie Covid19 v budove PartnerOrganisation”. Email obsahoval infikovanú prílohu, ktorá po otvorení spustila škodlivý kód TrickBot s riadiacim serverom utocnik.example.
- Útočník získal práva lokálneho administrátora prostredníctvom obfuskovaného nástroja Mimikatz.
- Útočník získal NTLM hash doménového administrátora z pamäte za použitia nástroja Mimikatz.

Z incidentu bola vypracovaná komplexná správa, ktorá obsahovala:

- Manažérske zhrnutie
- Časový priebeh incidentu
- Aktivity útočníka v infraštruktúre
- Identifikované zraniteľnosti v infraštruktúre zistené pri forenznej analýze
- Návrhy odporúčaní pre zabezpečenie infraštruktúry.

Špeciálna forenzná analýza

Popis:

Pri hlbšom vyšetrovaní incidentu je potrebné vykonať dodatočné analytické kroky nad rámec základnej forenznej analýzy. Ide napríklad o prípady súvisiace s únikom informácii (data exfiltration), prípady pokročilých cielených útokov, prípady vnútorného narušiteľa a podobne.

Predpoklady:

- Rovnaké ako pri Štandardnej forenznej analýze
- Akékoľvek ďalšie stopy, konkrétnosti závisia od typu prípadu

Služba zahŕňa:

- Všetky body zahrnuté v Základnej forenznej analýze
- Špecifické kroky potrebné pre daný prípad - výber je závislý od okolností prípadu a požiadaviek klienta. Môže ísť napríklad o:
    - Podrobnú analýzu správania používateľa: k akým zdrojom pristupoval a kedy, či použil anonymizačné alebo šifrovacie nástroje a podobne
    - Analýzu emailov
    - Analýza súborových systémov, rekonštrukcia vymazaných častí, kde je to možné
    - Analýza prístupu k databázam
    - Analýza exfiltrácie

Výstupy:

- Report s podrobnými výsledkami analýzy pre každú poskytnutú digitálnu stopu (disk, image disku, export logov a pod.)
- Manažérske zhrnutie výstupov analýzy v osobitnom dokumente
- Časová os útoku a najvýznamnejších udalostí v priebehu incidentu
- Odpovede na otázky stanovené pre danú analýzu, napríklad:
    - Zistenie či boli exfiltrované nejaké dáta a ak áno, ktoré dokumenty unikli
    - Zistenie či a aké dáta boli zo systému vymazané, ktoré používateľské konto či aký nástroj boli na ich odstránenie použité
- V prípade potreby je možné aj spracovanie znaleckého posudku v odvetviach:
    - Kriminalistická informatika
    - Bezpečnosť a ochrana informačných systémov

Uvedené typy forenznej analýzy sú v prípade potreby doplnené :

- **Sieťová forenzná analýza.** V rámci tejto analýzy dochádza k analýze zachytenej komunikácie (full packet capture) alebo analýze netflow.
- **Analýza logov**. V rámci tejto analýzy dochádza k analýze logov sieťových a bezpečnostných prvkov, centrálneho úložiska logov (Log Management Solutions) alebo analýze prostredníctvom nástrojov SIEM.
- **Analýza pamäte**. Analýza zaistenej pamäte (RAM) zariadení.

IstroSec

Data Sheet

Prečo práve my?

Skúsenosti a znalosti

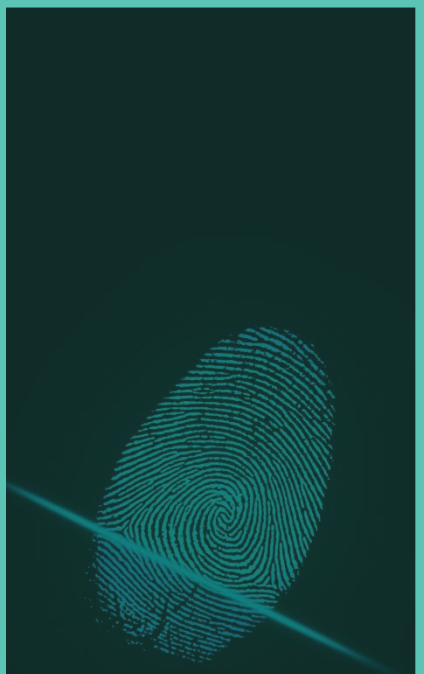
Špecialisti **Istro**Sec majú skúsenosti s digitálnou forenznou analýzou, kde postupujú v zmysle medzinárodne uznávaných štandardov, poznajú taktiky, techniky a postupy útočníkov Poznajú taktiky, techniky a postupy útočníkov a majú znalosti potrebné na to, aby Vám v rámci reakcie na incidenty umožnili robiť rozhodnutia na základe analýzy postupov útočníkov použitých v rámci útoku.

Expertíza v oblasti DFIR

Expertíza v oblasti reakcie na incidenty, digitálnej forenznej analýzy a mnohých ďalších oblastiach, ako napr. a riadenia informačnej bezpečnosti, audit, či 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 3

Typ organizácie: Súkromný poskytovateľ zdravotníckych služieb

Poskytnutá služba: Digitálna forenzná analýza

Riešenie: Špeciálna forenzná analýza

Nadviažeme na vyššie popísaný prípad incidentu infekcie ransomvérom REvil.

Na základe výsledkov forenznej analýzy kompromitovaných zariadení sa zákazník rozhodol pre vykonanie špeciálnej forenznej analýzy. Bola vykonaná kompletná analýza exfiltrácie pre zariadenia File01.organizacia.local a Database05.organizacia.local s cieľom identifikovať dokumenty uniknuté z týchto serverov. V rámci forenznej analýzy bola vykonaná analýza vytvorených, modifikovaných alebo kopírovaných súborov útočníkom. Súčasne bolo identifikované, že útočník pristupoval aj k lokálnym databázam prostredníctvom integrovaného nástroja SQL Server Management Studio. V rámci analýzy boli identifikované údaje, ktoré boli v rámci databáze menené útočníkom.

Z analýzy bola vypracovaná komplexná správa, ktorá obsahovala:

- Manažérske zhrnutie
- Report s podrobnými výsledkami analýzy pre každú poskytnutú digitálnu stopu (disk, image disku, export logov a pod.)
- Zoznam dokumentov, ktoré boli s najväčšou pravdepodobnosťou exfiltrované zo serverov