IstroSec

Arkusz danych

Kryminalistyka cyfrowa

Cyfrowa analiza kryminalistyczna to systematyczne badanie urządzenia, systemu, komunikacji sieciowej lub obrazu pamięci. W kontekście rozwiązywania incydentów z zakresu cyberbezpieczeństwa jej celem jest udzielanie odpowiedzi na pytania w zależności od rodzaju analizy.

Cyfrowa analiza kryminalistyczna składa się z wielu faz:

- Pozyskiwanie dowodów cyfrowych
- Analiza dowodów cyfrowych
- Sporządzanie raportu/briefingu lub ekspertyzy do postępowania sądowego

Podczas pozyskiwania dowodów cyfrowych ważne jest, aby zapewnić:

- **Precyzję - uzyskane dowody są identyczne z danymi z oryginalnych nośników**
- **Integralność - zdobyte dowody nie mogą ulec zmianie w czasie (ich zmiana musi być możliwa do wykrycia)**
- **Autentyczność - pozyskiwane dowody pochodzą z analizowanego urządzenia/systemu/źródła w ustalonym okresie czasu**
- **Poufność i dostępność**

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)

Metodologia IstroSec:

W IstroSec mamy własną metodologię, która zapewnia spełnienie wszystkich powyższych punktów podczas pozyskiwania dowodów cyfrowych ze stacji roboczych, serwerów, nośników zewnętrznych, telefonów komórkowych, chmury oraz technologii sieciowych lub bezpieczeństwa.

Podczas akwizycji nasi specjaliści korzystają z najnowszych najlepszych praktyk uznanych w sądach amerykańskich, unijnych i słowackich.

Rodzaje kryminalistyki cyfrowej:

- Triage kryminalistyczny
- Standardowa kryminalistyka cyfrowa
- Specjalna kryminalistyka cyfrowa

Triage kryminalistyczny

Opis

Strategia triage'u kryminalistycznego polega na zidentyfikowaniu podstawowych wskaźników kompromitacji (IoC), zwykle przy użyciu zautomatyzowanych narzędzi. Triage kryminalistyczny jest szczególnie ważny w przypadkach, w których potencjalnie zagrożone jest wiele urządzeń oraz w zakresie reagowania na incydenty. W takim przypadku istotne jest, aby określić, które z urządzeń zostały zhakowane, które urządzenie zostało zainfekowane jako pierwsze lub które zostało użyte przez atakujących do złamania zabezpieczeń innych systemów.

Warunki wstępne:

- Dostarczenie dysku lub obrazu kryminalistycznego dysku z urządzenia będącego przedmiotem dochodzenia lub pozyskanie dowodów cyfrowych
- Zapewnienie lokalnych dzienników systemowych (dzienniki zdarzeń Windows), dzienniki dostępu do serwera www
- Dostarczanie logów z centralnego systemu logowania w przypadku, gdy logi są scentralizowane w rozwiązaniu do zarządzania logami

Usługa obejmuje:

- Skanowanie dostarczonych urządzeń i danych w poszukiwaniu znanego złośliwego oprogramowania
- Skanowanie w poszukiwaniu odpowiednich wskaźników kompromitacji (IoC) w przypadku podejrzenia określonego napastnika lub grupy hakerskiej przy użyciu wiedzy o jej taktykach, technikach i procedurach (TTP)
- Poszukiwanie wskaźników trwałości (ponad 100 różnych źródeł trwałości)
- Poszukiwanie dowodów wskazujących na wykonanie programu
- Poszukiwanie dowodów wskazujących na otwieranie lub przeglądanie plików i folderów
- Poszukiwanie dowodów wskazujących na ruch boczny (ruch między urządzeniami)
- Wyszukiwanie dowodów na szyfrowanie
- Automatyczna i częściowo ręczna analiza rejestrów

Elementy dostarczane:

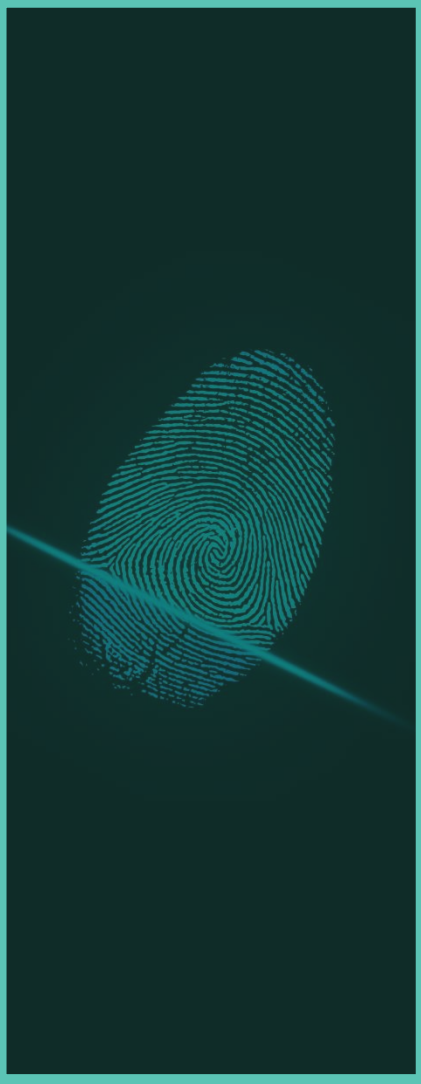
- Podsumowanie wyników analizy z informacjami umożliwiającymi podjęcie działań, aby wspomóc reagowanie na incydenty związane z bezpieczeństwem w fazie powstrzymywania, eliminacji i odzyskiwania.

Triage kryminalistyczny zazwyczaj odpowiada na pytania takie jak:

- Czy analizowane urządzenie jest zagrożone?
- Czy system zawiera wskaźniki IoC związane ze sprawą będącą przedmiotem dochodzenia?
- Które systemy zostały zaatakowane z analizowanego systemu?
- Jakie urządzenia uzyskały dostęp do analizowanego systemu?
- Które konta zostały przejęte?
- Jakiej metody użył atakujący, aby uzyskać dostęp do C2 (Sterowanie i kontrola)?
- Jakie mechanizmy trwałości zostały wykorzystane?
- Czy były próby pozbycia się dowodów?
- Czy mechanizmy bezpieczeństwa w systemie są nienaruszone?
- Czy system zawiera złośliwe oprogramowanie?

IstroSec

Arkusz danych



Studium przypadku 1

Rodzaj firmy: Prywatny dostawca usług opieki zdrowotnej

Świadczone usługi: Kryminalistyka cyfrowa

Rozwiązanie: Triage kryminalistyczny

Incydent bezpieczeństwa ma miejsce w organizacji, rozprzestrzenia się w niej oprogramowanie ransomware REvil. Zespół kryminalistyki **Istro**Sec otrzymał obraz kryminalistyczny stacji roboczej zaatakowanej przez oprogramowanie ransomware.

Zadaniem zespołu jest przeprowadzenie triage'u kryminalistycznego i uzyskanie wskaźników narażenia, zweryfikowanie istnienia trwałości oraz zidentyfikowanie sposobu rozprzestrzeniania się ransomware.

Zespół kryminalistyki **Istro**Sec przeprowadził triage i ustalił, co następuje:

- Próbka złośliwego oprogramowania z MD5 544900a52XXXXf2e4fe7598985bc688f znajduje się w katalogu C:\Users\Public\ z losową nazwą.
- Ransomware jest uruchamiane przez zaplanowane zadanie w katalogu C:\Windows\System32\Tasks o nazwie WindowsUpdate.job
- Oprogramowanie ransomware jest dystrybuowane z kontrolera domeny MAINDC01.organization.local poprzez politykę domeny o nazwie „ServerHardening”
- Do uruchomienia zadania służy konto Organization.local\BackupAdmin
- Na stacji roboczej w katalogu C:\Windows\SysWow64\ znajduje się złośliwe oprogramowanie TrickBot o nazwie wmicmain.exe
- Trwałość złośliwego oprogramowania jest zabezpieczana za pomocą klucza rejestru HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run o nazwie WindowsTelemetry.

Informacje uzyskane poprzez triage kryminalistyczny zostały wykorzystane do zapobiegania rozprzestrzenianiu się złośliwego kodu poprzez odłączenie kontrolera domeny MAINDC01.organizacia.local od sieci. Zespół ds. incydentów napisał rozszerzenie dla EDR używanego w organizacji, które usunęło następnie infekcję z organizacji.

Standardowa kryminalistyka cyfrowa

Opis

W standardowej analizie kryminalistycznej badany jest co najmniej jeden potencjalnie zagrożony system. Analizujemy pliki, które pozostają w systemie po zainstalowaniu lub uruchomieniu programów, rejestrów systemu Windows lub dzienników zdarzeń. Dowiadujemy się, w jaki sposób użytkownicy wchodzili w interakcję z systemem, kiedy się logowali i wylogowywali, jakich programów używali i kiedy, do jakich plików mieli dostęp etc.

Standardowa analiza kryminalistyczna obejmuje szeroki zakres spraw, takich jak badanie incydentów związanych ze złośliwym kodem lub oprogramowaniem ransomware, a także badanie naruszeń danych, aż do całkowitego włamania się do systemów i identyfikacja podejrzanych transakcji.

IstroSec

Arkusz danych

Warunki wstępne:

- Przesłanie dysku lub obrazu urządzenia będącego przedmiotem dochodzenia lub pozyskanie dowodów cyfrowych przez ekspertów IstroSec
- Dostarczenie dodatkowych danych, takich jak kopie zapasowe lokalnych dzienników systemowych zawierających dane wykraczające poza dane już znajdujące się na dostarczonym dysku/obrazie, dzienniki dostępu do serwera WWW i inne
- Obraz pamięci RAM urządzenia

Usługa obejmuje:

- Zbieranie danych systemowych
- Poszukiwanie wskazówek wskazujących na przyczółek napastnika
- Automatyczne skanowanie dostarczonych dowodów na obecność znanych zagrożeń (AV, Loki)
- Poszukiwanie dowodów wskazujących na wykonanie programu
- Poszukiwanie dowodów wskazujących na otwieranie lub przeglądanie plików i folderów
- Poszukiwanie dowodów wskazujących na ruch boczny (ruch między urządzeniami)
- Wyszukiwanie dowodów na szyfrowanie
- Kompleksowa analiza rejestrów
- Analiza osi czasu
- Analiza aktywności użytkowników, historia aktywności w Internecie
- Automatyczna i ręczna analiza dzienników zdarzeń firmy Microsoft i innych dzienników znajdujących się na urządzeniu
- Analiza pamięci RAM

Elementy dostarczane:

- Raport ze szczegółowymi wynikami analizy dla każdego dostarczonego dowodu cyfrowego (napęd, obraz kryminalistyczny, eksport rejestrów itp.)
- Podsumowanie wyników analizy w osobnym dokumencie
- Kalendarium ataku i najważniejsze wydarzenia podczas incydentu
- W razie potrzeby istnieje również możliwość sporządzenia opinii biegłego sądowego z następujących branż:
    - Informatyka kryminalistyczna
    - Bezpieczeństwo i ochrona systemów informatycznych

Standardowa kryminalistyka cyfrowa zazwyczaj odpowiada na pytania takie jak:

- **Które urządzenie zostało zainfekowane jako pierwsze?** (Pacjent 0)
- Jak atakujący włamał się do pierwszego urządzenia? (Pacjent 0)
- Jaką aktywność wykonał atakujący na urządzeniu?
- Jakiej luki użył atakujący, aby zhakować oryginalne urządzenie?
- Jakie pliki otworzył lub wyświetlił atakujący?
- Czy użytkownik kliknął wiadomość e-mail z spear phishingiem?
- Czy dane zostały eksfiltrowane?
- Czy atakujący uzyskał dostęp do konkretnej bazy danych?
- Czy atakujący zmodyfikował dokumenty na urządzeniu?

Studium przypadku 2

Rodzaj firmy: Prywatny dostawca usług opieki zdrowotnej

Świadczone usługi: Kryminalistyka cyfrowa

Rozwiązanie: Standardowa kryminalistyka cyfrowa

W organizacji ma miejsce incydent z zakresu bezpieczeństwa. Rozprzestrzenia się w niej oprogramowanie ransomware REvil. Zespół kryminalistyki IstroSec otrzymał obraz stacji roboczej zaatakowanej przez oprogramowanie ransomware. Zadaniem zespołu jest przeprowadzenie analizy kryminalistycznej i zidentyfikowanie wektora ataku oraz zidentyfikowanie urządzenia, które zostało zaatakowane jako pierwsze. Zespół kryminalistyki przeprowadził analizę kryminalistyczną przesłanego obrazu i stwierdził, że oprogramowanie ransomware zostało rozesłane z kontrolera domeny MAINDC01.organization.local jako zaplanowane zadanie za pomocą polityki domeny o nazwie „Server-Hardening". Oprócz REvil rozprowadzany był również złośliwy kod TrickBot. Na urządzeniu nie zidentyfikowano żadnego innego dostępu atakującego. Analiza wykazała, że złośliwe oprogramowanie TrickBot na tym urządzeniu nie otrzymywało żadnych poleceń z serwera kontrolnego.

Po uzyskaniu obrazu pamięci i dysków kontrolera domeny MAINDC01.organization.local przeprowadzono analizę kryminalistyczną na tym urządzeniu i stwierdzono, że:

- Atakujący był obecny na urządzeniu 6 miesięcy przed uruchomieniem oprogramowania ransomware w organizacji
- Atakujący uzyskał dostęp do kontrolera domeny z adresu IP 10.10.15.29
- Atakujący uzyskał dostęp do serwera plików File01.organization.local i serwera bazy danych Database05.organization.local z urządzenia domeny, pobrał plik x.zip i wysłał go za pomocą narzędzia WinSCP na adres serwera kontrolnego attacker.example

Na podstawie powyższych ustaleń pobrano dowody cyfrowe ze stacji roboczej 10.10.15.29 oraz serwerów File01.organization.local i Database05.organizacia.local. Standardową analizę kryminalistyczną należy przeprowadzić dla 10.10.15.29. Dla urządzeń File01.organization.local i Database05.organization.local zalecono wykonanie pełnej analizy eksfiltracji danych z wyżej wymienionych serwerów w celu zidentyfikowania wyciekających dokumentów - patrz poniżej.

Przeprowadzono analizę kryminalistyczną urządzenia w dniu 10.10.15.29 i stwierdzono, że:

- Urządzenie z 10.10.15.29 to Pacjent 0 infekcji.
- 10 stycznia 2021 r. użytkownik john.smith kliknął wiadomość e-mail typu spear phishing od anna.bell@partnerOrganisati0n.com z tematem „Środki podczas pandemii Covid19 w budynku PartnerOrganization". Wiadomość e-mail zawierała zainfekowany załącznik, który po otwarciu uruchamiał złośliwy kod TrickBota na serwerze kontrolnym attacker.example
- Atakujący uzyskał uprawnienia administratora lokalnego za pomocą utajonego narzędzia Mimikatz.
- Atakujący uzyskał z pamięci skrót NTLM administratora domeny za pomocą Mimikatz.

Z przeprowadzonej kryminalistyki cyfrowej sporządzono obszerny raport, który obejmował:

- Streszczenie
- Kalendarium incydentu
- Aktywność atakującego w infrastrukturze ofiary
- Słabe punkty zidentyfikowane w infrastrukturze podczas cyfrowej analizy kryminalistycznej
- Rekomendacje dotyczące poprawy bezpieczeństwa infrastruktury.

Specjalna kryminalistyka cyfrowa

Opis:

Dogłębne badanie incydentu wymaga dodatkowych kroków analitycznych wykraczających poza podstawową analizę kryminalistyczną. Są to na przykład sprawy związane z eksfiltracją danych, przypadki zaawansowanych ataków ukierunkowanych, przypadki ataków z wykorzystaniem informacji wewnętrznych etc.

Warunki wstępne:

- Takie same jak w przypadku standardowej kryminalistyki cyfrowej
- Każdy inny rodzaj dowodów cyfrowych, w zależności od rodzaju incydentu

Usługa obejmuje:

- Takie same jak w przypadku standardowej kryminalistyki cyfrowej
- Konkretne kroki w konkretnej sprawie – w dużej mierze zależne od okoliczności sprawy i wymagań klienta. Na przykład:
  - Szczegółowa analiza zachowań użytkowników; do jakich zasobów uzyskano dostęp i kiedy, czy użyto narzędzi do anonimizacji lub szyfrowania itp.
  - Analiza wiadomości e-mail
  - Analiza systemu plików, rekonstrukcja usuniętych plików tam, gdzie to możliwe
  - Analiza dostępu do bazy danych
  - Analiza eksfiltracji

Elementy dostarczane:

- Raport ze szczegółowymi wynikami analizy dla każdego dostarczonego dowodu cyfrowego (napęd, obraz kryminalistyczny, eksport logów itp.)
- Podsumowanie wyników analizy w osobnym dokumencie
- Kalendarium ataku i najważniejsze wydarzenia podczas incydentu
- Odpowiedzi na pytania zadane do analizy, na przykład:
  - Czy jakiekolwiek dane zostały wykradzione, a jeśli tak, to jakie dokumenty wyciekły
  - Czy i jakie dane zostały usunięte z systemu, jakie konto użytkownika lub jakie narzędzie zostało użyte do ich usunięcia
- W razie potrzeby istnieje również możliwość sporządzenia opinii biegłego sądowego z następujących branż:
  - Informatyka kryminalistyczna
  - Bezpieczeństwo i ochrona systemów informatycznych

W razie potrzeby powyższe rodzaje kryminalistyki cyfrowej można rozszerzyć o następujące elementy:

- **Network forensics** – analiza przechwyconej komunikacji sieciowej (Full-packet Capture) lub analiza netflow.
- **Analiza rejestrów** – analiza logów sieci i urządzeń bezpieczeństwa, analiza rozwiązań centralnego zarządzania logami lub analiza z wykorzystaniem rozwiązań SIEM.
- **Analiza pamięci** – analiza pamięci RAM przechwyconej z urządzenia.

IstroSec

Arkusz danych

Dlaczego my?

Doświadczenie i wiedza

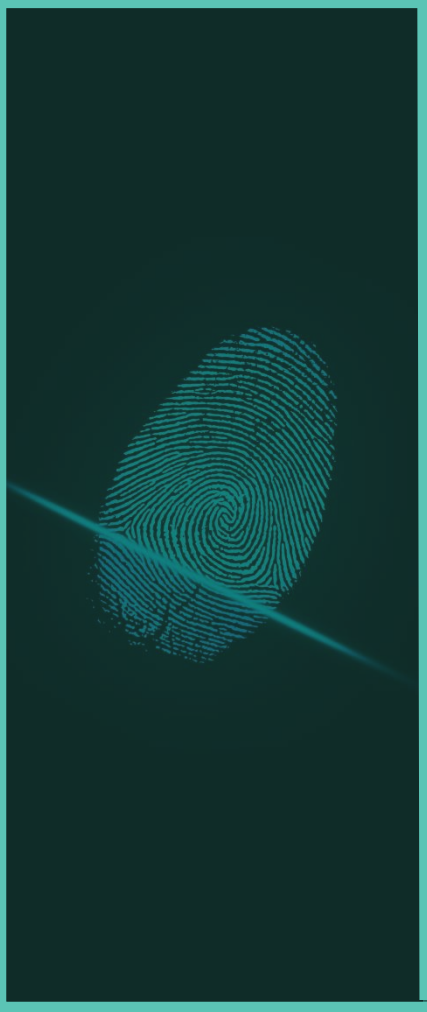
Specjaliści IstroSec mają doświadczenie w cyfrowej analizie kryminalistycznej, zgodnie z przyjętymi międzynarodowymi ramami. Znają taktykę, techniki i procedury atakujących oraz mają wiedzę niezbędną do podejmowania decyzji podczas reakcji na incydent w oparciu o analizę działań napastników podczas ataku.

Specjalistyczna wiedza DFIR

Specjalistyczna wiedza w zakresie kryminalistyki cyfrowej i reagowania na incydenty (DFIR) oraz wielu innych obszarach bezpieczeństwa informacji, takich jak zarządzanie bezpieczeństwem informacji, audyt czy światowej klasy analiza złośliwego oprogramowania, którą wielokrotnie wykazali się podczas radzenia sobie z cyberatakami wspieranymi przez państwo, atakami na organizacje z listy Fortune 500, a także udział czterech ekspertów IstroSec w zwycięskim zespole ćwiczenia Locked Shields 2016.

Certyfikowani profesjonaliści

Eksperci IstroSec są również posiadaczami uznanych na całym świecie certyfikatów w tych 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.



Studium przypadku 3

Rodzaj firmy: Prywatny dostawca usług opieki zdrowotnej

Świadczone usługi: Kryminalistyka cyfrowa

Rozwiązanie: Specjalna kryminalistyka cyfrowa

Zajmiemy się opisanym powyżej przypadkiem infekcji ransomware REvil.

Na podstawie wyników analizy kryminalistycznej zhakowanych urządzeń klient poprosił o wykonanie specjalnej analizy kryminalistycznej. Przeprowadzono pełną analizę eksfiltracji danych z urządzeń File01.organization.local i Database05.organization.local w celu zidentyfikowania dokumentów wyciekających z tych serwerów. W ramach analizy kryminalistycznej przeprowadzono analizę plików utworzonych, zmodyfikowanych lub skopiowanych przez atakującego. Jednocześnie stwierdzono, że atakujący uzyskał również dostęp do lokalnych baz danych za pośrednictwem zintegrowanego SQL Server Management Studio. Analiza zidentyfikowała dane w tej bazie danych, które zostały zmienione przez atakującego.

Z przeprowadzonego dochodzenia kryminalistyki cyfrowej sporządzono obszerny raport, który obejmował:

- Streszczenie
- Raport ze szczegółowymi wynikami analizy dla każdego dostarczonego dowodu cyfrowego (napęd, obraz kryminalistyczny, eksport rejestrów itp.)
- Lista najprawdopodobniej wykradzionych dokumentów z serwerów