CASE STUDY

O Kliencie

Podczas rosyjskiej inwazji na pełną skalę, klient, jeden z ukraińskich organów ścigania, stanął przed bezprecedensowymi wyzwaniami w zakresie cyberbezpieczeństwa. Wraz ze wzrostem napięcia i zwiększonym prawdopodobieństwem cyberataków, infrastruktura klienta była narażona na najwyższe ryzyko bycia celem wyrafinowanych prób ataków hakerskich, mających na celu zakłócenie jego działalności, kradzież poufnych informacji oraz rozpowszechnianie dezinformacji. Zapewnienie bezpieczeństwa infrastruktury cyfrowej stało się kwestią nadrzędną, wymagającą solidnych mechanizmów obronnych i stałej czujności w celu ochrony przed potencjalnymi naruszeniami i szpiegostwem w cyberprzestrzeni, organizowanym przez przeciwników.

Infrastruktura klienta:

- do 350 hostów LAN
- do 10 podsieci VLAN

Wyzwanie

Infrastruktura klienta zawierała wiele danych związanych z informacjami o wysoce ograniczonym dostępie. Konieczne było wzmocnienie następujących obszarów infrastruktury IS: wykrywanie potencjalnie niepożądanej aktywności w sieci LAN, próby nieautoryzowanego dostępu do systemów wewnętrznych oraz wykrywanie i kontrola ruchu bocznego w łańcuchu ataku sieciowego.

Realizacja

W ciągu jednego dnia wdrożono konsolę Labyrinth AdminVM i jeden węzeł WorkerVM, który obsługiwał wszystkie niezbędne segemty sieci VLAN poprzez połączenie TRUNK. Przynęty plikowe zostały umieszczone tylko na serwerach w infrastrukturze klienta.

Rozwiązanie

W pierwszym etapie wdrożono typy wabików, które maksymalnie "pasowały" do istniejącego zestawu systemów/usług sieciowych i były najbardziej podobne do istniejących konfiguracji w sieci klienta. Następnie przeprowadzono szereg różnych ataków testowych, zebrano dane dotyczące wykrywania oraz alertów utworzonych przez Labyrinth, a do ogólnego planu reagowania na incydenty w infrastrukturze dodano dodatkowe informacje związane z wykorzystaniem istniejącego systemu decepcji.

W drugiej fazie znacznie zwiększono liczbę typów wabików, skonfigurowano wiele niestandardowych typów wabików oraz, w oparciu o metodologię Moving Target Defense, okresowo regenerowano zestaw wabików sieciowych. Dało to dodatkową dynamikę infrastrukturze i zwiększyło złożoność jej eksploracji przez atakującego.

Rezultaty

Po objęciu ochroną znacznej części infrastruktury klienta i wykorzystaniu szerokiej gamy różnych typów wabików sieciowych, zidentyfikowano intruza wewnętrznej polityki bezpieczeństwa, który zaczął przeprowadzać rażące ataki na wabiki SCADA.

O firmie Labyrinth

Labyrinth to zespół doświadczonych inżynierów cyberbezpieczeństwa i testerów penetracyjnych, który specjalizuje się w opracowywaniu rozwiązań do wczesnego wykrywania cyberzagrożeń i zapobiegania im.

NASZĄ WIZJĄ jest przesunięcie układu sił na korzyść obrońców. NASZĄ MISJĄ jest dostarczenie wszelkiego rodzaju organizacjom prostego i wydajnego narzędzia do jak najwcześniejszego wykrywania napastników wewnątrz sieci korporacyjnej.

KLUCZOWE KORZYŚCI

- WCZESNE WYKRYWANIE ZAGROŻEŃ
- SPOWOLNIENIE CYBERATAKU
- ŁATWOŚĆ WDROŻENIA I UTRZYMANIA
- ELASTYCZNE OPCJE LICENCJONOWANIA

KLUCZOWE CECHY

- WDROŻENIE LOKALNE (ON-PREMISE)
- CENTRALNIE ZARZĄDZANE WABIKI IT/OT
- INTEGRACJE Z ROZWIĄZANIAMI FIRM TRZECICH
- OBSŁUGA WIELU PLATFORM
- MULTI-TENANCY DLA DUŻYCH LUB ROZPROSZONYCH ARCHITEKTUR

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

CISO CHOICE AWARD 2025
FINALIST