LABYRINTH

CASE STUDY

O Kliencie

Państwowa agencja Ukravtodor została utworzona jako korporacja państwowa w 1990 roku, zastępując Ministerstwo Dróg Ukrainy Radzieckiej jako państwowy organ zarządzający drogami samochodowymi we współczesnej Ukrainie. Jest ona uzupełniana przez instytut projektowy Ukrhiprodor, który projektuje obiekty zarządzania drogami.

Ukravtodor jest nadzorowany przez Ministerstwo Infrastruktury Ukrainy. W dniu 28 lutego 2002 roku, na mocy dekretu prezydenckiego, utworzono państwową otwartą spółkę akcyjną "Avtomobilni dorohy Ukrainy" (ADU).

Firma była bezpośrednio zaangażowana w budowę i utrzymanie dróg. W 2016 roku. ADU została połączona z Ukravtodorem, który obecnie posiada 100% jej udziałów.

Infrastruktura klienta:

- do 750 hostów LAN
- do 100 podsieci VLAN

Wyzwanie

Infrastruktura klienta składa się głównie z serwerów i różnych urządzeń sieciowych. Odsetek stacji roboczych jest nieznaczny. Główną cechą jest to, że krytyczne zestawy hostów są rozproszone geograficznie.

Głównym zadaniem wdrożenia systemu decepcji było zwiększenie widoczności działań atakujących w odniesieniu do wszelkiego rodzaju aplikacji / usług sieciowych, z których wiele znajduje się w infrastrukturze klienta.

Rozwiązania klasy NTA mogły być bardziej racjonalne w takiej architekturze sieci. Wolumen Web-UI był ogromny: na sprzęcie sieciowym i specjalistycznym oprogramowaniu stworzonym specjalnie dla tej firmy.

Realizacja

Maszyna wirtualna Labyrinth Admin i 4 maszyny wirtualne Worker zostały wdrożone na hiperwizorze VMware vSphere w segmencie zarządzania (LAN management) Przy użyciu systemu orkiestracji, obecnego w firmie, agenty osadzające (Seeder Agents) zostały rozesłane do większości serwerów.

Całkowita liczba przynęt plikowych wynosi ponad 4500. Utworzono ponad 55 sieci Honeynet do hostowania przynęt sieciowych Points, odpowiedzialnych za ochronę określonych podsieci VLAN.

W każdej z sieci VLAN około 15% przestrzeni adresowej zostało przydzielone dla przynęt sieciowych (Points).

Rozwiązanie

1. Wpierw zidentyfikowano najbardziej krytyczne usługi z interfejsami WebUI / REST API i najbardziej atrakcyjne cele dla potencjalnego atakującego.

2. Następnym krokiem było stworzenie wielu wabików usług sieciowych, które były dynamicznymi emulacjami istniejących interfejsów sieciowych w infrastrukturze firmy. Emulacje te zawierały wiele rodzajów luk w zabezpieczeniach sieci, zapewniając atakującemu więcej opcji rozwoju ataku, jednocześnie zwiększając szanse na wykrycie penetracji sieci i zebranie danych o metodach / narzędziach ze strony atakujących.

3. Na wszystkich serwerach plików uruchomiono agenty Seeder, za pośrednictwem których system platformy decepcji Labyrinth rozesłał przynęty plikowe na prawdziwe hosty, by te przekierowały atakujących na działające przynęty sieciowe (Points).

4. Szczególną uwagę zwrócono na propagację różnych wabików sieciowych w segmencie DMZ. Wabiki sieciowe w tej części sieci są najczęściej regenerowane, aby środowisko nie wyglądało statycznie. Regeneracja trwa do trzech minut.

Rezultaty

Wdrożenie systemu decepcji znacząco podniosło poziom wykrywalności zdarzeń intranetowych, co potwierdziły testy penetracyjne przeprowadzone po wdrożeniu systemu.

System wykazał wysoką skuteczność w trakcie testów penetracyjnych, zabierając atakującym dużo czasu i rozpraszając ich wieloma przynętami sieciowymi, rozsianymi po podsieciach klienta.

Efektem ubocznym z zatosowania systemu Labyrinth były wykrycia związane z zasobami shadow IT w postaci zapomnianych skanerów bezpieczeństwa i oprogramowania do zarządzania zasobami.

Wabiki sieciowe w segmencie DMZ umożliwiły zbieranie informacji, które pozwoliły poprawić ustawienia ochrony infrastruktury na brzegu sieci firmowej.

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