CASE STUDY

O Kliencie

Klient jest wiodącym dostawcą usług audytu frachtu i widoczności logistycznej, który świadczy usługi informacyjne jako pośrednik B2B w budowaniu łańcuchów dostaw. Ochrona danych jest kluczową kwestią dla tego typu działalności.

Infrastruktura klienta:

- do 500 hostów LAN
- 6 głównych usług sieciowych w DMZ na różnych serwerach

Wyzwanie

W krótkim okresie czasu (w kilka tygodni) paru konkurentów Klienta zostało jednocześnie zhakowanych, co doprowadziło do eksfiltracji danych wszystkich użytkowników i wystawienia ich na sprzedaż przez hakerów lub pośredników.

Oczekiwaniem Klienta było natychmiastowe zwiększenie widoczności infrastruktury firmy w zakresie bezpieczeństwa informacji, a także rozszerzenia możliwości wykrycia potencjalnie zaistniałego ataku, który mógł się przedrzeć przez zabezpieczenia brzegu sieci firmowej.

Realizacja

Maszyny wirtualne Labyrinth Admin i Worker zostały wdrożone w segmencie zarządzania LAN na hiperwizorze VMware vSphere.

Utworzono 3 podsieci Honeynet w celu uruchomienia wabików sieciowych (Points):

- w segmencie DMZ (12 IPs),
- w segmencie dev/test (30 IPs),
- w segmencie dir-hosts (58 IPs).

Dla stworzenia pułapek w segmencie DMZ użyto UniversalWebPoint, podczas gdy dla pozostałych dwóch segmentów wybrano wszystkie dostępne typy wabików.

Agenty Seeder zostały rozmieszczone na:

- fizycznych serwerach z uruchomionymi produkcyjnymi usługami internetowymi,
- wszystkich serwerach dev/test,
- laptopach i stacjach roboczych w segmencie dir-hosts.

Rozwiązanie

Wdrożenie systemu Labyrinth i pokrycie infrastruktury sieciowej Klienta odbywało się w dwóch kierunkach.

Po pierwsze - wdrożenie kilku pułapek typu UniversalWebPoint w strefie DMZ obok prawdziwych serwerów produkcyjnych i otwarcie dostępu do nich z poziomu sieci Internet.

Ten wektor ma na celu zebranie danych o atakującym i określenie najbardziej pożądanego zasobu lub zbioru danych, wykrywając najbardziej istotne dane dla atakującego z zakresu usług produkcyjnych.

Po drugie - integracja zestawu pułapek w segmentach sieci: serwery deweloperskie i testowe oraz VLANy używane przez komputery kadry zarządzającej i działu finansowego u Klienta.

Integracja ta miała na celu wykrycie atakującego, który już przeniknął do LAN poprzez kanały zdalnego dostępu, korporacyjną sieć VPN, w czasie gdy większość pracowników pracowała zdalnie.

Dla wszystkich usług internetowych utworzono imitacje na bazie UniversalWebPoint, z niewielkimi różnicami wizualnymi w stosunku do oryginalnych i emulowano podatności (DirTraversal, LFI, RCE). Wygenerowano subdomeny, do których dostęp można uzyskać przez Internet. Całe wdrożenie systemu decepcji w infrastrukturze Klienta zajęło mniej niż dwie godziny.

Rezultaty

Zespół oceniający próby ataków stwierdził, że wysiłki atakujących były skierowane na bazę danych niezakończonych transakcji, podczas gdy wcześniejsze założenie Klienta było takie, że głównym celem ataku będzie baza danych firm korzystających z jego usług.

Na podstawie otrzymanych informacji, dokonano natychmiastowego, dodatkowego przeglądu kodu pod kątem wszystkich punktów odbioru danych od użytkownika przez aplikację webową, związanych konkretnie z niezakończonymi transakcjami.

Dla drugiego wektora odkryto, że skanowanie sieci LAN odbywa się z domowej stacji roboczej jednego z twórców oprogramowania u klienta, łączącego się przez VPN w czasie wolnym od pracy i przeprowadzającego rozpoznanie hostów znajdujących się w segmencie dev/test. Ponadto wykryto ataki siłowe (bruteforce) i próby wykorzystania luk (exploity) na usługi sieciowe, z dalszym działaniem wskazującym na eskalację uprawnień. Stacja robocza tego pracownika została odizolowana i przekazana do analizy kryminalistycznej.

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