CASE STUDY

O Kliencie

Klientem jest instytucja finansowa, która pełni specjalne funkcje w zakresie gwarantowania depozytów osób fizycznych i usuwania niewypłacalnych banków z rynku. Status prawny: podmiot prawa publicznego.

Klient jest niezależną ekonomicznie instytucją, która nie dąży do osiągnięcia zysku. Głównym zadaniem instytucji jest zapewnienie funkcjonowania systemu gwarantowania depozytów, usuwanie niewypłacalnych banków z rynku i ich likwidacja.

Główne obszary działalności Klienta:

- prowadzi rejestr uczestników,
- gromadzi środki oraz monitoruje kompletność i terminowość przekazywania opłat przez każdego członka instytucji,
- podejmuje działania w celu zorganizowania wypłaty rekompensat depozytowych w przypadku decyzji o cofnięciu licencji bankowej i likwidacji banku,
- reguluje uczestnictwo banków w systemie gwarantowania depozytów,
- podejmuje działania mające na celu informowanie społeczeństwa o funkcjonowaniu systemu gwarantowania depozytów,

ochronę praw i prawnie chronionych interesów deponentów oraz podnoszenie poziomu wiedzy finansowej społeczeństwa.

Wyzwanie

Ponieważ Klient posiada duże ilości danych związanych z informacjami finansowymi wielu banków i podmiotów prawnych, jest kuszącym celem ataku.

Klient posiadał dużą liczbę serwerów z systemem MS Windows. Większość stacji roboczych również korzystała z systemu operacyjnego Windows w różnych wersjach.

Infrastruktura sieciowa Klienta wykorzystuje oprogramowanie opracowane specjalnie dla niego i współdzielone przez agencje rządowe. Jedno z rozwiązań jest kluczowym elementem infrastruktury do świadczenia usług elektronicznych dla obywateli i organizacji, zapewniając wygodny, ujednolicony dostęp do danych z rejestrów państwowych.

Oprogramowanie to posiada wiele interfejsów interakcji, w tym różne usługi sieciowe.

Kierownictwo firmy postawiło przed działem systemów informatycznych zadanie zmniejszenia ryzyka potencjalnych włamań i nieautoryzowanego dostępu do sieci LAN oraz poprawy zdolności wykrywania ataków w sieci; ochrona brzegu została zbudowana w oparciu o produkty firm Cisco i CloudFlare.

Realizacja

Wdrożono konsolę zarządzającą AdminVM i dwa węzły robocze WorkerVM, ponieważ prezentacja wszystkich podsieci VLAN na jednym łączu typu TRUNK była niemożliwa. W tym samym czasie maszyny WorkerVM były rozmieszczone na różnych klastrach serwerów wirtualizacji. Jedna maszyna WorkerVM obsługiwała segmenty sieci ze stacjami roboczymi, a druga została wdrożona w podsieciach serwerów.

Agenty Seeder zostały rozmieszczone na 25% stacji roboczych i na wszystkich dostępnych serwerach Windows. Umożliwiło to utworzenie ok. 10 000 wabików plikowych, które dynamicznie zmieniają się po wprowadzeniu zmian w wabikach sieciowych.

Rozwiązanie

Po pierwsze, stworzono dużą liczbę wabików sieciowych, które:

- imitowały hosty Windows,
- symulowały zachowania użytkowników: surfowanie po sieci, dostęp do udziałów SMB, zapytania DNS, itp.

Takie działania pozwoliły stworzyć środowisko, w którym Labyrinth mógł wykryć próby ataków MiTM (man-in-the-middle) i zapewnić atakującemu wiele fałszywych celów, które wyglądały całkowicie naturalnie wśród rzeczywistych systemów w sieci.

Po drugie, w segmencie serwerów wdrożono wabiki imitujące VMware ESXi i Ascod. Oprócz nich stworzono imitacje wszystkich usług sieciowych przy użyciu wabików UniversalWeb Point (w tym interfejsów webowych wszystkich urządzeń Cisco).

Rezultaty

Wdrożenie systemu pozwoliło poprawić wykrywanie prób ataków typu MiTM i wykorzystania danych uzyskanych z ruchu do przeprowadzenia dalszych ruchów bocznych. Jednocześnie wykrywanie to było znacznie łatwiejsze niż korzystanie z systemu SIEM z wieloma regułami korelacji dla podobnych zadań.

Po wdrożeniu wabików sieciowych, które emulowały wszystkie istniejące usługi sieciowe, zadanie atakującego, polegające na niezauważonym poruszaniu się po infrastrukturze, stało się niemożliwe do realizacji.