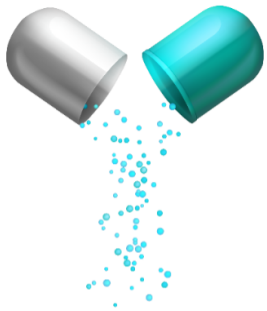
LABYRINTH

CASE STUDY

O Kliencie

Klientem jest duża firma farmaceutyczna, działająca na rynku od ponad dekady. Jako lider branży oferuje portfolio produktów, które obejmuje zarówno leki generyczne, jak i oryginalne produkty lecznicze w 11 z 14 grup farmakoterapeutycznych.



Infrastruktura klienta:

- do 900 hostów LAN
- do 80 podsieci VLAN

Wyzwanie

Każdego dnia pracownicy firmy obsługują wiele wiadomości poczty elektronicznej.

U Klienta system antyspamowy przetwarza wiadomości przychodzące w oparciu o system analizy sygnatur i konieczne było dodanie kolejnej warstwy ochrony, która byłaby odpowiedzialna za wykrywanie udanych ataków phishing'owych i nie opierałaby się na sygnaturach.

Realizacja

Maszyna wirtualna Labyrinth Admin i kilka maszyn wirtualnych Worker zostały wdrożone na hiperwizorze VMware vSphere w segmencie zarządzania (LAN management) Przy użyciu systemu orkiestracji, obecnego w firmie, agenty osadzające (Seeder Agents) zostały dystrybuowane na hostach.

Utworzono ponad 15 sieci Honeynet do hostowania przynęt sieciowych Points, odpowiedzialnych za ochronę określonych podsieci VLAN.

W każdej z sieci VLAN około 20% przestrzeni adresowej zostało przydzielone dla przynęt sieciowych (Points).

Rozwiązanie

Specjaliści Labyrinth przydzielili agentów Seeder do wszystkich stacji roboczych w sieci Klienta.

Za ich pomocą platforma decepcji Labyrinth rozesłała przynęty plikowe na prawdziwe hosty, by te przekierowały atakujących na działające przynęty sieciowe.

Dla każdej stacji roboczej wygenerowano co najmniej 20 wabików plikowych, z których każdy wskazywał jeden lub więcej wabików sieciowych.

Zmaksymalizowano wykorzystanie wabików sieciowych dla segmentów sieci zawierających krytyczne zasoby IT. Były to pułapki imitujące DBMS i aplikacje webowe.

System Labyrinth automatycznie weryfikuje i utrzymuje adekwatność przynęt plikowych, tak aby w pełni uwzględniały zmiany, gdy zmieniają się wabiki sieciowe.

Dodatkowo zintegrowano platformę decepcji z systemem SIEM w celu wzbogacenia kontekstu wykrywanych zdarzeń oraz dwukierunkowej wymiany informacji.

Rezultaty

Po wdrożeniu systemu w sieci Klienta wykryto kilka przypadków, w których strona atakująca ominęła system analizy sygnatur wiadomości pocztowych i uzyskała dostęp do stacji roboczych.

W drugim etapie ataku udało zebrać się istotne informacje na stacjach roboczych, które pomogłyby w zdobyciu przyczółka i rozwinięciu ataku w głąb sieci firmowej.

Intruzi zostali ujawnieni przy użyciu informacji z przynęt plikowych znalezionych przez nich na hostach, które wskazywały na imitacje baz danych.

Oprócz wykrycia faktu penetracji sieci, system Labyrinth wygrywał więcej czasu dla zespołu SOC na reakcję i podjęcie decyzji co do dalszych kroków w odpowiedzi na incydent.

Pomimo tego zaawansowanego wykrywania naruszeń, złożoność ataku i późniejsze naruszenie danych uwypukliły potrzebę zastosowania u Klienta zintegrowanego, wielowarstwowego podejścia do bezpieczeństwa cyfrowego.

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.