CASE STUDY

O Kliencie

Klientem jest firma poligraficzna, która ma pozycję lidera w produkcji dokumentów identyfikacyjnych, formularzy papierów wartościowych, bezpiecznych produktów poligraficznych, itp.

Infrastruktura klienta:

- do 1000 hostów LAN,
- 3 usługi internetowe w strefie DMZ,
- do 9 usług innych niż internetowe w DMZ na różnych serwerach.

Wyzwanie

Kluczowymi zadaniami dla zespołu IT było uzyskanie maksymalnej widoczności zdarzeń w sieci firmowej i wykrywanie anomalii w działaniach pracowników, zwłaszcza łączących się z siecią firmową przez tunele VPN w czasie pandemii.

Niezbędne było również zebranie większej ilości danych o segmencie DMZ i hostach wchodzących w interakcję z nim.

Istotne było również zabezpieczenie dostępu do systemu elektronicznego zarządzania dokumentami w obrębie sieci Klienta.

Realizacja

Wdrożono maszynę wirtualną Labyrinth Admin i kilka maszyn wirtualnych Labyrinth Worker na hiperwizorze VMware vSphere w segmentach LAN i DMZ.

Utworzono 5 sieci Honeynet:

- dla wabików w strefie DMZ (25 IPs),
- dla wabików w segmencie testowym (dla 45 Punktów (Points)),
- dla wabików w segmencie urządzeń bezpieczeństwa fizycznego (30 IPs),
- dla wabików sieciowych w segmencie zarządzania (120 IPs),
- dla wabików sieciowych w segmencie produkcji (64 IPs);

Wabik typu UniversalWebPoint był używany w większości przypadków we wszystkich segmentach. W segmencie zarządzania dodatkowo wykorzystywany był wabik imitujący system elektronicznego zarządzania dokumentami (EZD).

Agenty imitacji Seeder agents zostały rozmieszczone na:

- serwerach produkcyjnych z usługami internetowymi,
- serwerach testowych,
- na laptopach i stacjach roboczych w segmencie zarządzania,
- laptopach domowych, które były używane do połączeń VPN z firmą.

Rozwiązanie

Wdrożenie systemu Labyrinth i pokrycie infrastruktury Klienta odbyło się w kilku kierunkach:

- wdrożono szereg pułapek typu UniversalWebPoint w strefie DMZ, imitujących prawdziwe usługi w tym segmencie sieci oraz pułapek imitujących usługi zdalnego dostępu: ssh, rdp, rest-api -api.
- w ramach segmentu zarządzania firmą zastosowano dwa rodzaje pułapek: jeden dla systemu EZD, a drugi dla symulacji stacji roboczych z użyciem usług rdp, wmi, ssh, netbios, itp.
- segment IT został wypełniony szeroką gamą wabików sieciowych IT dla zapewnienia atakującym maksymalnej liczby różnych wektorów dalszych "ataków".
- Sieć LAN została wypełniona wabikami imitującymi różne magazyny plików: ftp, sftp, samba, nfs, webdav. Powstały też imitacje różnych baz danych.
- na krytycznych hostach ulokowano wiele przynęt (breadcrumbs) aby odwrócić uwagę atakującego od symulowanych usług / hostów.

Rezultaty

Przed wdrożeniem platformy Labyrinth w obrębie sieci Klienta, nie używano żadnego narzędzia zwiększającego widoczność działań użytkowników i oprogramowania sieciowego.

Po wdrożeniu systemu Labyrinth można było wykryć anomalne zachowanie oprogramowania w segmencie DMZ, co było wynikiem błędnej konfiguracji.

Przypadki nieautoryzowanego użycia zasobów sieci LAN przez użytkowników, którzy łączyli się z siecią firmową poprzez VPN z powodu kwarantanny, zostały zidentyfikowane i zbadane.

Na jednej ze stacji roboczych zostały zidentyfikowane podejrzane skrypty, które skanowały sieć i przeprowadzały ataki typu bruteforce na usługach ssh i rdp.

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