Autor – Rafał Bogacz

Scenariusz: Detekcja podejrzanego e-maila phishingowego przez system SIEM

Otrzymujesz alert o prawdopodobnie phishingowym emailu z systemu SIEM

Analize rozpoczynam od sprawdzenia informacji o nadawcy

Najpierw sprawdzam „Nagłówek" a tam pierwszą uwagę zwracam na adress email czy jest poprawny czy nie zawiera błędów albo nie pochodzi z złośliwych domen (złośliwą domene identyfikuje sprawdzając kiedy została założona,kto jest właścicielem i co zostaje z niej rozsyłane, do sprawdzenia używam narzędzia IP VOID), porównuje go z listą zaufanych dostawców (Do listy zaufanych dostawców należa stali klienci, pracownicy, vendorzy, emaile sądowe), jeśli to mi nie wystarczy mogę sprawdzić serwery SMTP używane do wysłania emaila(sprawdzam je wyszukując: Wpis „**Received**" pokazuje on przez jakie serwery przeszła wiadomość. Analizuje je od dołu do góry, zaczynając od pierwszego serwera, który odebrał wiadomość. Sprawdzam czy serwery są wiarygodne, a adresy IP są zgodne z domenami nadawcy.), następnie sprawdzam SPF, DMARC, DKIM,

Czym jest SPF,DMARC,DKIM i po co nam to?

SPF, DMARC i DKIM sprawdza się w e-mailach, aby zapobiegać phishingowi i spoofingowi, zapewniając, że wiadomości pochodzą z autoryzowanych źródeł i nie zostały zmodyfikowane.

SPF (Sender Policy Framework): Sprawdza, czy e-mail pochodzi z serwera autoryzowanego do wysyłania wiadomości w imieniu danej domeny, co pomaga zapobiegać podszywaniu się pod nadawcę.

DKIM (DomainKeys Identified Mail): Weryfikuje, czy e-mail nie został zmodyfikowany po wysłaniu, dzięki cyfrowemu podpisowi przypisanemu do domeny nadawcy.

DMARC (Domain-based Message Authentication, Reporting & Conformance): Określa, co zrobić z e-mailami, które nie przeszły weryfikacji SPF lub DKIM, oraz zapewnia raportowanie o próbach fałszowania wiadomości.

Jak to sprawdzam? W SPF sprawdzam czy email został wysłany z autoryzowanego serwera sprawdzam to po prostu sprawdzając nagłówek **Received SPF**: mamy pass oznacza to że wiadomość przeszłą weryfikacje pomyślnie jeśli fail oznacza to że serwer nie jest autoryzowany

Następnie w DKIM sprawdzam czy wiadomość nie została zmodyfikowana i czy jest podpisana cyfrowo przez nadawcę sprawdzam to w nagłówku **Authentication-Results**: dkim= pass oznacza ze wiadmość jest poprawna i podpisana i pochodzi z podanej domeny w przypadku phishingu będziemy mieli zamiast pass to fail, następnie sprawdzamy DMARCa który łączy wczesniej dwa opisane mechanizmy i dodatkowo mówi nam jak postąpić sprawdzamy go pod nagłówkiem **Authentication-Results** dmarc=pass który informuje nas ze wiadomość przeszła pomyślnie wszystkie procesy weryfikacji w przypadu dmarc=fail mamy dodatkowo informacje p=reject która informuje nas ze mamy do czynienia z phishingiem.

Następnie skupiam się na analizie treści emaila w poszukiwaniu znamion złośliwości, sprawdzam poprawność składni czyli błedy gramatyczne i stylistyczne sugerujące że może to być phishing, anlizując tekst sprawdzam czy są elementy socjologii czyli zdania sugerujące że muszę zrobić coś natychmiast, sprawdzam linki czy nie prowadzą do podejrzanych, złośliwych lub nieznanych adresów URL,

Autor – Rafał Bogacz

Jak to sprawdzam? Używam virus total/sandbox/ip.void/ url scanio/anyrun. w IP Voidzie sprawdzamy przekierowania i do kogo należy domena. sprawdzam czy wiadomość zawiera załączniki jeśli tak to przesyłam go do piaskownicy w celu dynamicznej analizy, ustalam czy to złośliwe oprogramowanie ukryte w pliku np. exe lub makrze pliku xls

Jak działa sandbox? Pokazuje ci dokladna analize pliku, wszystkie akcje i procesy które zostana uruchomione przez plik.

Następnie przechodze do klasyfikacji incydentu

Jeśli email nie wykazywał znamion złośliwości to klasyfikuje go jako false positive i zamykam incydent.

Jeśli email wykazał oznaki zagrożenia no to klasyfikuje go jako true positive i przechodzę do dalszych działań.

Blokuje adres email lub domene jeśli mam pewność ze to domena phishingowa np. **hilkodrq.shop** poprzez wprowadzenie reguł blokady w firewallu oraz bramie pocztowej i sprawdzam czy emaile z tego adresu bądź domeny były już wysyłane do kogoś z naszej organizacji. (sprawdzam w całej organizacji czy ktoś pobrał załącznik lub wszedł w ULRa), Jeśli tak to sprawdzam czy dana osoba uruchomiła załącznik lub podała wrażliwe dane np. login i hasło do konta pracownika(mogę to sprawdzic poprzez kontakt chociażby z użytkownikiem), jeśli podała to mamy tutaj w zależności od stanowiska pracownika incydent w skali severity oceniany na 2 lub 3. W tym przypadku dokonujemy tymczasowej izolacji systemu/konta od sieci aby zminimalizować rozprzestrzenienie się zagrożenia, przeprowadzamy analize techniczną skanując system pod kątem wskaźników kompromitacji czyli zmian w systemie czy w poszukiwaniu złośliwego oprogramowania oraz wymuszamy zmiane hasła na wszystkich kontach użytkownika.

Następnie aktualizujemy dokumentacje incydentu, opisując wszystkie podjęte kroki oraz wyniki analizy.

Autor – Rafał Bogacz

Scenariusz: Nietypowa aktywność logowania z wielu lokalizacji

Otrzymujesz alert o nietypowej aktywności logowania

Sprawdzam czy logowania pochodzą z różnych geolokalizacji w krótkim czasie np. Polska – Rosja albo Polska – Chiny czy w dłuższym ponieważ w przypadku krótkiego jest większe prawdopodobieństwo nieautoryzowanego logowania, czy pochodzą z różnych przeglądarek. Następnie weryfikujemy czy użytkownik jest znany i powinien mieć dostęp z tych lokalizacji, sprawdzam czy użyto wieloskładnikowego uwierzytelniania i przede wszystkim kontaktuje się z użytkownikiem i zgłaszam sprawę menadżerowi wcześniej sprawdzając czy w systemie ticketowym np. ServiceNow nie ma inforacji o delegacji użytkownika.

Następnie przechodzimy do klasyfikacji incydentu.

Jeśli okazało się że użytkownik jest na delegacji albo logowanie było autoryzowane przez VPN zamykamy incydent i oznaczamy jako false positive

Jeśli użytkownik lub manager potwierdzi że nie powinno być logowania z tych lokalizacji to tworzymy raport oznaczamy go jako true positive, prydzielamy skale severity 2/3 , tymczasowo blokujemy konto i wymuszamy zmiane hasła a następnie analizujemy w jaki sposób doszło do nieatoryzowanego logowania np. przeprowadzamy analizę logów w poszukiwaniu wskaźników kompromitacji na komputerze użytkownika. Jeśli znajdę wskaźnik kompromitacji to przywracam system z „recovery”(chodzi o Backup)

Następnie aktualizujemy dokumentacje incydentu, opisując wszystkie podjęte kroki oraz wyniki analizy.

Scenariusz: Użycie narzędzi typu brute force na kontach użytkowników
Otrzymujesz alert o próbach logowania wskazujących na atak brute force na konta użytkowników.
Najpierw sprawdzam, ile razy próbowano zalogować się na dane konto, identyfikuję adresy IP, z których pochodziły próby logowania, i badam, czy były krótkie, czy trwały przez dłuższy czas oraz czy były to wewnętrzne, czy zewnętrzne adresy IP. Opcjonalnie kontaktuję się z użytkownikiem, czy próbował się zalogować w tym czasie na dane konto. Sprawdzam również, czy błędne logowania nie wynikają ze zautomatyzowanego procesu logowania na stare hasło.

Klasyfikacja incydentu
Jeśli logowania były błędnymi próbami użytkownika, zamykamy incydent jako false positive.
Jeśli faktycznie doszło do ataku brute force, to wymuszam zmianę hasła, blokuję adresy IP, z których pochodzą próby brute force, opcjonalnie tymczasowo blokuję konto użytkownika, aby upewnić się, że nie doszło do nieautoryzowanego logowania, a jeśli atak pochodził z wewnętrznego adresu IP, identyfikuję stację roboczą i zlecam jej przeskanowanie pod kątem kompromitacji.

Autor – Rafał Bogacz

Scenariusz: Wykrycie malware lub ransomware na urządzeniach końcowych

Identyfikuję źródło, czyli do kogo należy komputer, oraz sprawdzam, czy są wykonywane nietypowe operacje, takie jak szyfrowanie danych, zmiana nazw plików oraz komunikacja z zewnętrznymi adresami, albo po prostu jeśli EDR wskaże mi, że kilka plików na dysku lokalnym zostało zaszyfrowanych albo ich rozszerzenia uległy zmianie, to natychmiast dokonuję izolacji urządzenia od sieci, aby zapobiec dalszemu rozprzestrzenianiu się ransomware oraz tworzę incydent i oznaczam go wysoką skalą w zależności od możliwości rozpowszechnienia (0-1). Używam narzędzia EDR, aby odciąć urządzenie od wszystkich połączeń sieciowych, poza połączeniem z systemem zarządzania EDR. Identyfikuję złośliwy plik, poddaję go analizie z bazą danych, a następnie usuwam zagrożenie. Jeśli nie ma możliwości usunięcia zagrożenia, to zlecam przywrócenie urządzenia z kopii zapasowej wykonanej przed incydentem, jeśli jest to możliwe, bo ransomware nie usunął kopii zapasowej.

Komenda vssadmin delete shadows /for=<ForVolumeSpec> [/oldest | /all | /shadow=<ShadowID>] [/quiet] używana do usunięcia kopii zapasowej. Usuwa kopię zapasową bez poinformowania użytkownika.

- /quiet Specifies that the command won't display messages while running.
- /oldest Deletes only the oldest shadow copy.
- /all Deletes all of the specified volume's shadow copies.

(Zapamiętaj przypadek, w którym usuwanie kopii zapasowej może okazać się false positive – np. aktualizacja oprogramowania, wtedy stara kopia jest zastąpiona nową, jednak nie tyczy się to systemów Windows).
Następnie tworzę szczegółowy raport z incydentu, obejmujący wszystkie zebrane dane, przeprowadzone analizy, podjęte kroki i wnioski oraz monitoruję środowisko przez kolejne dni, aby upewnić się, że nie pojawią się nowe wskaźniki zagrożeń.

Autor – Rafał Bogacz

Scenariusz: Wykrycie podejrzanego ruchu sieciowego (np. do złośliwych IP)

Najpierw identyfikuję stację roboczą, z której wychodzą złośliwe adresy IP. Następnie: Sprawdzam dzienniki proxy i firewall, aby zidentyfikować, z jakiego oprogramowania lub procesu pochodzi ruch na złośliwe adresy IP. Następnie weryfikuję reputację docelowych adresów IP w bazach Threat Intelligence, czy te adresy nie są powiązane np. ze znanymi botnetami albo znanymi serwerami do dystrybucji malware. Sprawdzam, czy mamy do czynienia ze skanerem portów albo z beaconingiem. Jeśli adresy okazują się złośliwe, to je blokuję i dodaję nowe reguły do firewalla oraz sprawdzam, czy inne urządzenia w sieci nie komunikowały się z tymi adresami IP, aby upewnić się, że infekcja nie rozprzestrzeniła się na następne komputery. Aktualizuję zgłoszenie, przypisując skalę severity 2. Następnie analizuję, czy ruch pochodził z jednego procesu, czy wielu, i zlecam skanowanie systemu za pomocą EDR oraz odłączam go od sieci, zostawiając tylko połączenie z EDR. Następnie korzystam z narzędzi EDR, aby prześledzić wszystkie procesy uruchomione na urządzeniu, zidentyfikować nieznane lub podejrzane oprogramowanie oraz potencjalne punkty wejścia i je usunąć. A po wszystkim sporządzam szczegółowy raport incydentu, zawierający zebrane dowody, przeprowadzone analizy, podjęte działania oraz wnioski.

Co to Threat Intelligence
Nie jest jedynie bazą danych; to bardziej zestaw procesów i narzędzi, które pomagają gromadzić i analizować informacje o zagrożeniach. Źródła danych mogą obejmować logi systemowe, raporty o incydentach, informacje od dostawców zabezpieczeń, źródła open-source, a także dane z Dark Webu i innych platform. Analiza tych danych pozwala na wykrywanie wzorców i przewidywanie potencjalnych ataków.

Beaconing
W cyberbezpieczeństwie to technika, w której złośliwe oprogramowanie (np. trojany, botnety) regularnie komunikuje się z serwerami C&C (Command and Control). Wysyła małe sygnały ("beacony") w celu pobierania nowych poleceń lub przekazywania danych. Ze względu na minimalną i losową ilość przesyłanych danych, beaconing jest trudny do wykrycia w ruchu sieciowym.

Scenariusz: Próby nieautoryzowanego dostępu do zasobów wewnętrznych
Analizę rozpoczynam od ustalenia źródłowego adresu IP i czy należy do jednego z pracowników. Następnie sprawdzam historię logowań z tego adresu IP oraz innych urządzeń użytkownika, aby zidentyfikować, czy te próby były częścią regularnej pracy, czy stanowią anomalię. Zwracam uwagę na czas prób logowania, czy miały miejsce poza normalnymi godzinami pracy użytkownika.

Jeśli widzę, że w ciągu 30 minut z adresu IP 192.168.50.23 nastąpiło ponad 50 nieudanych prób logowania do konta administracyjnego na serwerze, to blokuję adres IP atakującego oraz wymuszam zmianę hasła do konta administracyjnego. W przypadku udanych prób logowania, sprawdzam, do jakich plików użytkownik miał dostęp i natychmiast blokuję konto oraz IP. Aktualizuję incydent do True Positive, przypisując skalę 2 Następnie monitoruję, czy następują kolejne próby ataku oraz sporządzam raport z podjętych działań.

Autor – Rafał Bogacz

Scenariusz: Anomalie w przesyłaniu dużych ilości danych poza firmę

W pierwszej kolejności identyfikuję urządzenie o podanym adresie i sprawdzam, do którego pracownika należy. Następnie weryfikuję, do jakiego serwera zewnętrznego są wysyłane dane, np. serwer, Dropbox. Jeśli źródło nie jest w naszej bazie danych, uznaje się je za podejrzane. W przypadku serwisów ogólnych, takich jak Dropbox, dane tam zostaną i nie będzie możliwości ich usunięcia. Jeżeli nie znam źródła, do którego konto wysyła dane, natychmiast blokuję konto.

Sprawdzam, czy serwer zewnętrzny jest oznaczony w bazie danych jako potencjalne źródło niebezpieczeństwa. Analizuję logi logowania oraz aktywność zidentyfikowanego użytkownika w celu wykrycia nietypowych logowań z innych adresów IP lub nietypowych zachowań, które mogą świadczyć o kompromitacji systemu lub przejęciu konta. Jeśli po przeprowadzeniu analizy nadal nie jestem pewny, czy konto mogło zostać skompromitowane, kontaktuję się z menadżerem.

W przypadku 100% pewności, że mamy do czynienia z inside malicious lub skompromitowanym kontem, blokuję tymczasowo użytkownika, kontaktuję się z menadżerem, aktualizuję incydent do True Positive i przypisuję mu skalę severity 2.

Wykrycie podejrzanych skryptów lub plików wykonywalnych na serwerach

Identyfikuję potencjalnie złośliwy proces i sprawdzam, jak został uruchomiony i przez kogo oraz jakie zadanie wykonał. W tym celu skanuję go EDR w poszukiwaniu nietypowych operacji, takich jak komunikacja z zewnętrznymi podejrzanymi adresami IP, sprawdzenie kopii zapasowych (bo po co proces niezwiązany z Dell'em ma patrzeć w backup Della), nadmierna modyfikacja rejestrów ogólnych, np. związanych z logowaniem. Jeśli udaje mi się ustalić, że plik lub skrypt jest złośliwy, to tymczasowo izoluję serwer i uruchamiam backup serwera. Sprawdzam, do czego jest serwer, kontaktuję się z administratorami serwera, aby dowiedzieć się, do czego jest on przeznaczony, bo np. serwer od logowania musi działać cały czas. Staram się wyodrębnić sygnaturę i porównać z bazami danych, aby potwierdzić zidentyfikowane zagrożenie. Aktualizuję incydent jako True Positive i przypisuję skalę severity 1 w przypadku serwera głównego oraz 2 w przypadku serwera, który nie ma dużego business impactu. Następnie czyszczę system, a jeśli to nie jest możliwe, przywracam z kopii zapasowej.

Analiza Szczegółowa Potencjalnego Ataku XSS (Cross-Site Scripting)

Sprawdzam URL, który wykazuje potencjalne zagrożenie XSS, w szczególności analizuję parametr query, który może zawierać złośliwy kod JavaScript. Przechodzę do kodu źródłowego strony, aby sprawdzić, czy parametry zapytania są odpowiednio filtrowane i kodowane przed wyświetleniem na stronie. Skupiam się na funkcjonalności wyszukiwania, aby ocenić, czy istnieje podatność na XSS, opcjonalnie używam BurpSuite do przetestowania strony. Sprawdzam logi serwera, aby zobaczyć, czy są tam wpisy dotyczące podejrzanych zapytań lub ataków, które mogą potwierdzać próbę wstrzyknięcia kodu. Sprawdzam, czy w pamięci podręcznej aplikacji nie zostały zapisane złośliwe dane, które mogą być dostępne dla użytkowników. Jeśli moja analiza wykazuje możliwość wykorzystania podatności XSS, to aktualizuję incydent jako True Positive, przypisuję mu skalę severity 2 i tymczasowo wyłączam stronę do momentu usunięcia podatności.

Notatka: Przeglądarki mają narzędzia deweloperskie, mogę na maszynach wirtualnych sprawdzić połączenie sieciowe, sprawdzam ruch sieciowy, który łączy się z serwerem podejrzanym i przesyła dane.