# OS Hardening techniques

Jesteś analitykiem ds. cyberbezpieczeństwa w witrynie yummyrecipesforme.com, która sprzedaje przepisy i książki kucharskie. Niezadowolony piekarz postanowił opublikować na stronie internetowej najlepiej sprzedające się przepisy, aby opinia publiczna miała do nich bezpłatny dostęp.

Piekarz przeprowadził atak siłowy, aby uzyskać dostęp do hosta internetowego. Wielokrotnie wprowadzali kilka znanych domyślnych haseł do konta administracyjnego, aż poprawnie odgadł właściwe. Po uzyskaniu danych logowania mogł uzyskać dostęp do panelu administracyjnego i zmienić kod źródłowy witryny. W kodzie źródłowym osadził funkcję javascript, która zachęcała odwiedzających do pobrania i uruchomienia pliku po odwiedzeniu strony internetowej. Po uruchomieniu pobranego pliku klienci są przekierowywani na fałszywą wersję strony, na której dostępne są za darmo przepisy sprzedawcy.

Kilka godzin po ataku wielu klientów wysłało e-maile do działu pomocy yummyrecipesforme. Skarżyli się, że strona internetowa firmy skłoniła ich do pobrania pliku aktualizującego ich przeglądarki. Klienci twierdzili, że po uruchomieniu pliku zmienił się adres strony internetowej, a ich komputery osobiste zaczęły działać wolniej.

W odpowiedzi na ten incydent właściciel witryny próbuje zalogować się do panelu administracyjnego, ale nie może, dlatego kontaktuje się z dostawcą usług hostingowych. Ty i inni analitycy ds. bezpieczeństwa cybernetycznego macie za zadanie zbadanie tego zdarzenia związanego z bezpieczeństwem.

Aby zareagować na incydent, tworzysz środowisko piaskownicy, aby obserwować podejrzane zachowanie witryny. Uruchom analizator protokołów sieciowych tcpdump, a następnie wpisz adres URL strony internetowej yummyrecipesforme.com. Gdy tylko witryna się załaduje, zostaniesz poproszony o pobranie pliku wykonywalnego w celu zaktualizowania przeglądarki. Akceptujesz pobieranie i zezwalasz na uruchomienie pliku. Następnie zauważasz, że Twoja przeglądarka przekierowuje Cię do innego adresu URL, greatrecipesforme.com, który ma wyglądać jak oryginalna strona. Jednak przepisy, które sprzedaje Twoja firma, są teraz bezpłatnie publikowane na nowej stronie internetowej.

Dzienniki przedstawiają następujący proces:

1. Przeglądarka żąda rozwiązania DNS adresu URL yummyrecipesforme.com.
2. DNS odpowiada poprawnym adresem IP.
3. Przeglądarka inicjuje żądanie HTTP dla strony internetowej.
4. Przeglądarka inicjuje pobieranie złośliwego oprogramowania.
5. Przeglądarka żąda innej rozdzielczości DNS dla witryny greatrecipesforme.com.
6. Serwer DNS odpowiada nowym adresem IP.
7. Przeglądarka inicjuje żądanie HTTP na nowy adres IP.

Twoim zadaniem jest szczegółowe udokumentowanie incydentu, w tym identyfikacja protokołów sieciowych używanych do nawiązania połączenia między użytkownikiem a witryną. Powinieneś również zalecić działanie bezpieczeństwa, które należy podjąć, aby zapobiec atakom siłowym w przyszłości.

**Materiały pomocnicze znajdziemy w folderze scenariusza**

# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| Protokołami zaangażowanymi w incydencie są protokoły DNS, TCP oraz HTTP.  Nośnikiem szkodliwego oprogramowania jest protokół HTTP za pomocą którego strona pobierała szkodliwe oprogramowanie. Proces zachodził w warstwie aplikacji modelu TCP/IP |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Incydent został zauważony przez klientów którzy zauważyli pobieranie podejrzanych plików oraz spadek wydajności komputera podczas korzystania z witryny yummyrecipesforme.com. W odpowiedzi na incydent administrator strony próbował zalogować się do panelu administracyjnego do którego utracił dostęp. Sugeruje to że konto administracyjne zostało przejęte przez złośliwego aktora.  Podczas analizy TCPdump zauważono szczegóły działania incydentu:  Urządzenie przesyła żądanie do serwera DNS w celu rozwiązania nazwy domeny yummyrecipesforme.com do adresu IP. W odpowiedzi otrzymuje prawidłowy adres IP.  Po zdobyciu prawidłowego adresu IP, przeglądarka wysyła żądanie HTTP do serwera webowego w celu otrzymania strony internetowej. W tym procesie pobierane jest złośliwe oprogramowanie które przekierowuje użytkownika do sfałszowanej strony greatrecipesforme.com powtarzając proces żądania do serwera DNS i rozwiązywania adresów IP. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| W ramach przeciwdziałania powtórzenia się incydentu wstępnie sugerujemy implementacje polityki silnych haseł. Wiemy że organizacja korzystała z domyślnych haseł których złamanie było trywialne. Implementacja skomplikowanych haseł skutecznie powstrzyma proces ataku brute force |