Biuletyn Bezpieczeństwa Komputerowego

Wykryj i zatrzymaj ataki w wiadomościach tekstowych

Czym są ataki wykorzystujące wiadomości tekstowe?

Smishing (połączenie słów SMS i phishing) to atak, w którym cyberprzestępcy używają SMS-ów i innych technologii przesyłania wiadomości, aby nakłonić Cię do podjęcia działania, którego nie powinieneś podejmować. Mogą nakłonić Cię do podania danych karty kredytowej, zadzwonienia pod numer telefonu w celu uzyskania informacji bankowych lub wypełnienia ankiety online w celu zebrania danych osobowych. Podobnie jak w przypadku phishingu rozpowszechnianego drogą mailową, atakujący często grają na emocjach, aby skłonić do działania, na przykład tworząc poczucie obowiązku lub ciekawości. Fakt, że w wiadomościach SMS jest znacznie mniej informacji niż w wiadomości e-mail usypia naszą czujność i sprawia, że ataki tego typu są bardziej niebezpieczne, ponieważ trudniej wykryć, że coś jest nie tak.

Powszechnym oszustwem jest wiadomość informująca o wygraniu m.in. iPhone'a. Wystarczy kliknąć w link i wypełnić ankietę, aby go odebrać. W rzeczywistości do wygrania nie ma żadnego telefonu, a ankieta ma na celu zebranie danych osobowych. Innym przykładem może być wiadomość informująca, że paczka nie mogła zostać dostarczona do adresata z powodu niedopłaty. Link do strony przekierowuje do fałszywego panelu logowania do bankowości internetowej, w którym użytkownik jest proszony o podanie informacji potrzebnych do zalogowania się na konto bankowe. W niektórych przypadkach strony mogą nawet nakłaniać do zainstalowania szkodliwej aplikacji mobilnej, która przejmuje kontrolę nad urządzeniem.

Czasami atakujący łączą nawet ataki na telefon z wiadomościami SMS. Na przykład możesz otrzymać SMSa z banku z pytaniem, czy autoryzowałeś płatność. Nadawca wiadomości poprosi o odpowiedź TAK lub NIE. Jeśli odpowiesz, atakujący zadzwoni do Ciebie, podszywając się pod pracownika banku. Następnie spróbuje wyciągnąć od Ciebie informacje, takie jak login i hasło do konta bankowego.

Wykrywanie i zatrzymywanie ataków w wiadomościach tekstowych

Oto kilka pytań, które należy sobie zadać:

- Czy wiadomość wywołuje poczucie obowiązku i sprawia, że robisz jakieś działania w pośpiechu?
- Czy linki w wiadomości prowadzą do witryn, które nakłaniają do podania danych osobowych, karty kredytowej, hasła lub innych poufnych informacji, do których nikt oprócz Ciebie nie powinien mieć dostępu?
- Czy wiadomość brzmi zbyt dobrze, by mogła być prawdziwa? Czy tak naprawdę wygranie iPhone'a w podejrzanej loterii może być realne?

- Czy podlinkowana strona lub usługa zmuszają Cię do płacenia za pomocą niestandardowych metod, takich jak Bitcoin, karty podarunkowe lub przelewy Western Union?
- Czy w wiadomości pojawia się pytanie o wieloskładnikowy kod uwierzytelniający, który został wysłany na Twój numer telefonu lub wygenerowany przez aplikację?
- Czy wiadomość wygląda jakby została wysłana do nieodpowiedniej osoby? Jeśli tak, nie powinieneś odpowiadać na takie wiadomości ani kontaktować się z nadawcą. Najlepiej będzie takie wiadomości usuwać

Jeśli otrzymasz wiadomość od oficjalnej firmy, oddzwoń bezpośrednio na infolinię tej firmy. Do kontaktów używaj wyłącznie numerów telefonu podanych na oficjalnej stronie internetowej. Jeśli otrzymujesz wiadomość o problemie z kontem bankowym, z kartą kredytową, skontaktuj się bezpośrednio ze swoim bankiem lub firmą, która obsługuje kartę kredytową. Numer telefonu znajduje się na oficjalnej stronie internetowej banku lub na odwrocie karty kredytowej. Pamiętaj też, że większość instytucji rządowych, nigdy nie skontaktuje się z Tobą za pomocą wiadomości tekstowych. Zazwyczaj będą wymieć inną drogę komunikacji, np. za pomocą poczty.

Nasza czujność oraz logiczne myślenie jest najlepszą linią obrony przed wszelkimi atakami i oszustwami.

Redaktor gościnny

Jeff Lomas jest detektywem grupy śledczej ds. cyberbezpieczeństwa w Metropolitan Police Department w Las Vegas i prowadzi kurs SANS SEC487 Open-Source Intelligence Gathering and Analysis (OSINT). Jeff bada zaawansowane technologicznie przestępstwa finansowe, w tym kompromitacje biznesowej poczty e-mail, smishing, ransomware oraz złożone przypadki kradzieży kryptowalut.

Źródła

Powstrzymać phishing: https://www.sans.org/newsletters/ouch/stop-that-phish/
Ataki socjotechniczne: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Ataki i oszustwa telefoniczne: https://www.sans.org/newsletters/ouch/vishing/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz