OUCH! Lipiec 2024

OUCH!
SANS SECURITY AWARENESS
Biuletyn Bezpieczeństwa Komputerowego

Ataki za pomocą wiadomości tekstowych

Marek zmartwił się wiadomością tekstową od firmy kurierskiej o treści: "Próba dostawy nie powiodła się! Kliknij, aby zmienić termin, w przeciwnym razie Twoja paczka zostanie zwrócona.” Marek nie zamawiał ostatnio niczego przez Internet, jednak zazwyczaj zamawia tak dużo produktów, że mógł o czymś zapomnieć. Nie chciał stracić swojej paczki, więc kliknął w link i został przeniesiony na stronę, na której został poproszony o podanie danych kontaktowych w celu „zmiany terminu." Wiadomość wydawała się nieco dziwna, ale Marek uznał, że lepiej dmuchać na zimne. Wpisał swoje dane kontaktowe oraz dodatkowe informacje, w tym dane karty kredytowej. Nadawcą wiadomości była firma znana Markowi, więc zrobił wszystko, o co został poproszony. W następnym kroku na stronie pojawiła się informacja, że paczka powinna zostać wkrótce dostarczona. Następnie w ciągu piętnastu minut Marek odebrał telefon z banku. Konsultant powiadomił go, że za pomocą jego karty zostało dokonanych wiele płatności. Marek uzmysłowił sobie, że nie było żadnej paczki, a SMS był oszustwem mającym na celu wyłudzenie, gdy zdał sobie sprawę, że nie było paczki, a wiadomość tekstowa była oszustwem mającym na celu wyłudzenie poufnych danych.

Czym są ataki wykorzystujące wiadomości tekstowe

Ataki za pośrednictwem wiadomości SMS, zwane także smishingiem, mają miejsce, gdy cyberprzestępcy wykorzystują SMS-y lub komunikatory aby nakłonić do podjęcia działania, którego nie powinno się podejmować pod presją czasu, np. rezygnacji z karty kredytowej, podania hasła do konta bankowego lub zainstalowania fałszywej aplikacji mobilnej. Podobnie jak w przypadku ataków typu phishing cyberprzestępcy często grają na emocjach, na przykład wywołując poczucie pilności 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.

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

Oto kilka najczęstszych wskazówek świadczących o tym, że możesz mieć do czynienia z atakiem:

- **Pilne działanie**: Każda wiadomość, która stwarza poczucie ogromnej pilności, gdy ktoś próbuje wywierać na presję, abyś podjął działanie, na przykład domagając się zamknięcia konta.
- **Chęć wzbogacenia się**: Czy wiadomość brzmi zbyt dobrze, by mogła być prawdziwa? Czy tak naprawdę wygranie iPhone'a w podejrzanej loterii może być realne?
- **Ciekawość**: Jeśli otrzymasz wiadomość, która wydaje się pomyłką, lub wiadomość z nieznanego numeru, nie odpowiadaj na nią ani nie próbuj kontaktować się z nadawcą, po prostu usuń tę wiadomość. Są to próby nawiązania kontaktu przez cyberprzestępców.
- **Dane osobiste**: Czy 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?
- **Płatności**: Zachowaj czujność w przypadku nietypowych próśb o płatność, takich jak wysyłanie pieniędzy za pośrednictwem kryptowalut lub przekazów.

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

Destiney Plaza jest inżynierem ds. cyberbezpieczeństwa w Carnegie Mellon University's Software Engineering Institute. Inspiruje wygłaszając prelekcje dla różnorodnych odbiorców, od osób nietechnicznych po specjalistów ds. cyberbezpieczeństwa. Posiada tytuł CISSP, stopień naukowy z informatyki oraz z zarządzania systemami informatycznymi.

Źródła

Zasady biezpiecznych rozmów: https://www.sans.org/newsletters/ouch/messaging-dos-and-donts/
Zatrzymaj oszustwa związane z połączeniami telefonicznymi: https://www.sans.org/newsletters/ouch/stop-phone-call-scams/
Działania na emocjach - o tym jak cyberprzestępcy oszukują: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz