Biuletyn Bezpieczeństwa Komputerowego

Ataki i oszustwa telefoniczne

Wstęp

Kiedy myślisz o cyberprzestępcy, prawdopodobnie masz przed oczami złego geniusza siedzącego za komputerem i przeprowadzającego wyrafinowane ataki przez Internet. Niektórzy współcześni cyberprzestępcy korzystają z zaawansowanych technologii, jednak wielu po prostu używa telefonu, aby oszukać swoje ofiary. Korzystanie z telefonu ma dwie duże zalety: W przeciwieństwie do innych ataków istnieje mniej technologii, które mogą wykryć i powstrzymać atak telefoniczny. Ponadto przestępcom znacznie łatwiej jest zbudzać emocje i budować zaufanie przez telefon, co ułatwia oszukanie ich ofiar. Nauczmy się, jak wykrywać te ataki i jak im przeciwdziałać.

Jak działają ataki telefoniczne?

Przede wszystkim, musisz zrozumieć, że przestępcy zwykle szukają twoich pieniędzy, informacji lub dostępu do twojego komputera (lub komputerów). Robią to, nakłaniając do zrobienia czegoś, czego nie powinieneś robić, poprzez technikę zwaną socjotechniką. Cyberprzestępcy podczas rozmowy często inicjują sytuacje, które wydają się bardzo pilne. Oto niektóre z najczęstszych przykładów:

- Dzwoniący udaje, że jest pracownikiem Urzędu Skarbowego i informuje, że masz niezapłacone podatki. Wyjaśnia, że jeśli nie zapłacisz podatków od razu, pójdziesz do więzienia, a następnie wywiera na Tobie presję, aby zapłacić kartą kredytową przez telefon. Jest to oszustwo. Urząd Skarbowy wysyła oficjalne powiadomienia tylko pocztą.
- Dzwoniący udaje, że pochodzi z firmy takiej jak Amazon, Apple lub Microsoft Tech Support i wyjaśnia, że komputer jest zainfekowany. Gdy przekonają Cię, że Twój komputer jest zainfekowany, wywierają presję, abyś umożliwił im zdalny dostęp do komputera.
- Automat informuje Cię, że konto bankowe lub karta kredytowa zostały zablokowane. Następnie prosi Cię o potwierdzenie tożsamości, a także odpowiedzi na wszelkiego rodzaju pytania. To nie jest Twój bank. Po prostu rejestrują wszystkie informacje na Twój temat w celu kradzieży tożsamości.

Chroń siebie

Najlepszą obroną przed atakiem telefonicznym jesteś Ty sam. Pamiętaj o następujących rzeczach:

- Za każdym razem, gdy ktoś dzwoni do Ciebie i wywołuje poczucie pośpiechu lub presji, bądź uważny. Atakujący próbują zmusić cię do popełnienia błędu. Nawet jeśli na początku rozmowa telefoniczna wydaje się być w porządku, w momencie, kiedy zacznie wydawać się podejrzana, możesz przerwać rozmowę.

- Zachowaj szczególną ostrożność w przypadku rozmówców, którzy nalegają na zainstalowanie na komputerze konkretnego programu.
- Nigdy nie ufaj nazwie ID dzwoniącego. Atakujący często fałszują numer, więc może wyglądać na to, że pochodzi z prawdziwej organizacji lub ma ten sam numer kierunkowy co Twój numer telefonu.
- Nigdy nie pozwalaj rozmówcy przejąć tymczasowej kontroli nad komputerem ani nie zgadzaj się na pobranie dodatkowego oprogramowania. W ten sposób ktoś może zainfekować twój komputer.
- Nigdy nie podawaj osobie po drugiej stronie słuchawki informacji, które powinna już mieć. Na przykład, jeśli zadzwoni do Ciebie bank, nie powinien pytać o numer konta.
- Jeśli uważasz, że rozmowa telefoniczna jest atakiem, po prostu się rozłącz. Jeśli chcesz potwierdzić, że rozmowa telefoniczna była wiarygodna, przejdź do witryny internetowej organizacji (np. Banku) i zadzwoń bezpośrednio na numer obsługi klienta. W ten sposób możesz się upewnić, że rozmawiasz z wiarygodną organizacją.
- Jeśli dzwoni ktoś, kogo nie znasz osobiście, niech nagra się na pocztę głosową. W ten sposób możesz przeglądać nieznane połączenia w odpowiednim czasie. Co więcej, na wielu telefonach można to domyślnie włączyć za pomocą funkcji „Nie przeszkadzać".

Liczba oszustw i ataków telefonicznych stale rośnie. Jesteś najlepszą bronią w ich wykrywaniu i zatrzymywaniu.

Redaktor gościnny

Jen Fox zdobyła czarną odznakę podczas DEF CON 23 w kategorii Social Engineering. Zajmuje się zwiększaniem świadomości bezpieczeństwa komputerowego w firmie Domino. Jen na Twitterze @j_fox.

Zródła

Ataki socjotechniczne: https://www.sans.org/security-awareness-training/resources/social-engineering-attacks
Oszustwa bazujące na wiadomościach tekstowych: https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks
Spersonalizowane oszustwa: https://www.sans.org/security-awareness-training/resources/personalized-scams
Zgłaszanie oszustw: https://policja.pl/pol/form/dodaj153,Formularz-kontaktowy-Cyberprzestepczosc.html

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz