SANS SECURITY AWARENESS

OUCH!

Biuletyn Bezpieczeństwa Komputerowego

Oszustwa Telefoniczne oraz Scam

Wstęp

Słysząc hasło cyberprzestępca prawdopodobnie wyobrażasz sobie nieprzeciętnie inteligentnego "mózgowca", przeprowadzającego zaawansowane ataki za pośrednictwem Internetu. Podczas gdy wielu z nich wykorzystuje rozwiązania takie jak wiadomości e-mail czy komunikatory tekstowe, dla niektórych środkiem do przeprowadzenia ataku będzie po prostu telefon. Ten zaś posiada dwie zasadnicze dla przestępców zalety. Po pierwsze, w przeciwieństwie do wiadomości e-mail, rozmowy telefoniczne posiadają mniej rozwiązań pozwalających na monitorowanie ich treści, wykrycie próby ataku oraz powstrzymanie go. Po drugie, przestępcom w trakcie bezpośredniej rozmowy telefonicznej o wiele łatwiej jest zmanipulować rozmówcę, nakłaniając do podjęcia niekorzystnej dla niego decyzji. Poniżej prezentujemy kilka sposobów umożliwiających rozpoznanie i ochronę przed oszustwami telefonicznymi.

Jak przeprowadzane są ataki telefoniczne?

Pierwszym krokiem jest zrozumienie celu przestępców. Zazwyczaj jest to kradzież środków finansowych, pozyskanie informacji, uzyskanie dostępu do komputera ofiary lub osiągnięcie wszystkich tych celów jednocześnie. Przestępcy manipulują swoimi rozmówcami w taki sposób, by wykonywali wskazane przez nich instrukcje. Prowadząc rozmowę, kreują sytuacje wymagające podejmowania pilnych działań. Atakujący może próbować wyprowadzić ofiarę z równowagi emocjonalnej, np. strasząc ją, po to by działała w pośpiechu i nieracjonalnie. W ten sposób zmusza się ją do podjęcia nieprzemyślanych działań. Poniżej kilka przykładów:

Osoba dzwoniąca przedstawia się jako pracownik urzędu skarbowego i twierdzi, że posiadasz nieuregulowane płatności. Tłumaczy, że jeśli nie zostaną one niezwłocznie wykonane, możesz trafić do więzienia. Dzwoniący wywiera presję, zachęcając do płatności kartą, prosząc o przedyktowanie znajdujących się na karcie danych przez telefon. Jest to przykład wyłudzenia danych. Większość urzędów skarbowych nie informuje o zadłużeniach za pośrednictwem poczty e-mail czy telefonu. Takie powiadomienia są rozsyłane listownie w formie oficjalnych pism urzędowych.

Kontaktuje się z Tobą osoba oznajmiająca, że jest przedstawicielem firmy Microsoft i informuje o zainfekowaniu komputera złośliwym oprogramowaniem. Następnie namawia Cię do zakupu dedykowanej aplikacji lub prosi, byś umożliwił jej uzyskanie zdalnego dostępu do komputera. Microsoft nie będzie do Ciebie dzwonił.

Otrzymałeś wiadomość na skrzynkę poczty głosowej informującą o zawieszeniu Twojego konta bankowego. Wiadomość zawiera instrukcję ponownej aktywacji konta. Sugeruje ona wykonanie połączenia na wskazany numer. Dzwoniąc na podany numer telefonu zostanie przeprowadzona rzekoma weryfikacja tożsamości, polegająca na udzieleniu odpowiedzi na przygotowaną listę pytań. Banki nie działają w ten sposób. Jest to próba wyłudzenia danych w celu kradzieży tożsamości.

Jak się chronić

Najważniejszym elementem obrony przed oszustwem telefonicznym jesteś Ty sam. Pamiętaj o kilku podstawowych zasadach.

Zawsze, gdy ktoś zadzwoni do Ciebie i będzie podczas rozmowy ponaglał Cię do czegoś, zachowaj czujność. Nawet jeżeli rozmowa telefoniczna na początku nie brzmi podejrzanie, ale z czasem jakiś jej element zaczyna Cię niepokoić, masz prawo powiedzieć "nie" w dowolnym momencie.

Jeżeli masz wrażenie, że rozmowa może być próbą ataku, rozłącz się. Chcąc zweryfikować wiarygodność dzwoniącego, wejdź na stronę organizacji (np. Twojego banku) i samodzielnie zadzwoń na firmową infolinię. Dzięki temu będziesz wiedział, że rzeczywiście rozmawiasz z przedstawicielem organizacji.

Nigdy nie ufaj wyświetlanemu identyfikatorowi osoby dzwoniącej. Przestępcy często fałszują wyświetlany numer tak, by wyglądał na pochodzący od prawdziwej organizacji i nie wzbudzał Twoich podejrzeń.

Nigdy nie pozwalaj osobie dzwoniącej na tymczasowe przejęcie kontroli nad Twoim komputerem oraz nie pobieraj sugerowanego przez nią oprogramowania. Tą metodą przestępcy mogą zainfekować Twój komputer.

Jeśli połączenie wykonywane jest z numeru osoby, której osobiście nie znasz, nie odbieraj go. Możesz później odsłuchać wiadomość ze skrzynki głosowej. Obecnie w większości telefonów można skorzystać z funkcji "Do not disturb" automatycznie przekierowującej połączenie do skrzynki głosowej.

Coraz częściej można spotkać się z oszustwami przeprowadzanymi z wykorzystaniem połączeń telefonicznych. To, jak szybko uda Ci się wykryć i powstrzymać próbę ataku zależy w głównej mierze właśnie od Ciebie.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Redaktor Gościnny

Jen Fox *pracuje jako starsza konsultantka ds. bezpieczeństwa w All Covered. W ramach pracy świadczy usługi związane ze zwiększaniem świadomości zagrożeń w cyberprzestrzeni, zarządzaniem ryzykiem oraz problematyką socjotechniki. Na Twitterze można znaleźć ją jako* @j_fox.

Przydatne linki

Socjotechnika: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_po.pdf
Informacja UKE na temat niezgodnego z prawem wykorzystywania usług telekomunikacyjnych:
https://cik.uke.gov.pl/gfx/cik/userfiles/m-pietrzykowski/cik/niezgodne_z_prawem_wykorzystanie_uslug.pdf