Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

- Wstęp
- Scenariusz oszustwa
- Jak się chronić

Oszustwa telefoniczne pod przykrywką pomocy technicznej

REDAKTOR GOŚCINNY

Redaktorem gościnnym tego wydania biuletynu OUCH! jest Lenny Zeltser. Zajmuje się zabezpieczaniem procesów IT w firmie NCR Corp oraz naucza z ramienia Instytutu SANS sposobów walki ze złośliwym oprogramowaniem. Jest bardzo aktywny na Twitterze (@lennyzeltser) oraz prowadzi blog pod adresem http://blog.zeltser.com.

WSTĘP

Wiele z cyberataków na użytkownika Internetu to próby oszustw w celu wyłudzenia pieniędzy lub poufnych danych osobowych. Sztandarowym przykładem jest phishing, czyli wiadomości email, w których przestępca podszywa się pod zaufaną osobę lub instytucję, np. Twojego przyjaciela lub bank w którym masz konto. Przestępcza aktywność tego rodzaju ciągle stanowi problem, jednakże cyberprzestępcy sięgają także po inne metody, takie jak wykonywanie telefonów do nieświadomych zagrożenia ludzi. W dalszej części biuletynu przedstawimy jak działa "oszustwo na telefon", a zwłaszcza jego wersja w postaci "fałszywego telefonu pomocy technicznej". Opiszemy także metody w jaki sposób bronić się przed tego rodzaju oszustwami.

SCENARIUSZ OSZUSTWA

Żadne z dwóch oszustw nie jest identyczne, ale większość z nich zawiera podobne do siebie elementy, które tu przytoczymy. Z reguły po odebraniu telefonu przedstawia się nam osoba twierdząc, że dzwoni z firmy zajmującej się pomocą techniczną oraz w jakiś sposób spokrewnionej z dobrze znaną użytkownikowi marką, np. Microsoft. Zwykle powodem kontaktu z użytkownikiem jest rzekome wykrycie, że jego komputer jest zarażony wirusem i przejawia niecodzienne zachowanie w Internecie. Dzwoniący oferuje pomoc w usunięciu zagrożenia, która z reguły polega na wykupieniu licencji na jakieś oprogramowanie. Oszust stara się zdezorientować osobę, do której dzwoni używając jak największej ilości technicznych zwrotów. Przykładem działań, do wykonania których oszust może nakłaniać jest skorzystanie z serwisu online lub pobranie i instalacja programu umożliwiającego zdalny dostęp do Twojego komputera. Wszystko to pod pretekstem chęci niesienia pomocy i potwierdzenia infekcji wirusem. Często programy z serwisów takich jak LogMeIn.com lub ShowMyPC.com, do instalacji których próbują nakłonić oszuści, są nieszkodliwe w swojej naturze i nie będą wykryte przez programy antywirusowe, ale dają oszustowi kontrolę nad Twoim komputerem. Jeżeli ją zdobędzie może zacząć usuwać zabezpieczenia przeciwko złośliwemu oprogramowaniu lub nawet nieodwracalnie uszkodzić system operacyjny doprowadzając do sytuacji, iż poprawnie działający wcześniej komputer zacznie raportować błędy oraz problemy z funkcjonowaniem. Część z tych działań

Bezpieczne korzystanie z chmury

może zostać wykonana przez użytkownika po otrzymaniu stosownych poleceń od "personelu technicznego", tak aby dodatkowo uśpić czujność, zastraszyć i ułatwić tym samym wyłudzenie pieniędzy lub danych osobowych.

Pamiętaj, że wszystko do czego przestępca stara się Cię przekonać to kłamstwo. Praktycznie nie istnieje sposób, który umożliwia obronę przed oszustwem telefonicznym, dlatego miej się na baczności. Przestępca wykorzystując telefon może znacznie skuteczniej wywołać uczucie potrzeby podjęcia natychmiastowego działania niż ma to miejsce w czasie czytania zwykłej wiadomości email. Dlatego najlepszą obroną przed tego rodzaju atakami nie jest technologia sama w sobie lecz dobre praktyki.

JAK SIĘ BRONIĆ

Od czasu do czasu zdarza się, że firmy z usług których korzystasz (np. banki) dzwonią, aby uzupełnić lub uaktualnić dane o Tobie. Prawdziwym wyzwaniem jest odróżnienie prawdziwych rozmówców od oszustów polujących na Twoje pieniądze. Poniżej prezentujemy kilka dobrych rad, które mogą się okazać pomocne w takiej sytuacji

- Jeżeli ktoś prosi Cię o podanie poufnych danych lub chce abyś coś wykonał, postaraj się najpierw potwierdzić tożsamość rozmówcy zanim cokolwiek zrobisz. Upewnij się z jakiej firmy dzwoni i jeżeli wcześniej o niej nie słyszałeś może to oznaczać próbę wyłudzenia. Jeżeli znasz firmę, którą podaje rozmówca zaproponuj, aby podał Ci swoje imię, nazwisko oraz numer wewnętrzny pod którym można się z nim skontaktować. Posiadając te dane możesz z łatwością zweryfikować ich prawdziwość, np. sprawdzając firmę w Internecie, a później oddzwaniając do tej osoby.

Bądź ostrożny w przypadku gdy ktokolwiek prosi Cię o zdalny dostęp do Twojego komputera lub stara się wymusić zakup oprogramowania, które rzekomo go zabezpieczy. Tego typu telefony to z pewnością próba oszustwa.

- Jeżeli rozmówca stara się wywrzeć na Tobie presję i twierdzi, że potrzebne jest natychmiastowe działanie i nie można już dłużej zwlekać, to z dużą dozą pewności jest to próba wyłudzenia. Nie ufaj niczemu co mówi taka osoba i zakończ jak najszybciej rozmowę.

Bezpieczne korzystanie z chmury

- Jeżeli będziesz chciał zweryfikować tożsamość dzwoniącego, nie polegaj wyłącznie na numerze jaki wyświetla się na ekranie telefonu. Bardzo często oszuści używają technik, które umożliwiają im spreparowanie takiego numeru w taki sposób, że gdy odbierasz telefon widzisz numer swojego banku lub innej zaufanej instytucji.
- Nigdy, ale to przenigdy nie zdradzaj swojego hasła dostępu. Nie ważne, kto o nie prosi i za kogo się podaje. Żadna z prawdziwych firm nigdy nie będzie Cię prosić o podanie hasła.
- Nigdy nie podawaj informacji, które dana instytucja już powinna posiadać, np. jeżeli odbierasz telefon z banku to rozmówca powinien znać już numer Twojego rachunku.

ŹRÓDŁA

W celu poprawy czytelności tekstu niektóre odnośniki w biuletynie zostały skrócone przy użyciu usługi TinyURL. Dla zachowania bezpieczeństwa, OUCH! używa funkcji podglądu TinyURL, która pozwala podejrzeć docelowy adres odnośnika oraz pyta o pozwolenie przed wejściem na stronę o docelowym adresie.

Recording of Actual Tech-Support Scam:
http://preview.tinyurl.com/cbg9kku

Microsoft On Tech-Support Scams:
http://preview.tinyurl.com/cxpwkc9

Symantec on Tech-Support Scams:
http://preview.tinyurl.com/244raev

Reporting Scams:
https://www.ftccomplaintassistant.gov

ISC Survey on Tech-Support Scams:
https://isc.sans.edu/reportfakecall.html

Common Security Terms:
http://preview.tinyurl.com/6wkpae5

SANS Security Tip of the Day:
http://preview.tinyurl.com/6s2wrkp

DOWIEDZ SIĘ WIĘCEJ

Zasubskrybuj comiesięczny Biuletyn Bezpieczeństwa Komputerowego – SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS z zakresu bezpieczeństwa komputerowego i osobowego. Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

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

Redakcja: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz