OUCH! | Listopad 2014

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

- **Socjotechnika**
- **Wykrywanie / Powstrzymanie ataku socjotechnicznego**
- **Zapobieganie atakom socjotechnicznym w przyszłości**

Socjotechnika

Wstęp

W powszechnym, błędnym mniemaniu wielu osób przestępcy internetowi używają zaawansowanych narzędzi i technologii, aby włamać się do komputerów, na konta internetowe i urządzenia mobilne. Jest to po prostu nieprawda. Przestepcy nauczyli się, że jednym z najprostszych sposobów, aby wykraść informacje lub włamać się na komputer jest po prostu oszukanie Ciebie. W tym biuletynie dowiemy się, jak działają takie ataki na człowieka, zwane także socjotechniką, oraz co można zrobić, aby się przed nimi ochronić.

Redaktor gościnny

Alissa Torres jest certyfikowanym instruktorem SANS, specjalizuje się w zaawansowanej informatyce śledczej i reagowaniu na incydenty. Jej doświadczenie obejmuje służbę na pierwszej linii frontu jako specjalista obsługi incydentów i pracę w zespole bezpieczeństwa wewnętrznego jako śledczy informatyczny. Alissę można znaleźć na Twitterze jako **@sibertor**.

Socjotechnika

Socjotechnika jest rodzajem ataku psychologicznego polegającym na tym, że atakujący nakłania swoją ofiarę do wykonania jakiejś czynności. Socjotechnika istnieje od tysięcy lat - oszustwa i naciągacze to przecież nic nowego. Jednak oszuści komputerowi doskonale wiedzą, że użycie tych technik w Internecie jest wyjątkowo skuteczne i może być stosowane na milionach osób. Najprostszym sposobem, aby zrozumieć, jak działa inżynieria społeczna, jest przyjrzenie się przykładom z życia.

Odbierasz telefon od kogoś podającego się za pracownika serwisu komputerowego, dostawcę usług internetowych albo wsparcie techniczne firmy Microsoft. Rozmówca wyjaśnia, że zauważył, że Twój komputer zachowuje się dziwnie, np. skanuje Internet lub wysyła spam, i są przekonani, że jest on zainfekowany. Chce pomóc Ci przez zbadanie problemu i zabezpieczenie komputera. Następnie używając niezrozumiałych dla przeciętnego użytkownika terminów technicznych prowadzi Cię przez wiele skomplikowanych kroków, próbując stwierdzić, że Twój komputer jest zainfekowany.

Przykładowo, może poprosić o sprawdzenie, czy masz pewne pliki na komputerze i pokaże Ci krok po kroku jak je znaleźć. Po zlokalizowaniu plików rozmówca będzie zapewniał, że pliki te są oznaką zainfrkowania komputera, gdy w rzeczywistości są to popularne pliki systemowe znajdujące się na każdym komputerze. Kiedy już wmówi Ci, że twój komputer jest zainfekowany, będzie Cię skłaniać do odwiedzenia ich strony i zakupu oprogramowania zabezpieczającego lub poprosi o przyznanie zdalnego dostępu do komputera, aby mógł go naprawić. Jednak oprogramowanie, które sprzedają to w rzeczywistości złośliwy program. Jeśli zakupisz i zainstalujesz to oprogramowanie, zostałeś nie tylko nakłoniony do zainfekowania swojego własnego komputera, ale wręcz Ty sama po prostu zapłaciłaś im, aby to zrobili. Jeśli dasz mu zdalny dostęp do komputera zainfekuje go złośliwym oprogramowaniem i przejmie nad nim kontrolę.

Socjotechnika

Należy pamiętać, że podobne ataki socjotechniczne nie ograniczają się do rozmów telefonicznych. Mogą zdarzyć się przy użyciu niemal każdej technologii, w tym ataków phishingowych poprzez e-mail, SMS, wiadomość na portalach społecznościowych jak Facebook czy Twitter lub czatach internetowych. Najważniejsze jest, aby wiedzieć, na co zwracać uwagę.

Naucz się jak zapobiegać, wykrywać i zatrzymać atak socjotechniczny, bo jest to najlepszy sposób, w jaki możesz się ochronić.

Wykrywanie / Powstrzymanie ataku socjotechnicznego

Najprostszym sposobem obrony przed atakami inżynierii społecznej jest zachowanie zdrowego rozsądku. Jeśli coś wydaje się podejrzane lub niewłaściwe, może to być atak socjotechniczny. Oto powszechne symptomy wskazujące na atak socjotechniczny:

- Ktoś tworzy wrażenie potrzeby podjęcia bardzo szybko decyzji. Jeśli czujesz się pod presją by szybko podjąć decyzję, bądź podejrzliwy.
- Ktoś prosi o informacje, do których nie powinien mieć dostępu ani nie powinien ich znać.
- Coś zbyt piękne, aby mogło być prawdziwe. Typowym przykładem jest przekazanie informacji o wygranej na loterii, pomimo że nigdy nie brało się w niej udziału.

Jeśli podejrzewasz, że ktoś próbuje zrobić z Ciebie ofiarę ataku socjotechnicznego, nie komunikuj się więcej z tą osobą. Jeśli robi to przez telefon, po prostu odrzuć połączenie. Jeśli rozmawia z tobą online, zakończ czat. Jeśli jest to e-mail, w który do końca nie wierzysz, usuń go. Jeśli atak jest związany z Twoją pracą, należy natychmiast zgłosić go do działu help desk lub zespołu bezpieczeństwa informacji.

Zapobieganie atakom socjotechnicznym w przyszłości

Na szczęście istnieją środki ostrożności, które można podjąć, aby nie narażać się na przyszłe ataki socjotechniczne.

- **Nigdy nie dziel się swoim hasłem**. Żadna szanująca się organizacja nigdy nie skontaktuje się z prośbą o podanie hasła. Jeśli ktoś prosi o podanie hasła, to jest próba ataku socjotechnicznego.

- **Nie udostępniaj zbyt wiele**. Im więcej atakujący wie o tobie, tym łatwiej jest wprowadzić Cię w błąd i nakłonić do robienia tego, czego chcą. Nawet udostępnianie z pozoru nieznaczących szczegółów, które z czasem połączone w całość, może stworzyć kompletny obraz Ciebie. Im mniej udostępniasz publicznie na portalach społecznościowych, w recenzjach produktów lub na publicznych forach i listach mailingowych, tym mniej prawdopodobne, że zostaniesz zaatakowany.

Socjotechnika

- **Sprawdź kontakt**. Czasami, z uzasadnionych powodów, może zadzwonić do Ciebie ktoś z banku, wydawca karty kredytowej, dostawca usług telefonii komórkowej lub innych organizacji. Jeśli masz jakiekolwiek wątpliwości co do tego, czy pytanie o udzielenie informacji jest uzasadnione, poproś osobę, która dzowni o jej imię i nazwisko i numer telefonu. Następnie weź numer telefonu tej firmy z zaufanego źródła, takiego jak numer na odwrocie karty kredytowej, numer z wyciągu bankowego, albo numer na stronie internetowej firmy (wpisz sam adres URL w przeglądarce). Tym sposobem, kiedy sam wykonujesz telefon, wiesz, że naprawdę z rozmawiasz z tym za kogo się podają. Choć może wydawać się, że te czynności mogą być kłopotliwe, warto jest je wykonać dla ochrony tożsamości i swoich danych osobowych.

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące 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

Źródła

Email i ataki phishingowe:	http://www.securingthehuman.org/ouch/2013#february2013
Bezpieczeństwo w serwisach społecznościowych:	http://www.securingthehuman.org/ouch/2013#march2013
Unikaj oszustw w internecie (ang.):	http://www.onguardonline.gov/topics/avoid-scams

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Siewierski

