SANS SECURITY AWARENESS
CERT.PL
OUCH! | Listopad 2017
Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- **Fałszywe sklepy internetowe**
- **Twój komputer / Urządzenie mobilne**
- **Korzystanie z karty płatniczej**

Bezpieczne zakupy w sieci

Sezon na ostrożność

Wielkimi krokami zbliża się czas przedświąteczny i już wkrótce mnóstwo osób zajmie się poszukiwaniem prezentów dla rodziny i przyjaciół. Wiele osób, chcąc uniknąć nerwowego przepychania się między półkami sklepowymi oraz stania w kolejkach, zdecyduje się na zakupy online. Niestety okres przedświąteczny to również moment zwiększonej aktywności przestępców. W tym czasie powstaje wiele stron internetowych fałszywych sklepów mających na celu kradzież danych oraz środków finansowych. W tym numerze OUCH! wyjaśnimy zagrożenia związane z zakupami online oraz przedstawimy metody ochrony przed działającymi w sieci oszustami.

Redaktor gościnny

Lenny Zeltser jest inżynierem bezpieczeństwa w Minerva Labs oraz prowadzi szkolenia z analizy szkodliwego oprogramowania w instytucie SANS. Lenny jest aktywnym blogerem, a jego wpisy dostępne są na stronie **zeltser.com** oraz na twitterze **@lennyzeltser**.

Fałszywe sklepy internetowe

Większość sklepów internetowych jest legalna i bezpieczna. Istnieją jednak takie, które są fałszywymi stronami, przygotowanymi przez przestępców. Takie spreparowane strony powstają zazwyczaj przez skopiowanie wyglądu i wykorzystania nazwy znanych sklepów. Gdy taki sklep już funkcjonuje, oszuści starają się przyciągnąć do niego użytkowników szukających najbardziej korzystnej cenowo oferty. Szukając produktu w najniższej cenie, możliwe jest natrafienie na jeden z takich fałszywych sklepów. Wybierając sklep internetowy lub serwis aukcyjny zachowaj ostrożność w przypadku tych, które oferują wyjątkowo niskie ceny w porównaniu do znanej Ci konkurencji. Powodem, dla którego różnica w cenie jest tak znacząca może być to, że po zakupie otrzymamy towar podrobiony, kradziony albo po prostu wcale do nas nie dotrze. Zabezpiecz się przed takimi sytuacjami postępując zgodnie z poniższymi zaleceniami:

- Jeśli to możliwe, dokonuj zakupów poprzez strony, które znasz lub z których już korzystałeś.
- Sprawdź czy sklep posiada adres mailowy, numer telefonu do działu sprzedaży lub wsparcia, do których można skierować dodatkowe pytania. Jeśli witryna wygląda podejrzanie, zadzwoń pod podany numer telefonu i porozmawiaj z osobą odpowiedzialną za sprzedaż. Jeśli nie uda się nawiązać kontaktu z pracownikiem, może to być pierwszy sygnał ostrzegawczy i należy dokładniej sprawdzić wiarygodność sprzedawcy.
- Zwróć uwagę na oczywiste wskazówki, takie jak rażące błędy gramatyczne i ortograficzne lub oferty zbyt korzystne by mogły być prawdziwe.
- Zachowaj ostrożność jeśli strona internetowa do złudzenia przypomina witrynę innego dobrze znanego sklepu lub serwisu aukcyjnego, ale jej adres różni się od oryginalnego nawet w niewielkim stopniu (np. jedną literą). Przykładowo, planując zakupy w serwisie Allegro chcesz odwiedzić stronę https://allegro.pl/. Istnieje możliwość, że w wyniku podpowiedzi wyszukiwarki lub otwarcia linku z wiadomości mailowej ostatecznie znajdziesz się na domenie, udającej ten serwis aukcyjny np. pod adresem http://alleegro.pl.
- Wpisz nazwę sklepu lub adres URL do wyszukiwarki i zobacz, co inne osoby napisały o tej stronie w przeszłości.

Bezpieczne zakupy w sieci

Dobra reputacja stony może być wskaźnikiem, który pomoże podjąć decyzję o zakupie produktu z takiego sklepu. Zwróć uwagę na takie części opisów jak “oszustwo”, “SCAM” lub “fałszywy”. Brak opinii to też nie jest dobry znak, ponieważ oznacza, że strona jest nowa. Nie traktuj jednak opinii dostępnych w internecie jako ostatecznego osądu nad uczciwością danego serwisu gdyż bywają przypadki kiedy takie pozytywne opinie były sztucznie generowane przez przestępców lub wręcz przejmowane po dawniej działających sklepach.

- Przed zakupem czegokolwiek upewnij się, że strona korzysta z szyfrowanego połączenia. Większość przeglądarek wyświetla takie połączenia z logiem kłódki oraz ciągiem znaków HTTPS na zielono przed nazwą strony. Niestety, ze względu na istnienie portali umożliwiających darmowe generowanie certyfikatów służących do szyfrowania połączenia, przestępcy coraz częściej również posiadają na swoich stronach komunikację za pomocą HTTPS.

Ochroń się robiąc zakupy on-line tylko na zaufanych stronach o dobrej reputacji.

Pamiętaj, że jeśli strona wygląda profesjonalnie, nie oznacza od razu, że jest prawdziwa. Jeśli jakiś aspekt serwisu wydaje Ci się podejrzany, lepiej poświęcić trochę czasu na sprawdzenie, czy sklep nie jest próbą oszustwa. Jeśli nie masz pewności czy sklep jest prawdziwy, to po prostu z niego nie korzystaj. Zamiast ryzykować, lepiej skorzystać ze sprawdzonego serwisu, co do którego masz pewność, że nie został spreparowany przez przestępców. Wówczas masz szansę otrzymać oryginalny produkt, a Twój wyciąg z konta bankowego nie zaskoczy Cię.

Bezpieczny komputer / urządzenie mobilne

Robienie zakupów tylko w bezpiecznych sklepach nie uchroni nas w zupełności przed próbami kradzieży danych lub środków finansowych. Również komputer, który jest wykorzystywany do wykonywania transakcji online musi być odpowiednio zabezpieczony. Przestępcy stale próbują infekować urządzenia za pomocą różnorodnych metod aby zdobyć numery kart kredytowych, dane logowania do serwisów bankowych oraz innych ważnych usług. Podejmij następujące kroki, aby Twoje urządzenia były bezpieczne:

- Jeśli masz w domu dzieci, rozważ korzystanie z różnych urządzeń przez dzieci i dorosłych. Dzieci są ciekawskie i lubią klikać w kolorowe i interaktywne obrazki, a w rezultacie łatwo może dojść do zainfekowania urządzenia, z którego korzystają. Dzięki osobnemu urządzeniu tylko do transakcji internetowych, takich jak bankowość i zakupy, można zmniejszyć ryzyko kompromitacji wrażliwych danych oraz zarażenia. W ostateczności można również stworzyć oddzielne konta na wspólnym komputerze i skonfigurować je tak aby dzieci nie miały na nim uprawnień administracyjnych.
- Zawsze instaluj najnowsze aktualizacje systemu operacyjnego i posiadaj uruchomiony program antywirusowy z aktualną bazą sygnatur. To sprawi, że zainfekowanie Twojego urządzenia dla przestępców będzie o wiele trudniejsze.

Karta płatnicza

Regularnie sprawdzaj wyciąg z karty płatniczej dzięki czemu szybko będziesz mógł wykryć podejrzane transakcje, zwłaszcza

Bezpieczne zakupy w sieci

po dokonaniu zakupu w sklepie online, co do którego nie miałeś pełnego zaufania. Niektóre banki dają możliwość włączenia powiadomień SMS albo email dla każdej realizowanej płatności powyżej ustalonej kwoty. Zalecamy uruchomienie takiej usługi, aby natychmiast otrzymywać informacje o wszelkich zmianach salda karty. Innym rozwiązaniem jest posiadanie oddzielnej karty wyłącznie do transakcji internetowych. W przypadku wycieku danych karty, jej wymiana nie będzie wpływać na resztę Twoich operacji. Jeśli podejrzewasz, że dane karty kredytowej zostały podane na fałszywej stronie internetowej, jak najszybciej zadzwoń do banku i zablokuj kartę. Z tego powodu karty kredytowe są lepsze od zakupów online niż karty debetowe. Karty debetowe pobierają pieniądze bezpośrednio z konta bankowego i jeśli zostało popełnione oszustwo, może być znacznie trudniej otrzymać zwrot pieniędzy.
Istnieją również rozwiązania pozwalające na wykonywanie płatności bez narażania swojej karty kredytowej. Rozważ korzystanie z serwisów pośredniczących w płatnościach, takich jak PayPal albo PayU, które nie wymagają ujawnienia numeru karty sprzedawcy.

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 securingthehuman.sans.org/ouch/archives 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

Inżynieria społeczna:	https://securingthehuman.sans.org/ouch/2017#january2017
Cztery kroki do bezpieczeństwa:	https://securingthehuman.sans.org/ouch/2016#october2016
Zabezpieczanie sieci domowej:	https://securingthehuman.sans.org/ouch/2016#february2016
Wskazówka bezpieczeństwa dnia SANS:	https://www.sans.org/tip_of_the_day.php

Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Polski przekład (NASK/CERT Polska): Sebastian Kondraszuk, Michał Strzelczyk, Jacek Sikorski

