Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

Fałszywe strony

REDAKTOR GOŚCINNY

Arrigo Triulzi jest redaktorem gościnnym tego wydania. Jest certyfikowanym instruktorem SANS i niezależnym konsultantem bezpieczeństwa z Genewy.

WSTĘP

Jedną z zalet zakupów on-line jest możliwość znalezienia produktów lub usług po niższych cenach niż w zwykłych sklepach. Przestępcy doskonale o tym wiedzą i będą próbowali wykorzystać chęć znalezienia dobrej okazji w Internecie. Aby osiągnąć swój cel tworzą fałszywe strony internetowe, które wyglądają zupełnie legalnie, ale sprzedawane są na nich towary podrobione lub, co gorsza, po zapłacie nie są dostarczane do kupującego wcale. W tym biuletynie przedstawimy przykład takiego ataku a następnie wyjaśnimy w jaki sposób można zabezpieczyć się przed podobnymi oszustwami.

PRZYKŁAD FAŁSZYWEJ STRONY

Załóżmy, że chcesz kupić nosidełko dla dziecka, na przykład jako prezent dla znajomego lub krewnego z rodziny gdzie ostatnio pojawił się noworodek. Zdecydowałeś się poszukać okazji w Internecie i szukasz nosidełek dziecięcych konkretnej marki X, gdyż wiesz że jest to marka preferowana przez Twojego przyjaciela. Szukając nosidełek marki X szybko się orientujesz, że wiele witryn sprzedaje je w bardzo zróżnicowanych cenach. Wybierasz stronę, która ma najniższe ceny i kupujesz produkt on-line. Kilka tygodni później otrzymujesz produkt, ale odkrywasz, że nie wygląda on dobrze: niektóre części są zepsute, materiał jest uszkodzony lub produkt jest używany. Otwierasz stronę internetową aby zwrócić produkt, ale okazuje się, że nie ma na niej żadnego numeru telefonu. Wówczas wysyłasz wiadomość e-mail do serwisu, ale nigdy nie otrzymujesz odpowiedzi na swoją reklamację. Właśnie się okazało, że kupiłeś fałszywy (lub kradziony) produkt z podrobionej strony internetowej.

Przestępcy po prostu skopiowali oryginalną stronę producenta (w tym przypadku marki X), umieścili tę stronę pod nową nazwą domeny, nad którą mieli kontrolę, a następnie znacząco obniżono ceny, aby zachęcić ludzi do zakupu. Produkty które dostarczają są sfałszowane, skradzione lub używane albo po prostu nie są wysyłane w ogóle. A w tym wypadku niezależnie jaką cenę zapłacisz, to dla nich czysty zysk.

JAK SIĘ BRONIĆ

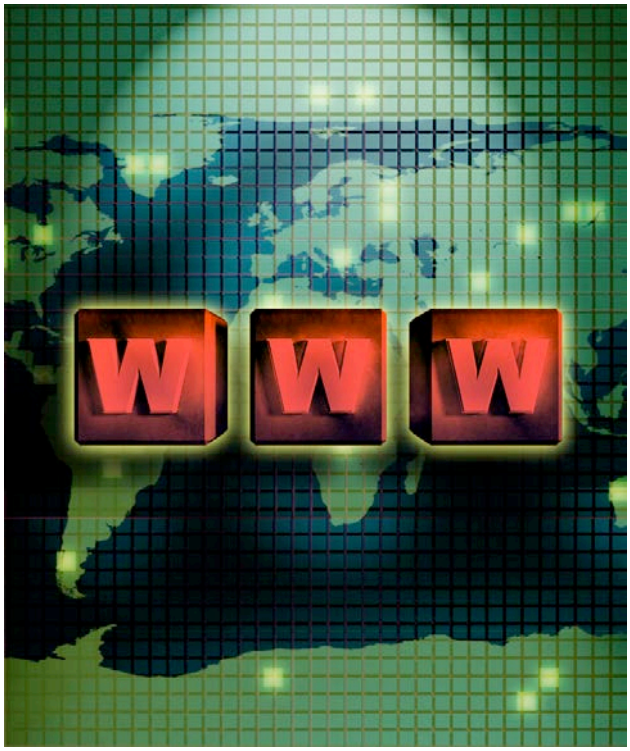
To zrozumiałe że chcesz wykorzystać możliwości jakie daje Internet, w tym także do robienia zakupów on-line. Oto kilka kroków, które można podjąć, aby chronić się przed atakami takimi jak opisane powyżej:

1. Jeśli cena wydaje się być zbyt atrakcyjna, bądź bardzo podejrzliwy.
2. Zadzwoń na numer obsługi klienta. Brakuje obsługi

Fałszywe strony

klienta czy jakiegokolwiek innego numeru? Kolejna czerwona lampka.

3. Często przestępcy, którzy instalują fałszywe strony internetowe nie mówią w rodzimym języku witryny. Tekst w wysyłanych do klienta e-mailach często jest niepoprawny gramatycznie i ma proste błędy ortograficzne. W przypadku sfałszowanej strony z nosidełkiem, jeden z e-maili może brzmieć *"Chcemy zaprosić Państwa do zakup nosidełku marka X! Tani niemowlęcym przewoźnika marki X na sprzedaży, wysyłki free"*. Szanowane firmy sprawdzają wiadomości pod kątem poprawności przed wysłaniem ich do klientów. Kiedy dostrzeżesz słabą gramatykę lub pisownię, bądź podejrzliwy.
4. Przestępcy często używają nazwy marki towarów, których poszukujesz w adresie URL aby zachować pozory legalności. Ale również często zmieniają adresy URL swoich fałszywych stron internetowych, przez co trudniej jest je zlikwidować. W rezultacie, przestępcy często wykorzystują kilka różnych nazw domen i adresów e-mail w trakcie zakupów. Na przykład, w naszym przykładzie na stronie internetowej nosidełka dla dziecka, cyberprzestępcy mogą mieć jedną nazwę domeny dla strony internetowej, np. www.markaxnosidelkadzieciece.com, a inną nazwę domeny dla e-maili, które wysyłają sprzedaz@markaxnosidelka.com i trzecią nazwę domeny dla e-maili pomocniczych, takich jak wsparcie@dzieciecenosidelkamarkax.com. Różne nazwy domenowe są kolejną czerwoną lampką.
5. Legalne sklepy internetowe powinny zawsze korzystać z szyfrowania w procesie zakupu. Jeśli podczas transakcji szyfrowanie nie jest wykorzystywane to najlepiej nie korzystać z danej strony. Można łatwo sprawdzić czy strona używa szyfrowania, jeśli w adres strony zaczyna się od „https" a przeglądarka wyświetla symbol kłódki.
6. Wyszukaj nazwę lub adres URL sklepu internetowego, sprawdź czy ktoś inny nie opublikował żadnych skarg na daną stronę internetową, które wskazywałyby na oszustwo. Na przykład, jeśli kupujesz przedmioty z www.markaxnosidelka.com, wyszukaj najpierw ten URL i zobacz, czy inni nie skarżyli się na fałszywe towary.
7. Korzystaj z systemu PayPal lub innych mechanizmów, które nie ujawniają podstawowych informacji o karcie kredytowej kupującego. Na przykład, niektórzy dostawcy kart kredytowych



Jeśli sklep internetowy oferuje produkty po zbyt okazyjnej cenie, bądź podejrzliwy, ta strona może być fałszywa.

Fałszywe strony

oferują jednorazowe numery kart kredytowych tylko do wykonania pojedynczego zakupu. Innym rozwiązaniem jest korzystanie z kart upominkowych.

8. Rozważ używanie oprogramowania zabezpieczającego pomagającego ocenić poziom zaufania odwiedzanych witryn.
9. Jeśli obawiasz się, że nie można stwierdzić czy witryna jest wiarygodna czy nie, lepiej z niej nie korzystaj. Zamiast tego możesz kupić produkt ze znanej strony, której ufasz. Możesz nie uzyskać najlepszej oferty, ale najprawdopodobniej otrzymasz właściwy produkt z ewentualną możliwością zwrotu lub reklamacji.
10. Jeśli padniesz ofiarą oszustwa internetowego, zgłoś to na policję. Ponadto, należy skontaktować się z dostawcą karty kredytowej, aby zablokować swoją dotychczasową kartę kredytową, chroniąc się przed kolejnymi nadużyciami internetowymi i wnioskować o wydanie nowej.

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.

Policja – porady :

http://preview.tinyurl.com/dxqovnc
http://preview.tinyurl.com/cskx3ao

Oprogramowanie SiteAdvisor: https://www.siteadvisor.com/

Web of Trust (EN): http://www.mywot.com/

Słownik pojęć bezpieczeństwa (EN):
http://preview.tinyurl.com/6wkpae5

Porada dnia SANS Security (EN):
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