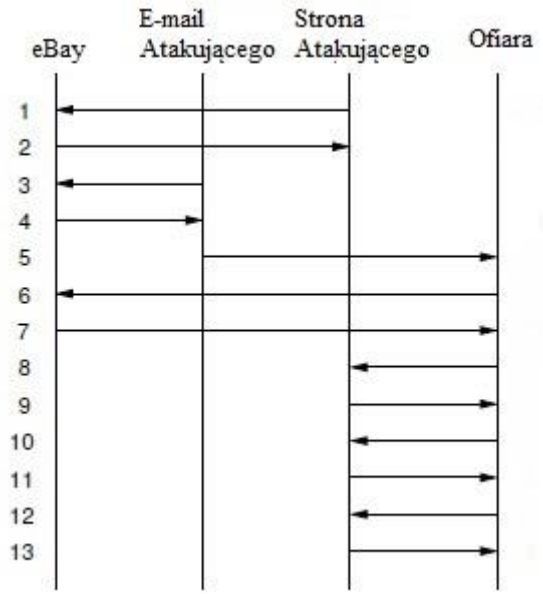
Anatomia oszustw internetowych: eBay

1. Wstęp

Przestępcy od dawna żerują na oczekiwaniach użytkowników, których można oszukać, robiąc rzeczy, których nie powinni. Fakt, że można to zrobić teraz online - gdzie oszukiwanie kogoś na całym świecie jest tak proste, jak oszukiwanie kogoś w mieście nie powinno nikogo dziwić. Poniżej rozważamy niedawny schemat skierowany do użytkowników serwisu eBay, aby zebrać ich nazwy użytkownika, hasła i numery kart kredytowych. System obejmował wysyłanie wiadomości e-mail do użytkowników serwisu eBay, informując ich, że wystąpił problem z kartą kredytową, i prosząc ich o odwiedzenie strony eBay, podając link. Wyglądał na to, że pochodził z serwisu eBay, ale e-mail pochodził z domeny użytkownik modemu kablowego w Kanadzie. Podążając za linkiem w e-mailu, użytkownik nie wejdzie na stronę eBay, ale oszust

2 Architektura schematu

W tym schemacie były kierowane dwie krytyczne informacje: dane uwierzytelniające (tj. Nazwa użytkownika i hasło) oraz informacje o karcie kredytowej użytkownika. Rysunek pokazuje najważniejsze etapy schematu od początku do końca.



1. Atakujący wysyła żądanie do serwisu eBay ze źródła
2. Serwer internetowy eBay podaje źródło
3. Atakujący pobiera dodatkowe źródło z serwisu eBay
4. Serwer internetowy eBay podaje źródło
5. " Proszę ponownie przesłać numer karty kredytowej”
6. Klient poczty żąda prawdziwych obrazów serwisu eBay
7. Witryna internetowa serwisu eBay dostarcza obrazy na żądanie
8. Ofiara klika link, myśląc, że to do serwisu eBay
9. Strona internetowa atakującego, wygląda jak eBay
10. Użytkownik wpisuje nazwę użytkownika i hasło
11. Atakujący akceptuje hasło, prosi o kartę kredytową

12. Użytkownik przesyła informacje o karcie kredytowej
13. Atakujący dziękuje ofierze za "aktualizację"

Każdy z trzynastu opisanych tutaj etapów wspiera jeden z trzech celów potrzebnych złodziejowi do osiągnięcia tego celu. Cele te polegają na utworzeniu fałszywej witryny eBay, skierowaniu użytkowników do fałszywej witryny, a następnie zarządzaniu fałszywą witryną, tak aby użytkownicy nigdy nie podejrzewali, co się stało.

2.1 Tworzenie fałszywej witryny eBay

Stworzenie fałszywej witryny jest oczywiście konieczne dla tego, aby użytkownicy byli skłonni do wprowadzenia poufnego uwierzytelniania i informacji finansowych.

Krok 1. Aby zbudować fałszywą stronę internetową, osoba atakująca wysyła żądania do serwisu eBay dotyczące znaczników HTML i obrazów potrzebnych do renderowania krytycznych stron serwisu eBay. Ponieważ sieć działa poprzez pobieranie klientów (takich jak Mozilla lub Internet Explorer) z serwera, a następnie wyświetlanie wyników użytkownikom, serwis eBay nie może powstrzymać użytkowników przed pobraniem ich źródła. W rzeczywistości łatwość powielania treści z jednej witryny sieci Web na drugą jest kluczową cechą sieci. Poinstruowanie strony eBay, aby wysłała kopię źródła, jest tak proste, że atakujący kieruje swoją przeglądarkę na stronę http://www.ebay.com/.

Krok 2. Witryna serwisu eBay odpowiada na żądanie klienta, przesyłając źródło HTML żądanej strony. Przechwytywanie tych informacji, zamiast używać ich wyłącznie do wyświetlania na monitorze atakującego, jest tak proste jak korzystanie z opcji menu "Zapisz jako" w przeglądarce. Osoba atakująca ma teraz kod źródłowy potrzebny do odtworzenia "wyglądu i sposobu działania" serwisu eBay na dowolnym wybranym serwerze. Z niewielkimi modyfikacjami kodu, wyniki formularzy mogą być wysyłane do nowych programów, które znajdują się na komputerze atakującego, zamiast legalnego oprogramowania do przetwarzania formularzy na prawdziwej stronie internetowej eBay.

Krok 3. Potrzebne mogą być dodatkowe dane, aby pobrać takie rzeczy jak obrazy ze strony internetowej serwisu eBay lub sprawdzić, jak faktycznie wygląda poczta e-mail z serwisu eBay.

Krok 4. Serwis eBay w naturalny sposób odpowie na prośby atakującego, które same w sobie są uzasadnione. Ważne jest, aby zrozumieć, że z perspektywy serwisu eBay żadna oszukańcza działalność (jeszcze) nie miała miejsca. Jednak w serwisie eBay osoba atakująca nie wyświetlała po prostu danych, które pobrał. Stworzył własną stronę, korzystając z HTML i obrazów z serwisu eBay, z modyfikacjami, aby zapewnić, że dane przesłane przez użytkownika zostaną zebrane przez stronę atakującego, a nie przesłane do legalnej strony internetowej serwisu eBay. Gdy strona jest już gotowa, zostaje umieszczona w Internecie, gdzie czeka na użytkowników, którzy przesyłają do niej swoje informacje.

2.2 Kierowanie użytkowników do nieuczciwej witryny

Krok 5. Użytkownicy serwisu eBay muszą teraz zostać przekonani, aby połączyć się z fałszywą witryną internetową. Można to zrobić, wysyłając wiadomość e-mail, stworzoną przy użyciu wyglądu i sposobu działania serwisu eBay, a nawet obrazu logo eBay. Tekst wiadomości jest dokładnie odtworzony tu :

„Niedawno podjęliśmy próbę autoryzacji płatności Twojej karty kredytowej, którą mamy dla Ciebie, ale została ona odrzucona. Ze względów bezpieczeństwa nasz system automatycznie usuwa dane karty kredytowej z konta, gdy wystąpi problem lub karta wygaśnie. Prześlij ponownie numer karty kredytowej i przekaż nam nowe i kompletne informacje. Aby ponownie przesłać informacje o karcie kredytowej za pośrednictwem naszego bezpiecznego serwera, kliknij następujący link:

http://cgi3.ebay.com/aw-cgi/eBayISAPI.dll? SignIn

Jest to najszybszy i najłatwiejszy sposób uzyskania informacji o karcie kredytowej. Korzystanie z bezpiecznego serwera zapewni, że karta kredytowa zostanie umieszczona na koncie w ciągu 24 godzin.

Z wyjątkiem obcinanej informacji o prawach autorskich, wydaje się, że niewiele wskazuje na to, że coś jest nie w porządku. Rzeczywiście, dla osób niebędących ekspertami, uzasadnienie usunięcia danych karty kredytowej może nawet wydawać się wiarygodne.

Krok 6. Klient poczty żąda prawdziwych obrazów serwisu eBay. Ponieważ klient poczty e-mail użytkownika wyświetla fałszywy komunikat, będzie zgodny z dyrektywą HTML w celu pobrania obrazu logo serwisu eBay ze strony internetowej serwisu eBay. Uważny użytkownik może nawet zwrócić uwagę na źródło logo serwisu eBay, które może potwierdzać wniosek, że wiadomość jest prawidłowa.

Krok 7. Serwis eBay zwraca prawdziwe obrazy do klienta w celu wyświetlenia w nieuczciwym e-mailu. W ten sposób kod HTML zostaje skradziony z serwisu eBay i zmodyfikowany, wysłany przez osobę atakującą, obrazy pochodzą bezpośrednio z serwisu eBay, a link nie połączy użytkownika z prawdziwym serwisem eBay, ale z oszukańczą stroną internetową.

2.3 Nieuczciwe działanie strony

Krok 8. Ofiara klika link, żądając źródła od serwera internetowego atakującego. Co ciekawe, link wyświetlany użytkownikowi nie jest rzeczywistym identyfikatorem URI łącza. Dokładne sprawdzenie źródła HTML e-maila pokazuje rzeczywisty link. Poniższy rysunek pokazuje źródło HTML akapitu i sam link.

<p> Prześlij ponownie kartę kredytową i przekaż nam nowe i kompletne informacje. Aby ponownie przesłać informacje o karcie kredytowej za pośrednictwem naszego bezpiecznego serwera kliknij poniższy link: </ p>

<p>

http://cgi3.ebay.com/aw-cgi/eBayISAPI.dll? SignIn

</ p>

Identyfikator URI jest bardzo starannie skonstruowany, aby wyglądać na zgodny z prawem, ale przekierowuje do fałszywej witryny sieci Web. Tutaj rozbijamy URI na jego części. http: // To jest

identyfikator protokołu i znaki separatora pokazujące zewnętrzny link. Protokół w tym przypadku to HTTP, niezaszyfrowany. (Typowy niezabezpieczony link do strony internetowej.)

cgi3.ebay.com: Jest to opcjonalna sekcja URI, zarezerwowana dla nazwy użytkownika logującego się, oraz token separatora (:) używany do odróżnienia go od następnej sekcji.

aw-cgieBayISAPI.dllSignInRegisterEnterInfo & amp; siteid = 0co partnerid = 2 @. Ta trudna sekcja jest oczywiście skonstruowana tak, aby wyglądała jak połączenie w głąb strony internetowej serwisu eBay, ale w rzeczywistości jest umieszczana w opcjonalnym elemencie hasła identyfikatora URI. Wskazówką jest znak @ na końcu, co oznacza, że kontynuowane są dane użytkownika i / lub hasło.

www.john33.net rms.com/ Prawdziwa nazwa strony, z którą klient się połączy

Krok 9. Serwer sieciowy Atakującego odpowiada na żądanie klienta, wysyłając fałszywy kod HTML przeglądarki użytkownika do wyświetlenia. W tym momencie użytkownik uważa, że podąża za legalnym linkiem do strony internetowej serwisu eBay. To, co widzi użytkownik, to nielegalna kopia witryny eBay utworzonej w krokach od pierwszego do czwartego.

Krok 10. Myśląc, że widzi prawdziwą stronę eBay, użytkownik wprowadza swoją nazwę użytkownika i hasło, wysyłając je do złodziei prowadzących oszukańczą stronę.

Krok 11. Nieuczciwa strona internetowa zapisuje nazwę użytkownika i hasło (pozwalając atakującemu zalogować się na konto użytkownika w prawdziwej witrynie eBay) i wyświetla stronę, która prosi użytkownika o ponowne wprowadzenie danych karty kredytowej. Zauważ, że niezależnie od tego, co użytkownik wprowadzi, fałszywa strona będzie zachowywać się tak, jakby nazwa użytkownika i hasło zostały wprowadzone poprawnie. To wzmacnia wiarę użytkownika, że strona jest poprawna: gdy użytkownik wprowadzi odpowiednie poświadczenia uwierzytelnienia, witryna akceptuje je, a tylko użytkownik i serwer serwisu eBay powinien wiedzieć, jakie są te poświadczenia.

Krok 12. Użytkownik wprowadza dane swojej karty kredytowej i trafia, przesyłając dane karty kredytowej, nie do serwisu eBay, ale do fałszywej witryny. Zwróć uwagę, że ponieważ strona nie korzysta z metod kryptograficznych do uwierzytelniania lub poufności sesji, karta kredytowa jest również narażona na działanie podsłuchujących.

Krok 13. Oszukańcza strona odsyła stronę z podziękowaniami, obiecując aktualizację konta eBay w ciągu dwudziestu czterech godzin. Pod koniec sesji użytkownik uważa, że zaktualizował swoje konto eBay, a osoba atakująca zebrała nazwa użytkownika, hasło i informacje o karcie kredytowej użytkowników serwisu eBay, którzy wpadli w oszustwo.

3 Zgłaszanie oszustwa

Dwaj wspólnicy (lub jedna osoba robiąca dwie rzeczy) pracowali nad uruchomieniem programu: nadawcy fałszywego e-maila i operatora oszukańczej strony internetowej.

3.1 Wyszukiwanie strony internetowej

Najpierw chcieliśmy zidentyfikować oszukańczą stronę internetową, ponieważ była ona nadal aktywna i zdolna do zbierania poufnych informacji. Jak zostało zidentyfikowane powyżej (w kroku 8), strona internetowa, do której skierowano klientów, to www.john33.netfirms.com. Teoretycznie zapisy WHOIS powinny pomóc nam skontaktować się z odpowiednimi osobami. Ponieważ jednak rejestracja nazw domen jest otwarta dla każdego, sprawcy oszustw często przesyłają fałszywe informacje kontaktowe do tych rejestrów. Ponadto, niektóre inne legalne domeny wypełniają zapisy WHOIS

fałszywymi danymi, aby uniknąć ataków spamerów. NetFirms jest dość dobrze znaną usługą hostingową, więc prawdopodobieństwo, że ich rekordy WHOIS były nieprawidłowe, nie było szczególnie wysokie. Ponieważ rejestracja numerów internetowych jest znacznie ściślej kontrolowana, rejestry WHOIS dotyczące numerów sieci są znacznie lepiej utrzymywane i rzadziej zawierają fałszywe informacje. Mimo że sprawdzanie rekordu WHOIS dla NetFirms prawdopodobnie dostarczyłoby nam informacje, których potrzebowaliśmy w tym przypadku, zdecydowaliśmy się dopasować adres IP do kontaktu sieciowego, ponieważ jest on bardziej ogólny i będzie działał nawet w przypadku ukrywania fałszywej witryny internetowej. w sieci, z którą trudno było skontaktować się z administratorami. Korzystanie z narzędzi wiersza polecenia, takich jak host lub nslookup2, ujawniłoby adres IP jak [209.171.43.26]. Korzystając z narzędzia wiersza polecenia whois, byliśmy w stanie zidentyfikować TELUS Communications jako administratora sieci. Zadzwoniliśmy do TELUSa i skontaktowano nas z pomocnymi ludźmi, którzy dali nam numer telefonu do kontaktu w sprawach bezpieczeństwa i nadużyć. Pewien dżentelmen, który odebrał telefon, poprosił nas o przesłanie informacji e-mailem wraz z przesłaną kopią wiadomości z linkiem do oszukańczej strony do osoby, która nadużyła kontaktu, i przesłanie mu również kopii. Następnie obiecał zadzwonić do grupy bezpieczeństwa, aby mieć pewność, że ktoś szybko się jej przyjrzy.

3.2 Śledzenie wiadomości e-mail

Naszym następnym krokiem było zidentyfikowanie źródła wiadomości e-mail. Czytając nagłówki wiadomości (pokazane na rysunku poniżej),

```
Return-path: <support@ebay.com>
Received: from ms-mta-02.socal.rr.com ([10.10.4.126]) by
 ms-mss-03.socal.rr.com (iPlanet Messaging Server 5.2 HotFix 1.12
 (built Feb 13 2003)) with ESMTP id
 <0HGH006M6R8EL2@ms-mss-03.socal.rr.com>; Sat, 14 Jun 2003 14:48:14
 -0700 (PDT)
Received: from lamx02.mgw.rr.com (lamx02.mgw.rr.com [66.75.160.13])
 by ms-mta-02.socal.rr.com (iPlanet Messaging Server 5.2 HotFix 1.12
 (built Feb 13 2003)) with ESMTP id
 <0HGH0054OQDXBO@ms-mta-02.socal.rr.com>; Sat, 14 Jun 2003 14:29:58
 -0700 (PDT)
Received: from ebay.com (u201n212.hfx.eastlink.ca [24.222.201.212])
 by lamx02.mgw.rr.com (8.12.8p1/8.12.8) with SMTP id h5ELm8Vb002000;
 Sat, 14 Jun 2003 17:48:09 -0400 (EDT)
Date: Sat, 14 Jun 2003 14:25:40 +1000
From: support@ebay.com
Subject: Billing Update Requested (URGENT)
To: mail@lamx02.mgw.rr.com
Message-id: <001400e8db46$dae47575$14814366@qijuhor.pgh>
MIME-version: 1.0
X-Mailer: QUALCOMM Windows Eudora Version 5.1
Content-type: multipart/mixed;
 boundary="----=_NextPart_000_00A0_62D10B0B.E5271C86"
Importance: Normal
X-Priority: 1
X-Virus-Scanned: Symantec AntiVirus Scan Engine
```

widzimy, że źródłem jest u201n212.hfx.eastlink.ca [24.222.201.212]. Telefon do Eastlink (w Halifax w Nowej Szkocji) informuje Eastlink o problemie. Pomocni ludzie pytają o kopię wiadomości, która ma zostać wysłana do ich kontaktu z ofiarami. Gdyby ta wiadomość pochodziła z zagranicy, znalezienie

rozsądnego punktu kontaktowego mogło być trudniejsze. W tym konkretnym przypadku wydaje się, że połączenie internetowe z szybkim modemem kablowym jest wysyłane do czyjegoś domu. Technicznie, telefon był niepotrzebny, ale umieściłem go, ponieważ chciałem poinformować ich, co prawdopodobnie było ciągłym incydentem międzynarodowego oszustwa i prawdopodobnie wiele innych rzeczy. To znacznie większy bałagan niż, powiedzmy, wysyłanie spamu i chciałem mieć pewność, że nie siedział w kolejce godzinami lub dniami, zanim ktoś zdawał sobie sprawę z tej sytuacji. Może to być rzecz, na którą administrator chciałby (po weryfikacji) odpowiedzieć natychmiast

3.3 Zgłaszanie do serwisu eBay

Wreszcie, podszywający się pod serwis eBay, najprawdopodobniej chciałby zostać poinformowany o incydencie, aby zachować bezpieczeństwo kont użytkowników, być może blokując wszystko, co może wydawać się być zaangażowane w oszukańczą działalność. Warto zauważyć, że użytkownik, który pierwotnie próbował fałszywej wiadomości e-mail, próbował znajść sposób zgłoszenia tego zdarzenia do serwisu eBay, ale nie był w stanie znaleźć miejsca do zgłoszenia tego rodzaju działalności. Ostatecznie zgłosiliśmy się do fraud@ebay.com i obserwowaliśmy, czy pojawiło się odstępstwo

4 Samoobrona

Istnieje lekcja dla użytkowników końcowych systemów, które mogą pomóc im uniknąć ofiar oszustw internetowych.

1. Nie daj się poganiać.

Oszustwo często zależy od tego, czy ktoś podejmie szybką decyzję, zanim zdąży rozważyć możliwe implikacje. Zastanów się nad oryginalnym tekstem fałszywego e-maila: „ To jest najszybszy sposób pozyskania do nas informacji. "Jeśli, jak stwierdzono w e-mailu, dane konta zostały usunięte, dane krytyczne byłyby bezpieczne, a w najgorszym przypadku scenariusz byłby taki, że użytkownik nie dostałby czegoś, za co wygrał licytację.

2. Wykonaj ustaloną procedurę

Jeśli wydaje się dziwne, że ktoś prosi o jakąś informację w dziwnej sekwencji wydarzeń lub w dziwnym czasie, strzeż się. Jeśli dokonałeś zakupu kartą kredytową, to albo zostanie ona zaakceptowana, albo odrzucona wkrótce - zwykle natychmiast. Jeśli dostawca ma mechanizm wprowadzania poufnych informacji, wykonaj go. Uważaj na zagrożenia, które mogą wynikać z pojawienia się głębokich powiązań.

3. Pytaj o rzeczy, których nie rozumiesz

Jeśli nie ma sensu, aby sprzedawca prosił o podanie numeru karty kredytowej, nie bój się go kwestionować. Jeśli wyjaśnienie brzmi nieśmiało, nie bój się go kwestionować. Pamiętaj, że kiedy robisz zakupy, jesteś szefem.

4. Sprawdź, czy mówisz do witryny, którą uważasz za swoją

Kiedy łączysz się z witryną, która obejmuje jakąkolwiek transakcję finansową, połączenie powinno być „zabezpieczone. "W przeglądarce pojawi się mała kłódka, która zostanie zablokowana, co oznacza, że połączenie jest szyfrowane, ale nie weryfikuje, z kim rozmawiasz, kliknięcie na zamek otworzy nowe okno dialogowe i wyświetli opcję przeglądania certyfikatu w użyciu. Spójrz na niego i upewnij się, że identyfikator URI jest dokładnie taki, jaki myślisz. W tym konkretnym przypadku, fałszywa strona nie podjęła żadnych poważniejszych prób podszywania się pod zabezpieczony serwer serwisu eBay, dlatego zamek nigdy się nie zamknął.

5. Wniosek

Ponieważ Internet staje się bardziej normalną częścią codziennego życia i handlu, będzie coraz częściej wykorzystywany jako środek, za pomocą którego złodzieje próbują popełnić swoje czyny. Użytkownicy muszą zdawać sobie sprawę z niebezpieczeństw, rozumieć granice tego, jak dobrze mogą być chronieni przez innych oraz potrzebę obrony. Przedsiębiorstwa, które prowadzą interesy w Internecie, w szczególności z konsumentami, muszą zrozumieć, że będą częstym celem tego rodzaju działalności. Firmy takie muszą mieć pewność, że zachęcają do dobrych praktyk bezpieczeństwa, tak aby napastnik nie mógł wysłać coś, co zwykle przyjmuje tego głupca, który robi coś złego. Skuteczne zabezpieczenia będą wymagać od nas starannej współpracy w celu zidentyfikowania i powstrzymania oszustw i innych przestępstw elektronicznych. Nie będzie to szybkie i nie będzie łatwe, ale można to zrobić, rozsądnie i skutecznie