CHRISTOPHER HADNAGY
MICHELE FINCHER

MROCZNE ODMĘTY PHISHINGU

Nie daj się złowić!

Helion

Tytuł oryginału: Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails

Tłumaczenie: Rafał Ociepa

ISBN: 978-83-283-2906-5

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/mrodph
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

ROZDZIAŁ

1

Wypływamy na odmęty phishingu

Lana: Nie uważasz, że to może być pułapka?
Archer: Co? Nie, nie uważam, że to pułapka! Chociaż… nigdy tak nie uważam… A często to wtedy jest pułapka.

— *Archer*, sezon 4, odcinek 13

Jako że spędzimy razem sporo czasu, mam wrażenie, że powinnam zacząć naszą relację od ujawnienia czegoś o sobie. Choć uważam się za relatywnie inteligentnego człowieka, popełniłam niezliczoną ilość głupich błędów. Wiele z nich zrodziło się z momentów, w których zawołałam: „Hej, popatrzcie na mnie!" lub gdy pomyślałam sobie: „Ciekawe, co się stanie, jeśli *tu wstaw niebezpieczną/głupią sytuację*". Ale najczęściej moje błędy brały się nie z próby przelicytowania kogoś innego czy z zastanawiania się nad możliwymi konsekwencjami, a właśnie z *braku zastanowienia*. Ten brak zastanowienia zazwyczaj prowadził do jednej i tej samej rzeczy: podjęcia impulsywnego działania. W jakimś poprzednim wcieleniu na pewno trafiali na mnie scamerzy, przestępcy i oszuści, bo taka cecha to jeden z kluczowych aspektów potrzebnych im do skutecznych ataków. Phishing w różnych postaciach stał się ważnym wektorem ataku dla takich ludzi, ponieważ jest dość prostym sposobem na dotarcie do ofiar i skłonienie ich do działania bez zastanowienia.

UWAGA **Zanim na dobre zaczniemy, chcę zwrócić uwagę na jeszcze jedną rzecz. Być może zauważyliście, że kiedy mówię o atakującym, używam zaimka „on" (właśnie, nawet „atakujący" jest rodzaju męskiego). To nie wynik moich uprzedzeń ani tego, że wszyscy atakujący są mężczyznami. Jest to po prostu łatwiejsze niż pisanie „on lub ona", dzięki czemu unikamy niepotrzebnych komplikacji na dodatkowym poziomie językowym. A zatem to „on" popełnia przestępstwa. Niemniej jednak atakujący może być dowolnej płci.**

ABC phishingu

Zacznijmy od podstawowych informacji. Co to jest *phishing*? Definiujemy to zjawisko jako wysyłanie e-maili, które wydają się pochodzić z wiarygodnych źródeł, a mają na celu wpłynięcie na odbiorcę lub pozyskanie danych osobowych. To przydługi sposób powiedzenia, że phishing to podstępne e-maile od złych ludzi. Łączy w sobie socjotechnikę i sztuczki technologiczne. Może obejmować załącznik do e-maila wczytujący do komputera malware (złośliwe oprogramowanie). Może to też być link do podstawionej strony internetowej. Strony takie mogą podstępem skłaniać nas do pobierania malware'u lub podawania poufnych danych. Istnieje również tzw. *spearphising*, czyli forma phishingu nacelowana na daną osobę. Atakujący zwykle poświęcają dużo czasu na poznanie celu i utworzenie wiadomości spersonalizowanych, związanych z sytuacją danej osoby. Dlatego tego typu wiadomości mogą być trudne do wykrycia, a jeszcze trudniej jest się przed nimi bronić.

Prawdopodobnie każda osoba na świecie posiadająca adres e-mail otrzymała wiadomość phishingową, a patrząc na dane statystyczne z raportów, można powiedzieć, że wiele tych osób kliknęło w link czy załącznik. Powiedzmy sobie pewną rzecz bardzo jasno. To, że ktoś tam klika, bynajmniej nie znaczy, że ten ktoś jest głupi. To błąd, który zdarza się, kiedy nie poświęcamy odpowiednio dużo czasu na przemyślenie tego, co robimy, lub kiedy nie mamy informacji potrzebnych do podjęcia właściwej decyzji (dla porównania: głupie było *to*, że przejechałam jednym ciągiem z Biloxi w stanie Missisipi do Tucson w Arizonie).

Można powiedzieć, że są pewne typowe cele i typowi atakujący. Motywacje phisherów na ogół są dość standardowe: pieniądze lub informacje (dzięki którym można zdobyć pieniądze). Jeśli, jak wiele innych osób, otrzymaliście kiedyś e-mail, w którym proszono o udzielenie pomocy zdetronizowanemu księciu chcącemu przenieść swój majątek, to byliście po prostu częścią swoistej loterii. Niewiele osób jest bajecznie bogatych. Ale jeśli phisherowi uda się nakłonić grupę przeciętnych osób do wspomożenia księcia przez przekazanie małej „opłaty za przelew", pomagającej przenieść jego fundusze (takie prośby często pojawiają się w tego typu przekrętach), to ziarnko do ziarnka i zbiera się niezła sumka. A z kolei jeśli e-mail od „mojego banku" spowoduje, że podam swoje poufne dane, to jeśli ktoś ukradnie moją tożsamość, może to mieć dla mnie poważne konsekwencje finansowe.

Do częstych celów należą również szeregowi pracownicy danej firmy. Co prawda każdy z osobna może nie dysponować większymi zasobami informacji, ale przez omyłkowe podanie swojego loginu i hasła może umożliwić atakującemu dostęp do firmowego intranetu. To może być jego ostatecznym celem, jeśli zyski z tego są wystarczająco duże, ale może to też być sposób na eskalację ataku na inne cele.

Oczywiście poza zwykłymi ludźmi są też cele o większej wartości, takie jak osoby na wyższych szczeblach piramid organizacyjnych dużych korporacji czy rządów. Im wyżej ktoś stoi w hierarchii danej organizacji, tym większe jest prawdopodobieństwo, że stanie się celem ataku spearphishingowego ze względu na stosunek czasu i pracy potrzebnych do przygotowania ataku względem jego skutków. Wtedy właśnie konsekwencje ataków stają się poważne dla całej gospodarki, a nie tylko dla pojedynczych osób.

Jeśli wyjdziemy poza przeciętnych przestępców oraz zwyczajowe pobudki zdobycia pieniędzy, to okazuje się, że mamy do czynienia z szeroko zakrojonymi atakami, osnutymi na poważnych motywach. Z jednej strony możemy mieć tu do czynienia z osobami zainteresowanymi skompromitowaniem jakiejś dużej organizacji z przyczyn osobistych lub politycznych. Na przykład Syryjska Armia Elektroniczna (ang. *Syrian Electronic Army*, SEA) miała związek z wieloma niedawnymi przypadkami e-maili phishingowych, które doprowadziły do włamań do różnych organizacji medialnych, w tym m.in. Associated Press[i], CNN[ii] i magazynu „Forbes”[iii]. Naturalnie pojawiły się konsekwencje finansowe: na przykład włamanie na konto AP na Twitterze spowodowało spadek indeksu Dow Jones o 143 punkty (rysunek 1.1). Takie coś to nie płotka, ale co z utratą reputacji ważnego źródła informacji? Moglibyśmy przez cały dzień dyskutować sobie, które z tych konsekwencji są w praktyce większe. Miało to też jednak pewien pozytywny skutek: zmusiło nas do zastanowienia się, czy rzeczywiście serwisy społecznościowe to najlepsze miejsce do śledzenia wiarygodnych, najświeższych wiadomości.

Rysunek 1.1. Zhakowany tweet AP o treści: „Pilne: dwie eksplozje w Białym Domu; Barack Obama ranny”

Schodząc jeszcze głębiej, trafimy na poziom cyberszpiegostwa na skalę przemysłową, a nawet międzypaństwową. Tu gra toczy się o tajemnice handlowe, gospodarkę światową i bezpieczeństwo narodowe. Konsekwencje tego są jasne nawet dla osób zupełnie niezorientowanych w temacie. Nagłaśniane jest teraz w mediach międzynarodowych podejrzenie, że chińscy hakerzy wojskowi włamali się do systemów pięciu ważnych firm amerykańskich i pewnego związku zawodowego[iv]. Firmy te zajmują się produkcją energii jądrowej, słonecznej i stali.

Po raz pierwszy w dziejach Stany Zjednoczone oskarżyły inne państwo o szpiegostwo internetowe[v]. A wszystko to zaczęło się od prostych e-maili.

Chcę przez to powiedzieć, że z phishingiem powinien być choć trochę obeznany każdy, a nie tylko pasjonaci bezpieczeństwa. Może i nie myślicie za często o cyberszpiegostwie, ale założę się, że sporo uwagi poświęcacie swojemu kontu bankowemu i zdolności kredytowej. Moja mama *nadal* nie wie, jak odsłuchać wiadomość w poczcie głosowej (serio!), ale zdecydowanie wie, że nie powinna otwierać e-maili od obcych osób. Wasze mamy też powinny się stosować do tej zasady.

A teraz, skoro wiecie już, „co", „kto" i „dlaczego", porozmawiajmy o „jak".

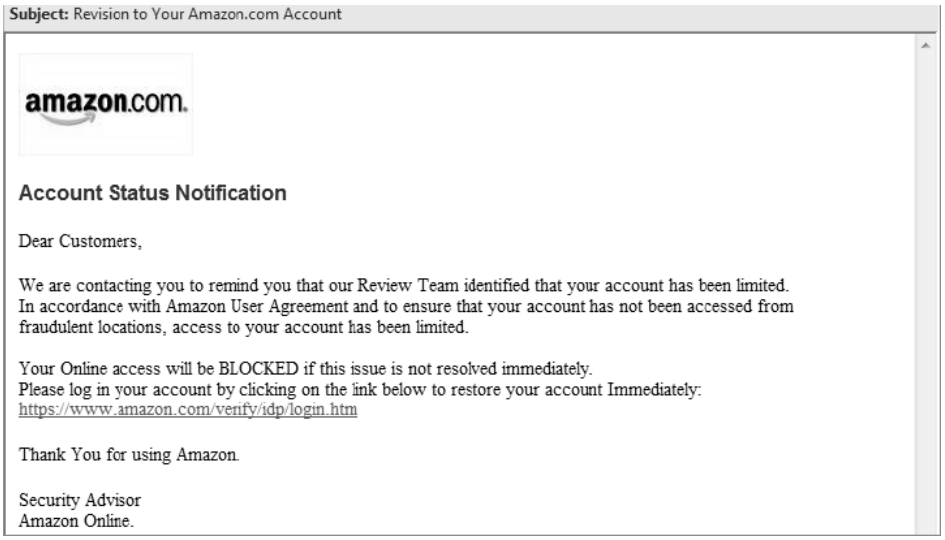
Jak idzie się na phishing

Rozpoznanie podejrzanego e-maila byłoby banalnie proste, gdyby jego nadawca nazywał się „Dawaj Kasę". Niestety, jeden z najprostszych sposobów naciągania ofiar polega na *spoofingu adresu e-mail*, czyli fałszowaniu informacji w polu *Od* wiadomości e-mail, przez co wiadomość wydaje się pochodzić od osoby znajomej lub z innego wiarygodnego źródła (np. od operatora usług telewizyjnych czy internetowych). W rozdziale 4. opisujemy pewne łatwe kroki, jakie można podjąć, żeby sprawdzić, czy nadawca jest tym, za kogo się podaje. W międzyczasie warto pamiętać, że uznawanie e-maila za bezpieczny tylko dlatego, że znamy nadawcę, nie zawsze jest dobrym pomysłem.

Kolejną techniką, za pomocą której scamerzy podnoszą swoją wiarygodność, jest stosowanie *klonowania stron*. Ta technika polega na kopiowaniu prawdziwych stron w celu skłonienia ofiary do tego, żeby podała swoje dane osobowe lub dane logowania. Za pomocą takich fałszywych stron można też bezpośrednio atakować komputer odbiorcy. Chris osobiście spotkał się na przykład z fałszywą stroną *Amazon.com*. To świetny przykład z kilku powodów. Po pierwsze, to powszechny przekręt, bo wiele osób, nie tylko w USA, ma konta na *Amazon.com*. Widzieliśmy stronę serwisu i wysyłane przez niego e-maile już tyle razy, że raczej nie przyglądamy im się bacznie. Po drugie, fałszywka jest na tyle dobra, że prawie złapał się na nią nawet ktoś, kto ma dużo doświadczenia z podstępnymi zabiegami scamerów.

Chris od lat stosuje phishing wobec naszych klientów (oczywiście za ich zgodą). Wysłał setki tysięcy takich e-maili i doskonale wie, jak są tworzone i dlaczego działają. W zeszłym roku otrzymał e-mail informujący go, że dostęp do jego konta na *Amazon.com* ma zostać zablokowany. Tak się złożyło, że e-mail ten zbiegł się w czasie z naszymi przygotowaniami do dorocznego turnieju na

konferencji DEF CON. Chris jest praktycznie zawsze zajęty, ale na miesiąc przed tą konferencją co roku zaczyna się w jego biurze coś, co można porównać tylko do dziewięciu kręgów piekielnych Dantego — naraz. Nie wiem, co sobie pomyślał czy powiedział na głos, kiedy dostał ten fałszywy e-mail z Amazona, ale pewnie domyślacie się, jaki jest ciąg dalszy tej anegdoty. Rysunek 1.2 pokazuje właśnie ten e-mail, który dostał.



Rysunek 1.2. Niesławny e-mail phishingowy, rzekomo z Amazon.com[1]

Jeśli przeczytacie tę wiadomość z uwagą, to zauważycie, że jej język nieco odbiega od zwykłego poziomu i zdarzają się tam pewne nieprawidłowości, na przykład zapisywanie niektórych słów wielką literą bez powodu. Takie cechy są typowe dla wiadomości phishingowych, bo dla wielu z ich twórców angielski

[1] Treść e-maila:

„Drodzy Klienci,

kontaktujemy się z Wami, aby przypomnieć Wam, że nasz Zespół Oceny stwierdził, że Wasze konto zostało ograniczone. Zgodnie z Regulaminem Użytkowników Amazona oraz aby zapewnić, że logowanie na Wasze konto nie nastąpiło z niewłaściwych lokalizacji, dostęp do Waszego konta został ograniczony. Wasz dostęp Internetowy zostanie ZABLOKOWANY, jeśli ten problem nie zostanie natychmiastowo rozwiązany. Prosimy, zalogujcie się na swoje konto, klikając w link poniżej, żeby przywrócić swoje konto Natychmiastowo.

https://www.amazon.com/verify/idp/login.htm

Dziękujemy za korzystanie z Amazona.

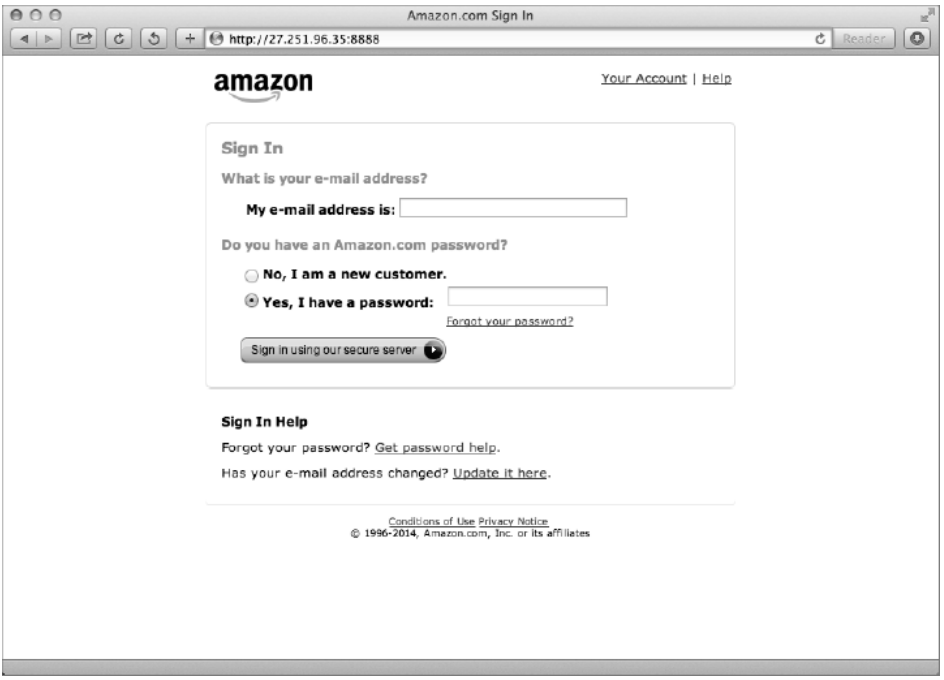
Konsultant ds. bezpieczeństwa

Amazon Online"

— *przyp. tłum.*

nie jest językiem ojczystym. Najważniejsze jest jednak to, że jakość tego e-maila jest na tyle wysoka, że nie zwróci uwagi rozgorączkowanego, śpieszącego się odbiorcy.

Chris kliknął na link i trafił na stronę wyglądającą ze wszech miar jak strona *Amazon.com*, co widać na rysunku 1.3. Nawet dokładne oględziny nie ujawniłyby, że to fałszywa strona, bo została sklonowana.



Rysunek 1.3. Fałszywa strona Amazon.com

W tym momencie zadziałały lata praktyki Chrisa. Spojrzał na URL strony (czyli jej adres) i zrozumiał, że nie jest prawdziwa. Gdyby podał tutaj swoje dane logowania, jak wymagała tego przesłana wiadomość, to ktoś zyskałby dostęp do jego konta na Amazonie, zawierającego dane osobowe Chrisa i dane jego karty kredytowej. Prawie się to udało, bo strona była dokładną kopią oryginału, a e-mail przyszedł do Chrisa w momencie, kiedy był akurat zajęty, zmęczony i rozkojarzony — co poważnie ogranicza ludzką zdolność do krytycznego myślenia (omówimy to bliżej w rozdziale 4.). Sednem sprawy jest fakt, że klonowanie stron to bardzo sugestywny sposób na przekonanie odbiorcy, że wiadomość phishingowa jest prawdziwa.

Kolejną sztuczką lubianą przez scamerów jest dzwonienie do ofiary po wysłaniu jej e-maila phishingowego. Taki zabieg znany jest jako *vishing* (z angielskiego *voice phishing*) czy *phishing telefoniczny*. Vishing ma wiele niecnych celów,

od zwiększenia wiarygodności e-maila po różne sposoby bezpośredniego wydobywania od rozmówcy poufnych informacji. Ta technika jeszcze bardziej unaocznia nam, jak bardzo powinniśmy chronić nasze dane osobowe. Dorastałam w czasach, kiedy na czekach dawanych pracownikom na koniec miesiąca regularnie drukowane były ich numery telefonów i numery Social Security[2], zaraz pod adresem pracownika, co praktycznie wołało: „Panie złodzieju, proszę ukraść moją tożsamość!". Wyobraźmy sobie, jak przekonująca byłaby sytuacja, w której otrzymujecie e-mail, a zaraz po nim telefon od „pracownika banku", który namawia Was do kliknięcia w link z e-maila, wejście na stronę i zaktualizowanie danych konta.

Niedawno taka sytuacja miała rzeczywiście miejsce w świecie korporacji. Zostało to ochrzczone mianem „frankofonii", bo wzięte na cel firmy działały przede wszystkim na terenie Francji[vi]. Atak był dobrze zaplanowany. Asystentka ds. administracyjnych w jednej z firm otrzymała e-mail w sprawie faktury, po którym nastąpił telefon od kogoś, kto przedstawił się jako jeden z wiceprezesów firmy. Rozmówca poprosił asystentkę o niezwłoczne zajęcie się tą fakturą. Asystentka kliknęła więc w e-mailu w link, który prowadził do pliku uruchamiającego na komputerze malware. To złośliwe oprogramowanie pozwoliło atakującym przejąć kontrolę nad komputerem i wykraść informacje. Przykład ten jest interesujący dlatego, że pojawia się w nim wiele czynników, takich jak wykorzystanie pozycji władzy i różnic płci, ale najważniejszym morałem z tej historii jest to, że każda rzecz wydaje się bardziej prawdopodobna, jeśli usłyszymy o niej z kilku źródeł.

Przykłady

Nie wiem jak Wy, ale ja i Chris najlepiej uczymy się na przykładach. W tej części książki wspomnimy o głośnych włamaniach, które zaczęły się od phishingu, a także o najczęściej stosowanych obecnie zabiegach phishingowych. Omówimy też, dlaczego tak często są one skuteczne.

Przede wszystkim musimy tutaj wspomnieć o Anti-Phishing Working Group (APWG — *www.apwg.org*). Moglibyśmy poświęcić całe strony peanom na cześć tych wspaniałych ludzi, ale najważniejsze jest to, że stanowią międzynarodowe konsorcjum pasjonatów bezpieczeństwa, którzy badają, definiują i przygotowują raporty na temat tego, jak funkcjonuje phishing na świecie.

[2] Numer identyfikacyjny powszechnie stosowany w USA w sposób podobny do numeru PESEL w Polsce, związany zarazem z dostępem do świadczeń społecznych — *przyp. tłum.*

Według raportu APWG z sierpnia 2014 roku statystyki phishingowe nadal zwalają z nóg. W drugim kwartale 2014 roku APWG otrzymało od konsumentów zgłoszenia o 128 378 unikatowych stronach phishingowych i 171 801 unikatowych e-mailach[vii]. Odkąd APWG zaczęło prowadzić te statystyki, tylko raz wykryto większą liczbę stron phishingowych w ciągu jednego kwartału. Na cel atakujący brali najczęściej (w 60% ataków) serwisy płatnościowe i sektor finansów, ale w tej kategorii pojawił się też nowy trend: coraz częściej phishing wymierzany był w płatności internetowe i użytkowników kryptowalut.

Skoro mamy już za sobą ogólny rzut na statystyki, czas przejść do konkretów.

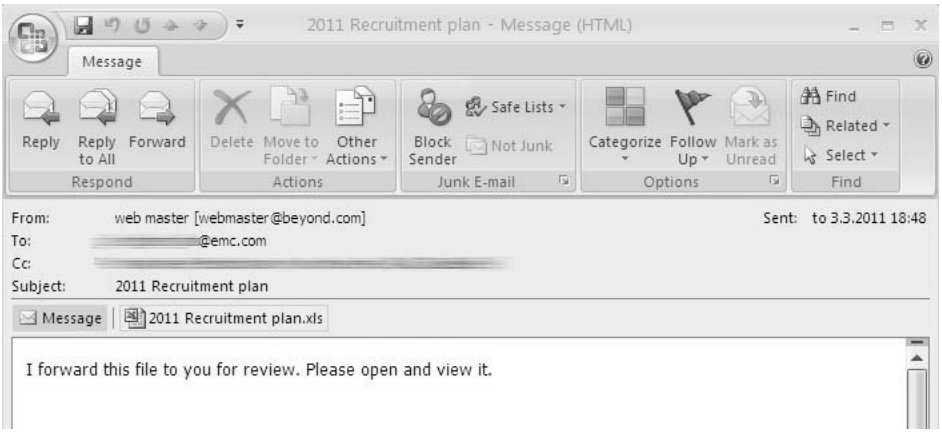
Głośne włamania

Chyba jednym z najgłośniejszych, jak dotąd, włamań jest przypadek Target Corporation. Atak ten dotknął niemal 110 milionów konsumentów — szacunki mówią o 40 milionach kart kredytowych i 70 milionach osób, których dane osobowe wykradziono; przy takich wynikach nawet część z Was mogła znaleźć się w tej grupie[viii]. Najciekawsze w tej sprawie jest jednak to, że wydaje się, iż atak nie był skierowany konkretnie przeciwko firmie Target[ix]. To świetny przykład eskalacji ataku. Target stał się ofiarą z przypadku, kiedy nadarzyła się okazja po rzeczywistym, zaplanowanym włamaniu. Pierwszą ofiarą był dostawca urządzeń klimatyzacyjnych dla sklepów Target, który miał dostęp do ich wewnętrznej sieci. Jakiś pracownik tej firmy klimatyzacyjnej dostał wiadomość phishingową i kliknął w link, który spowodował zainstalowanie na jego komputerze malware, które z kolei wykradło dane do logowania. Sieć firmy wykonawczej była powiązana z systemem sieciowym firmy Target na potrzeby wystawiania rachunków i przedstawiania zleceń. Nie znamy wszystkich szczegółów ataku, ale po tym, jak atakujący rozeznali się w systemach wykonawcy, znaleźli możliwość dostępu na serwery korporacyjne firmy Target i włamali się do systemu płatności.

Choć w tej chwili nie jest do końca jasne, jakie ostatecznie szkody poniosą konsumenci, to włamanie to kosztowało już ponad 200 milionów dolarów — to cena, jaką instytucje finansowe zapłaciły za ponowne wydanie kart kredytowych, których dane wykradziono; zarazem ta kwota nie uwzględnia kosztów potencjalnych spraw o oszustwo, za co nie ponoszą finansowej odpowiedzialności konsumenci. Podsumowując, była to dramatyczna i droga lekcja na temat zagrożeń związanych z phishingiem.

Inne ważne włamanie, o którym może nawet nie pamiętacie, dotknęło RSA. W tej chwili chyba każda wzmianka o RSA w jakiś sposób wiąże się z debatą o szyfrowaniu, która zaczęła się pod koniec 2013 roku w związku z działaniami National Security Agency. Sprawa ta była tak głośna, że niemal zupełnie przysłoniła włamanie, którego ofiarą padła ta firma w 2011 roku[x].

W odróżnieniu od wykorzystującego łut szczęścia ataku na Target włamanie do RSA było prawdopodobnie efektem dobrze przemyślanych działań skierowanych przeciwko pracownikom tej firmy. Wszystko wskazuje na to, że nastąpiło w wyniku przesłania złośliwego arkusza kalkulacyjnego Excel w załączniku e-maila wysłanego do niskich szczeblem pracowników RSA (rysunek 1.4).



Rysunek 1.4. Wiadomość phishingowa do RSA o treści: „Przesyłam ten plik do wglądu. Proszę otwórz i zapoznaj się z nim."

Filtry spamu RSA podobno przechwyciły te e-maile i skierowały je do folderów ze spamem na kontach użytkowników. Co ciekawe, użytkownicy przejęli kontrolę nad automatycznymi funkcjami, które zadziałały w tym przypadku tak, jak powinny. Przynajmniej jeden z odbiorców otworzył e-mail i jego załącznik. Dało to atakującym dostęp do intranetu firmy i umożliwiło im kradzież informacji związanych z niektórymi produktami RSA. Według dostępnych informacji w kwartale po włamaniu spółka matka RSA, EMC, wydała 66 milionów dolarów na działania związane z usuwaniem szkód, takie jak monitorowanie transakcji oraz wymiana tokenów szyfrowania.

Innym godnym uwagi włamaniem do firmy produktowej był atak na Coca-Colę w 2009 roku[xi]. Ta sprawa zaczęła się od bardzo spersonalizowanego ataku na kierownictwo Coca-Coli — o temacie „Save power is save money! (from CEO)", czyli „Oszczędzać prąd to oszczędzać pieniądze (od CEO)". Ten temat brzmi źle, ale trzeba wziąć pod uwagę dwie inne rzeczy: po pierwsze, e-mail jako nadawcę podawał wysoko postawioną osobę w dziale prawnym firmy. Po drugie, w czasie tego ataku Coca-Cola prowadziła kampanię promującą oszczędzanie energii (atakujący dobrze się przygotowali). Dyrektor będący celem ataku otworzył wiadomość i kliknął w link, który miał prowadzić do dalszych informacji na temat programu oszczędzania energii. Ale zamiast tego wczytał na komputer rozmaite złośliwe oprogramowanie, w tym keyloggera,

który przez tygodnie zapisywał wszystko, co użytkownik wpisał na klawiaturze zainfekowanego komputera. To włamanie umożliwiło chińskim hakerom dostęp do intranetu firmy i wykradanie danych aż do momentu, kiedy włamanie wykryto — kilka tygodni później.

Włamanie nastąpiło w lutym 2009 roku, a Coca-Cola dowiedziała się o nim dopiero w marcu, od FBI. Do tamtej pory wykradziono ogromne ilości poufnych danych. Atak miał miejsce zaledwie kilka dni przed podjętą przez Coca-Colę — i ostatecznie nieudaną — próbą kupienia za 2,4 miliarda dolarów jednego z chińskich producentów napojów. Gdyby transakcja ta doszła do skutku, byłaby największym, jak dotąd, nabyciem chińskiej firmy przez podmiot zagraniczny. Wyjaśnienia powodów, dla których nie doszło do transakcji, są sprzeczne, ale co najmniej jedna firma zajmująca się bezpieczeństwem twierdzi, że stało się to za sprawą wycieku istotnych informacji dotyczących strategii i polityki cenowej, przez co Coca-Cola nie była w stanie negocjować warunków zakupu.

Jak wspomnieliśmy wcześniej, włamanie na konto AP było imponujące już choćby ze względu na to, jak wielki wpływ na giełdę miał jeden tweet[xii]. Natomiast sposób, w jaki atakujący zyskali dostęp do konta, sprowadzał się do prostej wiadomości spearphishingowej wysłanej do wybranych pracowników AP z adresu wydającego się adresem jednego z ich współpracowników (rysunek 1.5).

Wysłano: wto 23/4/2013 12:12

Od: [Pracownik AP]

Temat: News

Cześć,

Przeczytaj proszę poniższy artykuł, to ważna sprawa:

http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/

[Inny pracownik AP]

Associated Press

San Diego

tel. kom. [usunięto]

Rysunek 1.5. Wiadomość spearphishingowa do Associated Press

Choć treść tego e-maila jest dość niekonkretna, trzeba pamiętać, że pochodził on ze „znanego" źródła i wydawał się kierować na rzeczywistą stronę w serwisie gazety „The Washington Post". Ofiary, które kliknęły w link z wiadomości,

były przekierowywane na podstawioną stronę zbierającą od nich dane logowania. Podejrzewa się, że podstawiona strona pozwalała na logowanie z użyciem konta na Twitterze, co doprowadziło do włamania na konto AP.

Jak wyraźnie widać, korporacje są równie podatne na phishing, jak zwykli ludzie, mimo swoich działów technicznych i polityk bezpieczeństwa. A co z phishingiem nastawionym na mniejsze cele? Kolejna część rozdziału opisuje kilka często spotykanych przykładów, na które mogliście się natknąć nawet sami.

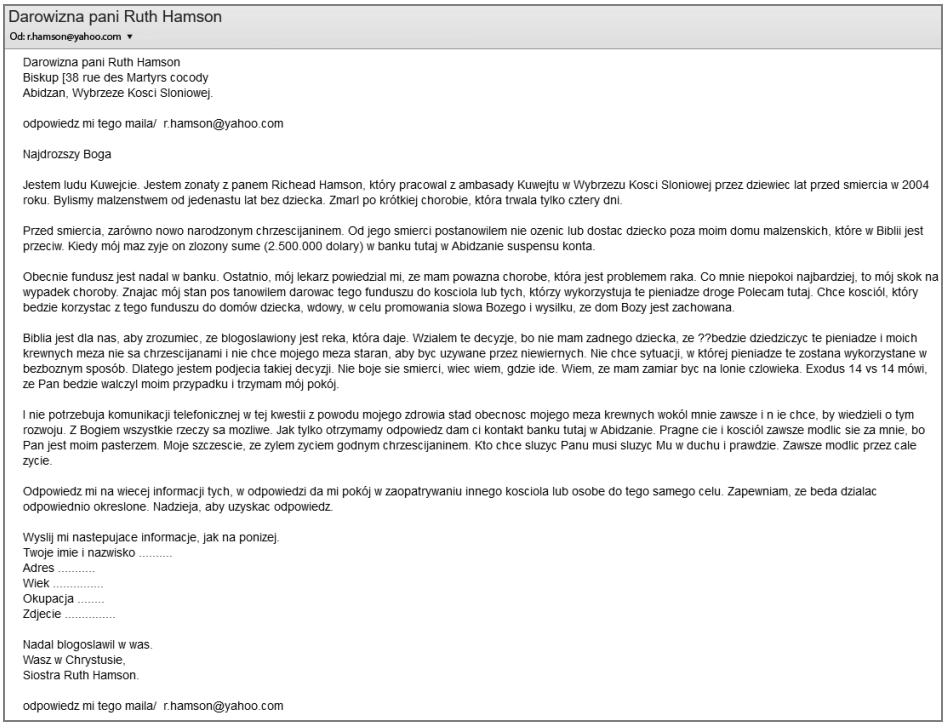
Fisze w środowisku naturalnym

Jakkolwiek na to spojrzeć, nie możemy omawiać na poważnie tematu phishingu, nie zaczynając od *przekrętu nigeryjskiego* (zwanego też *afrykańskim szwindlem* lub *przekrętem 419*). Ten typ oszustwa, znany też jako *wyłudzenie zaliczki*, stosowany jest podobno od ponad 200 lat (jak możecie sobie wyobrazić, cały proces prowadzony tradycyjną pocztą trwał znacznie dłużej, ale też miał miejsce). Najnowszą nazwę zawdzięcza złej sławie Nigerii, która rzekomo jest ojczyzną największej liczby przypadków takich wyłudzeń. Liczba 419 wzięła się stąd, że w kodeksie karnym Nigerii paragraf 419 odnosi się do wyłudzeń.

Niewątpliwie spotkaliście się z różnymi wariacjami na temat tego oszustwa. Dla przykładu: bogaty książę został zdetronizowany i potrzebuje pomocy, żeby przenieść swój ogromny majątek, albo umierający człowiek chce zrehabilitować się za to, że był niemiłym człowiekiem, i potrzebuje pomocy w przekazaniu pieniędzy na cele charytatywne. Niezależnie od tego, jaka jest przykrywka, są tu pewne stałe elementy:

- Chodzi o ogromne sumy.
- Nadawca powierza właśnie *Tobie*, osobie zupełnie dla siebie obcej, przekazanie funduszy, dysponowanie nimi lub ich przechowanie.
- Nadawca oferuje Ci jakąś kwotę za fatygę, ale najpierw musisz zrobić którąś z następujących rzeczy:
  - Podać dane swojego konta bankowego, żeby nadawca mógł wpłacić na nie pieniądze.
  - Pomóc mu, opłacając koszty przekazu, najczęściej ze względu na jakąś trudną sytuację polityczną lub osobistą.

Rysunek 1.6. pokazuje wzięty z życia e-mail, który niedawno krążył w internecie. Dobra, akurat ten e-mail przysłał ktoś z Wybrzeża Kości Słoniowej, ale rozumiecie zasadę.



Darowizna pani Ruth Hamson

Od: r.hamson@yahoo.com

Darowizna pani Ruth Hamson
Biskup [38 rue des Martyrs cocody
Abidzan, Wybrzeze Kosci Sloniowej.

odpowiedz mi tego maila/ r.hamson@yahoo.com

Najdrozszy Boga

Jestem ludu Kuwejcie. Jestem zonaty z panem Richead Hamson, który pracowal z ambasady Kuwejtu w Wybrzezu Kosci Sloniowej przez dziewiec lat przed smiercia w 2004 roku. Bylismy malzenstwem od jedenastu lat bez dziecka. Zmarl po krótkiej chorobie, która trwala tylko cztery dni.

Przed smiercia, zarówno nowo narodzonym chrzescijaninem. Od jego smierci postanowilem nie ozenic lub dostac dziecko poza moim domu malzenskich, które w Biblii jest przeciw. Kiedy mój maz zyje on zlozony sume (2.500.000 dolary) w banku tutaj w Abidzanie suspensu konta.

Obecnie fundusz jest nadal w banku. Ostatnio, mój lekarz powiedzial mi, ze mam powazna chorobe, która jest problemem raka. Co mnie niepokoi najbardziej, to mój skok na wypadek choroby. Znajac mój stan pos tanowilem darowac tego funduszu do kosciola lub tych, którzy wykorzystuja te pieniadze droge Polecam tutaj. Chce kosciól, który bedzie korzystac z tego funduszu do domów dziecka, wdowy, w celu promowania slowa Bozego i wysilku, ze dom Bozy jest zachowana.

Biblia jest dla nas, aby zrozumiec, ze blogoslawiony jest reka, która daje. Wzialem te decyzje, bo nie mam zadnego dziecka, ze ??bedzie dziedziczyc te pieniadze i moich krewnych meza nie sa chrzescijanami i nie chce mojego meza staran, aby byc uzywane przez niewiernych. Nie chce sytuacji, w której pieniadze te zostana wykorzystane w bezboznym sposób. Dlatego jestem podjecia takiej decyzji. Nie boje sie smierci, wiec wiem, gdzie ide. Wiem, ze mam zamiar byc na lonie czlowieka. Exodus 14 vs 14 mówi, ze Pan bedzie walczyl moim przypadku i trzymam mój pokój.

I nie potrzebuja komunikacji telefonicznej w tej kwestii z powodu mojego zdrowia stad obecnosc mojego meza krewnych wokól mnie zawsze i n ie chce, by wiedzieli o tym rozwoju. Z Bogiem wszystkie rzeczy sa mozliwe. Jak tylko otrzymamy odpowiedz dam ci kontakt banku tutaj w Abidzanie. Pragne cie i kosciól zawsze modlic sie za mnie, bo Pan jest moim pasterzem. Moje szczescie, ze zylem zyciem godnym chrzescijaninem. Kto chce sluzyc Panu musi sluzyc Mu w duchu i prawdzie. Zawsze modlic przez cale zycie.

Odpowiedz mi na wiecej informacji tych, w odpowiedzi da mi pokój w zaopatrywaniu innego kosciola lub osobe do tego samego celu. Zapewniam, ze beda dzialac odpowiednio okreslone. Nadzieja, aby uzyskac odpowiedz.

Wyslij mi nastepujace informacje, jak na ponizej.
Twoje imie i nazwisko .....
Adres .....
Wiek .....
Okupacja .....
Zdjecie .....

Nadal blogoslawil w was.
Wasz w Chrystusie,
Siostra Ruth Hamson.

odpowiedz mi tego maila/ r.hamson@yahoo.com

Rysunek 1.6. Nigeryjski phishing

Znakomita większość odbiorców dość łatwo pozna, że to przekręt, ale jakie konkretnie elementy pomogły mi określić, że to nie jest prawdziwa oferta od jakiejś rodziny ambasadora w Afryce?

- Nie znam nikogo mieszkającego w Abidżanie. Nie znam nikogo nazwiskiem Hamson.
- Nie ma też powodu, żeby Ruth Hamson miała znać mnie. Zresztą najwyraźniej wcale mnie nie zna, bo nie zwróciła się do mnie po imieniu. Taki złoty interes, a ona nawet *nie wie, jak się nazywam*?!?
- Cenię sobie spontaniczność, ale ta propozycja naprawdę wzięła się nie wiadomo skąd.
- Powierza mi (a nie bezpośrednio kościołowi, fundacji czy choćby kancelarii prawniczej) 2,5 miliona dolarów. Wyobraźcie sobie na chwilę tę kwotę. Chciałabym myśleć, że jestem osobą zasadniczo godną zaufania, ale wiecie, *ile krabów i ciasta* można zjeść za 2,5 miliona dolarów?

Nigeryjski szwindel to przekręt phishingowy dla początkujących. Jest dość oczywiste, że to próba wyłudzenia i dość łatwo go rozpoznać. Można się zatem spodziewać, że po 200 latach nie powinniśmy się już na niego łapać. Niemniej

nadal ma się dobrze i wciąż znajduje kolejne ofiary, pewnie nawet teraz, kiedy czytacie tę książkę. Dlaczego nadal jest skuteczny?

- **Chciwość:** To pierwszy, a zarazem najbardziej prozaiczny powód. Większość z nas nigdy nawet nie zobaczy kwot tak dużych, jak te proponowane w przekrętach 419, i to samo w sobie wystarczy, by wiele osób nie podeszło do sprawy na chłodno. W końcu zawsze jest szansa, że ta historyjka jest prawdziwa, nie? Właśnie nie. Ale jeśli ktoś potrafi wmówić sobie, że ma naprawdę szansę wygrać na loterii, to nie wymaga pewnie od niego wiele więcej wysiłku przekonanie samego siebie, że obca osoba rzeczywiście chce przekazać mu swój majątek.
- **Brak wiedzy:** Omawiamy ten czynnik znacznie dokładniej w dalszych częściach książki, ale na świecie jest niemała grupa ludzi (do których do niedawna zaliczała się moja mama), którzy nie wiedzą, że źli ludzie mogą spróbować ukraść ich tożsamość lub pieniądze za pomocą e-maili.
- **Zwykła naiwność:** Są ludzie, którzy całkowicie ufają innym na słowo. Byłoby cudownie, gdybyśmy żyli w świecie, w którym taka ufność nie wystawiałaby nas na niebezpieczeństwo.

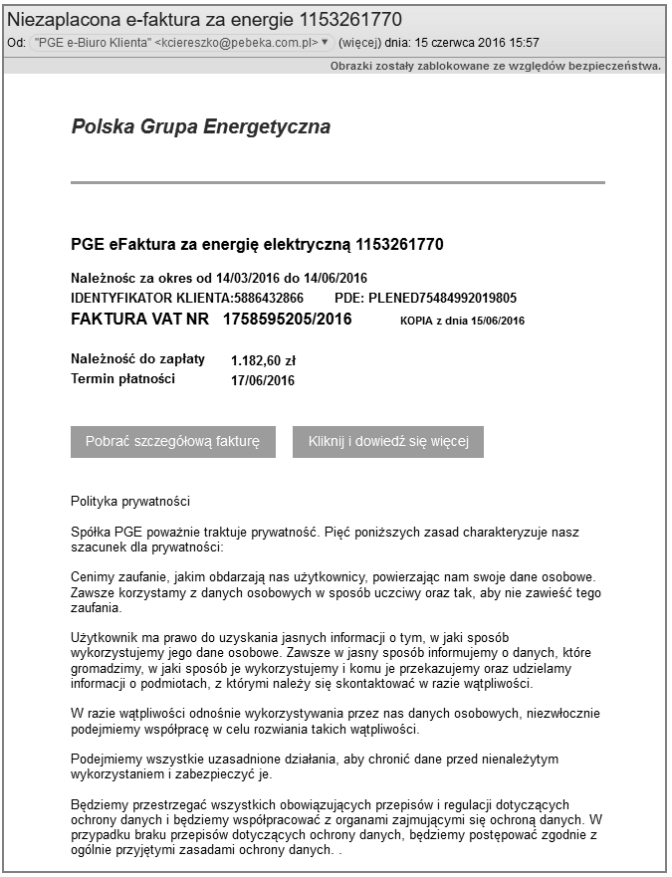
Poza przypadkami, kiedy ktoś proponuje nam ogromny majątek, pojawiają się też inne częste motywy chętnie wykorzystywane przez naciągaczy. Niektóre z nich są na tyle przekonujące, że zmuszają do zastanowienia.

Motywy finansowe

Motywy finansowe są jednym z większych „przebojów" wśród phisherów. Większość z nas coś robi z pieniędzmi, obraca nimi, płaci podatki, a zatem otrzymanie zawiadomienia z jakiejś instytucji finansowej najczęściej wystarczy, żebyśmy przynajmniej otworzyli taki e-mail. Wspomniany phishing ma nieskończenie wiele odmian, ale najczęściej wymaga od odbiorcy potwierdzenia tożsamości przez podanie szczegółowych danych konta w jakimś formularzu internetowym. Najpowszechniejsze phishe finansowe to między innymi:

- Nastąpiło wiele nieudanych prób zalogowania na twoje konto.
- Twój bank zmienił zabezpieczenia online.
- Zalegasz z płatnością za kredyt lub z podatkami.

Rysunki 1.7 – 1.10 pokazują przykłady phishy w środowisku naturalnym. Większość tych prób jest zdecydowanie lepsza i bardziej dopracowana niż przekręt nigeryjski, mogą na przykład zawierać logo i elementy graficzne, dzięki czemu wyglądają bardziej wiarygodnie. Powiedzmy, że jest to średnio zaawansowany poziom phishingu.



Niezaplacona e-faktura za energie 1153261770

Od: "PGE e-Biuro Klienta" <kciereszko@pebeka.com.pl> (więcej) dnia: 15 czerwca 2016 15:57

Obrazki zostały zablokowane ze względów bezpieczeństwa.

Polska Grupa Energetyczna

PGE eFaktura za energię elektryczną 1153261770

Należnośc za okres od 14/03/2016 do 14/06/2016
IDENTYFIKATOR KLIENTA:5886432866 PDE: PLENED75484992019805
FAKTURA VAT NR 1758595205/2016 **KOPIA z dnia 15/06/2016**

Należność do zapłaty **1.182,60 zł**
Termin płatności **17/06/2016**

Pobrać szczegółową fakturę | Kliknij i dowiedź się więcej

Polityka prywatności

Spółka PGE poważnie traktuje prywatność. Pięć poniższych zasad charakteryzuje nasz szacunek dla prywatności:

Cenimy zaufanie, jakim obdarzają nas użytkownicy, powierzając nam swoje dane osobowe. Zawsze korzystamy z danych osobowych w sposób uczciwy oraz tak, aby nie zawieść tego zaufania.

Użytkownik ma prawo do uzyskania jasnych informacji o tym, w jaki sposób wykorzystujemy jego dane osobowe. Zawsze w jasny sposób informujemy o danych, które gromadzimy, w jaki sposób je wykorzystujemy i komu je przekazujemy oraz udzielamy informacji o podmiotach, z którymi należy się skontaktować w razie wątpliwości.

W razie wątpliwości odnośnie wykorzystywania przez nas danych osobowych, niezwłocznie podejmiemy współpracę w celu rozwiania takich wątpliwości.

Podejmiemy wszystkie uzasadnione działania, aby chronić dane przed nienależytym wykorzystaniem i zabezpieczyć je.

Będziemy przestrzegać wszystkich obowiązujących przepisów i regulacji dotyczących ochrony danych i będziemy współpracować z organami zajmującymi się ochroną danych. W przypadku braku przepisów dotyczących ochrony danych, będziemy postępować zgodnie z ogólnie przyjętymi zasadami ochrony danych. .

Rysunek 1.7. Przykład wiadomości phishingowej „PGE”

Blokada rachunku BZWBK

Od: "Pomoc BZ WBK" <vika@sunnymusic.pl> (więcej) dnia: 30 września 2016 18:34

Więcej

Data:30.09.2016

Bezzwłoczna weryfikacja rachunku Bank Zachodni WBK!

W dbałość o bezpieczeństwo naszych użytkowników zablokowaliśmy rachunek w systemie BZWBK24 internet, przyczyną jest nieautoryzowany dostęp do konta.
W celu zdobycia informacji, oraz odblokowania dostępu, prosimy o uwierzytelnienie właściciela konta, wchodząc na:

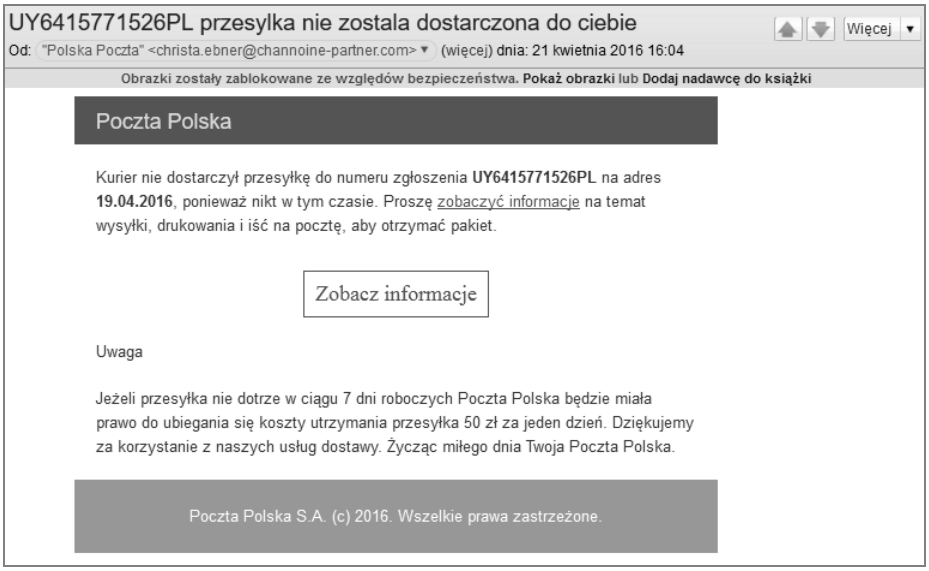
Uwierzytelnienie

Życzliwie pozdrawiamy,
Wsparcie techniczne Bank Zachodni WBK S.A.

W przypadku wątpliwości prosimy o kontakt z Infolinia 1 9999

Ten e-mail został wygenerowany automatycznie. Prosimy na niego nie odpowiadać. Bank Zachodni WBK S. A. z siedzibą z siedzibą w Warszawie przy ul. Puławskiej 15, 02-515 Warszawa, zarejestrowana w Sądzie Rejonowym dla m.st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000026438; NIP: 525-000-77-38 REGON: 016298263; kapitał zakładowy (kapitał wpłacony) 1 250 000 000 zł.

Rysunek 1.8. Przykład wiadomości phishingowej banku „BZWBK”


UY6415771526PL przesylka nie zostala dostarczona do ciebie

Od: "Polska Poczta" <christa.ebner@channoine-partner.com> (więcej) dnia: 21 kwietnia 2016 16:04

Obrazki zostały zablokowane ze względów bezpieczeństwa. **Pokaż obrazki** lub **Dodaj nadawcę do książki**

Poczta Polska

Kurier nie dostarczył przesyłkę do numeru zgłoszenia **UY6415771526PL** na adres **19.04.2016**, ponieważ nikt w tym czasie. Proszę zobaczyć informacje na temat wysyłki, drukowania i iść na pocztę, aby otrzymać pakiet.

Zobacz informacje

Uwaga

Jeżeli przesyłka nie dotrze w ciągu 7 dni roboczych Poczta Polska będzie miała prawo do ubiegania się koszty utrzymania przesyłka 50 zł za jeden dzień. Dziękujemy za korzystanie z naszych usług dostawy. Życząc miłego dnia Twoja Poczta Polska.

Poczta Polska S.A. (c) 2016. Wszelkie prawa zastrzeżone.

Rysunek 1.9. Przykład wiadomości phishingowej „Poczty Polskiej"


Od: Allegro <powiadomienia@allegro.pl>
Temat: Allegro Konto Zawieszone
Data: 28 sierpnia 2016 16:11
Do: [redacted]

allegro

Witaj!
Musisz potwierdzić swoje konto.

Ab y potwierdzić rejestrację, że jesteś właścicielem tego konta.
Kliknij na poniższy link i wpisać swoje dane konta
Zaloguj się Allegro dane konta

Przydatne informacje

- Potwierdzenie rejestracji oznacza akcep tację Regulaminu Allegro. pl
- Jeżeli masz kłopoty z dokończeniem rejestracji, zajrzyj do Pomocy

Poz drawiamy,
Zesp& #322; Allegro

Rysunek 1.10. Przykład wiadomości phishingowej „Allegro"

Mimo że te próby są bardziej wysublimowane, to nadal pojawiają się w nich szczegóły, które pozwalają nam rozpoznać oszustwo:

- Zwroty do adresata są na ogół nieprecyzyjne: przecież bank powinien wiedzieć, jak nazywa się jego własny klient. „Witaj!" się tu nie liczy.

- Ortografia, gramatyka i użycie wielkich liter są na wyższym poziomie, ale czegoś im nadal brakuje.
- Linki do formularzy internetowych pokazują, że adres URL wcale nie należy do rzekomego nadawcy.
- Stosowanie ponaglających zwrotów („Jeżeli przesyłka nie dotrze w ciągu 7 dni roboczych Poczta Polska będzie miała prawo do ubiegania się koszty utrzymania przesyłka 50 zł za jeden dzień").

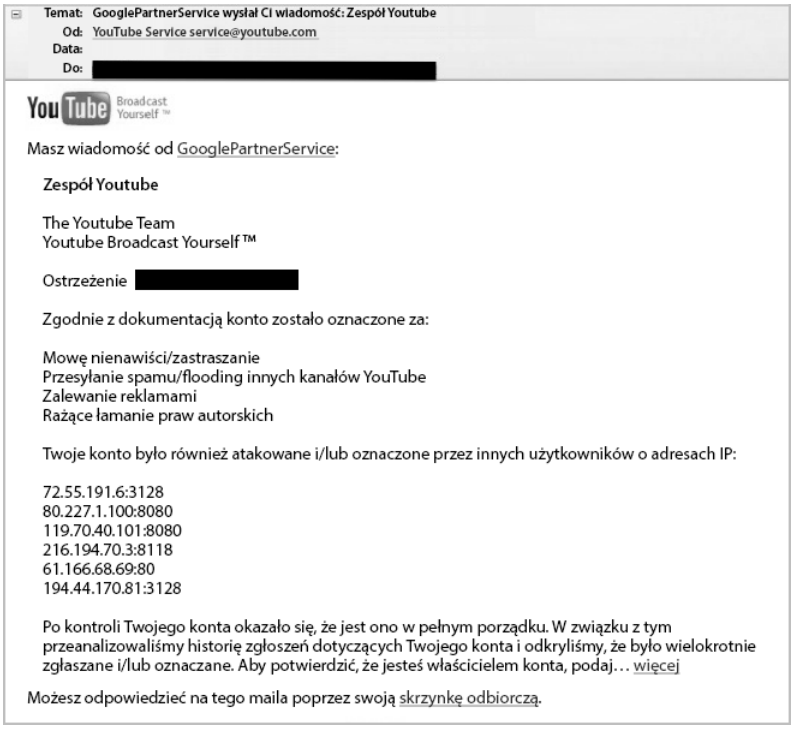
Te e-maile wymuszają na odbiorcy działanie przede wszystkim przez wprowadzenie pewnego strachu czy niepokoju. Wszystko, co stawia pod znakiem zapytania możliwość dostępu do naszych pieniędzy, jest dla nas straszne. Większość przykładów, które przytaczamy w tej części, ma sporo wspólnych cech, zwłaszcza jeśli chodzi o metody, którymi skłaniają odbiorców do działania:

- **Przyjęcie pozycji władzy:** To jedna z zasad wpływu omówionych szerzej w rozdziale 3.; w skrócie można powiedzieć, że ludzie są stworzeniami społecznymi i wszyscy reagują na jakieś formy autorytetu.
- **Ograniczenia czasowe:** O nie! Piszą, że stracisz dostęp do konta w ciągu 48 godzin! Takie sformułowania powodują naprawdę duży lęk. Nasz wrodzony instynkt przetrwania sprawia, że wszystko, co stanowi zagrożenie dla możliwości dostępu do jakichś zasobów, odbieramy jako istotne niebezpieczeństwo.
- **Możliwość włamania:** Naprawdę przeraża nas możliwość, że nasz bank odkrył niepowołane próby wejścia na nasze konto. Jest tylko jedna osoba, która może pławić się w moim złocie: ja. No i może jeszcze Smaug.

Zagrożenia w mediach społecznościowych

Innym motywem często pojawiającym się w phishingu jest korzystanie z mediów społecznościowych. W końcu są one właśnie po to, żebyśmy uczestniczyli w społeczności. A zatem e-mail od któregoś z tych serwisów z prośbą, by dodać kogoś jako kontakt lub obejrzeć jakiś link, wydaje się całkowicie uzasadniony. Na ogół tego typu wiadomości mają zbliżony poziom do phishy dotyczących usług finansowych i można je rozpoznać po podobnych szczegółach. Niemniej, moim zdaniem, na niektóre z nich łatwiej się nabrać, bo jeśli należymy do jakiegoś serwisu społecznościowego, to często dostajemy jakieś zaproszenia — a co ważniejsze, liczymy na to, że będziemy je dostawać. Dodatkowo takie wiadomości, w odróżnieniu od niespodziewanego e-maila z banku, mogą nie budzić podejrzeń, więc odbiorca nie jest aż tak ostrożny.

Podobnie jak phishing związany z usługami finansowymi, tak i tego typu e-maile często odwołują się do strachu przed czymś w celu nakłonienia do określonych działań (rysunek 1.11).


Temat: GooglePartnerService wysłał Ci wiadomość: Zespół Youtube
Od: YouTube Service service@youtube.com
Data:
Do: [redacted]

YouTube Broadcast Yourself™

Masz wiadomość od GooglePartnerService:

Zespół Youtube

The Youtube Team
Youtube Broadcast Yourself™

Ostrzeżenie [redacted]

Zgodnie z dokumentacją konto zostało oznaczone za:

Mowę nienawiści/zastraszanie
Przesyłanie spamu/flooding innych kanałów YouTube
Zalewanie reklamami
Rażące łamanie praw autorskich

Twoje konto było również atakowane i/lub oznaczone przez innych użytkowników o adresach IP:

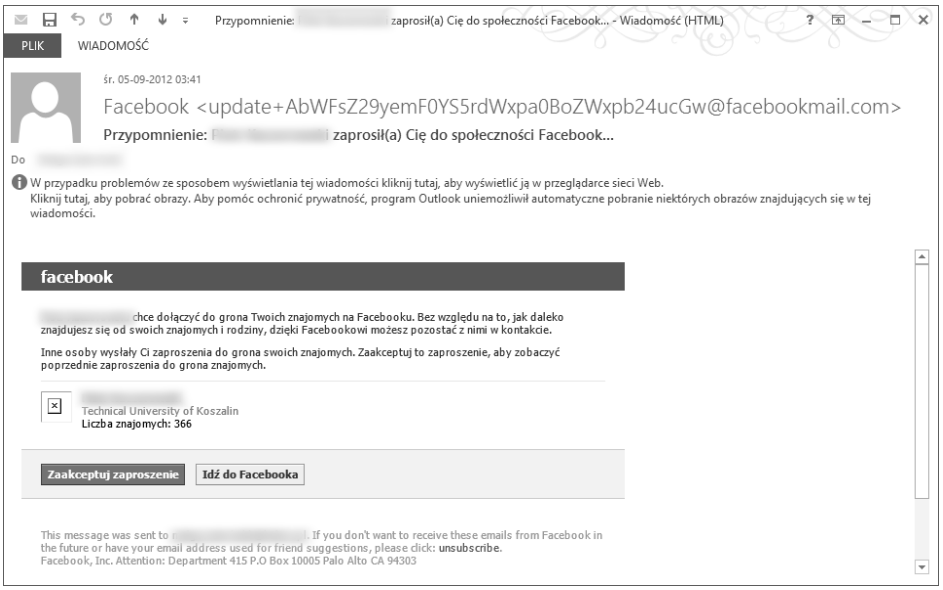
72.55.191.6:3128
80.227.1.100:8080
119.70.40.101:8080
216.194.70.3:8118
61.166.68.69:80
194.44.170.81:3128

Po kontroli Twojego konta okazało się, że jest ono w pełnym porządku. W związku z tym przeanalizowaliśmy historię zgłoszeń dotyczących Twojego konta i odkryliśmy, że było wielokrotnie zgłaszane i/lub oznaczane. Aby potwierdzić, że jesteś właścicielem konta, podaj… więcej

Możesz odpowiedzieć na tego maila poprzez swoją skrzynkę odbiorczą.

Rysunek 1.11. Przykład wiadomości phishingowej „YouTube"

Strach motywuje bardzo mocno, ale utrata dostępu do konta w jakimś serwisie społecznościowym jest raczej niedogodnością niż poważną sprawą (przynajmniej dla *większości* z nas). Niemniej jednak pretekst, jaki dają media społecznościowe, pozwala też atakującym na stosowanie metod innych niż budzenie strachu, żeby skłonić odbiorcę do reakcji. Ataki te zasadzają się też na poczuciu obowiązku. Serwisy społecznościowe rozwijają się dzięki tworzonym w nich relacjom. Uczestnictwo w nich jest frajdą, bo dzięki temu możemy należeć do jakiejś grupy. Źródłem ataków phishingowych są te same motywacje. Wiele osób klika w przesłany link dlatego, że nie chce zrobić przykrości innej osobie (czyli odrzucić zaproszenie do grona znajomych) albo nie chce robić złego wrażenia i nie odpowiadać — nawet na zaproszenia od nieznanych osób (rysunki 1.12 i 1.13).



Rysunek 1.12. Przykład wiadomości phishingowej „Facebooka”

Rysunek 1.13. Przykład wiadomości phishingowej „LinkedIn”

UWAGA **Kiedy byłam dzieckiem, utrzymywałam swego rodzaju znajomość wirtualną. Miałam przyjaciółkę korespondencyjną. Dokładnie pamiętam, że nie czułam wtedy takiej siły i bezpośredniości tej przyjaźni, jaka dla wielu osób zdaje się cechować obecne wirtualne relacje. Zjawisko mediów społecznościowych jest dla mnie wciąż bardzo interesujące. Dzięki niemu ludzie mają do dyspozycji szybki i niewymagający wysiłku sposób na budowanie więzi dalece wykraczających poza ich normalne kręgi znajomych i współpracowników. Niestety z tych samych**

powodów osoby zainteresowane poznawaniem nowych ludzi i rozwijaniem swojej sieci znajomych są szczególnie podatne na phishing należący do tej kategorii. W tym przypadku dobrze jest udawać, że żyje się w jaskini. Na jednym z moich kont czekają na mnie od dawna 34 prawdziwe zaproszenia. Pewnie powinnam zacząć się tym bardziej przejmować, bo jeszcze ludzie sobie pomyślą, że nie chcę mieć żadnych przyjaciół.

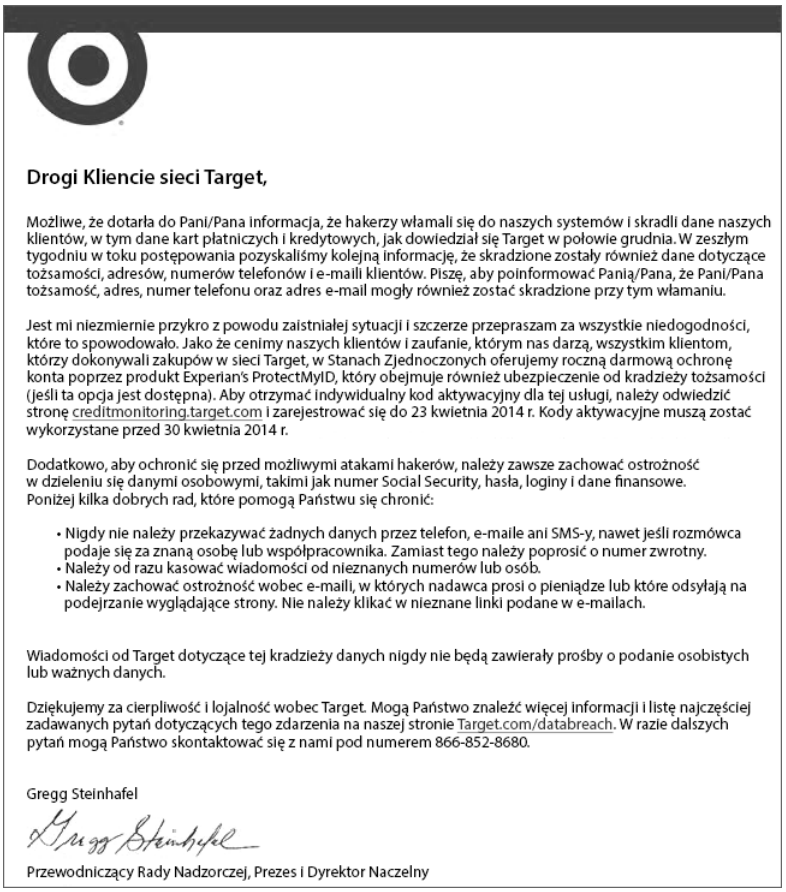
Przekręty związane z głośnymi wydarzeniami

Ostatnia kategoria phishy w środowisku naturalnym jest wyjątkowo obrzydliwa. Należą do niej e-maile, które oszuści wysyłają bezpośrednio po jakimś nagłośnionym wydarzeniu: katastrofie naturalnej, rozbiciu się samolotu, ataku terrorystycznym — nadaje się do tego wszystko, czemu media poświęcają bardzo dużo uwagi, a co w związku z tym bardzo zajmuje opinię publiczną. Oszuści tacy żerują na naszych naturalnych reakcjach, czyli obawach, ciekawości i współczuciu. Przykłady te w większości są na poziomie dość zaawansowanym, jeśli przyjrzeć się im krytycznie. Nadal jednak zawierają pewne oznaki pozwalające stwierdzić, że są nieprawdziwe. Niemniej niektóre osoby są podatne na tego typu ataki choćby ze względu na własną reakcję emocjonalną na dane wydarzenie. A jaki jest najlepszy sposób na to, żeby ofiara nie myślała trzeźwo? Wzbudzić w niej silne emocje. Rozdział 2. opisuje ciekawe zjawisko zwane „porwaniem przez ciało migdałowate".

Nie minęła doba od czasu, gdy Target podał do wiadomości publicznej informacje o włamaniu, a scamerzy zaczęli już wykorzystywać obawy, jakie ludzie mieli w związku ze stanem swoich danych osobowych i kredytowych. Zidentyfikowano wtedy co najmniej 12 różnych oszustw, z których jedno obejmowało e-mail identyczny z wiadomością, którą Target wysyłał klientom, by wyjaśnić sytuację i zaproponować darmowy monitoring karty kredytowej[xiii]. Jak pokazujemy na rysunku 1.14, ten przekręt trudno było wyłapać nawet specjalistom. Ponieważ sama treść była dokładną kopią wiadomości przesłanej przez Target, trzeba było sprawdzić adres nadawcy lub linki. Kolejnym szczegółem, który utrudniał właściwą decyzję, było to, że prawdziwy e-mail wysłany przez Target pochodził z adresu *TargetNews@target.bfi0.com*, który dla każdego wyglądał podejrzanie. Zapanowały strach i niepewność, a oszuści wykorzystali sytuację.

Naturalnie najpodatniejsze na ten atak były osoby posiadające konta Target. Target jest jednak ogromną siecią sklepów, przez co właściwie każdemu nieco skoczyło ciśnienie na wieść o włamaniu. Trudno znaleźć w USA (i nie tylko) kogoś, kto ani razu nie kupił czegoś w sklepie tej sieci.

Chcemy z Chrisem przede wszystkim edukować, a nie osądzać, ale warianty oszustw stosowane bezpośrednio po katastrofach są szczególnie godne potępienia. Ataki te zamiast prób zastraszenia odbiorcy (co samo w sobie jest ohydną rzeczą)



Drogi Kliencie sieci Target,

Możliwe, że dotarła do Pani/Pana informacja, że hakerzy włamali się do naszych systemów i skradli dane naszych klientów, w tym dane kart płatniczych i kredytowych, jak dowiedział się Target w połowie grudnia. W zeszłym tygodniu w toku postępowania pozyskaliśmy kolejną informację, że skradzione zostały również dane dotyczące tożsamości, adresów, numerów telefonów i e-maili klientów. Piszę, aby poinformować Panią/Pana, że Pani/Pana tożsamość, adres, numer telefonu oraz adres e-mail mogły również zostać skradzione przy tym włamaniu.

Jest mi niezmiernie przykro z powodu zaistniałej sytuacji i szczerze przepraszam za wszystkie niedogodności, które to spowodowało. Jako że cenimy naszych klientów i zaufanie, którym nas darzą, wszystkim klientom, którzy dokonywali zakupów w sieci Target, w Stanach Zjednoczonych oferujemy roczną darmową ochronę konta poprzez produkt Experian's ProtectMyID, który obejmuje również ubezpieczenie od kradzieży tożsamości (jeśli ta opcja jest dostępna). Aby otrzymać indywidualny kod aktywacyjny dla tej usługi, należy odwiedzić stronę creditmonitoring.target.com i zarejestrować się do 23 kwietnia 2014 r. Kody aktywacyjne muszą zostać wykorzystane przed 30 kwietnia 2014 r.

Dodatkowo, aby ochronić się przed możliwymi atakami hakerów, należy zawsze zachować ostrożność w dzieleniu się danymi osobowymi, takimi jak numer Social Security, hasła, loginy i dane finansowe. Poniżej kilka dobrych rad, które pomogą Państwu się chronić:

- Nigdy nie należy przekazywać żadnych danych przez telefon, e-maile ani SMS-y, nawet jeśli rozmówca podaje się za znaną osobę lub współpracownika. Zamiast tego należy poprosić o numer zwrotny.
- Należy od razu kasować wiadomości od nieznanych numerów lub osób.
- Należy zachować ostrożność wobec e-maili, w których nadawca prosi o pieniądze lub które odsyłają na podejrzanie wyglądające strony. Nie należy klikać w nieznane linki podane w e-mailach.

Wiadomości od Target dotyczące tej kradzieży danych nigdy nie będą zawierały prośby o podanie osobistych lub ważnych danych.

Dziękujemy za cierpliwość i lojalność wobec Target. Mogą Państwo znaleźć więcej informacji i listę najczęściej zadawanych pytań dotyczących tego zdarzenia na naszej stronie Target.com/databreach. W razie dalszych pytań mogą Państwo skontaktować się z nami pod numerem 866-852-8680.

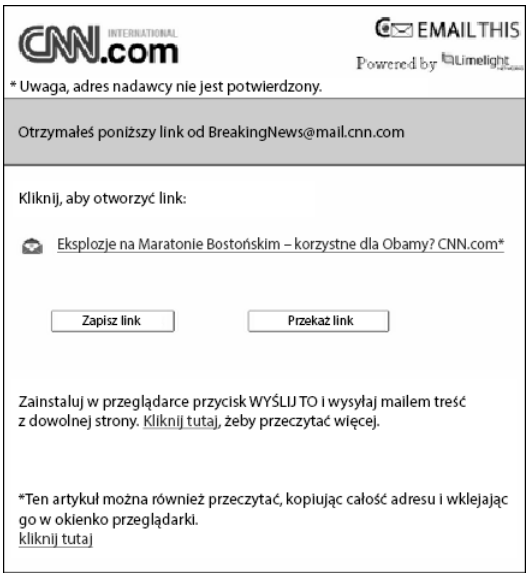
Gregg Steinhafel

Przewodniczący Rady Nadzorczej, Prezes i Dyrektor Naczelny

Rysunek 1.14. Prawda czy phish?

wykorzystują jego empatię. Oszuści atakowali w ciągu zaledwie kilku godzin od zamachu bombowego podczas maratonu w Bostonie w 2013 roku[xiv]. Wiele ataków było prostymi e-mailami, które zawierały linki do rzekomych nagrań eksplozji. Linki te, wykorzystujące naturalną ludzką ciekawość, prowadziły do stron, które wgrywały malware na komputer ofiary. W innym wariancie tego ataku skorzystano z takich aspektów, jak ciekawość i pozycja władzy, i podszyto się pod e-mail od CNN (rysunek 1.15).

Najgorsze są oczywiście te ataki, które żerują na chęci pomocy innym. Scamerzy często wysyłają wiadomości zawierające prośbę o pomoc już w kilka godzin po dowolnym tragicznym zdarzeniu. Rysunek 1.16 pokazuje jeden z e-maili, które pojawiły się po tym, jak w 2011 roku nastąpiło w Japonii najpierw trzęsienie ziemi, a zaraz po nim — tsunami. Według niektórych sprawozdań ataki zaczęły się zaledwie trzy godziny po pierwszym trzęsieniu ziemi.



CNN.com INTERNATIONAL

EMAILTHIS
Powered by Limelight

* Uwaga, adres nadawcy nie jest potwierdzony.

Otrzymałeś poniższy link od BreakingNews@mail.cnn.com

Kliknij, aby otworzyć link:

Eksplozje na Maratonie Bostońskim – korzystne dla Obamy? CNN.com*

Zapisz link | Przekaż link

Zainstaluj w przeglądarce przycisk WYŚLIJ TO i wysyłaj mailem treść z dowolnej strony. Kliknij tutaj, żeby przeczytać więcej.

*Ten artykuł można również przeczytać, kopiując całość adresu i wklejając go w okienko przeglądarki.
kliknij tutaj

Rysunek 1.15. Wariant ataku po zamachu podczas maratonu w Bostonie

Od: Brytyjski Czerwony Krzyż supportercare@redcross.org.uk
Do: [redacted]
Data: Wt., 15 Marca 201111
Temat: Apel po Tsunami w Japonii, Brytyjski Czerwony Krzyż
Potężne trzęsienie ziemi, siódme co do wielkości w historii, nastąpiło na wschodnim wybrzeżu Japonii w piątek 11 marca.

Trzęsienie o sile 9,0 w skali Richtera wywołało tsunami, które uderzyło we wschodnie wybrzeże Japonii siedmiometrowymi falami, pozostawiając po sobie ogromne zniszczenia.

Doniesienia mówią o ponad 1000 ofiar i wielu więcej zaginionych i rannych. Trzęsienie ziemi pociągnęło za sobą pożary i zniszczenia wielu budynków, pozostawiając ponad 5 milionów domów bez prądu i milion gospodarstw bez wody.

Japoński Czerwony Krzyż jest na miejscu od samego początku, pracuje tam 86 zespołów złożonych z około 600 lekarzy, pielęgniarek i członków personelu pomocniczego niosących pierwszą pomoc i opiekę medyczną oraz rozpoznających straty i potrzeby społeczności dotkniętych katastrofą.

Ponad 300 000 ludzi ewakuowanych przed uderzeniem fali zostało umieszczonych w tymczasowych miejscach schronienia przygotowanych w szkołach i innych budynkach użyteczności publicznej, gdzie Czerwony Krzyż rozdaje tysiące kocy.

Japoński Czerwony Krzyż wyraził zgodę na przesyłanie pomocy finansowej od obywateli Wielkiej Brytanii.

Jeśli kwota wsparcia przekazana na Apel po Tsunami w Japonii przekroczy taką, którą Japoński Czerwony Krzyż i Międzynarodowy Ruch Czerwonego Krzyża i Czerwonego Półksiężyca będą w stanie zasadnie i skutecznie wydać, nadwyżka funduszy zostanie przekazana na przygotowanie i przeprowadzenie innych akcji humanitarnych po katastrofach zarówno w Wielkiej Brytanii, jak i za oceanem.

Pomóż ofiarom katastrofy i przekaż środki na Apel po Tsunami w Japonii.

Możesz przekazać środki poprzez MoneyBookers, przesyłając pieniądze na adres [redacted] @yahoo.com.

Nie masz konta na MoneyBookers? Kliknij na http://www.moneybookers.com/, żeby się zarejestrować.

Brytyjski Czerwony Krzyż, 2011

Rysunek 1.16. Atak phishingowy po tsunami w Japonii

Przykład z rysunku 1.16 można łatwo rozpoznać jako phishing, dlatego że Czerwony Krzyż przyjmuje dotacje bezpośrednio na swojej stronie internetowej, a nie korzysta z przelewów za pośrednictwem serwisów takich jak MoneyBookers, przeznaczonych dla konta pod adresem e-mailowym w domenie *yahoo.com*. Ale musimy pamiętać, że po takim bolesnym i głośnym wydarzeniu wiele osób po prostu chciało pomóc. Osoby odpowiedzialne za te, często proste i łatwe do rozpoznania, ataki wzmacniają je telefonami, a czasem nawet nachodzeniem ludzi w domach, co zwiększa wiarygodność tych ataków.

Fisze na talerzu

Podsumowując, phishe mają różne rodzaje i postaci, ale powtarzają się w nich pewne elementy:

- przekręt nigeryjski (warianty zaliczkowe lub kradzieży tożsamości),
- usługi finansowe/płatnicze,
- serwisy społecznościowe,
- wykorzystywanie głośnych wydarzeń.

Ta lista w praktyce mogłaby być znacznie dłuższa i zawierać dowolne podmioty, które mogą komunikować się przez internet (takie jak eBay, Netflix, Allegro, producenci oprogramowania czy choćby Poczta Polska), ale chyba rozumiecie już ogólną zasadę. Można powiedzieć, że większość ataków jest na podstawowym lub zaawansowanym poziomie złożoności; mają też one wiele elementów wspólnych. Żeby skłonić ofiarę do działania, stosuje się w nich na przykład jeden z poniższych elementów:

- chciwość,
- strach,
- szacunek dla władzy,
- chęć nawiązania kontaktu,
- ciekawość,
- współczucie.

Większość ataków na tym poziomie ma cechy, które pozwalają nam rozpoznać, że są oszustwami. Natomiast należy pamiętać, że kiedy mamy do czynienia z bardziej rozwiniętymi przypadkami phishingu, następujące cechy stają się mniej oczywiste:

- niekonkretne powitanie/pożegnanie,
- nieznany/podejrzany nadawca,

- linki do nieznanych/podejrzanych stron,
- literówki, błędy gramatyczne, ortograficzne i interpunkcyjne,
- mało prawdopodobne preteksty (zwłaszcza w przekrętach nigeryjskich),
- naglące sformułowania.

Fisze z ostrymi zębami

Czy macie już wrażenie, że toniecie w odmętach oszustw? Przebiegłość, jaką wykazują ludzie, żeby okraść innych, jest naprawdę obezwładniająca. Co gorsza, przykłady przytoczone wcześniej należą właściwie do najprostszych ataków. Są różne ich wariacje, które wynoszą je na nowe (i jeszcze bardziej przygnębiające) poziomy.

Zaczęliśmy z Chrisem kategoryzować poziomy trudności ataków, żeby ułatwić naszym klientom zrozumienie, z czym mają do czynienia, a także po to, by śledzić postępy naszych klientów w rozpoznawaniu coraz bardziej skomplikowanych przekrętów. Szczegółowym opisem poszczególnych poziomów trudności zajmiemy się w rozdziale 6.

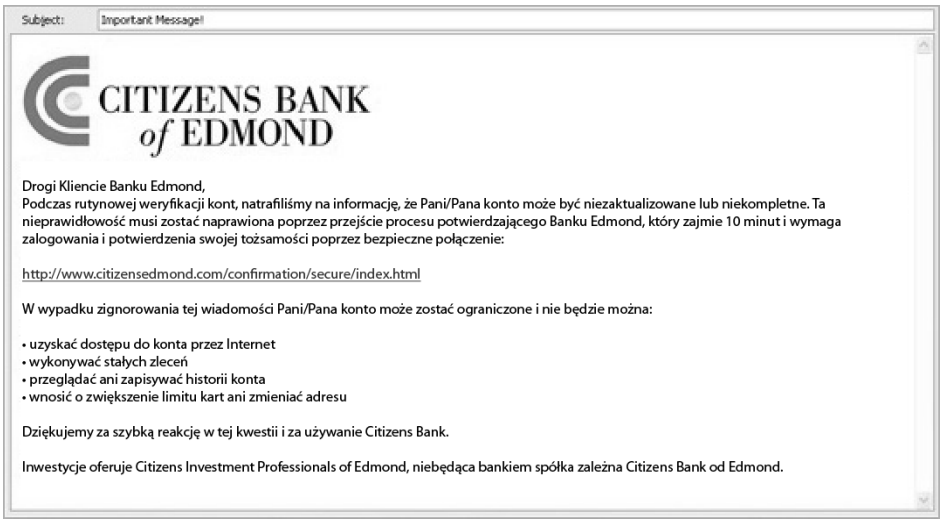
Ataki zaawansowane

Przykłady, które widzieliście wcześniej, należą głównie do poziomów: podstawowego i zaawansowanego, ale niektóre z nich stawiamy na górnym końcu skali przypadków zaawansowanych. Na przykład fałszywa wiadomość od sieci Target była dokładną kopią prawdziwego e-maila, tyle że zawierała linki do złośliwych stron. Wypłyńmy więc na głębsze wody i rozłóżmy na czynniki pierwsze kilka trudniejszych przypadków.

Pierwszym z nich jest kolejna wiadomość podszywająca się pod wiadomość z banku (rysunek 1.17).

Zastanówmy się, co zostało tutaj zrobione „dobrze". Co mogło skłonić odbiorców do kliknięcia w link w tym e-mailu?

- **Logo banku:** Pewnie zauważyliście to już wcześniej, ale wiele zaawansowanych ataków wykorzystuje prawdziwe logo i grafiki, dzięki czemu takie wiadomości wydają się bardziej wiarygodne. Przywykliśmy już do tego, że kiedy kontaktują się z nami duże firmy, widzimy markę firmy, więc logo jest dobrym sposobem na upozorowanie fałszywej wiadomości tak, aby wydawała się prawdziwa, i na uśpienie naszej czujności.


Subject: Important Message!

CITIZENS BANK of EDMOND

Drogi Kliencie Banku Edmond,
Podczas rutynowej weryfikacji kont, natrafiliśmy na informację, że Pani/Pana konto może być niezaktualizowane lub niekompletne. Ta nieprawidłowość musi zostać naprawiona poprzez przejście procesu potwierdzającego Banku Edmond, który zajmie 10 minut i wymaga zalogowania i potwierdzenia swojej tożsamości poprzez bezpieczne połączenie:

http://www.citizensedmond.com/confirmation/secure/index.html

W wypadku zignorowania tej wiadomości Pani/Pana konto może zostać ograniczone i nie będzie można:

• uzyskać dostępu do konta przez Internet
• wykonywać stałych zleceń
• przeglądać ani zapisywać historii konta
• wnosić o zwiększenie limitu kart ani zmieniać adresu

Dziękujemy za szybką reakcję w tej kwestii i za używanie Citizens Bank.

Inwestycje oferuje Citizens Investment Professionals of Edmond, niebędąca bankiem spółka zależna Citizens Bank od Edmond.

Rysunek 1.17. Zaawansowany atak „z banku"

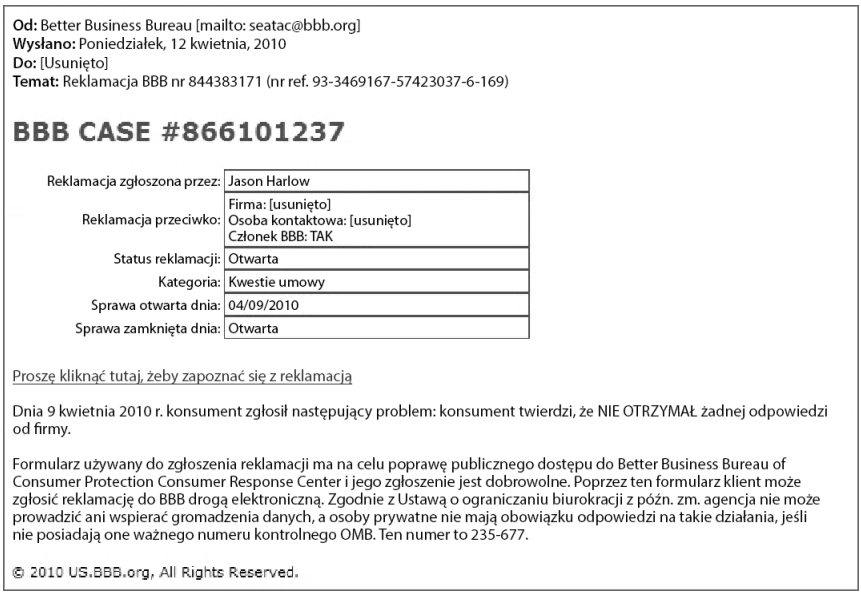
- **Wykorzystanie strachu/niepewności:** W tym e-mailu stwierdzono, że jeśli odbiorca nie podejmie pewnych działań, to jego dostęp do środków może zostać ograniczony.
- **Stosowanie ponagleń:** W tym e-mailu nie posunięto się do stwierdzenia, że odbiorca musi podjąć działanie w określonym przedziale czasu, ale zdecydowanie zachęca się do działania bez zwłoki.

Po tym, co omówiliśmy do tej pory, liczę, że nie było Wam trudno rozpoznać oszustwa z rysunku 1.17. Czy wychwyciliście charakterystyczne oznaki?

- bezosobowe powitanie,
- brak wskazania nadawcy,
- nieprawidłowości gramatyczne, w tym mało prawdopodobny temat wiadomości,
- przekierowanie linku — jeśli sprawdzicie link, to pewnie okaże się, że wcale nie prowadzi na stronę banku (np. zamiast kierować na *www.citizensedmond.com* prowadzi na *www.nieznanaosobaozlych zamiarach.com*).

OSTRZEŻENIE **Przez „sprawdzenie" rozumiemy przesunięcie kursora nad link, tak żeby tylko wyświetlić adres strony. Absolutnie nie należy klikać w link ani wklejać adresu do przeglądarki, chyba że jest się specem od bezpieczeństwa i ma się solidnie „ufortyfikowany" komputer.**

Na pierwszy rzut oka przykład z rysunku 1.18 jest podobny do poprzedniego e-maila „z banku", ale warto zwrócić uwagę na kilka rzeczy, przez które może być trudniej rozpoznać, że to fałszywka. Przyjrzyjcie się.



Od: Better Business Bureau [mailto: seatac@bbb.org]
Wysłano: Poniedziałek, 12 kwietnia, 2010
Do: [Usunięto]
Temat: Reklamacja BBB nr 844383171 (nr ref. 93-3469167-57423037-6-169)

BBB CASE #866101237

Reklamacja zgłoszona przez:	Jason Harlow
Reklamacja przeciwko:	Firma: [usunięto] Osoba kontaktowa: [usunięto] Członek BBB: TAK
Status reklamacji:	Otwarta
Kategoria:	Kwestie umowy
Sprawa otwarta dnia:	04/09/2010
Sprawa zamknięta dnia:	Otwarta

Proszę kliknąć tutaj, żeby zapoznać się z reklamacją

Dnia 9 kwietnia 2010 r. konsument zgłosił następujący problem: konsument twierdzi, że NIE OTRZYMAŁ żadnej odpowiedzi od firmy.

Formularz używany do zgłoszenia reklamacji ma na celu poprawę publicznego dostępu do Better Business Bureau of Consumer Protection Consumer Response Center i jego zgłoszenie jest dobrowolne. Poprzez ten formularz klient może zgłosić reklamację do BBB drogą elektroniczną. Zgodnie z Ustawą o ograniczaniu biurokracji z późn. zm. agencja nie może prowadzić ani wspierać gromadzenia danych, a osoby prywatne nie mają obowiązku odpowiedzi na takie działania, jeśli nie posiadają one ważnego numeru kontrolnego OMB. Ten numer to 235-677.

Rysunek 1.18. Zaawansowany atak phishingowy „BBB"

Jeśli zwróciliście baczną uwagę, to zauważyliście pewnie kilka następujących elementów, dzięki którym wiadomość z rysunku 1.18 jest bardziej przekonująca od przeciętnego ataku:

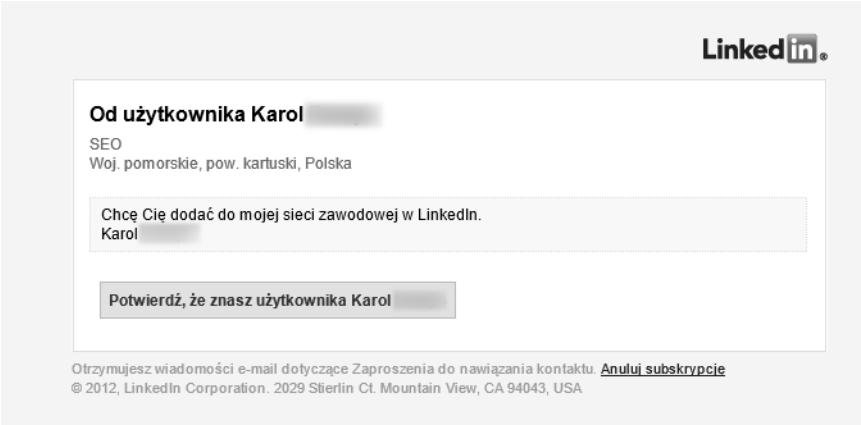
- **Personalizowanie:** Widać, że ta wiadomość została wysłana do danej osoby, a w treści znajduje się wzmianka o firmie adresata. Chociaż nie pojawia się tu logo ani grafika, to Better Business Bureau jest w USA dobrze znaną organizacją.
- **Lepsze wykorzystanie strachu/niepewności:** Ten e-mail jest reklamacją, pochodzi od BBB i powołuje się na problemy z umową *oraz* na to, że firma adresata nie zareagowała na reklamację. Każda z tych rzeczy budzi niepokój przedsiębiorcy.
- **Wykorzystanie pozycji władzy:** Pojawia się masa numerów referencyjnych, numerów sprawy, numerów Office of Management and Budget — wszystko wygląda bardzo oficjalnie.
- **Adres e-mail:** Adres nadawcy wygląda wiarygodnie, a e-mail wydaje się pochodzić z domeny *@bbb.org*.

Na szczęście ten e-mail ma też słabe punkty. Znaleźliście je?

- Numer sprawy w tytule nie zgadza się z numerem sprawy w treści.
- Brak wskazania nadawcy. Owszem został wysłany przez BBB, ale można by się spodziewać, że do sprawy zostałaby przydzielona jakaś osoba kontaktowa.
- I tym razem, gdybyśmy *sprawdzili* link prowadzący do reklamacji, zauważylibyśmy, że nie prowadzi do domeny należącej do BBB.
- Pojawiają się drobne błędy gramatyczne.
- Nie ma czegoś takiego jak Better Business Bureau of Consumer Protection Consumer Response Center. Sprawdziłam.

Phishing dla zaawansowanych

Dobra, czas zająć się czymś trudniejszym do rozszyfrowania. Przykład z rysunku 1.19 to zaawansowany atak phishingowy. W odróżnieniu od e-maila z „LinkedIn", pokazanego na rysunku 1.13, w tej wiadomości niełatwo rozpoznać fałszywkę. Podejrzewam, że to kopia e-maili, w których zachęca się do dodania kontaktu w serwisie, podobnie jak kopią był e-mail od sieci Target z rysunku 1.14.



Rysunek 1.19. Zaawansowana wiadomość phishingowa od „LinkedIn"

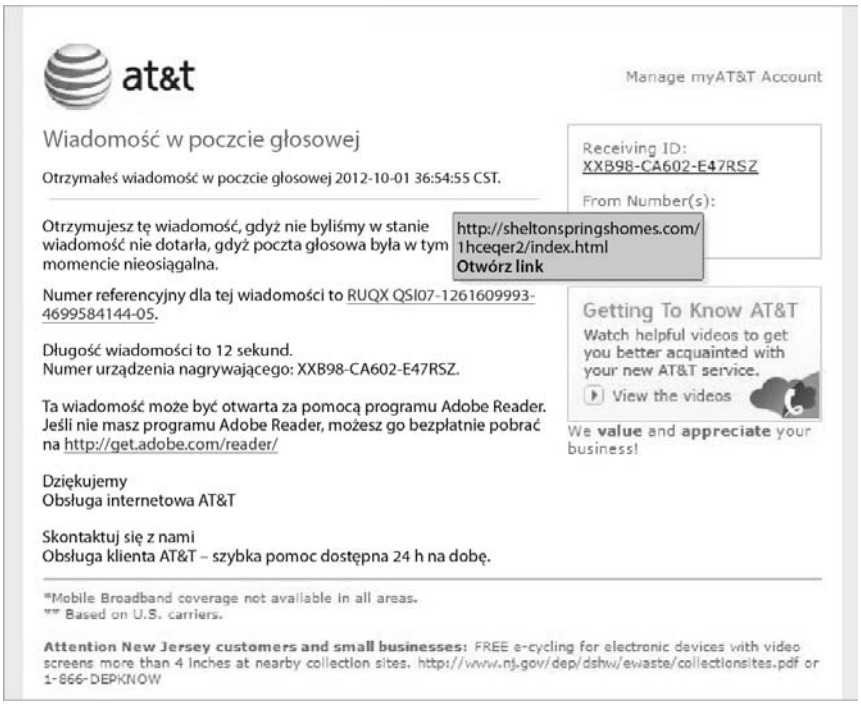
Dlaczego ten e-mail może zadziałać?

- Pochodzi od „prawdziwej" osoby. Ma ona konto w serwisie LinkedIn, więc na pewno taka osoba istnieje, prawda?
- To serwis społecznościowy, więc jesteśmy przyzwyczajeni do zaproszeń od nieznanych osób.
- Ma znaki firmowe i jest taki sam jak inne zaproszenia z LinkedIn.

Fakt, phish z rysunku 1.19 jest dobrą podróbką. Jeśli rzeczywiście jest sklonowanym e-mailem, to nie będzie miał żadnych widocznych oznak w postaci języka, formatowania czy znaków graficznych, po których będzie go można rozpoznać. W tym przypadku trzeba sprawdzić go dokładniej.

- Sprawdzamy, dokąd prowadzą linki (i przypomnę, że *sprawdzamy* nie znaczy *klikamy w nie*!).
- Sprawdzamy, czy adres, na który przyszedł ten e-mail, to adres podany przez nas na naszym koncie w serwisie LinkedIn (test na myślenie krytyczne).
- Osoby szczególnie ostrożne mogą zignorować tę wiadomość i zalogować się na swoje konto LinkedIn, żeby sprawdzić, czy tam też pojawiło się takie zaproszenie.

Wiadomość z rysunku 1.20 dostał pewien mój znajomy. E-maile od AT&T nie są dla niego rzadkością, bo ta właśnie firma jest jego operatorem komórkowym. Na swoje szczęście jest on też specem od bezpieczeństwa i ma lekką paranoję zawodową, więc zanim zareagował, sprawdził pewne rzeczy. Zdecydowanie sklasyfikowałabym ten atak jako zaawansowany.



Rysunek 1.20. Zaawansowany atak „AT&T"

Nie wiem, czy e-mail z rysunku 1.20 to klon prawdziwego e-maila od AT&T, ale jeśli tak nie jest, to został *naprawdę* dobrze sfałszowany. Przeciętny odbiorca pewnie kliknąłby w link z powodu następujących cech:

- użyto logo AT&T, kolorów i grafik firmowych;
- brak jest ewidentnych problemów z gramatyką, ortografią czy interpunkcją;
- jako pretekst podano brak dostępu do poczty głosowej — w takiej sytuacji większość z nas zareagowałaby od razu.

Co zatem spowodowało, że mój znajomy nie stał się ofiarą oszustwa?

- Zajęło mu to chwilę, ale zorientował się, że adres e-mail, na który przyszła ta wiadomość, to nie ten adres, którego używał ze swoim kontem AT&T. Właściwie to właśnie ta jedna rzecz go uratowała.
- Wiadomość nie ma bezpośredniego zwrotu do odbiorcy.
- W e-mailu jest tylko *jeden* zły link! Mój znajomy sprawdził wszystkie linki i zauważył coś ciekawego. Z wyjątkiem jednego linku, prowadzącego do rzekomej wiadomości, *wszystkie* inne były prawdziwe. A zatem gdyby nie sprawdził ich wszystkich dokładnie, nie zauważyłby, że to nie jest prawdziwy e-mail.

Jak wyraźnie widać, w tym przykładzie trudno rozpoznać oszustwo; zdecydowanie przechodzi podstawowe testy. Na szczęście mój znajomy ma taki zwyczaj, że nigdy nie wchodzi na żadne ze swoich kont poprzez linki w e-mailach. Mam nadzieję, że kiedy przeczytacie tę książkę, też zastanowicie się nad swoimi przyzwyczajeniami w sieci.

Spearphishing

Na koniec rozdziału zajmijmy się spearphishingiem. Jak wspomnieliśmy, jest to atak phishingowy, który został przygotowany pod kątem określonego odbiorcy. Atakujący przeprowadził rozeznanie i zna co najmniej imię, nazwisko i adres e-mailowy swojego „celu". Jeśli ofiara jest osobą wysoko postawioną, mógł dowiedzieć się na jej temat o wiele więcej. Wystarczy odrobina poszukiwań w sieci i można znaleźć ofiarę w serwisach społecznościowych, na stronie firmowej czy w ramach innych przejawów jej obecności online. Jeśli ofiara jest naprawdę ważna, to atakujący może dowiedzieć się wszystkiego o jej hobby, zainteresowaniach i majątku, a nawet może zdobyć informacje o rodzinie ofiary. Ba, jeśli znajdzie coś naprawdę złego czy kompromitującego, to nie będzie nawet musiał uciekać się do phishingu, żeby zdobyć to, o co mu chodzi. Będzie mógł

wtedy po prostu szantażować ofiarę, żeby wyłudzić od niej pieniądze lub zmusić ją do ujawnienia jakichś informacji. Ale zmieniam temat, a przecież naszym tematem jest phishing.

Coś takiego jest bardzo niepokojące, a do tego skutkuje atakiem phishingowym, któremu bardzo trudno się oprzeć. Atakujący, któremu naprawdę zależy na pieniądzach czy danych wybranej ofiary, nie cofnie się przed niczym. Dowie się, że ofiara przeszła ciężką chorobę i wspomaga teraz organizacje charytatywne związane z taką chorobą. Dowie się, czy ofiara uprawia w sieci hazard, czy że ma kredyt hipoteczny przekraczający jej zdolność kredytową. To jest to, co leży u podstaw spearphishingu. Jest nieubłaganie personalny.

Rysunek 1.21 pokazuje przykład ataku spearphishingowego, którego celem byli niedawno dyrektorzy dużych firm[xv]. Wyobrażacie sobie, że dostajecie coś takiego?


You forwarded this message on 4/24/2008 8:21 AM

From: United States District Court [subpoena@uscourts.com]
To: [redacted]
Cc:
Subject: Subpoena in case #28-755-YCH

AO 88(Rev. 11/94) Subpoena in a Civil Case

UNITED STATES DISTRICT COURT

Issued by the
UNITED STATES DISTRICT COURT

Issued to: [redacted]

SUBPOENA IN A CIVIL CASE

Case number: 28-755-YCH
United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7,2008
9:00 a.m. PST

Rysunek 1.21. Atak spearphishingowy o treści: „NINIEJSZYM WZYWA SIĘ do stawienia się i zeznawania przed Ławą Przysięgłych Sądu Rejonowego Stanów Zjednoczonych w miejscu i czasie wskazanych poniżej."

Zróbmy jeszcze analizę e-maila z tego rysunku. Co sprawia, że to przekonująca wiadomość?

- Zawiera logo federalnego sądu rejonowego USA.
- Posiłkuje się strachem i szacunkiem wobec władzy. Czy dla kogokolwiek jest przyjemne, gdy znienacka dostaje wezwanie i NAKAZ stawienia się przed sądem?

- Wiadomość jest spersonalizowana do tego stopnia, że zawiera pełne nazwisko, adres e-mailowy, nazwę firmy i numer telefonu ofiary.
- Narzuca ograniczenia czasowe: podana jest data i godzina, o której odbiorca ma się stawić na miejscu — w przeciwnym razie poniesie konsekwencje.
- Nie ma tu oczywistych literówek ani błędów gramatycznych.
- Nadawca jest dość wiarygodny: *subpoena@uscourts.com*.

Szczerze mówiąc, nie ma osoby, która z łatwością wyłapałaby ten atak. Ja byłam w stanie znaleźć tylko dwie przesłanki:

- Link prowadzący do właściwego wezwania jest złośliwy. Link z tego przykładu prowadzi do strony, która instalowała na komputerze keyloggera.
- Adres nadawcy ma domenę *@uscourts.com*, która nie budzi zastrzeżeń, póki nie przypomnimy sobie, że sądy amerykańskie korzystają z domen *.gov*.

I tyle! Dwie szanse na to, żeby rozpoznać, że wiadomość, która powoduje u odbiorcy niepokój i potrzebę reakcji, jest nakierowanym atakiem. Jak wspomniałam wcześniej, jeśli ktoś nie ma wyrobionych dobrych nawyków, to łatwo może się złapać na ataki tej klasy.

Podsumowanie

Zapoznaliście się już ze światem phishingu. W tym momencie powinniście już znać:

- definicję phishingu,
- często spotykane cele i typy atakujących,
- powody stosowania phishingu,
- techniki stosowane przez oszustów,
- przykłady głośnych włamań, które zaczęły się od ataków phishingowych,
- powszechnie spotykane przykłady ataków,
- zarys poziomów złożoności ataków.

Mam nadzieję, że rozumiecie już lepiej, czym jest phishing, jaki jest jego zasięg i jakie są powody, dla których staje się dla wszystkich coraz większym problemem.

Podsumujmy ten rozdział wybranymi danymi statystycznymi. W krótkim przedziale czasu, od maja 2012 roku do kwietnia 2013 roku, ataki phishingowe zgłosiło ponad 37 milionów użytkowników. To ataki, które zostały zgłoszone *do jednej instytucji*, a zatem to tylko ta część ataków, o której wiemy. Szacuje się, że codziennie wysyłanych jest blisko 300 miliardów e-maili, a 90% z nich to spam i wirusy[xvi]. To niewyobrażalne statystyki, które jednak prowadzą do jednego, niezaprzeczalnego wniosku. A mianowicie: jeśli masz adres e-mail, to wcześniej czy później trafi do Ciebie wiadomość phishingowa. Bez dwóch zdań.

Siądźcie wygodnie, bo za chwilę zanurzymy się w bardzo mętnych wodach. W phishingu nie chodzi tylko o to, w co klikasz, ale o to, *dlaczego* w to klikasz. Zajrzymy pod maskę systemu operacyjnego marki Człowiek i sprawdzimy, jak działa. Zapowiada się świetna zabawa, co? Bierzmy się do pracy.

Przypisy

[i] Geoffrey Ingersoll, *Inside the Clever Hack That Fooled the AP and Caused the DOW to Drop 150 Points* („Kulisy przebiegłego ataku, który pokonał AP i spowodował spadek indeksu Dow Jones o 150 punktów"), „Business Insider", 22 listopada 2013, *http://www.businessinsider.com/inside-the-ingenious-hack-that-fooled-the-ap-and-caused--the-dow-to-drop-150-points-2013-11*.

[ii] Tim Wilson, *Report: Phishing Attacks Enabled SEA to Crack CNN's Social Media* („Raport: ataki phishingowe umożliwiły SEA włamanie do serwisów społecznościowych CNN"), *DarkReading.com*, 27 stycznia 2014, *http://www.darkreading.com/attacks--breaches/report-phishing-attacks-enabled-sea-to-crack-cnns-social-media/d/d-id/1141215?*.

[iii] Andy Greenberg, *How the Syrian Electronic Army Hacked Us: A Detailed Timeline* („Jak włamała się do nas Syryjska Armia Elektroniczna: oś czasu"), „Forbes", 20 lutego 2014, *http://www.forbes.com/sites/andygreenberg/2014/02/20/how-the-syrian-electronic--army-hacked-us-a-detailed-timeline/*.

[iv] Danny Yadron, *Alleged Chinese Hacking: Alcoa Breach Relied on Simple Phishing Scam* („Chiny podejrzane o hacking: włamanie do Alcoa polegało na prostym ataku phishingowym"), „The Wall Street Journal", 19 maja 2014, *http://www.wsj.com/news/articles/ SB10001424052702303468704579572423369998070*.

[v] Brett LoGiurato, *The US Government Indicts 5 Chinese Military Hackers on Cyberspying Charges* („Rząd USA stawia 5 chińskim hakerom wojskowym zarzuty cyberszpiegostwa"), „Business Insider", 19 maja 2014, *http://www.businessinsider.com/us-china-spying--charges-2014-5*.

[vi] Symantec Official Blog, *Francophoned — A Sophisticated Social Engineering Attack* („Frankofonia — wyrafinowany atak socjotechniczny"), 28 sierpnia 2013, *http://www.symantec.com/connect/blogs/francophoned-sophisticated-social-engineering-attack*.

[vii] Anti-Phishing Working Group, *Phishing Activity Trends Report, 2nd Quarter 2014* („Raport na temat trendów w działaniach phishingowych, 2. kw. 2014"), 28 sierpnia 2014, *http://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf*.

[viii] Michael Riley, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It* („Przegapione sygnały ostrzegawcze i 40 milionów skradzionych numerów kart kredytowych: jak Target pokpił sprawę"), 17 marca 2014, *http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data-p1*.

[ix] Brian Krebs, *Email Attack on Vendor Set Up Breach at Target* („Atak e-mailowy na podwykonawcę spowodował włamanie do sieci Target"), 12 lutego 2014, *http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/*.

[x] Avivah Litan, *RSA SecurID Attack Details Unveiled — Lessons Learned* („Szczegóły ataku RSA SecurID — wyciągnięte wnioski"), 1 kwietnia 2011, *http://blogs.gartner.com/avivah-litan/2011/04/01/rsa-securid-attack-details-unveiled-they-should-have-known-better/*.

[xi] Nicole Perlroth, *Study May Offer Insight into Coca-Cola Breach* („Dochodzenie może rzucić światło na włamanie do Coca-Coli"), 30 listopada 2012, *http://bits.blogs.nytimes.com/2012/11/30/study-may-offer-insight-into-coca-cola-breach/*.

[xii] Sarah Perez, *AP Twitter Hack Preceded by a Phishing Attempt, News Org Says* („Włamanie na konto na Twitterze należące do AP było poprzedzone próbą phishingu — jak donosi organizacja informacyjna"), *TechCrunch.com*, 23 kwietnia 2013, *http://techcrunch.com/2013/04/23/ap-twitter-hack-preceded-by-a-phishing-attempt-news-org-says/*.

[xiii] Catey Hill, *Email 'from Target' to Customers Is a Phishing Scam* („E-mail od »Targetu« do klientów to atak phishingowy"), *MarketWatch.com*, 20 grudnia 2013, *http://www.marketwatch.com/story/scammers-pounce-on-target-fiasco-2013-12-20*.

[xiv] Jovi Umawing, *Fake CNN Spam Use Boston Marathon Bombing as Lure* („Spam podszywa się pod CNN z wykorzystaniem zamachu na Maratonie Bostońskim jako przynęty"), 18 kwietnia 2013, *http://www.threattracksecurity.com/it-blog/fake-cnn-spam-use-boston-marathon-bombing-as-lure/*.

[xv] John Markoff, *Larger Prey Are Targets of Phishing* („Phishing bierze na cel grubsze ryby"), „The New York Times", 16 kwietnia 2008, *http://www.nytimes.com/2008/04/16/technology/16whale.html?_r=0*.

[xvi] Social-Engineer.Org, *The Social Engineering Infographic* („Infografika socjotechniki"), 28 kwietnia 2014, *http://www.social-engineer.org/resources/social-engineering-infographic/*.

Skorowidz

R

S

Ś

T

U

V

W

Z

Nie daj się złapać na haczyk! Strzeż swojego bezpieczeństwa!

Ataki za pomocą specjalnie spreparowanych wiadomości e-mail są jednym z najczęstszych i najbardziej uciążliwych zagrożeń. Mimo kampanii edukacyjnych i szeroko zakrojonych programów bezpieczeństwa phishing wciąż jest niezwykle skuteczną bronią przestępców. Jest tak, gdyż wykorzystuje odruchy, którymi kieruje się przeważająca większość ludzi. Aby więc ochronić się przed atakiem, trzeba poznać zarówno podstawy ataków e-mailowych, jak i pewne zasady psychologii i metody manipulacji ludzkim postępowaniem.

Trzymasz w ręku świetny przewodnik po mrocznym świecie phishingu. Opisano tu formy tego rodzaju ataków, przedstawiono sposoby rozpoznawania fałszywych wiadomości e-mail czy sklonowanych stron internetowych. Omówiono również socjotechniczne aspekty phishingu, dzięki czemu lepiej zrozumiesz psychologiczne mechanizmy rządzące postępowaniem ofiary. Po lekturze tej książki będziesz również wiedzieć, jak udoskonalić firmowy system bezpieczeństwa, aby skutecznie odpierać ataki e-mailowe — nawet te bardzo wyrafinowane!

W tej książce:

- opis słynnych włamań dokonanych za pomocą spreparowanych e-maili
- analiza celów ataku i korzyści, jakie osiągają atakujący
- psychologiczne i socjologiczne podstawy phishingu
- analiza przyczyn nieskuteczności firmowych programów budowania świadomości bezpieczeństwa informacji
- metody rozpoznawania ataków
- metody ochrony systemu informatycznego przed phishingiem

CHRISTOPHER HADNAGY jest założycielem spółki Social-Engineer. Od ponad 15 lat zajmuje się kwestiami bezpieczeństwa informacji. Specjalizuje się w badaniu socjotechnicznych metod zdobywania nieuprawnionego dostępu do informacji. Wzięty autor i aktywny uczestnik wielu konferencji. MICHELE FINCHER jest behawiorystką, badaczką i ekspertką w dziedzinie bezpieczeństwa informacji. Pracowała dla Sił Powietrznych USA — zajmowała się bezpieczeństwem informacji, włączając w to wykłady w Air Force Academy. Obecnie przyczynia się do sukcesu firmy Social-Engineer.

Helion

księgarnia internetowa

http://helion.pl

zamówienia telefoniczne

0 801 339900

0 601 339900

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

Sprawdź najnowsze promocje:
http://helion.pl/promocje
Książki najchętniej czytane:
http://helion.pl/bestsellery
Zamów informacje o nowościach:
http://helion.pl/nowosci

Informatyka w najlepszym wydaniu

sięgnij po WIĘCEJ

KOD KORZYŚCI

ISBN 978-83-283-2906-5

9 788328 329065

cena: 39,00 zł