



Haczyk, linka i ciężarek

O oszustwach typu phishing oraz o tym, jak nie dać się złapać!

Prawie każdego dnia w Internecie można przeczytać o „phishingu”, który czasami określany jest również jako „carding” lub ‘brand spoofing’. Co to jest, jak działa i jakie są skutki phishingu?

Phishing (słowo „fishing”, dosłownie oznaczające wędkarstwo, zostało napisane z błędem celowo) jest szczególną formą przestępstwa cybernetycznego. Polega ono na podstępym skłonieniu użytkowników komputerów do ujawnienia swoich danych personalnych (nazwa użytkownika, hasło, numer PIN lub inne informacje dostępne), a następnie wykorzystaniu tych informacji do wyludzenia pieniędzy. Jest to oszustwo: kradzież danych, a następnie pieniądze.

Phisherzy w dużym stopniu wykorzystują chwyt socjotechniki. Phishing to po prostu bardziej wyrafinowany sposób mówienia o „nietechnicznym” naruszeniu bezpieczeństwa systemu z wykorzystaniem interakcji personalnej: skłonieniu użytkowników do złamania zwykłych zasad bezpieczeństwa.

Socjotechnika jest powszechnie stosowana przez twórców wirusów i robaków w celu skłonienia niczego nie podejrzewających użytkowników do uruchomienia szkodliwego kodu. Może to oznaczać załączenie wirusa lub robaka do pozornie nieszkodliwej wiadomości email. Na przykład robak LoveLetter został rozesłany jako wiadomość email o temacie „I LOVE YOU” (kto z nas nie lubi otrzymywać listów miłosnych?) oraz treści „Kindly check the attached LOVELETTER coming from me”. Aby jeszcze bardziej zbić z tropu niczego nie podejrzewających użytkowników, załącznik zawierał podwójne rozszerzenie LOVE-LETTER-FOR-YOU.TXT.vbs: domyślnie system Windows nie wyświetla drugiego (prawdziwego) rozszerzenia i załącznik wgląda jak plik tekstowy. Trik ten wykorzystywało później wiele wirusów i robaków, w tym SirCam, Tanatos oraz Netsky.

Innym chwytem socjotechniki jest skonstruowanie wiadomości email w taki sposób, aby sprawiała wrażenie czegoś potrzebnego lub w inny sposób atrakcyjnego. Na przykład, robak Swen „udawał” zbiorczą łąkę Microsoftu, wykorzystując rosnącą świadomość użytkowników o konieczności zabezpieczania systemów operacyjnych przed atakami robaków internetowych. Tego typu maile nie są jedyną formą socjotechniki. Pojawiły się na przykład wiadomości przesyłane za pośrednictwem komunikatorów internetowych, które zawierały odnośniki do zainfekowanych stron internetowych.

W oszustwach typu phishing przestępca tworzy niemal idealną replikę strony internetowej wybranej instytucji finansowej. Następnie wyrusza „na połów”, wykorzystując metody spammerskie w celu rozesłania wiadomości e-mail, która imituje korespondencję od istniejącej instytucji finansowej. Phisherzy wykorzystują zwykle prawdziwe logotypy, odpowiedni styl biznesowy, a nawet wymieniają prawdziwe nazwiska osób z wyższego szczebla zarządu danej instytucji finansowej. Podrabiają także nagłówki maili, aby wyglądały, jakby pochodziły z banku. Ogólnie, listy te informują klientów, że bank zmienia swoją infrastrukturę IT i prosi wszystkich klientów o ponowne potwierdzenie swoich informacji osobowych. Czasami jako powód żądania powtórnego potwierdzenia danych personalnych klientów wymieniane są awarie sieci czy nawet ataki hakerów.

Rozsyłane przez phisherów fałszywe wiadomości email mają jedną rzecz wspólną: stanowią przynętę wykorzystywaną w celu nakłonienia klienta do kliknięcia zawartego w wiadomości odsyłacza. Gdy nieszczęsna „rybka” chwyci przynętę, może wyjawiać poufne dane, które pozwolą cyberprzestępcy uzyskać dostęp do jej konta bankowego. Odsyłacz kieruje użytkownika bezpośrednio na animowaną stronę, która do złudzenia przypomina prawdziwą stronę internetową banku. Strona ta zawiera formularz, który ma wypełnić użytkownik: jeśli to zrobi, przekaże wszystkie informacje, jakich potrzebuje przestępca, aby uzyskać dostęp do jego konta online i ukraść jego pieniądze.

Tak jak można się spodziewać, phisherzy atakują organizacje, które obsługują dużą ilość transakcji finansowych online z klientami. Do ich celi zaliczają się naturalnie wszystkie największe banki oraz inne organizacje (takie jak Amazon, AOL, BestBuy, eBay, MSN, PayPal oraz Yahoo). Nikogo nie powinno dziwić, że phisherzy nadal atakują głównie dostawców usług finansowych, zważywszy na to, że ich ostatecznym celem jest kradzież pieniędzy.



Oczywiście w każdym oszustwie typu phishing istnieje prawdopodobieństwo, że tylko niewielki odsetek odbiorców fałszywej wiadomości będą stanowili klienci banku lub organizacji, od której pochodzi rzekomo wiadomość; również tylko niewielka część tych osób może „połknąć przynętę”. Jednak podobnie jak w przypadku spamu, phisherzy wysyłają tak ogromne ilości fałszywych wiadomości, że nawet niewielki odsetek osób, które dadzą się oszukać, pozwoli im zebrać wystarczającą ilość danych, aby oszustwo opłaciło się.

Osobiste dane finansowe nie zawsze stanowią cel phisherów. Tak zwany „spear phishing” ma na celu skłonienie użytkownika korporacyjnego do ujawnienia poufnych danych, które mogą zostać wykorzystane do zdobycia szerszego dostępu do systemu korporacyjnego. Phisher podrabia zwykle adres e-mail, aby wyglądał, jakby pochodził od jakiejś „ważnej” osoby w firmie (z działu zarządzania zasobami ludzkimi, IT itd.). Wiadomość jest spersonalizowana, aby wydawała się jeszcze mniej podejrzana. Jeśli użytkownik odpowie, phisher będzie mógł wykorzystać te informacje w celu zdobycia dostępu do zasobów korporacyjnych.

Ponieważ w większości przypadków phishing wykorzystuje socjotechnikę, formy tego ataku są liczne i zróżnicowane. Na przykład, „mophishing” stanowi subtelną alternatywę „standardowego” ataku typu phishing opartego na poczcie elektronicznej. W tym przypadku phisherzy wykorzystują obawy użytkowników przed odpowiadaniem na wiadomości e-mail i proszą ich o przesłanie poufnych danych faksem. Oszuści próbują przekonać niczego nie podejrzewającego użytkownika, że metoda ta nie jest bezpieczna (tj. transakcje online) i proszą go, żeby skorzystał z „bezpieczniejszej” alternatywy i potwierdził swoje dane personalne faksem. W końcu dla cyberprzestępców liczą się dane, a nie sposób ich uzyskania!

W grę wchodzi wysokie stawki. Szacowane straty powstałe w wyniku oszustw typu phishing różnią się od siebie (w Sieci można znaleźć dane, które wahają się od 400 milionów do 2,4 miliarda dolarów). Jednak liczba ataków phishing i związanych z nimi kosztami wyraźnie wzrasta. W kwietniu 2006 roku liczba unikatowych stron phishingowych wykrytych przez Anti-Phishing Working Group (<http://www.antiphishing.org/>) (APWG) wyniosła 11 121, znacznie więcej niż w poprzednich miesiącach i stanowiła rekord APWG. Chociaż liczba unikatowych zgłoszeń phishingu spadła w stosunku do poprzedniego miesiąca (do 17 290), jest znacznie wyższa niż rok temu¹.

Jednak problem nie zawsze kończy się tylko na kosztach bezpośrednich. Niektórzy phisherzy umieszczają również na swoich stronach exploity wykorzystujące luki w przeglądarce Microsoft Internet Explorer (IE). Gdy po kliknięciu odsyłaacza ofiara zostanie przekierowana na fałszywą stronę internetową, exploit pobierze na komputer trojana. W rezultacie, nie tylko zostaną przechwycone informacje bankowe użytkowników, ale ich komputery staną się bezwiednymi „żołnierzami” w armii „zombie”, których będzie można wykorzystać do innych szkodliwych działań: np. do przeprowadzenia ataku DDoS (Distributed Denial of Service) w celu wyłudzenia pieniędzy od organizacji, jako platformę do dystrybucji spamu lub do rozprzestrzeniania wirusa, robaka, trojana czy programu „spyware”.

Niezły wynik jak na jeden dzień „połowów”!

Nikogo nie powinno zatem dziwić, że phishing tak bardzo przyciągnął uwagę mediów w ciągu ostatnich dwóch lat. Z drugiej strony, instytucje finansowe udzielają swoim klientom porad odnośnie potencjalnych niebezpieczeństw. W rezultacie, użytkownicy stają się coraz ostrożniejsi. To powoduje, że phisherzy zaczynają szukać coraz bardziej wyrafinowanych sposobów nakłonienia użytkowników do ujawnienia swoich osobistych informacji bankowych.

Aby ich oszustwa były mniej oczywiste, niektórzy phisherzy wykorzystują teraz luki (lub niechciane funkcje). Na przykład, luka w Internet Explorerze udokumentowana przez Microsoft pod koniec 2003 roku pozwalała phisherom na stworzenie fałszywej strony internetowej, która nie tylko do złudzenia przypomina legalną stronę instytucji finansowej, ale również wyświetla prawdziwy adres URL w oknie przeglądarki IE. Gdy użytkownik kliknie zawarty w wiadomości phishingowej odsyłaacz, przeglądarka internetowa wyświetla zawartość fałszywej strony, ale adres URL w oknie przeglądarki jest rzeczywistym adresem banku. Na stronie internetowej Microsoftu (<http://support.microsoft.com/?id=833786>) znajduje się pełny opis tej luki wraz ze wskazówkami odnośnie sposobów identyfikowania sfałszowanych stron internetowych.

¹) Dane pochodzą z APWG Phishing Trends Activity Report (http://www.antiphishing.org/reports/apwg_report_apr_06.pdf), kwiecień 2006.



Phisher może również załadować legalną stronę internetową, ale po chwili wyświetlić na niej okienko wyskakujące, które żąda od użytkownika wprowadzenia informacji osobowych. W takim przypadku niebezpieczne okienko wyskakujące wygląda jak legalna prośba z banku.

Phisherzy powszechnie maskują odsyłacz zawarty w wiadomości e-mail: prawdziwy adres ukryty jest pod odsyłaczem, który wygląda jak legalny (prawdziwy adres jest widoczny dopiero po najechaniu myszką na odsyłacz). Jest to dobry argument za używaniem czystego tekstu w wiadomościach e-mail zamiast HTML-a oraz wyłączenia wykonywania skryptów na komputerze. Trzeba być jednak ostrożnym. Niebezpieczny odsyłacz można ukryć nawet w wiadomości z czystym tekstem. Przyjrzyj się następującym adresom:

- <http://www.kaspersky.pl/>
- <http://www.kapersky.pl/>
- <http://www.kaspersky-antivirus.pl>
- <http://www.kasperksy.pl>

Wszystkie wyglądają dość niewinnie. Jednak tylko jeden jest prawdziwy. Przesuwając lub opuszczając litery, zastępując je liczbami (na przykład w miejsce litery „l” wstawiając cyfrę „1”) można zmylić niczego nie podejrzewającego użytkownika i skłonić go do kliknięcia odsyłacza.

Coraz więcej phisherów dąży do przekierowania użytkowników na sfałszowane strony internetowe bez konieczności klikania odsyłacza. W listopadzie 2004 roku phisherzy zaczęli wykorzystywać fakt, że w HTML-u można osadzić instrukcje skryptowe (łącznie z instrukcjami exploita), które zostaną wykonane automatycznie w momencie czytania wiadomości e-mail. Phisherzy wysyłają wiadomości w HTML-u zawierające instrukcje skryptowe dotyczące edytowania pliku hosts na komputerze ofiary. W rezultacie, gdy użytkownik następnym razem skieruje przeglądarkę na stronę internetową swojego banku, zostanie ona automatycznie przekierowana na fałszywą stronę, na której mogą zostać przechwycone wszelkie wprowadzane dane. Użytkownik nie kliknął żadnego odsyłacza. Nie ma również powodu podejrzewać, że uzyskał dostęp do sfałszowanej strony bankowej. Mimo to staje się ofiarą phisherów.

W celu „zautomatyzowania” procesu przekierowywania phisherzy wykorzystują również trojany. Trojan może zostać masowo wysłany przy użyciu technik spamerskich bezpośrednio do wyznaczonej grupy komputerów PC. Może również zostać pobrany na komputer ofiary podczas odwiedzenia przez nią strony internetowej, lub zainstalowany przez jakiś inny szkodliwy program (na przykład robaka). Po zainstalowaniu na komputerze ofiary trojan edytuje plik hosts lub modyfikuje ustawienia serwera DNS w celu przekierowania połączenia na fałszywy serwer internetowy. Serwer ten w większości przypadków będzie dostarczał właściwą zawartość, ale będzie również mógł przekierować wybrane żądania na fałszywą stronę internetową. Użytkownik nie kliknął odsyłacza i nie ma możliwości zorientowania się, że żądane dane zostały sfałszowane.

Phishing to specyficzny rodzaj cyberprzestępstwa, które w dużym stopniu wykorzystuje socjotechnikę, nietechniczne naruszenie bezpieczeństwa systemu, które opiera się na interakcji personalnej: innymi słowy, jest to podstępne skłonienie użytkowników do zrobienia czegoś, czego nie powinni zrobić. W tym sensie phishing to ruchomy cel. Cyberprzestępcy nieustannie próbują znaleźć nowe sposoby „złapania” użytkowników. Czasami wykorzystują do tego nowe technologie. Innym razem takim „haczykiem” może być po prostu odpowiedni temat wiadomości.



Z tego powodu nie jest możliwe stworzenie zamkniętej listy cech charakterystycznych phishingu. Poniższe zestawienie zawiera tylko niektóre z głównych wyróżników wiadomości phishingowych. Ma ono dostarczyć ogólne wskazówki odnośnie tego, jak zminimalizować ryzyko stania się ofiarą phisherów:

- Bądź ostrożny w stosunku do wszystkich wiadomości e-mail zawierających prośby o podanie informacji osobowych. Jest wysoce nieprawdopodobne, że Twój bank zażąda takich informacji za pośrednictwem poczty elektronicznej lub że dział IT Twojej firmy poprosi Cię o potwierdzenie loginu czy hasła systemowego. Jeśli będziesz miał jakieś wątpliwości, zadzwoń i sprawdź!
- Nie używaj odsyłaczy w wiadomościach e-mail w celu załadowania strony internetowej. Zamiast tego samodzielnie wpisz adres URL do przeglądarki internetowej.
- Nie wypełniaj formularzy załączanych do wiadomości e-mail, w których występują prośby o podanie informacji osobowych. Tego typu dane wprowadzaj tylko za pośrednictwem bezpiecznej strony internetowej. Sprawdź, czy adres URL zaczyna się od „https://”, a nie „http://”. Szukaj symbolu zamkniętej kłódki w prawym dolnym rogu przeglądarki i kliknij dwukrotnie, żeby sprawdzić prawdziwość certyfikatu cyfrowego. Jeśli masz wątpliwości, do zawierania transakcji używaj telefonu.
- Sprawdź, czy twój program antywirusowy blokuje strony phishingowe, lub rozważ zainstalowanie paska narzędzi przeglądarki internetowej, który będzie ostrzegał Cię przed znanymi atakami phishing.
- Regularnie sprawdzaj swoje konto bankowe (łącznie z kartami debetowymi i kredytowymi, wyciągami bankowymi itd.), aby upewnić się, że wyszczególnione transakcje są legalne.
- Używaj najnowszej wersji przeglądarki internetowej oraz instaluj wszystkie łaty bezpieczeństwa.
- Jeśli zauważysz coś podejrzanego, natychmiast powiadom o tym swój bank!
- Sprawdzaj wszystkie daty wymieniane w treści wiadomości e-mail. Uważaj na wiadomości zawierające przeszłe daty: na przykład, gdy minął już termin ostateczny wykonania określonej czynności.
- Bądź podejrzliwy, jeśli wiadomość email nie jest zaadresowana do ciebie osobiście: na przykład, jeśli zaczyna się od słów „Drogi Kliencie” lub podobnie.
- Bądź podejrzliwy, jeśli jesteś jednym z wielu odbiorców wiadomości. Jeśli bank będzie chciał skontaktować się z tobą odnośnie twojego osobistego konta bankowego, z pewnością nie wyśle tego maila do innych osób.
- Uważaj na błędy ortograficzne w prostych słowach oraz błędy gramatyczne, syntaktyczne i inne przykłady nieporadnego użycia języka. Aby dowiedzieć się więcej na temat ochrony przed oszustwami typu phishing oraz postępowania w sytuacji, gdy uważasz, że ujawniłeś swoje informacje osobowe, których nie powinieneś, przeczytaj Consumer Advice on Phishing na stronie APWG (<http://www.antiphishing.org/resources.html>).