Łowienie naiwnych

• Lech Piesik

Phishing po polsku jest groźniejszy, bo jest bardziej zrozumiały, a przez to staje się wiarygodniejszy od ataku „prośby” w języku obcym

Nazwa „phishing” jest skrzyżowaniem słów „fishing” (łowić ryby) z „personal data” – dane osobowe. Chociaż aż 85 proc. wykrytych przypadków phishingu dotyczy instytucji finansowych, to na wiosnę do skrzynek wielu polskich internautów trafił e-mail zalecający jak najszybsze pobranie i zainstalowanie uaktualnień dla systemu Windows. W rzeczywistości chodziło o wprowadzenie do komputera konia trojańskiego. Układ treści e-maila był typowy, czyli „prośba” (prosimy o jak najszybszą aktualizację systemu), po niej następowało „ostrzeżenie” (zignorowanie tej wiadomości i brak aktualizacji może spowodować całkowitą i bezpowrotną utratę danych z komputera) i „link na fałszywą stronę” (w celu aktualizacji kliknij w przycisk niżej „Pobierz teraz i zainstaluj”). To wszystko. Warto więc pamiętać, że Microsoft nigdy nie rozsyła poprawek dla swoich produktów pocztą elektroniczną.

Phishing polega na tworzeniu oszukańczych wiadomości e-mail i witryn WWW, które wyglądają identycznie jak serwisy internetowe firm o znanej marce, aby skłonić klientów tych firm do podania numeru karty kredytowej lub informacji o koncie bankowym. Ataki typu phishing zaczęły stanowić na tyle poważne zagrożenie, że zmusiły wielkie firmy oraz organizacje do zjednoczenia sił w walce z tym procederem. W grudniu 2004 roku powstała grupa Digital PhishNet skupiająca firmy IT takie jak Microsoft, America Online, eBay, PayPal i Visa oraz amerykańskie służby U.S. Secret Service i U.S. Postal Inspection Service i FBI, które podpisały umowę, na mocy której będą natychmiast informować o wykrytych przypadkach phishingu i wprowadzać je do centralnej bazy witryn-pułapek prowadzonej przez WholeSecurity. Firmy będą się też starały blokować strony oszustów.

W Polsce pierwsze przypadki phishingu zanotowano w 2001 roku. Ich liczba wzrasta z roku na rok. Według policji, codziennie likwiduje się do 10 stron internetowych podszywających się pod strony banków. Po pierwszych takich wypadkach polskie banki są już wyczulone na fałszywki swoich stron. Nie tak dawno mBank podał autora jednej z nich do sądu, ale okazało się, że strona była tylko przykładem i nie miała na celu jakichkolwiek wyłudzeń. Tu trzeba dodać, że policja ma mocno utrudnione zadanie, ponieważ 80 proc. tego typu fałszywych stron umieszczanych jest na zagranicznych serwerach ulokowanych najczęściej w USA i Chinach.

Polska na celowniku

Po niedawno przeprowadzonym ataku phishingowym na klientów mBanku, w którym odbiorca był proszony o „potwierdzenie swojej tożsamości”, tym razem rozsyłane były e-maile, w których oszuści podszywali się pod przedstawicieli Inteligo, konta prowadzonego przez PKO BP S.A. Wiele wskazuje na to, że przestępcza moda zawitała do Polski na dobre. Ataki na klientów mBanku i Inteligo pokazują, że żaden rodzimy bank nie powinien czuć się bezpiecznie, bo wbrew pozorom, taki atak może być skuteczny, a wtedy zebrane dane mogą posłużyć zarówno do włamania na konto albo – co najmniej – zostanie wykorzystany numer karty płatniczej. Ataki, zarówno na klientów mBanku, jak i Inteligo można nazwać klasyką gatunku. E-mail był wysłany również do osób, które w tych bankach konta nie mają. Ale to może też dobrze świadczyć o zabezpieczeniu baz klientów w bankach.

Szkody materialne banku nawet po takim udanym ataku będą zapewne znikome, ale znacznie gorsze mogą okazać się straty wizerunkowe. Chociaż bank będzie też ofiarą, podobnie jak jego klienci, to jednak właśnie on za wszystko „zapłaci”. Problem jest chyba większy niż się o tym mówi, bo również niedawno na stronach internetowych niektórych banków pojawił się złowieszczy komunikat przestrzegający przed fałszywym e-mailem, którego nadawcy podszywali się pod organizację VISA. Dysponując danymi z karty, przestępca może się nią swobodnie posługiwać i to nie tylko w Polsce. Uzyskiwanie ważnych informacji na temat kart płatniczych było i jest możliwe od dawna, jednak dotychczas nikt nie robił tego masowo w ten sposób. Do tej pory prosty phishing nie zagrażał bezpieczeństwu bankowości internetowej.

Jednak nic nie daje 100-procentowej gwarancji bezpieczeństwa i jak mówi polskie przysłowie „przyszła kryska na Matyska” również na nasz bank. Właśnie z powodu phishingu bank stracił ponad 1 mln zł. Był to pierwszy tak duży ujawniony przypadek kradzieży z banku internetowego. Poszkodowani zostali przede

FOT. DREAMSTIME

wszystkim klienci indywidualni, których konta nie były chronione hasłami jednorazowymi. Do kradzieży użyto koni trojańskich rozsyłanych pocztą elektroniczną do potencjalnych ofiar. Dobrze zamaskowany program monitorował aktywność użytkownika i zapisywał dane, które umożliwiały korzystanie z konta bankowego przez internet. Później dane były odsyłane na wcześniej przygotowane serwery. Danych nie używano natychmiast, przez co koń trojański po kilku dniach swojej „pracy" usuwał w komputerze ślady swojej działalności, po czym sam wydawał komendę odinstalowania siebie.

Ofiarami stali się klienci banku. W dogodnym momencie złodzieje logowali się do banku i transferowali pieniądze na swoje konta, zakładane na podstawie fałszywych dokumentów. Oczywiście z tych rachunków pieniądze były natychmiast pobierane. Całe zdarzenie miało miejsce w banku, który oferuje dostęp przez internet bez stosowania bezpiecznych metod uwierzytelnienia, takich jak tokeny lub hasła jednorazowe. Trudno powiedzieć, że banki wyciągnęły jakiekolwiek wnioski z tej lekcji za 1 milion zł, bo w dalszym ciągu na przykład logowanie do konta przy pomocy hasła i bez dodatkowej autoryzacji przelewów stosuje m.in. Citibank Handlowy. Dwa hasła, co prawda różne, do logowania i do przelewów są stosowane przez Millennium, Kredyt Bank i BPH, ale z punktu widzenia przestępców nie jest to żadnym utrudnieniem.

Piotr Walas, dyrektor techniczny Panda Software Polska:

– Ataki na właścicieli kont Inteligo nie były pierwszymi i zapewne nie ostatnimi tego typu. Okradanie kont stało się dla wielu cyberprzestępców sposobem na zarabianie. Tym bardziej, że dysponują oni coraz doskonalszymi narzędziami, które coraz rzadziej wymagają specjalistycznej wiedzy. Kilka dni przed atakiem na użytkowników kont Inteligo atakowani byli klienci mBanku. W obu przypadkach podający się za obsługę banku przestępcy rozsyłali e-maile, w których prosili o kliknięcie na link i podanie poufnych danych. To klasyczny przykład phishingu. Mimo że dużo się mówi o tej technice, to i tak wielu użytkowników internetu daje się „złowić". Spora grupa klientów chyba nadal nie wie, że banki nigdy nie proszą o podawanie poufnych danych przez internet. Cyberprzestępcy skrzętnie wykorzystują tę niewiedzę i rozsyłają do potencjalnych ofiar listy, które zawierają linki przekierowujące do spreparowanych stron WWW, na których ofiary będą zostawiać poufne dane. Są to strony, które wyglądają identycznie jak serwisy internetowe banków, więc klient banku, który nie podejrzewa podstępu wpisuje wszystko, o co „prosi" przestępca. Najczęściej są to numery kont, loginy i hasła. Phishing jest coraz popularniejszy wśród przestępców, ponieważ zapewnia dużą anonimowość. Podrobione strony WWW umieszczone są zwykle na serwerach w egzotycznych krajach lub jeszcze częściej na botnetach. Podobnie jest też z wysyłaniem fałszywych e-maili, które odbywa się z użyciem botnetów lub niezabezpieczonych serwerów pocztowych.

Marek Kłuciński, rzecznik prasowy PKO BP:

– Przypadki fal ataków typu phishing są sporadyczne. W ciągu minionego roku odnotowaliśmy w PKO BP dwie takie fale. Skala zgłoszonych przez klientów zauważonych incydentów łącznie nie przekroczyła 0,5 promila ogólnej liczby klientów bankowości elektronicznej.

Jeśli chodzi o poniesione przez klientów straty, to pragnę podkreślić, że żaden z klientów jak dotąd nie zgłaszał nam strat finansowych poniesionych w związku z atakami phishingowymi. Od klientów nie otrzymaliśmy również żadnych skarg czy roszczeń w związku z tymi atakami.

Jednocześnie pragnę poinformować, że bank prowadzi szeroko zakrojoną akcję uświadamiającą klientów. Informacje na ten temat są na stronach WWW, prowadzimy też akcję telefoniczną, mającą na celu podniesienie świadomości klientów zarówno co do możliwości wystąpienia takich zagrożeń, jak i mającą na celu edukowanie klientów odnośnie podstawowych zasad bezpieczeństwa sieci internetowych. Zachęcamy też do używania oryginalnego oprogramowania, które umożliwia automatyczną aktualizację i instalację łat, wyjaśniamy znaczenie programów antywirusowych i zasady ich działania, przestrzegamy przed podawaniem danych poufnych w odpowiedzi na e-maile lub telefony. Zachęcamy do kontaktowania się z bankiem w przypadkach wzbudzających niepokój klientów.

Nie jestem klientem

W piątek rano przeglądając skrzynkę mojej elektronicznej poczty trafiłem na korespondencję, która trafiła do skrzynki w czwartek (23 sierpnia) przed północą (23.08) i wyglądała tak:

Data: 21: 08: 2007
Od: Inteligo <info@inteligo.pl>
Odpowiedz: Inteligo <info@inteligo.pl>
Do: lpiesik@gb.pl
Temat: Wprowadzenie nowych zabezpieczen.

Wprowadzenie nowych zabezpieczeń tożsamo¶ci.
Informujemy, że Twoje konto będzie poddane nowej procedurze weryfikacji.
W tym celu prosimy o jak najszybsze zalogowanie kilikaj? c w link poniżej.
Aby nowe zabezpieczenia zaczęły funkcjonować, należy potwierdzić swoj? tożsamo¶ć.
Do tego czasu wszystkie opcje w twoim koncie bed? zablokowane.
(Cała procedura trwa kilka minut)

https://secure. inteligo. com. pl/? verification_code=6ywkcj0766153y2s42hjuu77hjbxrg4492mnpnt593e9d8ntzh&request_ssl=yes&secure=yes&op_code=012.
Pozdrawiamy,
Inteligo

Prosimy nie odpowiadać na tę wiadomo¶ć. Wiadomo¶ci przesyłane na tę skrzynkę e-mail nie s? czytane, a serwis Inteligo nie odpowiada na nie. Aby uzyskać pomoc, zaloguj się do swojego konta Inteligo i kliknij ł?cze Pomoc.

Ponieważ codziennie usuwam z poczty co najmniej kilkanaście różnych ofert i propozycji, które trafiają do mnie jako spam, więc nie zrobiło to na mnie specjalnego wrażenia i już miałem rutynowo całą korespondencję umieścić w koszu, ale moją uwagę zwróciło to, że zostałem uznany przez bank za ich klienta chociaż tak nie jest. Czytając taką korespon- ▸▸

dencję właściwie nie jest trudno zorientować się, że jest to próba uzyskania informacji (danych) pod pretekstem aktualizacji. Przede wszystkim:

- wszystkie banki wyraźnie informują, że nigdy nie kontaktują się ze swoimi klientami tylko i wyłącznie za pośrednictwem poczty elektronicznej (jak wyżej);
- gdyby była potrzeba weryfikacji danych, bank nie przeprowadzałby jej przez internet w takiej formie;
- podejrzenie powinien wzbudzić pośpiech (prosimy o jak najszybsze zalogowanie);
- stwierdzenie, że „Cała procedura trwa kilka minut" ma skłonić odbiorcę do tego, aby prośbę spełnił natychmiast logując się „kilikając w link poniżej". Oczywiście jest to inny adres niż ten, z którego korzysta się w normalnych kontaktach...

Warto też zwrócić uwagę na ostatni fragment tego e-maila z tekstem: Prosimy nie odpowiadać na tę wiadomość. Wiadomości przesyłane na tę skrzynkę e-mail nie są czytane. – Oczywiście, bo nie o nie chodzi, za to jeszcze raz przestępcy namawiają adresata: zaloguj się do swojego konta Inteligo i kliknij łącze Pomoc – to oczywiście na wszelki wypadek, gdybym miał wątpliwości, czy powinienem potwierdzić swoją tożsamość i inne dane.

W tym e-mailu rzucało się w oczy również to, że były problemy z kodowaniem polskich znaków. Warto przy tym zwrócić uwagę, że przestępcy nie popełnili już takiego błędu, jak nieudolne tłumaczenie jakiegoś zagranicznego tekstu, tak jak to było w pierwszych atakach przeprowadzanych w Polsce w naszym ojczystym języku. A było to tak:

„Wraz z dniem 14.06.2007,
Organizacja Visa, jeden z głównych wydawców kart kredytowych i debetowych na świecie, rozporządził nową ustawę dla Europejskich Systemów Bankowości.
Tym samym zobligował Polskie Banki do weryfikacji swoich klientów, jako właściwych posiadaczy kart kredytowych i debetowych. Cały proces weryfikacji ma na celu poprawienie bezpieczeństwa oraz zmniejszenie nadużyc związanych z płatnościami on-line. Dla każdego użytkownika, zostanie wygenerowane specjalne hasło oraz prywatny klucz, dzięki czemu osoby trzecie nie będą miały dostępu do poufnych informacji.
Klient który zostanie poproszony o weryfikacje, lecz się z niej nie wywiąże, może liczyć się z zablokowaniem numeru karty.
Naciśnij przycisk „Weryfikacja" w celu dokonania weryfikacji.
(Cały proces weryfikacji trwa do kilku minut)
Dziękujemy za poświęcony czas.
Listę Banków które prowadzą weryfikację znajdziejsz na stronie:
http://www.visa.pl/wydawcykartvisa/"

Warto też uświadomić wszystkim użytkownikom internetu (nie tylko klientom banków), że nie ma absolutnej ochrony przed przestępcami, a więc najlepszym zabezpieczeniem jest własna przezorność. Nie ulegajmy też złudzeniom, że Polska jest krajem szczególnym, bezpiecznym. Przestępcy sieciowi nie muszą przekraczać granic, co jest dla nich atutem, a dla nas dodatkowym zagrożeniem. I nie jest dla nas pocieszeniem, że to brytyjscy klienci amerykańskiego banku MBNA zostali zaatakowani przez oszustów za pośrednictwem poczty elektronicznej. Oczywiście konieczne było zalogowanie się na fałszywej stronie banku w związku z rzekomymi zmianami w systemie zabezpieczeń. Sprawa z MBNA jest najświeższym przykładem ataku typu „phishing" na klientów brytyjskich banków wykryta i nagłośniona przez SurfControl, firmę która dostarcza rozwiązania do filtrowania spamu.

Ochrona

Przeciwdziałanie phishingowi to przede wszystkim profilaktyka i informowanie o zagrożeniu. Użytkownicy internetu powinni nabrać pewnych prostych nawyków. Świadomy i rozsądny internauta jest zupełnie odporny na phishing również dlatego, że producenci oprogramowania antywirusowego rejestrują próbki phishingu i dodają je do bazy sygnatur zabezpieczeń, które służą do monitorowania przesyłanych e-maili. Porównują je z fragmentami kodów i oznaczają listy na podstawie zdefiniowanych w filtrach antyspamowych reguł jeszcze zanim znajdą się one w skrzynce adresata. Programy antywirusowe mają także funkcję blokowania adresów URL, pod którymi może znajdować się niebezpieczna zawartość – warto z nich skorzystać.

Współcześni przestępcy korzystają z botnetów, czyli sieci komputerów,

Filip Demianiuk, Technical Channel Manager – Trend Micro:

– Nowym narzędziem różnorodnych złośliwych działań jest botnet, czyli sieć maszyn zainfekowanych złośliwym oprogramowaniem. One zostały zidentyfikowane jako główna przyczyna phishingu, groźnej odmiany spamu. Trend Micro oferuje nie tylko swoim klientom, ale wszystkim użytkownikom internetu ochronę – Web Reputation Services – czyli usługę określającą reputację witryn internetowych, oraz umożliwiającą, w czasie rzeczywistym, blokowanie dostępu do witryn niebezpiecznych. Kilkaset serwerów, które skanują sieć, na bieżąco analizuje witryny internetowe, pod kątem ponad 50 różnych charakterystyk, między innymi treści, przechowywanych plików i odnośników do innych stron internetowych, które mogą stanowić zagrożenie. Analizowane są również informacje o lokalizacji witryny, zmienności miejsca jej rejestrowania i wiele innych. Po przeprowadzeniu tych testów systemy określają reputację witryny. Na jej podstawie, podczas próby odwiedzenia niebezpiecznej strony internetowej, dostęp do niej może zostać automatycznie zablokowany. Równocześnie użytkownik oprogramowania może zostać poinformowany, jakie zagrożenie niesie za sobą odwiedzenie tego adresu.

Tę technologię wykorzystujemy w produktach chroniących komputery firmowe (OfficeScan 8), komputery domowe (PcCillin) i firmowe bramki internetowe (rodzina produktów InterScan – IGSA, IWSA, IWSS). Z tej samej technologii korzysta również nasza darmowa wtyczka do przeglądarek internetowych (TrendProtect), ostrzegająca internautów o niebezpieczeństwach surfowania po sieci. Ponadto Trend Micro rozszerza ochronę przed phishingiem na serwery pocztowe, przez dedykowane pliki z sygnaturami, zawierające informacje o adresach witryn wykorzystywanych do phishingu. W ten sposób nie tylko uniemożliwimy potencjalnej ofierze odwiedzenie niebezpiecznej strony, ale zablokujemy samą wiadomość e-mail, zachęcającą do jej odwiedzenia, jeszcze zanim wiadomość ta trafi do skrzynki pocztowej.

nad którymi przejęli kontrolę za sprawą internetowego robaka lub trojana, którego naiwny użytkownik sam sobie zainstalował. Komputery, które znalazły się w tej sieci (tzw. zombie), posłusznie wykonują polecenia, a trzeba zaznaczyć, że największe zarejestrowane do tej pory botnety składały się z kilkudziesięciu tysięcy komputerów, a więc moc jaką dysponują przestępcy jest ogromna. Na przykład ataki typu DDoS (Distributed Denial od Service) są tym skuteczniejsze, im większa jest sieć zombie, ale do tworzenia fałszywych serwisów WWW i serwerów SMTP wystarczą znacznie mniejsze sieci, składające się nawet z kilkudziesięciu maszyn.

Phishing jest groźną i coraz bardziej powszechną formą spamu. Tylko w czerwcu 2006 roku botnety przyczyniły się do wysłania około 80 proc. spamu (o 30 proc. więcej niż rok wcześniej). Według najnowszych badań, spam stanowi już ponad 90 proc. korespondencji e-mail, trudno więc się dziwić, że jest to również jeden z głównych sposobów, jakimi przez internet dokonywana jest kradzież tożsamości firm i konsumentów. Dlaczego najczęściej banki (a właściwie ich klienci) są wybierane jako cel ataku? Odpowiedź wydaje się prosta: bo są to miejsca dające możliwość uzyskania dokładnych informacji o większej liczbie, nie spodziewających się niczego, klientów danej firmy i późniejszej kradzieży ich tożsamości. Typowy atak phishingowy składa się zwykle z dwóch części: autentycznie wyglądającego e-maila oraz fałszywej strony WWW.

Aby nie wzbudzać podejrzeń spam często zawiera profesjonalnie wyglądające wiadomości e-mail w formacie HTML, z użyciem logo firmy, jej kolorystyki, grafiki, stylu czcionki i innych charakterystycznych elementów. Korespondencja „gra na emocjach" i jest tak przygotowana aby:

- zmylić,
- zdenerwować
- podekscytować odbiorcę.

Typowe tematy wiadomości to:

- problemy z rachunkiem,
- zmiany na koncie,
- informacje dotyczące wznowienia ochrony,
- oferty nowego produktu lub usługi.

Odbiorca takiej wiadomości reaguje szybko. Klika na wysłany w wiadomości link, który kieruje go na zainfekowaną, specjalnie przygotowaną przez napastników stronę WWW. Jej zawartość, wraz z treścią wiadomości e-mail, ma przekonać ofiarę do ujawnienia poufnych informacji, takich jak:

- nazwa użytkownika,
- hasło,
- numery kart płatniczych lub kredytowych
- numery PIN kart magnetycznych lub szczegóły dotyczące kart kredytowych.

Fałszywa strona WWW jest łudząco podobna do prawdziwej. Często ma logo firmy, pod którą podszywają się przestępcy, grafikę, styl pisma, czcionkę i inne elementy strony, którą kopiuje. Może również zawierać graficzny interfejs użytkownika (GUI), aby skłonić użytkownika do podania informacji dotyczących rachunków bankowych, numerów kart kredytowych, haseł lub innych danych.

Warto pamiętać, że dopóki nie wyrobimy w sobie nawyku ochrony własnych danych, tak długo nie będziemy bezpieczni, bo zagrożenie nie przestanie istnieć. •

Środki ostrożności

- Korzystaj z bezpiecznych programów i upewniaj się, że strona internetowa, którą odwiedzasz jest bezpieczna (ikona kłódki, adres URL, rozpoczynający się od https://).
- Korzystaj z własnego komputera. W internetowej kafejce czy innym miejscu publicznym nigdy nie wiadomo, jakie oprogramowanie jest tak naprawdę zainstalowane.
- Nigdy nie należy odpowiadać na e-maile, których autorzy proszą o ujawnienie czy zweryfikowanie danych osobowych lub dotyczących konta bankowego, nigdy nie klikać w znajdujące się w tych e-mailach linki.
- Zawsze gdy dostajesz e-mail od banku, warto zadzwonić do banku i spytać, czy ktoś coś do nas wysyłał. Jeżeli nie, zawsze od razu zgłoś próbę oszustwa.
- Zawsze na stronę banku wchodzić ze znanego sobie adresu, zawsze wpisywanego samodzielnie w pole adresu przeglądarki.

AKTUALNOŚCI

SurfControl udostępnił nową wersję oprogramowania Enterprise Threat Shield. do ochrony stacji roboczych w przedsiębiorstwach.

LG wprowadza na nasz rynek 20" monitor panoramiczny TFT LCD z czasem reakcji 2 ms GtG, szerokim kątem widzenia – 170 stopni (pion i poziom), o jasności 300 cd/mkw. i kontraście 3000: 1 DFC.

SanDisk® Corporation przedstawiła atrakcyjną stację USB Flash SanDisk Extreme® Ducati Edition. Stacja ma pojemność 4 GB oraz szybkość odczytu i zapisu 20 megabajtów na sekundę.

Ricoh Polska wprowadza do oferty nowe modele faksów standardu Super G3, wyposażonych w najwyższej klasy zabezpieczenia – FAX3320L i FAX4430NF.

Quantum zaprezentował nowy system do backupu i replikacji danych. Platforma DXi-7500 została zaprojektowana dla przedsiębiorstw o rozproszonej strukturze.

EMC Corporation rozszerzyła swoją ofertę m.in. o nową serię systemów pamięci masowej klasy wyższej EMC® Symmetrix® DMX-4 oraz wieloprotokołowe systemy pamięci masowej EMC Celerra® NS20 i NS40.

PBG S.A. rozpoczęło wdrażanie systemu Oracle E-Business Suite (EBS), jako głównego systemu ERP do obsługi spółki. Wdrożenie prowadzą konsultanci Oracle Polska wspierani przez 30 specjalistów PBG.

P4, właściciel marki PLAY kupił technologię Oracle jako platformę bazodanową dla swoich systemów IT. Na bazie danych Oracle w P4 działa już: system bilingowy, ERP oraz portal i hurtownia danych.

Motorola będzie prawdopodobnie pierwszym producentem telefonów komórkowych z miniaturowym projektorem. PicoP został zbudowany przez Microvision w oparciu o chip Texas Instruments.

Passus wprowadził na polski rynek nową wersję oprogramowania AirMagnet Laptop Analyzer 7.5, które umożliwia dekodowanie i analizę sieci Wi-Fi 802.11n.

Opracował Lech Piesik