PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1156 — 2007
Informatyka Ekonomiczna 11

Andrzej Małachowski, Krzysztof Szymczak

NARZĘDZIA I TECHNIKI PHISHINGU

1. Wstęp

Otwarta przestrzeń sieci telekomunikacyjnych i teleinformatycznych, w tym Internetu, stanowiąca obszar aktywności e-biznesowych, przynosi szereg zagrożeń bezpieczeństwa realizowanych operacji. Rosnąca z roku na rok liczba użytkowników sieci, liczba realizowanych transakcji, wartość wolumenu obrotów finansowych pociąga za sobą również nasilenie się działań o charakterze przestępczym. W pracy [Małachowski 2005, s. 214-216] wskazano na podstawowe źródła (**podmioty**) niebezpiecznych dla użytkowników (przedsiębiorstw) przejawów funkcjonowania Internetu, którymi są m.in.:

- nierzetelni dostawcy sprzętu i oprogramowania,
- nierzetelni dostawcy oferowanych usług internetowych,
- nierzetelne przedsiębiorstwa i inne podmioty działające w przestrzeni internetowej, niezapewniające odpowiedniego poziomu bezpieczeństwa transakcji realizowanych z nimi lub za ich pośrednictwem,
- profesjonalni entuzjaści i hobbyści nowych technologii (np. hakerzy),
- przestępcy oraz grupy i organizacje przestępcze,
- inni użytkownicy.

Podstawowe zagrożenia wynikające z aktywności tych podmiotów, które musi brać pod uwagę i przed którymi powinien się odpowiednio zabezpieczyć użytkownik (przedsiębiorstwo), dotyczą m.in.:

- systemowych niedostatków i luk w sprzęcie i oprogramowaniu („dziury" w oprogramowaniu, montowane tylne drzwi, niedostateczny poziom ochrony, przenoszone w tym oprogramowaniu wirusy komputerowe (!) itp.),
- ułomnych, niewłaściwie zabezpieczonych rozwiązań sprzętowo-programowych oferowanych usług, nieetycznego podglądania aktywności użytkownika, propagacji w tym oprogramowaniu wirusów komputerowych,
- występujących w e-przedsiębiorstwach słabych zabezpieczeniach działających sieciowych systemów informatycznych, nierzetelnych pracowników tych przedsiębiorstw, fikcyjnych przedsiębiorstw (fikcyjne witryny) lub unikających wypełnienia swych zobowiązań wobec użytkownika,

- włamań do systemów i aplikacji użytkownika, kradzieży danych, w tym szczególnie „wrażliwych" i chronionych (numery kont, numery kart płatniczych, identyfikatory itp.), stosowania oprogramowania „węszącego", szpiegowskich agentów programowych, podszywania się pod użytkownika,
- ataków na konta bankowe, zwłaszcza za pomocą kart płatniczych, przekierowywania transakcji (opłaconych dostaw towarów),
- rozpowszechniania wirusów komputerowych we wszelkiego rodzaju dostępnych formatach plików,
- zalewania kont pocztowych niechcianą korespondencją (spam),
- propagowania treści nieobyczajnych, wulgarnych, obraźliwych,
- działań o charakterze przestępstw seksualnych,
- propagowania przemocy, antysemityzmu, faszyzmu, terroryzmu itp.

W bogatym leksykonie tych zagrożeń odnajdziemy także takie terminy, jak (por. [Ciesielczyk, Watras 2005, s. 109, 110]):

- **hacking** – przełamywanie systemów ochrony, najczęściej dla wykazania ich słabości; hakerzy kierują się swoistą etyką i oprócz pozostawienia śladów włamania nie wyrządzają większych szkód,
- **cracking** – przełamywanie haseł lub kluczy kryptograficznych, poprzez generowanie kolejnych wzorców, aż do momentu „trafienia"; zwykle związane jest z wyrządzaniem szkód,
- **phreaking, dialing** – podszywanie się pod numer dostępowy użytkownika (przez sieć telefonii stacjonarnej lub komórkowej) i wykorzystywanie go do własnych celów; niekiedy szkody (koszty fałszywych połączeń) mogą być znaczne,
- **sniffing** – podsłuchiwanie transmisji w celu przechwycenia haseł, identyfikatorów itp.,
- **phishing**[1] – technika wyławiania poufnych danych transakcyjnych (banki, sklepy, płatności); fałszywe e-maile z żądaniem potwierdzenia danych (numery kont, numery kart, dane osobowe itp.), fałszywe strony (sklepów, banków, płatności itp.),
- **web.hijacking** – przekierowywanie klienta na strony fałszywych sklepów, banków, dostawców usług itp.,
- **spoofing** – podszywanie się pod autoryzowany host lub serwer, poprzez łamanie ich zabezpieczeń, przekierowanie w konsekwencji użytkownika na fałszywe strony (por. *phishing*),
- **carding** – posługiwanie się skradzionymi numerami kart płatniczych, wykorzystywanie imitujących je (fałszywych – o prawdziwych danych) kart,
- **spaming** – wysyłanie setek tysięcy e-maili (zwykle reklamowych) na przypadkowe adresy użytkowników (przedsiębiorstw), w większości krajów prawnie zabronione,

[1] Co oznacza „na przynętę", „na rybkę" (przekształcone słowo ang. *fishing*).

- **mailbombing** – atakowanie wybranych serwerów i hostów setkami tysięcy e-maili, aż do ich całkowitego zablokowania,
- **Google bombing** – w darmowych portalach tworzy się prywatne „niby-strony" które z danej frazy (zwykle obraźliwej lub fałszywej) odsyłają na oficjalną witrynę firmy, organizacji czy też prywatnej osoby; nadużywa się tu mechanizmu wyszukiwarki, która porządkuje wyniki poszukiwań według liczby odnośników do danej (tj. oficjalnej) strony. Google bombing może być wykorzystane jako narzędzie nieetycznej walki konkurencyjnej, czego dowodzi m.in. przykład takich działań wobec znanego światowego lidera oprogramowania, na którego stronę kierowała fraza „gorszy od samego szatana",
- **spyware** – oprogramowanie szpiegujące, monitorujące pracę użytkownika; przynosi szczególne szkody przez przechwytywanie haseł, identyfikatorów, numerów kont, jednocześnie zbiera informacje o rodzajach aktywności klienta (adresy, słowa kluczowe, preferencje itp.). Należą do niego również szpiegujące agenty programowe,
- **dialery** – programy „przekierowujące" połączenia (najczęściej w sieciach operatorów telefonii stacjonarnej, przewodowej), instalują się jak wirusy (np. po operacji „kliknij tu").

W większości przypadków wszystkie te zagrożenia prowadzą do znacznych strat finansowych. Musimy przy tym pamiętać, że największe zagrożenia, niosące ponad 70% strat finansowych powyżej 100 tys. USD, powodują pracownicy (aktualni lub byli) firm sfery e-biznesu [Małachowski 2005].

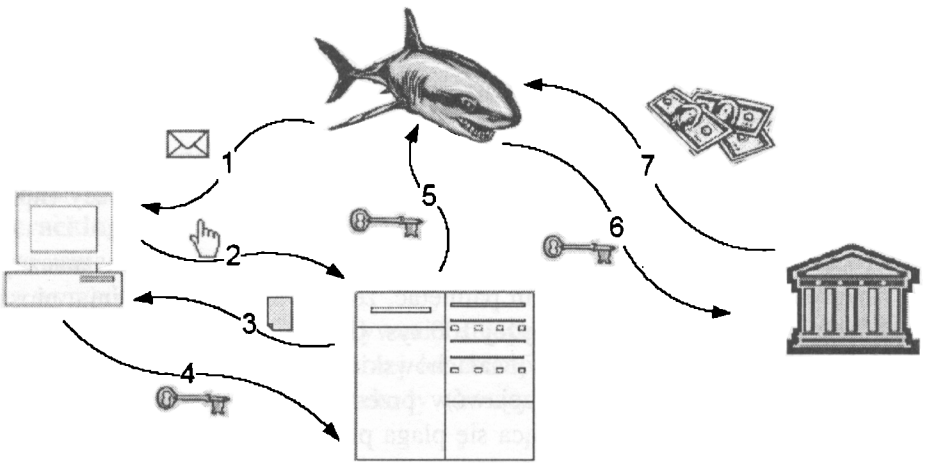
Jednym z najgroźniejszych przejawów przestępczości w zakresie e-biznesu (zwłaszcza internetowej) jest szerząca się plaga phishingu. Co ważniejsze, prawie 90% tego rodzaju przestępstw dotyczy operacji i instytucji finansowych [Anti Phishing... 2005]. Według dostępnych danych [Małachowski 2005, s. 220, 221] w USA przeciętny amerykański internauta traci w wyniku phishingu ponad 100 USD rocznie. Straty banków amerykańskich przekraczają według szacunków kwotę 100 mln USD rocznie. Łącznie, rocznie kwoty przechwytywane przez phisherów szacowane są na ok. 3 mld USD! [„Community Banker"... 2005; Gartner 2005]. Ta ogromna skala strat oraz samego zjawiska phishingu jest wyraźnie zaniżona. Pozostaje „ciemna" liczba udanych ataków phisherów nieujawnianych przez przedsiębiorstwa, zwłaszcza banki, z obawy o utratę reputacji i klientów [Pawlak, 2006]. Wykrywa się dziesiątki milionów (!) codziennych prób ataku tymi technikami [Anti Phishing... 2005]. Rośnie systematycznie liczba stron pojawiających się miesięcznie w Internecie związanych z tym rodzajem przestępczości: w grudniu 2004 r. było ich 1707, zaś w grudniu 2005 r. już 7197 [Anti Phishing... 2005]. Niestety, wraz z rozwojem technologii e-biznesowych (internetowych) obserwujemy stały postęp w doskonaleniu narzędzi i technik tej formy przestępczości. W naszych rozważaniach zaprezentujemy wybrane (by nie powiedzieć – najnowsze czy też najważniejsze) z nich. O skali zjawiska phishingu niech świadczy fakt, że powołano specjalną grupę roboczą do jego badania i profilaktyki

(Anti Phishing Work Group), z własną stroną internetową www.antiphishing.org, na której publikowane są bogate materiały z tej dziedziny.

2. Przegląd wybranych narzędzi i technik phishingu

Ogólnie phishing polega na „nęceniu" w różnorodnej formie użytkownika (przedsiębiorstwo) i powodowanie, by udostępniał w sposób świadomy lub nieświadomy swoje „wrażliwe" i poufne dane: loginy, hasła, numery kont, kart płatniczych i szereg innych istotnych danych.

Schemat ataku phishera pokazano na rys. 1.



Rys. 1. Schemat ataku phishera

Źródło: www.antiphishing.org.

Przestępcy (tzw. phisherzy) wykorzystują w celu manipulowania użytkownikiem przede wszystkim metody inżynierii społecznej oraz właściwości technologii e-biznesowych (w tym internetowych). Szczególnie groźne dla użytkowników i przedsiębiorstw są stosowane tu hybrydy tych metod[2]. Atakujący kontaktują się z ofiarą drogą elektroniczną (najczęściej przez e-mail lub SMS). Podstawowe przygotowania phishera do ataku obejmują: sporządzenie fałszywej wiadomości e-mail (SMS), spreparowanie fałszywej strony (serwisu) www, zarejestrowanie bliźniaczych domen, opracowanie *badware*. Poszczególne kroki w schemacie ataku są następujące:

1. Phisher wysyła informację (e-mail, SMS) do swojej ofiary. Jednym ze sposobów rozprzestrzeniania się tych wiadomości jest używanie botnetów i serwerów

[2] Psychologicznym podłożem phishingu jest łatwowierność, naiwność lub niewiedza użytkowników.

zombi[3] wysyłających spam do losowo wybranych użytkowników. Występujące tu ryzyko „nietrafienia" przez phishera na osobę zarejestrowaną w systemie, który zamierza zaatakować, jest kompensowane ogromną liczbą spamów. Znacznie skuteczniejszym sposobem dla phishera jest pozyskanie adresu przez sprawdzanie na stronach organizacji rejestrujących adresy użytkowników (np. banki, e-sklepy, e-aukcje). Phisher próbuje założyć nowe konto, podając jako adres e-mail (znany lub losowo sporządzony) adres ofiary. Systemy poczty eliminują próby zakładania kont o tym samym adresie przez tego samego użytkownika lub różnych użytkowników. W odpowiedzi przekazują informację, że taki adres jest już zarejestrowany i proszą o podanie innego. Phisher uzyskuje pewność, że dany użytkownik jest zarejestrowany np. w e-sklepie, banku. Wie zatem, że wysyłając wiadomość do potwierdzonego klienta (e-sklepu, banku), zwiększa szansę jego odpowiedzi na swój spreparowany e-mail. Według badań Anti Phishing Work Group (2005) dziennie na tzw. phishing e-mails pozytywnie odpowiada 6% użytkowników (tj. ponad 4,5 mln osób!).

2. Użytkownik podejmuje nieświadome działanie w odpowiedzi na e-mail, co grozi mu utratą danych. Typowymi takimi działaniami w odpowiedzi na atak phishera są: otworzenie załącznika instalującego złośliwe oprogramowanie na komputerze ofiary, wizyta na spreparowanej stronie przez wykorzystanie odnośnika w wiadomości phishera czy też wizyta na stronie zmienionego (fałszywego) adresu DNS.

3. Następnie użytkownik jest proszony o podanie poufnych danych. Procedura ta jest uruchamiana na prawidłowej stronie instytucji (opanowanej przez phishera) z wykorzystaniem programów logujących treść pisaną przez użytkownika, na spreparowanym serwerze lub z zainstalowanych na komputerze użytkownika webowych trojanów.

4. Niczego nieświadomy użytkownik ujawnia poufne informacje, przekonany, że działa prawidłowo, wedle zaleceń swojej instytucji. Po tym kroku jego prywatne dane są dostępne na serwerze atakującego.

5. Pozyskane informacje są przesyłane do phishera. Odbywa się to za pośrednictwem spreparowanego serwera lub bezpośrednio z komputera ofiary (w zależności od stosowanej techniki).

6. Phisher wykorzystuje pozyskane dane i podając się za użytkownika, dokonuje przestępczych operacji w celu osiągnięcia określonych korzyści (finansowych lub rzeczowych): kradzieży pieniędzy z konta banku, nielegalnych płatności, przejęcia dostawy z e-sklepu (aukcji, innych transakcji), korzystania z płatnych serwisów internetowych, sprzedaży danych osobowych itd.

7. Nielegalnie pozyskane korzyści trafiają do phishera.

Przedstawimy teraz wybrane narzędzia i techniki działania phisherów.

[3] Sieć przejętych logicznie i kontrolowanych przez atakującego komputerów.

3. Współczesne narzędzia i techniki phishingu

Platformami działania phisherów mogą być wszelkie technologie telekomunikacyjne i teleinformatyczne: tradycyjne sieci telekomunikacyjne, sieci telefonii komórkowej, sieci komputerowe, w tym Internet. Sygnały od phisherów mogą napływać via systemy *call center*, CRM, CSM, CSS, C/DSS (zob. [Małachowski 2005, s. 122-136]), lub ze stron (serwisów www) instytucji, z którymi współpracuje użytkownik (banków, sklepów, aukcji, serwisów finansowych, płatniczych i innych usług internetowych). Nowym kanałem komunikacyjnym opanowanym przez phisherów jest dostęp mobilny i sieć telefonii komórkowej (TK). Będzie o tym mowa w dalszej części naszych rozważań. Podstawową platformą pozostaje jednak Internet.

Do najczęściej stosowanych internetowych narzędzi i technik phishingu należy zaliczyć m.in. (por. [The Honeynet Project... 2005, 2005a, 2005b]):

- autentyczną stronę (serwis) instytucji opanowaną przez phishera,
- fałszywą stronę (serwis) instytucji, z którą współpracuje użytkownik,
- multiplikowanie fałszywych stron (serwisów),
- bliźniacze (podobne) domeny,
- podstawienie autentycznego adresu na fałszywej stronie,
- przekierowanie przez adresy IP,
- zamianę tablic kodów znaku w IDN (*International Domain Name*),
- podszywanie się pod serwery DNS (tzw. pharming),
- operacje w hierarchii serwerów DNS,
- podglądanie przez fałszywe serwery proxy (pośredniczące),
- przekierowanie poprzez pliki systemowe,
- wykorzystanie technologii mobilnych,
- wykorzystanie *badware* (złośliwego oprogramowania).

Przedstawimy je pokrótce.

Autentyczne strony (serwis) instytucji **opanowane przez phishera** są najwyższą kategorią tego typu przestępczości. Ich zastosowanie wymaga przełamania systemu zabezpieczeń danej instytucji, dyskretnego przeprojektowania stron (witryn) serwisu. Zmiany w autentycznej stronie dotyczą zwykle przekształceń w menu otwarcia[4], sposobów i miejsc nawigowania, akcji użytkownika (oferowanych usług) itp. Najczęściej tym sposobem atakowane są strony słabo zabezpieczone, rzadko monitorowane przez administratorów systemów, o relatywnie niewielkiej liczbie wejść (mało aktywne) i przeciwnie – strony o masowym strumieniu wejść (np. kilkaset tysięcy w ciągu dnia). W tym drugim przypadku nawet krótkotrwałe opanowanie autentycznej strony przez phishera przynosi mu setki czy tysiące „złowionych" klientów.

Fałszywe strony (serwis) instytucji, z którą współpracuje użytkownik, są jednym z pierwszych i najczęściej stosowanych narzędzi wykorzystywanych przez

[4] Na przykład przez instalowanie okienek pop-up.

phisherów. Podrabiają oni stronę (serwis) oryginalną, przesyłają w poczcie sfałszowaną (z wyglądem zbliżonym do oryginału) wiadomość od instytucji współpracującej z klientem i przez link w tej poczcie przekierowują klienta na sfałszowaną stronę. W treści wiadomości phisher podaje rzekome, istotne przyczyny konieczności kontaktu z instytucją (zmiany: numerów kont, pinów, haseł; weryfikacja danych, uzgadnianie sald, płatności itp.). Bardziej wyrafinowane fałszywe oferty dotyczą przyznawanych bonusów, wyróżnień, nagród, kart „specjalnego" klienta itp. W nakłanianiu klienta do reakcji na fałszywą wiadomość korzysta się z technik wywierania wpływu na ludzi. Badania pokazują (Anti Phishing... 2005), że rozstrzyga kilka pierwszych sekund po przeczytaniu fałszywej wiadomości. Jeśli użytkownik nie zdecyduje się w tym czasie na kliknięcie na podany fałszywy odnośnik, nie zrobi tego nigdy. Bogate archiwum phishing e-mails zawierające rzeczywiste przykłady stosowanych technik (treści) nakłaniania można znaleźć pod adresem: www.antiphishing.org/phishing_archive.html.

W technice **multiplikowania fałszywych stron (serwisów)** phisher zabezpiecza się przed usunięciem fałszywych stron przez administratorów systemów poprzez ich lokowanie na wielu różnych serwerach w sieci. Wabiony klient jest przekierowywany automatycznie[5] na fałszywą stronę kolejnego serwera. Według badań APWG (2005) średnio przez 5,3 dnia fałszywa strona jest dostępna w Internecie! Obrazuje to dobrze skalę zagrożeń phishingiem. Technika multiplikowania fałszywych stron wydłuża okres, w jakim możemy zetknąć się z takimi stronami. Zwiększa się tym samym skala przestępstw phishera.

W swej działalności phisherzy wykorzystują również zarejestrowane **bliźniacze (podobne) domeny**. Nazwy tych serwisów są na pierwszy rzut oka bardzo podobne do oryginalnych. Potwierdzają to przykłady (czcionka Times New Roman): www.paypa1/ miejsce poprawnej www.paypal; www.a11egro, zamiast www.allegro; www.wbkbz zastępująca www.bzwbk itp. Pod bliźniaczą domeną funkcjonuje „serwis" phishera.

Do **podstawiania autentycznego adresu na fałszywej stronie** korzysta się w phishingu z kodów JavaScript modyfikujących treść paska adresu. Podczas wizyty klienta na fałszywej stronie w oknie przeglądarki będzie się pojawiał podstawiony adres poprawnej strony instytucji [Kaminsky 2002]. Utwierdza on klienta w przekonaniu, że znajduje się na takiej (poprawnej) stronie i w serwisie.

W kolejnej technice **przekierowania przez adresy IP** po uruchomieniu wyszukiwania w pasku adresu wyszukiwarki pojawia się (fałszywy, zbliżony do autentycznego) adres IP instytucji klienta w miejsce nazwy strony (hosta). Dla dodania mu autentyczności rozszerzany jest o kolejne subdomeny zbliżone w nazwie do stosowanych przez daną instytucję, np. 62.129.43.106/nazwa/nazwa/SSL_secure_system[6]. Użytkownicy pomijają (bagatelizują) taką zamianę lub są przekonani, że są to chwilowe problemy techniczne. Trafiają na serwer phishera.

[5] Nosi nazwę *smart redirection* [RSA Security... 2006].

[6] Adres hosta jest wymyślony (może być prawdziwy!!!)

Zamiana tablic kodu znaku w IDN (*International Domain Name*) jest techniką polegającą na tym, że dla określonych znaków (np. w nazwie domen) następuje zamiana tablic kodowania, tzn. wybrany przez phishera znak ma inny kod niż reszta nazwy domeny. W IDN dostępny jest mechanizm umożliwiający stosowanie różnorodnych tablic kodowych (znaków międzynarodowych, tzw. *unicode*) w adresach stron www, co ułatwia wymianę informacji między serwerami DNS. Po takim zabiegu dokonanym przez phishera przykładowy adres www.pаypal.com[7] zostaje zakodowany w IDN jako www.xn--pypal-4ve.com (prawidłowy adres fałszywej strony) i wyświetlony użytkownikowi jako prawidłowy (!) www.paypal.com [Johanson 2005].

Podszywanie się pod serwery DNS (tzw. pharming) jest jedną z najnowszych technik stosowanych przez phisherów. Phisher przełamuje ochronę tych serwerów i podstawia pod adres prawidłowy, np. www.firma.subdomena.pl z odpowiadającym mu adresem IP, własny adres fałszywej, spreparowanej strony [Jeleśniański 2006]. Użytkownik nie jest świadomy, że nastąpiła taka zamiana.

Operacje w hierarchii serwerów DNS zalicza się do technik pharmingu[8]. W swej działalności przestępczej phisher wykorzystuje tu mechanizmy hierarchicznej struktury serwerów DNS [Albitz, Liu 1998; Haugsness 2005]. Atakujący phisher wysyła zapytanie o adres IP strony (witryny, serwisu) do jednego z serwerów DNS znajdującego się niżej w hierarchii (serwer A), ten z kolei kieruje pytanie o szukany adres do jednego z głównych serwerów DNS (serwer B). Phisher preparuje odpowiedź serwera B i dostarcza ją serwerowi A. Podany adres kieruje ruch na spreparowaną stronę. Mechanizm ten jest o tyle niebezpieczny, że serwery w celu przyspieszenia wyszukiwania lokują te fałszywe adresy w pamięci bufora i od tej pory przenoszą cały ruch z poprawnego adresu podanego przez użytkowników na serwer phishera. W ten sposób atakowani są wszyscy użytkownicy korzystający z określonego lokalnego serwera DNS.

W technice **podglądania przez fałszywe serwery proxy** phisherzy wykorzystują programowe serwery proxy (pośredniczące) wbudowane w kanał komunikacyjny pomiędzy klientem a jego instytucją. Użytkownik podaje dane na fałszywej stronie, które są przekazywane (via serwer proxy phishera) do serwera instytucji, serwer ten wysyła odpowiedź (poprzez fałszywy serwer proxy) do spreparowanego serwisu, który przekazuje dalej informacje użytkownikowi. Na serwerze proxy phisher może odczytywać dane, które użytkownik wysyła, nawet jeżeli są one w postaci zaszyfrowanej [Wikipedia... 2006].

W technice **przekierowania przez pliki systemowe** (zaliczanej niekiedy do pharmingu) phisherzy wykorzystują stosowane w sieciowych systemach operacyjnych pliki hosts służące m.in. przyspieszaniu komunikacji sieciowej. W nich są zapisywane m.in. adresy witryn najczęściej odwiedzanych przez użytkowników.

[7] Kod &#1072 odpowiada w *unicode* znakowi „?".

[8] Nie mylić z webfarmingiem.

Pliki te (zwykle ulokowane na komputerze użytkownika) są atakowane przez phishera np. przez dziury w systemie, a ich zawartość zmieniana tak, że użytkownik (wpisując poprawny adres) nieświadomie kierowany jest pod adres fałszywej strony.

Wraz z rozwojem i upowszechnianiem się **technologii mobilnych** phisherzy wykorzystują i te technologie do swej działalności przestępczej[9] [Vamosi 2005]. W technice tego rodzaju phishingu wykorzystuje się fałszywe (darmowe!) punkty dostępowe (hot-spot), o znacznie silniejszym sygnale od istniejących w pobliżu. Fałszywe hot-spoty phisherzy lokują (podobnie jak są instalowane autoryzowane) w miejscach o dużym natężeniu ruchu ludzi, takich jak centra handlowe, dworce i lotniska, centra rozrywki. Poprzez fałszywe hot-spoty i zainstalowane w nich programy węszące wszystkie dane, jakie wysyła użytkownik, są dostępne dla phishera. Możemy tymczasem się tylko pocieszać, że technika ta jest w fazie *in statu nascendi* i nie jest (na razie) powszechnie wykorzystywana przez phisherów.

Niezwykle bogaty arsenał środków w działalności przestępczej phisherów oparty jest na **wykorzystaniu** rozmaitego ***badware*** (złośliwego oprogramowania). Zgodnie z „regułami" phishingu mają wspólną cechę – służą przechwyceniu przez phishera „wrażliwych danych" z komputera użytkownika. Do tej klasy oprogramowania możemy zaliczyć zwłaszcza wymienione we wstępie: montowane tylne drzwi (tzw. konie trojańskie), oprogramowanie „węszące" (*sniffery*), oprogramowanie „szpiegujące" (*spyware*), a nawet specjalizowane funkcjonalnie agenty programowe. Najprostszym sposobem ich zainstalowania na komputerze użytkownika jest otwieranie przez nich załącznika do e-maila lub ściąganie z sieci plików ze stron www, zawierających wmontowane przez phisherów tego rodzaju oprogramowanie (lub tylko kody ich aktywowania). Pokrótce przedstawimy dwa przykłady najczęściej stosowanego przez phisherów oprogramowania „szpiegującego", z zaawansowanymi funkcjami typowymi dla agentów programowych. Pierwszym z nich jest oprogramowanie **monitorujące operacje klawiaturowe** użytkownika (tzw. *keyloggery*). Zapisują wszystkie znaki i operacje użytkownika wprowadzane z klawiatury. Zwykle liczba znaków i akcji klawiaturowych użytkownika jest znaczna – *keyloggery* mają możliwość filtrowania danych według ustalonych wzorców (ograniczając je do loginów, haseł, kont, pinów itp.) Działają w tle systemu i są dość trudne do wykrycia. Mają wbudowane (programowe) serwery poczty, za pomocą których przesyłają te dane do phishera. Drugim przykładem tego typu oprogramowania są **programy śledzące treści** (zawartość ekranów – tzw. *screenloggery*) w trakcie pracy użytkownika. Aktywowane są w rozmaity sposób: cyklicznie (w ustalonych odstępach czasu), na podany przez użytkownika określony adres (np. banku), rodzaj operacji (np. realizacja płatności), rodzaj aktywności na poprawnej stronie (np. klikanie na określone odnośniki). Doposażane są w mechanizmy filtrowania danych. Zapisują zawartości takich

[9] Określa się go mianem phishingu Wi-Fi.

ekranów (tzw. zrzuty) i przesyłają je do phishera w podobny sposób jak *key-loggery*.

4. Zakończenie

Przestępstwa phishingu, podobnie jak działalność hakerów czy propagowanie wirusów komputerowych, są, jak się wydaje, trwałym zjawiskiem, jakie nam towarzyszy podczas pracy w sieci. Pojawiły się stosunkowo niedawno, mają charakter masowy, stanowią poważne zagrożenie bezpieczeństwa, przede wszystkim operacji finansowych i innych transakcji realizowanych przez użytkowników (przedsiębiorstwa). Przynoszą nie tylko wymierne, bezpośrednie straty finansowe i materialne. Powodują konieczność ponoszenia dodatkowych nakładów na systemowe zabezpieczanie się przed plagą phishingu zarówno przez użytkowników, jak i przez przedsiębiorstwa. Szczególnie dla przedsiębiorstw, banków, instytucji finansowych, dystrybutorów w e-handlu udane ataki phisherów powodują niekiedy nieodwracalne skutki, jak zachwianie ich reputacji czy utratę klientów. Zagrożenie bezpieczeństwa powodowane phishingiem skłoniło np. do zmiany swego banku 6% klientów, a około 18% użytkowników zrezygnowało z zakupów w Internecie [Folsom i in. 2005]. Większe przedsiębiorstwa i korporacje realizują wspólne projekty mające na celu ochronę ich internetowej przestrzeni aktywności gospodarczej [Pawlak 2006a].

Musimy zdawać sobie z tego sprawę, że inwencja phisherów, podobnie jak „twórców" oprogramowania wirusowego, jest praktycznie nieograniczona. Pojawiają się i pojawiać się będą ciągle nowe generacje narzędzi i technik służących tego rodzaju przestępstwom.

Literatura

Albitz P., Liu C., *DNS and BIND in a Nutshell (3/e)*, O'Reilly & Associates Publ. 1998.

Anti Phishing Work Group *December Phishing Activity Trends Report*, http://www.antiphishing.org/reports/apwg_report_DEC2005_FINAL.pdf, 2005.

Ciesielczyk T., Watras G., *Bezpieczeństwo i-handlu*, [w:] *Wprowadzenie do i-handlu*, red. A. Małachowski, AE, Wrocław 2005.

„Community Banker", *Phishing in the Real World*, 2005.

Emigh A., *Online Identity Theft: Phishing Technology, Checkpoints and Countermeasures*, http://www.antiphishing.org/Phishing-dhs-report.pdf, 2005.

Folsom W.D., Guillory M.D., Boulware R.D., *Gone Phishing*, „Business & Economic Review" 2005.

Gartner Group (2005), Badania internetowe firmy Gartner 2005.

http://www.finextra.com/fullstory.asp?id=11778 oraz http://www.technologynewsdaily.com.

Haugsness K., *March 2005 DNS Poisoning Summary*, http://isc.sans.org/presentations/dnspoisoning.php, 2005.

Jeleśniański M., *Pharming – nadchodzi nowe zagrożenie?*, http://pccentre.pl/Article13599.htm, 2006.

Johanson E., *The State of Homograph Attacks*, http://www.shmoo.com/idn/homograph.txt, 2005.

Kaminsky D., *Hack Proofing your Network Second Edition,* Ryan Russell (ed.), 2002.
Małachowski A., *Środowisko wirtualnego klienta,* AE, Wrocław 2005.
Pawlak R., *CitiBank Handlowy SA ukrywał, że go okradli,* http://hacking.pl/5793, 2006.
Pawlak R., *Internauci będą mogli chronić swoje dane osobowe,* http://hacking.pl/5811, 2006a.
RSA Security Alert, *New Phishing Technique Identified: Smart Redirection Attack Helps Phishers Dodge Site Shutdowns,* http://www.rsasecurity.com/press_release.asp, 2006.
The Honeynet Project & Research Alliance, *Know your Enemy: Phishing. Behind the Scenes of Phishing Attacks,* http://www.honeynet.org/papers/phishing/, 2005.
The Honeynet Project & Research Alliance, *Know your Enemy: Phishing. Background on Phishing Attacks,* http://www.honeynet.org/papers/phishing/details/phishing-background.html, 2005a.
The Honeynet Project & Research Alliance, *Know your Enemy: Tracking Botnets. Using Honeynets to Learn More about Bots,* http://www.honeynet.org/papers/bots/, 2005b.
Vamosi R., (2005), *Beware Your Evil Twin (hot spot, that is* http://reviews.cnet.com/4520-3513_7-5630181-1.html, 2005.
Wikipedia, Encyklopedia Internetowa, wersja polska, http://pl.wikipedia.org/wiki/Atak_man_in_the_middle, 2006.

TOOLS AND METHODS OF PHISHING

Summary

Phishing – the method of acquining confidential transaction data from unaware clients – has become the basic problem of safety thread in e-business. Telecommunication and teleinformation technologies may serve as platforms for phishing activities. The paper presents a review of several advanced tools and methods used in this type of cyber crime.

Andrzej Małachowski – dr hab., prof. AE, kierownik Katedry Komunikacji Gospodarczej Akademii Ekonomicznej we Wrocławiu.
Krzysztof Szymczak – mgr, absolwent Akademii Ekonomicznej we Wrocławiu.