XX najpopularniejszych atakow w sieci na twoj komputer. Wykrywanie, usuwanie skutkow i zapobieganie

Autor: Maciej Szmit, Mariusz Tomaszewski, Dominika Lisiak, Izabela Politowska
ISBN: 83-246-1646-2
Format: 158x235, stron: 208

Naucz się rozpoznawać zagrożenia i zadbaj o bezpieczeństwo Twojego komputera!

- Jak rozpoznać atak na Twój komputer?
- Jak wykryć złośliwe oprogramowanie?
- Jak zabezpieczyć się przed podsłuchem sieciowym?

Pewnie myślisz, że Twojemu komputerowi nic nie grozi, bo nie przechowujesz na nim żadnych wartościowych danych. Albo wręcz przeciwnie – panicznie boisz się wirusów, niemal jak ognia piekielnego, ale w ogóle nie potrafisz ich rozpoznać. A może jesteś jedną z tych osób, które nigdy się nad tym nie zastanawiają? Pewnie nie zdajesz sobie sprawy, że przez nieprzemyślane działania możesz sam sobie (i swojemu komputerowi) bardzo zaszkodzić. Nadeszła zatem pora, aby podjąć radykalne kroki w celu zmiany tego stanu rzeczy – czas zrozumieć, na czym polega atak, i zabezpieczyć się przed nim. A oto Twój najwierniejszy sprzymierzeniec w tej walce a ta książka to właśnie Twój najwierniejszy sprzymierzeniec w tej walce!

Książka „13 najpopularniejszych sieciowych ataków na Twój komputer. Wykrywanie, usuwanie skutków i zapobieganie" pokaże Ci, jak wytropić wirusy, przechytrzyć złośliwe oprogramowanie, rozpoznać podsłuch sieciowy. Dowiesz się, jak szybko i skutecznie pozbyć się różnych rodzajów sieciowego oszustwa, takich jak DNS-spoofing, MITM, phishing i pharming. Nauczysz się zabezpieczać komputer przed wszelkimi próbami wtargnięcia na jego teren i pozbywać się infekcji z sieci komputerowej, pendrive'a czy telefonu komórkowego. Ten podręcznik poprowadzi Cię prosto do zwycięstwa w walce z sieciowym zagrożeniem.

- Wykrywanie podsłuchu sieciowego
- Sieci zbudowane w oparciu o przełączniki
- Sieci bezprzewodowe
- Zabezpieczenia przed podsłuchem sieciowym
- Złośliwe oprogramowanie
- Podszywanie się i oszustwa: DNS-spoofing, MITM, phishing i pharming
- Prawna ochrona bezpieczeństwa informacji
- Podstawy komunikacji sieciowej

Rozpoznaj, usuń, ochroń!
Ta książka to więcej niż polisa ubezpieczeniowa!

Wydawnictwo Helion
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl

Spis treści

Rozdział 3.

Podszywanie się i oszustwa: DNS-spoofing, MITM, phishing i pharming

Szyfrowanie przy użyciu algorytmów o odpowiedniej złożoności zapewnia obecnie bardzo dużą ochronę poufności transmitowanej informacji. Atakujący zatem, aby mieć możliwość przeprowadzenia skutecznego ataku, podejmują próby wykorzystania słabości związanych z innymi niż przesyłanie danych elementami procesu transmisji i przetwarzania danych. Przede wszystkim są to procesy rozwiązywania adresów symbolicznych i zestawiania połączenia pomiędzy stronami dialogu. Jeśli uda się przekonać zaatakowanego, żeby zamiast z właściwym serwerem połączył się z maszyną agresora, uzyskanie poufnych danych będzie już łatwe. Po nawiązaniu takiego połączenia atakujący będzie miał dostęp do wszystkich informacji, które będą próbowały dotrzeć do właściwego serwera. Można to wykonać albo za pomocą ataków na proces rozwiązywania nazw, albo przy użyciu złośliwego oprogramowania zainstalowanego na maszynie klienta.

Zwróć uwagę, że tego typu ataki są bardzo niebezpieczne ze względu na skutki, jakie mogą wystąpić po ich przeprowadzeniu. Jeśli nie zauważysz, że zamiast z prawdziwym serwerem połączyłeś się z komputerem atakującego, to możesz spodziewać się większych szkód, np. materialnych (łącząc się z fałszywą stroną internetową, możesz przekazać poufne informacje, dzięki którym atakujący będzie miał możliwość dysponowania Twoimi pieniędzmi). To tylko jeden z przykładów sytuacji, jakie mogą Ci się przytrafić, jeśli nie będziesz miał odpowiedniej wiedzy, jak zabezpieczyć się przed niepożądanym połączeniem.

Duże znaczenie przy zabezpieczaniu się przed takimi rodzajami ataków ma odpowiednia ochrona serwera DNS, o co powinien zadbać administrator sieci, z której korzystasz. Przede wszystkim powinien wprowadzić następujące zasady:

- ograniczenia liczby hostów, które mogą przesyłać zapytania do serwera,
- zablokowania wszystkich portów poza możliwością komunikacji dla zaufanych komputerów,

- uniemożliwienia odpytania serwera o właściwą wersję oprogramowania. (znajomość oprogramowania ułatwia atakującemu znalezienie w nim usterek oraz błędów i ich wykorzystanie w celu przeprowadzenia ataku),
- aktualizowania oprogramowania serwera oraz wprowadzanie poprawek systemowych.

Zapytaj swojego administratora, czy stosuje odpowiednie zabezpieczenia serwera DNS.

Nie wszystkie ataki skierowane są na serwer DNS. Często do przeprowadzenia ataku wykorzystywany jest komputer zaatakowanego (np. poprzez podmianę odpowiednich plików odpowiadających za translację adresów domenowych na adresy IP, łączenie się z pozorowaną stroną poprzez łącze z fałszywej wiadomości e-mail). Szczegółowy opis metod zabezpieczania i ochrony dla takich przypadków został przedstawiony w podrozdziałach 3.1., 3.2, 3.3., 3.4.

3.1. Atak 4: DNS-spoofing

Użytkownicy w sieci komputerowej najczęściej korzystają z nazw domenowych (np.: *www.onet.pl*, *www.wp.pl*). Są one łatwiejsze do zapamiętania i dlatego często są używane zamiast adresów IP. Przy przeglądaniu stron internetowych, łączeniu się z serwerami w oknie adresu wpisywana jest nazwa domenowa, która jest tłumaczona przez specjalne serwery DNS (ang. *Doman Name System* — system nazw domen) na adresy IP. Wykorzystywanie nazw domenowych niesie ze sobą niebezpieczeństwo poważnego ataku — *DNS-spoofingu*.

DNS-spoofing polega najczęściej na fałszowaniu odpowiedzi serwera DNS. Wykorzystuje lukę w protokole polegającą na braku autoryzacji źródła odpowiedzi. Jeśli posługujesz się nazwami domenowymi, jesteś narażony na ten typ ataków. Nazwa serwera, z którym chcesz się połączyć, może zostać odwzorowana na niewłaściwy adres IP. Taka sytuacja spowoduje, że zamiast do serwera dane będą trafiać do komputera atakującego. Do przeprowadzenia ataku wykorzystuje się fałszywy serwer DNS, który nasłuchuje zapytań o odwzorowania nazw domenowych. W odpowiedzi wysyła on fałszywe adresy IP. Klient wiąże nazwę domenową z przesłanym przez fałszywy serwer adresem IP. Inną metodą, znacznie trudniejszą, jest włamanie do serwera DNS i podmiana tablicy odwzorowań.

Zabezpieczenia

Statyczne odwzorowanie adresów IP na nazwy domenowe jest jednym z zabezpieczeń przed atakiem DNS-spoofing. W momencie nawiązywania połączenia poszukiwane odwzorowania będą rozwiązywane lokalnie. W systemie Windows w katalogu *C:\WINDOWS\system32\drivers\etc* w pliku *hosts* wpisz odwzorowanie, dodając wiersz, np.:

```
10.0.0.1 www.mojbank.com.pl
```

W systemie Linux wpisów należy dokonać w katalogu */etc* i mają one następującą składnię:

```
adres_IP nazwa_domenowa alias_nazwy
```

np.

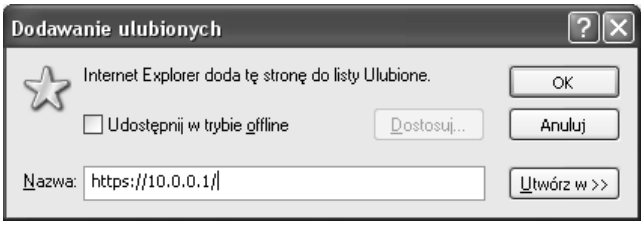
```
10.0.0.1 www.mojbank.com.pl mojbank
```

Alias nazwy jest skrótem, którego możesz użyć, by nie wprowadzać pełnej nazwy domenowej.

Ustaw uprawnienia tylko do odczytu do pliku *hosts* dla aplikacji systemowych. Będziesz miał pewność, że nie zostanie on zmodyfikowany przez złośliwe aplikacje.

Innym sposobem zabezpieczenia przed połączeniem z fałszywą stroną jest zapisanie w zakładce ulubione bezpośrednio adresu IP strony internetowej np. jak na rysunku 3.1.

Rysunek 3.1. *Dodawanie ulubionych stron internetowych*



Przy takim zapisie będzie pojawiać się komunikat weryfikujący certyfikat. Będziesz musiał weryfikować informacje, które pojawią się w alercie.

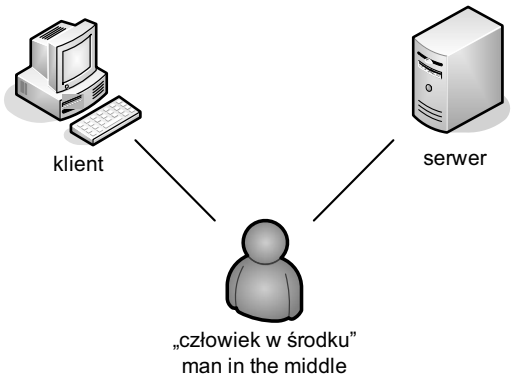
W sytuacjach, w których bezpieczeństwo odgrywa ważną rolę, najlepiej zrezygnuj z wykorzystywania protokołu DNS.

3.2. Atak 5: Man In The Middle (MITM)

Polega na tym, że próba połączenia się klienta z serwerem jest kierowana do fałszywego serwera lub też przechodzi przez komputer atakującego. Aby istniała możliwość przekierowania takich zapytań, dokonuje się ataku DNS-spoofing, który polega na fałszowaniu odpowiedzi z serwera lub ataku ARP-spoofing.

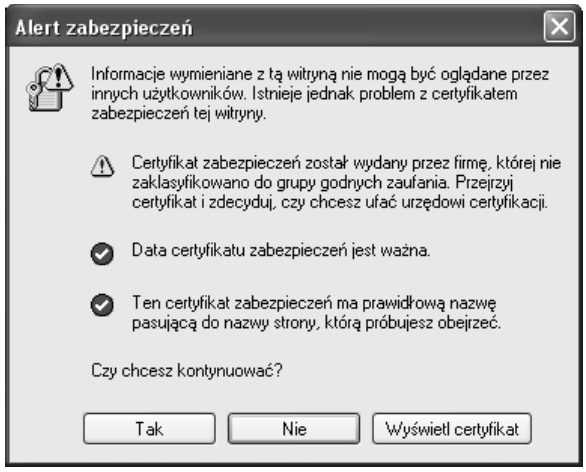
W przypadku ataku MITM atakujący jest osobą znajdującą się pomiędzy klientem a serwerem. Określany jest jako „człowiek w środku" (ang. *man in the middle*) (zobacz rysunek 3.2). Poprzez przekierowanie zapytania klienta do własnego komputera i przedstawienie mu fałszywego certyfikatu lub klucza publicznego atakujący uzyskuje dostęp do zaszyfrowanego połączenia. Następnie nawiązuje połączenie z rzeczywistym serwerem, udając właściwego klienta. Cały ruch między klientem a serwerem przechodzi przez komputer atakującego, a za pomocą wygenerowanych przez siebie kluczy atakujący ma możliwość odszyfrowania przesyłanych danych.

Rysunek 3.2.
Atak MITM



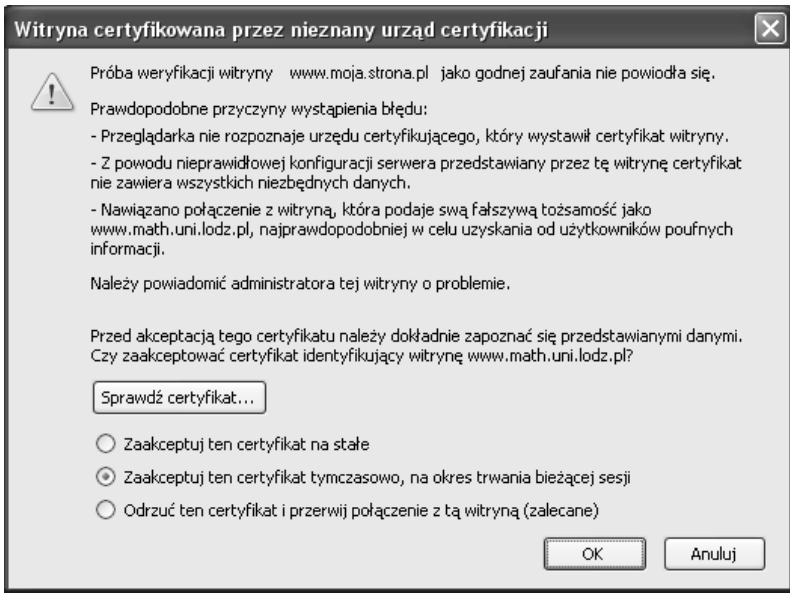
Na atak MITM musisz uważać w szczególności, gdy używasz bezpiecznego połączenia szyfrowanego np. za pomocą protokołu SSL. W momencie łączenia się z serwerem za pomocą przeglądarki i protokołu https serwer identyfikuje się swoim certyfikatem. Jeśli certyfikat jest kwalifikowany (tzn. jest zaufany, a jego autentyczność potwierdza urząd certyfikujący), przeglądarka akceptuje połączenie. Jeżeli natomiast w trakcie weryfikacji nastąpi błąd (tzn. przeglądarka nie zweryfikuje certyfikatu), wyświetli się komunikat jak na rysunku 3.3 lub 3.4. Teraz od Ciebie zależy, czy zaakceptujesz, czy odrzucisz to połączenie.

Rysunek 3.3.
Alert zabezpieczeń w przeglądarce Internet Explorer



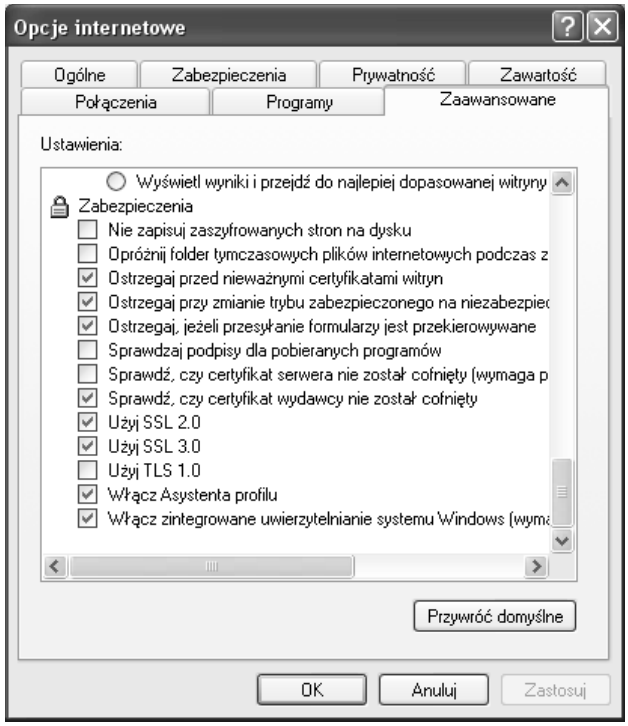
Nigdy nie akceptuj takiego alertu. Przejrzyj dokładnie informacje o certyfikacie (przycisk *wyświetl certyfikat*) i dopiero po tym zadecyduj o kontynuowaniu oglądania strony. Jeśli pochopnie zaakceptujesz taki certyfikat, przeglądarka zapisze go w magazynie certyfikatów i nie zapyta Cię ponownie o jego weryfikację. Takie uważne czytanie komunikatów pozwala ochronić się przed atakami MITM.

Można zwiększyć bezpieczeństwo, wyłączając obsługę protokołu SSL 3.0. W przypadku Internet Explorera z menu *Narzędzia* wybierz *Opcje internetowe*, przejdź do zakładki *Zaawansowane* i w podpunkcie *Zabezpieczenia* odznacz opcję *Użyj SSL 2.0*

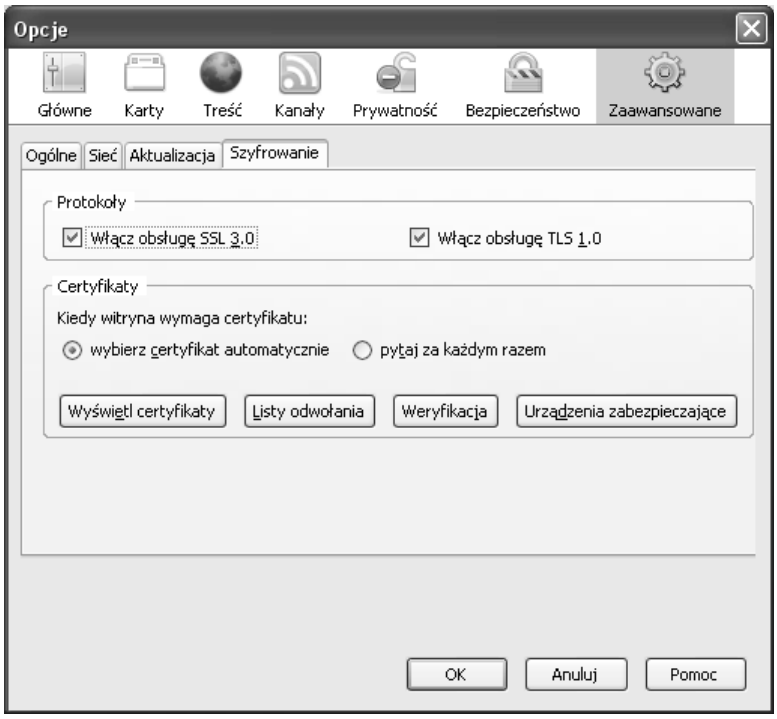


Rysunek 3.4. *Alert zabezpieczeń w przeglądarce Mozilla Firefox*

(zobacz rysunek 3.5). Przeglądarka Mozilla Firefox obsługuje tylko SSL 3 (zobacz rysunek 3.6). Należy pamiętać o tym, że niektóre strony po odznaczeniu lub całkowitym braku SSL 2.0 mogą nie uruchamiać się poprawnie.



Rysunek 3.5. *Opcje internetowe — Zaawansowane — Zabezpieczenia w przeglądarce Internet Explorer*



Rysunek 3.6. *Opcje Zaawansowane — Szyfrowanie w przeglądarce Mozilla Firefox*

Pamiętaj również, żeby stosować zasadę ograniczonego zaufania, jeśli z Twojego komputera korzysta wiele osób lub jeśli Ty korzystasz z komputera publicznie dostępnego (np. w kawiarence internetowej, w pracy, w szkole). Najlepiej nie przesyłaj w takich miejscach poufnych danych, ponieważ nie możesz mieć pewności, czy ktoś nie zaakceptował niebezpiecznych certyfikatów lub nie dodał do ich magazynu specjalnie wygenerowanych, by móc podsłuchiwać transmisję.

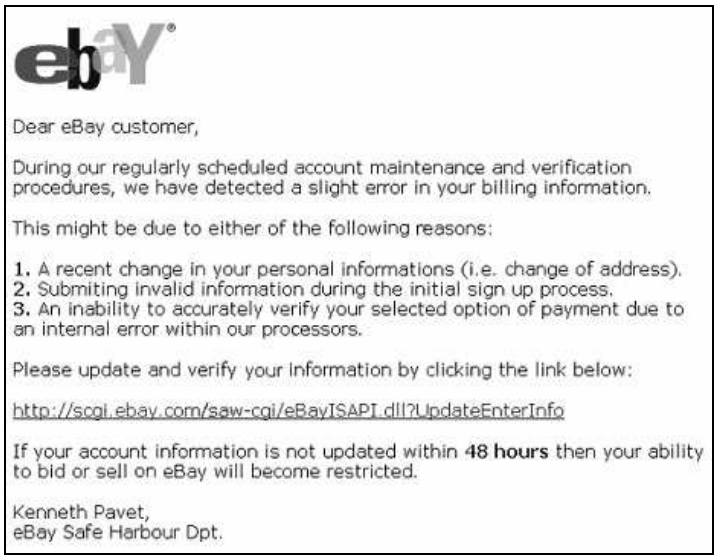
3.3. Atak 6: phishing

Phishing (ang. *password harvesting fishing* — łowienie haseł) jest atakiem mającym na celu pozyskanie poufnych informacji poprzez podszywanie się pod zaufane podmioty (np. banki, sklepy internetowe, serwisy aukcyjne, serwisy pocztowe).

Atak ten polega na wysyłaniu e-maili kierujących na fałszywą stronę, prawie identyczną z oryginalną, która w rzeczywistości przechwytuje wpisywane na niej informacje. Przykładowo: atakujący wysyła wiadomości e-mail z linkiem do udawanej strony Twojego banku z prośbą o zalogowanie i sprawdzenie informacji o najnowszych promocjach przy zakładaniu lokat bankowych. Klikasz link i logujesz się. W tym momencie Twój login i hasło przesyłane są zamiast do serwisu bankowego do atakującego, który ma już dostęp do Twojego konta bankowego.

Przykładowe e-maile phishingowe zostały przedstawione na rysunkach 3.7 i 3.8.

Rysunek 3.7. *Przykładowy e-mail phishingowy*



Dear eBay customer,

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information.

This might be due to either of the following reasons:

1. A recent change in your personal informations (i.e. change of address).
2. Submiting invalid information during the initial sign up process.
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.

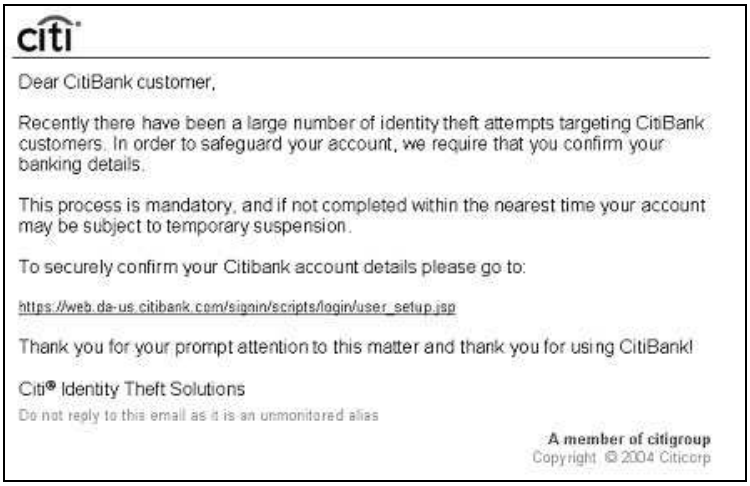
Please update and verify your information by clicking the link below:

http://scgi.ebay.com/saw-cgi/eBayISAPI.dll?UpdateEnterInfo

If your account information is not updated within **48 hours** then your ability to bid or sell on eBay will become restricted.

Kenneth Pavet,
eBay Safe Harbour Dpt.

Rysunek 3.8. *Przykładowy e-mail phishingowy*



citi

Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your Citibank account details please go to:

https://web.da-us.citibank.com/signin/scripts/login/user_setup.jsp

Thank you for your prompt attention to this matter and thank you for using CitiBank!

Citi® Identity Theft Solutions

Do not reply to this email as it is an unmonitored alias

A member of citigroup

Copyright © 2004 Citicorp

Poniżej przedstawiono kilka sformułowań, które w e-mailu powinny zwrócić Twoją szczególną uwagę:

„Sprawdź ustawienia swojego konta”. Firmy nie powinny prosić o przesyłanie haseł, nazw użytkownika, numerów PESEL czy innych informacji osobistych pocztą e-mail.

„W przypadku braku odpowiedzi w ciągu 48 godzin, Pani/Pana konto zostanie zamknięte”.

„Szanowny Kliencie”. Wiadomości e-mail związane z phishingiem są zwykle rozsyłane masowo i nie zawierają imienia ani nazwiska.

„Kliknij poniższe łącze, aby uzyskać dostęp do swego konta”. Łącze może prowadzić do sfałszowanej witryny.

Istnieje także pewna odmiana phishingu zwana *spear phishing*. Jest to próba kradzieży informacji, precyzyjnie skierowana przeciwko konkretnej grupie osób, takiej jak firma, w przeciwieństwie do phishingu, który jest skierowany raczej do dużej liczby osób.

Polega również na wysłaniu do takiej grupy wiadomości e-mail, która wygląda na oryginalną i prawdziwą. Odbiorca może ją potraktować jako autentyczną wiadomość wysłaną przez pracodawcę lub kolegę z pracy do każdego pracownika firmy. W treści maila jak zwykle pojawia się prośba mająca skłonić daną osobę do podania np. nazwy użytkownika lub hasła. Podczas gdy tradycyjny phishing kradnie informacje często od przypadkowych pojedynczych osób, atak typu spear phishing ma na celu uzyskanie dostępu do całej sieci przedsiębiorstwa.

Ochrona przed phishingiem

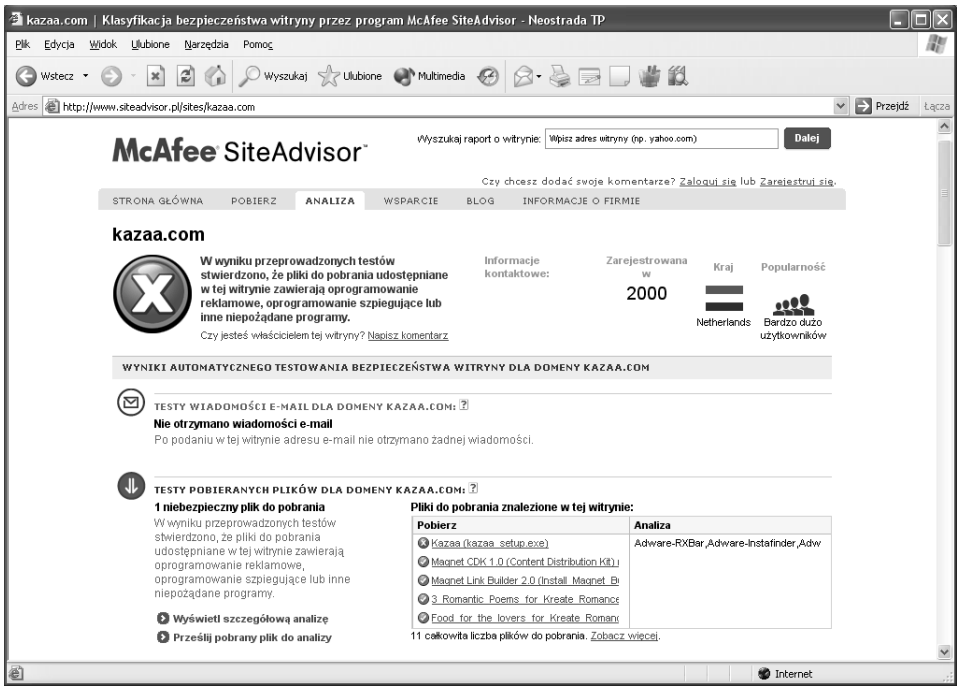
- Po pierwsze, instytucje takie jak banki, organizacje finansowe nigdy nie wysyłają e-maili z prośbą o ujawnienie poufnych danych. Sprawdzaj dokładnie wiadomości w Twojej skrzynce odbiorczej. Wiadomości przesyłane przez atakującego mogą być łudząco podobne do oryginalnych, dlatego bądź czujny i najpierw sprawdź autentyczność listu. Nie klikaj bezmyślnie każdego linka w e-mailach.
- Po drugie, łącz się bezpośrednio ze stronami banków internetowych, nie korzystaj z odsyłaczy. Po otwarciu strony sprawdź certyfikaty poprzez naciśnięcie znaku kłódki w dolnej części przeglądarki internetowej.
- Po trzecie, korzystaj z najnowszej wersji przeglądarek internetowych, uaktualniaj oprogramowanie. Starsze wersje przeglądarek mogą być podatne na błędy. Korzystaj z przeglądarek wyposażonych w filtry phishingowe np. Mozilla Firefox, Opera, Internet Explorer 7.0.
- Po czwarte, możesz użyć specjalnego oprogramowania chroniącego przed takimi atakami, np. Kaspersky Internet Security, ArcaVir System Protection, AntiVirenKit Internet Security.

Do badania witryn internetowych przydatne jest narzędzie firmy McAffe, z którego możesz skorzystać bezpośrednio ze strony internetowej *www.siteadvisor.pl* bądź instalując plugin do przeglądarek internetowych, takich jak Internet Explorer czy Mozilla Firefox.

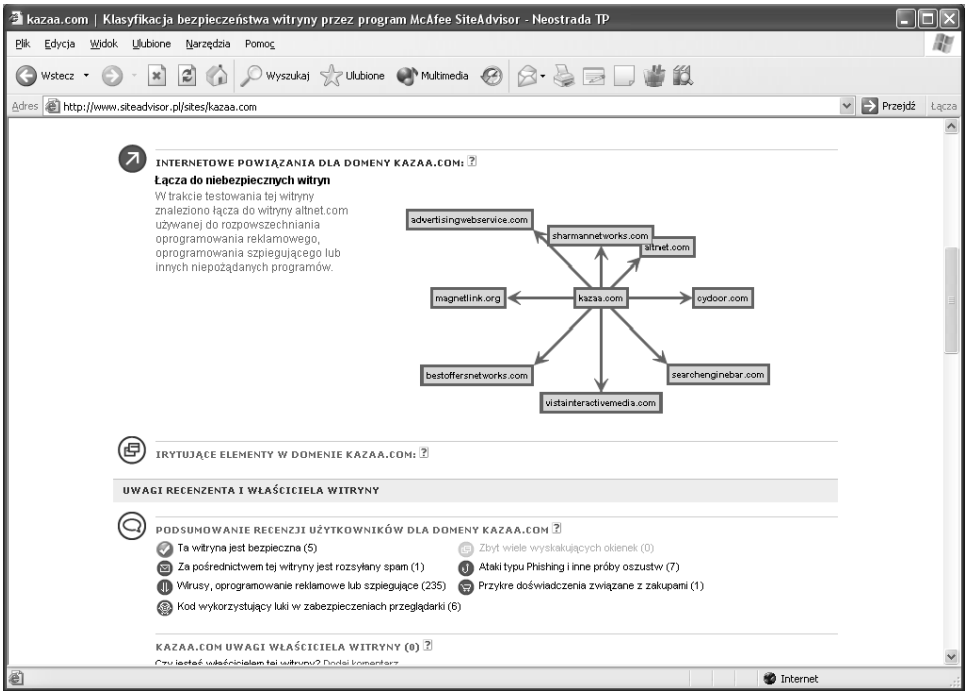
Narzędzie wykonuje szereg automatycznych testów badających bezpieczeństwo witryn, m.in.:

- testy wiadomości e-mail rozsyłanych do użytkowników danej strony,
- badanie plików możliwych do pobrania z witryny i irytujących elementów,
- badanie powiązań z innymi stronami, na które testowana strona próbuje skierować użytkownika, wykrywanie powiązań z witrynami niebezpiecznymi i (lub) podejrzanymi.

Na rysunkach 3.9 i 3.10 przedstawiony został przykładowy raport z testu strony kazaa.com wykonany narzędziem siteadvisor.



Rysunek 3.9. *Działanie narzędzia SiteAdvisor*



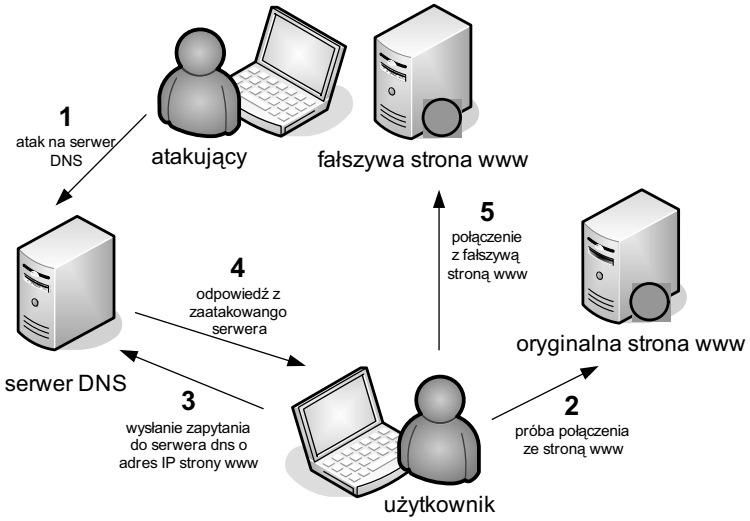
Rysunek 3.10. *Działanie narzędzia SiteAdvisor*

3.4. Atak 7: pharming

Pharming jest zaawansowaną formą phishingu Jest trudniejszy do wykrycia, ponieważ zaatakowany nie spodziewa się zagrożenia, bo nie otrzymuje żadnych fałszywych wiadomości e-mail. Łącząc się ze stroną np. banku internetowego, zaatakowany jest przekonany, że jest to prawidłowa strona (adres strony jest zgodny, strona wyglądem jest identyczna lub bardzo podobna), i przesyłając dane, przekazuje je prosto do atakującego. Atakujący działa zazwyczaj na jeden z dwóch sposobów: instaluje w komputerze zaatakowanego złośliwe oprogramowanie bądź przeprowadza atak DNS-spoofing. W pierwszym przypadku w najprostszej wersji złośliwe oprogramowanie modyfikuje wpisy w pliku *hosts* lub *lmhosts* (w których to plikach system operacyjny przechowuje informacje o odwzorowaniach nazw symbolicznych na adresy IP — wpisy w tych plikach są sprawdzane, zanim system wygeneruje zapytanie do DNS-a).

Na rysunku 3.11 przedstawiony został schemat ataku pharming.

Rysunek 3.11.
Atak pharming



1. Atakujący przeprowadza atak DNS-spoofing na serwer DNS,
2. Użytkownik próbuje nawiązać połączenie ze stroną WWW.
3. Następnie wysyła zapytanie do serwera DNS o adres IP szukanej strony.
4. Otrzymuje odpowiedź od zaatakowanego serwera.
5. Zamiast z oryginalną stroną łączy się z fałszywą stroną WWW wygenerowaną przez atakującego.

W celu ochrony przed takim atakiem, podobnie jak w przypadku phishingu, stosuj aktualne oprogramowanie antywirusowe oraz zaporę sieciową (ang. *firewall*), aby uniemożliwić podmianę pliku zawierającego adresy stron najczęściej odwiedzanych. Jeśli zauważysz na stronie nieprawidłowości, różnice w stosunku do oryginalnej, skontaktuj się z administratorem lub właścicielem tej strony.