BROWSING „WIRTUALNE” ZAGROŻENIA

Grzegorz Prujszczyk

Kamil Śliwowski

Październik 2010, wersja 1.0. Treść podręcznika dostępna jest na licencji:
Creative Commons – Uznanie Autorstwa – Na Tych Samych Warunkach 3.0 PL

Ilustracja na okładce aut. Richoz dostępna na licencji:
Creative Commons – Uznanie Autorstwa – Na tych Samych Warunkach.

SPIS TREŚCI

BROWSING – OGLĄDANIE STRON. JAK TO DZIAŁA?

OGLĄDANIE STRON. JAK TO DZIAŁA?

Przyzwyczajeni jesteśmy do kilku najprostszych sposobów poruszania się w sieci: otwierając przeglądarkę internetową, wpisujemy adres interesującej nas strony, wyszukujemy interesujące nas strony i tematy za pomocą wyszukiwarki lub poruszamy się po linkach (łączach), np. ze strony początkowej.

SŁOWNICZEK

Przeglądarka internetowa *– to program służący do pobierania i wyświetlania zawartości plików pobieranych z serwerów, czyli wyświetlania stron internetowych i plików multimedialnych. Współczesne przeglądarki mają możliwość komunikowania za pomocą wielu różnych protokołów, np. poczty e-mail, dzięki czemu mogą służyć rozbudowanym zadaniom. W systemie Windows domyślną przeglądarką jest Internet Explorer, w systemie Linuks najczęściej jest to Mozilla Firefox. Dodatkowo przeglądarki takie jak Mozilla Firefox, Opera oraz Chrome obsługują dodatkowe wtyczki, czyli małe programy rozbudowujące ich funkcjonalności, np. z zakresu bezpieczeństwa.*

Jeśli chcemy obejrzeć stronę, nasza przeglądarka w pierwszej kolejności wysyła do dostawcy treści następujące informacje:

- dane identyfikacyjne – informację o tym, jak nawiązać z nami połączenie, po którym wysłana zostanie strona;
- dane o dokumencie – informację o tym, jaki dokument nas interesuje, czyli to, co wpisujemy w adresie;
- dane o naszych preferencjach – jakie języki rozumiemy, jaka treść ma być przekazana oraz dodatkowe informacje zapisane przy poprzednich odwiedzinach w plikach „cookies”.

Następnie serwer dostawcy wysyła do nas podstawowy dokument z treścią. Nasza przeglądarka odczytuje dokument. Są w nim zawarte informacje, skąd należy pobrać dodatkowe elementy:

- Obrazki – tła, przyciski, zdjęcia itp.;
- Style – informacje o tym, jak ma wyglądać tekst, w jakim układzie ma być przedstawiony;
- Skrypty – czyli małe programy obsługujące wszelką aktywność na stronie, np. uruchamiające filmy i animacje (np. z reklamami lub dostosowujące wygląd stron itp.);
- Inne – animacje Flash, dźwięki, odtwarzacze video , będące w różnym stopniu mieszanką wymienionych elementów.

Elementy te ładowane są z różnych miejsc w sieci – niekoniecznie od dostawcy.

Teraz nasza przeglądarka po kolei ładuje te elementy, wysyłając za każdym razem tę samą informację co poprzednio.

SŁOWNICZEK

Ciasteczka (ang. cookies) *– małe pliki testowe zapisywane na dysku użytkownika podczas korzystania ze stron WWW, które zapamiętują określone informacje o ustawieniach przeglądarki (np. wybrany język strony WWW, dane logowania) lub przesyłające pewne informacje z powrotem na serwery danej strony, np. o ustawieniach zabezpieczeń, lub zapamiętane wcześniej produkty w koszyku w sklepie internetowym. Ciasteczka są systemem narażającym użytkownika na wiele zagrożeń, gdyż mogą zapamiętywać wiele wrażliwych informacji i działają bez świadomości większości użytkowników.*

Jakie dodatkowe elementy pobieramy?

Potrzebne – spełniające potrzebne nam funkcje, jak te opisane powyżej, czyli wszystkie elementy, których potrzebujemy by poprawnie wyświetlić stronę i jej treść. Nie wszystkie z tych elementów musimy widzieć, niektóre odpowiadają jedynie za działanie strony lub jej ustawienia. Różnorodność tych elementów sprawia, że łatwo zamieścić wśród nich rzeczy niechciane, np. reklamy, skrypty śledzące nasze działania czy niepotrzebne dodatki takiej, jak spadający sztuczny śnieg na stronie czy oczka śledzące ruch kursora myszki.

STRONY NAS ŚLEDZĄ. WSZYSTKIE

Jak jesteśmy śledzeni?

Strony śledzą następujące działania użytkowników:

- Wejście na serwis – zapisywana jest informacja skąd przyszliśmy;
- Poruszanie się po serwisie – zapisywane są kolejne dokumenty, które otwieramy;
- Poruszanie się po stronach – w większości wypadków można odtworzyć zdalnie wszystkie kolejne odwiedziny, tak jakby ktoś miał dostęp do naszej historii odwiedzin;
- Klikanie i aktywność w obrębie danej strony (nawet jeśli nie wychodzimy na inne strony);
- Niekiedy również wszystkie rzeczy, które wpisujemy na klawiaturze.

Dlaczego jesteśmy śledzeni? Część organizacji i osób jest zainteresowana poznaniem informacji o nas, ponieważ dokładna znajomość zachowań użytkowników jest warta całkiem sporych pieniędzy. Ponadto wyłączenie wszystkich funkcji śledzących jest prawie niemożliwe. Większość informacji zbieranych podczas śledzenia jest również konieczna do prawidłowego działania stron. Pamiętacie jak mówiliśmy, jak to działa?

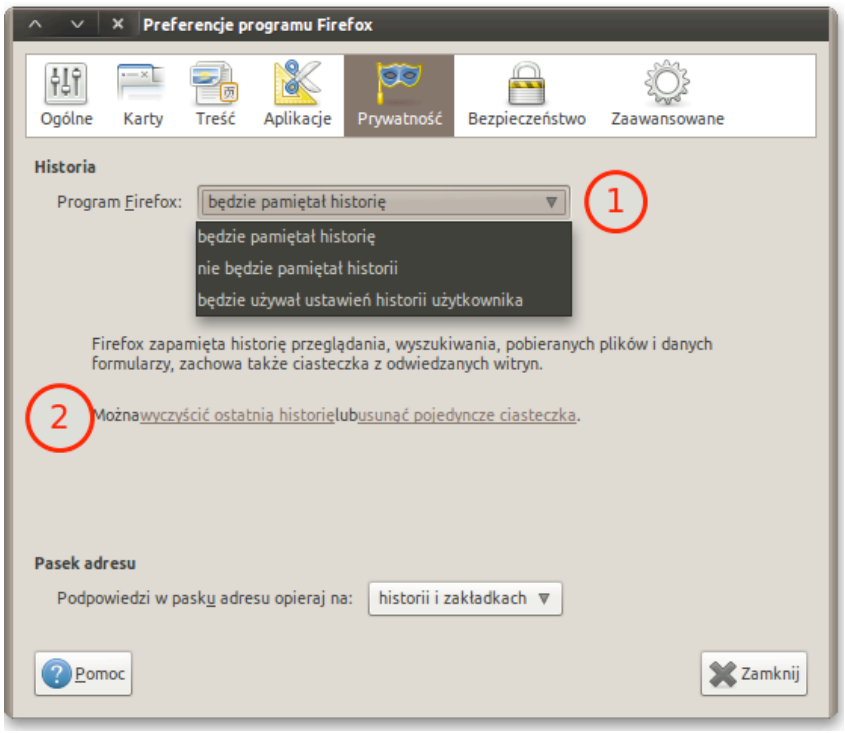
Do czego służą zebrane informacje? Właściciel serwisu uzyskuje informację statystyczną o popularnych linkach na stronie lub o efektywności interfejsu, czyli sposobu prezentacji strony i jej interakcji z użytkownikiem (na przykład: które menu jest dla nas łatwe do obsługi, a które jest dla nas zbyt trudne). Reklamodawcy mogą uzyskać statystyczne informacje o preferencjach użytkowników. Firmy tworzące i obsługujące reklamy identyfikują nas i starają się dopasować wyświetlane reklamy tak, abyśmy na nie kliknęli. Firmy dostarczające oprogramowanie do śledzenia mogą tworzyć modele zachowań użytkowników, ale również śledzić konkretnych użytkowników.

Nasze dane, ponieważ nie są bezpośrednio powiązane z nami jako osobami, nie są traktowane jako dane osobowe. Co za tym idzie, nie są objęte szczególną ochroną. Nie mamy ani prawa wglądu w te dane, ani również prawa żądania ich usunięcia. Natomiast często ma do nich dostęp wielu pracowników dużych organizacji, którzy mogą wykorzystać te informacje w niebezpieczny sposób.

Wyobraźmy sobie taki przypadek... Wchodzimy na stronę bardzo skrupulatnie śledzącą nasze ruchy. Logujemy się na niej loginem i hasłem. Przypadkiem jest to hasło do naszego konta bankowego... „Ha!” powiecie, „ale przecież nie mają numeru, którym loguję się do mojego konta bankowego!” Ale przypadkiem jest to również hasło do naszej poczty, gdzie wysyłane są PDFy z wyciągami, na bazie których można odczytać ten numer... W ten sposób zbierając dane z tych kilku miejsc, można uzyskać dostęp do naszego konta, poczty.

USTAWIENIA PRZEGLĄDARKI

Każda przeglądarka internetowa oferuje dziś ustawienia umożliwiające podstawowe zabezpieczenia naszej prywatności i komunikacji. Na przykładzie Mozilla Firefox pokażemy zalecane ustawienia. Warto zwrócić uwagę na różne wersje przeglądarek – nawet Mozilla Firefox może różnić się zależnie od wersji starszej bądź nowszej. Warto przeglądarki aktualizować do najwyższej stabilnej wersji, która zwykle jest najlepiej zabezpieczona.



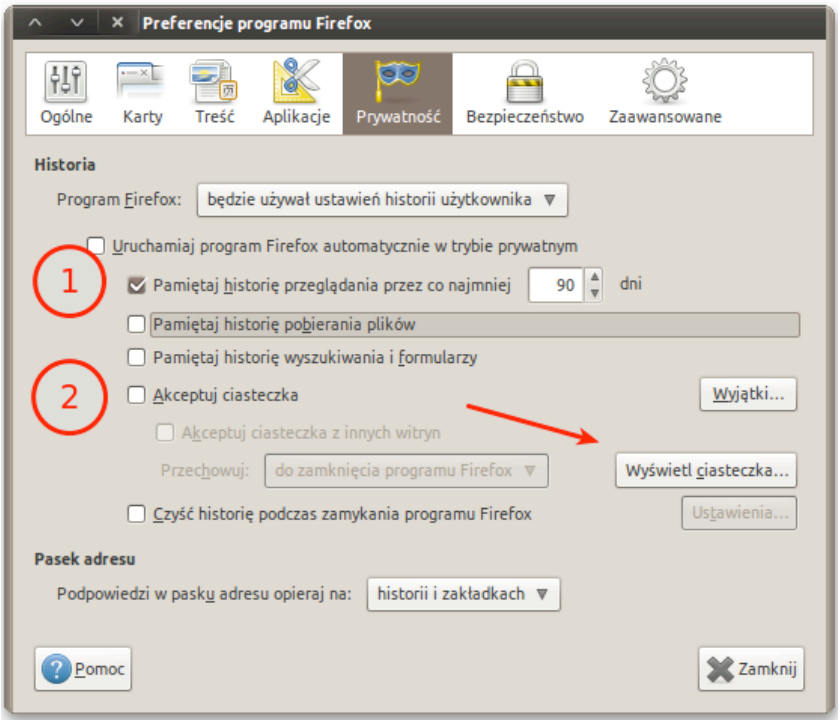
Rys.1. Historia. Po wejściu w menu przeglądarki *Edycja* → *Preferencje* lub *Narzędzia* → *Opcje* (w zależności od wersji przeglądarki) zobaczymy ustawienia w kilku zakładkach. W *Prywatność* możemy:

1. wybrać co przeglądarka będzie zapisywać z każdą sesją, wybranie opcji ustawień umożliwi nam dalszą konfigurację;
2. wyczyścić historię przeglądania lub ciasteczka.

WAŻNY LINK

http://www.cert.org/tech_tips/securing_

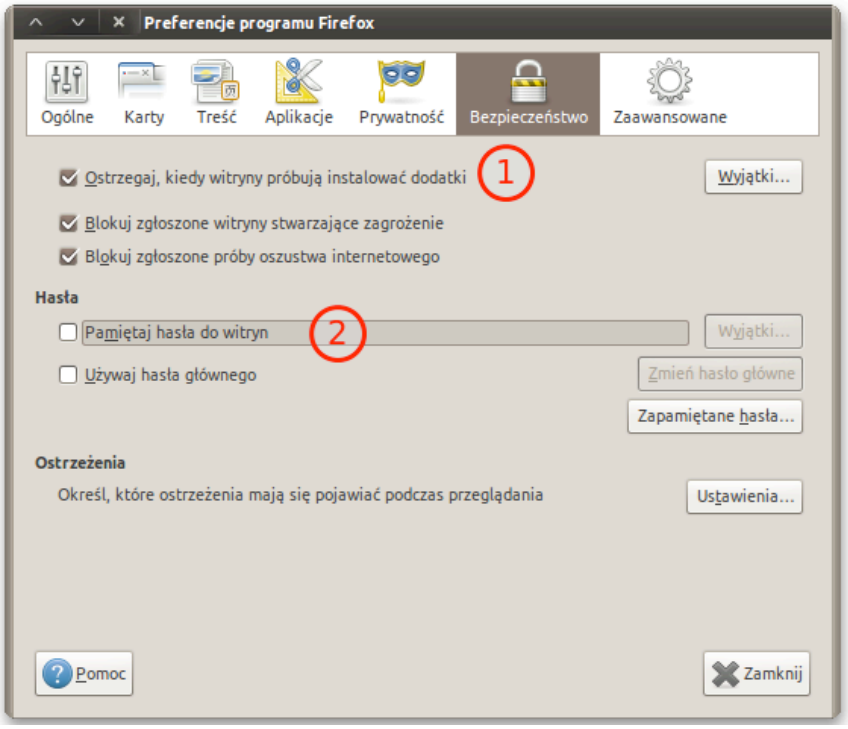
Przegląd ustawień bezpieczeństwa najpopularniejszych przeglądarek internetowych wraz z informacjami dodatkowymi, np. o społecznościowym wsparciu, rozwiązywaniu problemów, lukach w bezpieczeństwie.



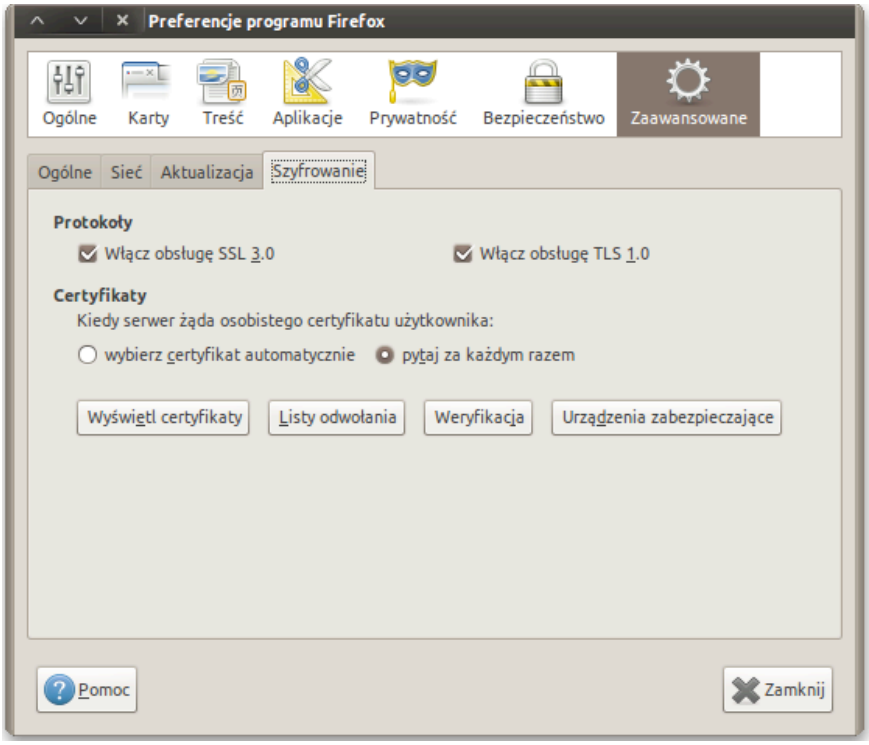
Rys.2. Ustawienia użytkownika. Po wybraniu opcji *Ustawienia użytkownika* możemy zdecydować czy:

1. przeglądarka ma pamiętać (i jak długo) historię przeglądania; dane takie jak, pobierane pliki, dane wpisywane w formularzach;
2. oraz czy ma akceptować ciasteczka.

Wyłączenia akceptacji ciasteczek może uniemożliwić nam korzystanie z wielu serwisów, np. poczty Gmail, ale możemy ustawić przeglądarkę tak, aby akceptowała je, lecz usuwała za każdym razem, kiedy zamykamy program.



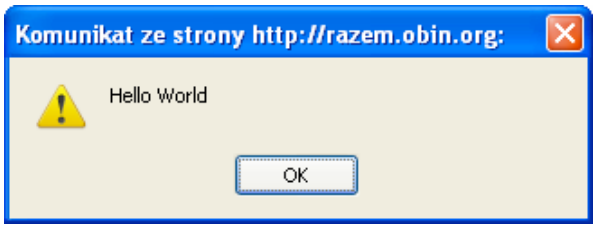
Rys.3. W zakładce *Bezpieczeństwo* możemy ustawić opcję powiadamiania nas o wykrytych przez przeglądarkę zagrożeniach (1) oraz wyłączyć jej zapamiętywanie haseł do witryn i serwisów (2) – obok możemy podejrzeć, do jakich serwisów przeglądarka posiada już zapamiętane hasła.



Rys.4. W zakładce *Zaawansowane* → *Szyfrowanie* możemy sprawdzić, czy na pewno mamy uruchomioną opcję obsługi protokołów SSL i TLS oraz ustawić dodatkową opcję pytania nas za każdym razem, gdy serwer wymaga certyfikatu użytkownika.

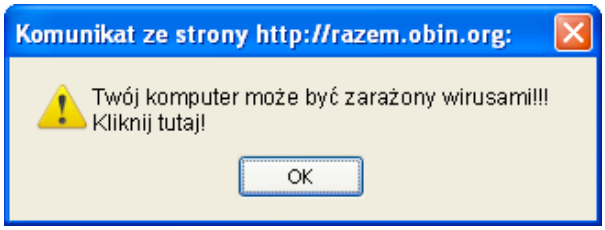
MANIPULACJE

Jestem wiarygodną informacją systemu. Niektóre reklamy i elementy na stronach usiłują prezentować się jako elementy systemu – żeby zdobyć nasze zaufanie. Są to wszelkiego rodzaju okienka wyglądające jak systemowe, informujące np. że nasz komputer jest zagrożony albo że wygraliśmy jakąś gigantyczną nagrodę. Na ogół prowadzą one na strony, które mają nas dalej zmanipulować i przekonać do zainstalowania jakiegoś niebezpiecznego dodatku albo programu. Porównanie:



Rys. 5. Porównanie komunikatów przed personalizacją.

Prawdziwy komunikat systemowy (powyżej) vs. fałszywy komunikat (poniżej).

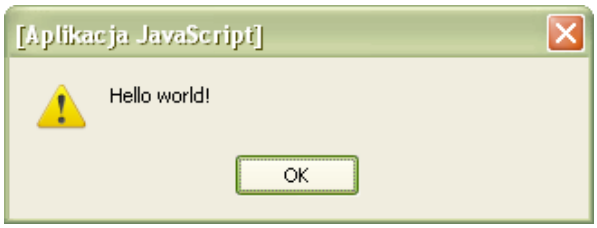


Ochrona:

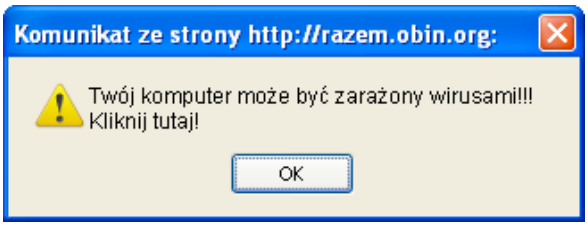
- personalizacja systemu i oprogramowania,
- blokowanie cookiesów,
- blokowanie reklam (np. za pomocą wtyczki AdBlock).

Personalizacja: Strona internetowa nie może sprawdzić naszych motywów kolorystycznych, dlatego wszystkie złośliwe reklamy wykorzystują standardowe motywy. Jeśli zmienimy motyw na inny, zmienimy rozmiar pasków itp., od razu będziemy w stanie rozpoznać fałszywe monity. Analogiczna metoda w przypadku przeglądarki pozwoli nam na obronę przed tymi fałszywkami, które próbują naśladować przeglądarkę. Podane przykłady to komunikaty z przeglądarki, które wyświetlają się w oknie systemowym (personalizacja systemu pozwala wykryć nieprawdziwe komunikaty).

Rys.6. Porównanie po personalizacji.

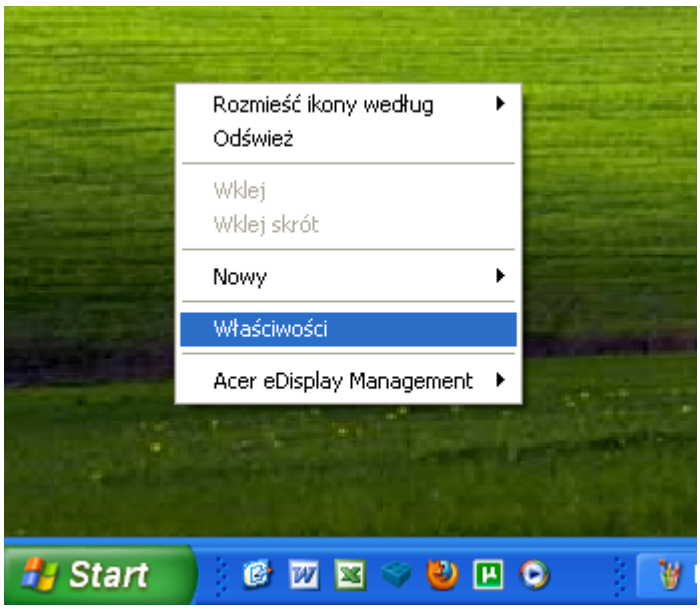


Prawdziwy komunikat systemowy (powyżej) vs. fałszywy komunikat systemowy (poniżej).

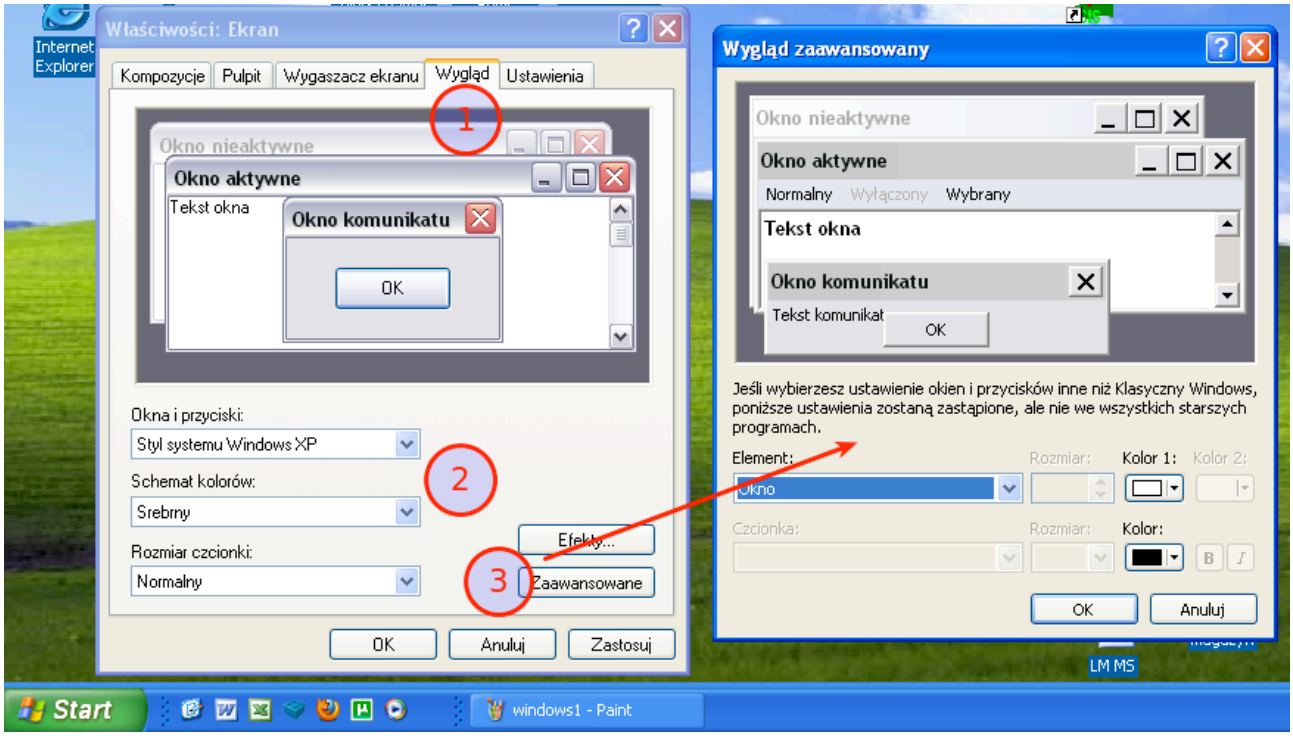


PERSONALIZOWANIE WYGLĄDU

W systemie Windows wystarczy kliknąć prawym przyciskiem na dowolne miejsce Waszego pulpitu i wybrać z paska kontekstowego (Rys.7) opcję Właściwości. Następnie przechodzimy do zakładki Wygląd (Rys.8) gdzie możemy zmienić standardowe ustawienia wyglądu naszego systemu operacyjnego.



Rys. 7. Uruchamianie właściwości wyglądu w systemie Windows.



Rys.8. Dostosowywanie ustawień wyglądu (personalizacja).

1. Przejdź do zakładki *Wygląd*.
2. Zmień standardowe kolory *Okien i przycisków*.
3. Klikając w opcje *Zaawansowane* możesz wybrać dowolny kolor, zmienić czcionki oraz szczegóły wyglądu okien.

Blokowanie cookiesów:

Do blokowania cookiesów dostępne są specjalne rozszerzenia. W Mozilla Firefox jest to plugin **BetterPrivacy**, który możemy zainstalować na stronie **addons.mozilla.org** – wystarczy kliknąć na przycisk *Zainstaluj*. Analogiczne dodatki istnieją do większości przeglądarek, np. Google Chrome. BetterPrivacy po zainstalowaniu jest skonfigurowany do automatycznego kasowania plików cookies LSO (związanych z plikami flash), które nigdy nie wygasają i wysyłają więcej informacji o działaniach użytkownika niż zwykłe „ciasteczka". Każda aktualna przeglądarka ma opcje czyszczenia cookies. Większość pozwala na niedopuszczanie lub automatyczne kasowanie cookies z wybranych stron. Wtyczka Firefoxa BetterPrivacy pozawala usuwać specjalny rodzaj „ukrytych" ciasteczek – **flashcookies**.

Blokowanie reklam:

Większość niebezpiecznych cookiesów jest związana z reklamami. Również większość manipulujących elementów stron to reklamy. Istnieją gotowe dodatki potrafiące skutecznie walczyć

z formami reklamowymi. Dla Mozilla Firefox jest to dodatek **AdBlock Plus** dostępny na stronie addons.mozilla.org – aby odnaleźć taki dodatek wchodzimy na stronę z rozszerzeniami do naszej przeglądarki.

SpyBot a śledzenie w sieci

Również program **SpyBot Seek&Destroy** pozwala na blokowanie części cookiesów. Powoduje on, że serwery firm śledzących użytkowników są z naszego komputera niedostępne. To z kolei uniemożliwia uruchomienie śledzącego kodu i zwiększa tym samym naszą anonimowość i bezpieczeństwo. Program Spybot ma też parę innych praktycznych funkcji, m.in. naprawę błędów w rejestrze systemu (powodowanych przez wirusy, szkodliwe oprogramowanie i uszkodzone programy). Rejestr to baza plików konfiguracyjnych w systemie Windows, błędy w niej możemy również prosto naprawić za pomocą programu CC Cleaner.

Program SpyBot jest dostępny za darmo na stronie: www.safer-networking.org. Procedura instalacji jest dokładnie opisana na stronie. Po instalacji wystarczy kliknąć na przycisk *Apply protections*.

INSTALACJA OPROGRAMOWANIA

Problemy i zagrożenia:

- Złośliwe oprogramowanie;
- Niestandardowe formaty;
- Licencje;
- Błędy/brak konfiguracji;
- Ataki hakerskie na źródła dystrybucji.

Złośliwe oprogramowanie może gromadzić wszelkie dane o użyciu komputera, które mógłby zbierać trojan, tj. każdy wciśnięty klawisz, odwiedzoną stronę, wprowadzone loginy i hasła. Dane te mogą być przesyłane lub automatycznie upubliczniane. Złośliwe oprogramowanie ma również tendencje do „rozrastania się", czyli instalowania kolejnych wersji, wtyczek do innych programów. Może również osłabiać nasze bezpieczeństwo przez posiadanie lub tworzenie luk bezpieczeństwa tzw. *backdoorów*.

UWAGA: Programy, które instalujemy, mają pełen dostęp do systemu!

SŁOWNICZEK

Backdoor *(pol. tylne drzwi, furtka) – to luka w zabezpieczeniach systemu lub programu stworzona umyślnie w celu późniejszego wykorzystania. Backdoor może być wykorzystany do ułatwienia włamań, podrzucania koni trojańskich lub do wykonania bez woli użytkownika jakiejś zdalnej komendy, np. zablokowania programu.*

DIGITAL RIGHTS MANAGEMENT I UPRAWNIENIE UŻYTKOWNIKA

SŁOWNICZEK

DRM (Digital Rights Management) *– oprogramowanie i sprzęt mające uniemożliwić działania niezgodne z prawem autorskim lub warunkami serwisu/ wolą producenta. DRM stosuje się w muzyce, filmach, grach i innych mediach. Opiera się na mechanizmach kryptograficznych, zabezpieczając np. przed nieautoryzowanym odczytem lub skopiowaniem.*

Jak pokazuje wiele przykładów, zabezpieczenie zysków firm nie koniecznie idzie w parze z wygodą i prywatnością użytkowników, a często nawet bezpieczeństwem systemu. Zasadniczym celem DRM jest kontrola wykorzystania mediów, więc wszelkie oprogramowanie z funkcjami DRM *de facto* pozwala na szpiegowanie użytkowników w mniejszym lub większym stopniu.

Zamknięte formaty czy formaty własnościowe oznaczają, że nie każdy program będzie w stanie odczytać dane programu, w którym je stworzono. Może to oznaczać stratę dostępu do danych, np. jeśli nie zapłaci się za licencję na kolejny rok.

Przykłady:

- iTunes, największy internetowy sklep muzyczny należący do firmy Apple, do 2009 r. ograniczał utwory przy użyciu DRM – ściągnięta muzyka działała tylko na sprzęcie i oprogramowaniu od Apple; można je było wypalić na płycie maksymalnie 7 razy. Mimo usunięcia ograniczeń z muzyki i teledysków, dalej dotyczą one innych mediów.

- Ostatnie gry firmy Ubisoft działają, tylko jeśli komputer przez cały czas gry połączony jest z serwerem firmy. Oznacza to, że jeżeli firma wyłączy serwery DRM lub będą one niedostępne, nie da się grać ani w trybie wieloosobowym, z realnymi przeciwnikami przez sieć (multiplayer), ani nawet w trybie jednoosobowym wyłącznie przeciw własnemu komputerowi (single player).

- Zamknięte własnościowe kodeki (programy odczytujące różne formaty wideo i audio) i formaty takie, jak Apple Intermediate Codec czy RealMedia są skonstruowane tak, żeby działały tylko na oprogramowaniu dostarczającej je firmy. Oznacza to, że aby odtworzyć plik Apple Intermediate musimy posiadać zainstalowany program iTunes. Określenia „zamknięte” używamy tu dla odróżnienia ich od „otwartych” kodeków FLOSS.

- Zabezpieczenia przeciw kopiowaniu płyt Sony BMG tworzyły dziury ułatwiające działanie złośliwego oprogramowania na komputerze, na którym je odtwarzano. Program zawarty na płycie miał uniemożliwić jej kopiowanie za pomocą popularnych przegrywarek płyt oraz ripowanie (zgrywanie płyty audio do formatów np. Mp3). Sony BMG później zostało na drodze sądowej zmuszone do wycofania płyt z takim oprogramowaniem i naprawienia szkód na komputerach użytkowników.

Licencje

Licencje są umową, kliknięcie *ok* jest jak podpis. Licencja może zobowiązywać do dodatkowych opłat, specjalnych warunków użytkowania, określać czas działania programu, np. licencja D&R License (*Death and Repudiation*) wymaga, żeby osoba używająca programu była martwa. Czy ktokolwiek z nas przeczytał kiedyś całą licencję?

Błędy w konfiguracji

Dotyczą systemu i wszystkich programów łączących się z siecią. Podstawowe „ataki hakerskie" sprowadzają się do wykorzystania domyślnych haseł. Źle skonfigurowane oprogramowanie p2p (np. Emule, uTorrent) może domyślnie udostępnić prywatne pliki. Bardzo często pozostawiamy domyślne ustawienia świeżo zainstalowanego programu, co może oznaczać również domyślne hasła dostępu lub ich brak. Jak powszechny jest to problem, pokazuje historia określanego mianem „hakera" Gary'ego McKinnona, który oczekuje na ekstradycję do USA, po tym jak „zhakował" blisko 100 komputerów w NASA, Ministerstwie Obrony, Marynarce i Armii USA. Zrobił to, używając skryptu wyszukującego komputery i oprogramowanie z domyślnymi hasłami. Przez błędy w konfiguracji programów p2p udostępniono też wiele prywatnych i tajnych dokumentów, w tym plany helikoptera prezydenta USA.

SŁOWNICZEK

FLOSS – Free Libre/Open Source Software *czyli Wolne i Otwarte Oprogramowanie. Cały kod programu jest dostępny dla każdego do analizy. Znacznie utrudnia to wykorzystanie programu na niekorzyść użytkowników. Społeczność tworząca programy FLOSS kładzie duży akcent na standardowe formaty, ułatwiając przenoszenie danych między programami oraz społecznościowe rozwiązywanie problemów z programami, np. szybkie reakcje na wykryte luki w bezpieczeństwie.*

WAŻNY LINK

Open Source Alternative – http://www.osalt.com/, strona zawierające tematyczną listę najpopularniejszego oprogramowania oraz jego Otwartych i Wolnych Alternatyw, np. dla programów graficznych rodziny Adobe (takich jak PhotoShop lub Indesign) możemy znaleźć GIMP i Scribus.

Unikanie problemów i obrona

Wyszukiwanie bezpiecznego oprogramowania. Przed zainstalowaniem programu musimy dobrze wiedzieć, co robi i jak działa. Polskojęzyczna, a tym bardziej angielskojęzyczna Wikipedia oraz fora tematyczne to świetne źródło wiedzy o oprogramowaniu. Czas poświęcony na czytanie o programie to czas oszczędzony na naprawie systemu i sprzątaniu po złym oprogramowaniu. Lepiej omijać programy typu:

- **„freeware”**, dostępne za darmo, lecz ograniczone wymogami licencji, np. zabezpieczone przed kopiowaniem lub wymagające udzielenia zgodny na śledzenie, jak ich używamy;
- **„shareware”**, program ograniczony użyciem w czasie, np. 30 dni – tzw. **trail** – lub o ograniczonych opcjach w wersji bezpłatnej, np. brak opcji zapisu.

Programy freeware i shareware częściej niż jakiekolwiek inne zawierają złośliwe oprogramowanie.

Przykładowe problemy z programami typu freeware i shareware:

- **Internet Explorer 6** – starsza wersja przeglądarki Microsoftu do dziś często nieaktualizowana przez użytkowników posiada wiele luk bezpieczeństwa ułatwiających pobieranie trojanów i wirusów na Twój komputer; jest również niekompatybilna ze standardami wyświetlania stron WWW przyjętymi przez większość firm i W3C (światową organizację standaryzacyjną zajmującą się internetem).
- **Quicktime i Windows Media Player** – popularne odtwarzacze muzyki i mediów dostarczane przez odpowiednio firmy Apple i Microsoft. Brakuje im obsługi wielu formatów, o które trudno je rozszerzyć.
- **iTunes** – program firmy Apple do obsługi multimediów na komputerze oraz komunikacji z jej urządzeniami przenośnymi, np. iPhone i iPod. Program zbiera informacje o użytkowniku i może być sterowany zdalnie przez centralę oprogramowania, np. może niezależnie od nas zablokować lub wyłączyć nam jakieś opcje. Posiada bardzo niekorzystną dla użytkownika licencję.

Zadanie

Znajdźmy na Wikipedii alternatywę dla gadu-gadu, która będzie miała możliwość podłączenia równocześnie kilku komunikatorów, np. GaduGadu i Gmail Chat, i będzie gwarantowała najlepsze bezpieczeństwo. Wyszukajmy hasło „porównanie komunikatorów internetowych” lub adres: http://pl.wikipedia.org/wiki/Porównanie_komunikatorów_internetowych

PARĘ SŁÓW O KONFIGURACJI I HASŁACH

Zawsze warto przejrzeć opcje konfiguracji nowego programu lub systemu. Zawsze trzeba zmienić domyślne hasła. Przeglądanie stron z konfiguracją może być nieciekawe, ale możemy dowiedzieć się o funkcjach programu, na które wcześniej nie zwróciliśmy uwagi. Taką funkcją może być np. udostępnianie widoku naszego pulpitu albo plików z jakiegoś katalogu. Niezmienione domyślne albo banalnie proste hasła to jak zostawienie otwartych drzwi do domu od strony ulicy. Czasami jednak może zdarzyć się, że oprogramowanie zawiera złośliwe elementy wbrew woli autorów. Każdy ściągnięty program warto sprawdzić programem antywirusowym, chociaż mogą zdarzyć się fałszywe wykrycia.

Większość dystrybucji systemu Linux automatycznie potwierdza autentyczność instalowanego oprogramowania, używając kluczy kryptograficznych, na systemach Windows i Mac jest to możliwe dla bardziej zaawansowanych użytkowników. **Sumy kontrolne znane też jako „klucze md5" lub „hashe kontrolne" pozwalają potwierdzić, że plik przez nas ściągnięty to ten sam, który udostępnił programista.** Sumy kontrolne działają na zasadzie automatycznej komunikacji między komputerem, który wysyła dane (w tym momencie oblicza sumę kontrolną i dołącza ją do pakietu danych), a komputerem odbierającym dane (który również oblicza sumę kontrolną z odebranych danych i sprawdza, czy suma uzyskana przez niego zgadza się z sumą odebraną z pakietem danych). Jeśli nie, to znaczy, że dane uległy zmianie po drodze, czyli mogą być niebezpieczne lub nieprawdziwe. Głośny wśród informatyków przypadek programu Unrealircd udowodnił, że jest to istotne – autorzy oprogramowania przez ponad pół roku udostępniali ze swoich serwerów wersję oprogramowania podstawioną przez wrogiego hakera, zawierającą backdoor pozwalający przejąć kontrolę nad serwerem.

TWORZENIE MOCNYCH HASEŁ

Mocne hasło to takie, które zmniejsza prawdopodobieństwo złamania, odgadnięcia lub wykrycia przez atak słownikowy. **Atak słownikowy** to atak, w którym stosowany jest słownik najpopularniejszych haseł lub haseł, które wyciekły do sieci, np. z bazy forum internetowego czy serwisu. O takich wyciekach w Polsce informuje serwis **niebezpiecznik.pl**.

WAŻNY LINK

http://niebezpiecznik.pl/ - serwis informujący o zagrożeniach w internecie w popularnych serwisach, np. wyciekach haseł, złamanych zabezpieczniach.

Podstawy tworzenia mocnego hasła:

- Nigdy nie używaj swojego imienia, identyfikatorów lub nicków jako hasła (nawet ze zmianą wielkości liter, lub pisane wspak etc.);
- Nie używaj Imienia i nazwiska w haśle ani informacji związanych z Tobą, np. daty urodzin, nr PESEL;
- Nie używaj samych cyfr ani prostych pojedynczych słów;
- Używaj znaków spoza alfabetu i cyfr (najlepiej równocześnie);
- Pamiętaj o zmianie hasła co pewien czas.

Inne dobre sposoby generowania mocnych haseł

Passphrases – hasła budowane ze zdań. Możesz zbudować hasło z pierwszych liter słów w zdaniu, co przypomina hasło z przypadkowych liter, np.:
Hasła poniżej 8 znaków są wyjątkowo nieskuteczne i niebezpieczne – będzie jako hasło wyglądało tak: *Hp8zswnin*.

W hasłach opartych o terminy słownikowe lub proste słowa **zmień kolejność** niektórych znaków lub podmień na inne. Dla przykładu: "Zbigniew" można przekształcić w "Ibz8gniew.

DODATKI I ROZSZERZENIA

CZYM SĄ DODATKI I CZYM MOGĄ NAM GROZIĆ?

Dodatki to programy rozszerzające funkcjonalności systemu, przeglądarki bądź innych programów. Nie funkcjonują same w sobie jako osobne programy. Często instalowane są w obrębie samego programu (bez konieczności uruchamiania instalatora).

- Mają dostęp do wszystkich danych użytkownika.
- Mogą dowolnie wysyłać informacje do sieci, otwierać połączenia i strony widoczne z sieci.
- Działają zawsze, kiedy nasz komputer jest włączony.

Przykłady: Widżety, np. z pogodą, rozszerzenia pulpitu, czytniki wiadomości, download managery, zmiany wyglądu interfejsu użytkownika.

Dodatki do wielu programów dostępne w sieci mogą być pisane przez każdego, a więc nie muszą posiadać informacji o swoim dokładnym działaniu. To doskonała okazja dla oszustów chcących np. dystrybuować niechciane reklamy, a nawet wirusy. Dodatki mogą również służyć do przejmowania kontroli nad naszym komputerem i wykorzystywania go bez naszej wiedzy jako pośrednika w nielegalnych działaniach, np. dystrybuowania nielegalnych treści lub rozsyłania spamu.

Dodatki potrafią również śledzić użytkownika – od jego ruchów w sieci po sposób korzystania z komputera (zbieranie informacji o używanych przez nas programach, oglądanych filmach, słuchanej muzyce itp.). W najgorszym wypadku mogą również zbierać dane o naszej tożsamości czy hasłach.

Dlaczego rozszerzenia są wykorzystywane do śledzenia i nadużyć? Kto na tym korzysta?

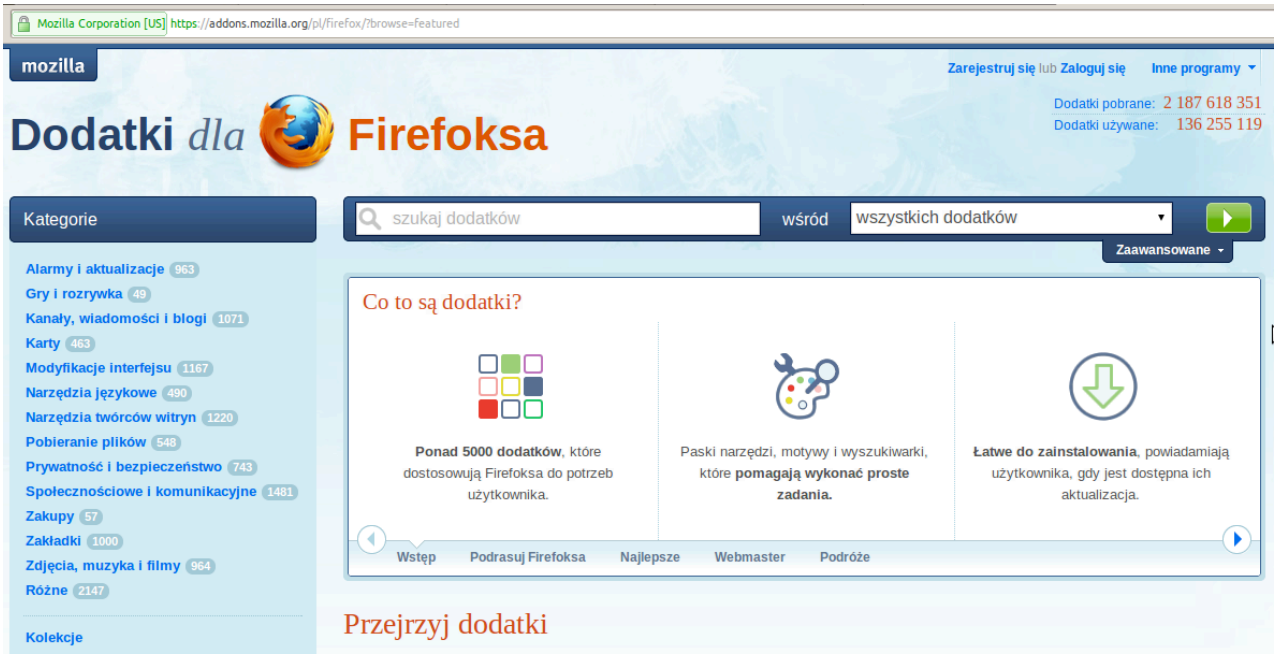
- Przestępcy – mogą uzyskać dostęp do naszych haseł, kont bankowych, danych osobowych i prywatnych;
- Hakerzy – mogą wykorzystać nasze komputery do wykonywania nielegalnych działań, ataków, pozostając anonimowymi;
- Firmy reklamowe – mogą śledzić nasze działania, poznawać dokładnie nasze preferencje;
- Organizacje – mogą sprzedawać informacje o popularności konkretnych działań w sieci.

Bundle

Nie wszystkie dodatki instalujemy świadomie. Część z nich instaluje się, oszukując nas i ukrywając prawdziwy cel swojego działania (inaczej zwane **Adware** – oprogramowanie z wykorzystaniem reklam). Bardzo często takie oprogramowanie jest wykorzystywane do szpiegowania naszych działań oraz naszego komputera. Czasami pozwala nawet przejąć kontrolę nad komputerem. W niektórych przypadkach o instalację zapyta nas normalny i celowo przez nas instalowany program jak np. eDonkey proponujący instalację spywaru „WhenUSave". Oprogramowanie Adware często znajdujemy na świeżo zakupionych komputerach, zwłaszcza laptopach. Warto wiedzieć, że może ono szkodzić lub spowalniać pracę naszego sprzętu.

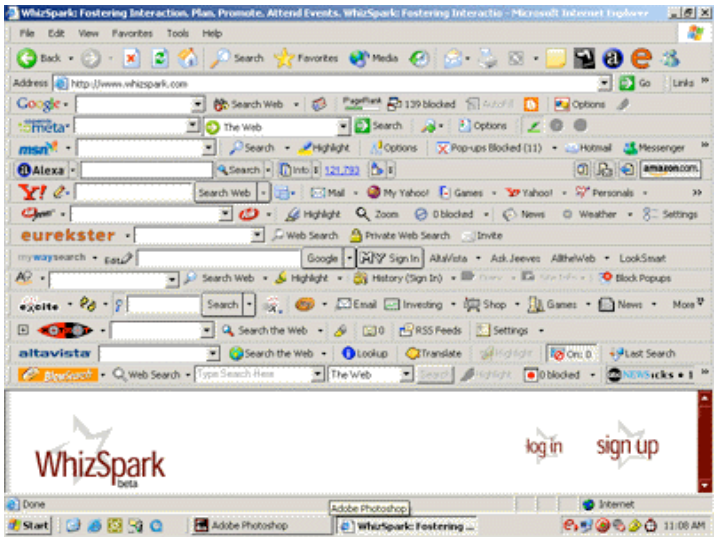
JAK SIĘ BRONIĆ PRZED SZKODLIWYMI DODATKAMI?

Bezpieczne dodatki. Większość producentów programów pozwalających tworzyć dodatki tworzy również stronę z ich listą, np. **addons.mozilla.org** dla Firefoxa, czy **chrome.google.com/extensions** dla Google Chrome. Wszystkie dodatki na tych stronach zostały sprawdzone przez twórców rozszerzanych programów i ich instalacja jest bezpieczna. Na ogół na stronach producentów jest też miejsce, w którym możemy komentować i czytać komentarze innych.



Rys.9. Strona główna dodatków dla Firefoksa – https://addons.mozilla.org/pl/.

Wiele niebezpiecznych dodatków stosuje dobrze znane chwyty mające nas przekonać do ich używania. Przed instalacją szkodliwych dodatków często pokazywana jest nam lista dodatkowych funkcji. Zasadniczo najprościej będzie nie instalować tego, co nie jest nam potrzebne. Ale bądźmy szczególnie podejrzliwi, jeśli zobaczymy słowa typu: **Bundle, Buddy, Toolbar, Advisor, Icon Set, Smilies**.



Rys.10. Skrajny przykład przeglądarki Internet Explorer przeładowanej kilkudziesięcioma dodatkami i toolbarami. Poza kwestiami estetyki i wygody pracy, każdy z dodatków zbiera informacje o naszych działaniach w sieci i jest nachalną reklamą.

Wyszukiwanie informacji

Programy są często analizowane i możemy ustalić, czy dodatek jest faktycznie niebezpieczny. Przed instalacją dodatku z niepewnego źródła poszukajmy informacji o nim w Wikipedii (jeśli to konieczne, również w angielskiej wersji). Możemy poszukać też w wyszukiwarkach: „nazwa dodatku spyware|adware". Dobrą metodą jest również przejrzenie forów dyskusyjnych. Dla większości szkodliwych rozszerzeń znajdziemy alternatywne oprogramowanie. Bardzo dobrym sygnałem jest fakt, że znaleziona alternatywa jest tzw. otwartym oprogramowaniem (FLOSS). Wynika to z tego, że społeczność programistów może analizować kod i informować innych o niebezpiecznym działaniu programów. Otwarte oprogramowanie jest dzięki temu pozbawione śledzących i szkodliwych dodatków.

Czyszczenie

Co zrobić, jeśli podejrzewamy, że już zainstalowaliśmy szkodliwe dodatki?

Zorientuj się! Po instalacji dowolnego dodatku lub oprogramowania uważnie obserwuj zachowanie systemu. Nabierz podejrzeń, jeśli pojawią się nowe ikonki w obszarze powiadomień, dodatkowe paski w przeglądarce, wszelkiego rodzaju dodatkowe elementy, których nie miało być w systemie.

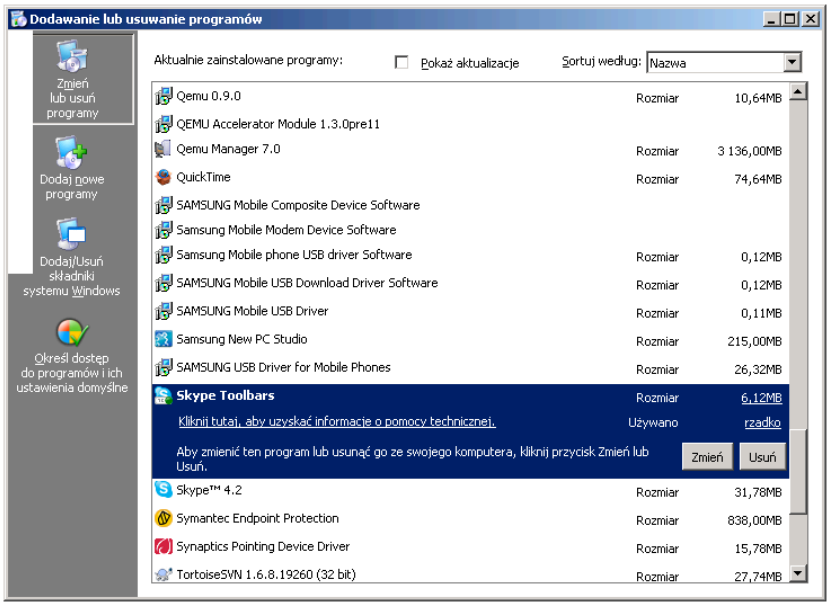
Rys.11. Pasek systemu. W przypadku systemu Windows należy bacznie obserwować pasek systemu,

komunikaty pojawiające się na nim, a w szczególności komunikaty od oprogramowania antywirusowego. Większość programów wcale nie musi działać w sposób stały i w tle.

Deinstalacja

W przypadku systemów Windows na ogół usunięcie konkretnego programu wystarczy. Powinniśmy przejrzeć listę zainstalowanych programów i zobaczyć, czy nie ma wśród nich nowych, nieznanych nam programów, które należałoby usunąć. Jeśli to nie pomaga, musimy usunąć dodatki za pomocą specjalnych programów. W takich przypadkach z pomocą przyjdzie nam doskonały program **SpyBot Seek & Destroy**. Jest on dostępny za darmo na stronie: www.safer-networking.org. W większości wypadków wystarczy ściągnąć program ze strony, uruchomić go i nacisnąć *Scan*. Na stronie znajdziemy bardzo dokładny opis, jak można wyczyścić komputer. Dokładna instrukcja instalacji: http://www.safer-networking.org/pl/tutorial/index.html.

Innym przydatnym programem jest **CC Cleaner** – umożliwia skuteczne usuwanie programów oraz zarządzanie historią w przeglądarkach internetowych. Podobnym programem dla użytkowników dystrybucji linuksa Ubuntu jest **Ubuntu Tweak**.



Rys.12. Panel sterowania. Widok opcji *Panelu Sterowania* w systemie Windows umożliwiający usuwanie zainstalowanych programów. *Panel sterowania → Dodaj lub usuń programy → usuń wybrany program*.

Zadanie

Zastanów się i sprawdź, czy programy, które zainstalowałeś z sieci, na pewno są bezpieczne? Czy ten program się sprawdził czy zaraz ściągnięty został jakiś kolejny? Czy odinstalowałeś ten pierwszy? Dlaczego te kryteria są istotne?

Wiele programów jest dystrybuowanych wyłącznie po to, by uzyskać nasze dane podczas

rejestracji, zainstalować dodatkowe oprogramowanie, np. reklamowe i śledzące. Dlatego wiele z nich posiada równocześnie ograniczone możliwości lub dość szybko okazuje się nieprzydatne.

WYSZUKIWANIE INFORMACJI

Zagrożenia:

- oszustwa i nadużycia w wynikach wyszukiwania,
- manipulacje SEO (search engine optimization),
- instalacja złośliwego oprogramowania,
- zbieranie danych behawioralnych i tworzenie profili osobowych.

Oszustwa i nadużycia – takie manipulacje nazwami stron i ich pozycją w wyszukiwarkach, aby zachęcić nas do wejścia w konkretne miejsce (w najlepszym razie nieudostępniające interesującej nas treści). **Śledzenie wyszukiwań** – ciągi kolejnych fraz tworzą dokładną historię na nasz temat, te ciągi są zapisywane i analizowane. Autorzy **złośliwego oprogramowania** mogą wykorzystywać to oprogramowanie, aby nas przekonać do jego instalacji; autorzy **złośliwych stron** – aby wyciągnąć od nas jak największą ilość danych osobowych; **organizacje reklamowe** – aby tworzyć modele behawioralne i pokazywać wycelowane w nas reklamy.

Ważne: samo wyszukiwanie nie jest bardzo niebezpieczne. Najbardziej trzeba uważać, w co klikamy, jak już wyszukamy informacje.

Jak szukamy?

- Świadomie: szukanie tematów, stron, osób, w obrębie konkretnej strony, plików i treści.
- Nieświadomie: wpisując nazwę strony (a nie jej adres) w pasku adresu; wykorzystując pola z „automatycznym podpowiadaniem”; nawigując po stronach z formularzami.

Gdzie szukamy?

- Lokalnie: nie wysyłając żadnych informacji poza swój lokalny komputer; w historii odwiedzin; w aktualnie otwartym dokumencie.
- Zdalnie: zlecając wyszukanie informacji serwerom w internecie, wyszukiwarkom treści z całego internetu, wyszukiwarkom tematycznym (szukanie plików, wiadomości, porównywarki cen itp.) lub konkretnym serwisom (sklepy, ogłoszenia, encyklopedie itp.).

„Oszustwa”

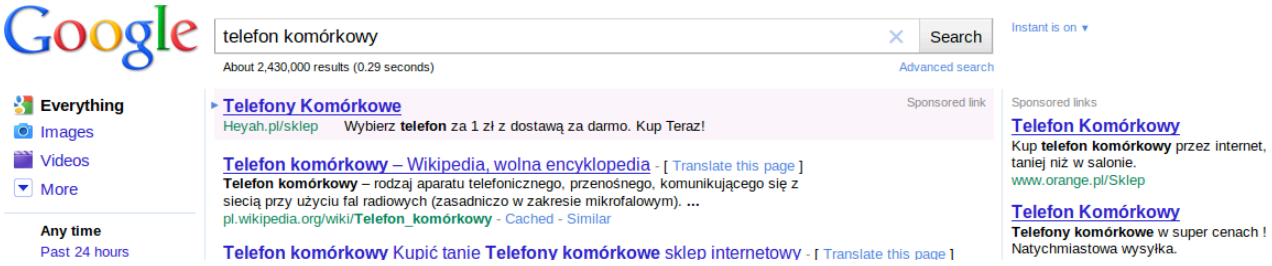
W sieci istnieją specjalnie spreparowane strony próbujące jak najlepiej dopasować się do naszego wyszukiwania i zachęcić nas do ich odwiedzenia, przy możliwie najmniejszych kosztach własnych. Największy koszt to w szczególności faktyczne dostarczenie nam tego, czego szukamy.

Stronom tym zależy głównie, żebyśmy w czasie poszukiwania interesującej nas informacji, jak najwięcej klikali i oglądali jak najwięcej reklam. Na ogół na tych stronach nie znajdziemy więc interesującej nas informacji, a ponieważ wyświetlane na nich rezultaty nie są w żaden sposób sprawdzane, możemy z nich trafić na stronę z niebezpieczną zawartością. W większości przypadków nie są to duże oszustwa, ale co najmniej oddalają nas od tego, czego w internecie szukamy. Czasami może się to jednak skończyć zawirusowanym komputerem.

SEO SPAM – strony, które nie posiadają żadnej zawartości bądź są na nich tylko kopie zawartości innych stron. Strony SEO spam utworzone są tak, aby zawsze pokazywać się na jak najwyższych wynikach w wyszukiwarkach, szczególnie przy ogólnych frazach. Często możemy je spotkać, np. wyszukując napisy do filmów.

Pseudo wyszukiwarki – zamiast trafiać na stronę z interesującą nas zawartością, z wyszukiwarki przechodzimy na stronę kolejnej wyszukiwarki pokazującej reklamowo spreparowane wyniki.

Linki sponsorowane – firmy płacą wyszukiwarkom za reklamowanie ich produktów, obchodząc mechanizmy wyszukiwania i dopasowując się tylko do części wyszukiwanej frazy.



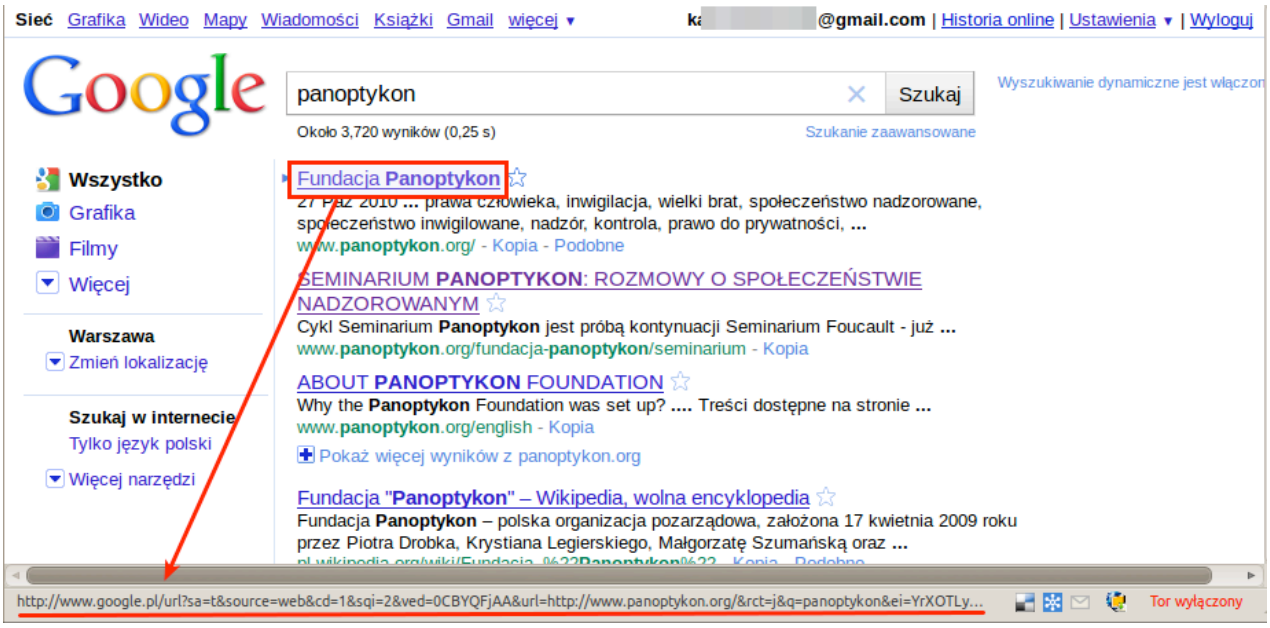
Rys.13. Linki sponsorowane. Oznakowane linki sponsorowane w wynikach wyszukiwania Google, w wielu mniejszych wyszukiwarkach linki sponsorowane nie są oznakowane. Kolejne wyniki również mogą być zaburzone, np. przez SEO spam.

W czasie wyszukiwania informacji, wiele wyszukiwarek bardzo dokładnie śledzi wyszukiwane przez nas frazy, bez względu na to czy szukamy świadomie, czy nie. Taka informacja służy później dostarczeniu nam reklam, na które jesteśmy bardziej podatni. Jest ona również dość długo składowana, co pozwala odtworzyć nasze zainteresowania, działania, a jeśli nie jesteśmy wystarczająco ostrożni – nawet sieci kontrahentów, znajomych, dane osobowe.

Historia wyszukiwanych fraz jest zapisywana nie tylko w historii przeglądania, ale również składowana (w samej wyszukiwarce, w oprogramowaniu strony, na którą trafiamy) i pamiętana przez część stron pośredniczących pomiędzy wyszukiwarką a interesującą nas stroną. Jeśli korzystamy z wyszukiwarki Google i jesteśmy równocześnie zalogowani do jednej z wielu usług tej

firmy historia naszych wyszukiwań zostaje zapisana również w pamięci naszego konta (jak ją usunąć zobacz w rozdziale Web 2.0).

Linkouty – systemy sprawdzające, na które wyszukiwane strony wchodzimy. Przykładowo każde kliknięcie na wynik wyszukiwania w Google oznacza przejście przez adres wysyłający informację do Google o tym, kto i w wyniku jakiej frazy wchodzi na jaką stronę.



Rys.14. Działanie link outu. Najechanie na link Fundacja Panoptykon wcale nie kieruje nas na adres podany pod wynikiem www.panoptykon.org – po drodze przechodzimy przez link widoczny w pasku stanu przeglądarki, który zbiera dane o naszym ruchu i przesyła je na serwery Google.

Jak się bronić?

„Oszustwa". Nieuczciwe strony na całe szczęście w większości wypadków łatwo zidentyfikować.

- **Linki**: patrzmy na linki, unikajmy stron, których adresy są wyjątkowo zbieżne z naszym wyszukiwaniem. Zwracajmy uwagę na długie domeny, posiadające naszą frazę, a po kropce „jakieś dziwne szlaczki". Tytuły i opisy stron wyglądają również zaskakująco podobnie do naszego wyszukiwania albo są ciągiem podobnych fraz. Jeśli po kliknięciu widzimy kolejną listę wyników – zamiast klikać, wróćmy do poprzedniej wyszukiwarki. Podobnie, jeśli widzimy stronę zawierającą same linki lub bardzo dużo reklam.
- **Frazy wyszukiwania**: starajmy się stosować możliwie skomplikowane frazy, dzięki temu szybciej trafimy do celu, a przy okazji uzyskujemy mniejsze prawdopodobieństwo zobaczenia którejś z nieuczciwych stron. Manipulujmy kolejnością słów w wyszukiwaniu – wyszukiwarki

traktują słowa na początku jako najważniejsze, na końcu jako najmniej ważne. Jeśli będziemy również korzystać z odpowiednio skonfigurowanej przeglądarki i posiadać system antywirusowy możemy liczyć, że przed wieloma zagrożeniami nas ostrzegą, lecz zawsze musimy być czujni.

Identyfikacja przeglądarki

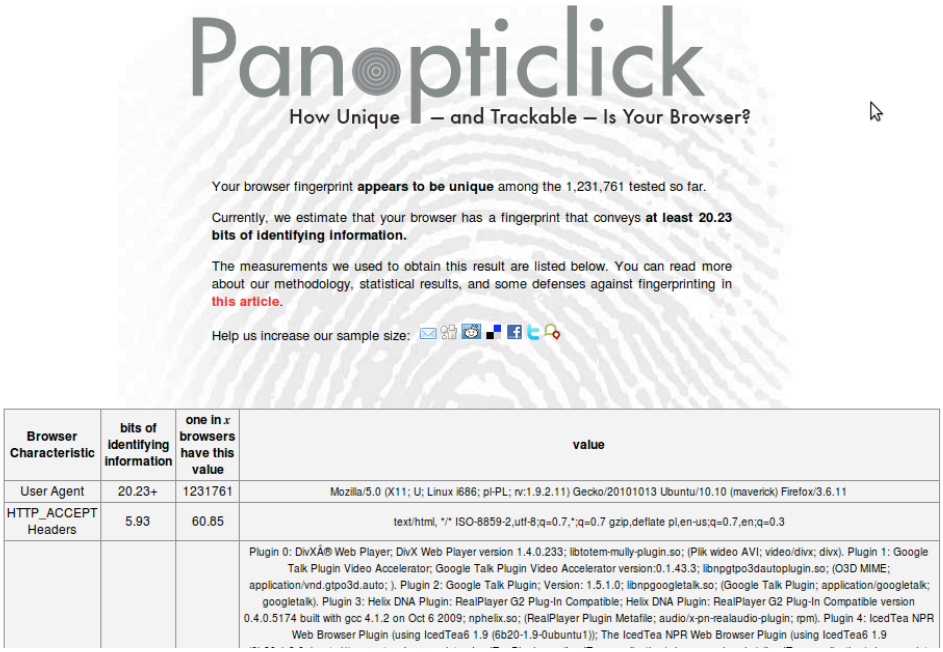
Każdy dodatek lub rozszerzenie zwiększa indywidualność naszej przeglądarki. W plikach cookies wysyłamy takie dane, jak rodzaj systemu operacyjnego, jego język, ale również rozdzielczość ekranu, informacje o oprogramowaniu wspierającym, jego wersjach, a tym samym nasza przeglądarka staje się wyjątkowo łatwo identyfikowalna. Dodatki i rozszerzenia również ułatwiają jej identyfikację. Jak bardzo nasze przeglądarki są unikalne możemy sprawdzić na stronie projektu Electronic Frontier Foundation – Panopticlik lub Privacy Protector.

WAŻNY LINK

Panopticlik : https://panopticlick.eff.org/

Privacy Protector: http://scanner.privacyprotector.eu/

Rys. 15. Panopticlick – wyniki unikalności przeglądarki autora.



Śledzenie

W internecie nie można pozostać anonimowym, ale można ograniczyć ilość organizacji mających możliwość śledzenia. Konfigurując przeglądarkę, możemy:

- Kazać przeglądarce czyścić pliki cookies przy zamknięciu, co uniemożliwi śledzącym identyfikację nas;
- Zainstalować dodatki blokujące reklamy: np. AdBlock;
- Zainstalować dodatki poprawiające prywatność: Better Privacy, Ghostery, które blokują inne formy śledzenia niż cookies.

SŁOWNICZEK

__Anonymizer__ lub __anonimowe proxy__ jest narzędziem służącym do ukrywania naszej aktywności w sieci w czasie realnym. Są to serwery proxy, które działają jako pośrednicy w komunikacji między komputerem klienckim a resztą Internetu, zabezpieczające dane komputera łączącego się z nimi. Przykładowymi anonimizatorami są __TOR__ (opisywany szczegółowo dalej) czy __I2P Sieć Anonimowa__.

WAŻNY LINK

What They Know **–** http://blogs.wsj.com/wtk/ projekt czasopisma „Wall Street Journal" wizualizujący ilość danych zbieraną za pomocą ciasteczek i danych z przeglądarki pozyskiwanych przez najpopularniejsze strony na świecie.

ŚCIĄGANIE DANYCH Z INTERNETU

Zagrożenia i problemy

Kiedy pobieramy dane, wysyłamy też sporo informacji o sobie. Dzięki analizie ruchu wiele o nas i o tym, co ściągamy może dowiedzieć się prawie dowolna osoba w sieci. O ile nie używamy sieci anonimizującej, takiej jak tor, freenet czy gnutella, zawsze można ustalić:

- źródło połączenia;
- adres IP;
- stronę, która skierowała nas na ten plik;
- wykorzystywany typ transmisji;
- używany do tego program;
- w przypadku przeglądarek ich ustawienia i adres IP.

Adres IP to zmienny, ale pozwalający zidentyfikować konkretny komputer adres sieciowy.

Przeglądarki domyślnie informują strony, jaka była poprzednia strona – z jakiej strony uruchomiono link, aby dojść na aktualną stronę; jaki protokół transmisji (sposób, „język" w jakim komunikuje się ze źródłem danych nasz komputer) został do tego użyty. Przeglądarki informując strony, zostawiają tzw. „odcisk", który wraz z innymi danymi dostępnymi źródłu pozwala zidentyfikować konkretny komputer.

Każdy pośrednik na drodze naszej komunikacji wie, skąd i dokąd jest połączenie, może określić jego typ i ilość danych, a o ile transfer nie jest szyfrowany – może poznać również jego zawartość. W przypadku niektórych protokołów P2P, np. BitTorrent, dostęp do informacji o tym, co i od kogo ściągamy może uzyskać każda osoba udostępniająca ten plik w ramach tego samego **trackera** (serwera sieci przekazującej informacje o innych użytkownikach pobierających ten sam plik). Informacje te może przejąć np. nasz dostawca internetu lub dowolna osoba w naszej lokalnej sieci. Do przejmowania danych służą takie programy jak **WireShark**, których obsługa nie wymaga wcale specjalistycznej wiedzy „hackerskiej".

SŁOWNICZEK

P2P *(od ang. peer-to-peer – równy z równym) – model komunikacji w sieci komputerowej, który zapewnia każdemu użytkownikowi takie same prawa (w przeciwieństwie do modelu klient-serwer, w którym klient musi polegać na serwerze). W sieciach P2P każdy komputer może jednocześnie pełnić zarówno funkcję klienta, jak i serwera. Cała komunikacja obywa się bez pośrednictwa centralnego serwera, co zapewnia jej elastyczność i brak ograniczeń dla nowych użytkowników przed przyłączeniem się. Najpopularniejszymi systemami opartymi o model P2P są sieci wymiany plików takie jak BitTorrent oraz komunikatory, np. Skype.*

Torrent (protokół BitTorrent) *– protokół wymiany i dystrybucji plików przez Internet, opracowany w celu zmniejszenia ruchu na głównym serwerze udostępniającym pliki. Jego największą zaletą jest podział pasma pomiędzy osoby, które w tym samym czasie pobierają dany plik, czyli w momencie ściągania pliku równocześnie udostępniamy go kolejnym użytkownikom.*
System jest zintegrowany ze stroną WWW serwera (trackerem), a sam proces pobierania plików różni się od zwykłego pobierania plików z serwera koniecznością ściągnięcia publicznie dostępnych metaplików o rozszerzeniu .torrent. Te małe pliki odpowiadające za znalezienie docelowego pliku uruchamiane są za pomocą klienta Torrensu, np. Programu uTorrent lub Azureus, które ściągają plik docelowy.

Uszkodzenia danych

Przy pobieraniu danych z użyciem przeglądarek i ich standardowych narzędzi do pobierania możliwe jest uszkodzenie pobieranego pliku, np. w razie tymczasowego zerwania połączenia. Aby tego uniknąć należy weryfikować źródła – czy źródło rzeczywiście zawiera dane, które chcemy ściągnąć? Samo pojawienie się w wynikach wyszukiwania interesującego nas zwrotu nie gwarantuje, że rzeczywiście są tam interesujące nas pliki. Znacznie lepiej wykorzystywać znane i zaufane strony. Informacje na temat większości popularnych stron znajdziemy na Wikipedii lub wyszukując ich nazwę. Nigdy nie instalujemy żadnego oprogramowania, którego strony „wymagają", żeby dostarczyć nam interesującą nas treść. Więcej informacji znajdziemy w części kursu dotyczącej wyszukiwania informacji.

Szyfrowanie transmisji

- Wiele stron umożliwia transfer przy użyciu protokołu SSL. Żeby sprawdzić, czy jest to możliwe wystarczy zmienić protokół w adresie strony: z http://przyklad.pl na https://przyklad.pl.

- Programy typu p2p mają zazwyczaj opcję szyfrowanego transferu.
- Zamiast FTP możemy używać szyfrowanej alternatywy – SFTP.

Weryfikacja zawartości

Większość programów BitTorrent pozwala nam sprawdzić zawartość „torrenta" przed ściągnięciem go na dysk. W przypadku systemu Windows zawsze pierwszym krokiem po ściągnięciu powinno być przeskanowanie plików przy użyciu programu antywirusowego. Na systemach Linuxowych bez problemu możemy sprawdzić hash MD5 i potwierdzić, że plik nie został zmieniony ani uszkodzony podczas transferu (sprawdzanie sum kontrolnych MD5 wykorzystywane jest np. przy ściąganiu płyt instalacyjnych z systemami Linux i pozwala potwierdzić, że plik dotarł do nas nienaruszony).

SŁOWNICZEK

SFTP *(ang. SSH File Transfer Protocol) – protokół typu klient-serwer, który umożliwia przesyłanie plików z i na serwer poprzez sieć TCP/IP. Jest on pozbawiony wad, które posiada zwykły protokół FTP. Przesyłając plik przy użyciu protokołu FTP, uzyskujemy szybki transfer danych, ale nie zyskujemy bezpieczeństwa, np. brak szyfrowania haseł. Znaczną poprawę bezpieczeństwa przynosi protokół SFTP, który nie wymaga na danym hoście posiadania serwera FTP, wystarczy konto SSH którego jest on rozszerzeniem, używa jego struktury oraz przez nie się łączy. Program* ***FileZilla*** *obsługuje protokół SFTP jak również FTPS (FTP z użyciem szyfrowania SSL).*

GRY

Co nam grozi?

- Zapisywanie danych przez aplikacje interaktywne (quizy, gry);
- Wykorzystywanie aplikacji (np. ankiet) do pozyskiwania adresów emailowych i danych osobowych;
- Łudzenie korzyścią (np. wirtualną walutą), żeby wykorzystać graczy;
- Nieuczciwa konkurencja ze strony innych graczy (skrypty i boty);
- Nieuczciwość organizatora roz(g)rywki.

SŁOWNICZEK

***BOT** - to program, który wykonuje pewne czynności w zastępstwie człowieka w grach (np. fikcyjny przeciwnik), programach i serwisach (np. boty w Wikipedii poprawiają proste błędy edytorów). Czasem zadaniem bota może być udawanie człowieka w celu oszustwa lub wyłudzenia danych.*

Zapisywanie danych przez aplikacje interaktywne

Dane często są gromadzone w taki sposób, że na dysku komputera oraz na serwerach, na których działa aplikacja, pozostaje dokładny zapis sieciowej aktywności użytkownika. Zapis na dysku lokalnym może oznaczać, że np. ktokolwiek z dostępem do tego komputera może poznać nasze odpowiedzi w psychoteście albo sprawdzić, czym zajmowaliśmy się w trakcie pracy.

Pozyskiwanie adresów emailowych i danych

Podając adres email jakiejkolwiek aplikacji, można założyć, że wyląduje on na listach spamerów. Nawet najbardziej znane firmy informatyczne i komunikacyjne mają problemy z bezpiecznym przetrzymywaniem danych. Aplikacje (gry, quizy) na Facebooku mogą uzyskać dostęp do danych osobowych osoby, która ich używa i wszystkich jej przyjaciół – zatwierdzając domyślny dostęp do profilu dla aplikacji na Facebooku możemy dać jej dostęp do wszystkich danych w profilu naszym i wszystkich naszych znajomych. Wyciek danych ze strony AT&T ujawnił dane (między innymi nazwiska i adresy email) 114 tysięcy użytkowników iPadów.

Łudzenie korzyścią

Wykorzystywanie graczy jest często prostym sposobem osiągnięcia celu finansowego. Wiele gier i usług wykorzystuje wirtualne waluty, czyli punkty zakupywane za realne pieniądze lub za wykonywane czynności. Wirtualna waluta może być niską ceną za nasze dane osobowe lub prozaiczne działania, jak zwiększanie ruchu na stronach z reklamami. Wirtualną walutę FarmVille (gry na Facebooku) można było zdobyć, między innymi instalując belkę (bar) Zwinky zawierającą oprogramowanie szpiegujące użytkowników – była to część oficjalnej oferty firmy odpowiedzialnej za grę. Punkty można było też dostać za wysłanie do kongresmenów USA listu protestacyjnego przeciw reformie służby zdrowia.

Nieuczciwa konkurencja

Jeśli w grę wchodzą pieniądze, zawsze należy zakładać, że inni gracze mogą oszukiwać, np. nigdy nie wiemy, jakie oprogramowanie ma u siebie osoba, z którą gramy. Nasz przeciwnik sam może być równie dobrze programem (botem). Skrypty mogą pomóc innym graczom uzyskać nieuczciwą przewagę w grze. W grach pokerowych możliwe jest wykorzystanie skryptów do liczenia kart albo botów grających (czasami w parę) przeciw ludzkim graczom tak, żeby uzyskać przewagę nad ludźmi. Już w tej chwili istnieją programy zdolne w rozmowie wyłudzić od ludzi dane osobowe. Interakcja w grze jest na znacznie niższym poziomie, więc łatwiej ukryć fakt, że nie gramy przeciwko człowiekowi.

Nieuczciwość organizatora rozrywki

Może przejawiać się rozmaicie, np. przez ukrywanie opłat, konstruowanie gry na niekorzyść gracza. Nigdy nie mamy też pewności czy pracownicy firmy odpowiedzialnej za grę są uczciwi i nie uzyskają dostępu do opcji administracyjnych. Znany jest przypadek pracownika strony pokerowej, który wykorzystywał możliwość podglądania kart przeciwników.

Kradzież wirtualnych obiektów i tożsamości

Wirtualny obiekt być można ukraść łatwiej niż fizyczny przedmiot. Nierzadko kradzione są wirtualne obiekty o wartości tysięcy złotych. Kradzież obiektów lub postaci z gry może przynieść wymierne korzyści graczom, np. na aukcjach. W czerwcu 2010 r. grupa nastoletnich złodziei z Danii ukradła „meble” z gry „Hobbo hotel” o wartości 4 tys. euro. Dochodzenie w tej sprawie prowadziła policja z Finlandii. W lutym 2008 r. policja stanu Minnesota odmówiła przyjęcia zgłoszenia kradzieży przedmiotów i wirtualnej waluty wartej około 4 tys. dolarów. Można szacować, że dochodzi do wielu znacznie mniejszych kradzieży, które nigdy nie są odnotowywane.

Jak się bronić? Zawsze należy się zastanowić zamiast bezmyślnie klikać ok!

Należy podejść ze szczególną uwagą do sytuacji wymagających płatności i podawania danych. Wielu zagrożeń i błędów da się uniknąć, czytając uważnie komunikaty i instrukcje. Podstawą jest również nieudostępnianie niepotrzebnych danych oraz czyszczenie cookies i flashcookies (patrz. Ustawienia przeglądarki). Bardzo przydatnym jest również używanie tzw. disposable email w sytuacjach niewymagających stałego korzystania z danych rejestracyjnych.

Przeciwko graczom może zostać wykorzystany cały arsenał internetowych oszustw, np. propozycje ściągnięcia niebezpiecznego oprogramowania, sfingowane emaile mające wyłudzić od nas dane logowania. Trzeba brać to pod uwagę w przypadku każdej aplikacji, gdzie w grę wchodzą pieniądze lub prestiż. Najlepszą formą obrony jest zawsze uwaga i rozważne działanie. Nie da się stworzyć listy wszystkich zagrożeń, ale istnieje prosta recepta na ominięcie zdecydowanej większości – myślenie. Podejrzane propozycje i fałszywe emaile przeważnie można rozpoznać – wystarczy im się przyjrzeć. Ilekroć wrogo do nas nastawione osoby chcą nas wykorzystać, liczą przede wszystkim na naszą nieuwagę.

Udostępnianie danych

Zawsze udostępniamy możliwie najmniej danych i, o ile nie jest to absolutnie konieczne, nie podajemy prawdziwych danych. Pamiętajmy: po co gra czy quiz ma znać nasze imię i nazwisko? Po co email, jeśli kontaktujemy się już wewnątrz gry? Czy na prawdę koniecznie musimy dostać wyniki każdej ankiety, w której bierzemy udział? A może ktoś po prostu próbuje te dane wyłudzić, proponując fałszywe korzyści...?

Facebook

Założenie, że portal dba o naszą prywatność jest błędem. Domyślne ustawienia dążą do przekazania maksymalnej ilości informacji na nasz temat. Jeżeli to tylko możliwe, należy maksymalnie ograniczać dostęp do danych osobowych. Jeśli to niemożliwe, należy się zastanowić, czy rzeczywiście musimy skorzystać z danej aplikacji. Należy pamiętać o czyszczeniu cookies i flashcookies.