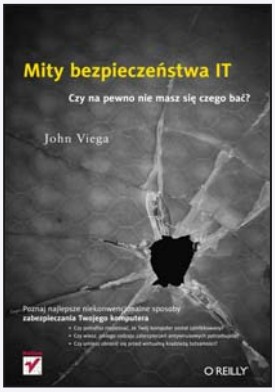
Mity bezpieczeństwa IT. Czy na pewno nie masz się czego bać?



Autor: John Viega
Tłumaczenie: Andrzej Grażyński
ISBN: 978-83-246-2588-8
Tytuł oryginału: The Myths of Security: What the Computer Security Industry Doesn't Want You to Know
Format: A5, stron: 280

Poznaj najlepsze niekonwencjonalne sposoby zabezpieczania Twojego komputera

- Czy potrafisz rozpoznać, że Twój komputer został zainfekowany?
- Czy wiesz, jakiego rodzaju zabezpieczeń antywirusowych potrzebujesz?
- Czy umiesz obronić się przed wirtualną kradzieżą tożsamości?

Jeśli Twoja odpowiedź na powyższe pytania była przecząca i nie masz pojęcia, czy w Twoim komputerze działa jakikolwiek program antywirusowy, powinieneś natychmiast przeczytać ten podręcznik. A jeśli odpowiedziałeś twierdząco i z racji wykonywanej pracy doskonale znasz się na zabezpieczeniach komputerów – ta książka jest również dla Ciebie. Oto masz przed sobą śmiało wyłożone kontrowersyjne poglądy (dotyczące zarówno bezpieczeństwa, jak i odpowiedzialności za jego brak), które raz na zawsze zmienią Twoją opinię na ten temat i zainspirują do niekonwencjonalnych działań w tym zakresie.

W książce „Mity bezpieczeństwa IT. Czy na pewno nie masz się czego bać?" znajdziesz niebanalne i kontrowersyjne informacje nie tylko na temat zabezpieczeń, ale także sposobów ich łamania, dzięki czemu zyskasz wiedzę, skąd może nadejść zagrożenie i w jaki sposób je rozpoznać. Dzięki temu podręcznikowi poznasz konkretne problemy i niedoskonałości systemów zabezpieczeń oraz sposoby wprowadzania zmian i nowych rozwiązań. Dowiesz się, jak sprawnie zarządzać aktualizacjami, przeciwdziałać kradzieżom tożsamości, a przede wszystkim szybko zidentyfikować groźbę ataku i możliwość zainfekowania Twojego komputera.

- Testy dobrego zabezpieczenia
- Antywirusy
- Systemy antywłamaniowe
- Bezpieczeństwo open source
- Sprawniejsze zarządzanie aktualizacjami
- Przeciwdziałanie kradzieżom tożsamości
- Optymalne uwierzytelnianie
- Niebezpieczeństwo sieci VPN
- Dowiedz się, czego naprawdę należy bać się w sieci i jak zapewnić bezpieczeństwo Twojego komputera!

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

Spis treści

Ułomny przemysł zabezpieczeń

Jako uczeń college'u współtworzyłem projekt Alice, kierowany przez Randy'ego Pauscha znanego ze swego *Ostatniego wykładu*[1]. System Alice był systemem trójwymiarowego symulowania rzeczywistości wirtualnej — praca nad nim nauczyła mnie kilku mądrych rzeczy. Pierwotne założenia Alice nie miały wiele wspólnego z rzeczywistością wirtualną ani efektami 3D, a skierowane były na łatwość budowania programów. Randy chciał opracować narzędzie umożliwiające uczniom tworzenie programów, bez konieczności uprzedniego zgłębiania arkanów programowania — pisaliby programy komputerowe, nawet o tym nie wiedząc.

Po początkowej euforii wywołanej walką świetlistym mieczem z robotami (trzymałeś w ręku latarkę, lecz w rzeczywistości wirtualnej rzucany przez nią snop światła wyglądał jak świetlisty miecz) skonstatowałem, że raczej nie jestem szczególnym entuzjastą grafiki komputerowej, zafascynowała mnie jednak łatwość, z jaką przeciętny użytkownik mógł tworzyć zaawansowane efekty graficzne.

Z Randym spotkałem się po raz pierwszy na zajęciach z inżynierii użyteczności (*Usability Engineering*), które prowadził; ich tematem było tworzenie oprogramowania łatwego w obsłudze. W tamtym czasie zastanawiałem się, czy w ogóle chcę się zajmować informatyką. Wiedziałem, że jestem w tym dobry, ale niektóre przedmioty mnie odstręczały, a wręcz zasypiałem

[1] Patrz m.in. *http://www.ostatni-wyklad.pl/ — przyp. tłum.*

na zajęciach z Fortranu czy matematyki dyskretnej. A tu Randy na pierwsze zajęcia przyniósł odtwarzacz wideo i pokazał, jak trudne mogą stawać się rzeczy banalne, w rodzaju ustawiania czasu w odtwarzaczu. Naciśnięcie wszystkich przycisków na raz powoduje, że trudno określić zamiary użytkownika; podobnie frustrujące mogą okazać się wyłączniki oświetlenia sterujące nie tymi sekcjami świateł, co powinny, albo drzwi otwierane „do siebie" zamiast „od siebie", jak można by się spodziewać.

Po czym Randy założył okulary ochronne i rozbił młotem wspomniany magnetowid oraz inne (podarowane) urządzenia z tandetnymi interfejsami użytkownika.

To było naprawdę inspirujące — wtedy uświadomiłem sobie, że właściwie cały przemysł elektroniki użytkowej jest ułomny, ponieważ nie dostarcza ludziom rozwiązań dobrych, a zaledwie akceptowalne. Projektanci zdają się wiedzieć a priori, czego chcą ich klienci, ale naprawdę o nic tych klientów nie pytają. Podobnie ma się rzecz z przemysłem oprogramowania dla komputerów. Minęło prawie 15 lat i właściwie niewiele się w tym względzie zmieniło — przeciętni użytkownicy nadal traktowani są po macoszemu. Znam wielu menedżerów projektu mających doskonałą koncepcję samego produktu, lecz tylko niewielu z nich stara się konfrontować swe wyobrażenia z opiniami przeciętnych użytkowników. Większość przywiązuje nadmierną wagę do rzeczy, które powinny być mniej znaczące od zadowolenia użytkownika — np. do intensyfikacji sprzedaży czy też tworzenia materiałów reklamowych.

Po ukończeniu college'u zająłem się zawodowo tematyką bezpieczeństwa i od 10 lat wciąż się nią zajmuję. To dziedzina niezmiernie pasjonująca, choćby z tego względu, że wszelkie niedostatki zabezpieczeń wyraźnie negatywnie odbijają się na wszelkich dziedzinach ludzkiej działalności, mających większe lub mniejsze związki z komputerami i informatyką. Użytkownicy Windows, niemal wszyscy, jakich znam, doświadczyli choć raz infekcji wirusa i w efekcie uszkodzenia ważnych plików, załamania systemu czy innych objawów skutkujących zmniejszeniem produktywności. Już w college'u mogłem się przekonać, jak luki w oprogramowaniu komputerów podłączonych do internetu umożliwiają hakerom zdalne manipulowa-

nie zawartością tych komputerów i w konsekwencji ich unieruchomienie. Wszystko przez niewiarygodnie subtelne (wydawałoby się) luki w oprogramowaniu pochodzącym od dostawców trzecich.

Bardzo szybko zgłębiłem już istniejące technologie i zacząłem się przygotowywać do swojego pierwszego uderzenia. Wraz z Garym McGrawem napisałem pierwszą książkę o tworzeniu oprogramowania wolnego od błędów bezpieczeństwa — *Building Secure Software* (Addison-Wesley) — a potem kilka innych; szczególnie dumny jestem z *Secure Programming Cookbook* (O'Reilly; *http://oreilly.com/catalog/9780596003944/*). Założyłem też firmę o nazwie Secure Software, zajmującą się tworzeniem narzędzi do automatycznego wyszukiwania potencjalnych problemów z zabezpieczeniami przy użyciu analizy kodu tworzonego przez programistów (firma ta została wchłonięta przez Fortify Software, gdzie obecnie jestem członkiem komitetu doradczego). Kolejny szczebel mojej kariery zawodowej to stanowisko wiceprezesa i głównego architekta zabezpieczeń (*Chief Security Architect*) w McAfee, znanego na całym świecie lidera w zakresie *dedykowanej* produkcji środków bezpieczeństwa IT (co prawda, Symantec jest kilkakrotnie większy, lecz zajmuje się także sprawami innymi niż zabezpieczenia, co McAfee pozwala dzierżyć palmę pierwszeństwa w zakresie zabezpieczeń sensu stricto). Po kilku latach, podczas których zajmowałem się przejęciami i fuzjami oraz zarządzaniem technologiami bazowymi dla większości produktów McAfee, m.in. silnikiem antywirusowym, odszedłem do nowo tworzonej firmy IT. Po rocznej przerwie wróciłem do McAfee jako dyrektor techniczny działu Software-as-a-Service.

Po dziesięciu latach mojego dyrektorowania świat zabezpieczeń nie wydaje się lepszy, a pod wieloma względami sprawy mają się nawet gorzej. Wszak społeczność internautów rozrosła się niepomiernie, a właściwa realizacja zabezpieczeń jest sprawą niewiarygodnie trudną.

I faktycznie, rozglądając się po świecie zabezpieczeń, widzę to, co mój przyjaciel Mark Curphey zwykł określać jako *security bullshit*. Producenci zabezpieczeń nie koncentrują się na dostarczaniu swoim klientom dobrych rozwiązań. Co gorsza, nie są też zainteresowani sprzedawaniem bezpieczniejszych rozwiązań, mimo że to właśnie sugerują.

Weźmy jako przykład podstawę wszelkich zabezpieczeń — programy antywirusowe — większość użytkowników zdaje sobie sprawę z konieczności ich posiadania. Jednak wielu uważa, że nie spełniają one należycie swej roli i trudno temu odczuciu odmówić racji, a przecież dostawcy oprogramowania AV wciąż doskonalą swe produkty. Rozwiązania antywirusowe często mają 15-letnią historię i zdają się być adekwatne właśnie do swych początków, a nie współczesności. Większość głównych graczy na rynku mogłaby przez ten czas wyprodukować coś znacznie lepszego, ale za sprawą inercji mamy do czynienia z oprogramowaniem zużywającym zbyt wiele zasobów systemu i zdolnym powstrzymywać bodaj nie więcej niż połowę potencjalnych infekcji.

Podobnie jak Randy Pausch obnażał wady koncepcyjne konstrukcji magnetowidu, tak ja zamierzam przyczynić się do lepszego zrozumienia, co złego dzieje się w przemyśle zabezpieczeń; czynię to z zamiarem uświadomienia przynajmniej wąskiej grupie ludzi, że potrzeby klientów powinni traktować jako nadrzędne.

Motywem przewodnim tej książki jest przedstawienie obecnego obrazu przemysłu zabezpieczeń z mojej perspektywy. Staram się, jak tylko to możliwe, nie tylko wskazywać konkretne problemy, lecz także przedstawiać konkretne propozycje koniecznych zmian. Mój krytycyzm odnosi się do większości firm, lecz nie jest to reguła, np. bardzo cieszę się z osiągnięć McAfee na przestrzeni kilku ostatnich lat. Osiągnięcia te są przede wszystkim owocem bacznego słuchania zdania klientów oraz wielu innych inteligentnych ludzi. Nie chcę tu nadmiernie eksponować samej firmy McAfee, jednak w większości przypadków opisywane problemy mają z nią związek — dla każdego problemu albo znaleźliśmy już rozwiązanie, albo go poszukujemy. Nie wierzę w żadne cudowne rozwiązania w zakresie bezpieczeństwa, jestem natomiast przekonany, że użytkownicy nie powinni żałować pieniędzy na narzędzia zapewniające im zarówno komfort pracy (np. oprogramowanie antywirusowe, które nie spowalnia komputera zbyt drastycznie), jak i wystarczający stopień bezpieczeństwa (czyli oprogramowanie na poziomie lepszym, niż dyktowany li tylko przez elementarną przyzwoitość). Niestety, wiele podstawowych rzeczy zrobiono zdecydowanie źle, co odcisnęło swe negatywne piętno na całym przemyśle zabezpieczeń — przemysł ten jest ułomny, bo ułomne są jego podstawy.

ROZDZIAŁ 2.

Bezpieczeństwo — któż się tym przejmuje?

To dziwne, jak powszechne wśród użytkowników komputerów jest niedocenianie ryku zabezpieczeń. Nie tak dawno przecież, w roku 2001, świat usłyszał o robakach Code Red, Nimda i Code Red II, a wszystkie czołowe dzienniki regularnie prześcigały się, podając nowinki o masowych infekcjach komputerów. Od tego czasu intensywność podobnych publikacji poczęła sukcesywnie maleć i jedynie Zotob z roku 2005 zdaje się niepodzielnie królować w tej materii (choć jego popularność nie może równać się tej z roku 2001), mimo iż Storm Worm stanowił dla użytkowników poważniejszy problem.

Tak było, gdy zacząłem pisać tę książkę. Gdy ją skończyłem, rewelacje na temat robaka Conficker wypełniały publikacje technologiczne ostatnich sześciu miesięcy. Każdy, kto zajmował się bezpieczeństwem (bądź w ogóle komputerami), o nim słyszał. Jednak zagadywani przeze mnie przyjaciele i rodzina nie wiedzieli nic o Confickerze, mimo codziennego studiowania serwisów informacyjnych — musieli widzieć artykuły na ten temat, ale prawdopodobnie pomijali je. Nawet niektórzy moi koledzy po fachu nie mieli o nim pojęcia — dotyczyło to szczególnie wielu z tych, którzy dawno temu przesiedli się na komputery Macintosh.

Obecnie problematyka zabezpieczeń zajmuje dużo miejsca na łamach prasy technicznej, natomiast reszta świata rzadko o niej słyszy, a przecież szkodliwe oprogramowanie (*malware*) wszelkiego autoramentu mnoży się w tempie wykładniczym. Dlaczego tak się dzieje, mimo inwestowania coraz

większych nakładów w zwalczanie szkodliwego oprogramowania (jak również w jego wytwarzanie)? Otóż, dziennikarze nie piszą o tym, ponieważ ludzi to nie interesuje, a niepojawianie się tematyki w codziennej prasie przekłada się na dalszy spadek zainteresowania tematem — i tak oto nakręca się spirala sprzężenia zwrotnego ignorancji bezpieczeństwa. Istnieją — oczywiście — i inne przyczyny nikłego zainteresowania zwykłego użytkownika problemami bezpieczeństwa. Oto one.

Szkodnik woli pozostawać w ukryciu

Zwykle pierwszymi objawami infekcji, jakich można by się spodziewać, są drastyczne spowolnienie komputera i zasypywanie użytkownika strumieniem reklam. Nietrudno jednak skonstatować, że objawy infekcji — w doprowadzenie do której zainwestowano być może mnóstwo pieniędzy — nie mogą być aż tak oczywiste dla użytkownika, ten bowiem mógłby wówczas natychmiast podjąć środki zaradcze. Dzisiejsze *malware* jest bardziej dyskretne: jeśli nawet powoduje wyświetlanie reklam, czyni to z umiarem, być może zastępując własnymi reklamami te prawdziwe. W efekcie użytkownik nie wie, iż jego komputer jest zainfekowany i pozostaje w błogim przekonaniu, że zabezpieczenia należycie spełniają swą rolę, a możliwość zaatakowania komputera nie wydaje mu się wielkim problemem.

Użytkownicy nie interesują się zabezpieczeniami

Jeśli wszystkie zabezpieczenia funkcjonują prawidłowo (czego nie można bezkrytycznie założyć), użytkownik jest należycie chroniony przed zagrożeniami, a wielu nawet nie zdaje sobie sprawy, że w ich komputerze funkcjonuje program antywirusowy. Po prostu nigdy nie widzieli go w akcji i nic nie wiedzą o jego roli.

Skutki infekcji nie muszą być poważne

Gdy zdarza się przechwycenie numerów kart kredytowych, haseł, kont i identyfikatorów na dużą skalę, mówi się o internetowej apokalipsie. Użytkownicy obawiają się transakcji internetowych, wielu całkowicie rezygnuje z dokonywania zakupów przez internet. Pozostali wykazują mniejszą nieufność, bo to firmy zajmujące się obsługą kart kredytowych ponoszą odpowiedzialność finansową. Zresztą przechwycenie numeru karty nastąpić może również w warunkach bardziej kameralnych niż

sieć, np. na zapleczu restauracji, gdy nieuczciwy kelner, przed włożeniem karty do terminala, korzystając z nieuwagi (ufnego) klienta, zeskanuje zawartość paska karty.

Temat zbyt nudny

Dla przeciętnego człowieka nazwy Code Red, Nimda, Zotob, Storm Worm oznaczają mniej więcej to samo. Bezpieczeństwo komputerowe nie jest wdzięczną tematyką i przy okazji nowego incydentu nagłówki gazet brzmią prawie tak samo jak poprzednio. Co prawda, inne są nazwy szkodników, szybkości i metody ich rozprzestrzeniania, skutki destrukcji itd., lecz przeciętny czytelnik nie czuje się jakoś szczególnie zagrożony i artykułów na ten temat zwyczajnie nie czyta, a dziennikarze przestają je pisywać. Cóż, biznes to biznes.

Brak zaufania do przemysłu zabezpieczeń

Ludzie uważają, że nieciekawy jest świat, w którym znajdują się wyłącznie rzeczy dobrze im znane, np. nie interesują ich specjalnie programy antywirusowe, które „przeważnie działają" i „spowalniają komputer". Prawda to czy nie (w tym przypadku akurat tak), ale przemysł zabezpieczeń nie ma zbyt dobrej prasy wśród przeciętnych użytkowników (iluż to pytało mnie, zupełnie serio, czy McAfee sam produkuje wirusy, które potem wykrywa jego oprogramowanie) i wszelkie historie opowiadane przez producentów i dostawców zabezpieczeń traktowane są jako nie do końca zasługujące na zaufanie.

To, że sama tematyka bezpieczeństwa komputerowego wywołuje u przeciętnego człowieka odruch ziewania, jest tylko spostrzeżeniem socjologicznym, ważniejsze są natomiast technologiczne konsekwencje tegoż dla przemysłu zabezpieczeń.

- Użytkownicy nie rozróżniają poszczególnych produktów, oczekując jednego, który wszystko załatwi.
- Użytkownicy nie są skłonni płacić zbyt wiele za zabezpieczenia. Oczekują pojedynczego produktu, czują się okradani, gdy proponuje im się pakiety zintegrowane, nie widzą zbytniej różnicy między darmowymi zwykle wersjami *entry-level* i płatnymi wersjami *premium*. Świadomość wartości oferowanych przez te ostatnie jest znikoma, często postrzegane są jak magazyn nikomu niepotrzebnej funkcjonalności.

- W powszechnym odczuciu użytkowników (zwłaszcza Windows) antywirus to coś, co „trzeba mieć", nawet jeśli nie jest się głęboko przekonanym o jego skuteczności.

Kolejną konsekwencją wspomnianej nieświadomości jest fakt, że wielu użytkowników nie interesuje się tym, czy ich oprogramowanie antywirusowe rzeczywiście działa! Często oprogramowanie to preinstalowane jest przez dostawcę sprzętu (OEM) na nowym komputerze i cechuje się ograniczonym okresem używalności, zwykle nie dłuższym niż rok. Po tym czasie konieczne jest odnowienie licencji, zakupienie pełnej wersji itp., zależnie od konkretnego produktu, o czym użytkownicy zapominają, przekonani, że otrzymali „darmowy" produkt na zawsze. Komunikaty przypominające o zbliżającym się upływie licencji są ignorowane, a gdy przychodzi „dzień zero", antywirus przestaje działać i komputer pozbawiony zostaje ochrony (czym użytkownik także się zbytnio nie przejmuje).

Nie wydaje się, by istniała prosta recepta na zmianę tej świadomości. Moim zdaniem, w wyobrażeniach klientów wartość ochrony komputerów systematycznie spada, szczególnie wskutek darmowych rozwiązań antywirusowych w rodzaju AVG, Avir czy Avast (przepraszam świat *open source*, nie wspomniałem o ClamAV). Jeśli nawet darmowe programy antywirusowe są produktami w gruncie rzeczy kiepskimi, znajdują licznych użytkowników, kierujących się raczej względami cenowymi niż jakościowymi. Nie chcę przez to powiedzieć, że bardziej znana marka koniecznie oznacza lepsze produkty, na pewno jednak znana marka jest dobrym punktem wyjścia do poszukiwań. W przekonaniu konsumentów program uznanej marki musi być wystarczająco kompetentny, w przeciwnym razie firma nie odniosłaby sukcesu.

Myślę, że droga będzie długa i ciernista. Konieczne jest przezwyciężenie wielu problemów, które postaram się naświetlić w następnych rozdziałach.

Trafią Cię łatwiej, niż myślisz

Znam wielu aroganckich geeków[1], którzy nie obawiają się zagrożenia ze strony *malware*, bowiem w swym przekonaniu postępują bardzo ostrożnie i żaden szkodnik nie ma prawa przedostać się na ich komputery. Wtórują im legiony użytkowników Apple przekonanych, że system operacyjny Mac OS X jest (magicznie) lepszy niż większość konkurentów, i — oczywiście — użytkownicy Visty, uważający ją za najbezpieczniejszy system na świecie, jaki kiedykolwiek stworzono.

Ludzie ci myślą tak, jak chcą intruzi czyhający na zasoby ich komputerów. „Trafienie" komputera jest wówczas łatwiejsze, niż można by się spodziewać, i w praktyce może oznaczać kilka rzeczy. Może sprowadzać się do zainstalowania szkodliwego oprogramowania, może także polegać na niekontrolowanym wycieku danych z komputera (za sprawą tegoż szkodliwego oprogramowania lub z innych przyczyn).

Zacznijmy od zainfekowania komputera (czyli od instalacji złośliwego oprogramowania). Najczęściej dokonuje tego własnoręcznie sam użytkownik. Wystarczyć w tym celu jedno nawet kliknięcie linku przesłanego pocztą elektroniczną bądź uruchomienie pobranej z internetu szkodliwej aplikacji, udającej „porządny" program lub uaktualnienie do tegoż.

Bogactwo technik podstępu, stosowanych przez hakerów, jest przeogromne. Wielką rolę gra tu ludzka psychika i środki socjotechniczne, prowadzące

[1] Patrz np. *http://pl.wikipedia.org/wiki/Geek — przyp. tłum.*

do tego, że użytkownik pobierający szkodnika przekonany jest, iż pobiera „przyzwoite" oprogramowanie. Przykładowo nastolatek pobierający efektowną tapetę na pulpit nie podejrzewa, że dołączona do niej „wtyczka do Media Playera" nie ma z tym ostatnim nic wspólnego (bądź — co gorsza — ma, ale skrywa jeszcze wirus, instalowany wraz z tym pluginem). Kliknięcie hiperłącza *click here* (rysunek 3.1) uruchamia proces pobierania i instalowania wymienionych komponentów. Żeby wszystko wyglądało jeszcze bardziej wiarygodnie, nowego dodatku można użyć do odtworzenia wideo.

Rysunek 3.1. *Malware można skutecznie maskować pod postacią niewzbudzającego podejrzeń odnośnika do pluginu Media Player*

Wśród oprogramowania skrywającego w sobie *malware* na czoło wysuwają się wygaszacze ekranów. We wszystkich serwisach oferujących bogaty repertuar wygaszaczy znajdują się też takie, które są jednocześnie źródłem *malware*. Podobnie prawdopodobnym jego źródłem mogą być darmowe gry i inne samowykonywalne (z rozszerzeniem *.exe*) aplikacje.

Oczywiście, szanujący się geek jest świadomy sytuacji i jednocześnie przekonany o swej przebiegłości: nie korzysta z linków, które nie cieszą się powszechnym uznaniem (czyli cechują się niskim licznikiem kliknięć), bo takowe nie pochodzą raczej z wiarygodnego źródła. To jednak nie wystarcza,

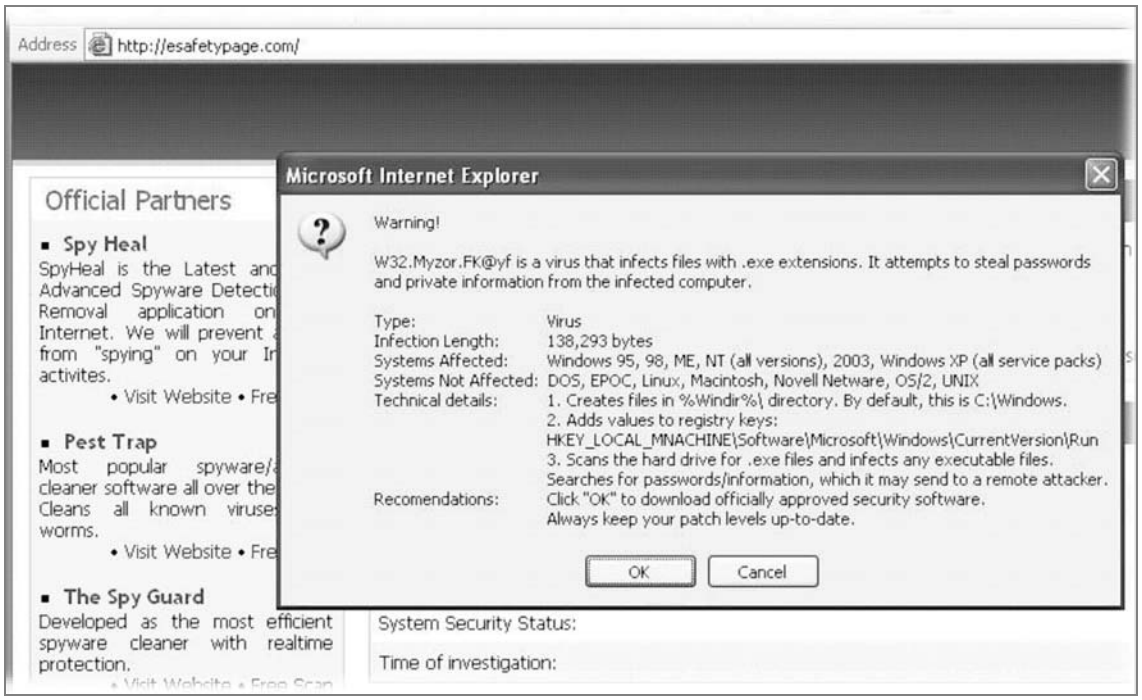
bowiem w wielu przypadkach, myśląc, że pobierasz pewną aplikację, możesz pobrać naprawdę inną. Dzieje się tak np. wtedy, gdy złośliwy użytkownik Twojej sieci lokalnej przypuści atak typu *man-in-the-middle* albo przeprowadzi zatrucie pamięci cache DNS (nie obawiaj się, jeśli pojęcia te nic Ci nie mówią; ich znaczenie nie jest w tej chwili istotne). Ataki takie zdarzają się jednak stosunkowo rzadko.

Innym sposobem „przejęcia" komputera jest wykorzystanie luk w mechanizmach bezpieczeństwa systemu operacyjnego, zwłaszcza w jego częściach komunikujących się z internetem oraz w przeglądarkach WWW. Przeglądarki są tak skomplikowane, że w ich masywnym kodzie nietrudno przeoczyć lukę, niezależnie od tego, jak bardzo chciałoby się jej uniknąć (do tej kwestii powrócę w kolejnych rozdziałach). Autorzy szkodliwych stron WWW celują w wykorzystywaniu takich luk: załadowanie spreparowanej strony WWW do „dziurawej" przeglądarki, działającej w „dziurawym" systemie operacyjnym prowadzi zwykle do zainstalowania *malware*.

Przeglądarki są ważną, lecz nie jedyną kategorią „dziurawego" oprogramowania. Równie dobrze lukę spotkać można w aplikacji biurowej, np. w MS Word, gdzie załadowanie spreparowanego dokumentu prowadzić może do zainstalowania *malware*.

Podobnie dziurawym komponentem systemu operacyjnego są usługi (*services*) firmy Microsoft — programy, które działają w tle, uruchamiane automatycznie wraz ze startem systemu lub w momencie zalogowania użytkownika. Zadaniem wielu z nich jest komunikowanie się z innymi komputerami w sieci. Intruz, znając lukę bezpieczeństwa w kodzie danej usługi, łączy się z nią i uzyskuje dostęp do komputera, z wiadomymi konsekwencjami, ale bez świadomości użytkownika. Rozmaite techniki — z zaporami sieciowymi na czele — mają za zadanie paraliżowanie tego typu poczynania przez ukrywanie wybranych usług przed światem zewnętrznym. Nawet i to nie likwiduje całkowicie ryzyka, bowiem usługi te widoczne są dla innych komputerów *wewnątrz* sieci korporacyjnej. Jednakże zestaw usług widocznych domyślnie dla innych komputerów ogranicza się do kilku podstawowych mechanizmów komunikacyjnych (choć w przeszłości nawet i one stanowiły nie lada problem).

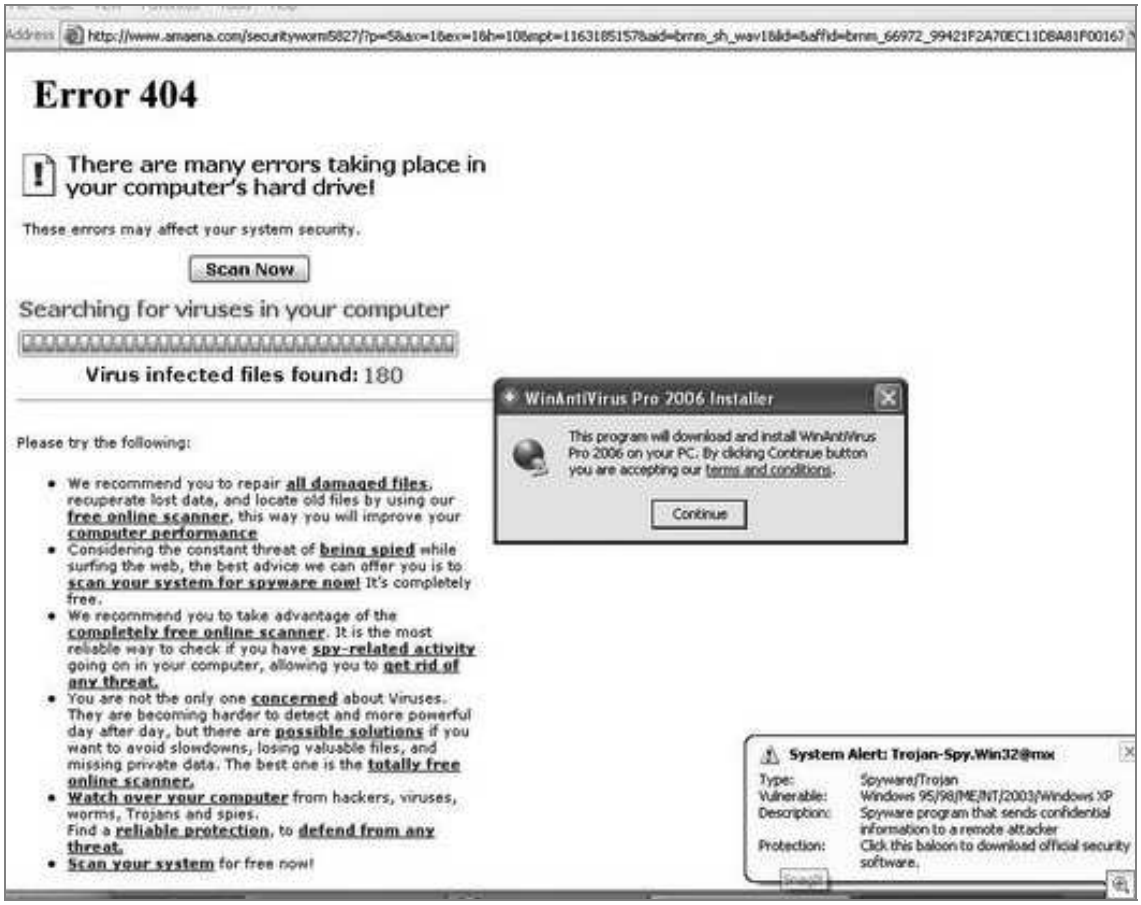
Jednak nawet załatanie wszystkich luk w zabezpieczeniach przeglądarki nie likwiduje zagrożenia, bowiem przed ekranem komputera znajduje się najbardziej zawodny element systemu — użytkownik. Zadziwiająco skutecznym chwytem jest podszywanie się programów szkodników pod legalne oprogramowanie — coś, co zewnętrznie wygląda bez zarzutu, kryje w sobie destrukcyjne mechanizmy; bezkrytyczne ufanie pozorom może prowadzić do katastrofy. Przykładowo drobny błąd literowy w adresie URL spowodować może przekierowanie do strony wyświetlającej komunikat o rzekomym zagrożeniu wirusowym i zalecenie pobrania „odtrutki"; kliknięcie przycisku *OK* (rysunek 3.2) powoduje, że zamiast odtrutki wsączana jest prawdziwa trucizna. Sugerowana odtrutka może też mieć formę oprogramowania antyszpiegowskiego (rysunek 3.3).



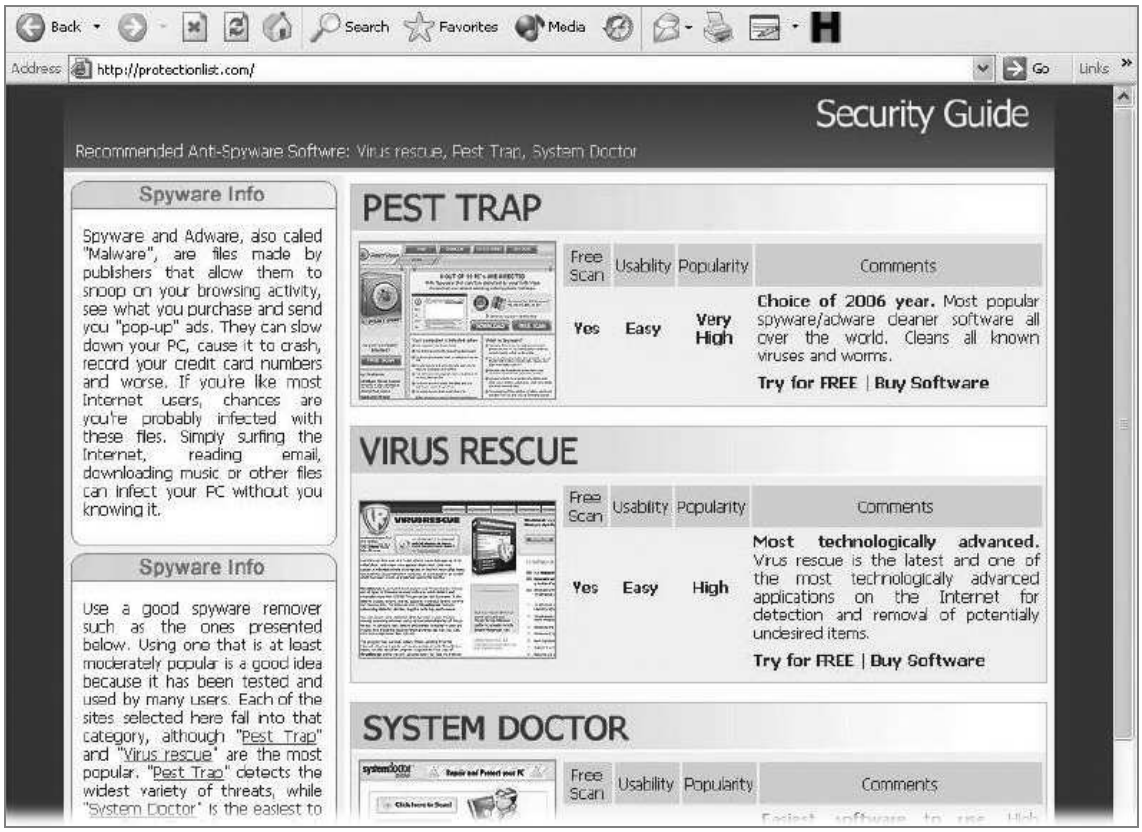
Rysunek 3.2. *Jeden z trików stosowanych przez producentów malware: oferowany antywirus jest w rzeczywistości malware*

Dla użytkowników Windows wyświetlane komunikaty zdają się być bardziej wiarygodne, jeśli wyglądają na pochodzące od producenta, czyli firmy Microsoft. Na rysunku 3.4 widzimy efektowny monit o zainstalowanie antywirusa, a bogactwo oferowanych opcji (rysunek 3.5) ma ów monit jeszcze bardziej uwiarygodnić.

Rysunek 3.3. *Podobny trik — sugerowane jest pobranie oprogramowania antyszpiegowskiego*



Rysunek 3.4. *Fałszywy monit wyglądający jak regularny komunikat Windows*



Rysunek 3.5. *Bardziej uwiarygodniona odmiana fałszywego monitu*

To wszystko nie przekonuje jednak wielu aroganckich użytkowników, którzy czują się bezpieczni, bo nie zaglądają na podejrzane strony, nie potrzebują zatem żadnego oprogramowania zabezpieczającego, a przed niepożądaną ingerencją z zewnątrz chroni ich komputer zapora sieciowa, która nie dopuszcza do nieuprawnionego wysyłania danych nawet wtedy, kiedy działające na komputerze usługi są zainfekowane.

Nie obawiają się też, że padną ofiarami *phishingu*. Nauczyli się już ignorować e-maile pochodzące z eBay, które nie zawierają ich osobistego identyfikatora (spamerzy nie używają indywidualnych identyfikatorów klientów, bo ich po prostu nie znają). Nie pobierają też „kartki od znajomego", jeśli imię i nazwisko nadawcy nie zostało wymienione. Mimo to znam kilka przypadków, kiedy ostrożność ta okazała się niewystarczająca.

Autorzy *phishingu* stosują w zasadzie te same, działające techniki, lecz czasem wrzucają wyższy bieg. Kilka tygodni przed napisaniem tych słów byłem świadkiem phishingowych e-maili zawierających informację o paczce kierowanej do adresata i niemożności dostarczenia jej z powodu braku dokładnych danych adresowych. E-maile wyglądały tak, jakby wysłane

zostały przez firmę UPS; podanie szczegółowych danych miało spowodować, że paczka zostanie doręczona. Jako że chwyt był na wskroś nowatorski, wielu nawet bardzo ostrożnych użytkowników dało się nabrać.

Pisherzy nie ustają w poszukiwaniu nowych technik. Jedną z nich jest phishing selektywny, tzw. *spearphishing*, kierowany do konkretnych firm lub nawet osób. Użytkownik otrzymuje e-mail wyglądający tak, jakby wysłany był z jego firmowej sieci; w treści komunikatu znajduje się prośba o zmianę hasła użytkownika na firmowym serwerze, bowiem okres ważności aktualnego hasła dobiega końca. Użytkownik loguje się za pomocą dotychczasowego hasła, wpisuje zmienione hasło — to pierwsze wędruje do rzeczywistego autora e-maila, drugie przepada bezpowrotnie, na serwerze nic się nie zmienia.

Spearphishing sprawdza się znakomicie w portalach społecznościowych, gdzie łatwo wykonać chwyt na „kartkę od znajomego". Chwyt rozpoczyna się od poznania adresu e-mail potencjalnej ofiary na podstawie imienia i nazwiska[2]. Jeżeli natomiast pisher dysponuje gotowym adresem e-mail, może wydedukować imię jego właściciela, np. za pomocą prostego przeszukiwania internetu (co daje się łatwo automatyzować).

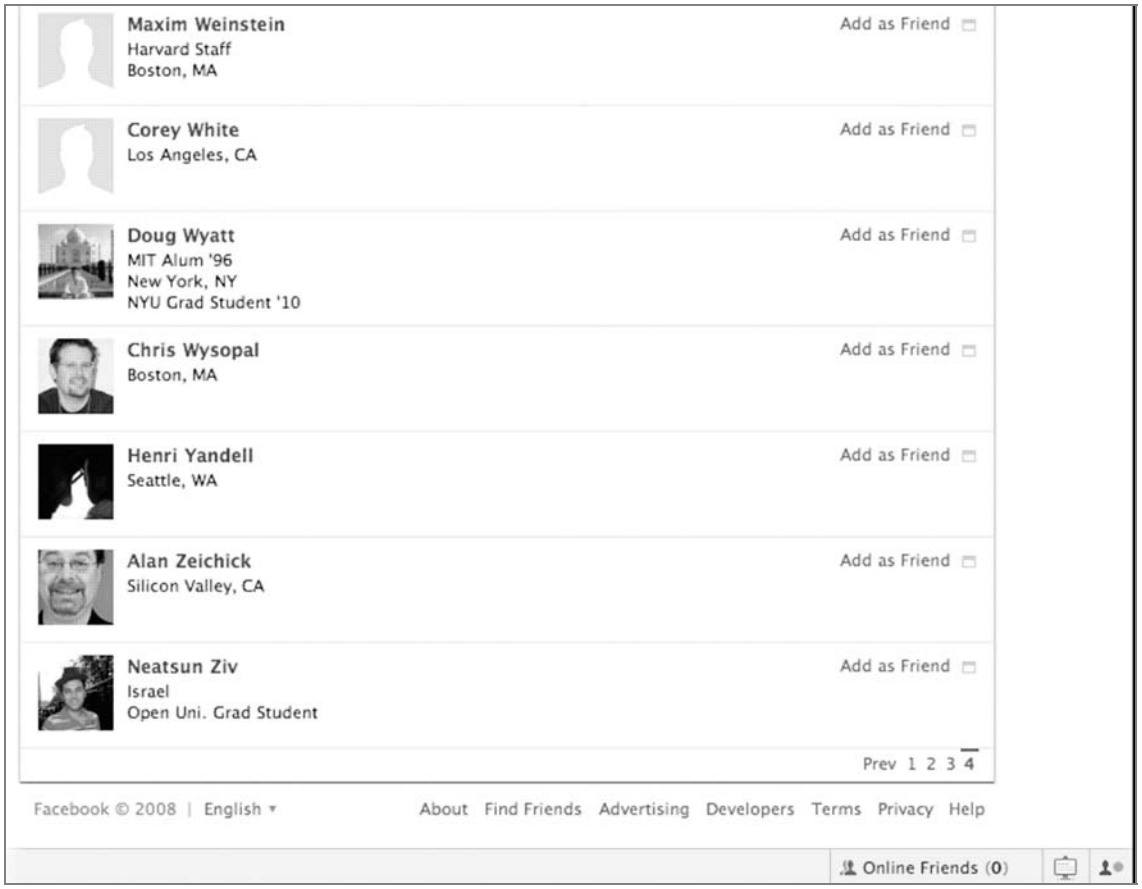
Gdyby wspomnianym pisherem był mój kolega, z pewnością odnalazłby mnie na Facebooku (rysunek 3.6 — na potrzeby tego eksperymentu utworzyłem nowe fikcyjne konto [bez znajomych], które potem skasowałem).

Skoro mamy już ofiarę — adresata — pora na znalezienie nadawcy, który wyda się mu wiarygodny. W tym celu najprościej przejrzeć listę jego znajomych (rysunek 3.7).

Wspaniale, jest z czego wybierać. Jeżeli fałszywy nadawca podszyje się pod osobę mieszkającą np. w Bostonie, MA, analizując mój życiorys zawodowy (rysunek 3.8), z pewnością znajdzie szczegóły zdolne dostatecznie uwiarygodnić treść e-maila.

[2] Ponieważ nie zawsze istnieje prosta odpowiedniość między ciągiem „imię.nazwisko" a adresem e-mail, phisher generuje serię prawdopodobnych adresów w nadziei, że któryś z nich okaże się autentyczny — *przyp. tłum.*

Rysunek 3.6. *Krok 1. eksperymentalnego phishingu: znalezienie ofiary na Facebooku*



Rysunek 3.7. *Krok 2.: wybór potencjalnego nadawcy spośród znajomych adresata*

Co prawda, Facebook umożliwia ukrycie listy znajomych przed światem zewnętrznym, domyślnie są oni jednak widoczni dla wszystkich i większość użytkowników nie zmienia tego ustawienia. Pisherzy wiedzą o tym, że znane portale wyposażone są w mechanizmy detekcji użytkowników próbujących pobierać zbyt wiele informacji na raz, toteż pobierają tę informację oszczęd-

Rysunek 3.8. *Krok 3: wybór informacji osobistych adresata*

nie. Mogą sobie na to pozwolić, bowiem ich celem jest wysłanie niewielkiej liczby *ukierunkowanych* e-maili, co i tak daje im większą szansę powodzenia niż zmasowana akcja spamerska.

Znam kilku skrajnie pewnych siebie geeków, którzy unikają nawet pobierania kartek z jawnie wskazanym nadawcą i adresatem, nawet tych, które wyglądają na wysłane przez matkę czy sympatię (takie też można łatwo spreparować, wybierając znajomych z tego samego miasta). Czują się odporni na wszystkie te zagrożenia, o których dotąd napisałem.

Czują się absolutnie odporni na wszelkie przejawy podstępu socjotechnicznego!

I, jak wspomniałem, nigdy nie zaglądają na „ryzykowne" strony. Czy na pewno? Nigdy nie zaglądali na *MLB.com* (to główna strona pierwszej ligi futbolowej), stronę Economist czy typowy serwis geeków, taki jak Slashdot?

Wszystkie te serwisy zbudowane zostały w dobrej wierze, lecz — mimo to — stanowić mogą źródło infekcji. Źli faceci wykupują legalną reklamę w uznanym serwisie i od czasu do czasu wrzucają tam nielegalną zawartość, np. reklamę fałszywego antywirusa, który w rzeczywistości może być programem szpiegowskim, albo reklamę wyglądająca normalnie, ale wykorzystującą znane luki w przeglądarkach. To wszystko może się zdarzyć w dowolnym serwisie oferującym reklamy, takim jak *CNN.com*. Oczywiście, w serwisach takich funkcjonują mechanizmy próbujące eliminować szkodliwe treści, co jednak nigdy nie daje stuprocentowej skuteczności, gdyż reklamy często zawierają sporą porcję kodu, a nie tylko statyczne obrazki. Kod ten tworzony jest najczęściej w języku ActionScript firmy Adobe.

Jeżeli — mimo wszystko — uważasz, że nie grozi Ci opisane niebezpieczeństwo ze strony reklam, jesteś naprawdę zadufany w sobie. Podejrzewam, że należysz do jednej z dwóch poniższych kategorii:

- myślisz, że nie można Cię przechytrzyć i zawsze używasz tylko najnowszej wersji przeglądarki,
- myślisz, że jesteś bezpieczny, bo pracujesz w bezpiecznym środowisku — Apple i (lub) Linux — bądź też używasz nietypowej, mało popularnej przeglądarki, takiej jak Opera, albo też stosujesz inne nietypowe rozwiązanie, co chroni Cię przed niebezpieczeństwem.

Rozumowanie typowe dla kategorii pierwszej ma tę wadę, że w najnowszej wersji przeglądarki mogą zostać wykryte nowe luki w zabezpieczeniach. Od tego „dnia zerowego" do momentu opracowania odpowiedniej poprawki zawsze mija trochę czasu. Na szczęście, sytuacje takie nie są zbyt częste.

Jeżeli należysz do drugiej kategorii, nie jesteś dla intruzów celem zbyt atrakcyjnym — taniej będzie poszukać im potencjalnych ofiar w innych środowiskach. To jednak tylko część prawdy, szczególnie użytkownicy Apple mają powody do obaw, co wkrótce wyjaśnię.