

## IDC: Piracki software niebezpieczny dla firmy

Jarek Michalski

2006-11-15, ostatnia aktualizacja 2006-11-15 16:18

**Jak obniżyć koszty prowadzenia biznesu korzystając z kradzionych programów? Okazuje się, że łatwo dostępne narzędzia do łamania zabezpieczeń same mogą być bardzo niebezpieczne dla komputera**



Programy do łamania zabezpieczeń pirackich kopii są powszechnie dostępne w internecie. Ale ich używanie może wiele kosztować

### ZOBACZ TAKŻE

[Powstaje partia internetowych piratów](#) (15-11-06, 08:44)

[Obtawa na pirackie kopie Windowsa?](#) (13-11-06, 19:22)

[Gdzie piraci mają kasę fiskalną?](#) (22-10-06, 19:54)

[Windows Vista nie dla piratów](#) (05-10-06, 19:51)

### SERWISY

[Internet, technologie](#)

Sprawa jest bardzo prosta. Korzystając z ogólnodostępnych sposobów wyszukiwania bez problemu odzyskasz w sieci sposoby na "zalegalizowanie" pirackiego oprogramowania. Czy to na stronach internetowych, czy w sieci wymiany plików (słynnych peer-to-peer) - zawsze znajdzie się ktoś, kto udostępni Ci za darmo np.: fałszywe klucze do programu. Albo generatory kodów. Ściągasz program, a on generuje kod, który sprawia, że skopiowana pokątnie wersja programu, jak za dotknięciem czarodziejskiej różdżki zmienia się w "legalną". Są jeszcze cracki. To programiki, które uruchamiasz na swoim komputerze, a one obchodzą zabezpieczenia i z wersji próbnej programu (np.: takiej, która działa tylko 30 dni), robią wersję pełną - bez żadnych ograniczeń.

Jak widzisz cała sprawa jest bajecznie prosta. Każdy, nawet mało doświadczony użytkownik komputera poradzi sobie z tym bez problemu. Ty na pewno też. W końcu jesteś sprytny, prawda? Prawda. Ale Ci, którzy udostępniają takie narzędzia są jeszcze sprytniejsi.

### Kowboje - gatunek wymarły.

Wizja hakera - samotnego kowboja, który walczy z potężnymi korporacjami by przynieść ulgę portfelom biednych i ciemężonych użytkowników komputerów - działa na wyobraźnię. Niestety ma niewiele wspólnego z rzeczywistością. Czasy, w których narzędzia do łamania zabezpieczeń programów umieszczano się w sieci za darmo, tylko dla satysfakcji, odchodzą w przeszłość i raczej już nie wrócą.

Firma badawcza IDC przeprowadziła badania, których celem było ustalenie stopnia ryzyka, na jakie naraża się użytkownik komputera korzystający z pirackich programów oraz narzędzi do obchodzenia zabezpieczeń i licencji. Nie chodziło w tym przypadku o kwestię kradzieży dóbr intelektualnych. Badanie było bardzo praktyczne i dotyczyło głównie bezpieczeństwa klientów biznesowych.

Metoda była prosta. Badacze odwiedzali miejsca, które oferowały nielegalne oprogramowanie, sfałszowane klucze produktów, cracki i generatory kodów. Miejscami tymi były strony internetowe oraz sieci wymiany plików. Drugim krokiem było sprawdzenie co potrafią tego typu narzędzia. Okazało się, że potrafią wiele. I myliłby się ten, kto sądziłby, że ich działanie ogranicza się do "legalizowania" programów.

### **Supermarket paserów.**

Pierwszy wniosek jaki płynie z badania jest taki, że odnalezienie w sieci stron oferujących narzędzia do obchodzenia zasad prawa własności intelektualnej jest bardzo proste. Odwiedziny 25% witryn udostępniających tego typu programy kończyło się próbą zainstalowania na komputerze złośliwych programów, czyli aplikacji, których nie zamierza instalować użytkownik komputera i które prawie na pewno uprzykrzą mu życie.

Stopień "uprzykrzenia" może być różny. Najmniej złośliwe narzędzia podmieniają domyślną stronę główną przeglądarki, sprawiają, że podczas korzystania z internetu wyskakują okienka z reklamami, wreszcie instalują dodatki, których wcale nie życzy sobie użytkownik.

Bardziej szkodliwe wersje zaraz po zainstalowaniu zaczynają wykorzystywać większość zasobów komputera, spowalniając jego pracę, aż do całkowitego paraliżu maszyny.

Najgroźniejsze wersje umożliwiają intruzom dostęp do zainfekowanego komputera, uruchomienie na nim dowolnego programu i przejęcie kontroli nad nim.

Tego typu narzędzia mogą instalować się automatycznie, choć czasami proces ten może wymagać zgody użytkownika. Ten ostatni jest jednak najczęściej przekonany, że instaluje np.: sterowniki ActiveX.

Złośliwe programy mogą również instalować się w momencie uruchamiania cracka. Jeśli będzie on pochodził ze strony www, szansa na to, że zainfekuje komputer wynosi 11%. Jeśli jednak ściągniesz go z sieci peer-to-peer prawdopodobieństwo to wzrasta do 59%.

### **Kosztownie i niebezpiecznie.**

Jakie są skutki korzystania z tych wszystkich generatorów kodów, cracków i witryn www z fałszywymi kodami?

Jeśli trafisz na złośliwy program - mogą być oślakane. Wyskakujące okienka może i są uciążliwe, ale to drobiazg w porównaniu z niezamierzonym udostępnieniem ważnych danych (np.: haseł do kont bankowych), czy zablokowaniem pracy komputera.

Oczywiście jest to też jakaś forma oszczędności. Tyle, że to, co uda się zaoszczędzić na legalnym programie bardzo szybko może stać się drobiazgiem w obliczu jednego włamania, podczas którego ktoś wymazał np.: wszystkie dane z bazy klientów, albo skasował plik poczty. Te koszty są trudne do wyliczenia, ale z pewnością wielokrotnie przewyższają cenę legalnego programu.

Niektóre koszty daje się jednak policzyć. Wykrycie problemu, backup danych, formatowanie dysku, powtórna instalacja systemu, etc Szacunkowe obliczenia (według danych z badań przeprowadzonych w 2002 r. w Stanach Zjednoczonych przez firmę Trend Micro Inc.) pokazują, że te koszty mogą zsumować się do okrągłego 1000\$. Nie uwzględniając straty czasu pracownika, który w czasie naprawy nie może korzystać z komputera.

Zawsze można powiedzieć, że w Polsce te koszty są pewnie niższe. Firma IDC przeprowadziła badania na zlecenie Microsoftu - znajdują się więc użytkownicy, którzy będą podważać ich wyniki.

Trzeba jednak pamiętać, że narzędzi umożliwiających korzystanie z pirackiego oprogramowania nie umieszcza się w sieci dla zabawy, ani dla satysfakcji. A przynajmniej nie tylko. To po prostu biznes - w dodatku wyjątkowo nieczysty, bo ktoś zawsze na nim traci. I niebezpieczny, bo Ci, którzy udostępniają tego typu programy są najczęściej sprytniejsi od tych, którzy uruchamiają je na swoich maszynach.

Nie warto mieć złudzeń. Żaden autor cracka nie nazywa się Neo.

ŹRÓDŁO: **Komputer w firmie**