

**BIAŁA KSIĘGA**

**Ryzyko związane z pozyskiwaniem i korzystaniem z pirackiego oprogramowania**

Badania z inicjatywy Microsoft

John F. Gantz Christian A. Christiansen

Al Gillen

październik 2006 r.

**W BIAŁEJ KSIĘDZE**

Niniejsza Biała Księga prezentuje wyniki przeprowadzonego przez IDC badania poświęconego obecności złośliwych kodów i niepożądanego oprogramowania na witrynach WWW oferujących pirackie programy, fałszywe klucze produktów, narzędzia do łamania zabezpieczeń oraz generatory kluczy (numerów seryjnych) dla produktów z rodziny Microsoft Windows XP i Microsoft Office. Analiza obejmowała także kody generatorów numerów seryjnych i narzędzi do łamania zabezpieczeń, udostępniane do pobrania za pośrednictwem różnorodnych stron WWW oraz sieci typu peer-to-peer.

Celem badania było sprawdzenie stopnia, w jakim użytkownicy uzyskujący i korzystający
z pirackiego oprogramowania, narażeni są na ryzyko zagrożenia bezpieczeństwa swoich komputerów w związku z opisanymi działaniami.

**STRESZCZENIE**

* Istnieje wiele sposobów pozyskiwania i korzystania z fałszywego oprogramowania.
Do najpowszechniejszych z nich zalicza się pozyskiwanie i korzystanie z fałszywych kluczy produktu, pozyskiwanie programów typu “generator klucza” oraz korzystanie z nich w celu stworzenia kluczy produktu, a także pozyskiwanie ”narzędzi do łamania zabezpieczeń”,
a następnie wykorzystywanie ich do obchodzenia mechanizmów licencjonowania i aktywacji.
*W ramach naszego badania zweryfikowaliśmy ryzyko zagrożenia dla bezpieczeństwa wynikające z (1) wizyt na stronach WWW oferujących fałszywe klucze produktu, generatory kluczy oraz narzędzia do łamania zabezpieczeń, jak również (2) niebezpieczeństwa wynikające z pobierania i korzystania z narzędzi do łamania zabezpieczeń i generatorów kluczy udostępnianych przez strony WWW oraz sieci peer-to-peer.*
* Mechanizm prostego wyszukiwania w sieci z łatwością pozwala znaleźć witryny oferujące pirackie oprogramowanie, fałszywe klucze, narzędzia do łamania zabezpieczeń, generatory kluczy itd. Również w sieciach peer-to-peer można bez problemu uzyskać generatory kluczy i narzędzia do łamania zabezpieczeń dla produktów z rodziny Microsoft Windows i Office.
Jak więc widać, nie trudno jest znaleźć poszukiwane oprogramowanie .
* 25% odwiedzonych przez nas stron WWW, oferujących fałszywe klucze produktu, pirackie oprogramowanie, generatory kluczy lub narzędzia do łamania zabezpieczeń, podejmowało próbę instalacji złośliwego lub potencjalnie niepożądanego oprogramowania. Istnieje więc znacząca liczba stron próbujących instalować złośliwy lub niepożądany kod.
* 11% generatorów kluczy oraz narzędzi do łamania zabezpieczeń pobranych ze stron WWW oraz 59% generatorów kluczy i narzędzi do łamania zabezpieczeń pobranych z sieci peer-to-peer zawierało złośliwe bądź potencjalnie niepożądane oprogramowanie.
*Istnieje więc znacząca ilość złośliwego lub niepożądanego kodu ukryta w generatorach kluczy i narzędziach do łamania zabezpieczeń.*

Koszty ponoszone przez organizacje w celu przywrócenia prawidłowej działalności po pojedynczym ataku złośliwego oprogramowania, mogą (w przypadku jednej stacji roboczej) przekroczyć tysiąc dolarów. Z kolei koszty ponoszone przez organizację w związku z utratą lub naruszeniem bezpieczeństwa danych mogą każdorazowo dochodzić do dziesiątek tysięcy dolarów. *“Oszczędności” wynikające z eksploatacji pirackiego oprogramowania mogą zostać pochłonięte
w wyniku nawet jednorazowego naruszenia bezpieczeństwa systemu wywołanego przez złośliwe oprogramowanie..*

Typy złośliwego i niepożądanego kodu, jakie znaleźliśmy, są związane ze zmianą podejścia
ich twórców do tworzenia złośliwego oprogramowania, zauważoną przez specjalistów
ds. bezpieczeństwa Twórcy złośliwego oprogramowania najpierw prowadzili działalność hackerską dla zabawy, a teraz prowadzą ją w celu poszukiwania informacji przechowywanych na komputerach. Pozwala im to na uzyskanie nienależnych korzyści. *Oferowanie pirackiego oprogramowania, narzędzi do łamania zabezpieczeń i generatorów kluczy, może stanowić dla atakujących jeszcze jeden sposób znalezienia kolejnych ofiar swych oszustw.*

W opinii IDC podczas badań znaleziono na tyle dużo złośliwego bądź niepożądanego kodu, żeby wysnuć wniosek wskazujący, że uzyskiwanie i korzystanie z pirackiego oprogramowania może stanowić poważne ryzyko zagrożenia bezpieczeństwa osób dopuszczających się takich działań.

**POZYSKIWANIE PIRACKIEGO OPROGRAMOWANIA**

Istnieje wiele sposobów na pozyskanie nielicencjonowanego, fałszywego lub pirackiego oprogramowania[[1]](#footnote-2) przez końcowych użytkowników.

Poza nieświadomym nabywaniem pirackiego oprogramowania w ramach kanału dystrybucji lub poprzez naruszenie warunków licencji ilościowej, do najpowszechniejszych metod zalicza się:

* Pozyskiwanie fałszywych kluczy produktu z ze stron WWW oraz korzystanie z nich wraz
z oprogramowaniem uzyskanym z takich źródeł, jak znajomi lub witryny pobierania plików.
* Fałszywe klucze produktu można podzielić na umyślnie podrobione (które wydają się być oryginalne, lecz nie zostały wygenerowane przez Microsoft) oraz skradzione
(klucze produktu, które zostały skradzione z legalnej kopii produktu z rodziny Windows lub Office, na przykład poprzez ich skopiowanie z nalepki na komputerze osobistym). Takie klucze produktu stosuje się w celu obejścia mechanizmów licencjonowania i aktywacji obecnych w oprogramowaniu Microsoft.
* Pobieranie generatorów kluczy ze stron WWW oraz sieci peer-to-peer, jak również ich wykorzystywanie do stworzenia kluczy produktu niezbędnych do pracy z oprogramowaniem uzyskanym z takich źródeł jak znajomi czy witryny pobierania plików. Tutaj ponownie, generowane klucze stosuje się w celu obejścia mechanizmów licencjonowania i aktywacji obecnych w oprogramowaniu Microsoft.

Pobieranie narzędzi do łamania zabezpieczeń z witryn WWW oraz sieci typu peer-to-peer oraz ich wykorzystywanie wraz z oprogramowaniem uzyskanym z takich źródeł jak znajomi czy witryny pobierania plików. Narzędzia do łamania zabezpieczeń to programy, które ingerują w samo oprogramowanie firmy Microsoft, celem obejścia mechanizmów licencjonowania i aktywacji. Przykładami takich narzędzi są programy usuwające liczniki dat w oprogramowaniu Microsoft tak, żeby oprogramowanie zawsze pracowało w okresie karencji oraz programy ingerujące w pliki binarne Microsoft odpowiedzialne za wymuszanie aktywacji produktu.

* Pobieranie pełnych kopii pakietów oprogramowania z witryn pobierania plików lub sieci typu peer-to-peer. Niektóre procesy pobierania plików mogą trwać nawet 24 godziny.
* Kupowanie nielegalnych kopii w Internecie za pośrednictwem takich witryn jak np. eBay.
* Kupowanie nielegalnych kopii oprogramowania na giełdach i bazarach lub w sklepach komputerowych.

Naszą analizę ograniczono do pierwszych trzech metod. Czas i energia potrzebne do pobrania pełnych kopii oprogramowania lub uzyskania pirackiego oprogramowania przez Internet lub
na giełdach, bazarach i sklepach komputerowych pozostawiono poza zakresem projektu
(patrz na marginesie: *Co z fizycznymi nośnikami*? oraz eBay: *Zbliżają się kłopoty.)* Nawet jednak
w przypadku oprogramowania pozyskanego przy użyciu pozostałych trzech metod, fałszywe klucze produktu, generatory klucza lub narzędzia do łamania zabezpieczeń mogą nadal okazać się niezbędne do używania tego oprogramowania.

**METODOLOGIA ANALIZY**

Żeby ocenić ryzyko uzyskania i korzystania z pirackiego oprogramowania, IDC sprawdziła,
czy odwiedzanie witryn sieci Web proponujących narzędzia i techniki korzystania z pirackiego oprogramowania oraz pobieranie i korzystanie z generatorów kluczy oraz narzędzi do łamania zabezpieczeń naraża użytkowników na zagrożenia związane ze złośliwym lub potencjalnie niepożądanym oprogramowaniem.

IDC powołała laboratorium testowe w ramach swego działu IT, a następnie przeprowadzała przez dwa tygodnie sierpnia 2006 r. analizę witryn sieci Web oferujących pirackie i fałszywe oprogramowanie, generatory kluczy bądź narzędzia do łamania zabezpieczeń. W celu identyfikacji złośliwego
i potencjalnie niepożądanego oprogramowania skorzystano z najnowszych, komercyjnie dostępnych wersji programów do wykrywania złośliwego kodu. Następnie swój wkład w badanie wniósł zespół ds. bezpieczeństwa Microsoft, pobierając generatory kluczy i narzędzia do łamania zabezpieczeń
z analizowanych przez nas stron WWW oraz z sieci peer-to-peer.

Szczegółowe informacje na temat metodologii testów i laboratorium IDC można znaleźć w części

*Protokół z testów.*

**WYNIKI ANALIZY**

W części poniżej przedstawiono wyniki badania, w podziale na trzy odrębne sekcje. W sekcji *"Poszukiwanie fałszywego oprogramowania"* omówiono ryzyko zagrożenia bezpieczeństwa, na jakie narażony jest użytkownik odwiedzający witryny sieci Web oferujące narzędzia i techniki pozwalające na użytkowanie pirackiego oprogramowania. W sekcji *"Korzystanie z generatorów kluczy oraz narzędzi do łamania zabezpieczeń"* opisano ryzyko zagrożenia bezpieczeństwa, na jakie narażony jest użytkownik korzystający z generatorów kluczy oraz narzędzi do łamania zabezpieczeń pobranych z witryn sieci Web oraz sieci typu peer-to-peer. Z kolei sekcja *"Charakterystyka złośliwego
i niepożądanego oprogramowania"* stanowi przegląd złośliwego i niepożądanego oprogramowania wykrytego podczas naszego badania.

***POSZUKIWANIE FAŁSZYWEGO OPROGRAMOWANIA***

W sumie dotarliśmy i poddaliśmy analizom 98 niezależnych stron WWW oferujących dostęp
do fałszywych kluczy produktów, pirackiego oprogramowania oraz narzędzi do łamania zabezpieczeń produktów z rodziny Windows XP i Office. Na rys. 1 pokazaliśmy, co znaleźliśmy na takich stronach WWW przy użyciu programów do wykrywania złośliwego kodu.

**RYS. 1**

**Witryny sieci Web udostępniające klucze, generatory kluczy lub narzędzia do łamania zabezpieczeń**



Wszystkie witryny

Witryny z wykrytymi wieloma przypadkami złośliwego lub potencjalnie niepożądanego oprogramowania

Witryny zawierające złośliwe lub potencjalnie niepożądane oprogramowanie

*Źródło: Analiza IDC, Ryzyko pozyskiwania i korzystania z pirackiego oprogramowania, 2006 r.*

25 z napotkanych przez nas 98 witryn sieci Web (25%) zawierało złośliwe bądź potencjalnie niepożądane oprogramowanie; przy czym na dwóch trzecich z nich odkryliśmy po kilka wystąpień takiego oprogramowania. W niektórych przypadkach strony WWW wykorzystywały słabości zabezpieczeń, podejmując próby automatycznej instalacji niepożądanego oprogramowania. W innych przypadkach użytkownikowi sugerowano samodzielne podjęcie określonych czynności takich jak instalacja kontrolki ActiveX. Jeżeli taka instalacja była absolutnie niezbędna (np. w celu pobrania generatora klucza lub narzędzia do łamania zabezpieczeń bądź w celu dalszego przeglądania witryny), podejmowaliśmy takie czynności, zakładając, że użytkownik też by tak postąpił.

W niektórych przypadkach złośliwe kody (tzw. exploity) znajdujące się na stronach internetowych próbowały wykorzystać dziury w oprogramowaniu, załatane już wcześniej przez odpowiednie poprawki bezpieczeństwa. Tym niemniej należy uznać, że intencje osób instalujących takie oprogramowanie na stronach WWW były nieczyste. Ponadto trzeba zwrócić uwagę na fakt, że nie wszyscy użytkownicy dysponują uaktualnionym programem wykrywającym złośliwy kod lub na bieżąco pobierają wymagane aktualizacje bezpieczeństwa.

***KORZYSTANIE Z GENERATORÓW KLUCZY ORAZ NARZĘDZI DO ŁAMANIA ZABEZPIECZEŃ***

Generatory kluczy oraz narzędzia do łamania zabezpieczeń pobierano z dwóch źródeł: stron WWW oraz sieci peer-to=peer. Na rys. 2 pokazano, co znaleźliśmy w tak pobranym oprogramowaniu.

Z witryn sieci Web pobrano 116 plików, z czego 13 (11%) okazało się zawierać złośliwe bądź potencjalnie niepożądane oprogramowanie. Z sieci typu peer-to-peer pobrano 94 pliki, z czego 55 (59%) okazało się zawierać złośliwe bądź potencjalnie niepożądane oprogramowanie.

**RYS. 2**

**Pobrane klucze, generatory kluczy i narzędzia do łamania zabezpieczeń**

 **Pliki z sieci typu peer-to-peer**  **Pliki z witryn sieci Web**

**Złośliwe lub potencjalnie niepożądane oprogramowanie 11%**

**Złośliwelub potencjalnie niepożądanne oprogramowanie**

**59%**

**Czyste**

**41%**

**Czyste 89%**

 94 116

*Źródło: Analiza IDC, Ryzyko pozyskiwania i korzystania z pirackiego oprogramowania, 2006 r.*

Należy zauważyć, że same sieci typu peer-to-peer mogą stanowić niezmiernie przydatne narzędzie wymiany danych, a niektóre sieci typu peer-to-peer dysponują zintegrowanym skanowaniem antywirusowym na potrzeby ładowania i pobierania treści. Takie rozwiązanie pozwala usunąć większość złośliwego oprogramowania przed rozpoczęciem procesu jego ściągania na komputer użytkownika.

Jednak, jak wskazują nasze analizy, użytkownicy w każdym wypadku muszą zachowywać ostrożność co do rodzajów oprogramowania pobieranego z takich sieci.

***CHARAKTERYSTYKA ZŁOŚLIWEGO LUB POTENCJALNIE NIEPOŻĄDANEGO OPROGRAMOWANIA***

Podczas badania znaleźliśmy wiele różnorodnego złośliwego i potencjalnie niepożądanego oprogramowania[[2]](#footnote-3), poczynając od oprogramowania stworzonego w celu otwierania połączeń
w systemie użytkownika i zezwalania osobom trzecim na pobieranie i wykonywanie programów na zainfekowanym systemie (W32/Beagle), kończąc na oprogramowaniu wprowadzającym treści reklamowe na górze i na dole stron internetowych (Zquest).

Podczas przeszukiwania stron WWW jeden z programów, który znaleźliśmy (xpladv470), wiele razy omawiany był w Websense Security Lab[[3]](#footnote-4) jako program o obserwowanej z czasem rosnącej złośliwości. Początkowo był zwykle wykorzystywany do instalacji niepożądanego oprogramowania, takiego jak fałszywe narzędzia typu anti-spyware, paski narzędzi i oprogramowanie reklamowe typu adware. Jednak na początku 2006 r. w ramach Websense zauważono, że pliki pobierane
przez program wykonują funkcje takie jak rejestracja uderzeń klawiszy podczas uzyskiwania
przez użytkownika dostępu do bankowości internetowej oraz przekierowywanie ruchu do fałszywych witryn PayPal.

Pobrane przez nas generatory klucza i narzędzia do łamania zabezpieczeń zawierały takie robaki jak Win32.Alcra.F i Win32.KwBotF.Worm; konie trojańskie typu Trojan Dropper - Win32.VB.GK; backdoory takie jak Backdoor.Bifrose i Infostealer.Ld.Pinch.E; oraz oprogramowanie adware, takie jak ZangoSearch i DollarRevenue. Te ostatnie programy mogą monitorować zawartość okien przeglądarki sieci Web i instalować dodatkowe oprogramowanie typu adware.

**CO TO OZNACZA DLA UŻYTKOWNIKÓW?**

Wyniki testu wskazują na niebezpieczeństwa związane z pozyskiwaniem i eksploatacją pirackiego oprogramowania. Analitycy rynku zabezpieczeń IDC dzielą zaobserwowane ryzyko na trzy kategorie zagrożeń:

*Zainfekowanie niepożądanym kodem* — przybierające postać łagodną, średnio-niebezpieczną
lub poważną. Łagodna postać to np. denerwujący kod, taki jak programy adware, z całym bagażem wyskakujących okien z reklamami i zastępowaniem strony domowej. Bardziej destrukcyjny kod, taki jak konie trojańskie, może potencjalnie zapychać zasoby systemowe aż do ostatecznego unieruchomienia urządzenia. Wreszcie istnieją też potencjalnie niszczące kody, takie jak boty
i rejestratory klawiszy, które mogą doprowadzić do przejęcia kontroli nad maszyną na potrzeby wysyłania spamu, składowania nielegalnych plików oraz udostępniania osobom trzecim newralgicznych danych.

*Naruszenie systemu zabezpieczeń* – złośliwe i niepożądane oprogramowanie, takie jak kod znaleziony podczas testów, znane jest z możliwości blokowania pracy i/lub pobierania aktualizacji przez programy antywirusowe oraz zapory firewall. Niektóre programy typu adware generują nawet uporczywe reklamy fałszywych narzędzi do usuwania oprogramowania typu spyware — czasami żądając od użytkownika zapłaty za oprogramowanie niezbędne do usunięcia właśnie wygenerowanych reklam.

*Zmniejszenie wydajności aplikacji* — problemy bezpieczeństwa nie zawsze ujawniają się w sposób bezpośredni. W wielu przypadkach użytkownik po prostu zauważa problemy z systemem i wzywa dział IT. Programy typu spyware są szczególnie znane ze spowalniania pracy sieci bądź dostępu
do Internetu lub powodowania problemów z logowaniem i trudności ze zdalnym dostępem.

Nasze badania wskazują, że nawet uaktualniane systemy z najnowszym oprogramowaniem wykrywającym złośliwy kod nie są wolne od zagrożeń. Wciąż pojawiają się nowe wirusy, konie trojańskie, robaki i programy typu spyware. Ponadto trzeba zadać sobie pytanie, ilu użytkowników pozostaje zawsze na bieżąco z instalacją aktualizacji bezpieczeństwa bądź korzysta z najnowszych wersji narzędzi do wykrywania złośliwego kodu?[[4]](#footnote-5)

**JAKIE JEST RYZYKO FINANSOWE?**

Dla konsumenta, zważywszy na ryzyko zagrożenia bezpieczeństwa, koszt pozyskania i eksploatacji pirackiego oprogramowania lub fałszywej kopii produktu z rodziny Windows czy Office może obejmować koszt jednego lub większej liczby zgłoszeń serwisowych w celu oczyszczenia systemu, straty danych zgromadzonych na zainfekowanym dysku (który trzeba sformatować) lub znacznie wyższy koszt kradzieży danych personalnych.

W przypadku przedsiębiorstw koszty mogą być jeszcze wyższe. Wyniki ankiety przeprowadzonej
w 2006 r. pośród 616 amerykańskich specjalistów ds. bezpieczeństwa[[5]](#footnote-6) przez Computer Security Institute wskazują, że 65% reprezentowanych w badaniu spółek doświadczyło ataku wirusa, 32% nieupoważnionego dostępu do informacji, 15% naruszenia bezpieczeństwa systemu, a 9% kradzieży zastrzeżonych informacji — przy czym wszystkie te zagrożenia powstały wskutek działania złośliwego oprogramowania takiego jak programy wykryte podczas naszej analizy.

Dane z tej ankiety, pokazane na rys. 3 — wskazującym koszt pojedynczego ataku wg jego rodzaju
na każdego respondenta – potwierdzają, że ryzyko finansowe eksploatacji takiego oprogramowania może być wysokie.

**RYS. 3**

**Koszty złośliwego kodu**

$ 21,500

Kradzież informacji

Usuwanie wirusów

Nieupoważniony dostęp

$ 10,617

$ 7,903

*Źródło: Obliczenia własne IDC na podstawie danych z ankiety FBI/Computer Security Institute, 2006 r.; N=616*

Dane z rys. 3 pokazują koszty pojedynczego incydentu przypadające na respondenta, nie ujawniają natomiast kosztów przypadających na stację roboczą. Ile kosztowałoby rozwiązanie problemu pojedynczego incydentu na jednym komputerze?

Odpowiedź oczywiście różni się w zależności od firmy lub użytkownika, a także od rodzaju incydentu. Wg przeprowadzonej w 2002 r. przez Trend Micro, Inc. analizy [[6]](#footnote-7), koszty zatrzymania pracy stacji roboczej, jej skanowania i usuwania złośliwego lub niepożądanego oprogramowania oraz dokumentacja całego procesu zamykają się kwotą ponad 1.000 USD. Czy dzisiaj taki kosztorys pozostaje aktualny? Prawdopodobnie tak. Koszty własne IDC związane z diagnozowaniem problemów z systemem spowodowanych złośliwym lub niepożądanym oprogramowaniem, przygotowaniem kopii zapasowej dotychczasowych danych, ponownym formatowaniem twardego dysku oraz ponownym sporządzeniem obrazu systemu kształtują się podobnie. Trzeba zaznaczyć, że koszty te nie obejmują jeszcze wartości utraconych danych, straty na wydajności użytkownika końcowego ani ponoszonego przez organizację kosztu utraty zastrzeżonych informacji.

To prawda, że nie wszystkie próby pozyskania i użytkowania pirackiego lub fałszywego oprogramowania prowadzą do zagrożenia bezpieczeństwa, lecz nasza analiza wskazuje, że ryzyko jest naprawdę realne.

**PERSPEKTYWY NA PRZYSZŁOŚĆ I WAŻNE WSKAZÓWKI**

W Stanach Zjednoczonych wg danych Business Software Alliance ponad jeden na pięć pakietów oprogramowania dla komputerów PC jest pirackim lub fałszywym produktem, przy czym wskaźnik ten nieznacznie obniżył się w ciągu ostatniej dekady. Jednocześnie zagrożenia dla bezpieczeństwa
w drastycznym tempie rosną.

Nie tylko zwiększa się liczba i rodzaj ataków – od komputerowych wirusów i robaków do wirusów, robaków, koni trojańskich, ataków typu denial-of-service, programów typu spyware, oprogramowania typu adware, downloaderów, Phisherów, botów i rootkitów — lecz zmianie ulegają też przyczyny ataków. W zeszłym roku wg Trend Micro[[7]](#footnote-8) “zdecydowana większość zagrożeń wynikała z chęci uzyskania korzyści finansowych, nie zaś z pragnienia uzyskania rozgłosu lub złej sławy, wpływającego na złośliwe działania hackerów w poprzednich latach.”

Jako przykład charakteru działań podejmowanych w świecie “malware”, w lipcu 2006 r. w ramach Websense Security Labs wykryto fałszywą witrynę Mistrzostw Świata w piłce nożnej World Cup 2006 Soccer, która infekowała system odwiedzającego koniem trojańskim, pobierającym do komputera PC dalsze złośliwe oprogramowanie. Strona korzystała z toolkita, zwanego Web Attacker, sprzedawanego przez rosyjską witrynę WWW. Narzędzie to posiada graficzny interfejs użytkownika oraz możliwość zbierania danych statystycznych na temat infekcji.

Atakujący znajdują coraz nowsze sposoby kompresji plików, powiązywania wielu zestawów złośliwego kodu, na przykład poprzez wykorzystanie jednego konia trojańskiego do pobrania kolejnego.
Co więcej, coraz więcej złośliwych kodów usuwa konkurencyjne kody. Produkcja takiego oprogramowania staje się przemysłem.

Dowodzi to faktu, że ryzyko, na jakie narażeni są użytkownicy chcący korzystać z pirackiego oprogramowania, może tylko wzrastać.

Istnieją sposoby zapobiegania atakom takim jak te wykryte przez nas. Można instalować zapory firewall, korzystać z uaktualnianego oprogramowania do wykrywania złośliwych kodów oraz pobierania i instalowania na bieżąco poprawek i aktualizacji bezpieczeństwa dla systemu. Najlepszym środkiem zapobiegania zagrożeniom bezpieczeństwa wskutek pozyskiwania i eksploatacji pirackiego oprogramowania jest po prostu przejście na produkty oryginalne. W dłuższej perspektywie koszty mogą być niższe.

***N A M A R G I N E S I E* : CO Z FIZYCZNYM NOŚNIKIEM?**

IDC nie sprawdzała fizycznych nośników. Dokonaliśmy jednak przeglądu prac przeprowadzonych wcześniej w tym roku przez Microsoft w ramach analizy dysków uzyskanych przez pracowników Microsoft, którzy nabyli fałszywe oprogramowanie o średniej jakości rynkowej w różnych krajach świata.

Jak oceniono fizyczne nośniki?

Tutaj problemem nie było wbudowane złośliwe oprogramowanie, lecz słabości wynikające
z wprowadzenia dodatkowego oprogramowania oraz programów zmieniających charakter oryginalnych pakietów. Zagrożenia powstawały w następujący sposób:

 Niektóre pakiety oferowano z oprogramowaniem niestanowiącym części oryginalnego programu
z rodziny Microsoft Windows (“dodatkowe pliki binarne”).

Niektóre dodatkowe pliki binarne były generatorami kluczy lub kodami, które faktycznie zmieniały charakter oryginalnego programu.

Na część dodatkowych plików binarnych składało się oprogramowanie firm zewnętrznych znane
ze swej podatności na zagrożenia.

W niektórych przypadkach oprogramowanie nie mogło obejść mechanizmów aktywacji Microsoft.
(W zasadzie 34% fałszywych dysków nie umożliwiało nawet pełnej instalacji).
Podsumowanie wyników zawarto poniżej:

**Ryzyko związane z fałszywymi nośnikami (odsetek dysków umożliwiających instalację)**

niepowodzenie

Obejście aktywacji

Dodatkowe "pliki binarne"

228 umożliwiających instalację dysków z 17 krajów

Dyski CD z generatorem

 klucza/kodem ingerującym w

 integralność oprogramowania

Dyski CD z dodatkowymi

 plikami binarnymi o znanej

 podatności na zagrożenia

Źródło: Analiza własna Microsoft, 2006 r.; pozyskano 348 dysków, z czego 228 umożliwiających instalację, 17 krajów

***N A M A R G I N E S I E* : EBAY: ZBLIŻAJĄ SIĘ KŁOPOTY**

Szukasz okazji? Dlaczego nie kupić oprogramowania w serwie eBay? Dla wielu osób może to być legalny sposób tańszego pozyskania oryginalnego oprogramowania.

Jednak nie wszystkie programy sprzedawane w serwisie eBay są legalne. Microsoft i eBay interweniują w przypadku około 50.000 aukcji rocznie oprogramowania uznanego za naruszające prawa autorskie. Kto wie, jaka jest wielkość sprzedaży realizowanej w ten sposób w sieci?

Wiedzą ci, którzy decydują się na ryzyko, o którym tutaj mówimy. W ramach testowych zakupów ponad 115 egzemplarzy fizycznych nośników nabytych za pośrednictwem serwisu eBay w 2005 r. zespół prawny Microsoft ustalił, że 39% było fałszywe. Kolejne 12% oferowano wraz z dodatkowymi składnikami w postaci fałszywego oprogramowania lub oryginalnego oprogramowania noszącego znamiona ingerencji.

Wskazuje to, że prawdopodobieństwo nabycia oryginalnego, zgodnie z prawem licencjonowanego oprogramowania w serwisie eBay jest mniejsze niż ½ — co nie wygląda zbyt kolorowo w przypadku produktu wykorzystywanego do przechowywania i przetwarzania ważnych oraz danych osobowych
i informacji gospodarczych (często wysoce poufnych).

**Zakupy testowe w serwisie eBay**

Noszące znamiona ingerencji

8%

**Oryginalne**

**49%**

**115 próbek**

Fałszywe 39%

Z fałszywymi składnikami 4%

*Źródło: Zespół ds. prawa i przestrzegania przepisów Microsoft, 2006 r.; oprogramowanie “noszące znamiona ingerencji” obejmuje zarówno oryginalne oprogramowanie z fałszywymi składnikami, jak i oryginalne oprogramowanie noszące znamiona ingerencji*

Ile z tych dysków doprowadziłoby do zagrożeń dla bezpieczeństwa? Nasza analiza nie obejmowała sprawdzenia nabytych nośników, jednak pirackie lub fałszywe oprogramowanie może wymagać klucza produktu, generatora klucza lub narzędzia do łamania zabezpieczeń. W takiej sytuacji użytkownicy pragnący z nich skorzystać napotkaliby takie same zagrożenia dla bezpieczeństwa, jakie my napotkaliśmy podczas badania.

**PROTOKÓŁ Z TESTÓW**

***ANALIZA WITRYN SIECI WEB***

Analiza witryn sieci Web przez IDC została wykonana na wirtualnych maszynach VMware
(stacja robocza VMware wersja 5.5.1) uruchomionych na trzech standardowych laptopach IDC. Wirtualne maszyny pracowały na standardowym systemie Windows XP (SP2) IDC uzupełnionym
o wszelkie aktualizacje bezpieczeństwa Microsoft oraz przeglądarkę Microsoft Internet Explorer 6.02.

Protokół testów obejmował zastosowanie oprogramowania do wykrywania złośliwego kodu
(McAfee VirusScan Enterprise 8.0i i Computer Associates’ eTrust Antivirus r8 for Windows) w celu monitorowania ruchu z witryn sieci Web dla identyfikacji wszelkich prób instalacji złośliwego bądź potencjalnie niepożądanego oprogramowania. Definicje na potrzeby oprogramowania typu anti-malware uaktualniono w dniu przeprowadzania testów.

Celem było sprawdzenie witryn sieci Web oferujących pirackie lub fałszywe oprogramowanie, fałszywe klucze produktu, generatory kluczy lub narzędzia do łamania zabezpieczeń pod kątem możliwych
do wykrycia zagrożeń dla bezpieczeństwa.

Poniżej krok po kroku omówiono proces analizy witryn sieci Web:

1. Wyszukiwanie stron WWW oferujących dostęp do bezpłatnego oprogramowania Microsoft, kluczy produktów, generatorów kluczy oraz narzędzi do łamania zabezpieczeń produktów
z rodziny Windows XP lub Office. Skorzystano z wyszukiwarek takich jak MSN Search, Yahoo oraz Google. Wyszukiwane wyrażenia to “Windows XP,” “Office,” “keygens”, “cracks” itd.
2. Po znalezieniu witryny otwarcie jej przy użyciu przeglądarki Internet Explorer.
3. Przeglądanie witryny w poszukiwaniu fałszywych kluczy produktu, generatorów kluczy
i narzędzi do łamania zabezpieczeń. Jeżeli witryna wymagała samodzielnych czynności takich jak instalacja kontrolki ActiveX, działania takie były podejmowane tylko wówczas, gdy były bezwzględnie konieczne (np. w celu aktywnej nawigacji po witrynie).
4. Rejestracja wszelkich przypadków wykrycia złośliwego i potencjalnie niepożądanego kodu przez oprogramowanie typu anti-malware.
5. Korzystanie z wszelkich łączy na stronie wskazujących na dodatkowe źródła "bezpłatnego" oprogramowania, kluczy produktu, generatorów kluczy lub narzędzi do łamania zabezpieczeń.
6. Powtórzenie procesu dla wszystkich znalezionych witryn sieci Web.

***ANALIZA GENERATORÓW KLUCZY I NARZĘDZI DO ŁAMANIA ZABEZPIECZEŃ***

Po zakończeniu testów witryn sieci Web przez IDC, zespół ds. bezpieczeństwa Microsoft pobierał generatory kluczy i narzędzia do łamania zabezpieczeń ze wskazanych przez IDC stron WWW oraz
z sieci peer-to-peer. Celem było sprawdzenie, czy takie generatory kluczy oraz narzędzia do łamania zabezpieczeń zawierały jakiekolwiek złośliwe bądź potencjalnie niepożądane oprogramowanie.

Analiza pobranego oprogramowania została wykonana na maszynach z systemem Microsoft Windows XP Gold (bez pakietów serwerowych ani poprawek bezpieczeństwa) oraz przeglądarką Internet Explorer 6.0. Warto zauważyć, że zakres zainstalowanych w systemie operacyjnym poprawek nie jest istotny podczas korzystania z pobranego oprogramowania. Ponieważ oprogramowanie byłoby uruchamiane ręcznie przez użytkownika, oddziaływałoby w tym samym stopniu niezależnie od tego czy system operacyjny byłby aktualizowany w ogóle lub w całości przy zastosowaniu odpowiednich poprawek.

Do wykrywania złośliwego i potencjalnie niepożądanego oprogramowania użyto następujących programów typu anti-malware: McAfee VirusScan Enterprise 8.0i, Computer Associates’ eTrust Antivirus r8 for Windows oraz Symantec’s Norton AntiVirus 2006. Tutaj także definicje na potrzeby programów typu anti-malware zostały uaktualnione na dzień realizacji testów.

Analiza pobranego oprogramowania była podobna do tej przeprowadzonej w odniesieniu do witryn sieci Web z tym zastrzeżeniem, że je najpierw pobrano (z witryn sieci Web i sieci typu peer-to-peer),
a dopiero później sprawdzono przy użyciu programu do wykrywania złośliwego kodu.

**ZASTRZEŻENIE O PRAWACH AUTORSKICH**

Zewnętrzna publikacja danych i informacji IDC — Wykorzystywanie wszelkich informacji IDC
w reklamie, informacji prasowej lub materiałach promocyjnych wymaga uprzedniej pisemnej zgody właściwego Wiceprezesa lub Dyrektora Krajowego IDC. Do każdego wniosku w tym zakresie należy dołączyć projekt treści proponowanej publikacji. IDC zastrzega sobie prawo do odmowy z dowolnej przyczyny wydania zgody na zewnętrzne wykorzystanie jej danych.

Copyright 2006 IDC. Powielanie bez pisemnej zgody bezwzględnie zabronione.

1. Jaka jest różnica między oprogramowaniem pirackim a fałszywym? Wg większości definicji “pirackie oprogramowanie”
to oprogramowanie w sposób nienależyty licencjonowane lub nielicencjonowane w ogóle, zaś “fałszywe oprogramowanie”
to oprogramowanie celowo prezentowane jako oryginalne, choć oryginalne nie jest. W niniejszej Białej Księdze możemy stosować oba terminy zamiennie z uwagi na wspólną dla obu metod potrzebę znalezienia oprogramowania w Internecie
i obejścia mechanizmów licencjonowania i aktywacji poprzez wykorzystanie fałszywych kluczy, kluczy stworzonych przez generatory kluczy bądź narzędzi do łamania zabezpieczeń. Bez względu na źródło samych programów starania zmierzające
do ich znalezienia i eksploatacji pociągają za sobą takie same ryzyko. [↑](#footnote-ref-2)
2. Należy zauważyć, że nazwy oraz klasyfikacje złośliwego i niepożądanego oprogramowania, przedstawione w niniejszej sekcji odpowiadają nazewnictwu stosowanemu w programach McAfee VirusScan Enterprise 8.0i, Symantec’s Norton AntiVirus 2006
i Computer Associates’ eTrust Antivirus r8 for Windows. [↑](#footnote-ref-3)
3. http://www.websense.com/securitylabs/alerts/alert.php?AlertID=395 [↑](#footnote-ref-4)
4. Trzeźwe spojrzenie na trendy w sferze zagrożeń bezpieczeństwa, z których część omówiono w niniejszej analizie, znajduje się w pozycji "Trendy w sferze zagrożeń w dzisiejszym świecie, coroczne podsumowanie za 2005 r. i prognoza na 2006 r."
(The Trend of Threats Today, 2005 Annual Roundup and 2006 Forecast); autorzy Jaime Lyndon, A. Yaneza i David Sancho, Trend Micro, publikacja dostępna pod adresem http://www.trendmicro.com/en/security/white-papers/overview.htm#annual-roundup. [↑](#footnote-ref-5)
5. "Jedenasta coroczna ankieta dotycząca przestępczości komputerowej i bezpieczeństwa" (Eleventh Annual CSI/FBI Computer Crime and Security Survey), 2006 r., Computer Security Institute, http://www.gocsi.com/; opublikowano za zgodą posiadacza stosownych praw. [↑](#footnote-ref-6)
6. "Rzeczywisty koszt epidemii wirusa" (The Real Cost of a Virus Outbreak), 1 marca 2002 r. http://www.trendmicro.com/ [↑](#footnote-ref-7)
7. Patrz http://www.trendmicro.com/en/security/white-papers/overview.htm#annual-roundup. [↑](#footnote-ref-8)