Obrona

Skuteczna obrona przed rootkitami

Grzegorz Błoński

stopień trudności

Głośno o rootkitach zaczęło się mówić od czasu skandalu w roku 2005. Ujawniono wtedy, że firma Sony BMG Music Entertaiment do ochrony praw własności wykorzystała rootkita (aries.sys) umieszczonego w oprogramowaniu XCP Content Protection DRM. Tak naprawdę rootkity zaczęły się pojawiać w systemach komputerowych w połowie lat 90-tych XX wieku.

Rootkit jest narzędziem pomocnym hakerom we włamaniach do systemów informatycznych, potrafi ukryć pliki oraz procesy, które osoba przygotowująca atak chce uczynić niewidocznymi dla użytkownika. Rootkity infekują jądro systemu – ukrywają siebie oraz inny złośliwy program (na przykład trojana), za pomocą którego atakujący może uzyskać dostęp do zainfekowanej maszyny. Wykrycie rootkita w systemie, czy to Windows czy Unix/Linux, nie należy do zadań łatwych, lecz jeszcze trudniejsze jest skuteczne pozbycie się nieproszonego gościa. Rootkity nie potrafią same się replikować. W związku z tym, aby z nich korzystać, hakerzy *doklejają* ich kod do wszelkiego rodzaju trojanów, backdoorów i innego rodzaju robaków, które świetnie potrafią się mnożyć. Dzięki temu napastnicy są w stanie doprowadzić do masowego rozprzestrzenienia się rootkita.

W miesiącu sierpniu tego roku ukazały się informacje publikowane przez różne strony internetowe na temat nowego *rootkitopodobnego* oprogramowania w kolejnym produkcie Sony – napędzie USB typu *pendrive* wyposażonym w czytnik linii papilarnych. Źródłem informacji jest fiński producent oprogramowania antywirusowego F-Secure, którego pracownicy wykryli, iż oprogramowanie produktu Sony MicroVault USM-F tworzy ukryty katalog na dysku. Nie ma do niego dostępu z Windows API i nie widzą go także niektóre programy antywirusowe. Sony utrzymuje, że katalog jest tworzony w celu ukrycia *odcisków* użytkownika przed dostępem osób niepowołanych, jednak według F-Secure możliwe jest jego wykorzystanie do innych celów i to już budzi obawy zarówno użytkowników, jak i specjalistów zajmujących się tego typu zagrożeniami. Warto zadać sobie pytanie, dlaczego duże koncerny

Z artykułu dowiesz się

- co to jest rootkit,
- jakie są rodzaje rootkitów,
- jak się bronić przed rootkitami.

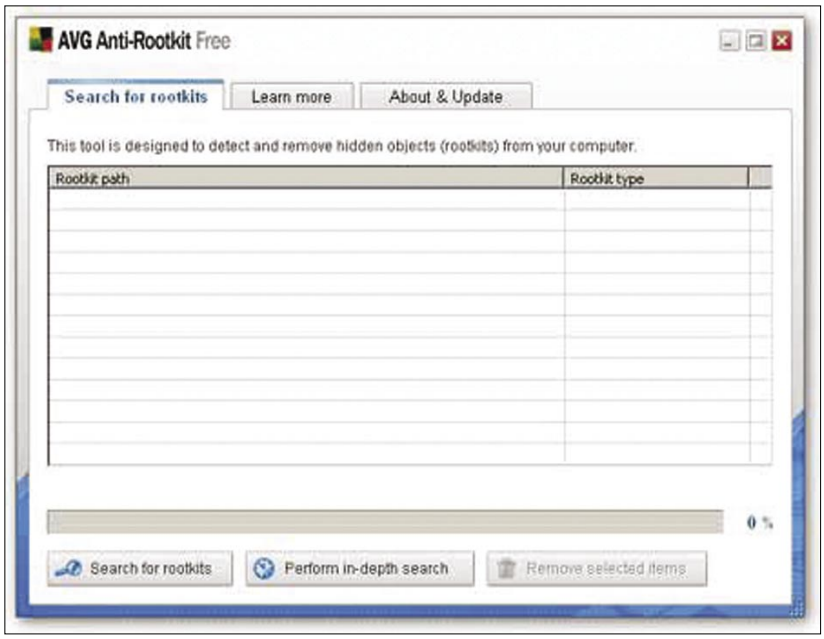
Co powinieneś wiedzieć

- znać obsługę linii poleceń w systemach Windows i Unix/Linux,
- umieć korzystać z edytora rejestru *regedit.exe*.

próbują stosować takie rozwiązania w swoich produktach, czym narażają ich użytkowników na niepotrzebne ryzyko.

Rodzaje rootkitów

- *Kernel-mode rootkit* – działający w jądrze systemu program, który potrafi ukryć swoją obecność poprzez podmianę fragmentu kodu jądra. Najczęściej można zainfekować się takim rodzajem rootkita poprzez instalację sterowników z nieznanego miejsca w sieci (dotyczy to w szczególności systemów Windows). W przypadku Linuksa sytuacja jest podobna, ponieważ tego typu rootkity infekują jądro poprzez mechanizm LKM (Loadable Kernel Modules), ładowalnych modułów.
- *Application rootkit* – podmieniający pliki binarne aplikacji rootkit, niemający dostępu do jądra systemu.
- *Memory-based rootkit* – rezydujący w pamięci operacyjnej komputera, groźniejszy dla serwerów, ponieważ te są dużo rzadziej restartowane niż komputery. Trudny do wykrycia, ponieważ większość programów zwalczających rootkity przeszukuje raczej zasoby dyskowe, a nie pamięć RAM.
- *Persistent rootkit* – łatwy do wykrycia, ponieważ nie ukrywa się. Zmieniając wpisy w rejestrze systemu zakłóca pracę plików systemowych, a przez to powoduje niestabilną pracę systemu.
- *User-mode rootkit* – jego działalność ograniczona jest prawami użytkownika, na których niekiedy łatwo jest mu się zainstalować w systemie.



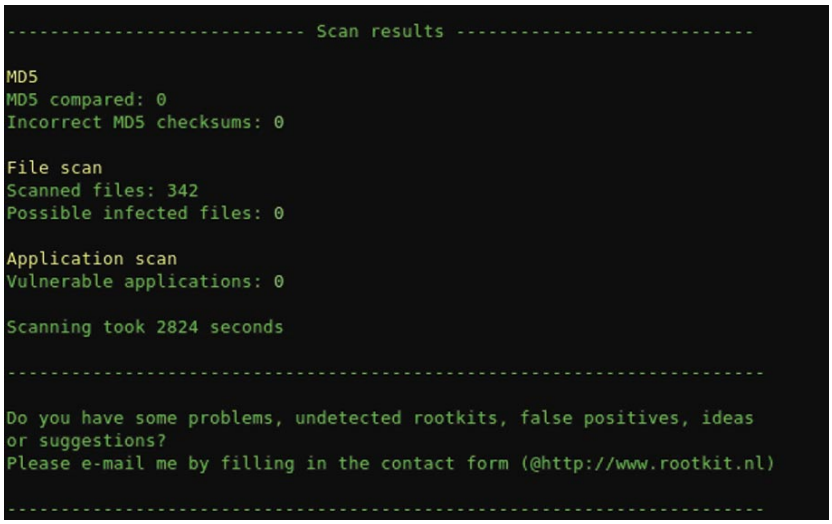
Rysunek 1. *Interfejs użytkownika programu AVG Anti-Rootkit.*

```
Rootkit Hunter 1.2.8 is running

Determining OS... Unknown
Warning: This operating system is not fully supported!
Warning: Cannot find md5_not_known
All MD5 checks will be skipped!


Checking binaries
* Selftests
     Strings (command)                                    [ OK ]


* System tools
     Skipped!


Check rootkits
* Default files and directories
   Rootkit '55808 Trojan - Variant A'...                  [ OK ]
   ADM Worm...                                            [ OK ]
   Rootkit 'AjaKit'...                                    [ OK ]
   Rootkit 'aPa Kit'...                                   [ OK ]
   Rootkit 'Apache Worm'...                               [ OK ]
```

Rysunek 2. *Rkhunter uruchomiony na nierozpoznanym systemie*

- *Root-mode rootkit* – rootkit, który korzysta z praw administratora/roota (w zależności od systemu, w jakim się znajdzie).

Poza powyższym podziałem związanym z trybem *pracy*, spotyka się inne rodzaje tych złośliwych programów. Istnieją zagrożenia związane z rootkitami, które mogą się zaszyć w pamięci podzespołów komputera. John Heasman z Next Generation Security Software w swoich publikacjach opisuje możliwość umieszczenia kodu rootkita w pamięci BIOS płyty głównej oraz karty graficznej. Z jego artykułów wnioskować można, iż praktycznie każdy podzespół komputera wyposażony nawet w niewielką ilość pamięci, którą można zapisać, może zostać wykorzystany jako nośnik – a zarazem kryjówka – dla rootkita. Heasman proponuje jako zabezpieczenie przed rootkitami stosowanie w komputerach układów TPM (*Trusted Platform Module*), które są dziełem Trusted Computer Group. Układy TPM umożliwiają między innymi szyfrowanie haseł dostępu. Poza tym podczas uruchamiania komputera układ TPM sprawdza zawartość BIOSu, którą porównuje z tym, co ma zapisane w rejestrach PCR (*Platform Configuration Registers*). Większość układów TPM produkowanych jest w firmach Infineon, National Semiconductor oraz Broadcom. W układy te wyposaża swoje produkty między innymi IBM, ale także Dell, HP i Toshiba.



Rysunek 3. *Rezultat pracy Rkhuntera.*

Pe386 na widelcu

Niektóre rootkity (na przykład *Pe-386*, znany też jako *Rustock.B vel lzx32 vel msguard*) działające w trybie kernel-mode wykorzystują do ukrywania funkcję ADS (*Alternate Data Streams*), która jest dostępna w systemie plików NTFS. ADS to dodatkowe strumienie danych, które można zapisywać – jako niewidoczne – pod innym plikiem na dysku. Dane w strumieniu są niewidoczne dla użytkownika, nie zmienia się nawet raportowany przez system operacyjny rozmiar pliku, pod którym jest zapisany strumień. Pliki w strumieniu zapisywane są po dwukropku, czyli na przykład plik o nazwie *xyz.sys* może zostać powiększony o strumień z plikiem *zzz.qqq*, którego nazwa będzie mieć postać *xyz.sys:zzz.qqq*. Podstawowy plik *xyz.sys* jest widoczny z poziomu Eksplorera Windows czy linii komend, lecz strumienie ADS i zapisane w nich pliki nie mogą być bezpośrednio zaobserwowane.

Rustock.B jest rodzajem konia trojańskiego, który został wyposażony w mechanizmy rootkita w celu ukrycia swej obecności w systemie. Nie można się nim zarazić bezwiednie. To użytkownik, pobierając pliki w sieciach *peer-to-peer*, ze stron z warezami, czy otwierając podejrzany załącznik w e-mailu uruchamia tego konia trojańskiego. Jeśli nie zostanie on natychmiast wykryty przez potrafiący go rozpoznać program antywirusowy, uruchamia rootkita, który zaszywa się w systemie. Złośliwy kod tworzy strumień danych ukrytych na ścieżce: *%windir %\System32:lzx32.sys* po czym dodaje ukrytą usługę o nazwie *pe386* oraz ścieżce do pliku jak powyżej. Kolejnym krokiem jest dodanie wpisów w rejestrze (Ramka Dodanie wpisów w rejestrze).

Ostatni wpis zawiera ciąg *Win23 lzx files loader* i tu nie ma błędu, to jest w istocie 23.

Następnie rootkit modyfikuje wybrane obszary jądra systemu, żeby zmienić funkcjonowanie poniższych funkcji API:

- `ZwOpenKey`
- `ZwEnumatereKey`
- `ZwQueryKey`
- `ZwCreateKey`

Rysunek 4. *Okno programu sigverif.exe*

- `ZwSaveKey`
- `ZwDeviceIoControlFile`
- `ZwQuerySystemInformation`
- `ZwInitializeRegistry`

Rootkit wyszukuje w obrazie jądra systemu ciągu *FATAL_UNHANDLED_HARD_ERROR* i nadpisuje go swoim kodem. Zmienia funkcjonowanie modułów systemowych (*ndis.sys, wanarp.sys, tcpip.sys)* odpowiedzialnych za komunikację sieciową – tak, by móc omijać firewalle i dokonywać ewentualnych zmian zawartości wysyłanych pakietów TCP/IP. Jego obecność w systemie może być rozpoznana po wzmożonym ruchu na interfejsach sieciowych, ponieważ jednym z jego zadań jest praca jako ukryty serwer proxy. Często też wykorzystywany jest do wysyłania spamu, zatem dodatkowo naraża komputer-ofiarę na jego otrzymywanie. Nierzadko zdarza się, że zainfekowany system daje nam sygnały, iż dzieje się w nim coś niedobrego – ciągłymi BSODami, które naprawdę potrafią uprzykrzyć życie. Wiele osób używa komputera nie podejrzewając, że spowolnione działanie systemu to właśnie taki *nieproszony* gość.

Aby pozbyć się Rustocka.B z komputera, należy wykonać kilka czynności zależnych od systemu operacyjnego. Jeśli nasz system to Windows NT/2K/XP/2K3, to w pierwszej kolejności musimy wyłączyć funkcję *Przywracanie Systemu*. W przypadku systemów Windows 9x pomijamy ten krok. Następnie należy uruchomić komputer za pomocą płyty instalacyjnej i po ukazaniu się okna dialogowego z wyborem operacji wcisnąć *R*, aby przełączyć się do konsoli odzyskiwania. W kolejnym oknie należy wybrać zainstalowany system, do którego chcemy się zalogować i podać hasło administratora zatwierdzając je klawiszem `Enter`. W linii poleceń należy wpisać polecenie `DISABLE pe386` i zatwierdzić klawiszem `Enter`, co spowoduje zatrzymanie usługi, którą wcześniej uruchomił rootkit. Teraz wystarczy w trybie awaryjnym przeskanować system przy pomocy programu antywirusowego z najnowszymi bazami wirusów w celu odnalezienia tego, co zostało na dysku po działalności rootikta.

Na koniec warto przy użyciu edytora rejestru pozbyć się wpisów, których dokonał rootkit podczas zarażania systemu. W sieci można znaleźć program o nazwie *Rustbfix.exe,* który potrafi wykryć oraz usunąć tego rootkita. Niestety w przypadku mojego systemu aplikacja ta zawiodła. Dopiero po wykonaniu wcześniej opisanych kroków udało mi się usunąć zagrożenie całkowicie.

Frank Boldewin na swojej stronie *www.reconstructer.org* opublikował obszerną analizę Rustocka.B, łącznie z jego kodem źródłowym. Artykuł ten nosi tytuł *A Journey to the Center of Rustock.B Rootkit*. Polecam go wszystkim czytelnikom pragnącym dowiedzieć się jeszcze więcej na temat tego rootkita.

Narzędzia

Ze względu na zagrożenia, jakie niesie za sobą możliwość zainfekowania rootkitami, każdy administrator pragnie zadbać o bezpieczeństwo systemów, którymi administruje. Metody obrony przed rootkitami możemy podzielić na trzy grupy:

- zapobieganie,
- wykrywanie,
- usuwanie.

Zapobieganie – jakkolwiek możliwe – jest bardzo trudne do zrealizowania, ponieważ kod rootkitów jest, jak wiadomo, wciąż udoskonalany i rozwijany. Wykrywanie jest realizowane za pomocą odpowiednich programów lub też przy użyciu specjalizowanych urządzeń przeznaczonych do tego celu.

W systemach operacyjnych Windows w celu zapobiegania infekcjom rootkitów mamy możliwość między innymi zastosowania programów różnych producentów, które w większości przypadków są darmowe, a ich nazwa zawiera słowa *Anti-Rootkit*. Przykładem niech będzie aplikacja AVG Anti-Rootkit.

Praktycznie każdy producent oprogramowania antywirusowego dla systemów Windows – czy to darmowego, czy też komercyjnego – ma w swojej ofercie również programy tego typu. Także Uniksy i Linuksy nie są pozbawione podobnych narzędzi, najbardziej znanymi i najczęściej używanymi są *chkrootkit* oraz *rkhunter.*

```
Microsoft(R) Windows XP - Kontroler plików systemu Windows Wersja 5.1
(C) 1999-2000 Microsoft Corp. Wszelkie prawa zastrzeżone

Skanuje chronione pliki systemowe i zastępuje niepoprawne wersje plików
poprawnymi wersjami firmy Microsoft.

SFC [/SCANNOW] [/SCANONCE] [/SCANBOOT] [/REVERT] [/PURGECACHE] [/CACHESIZE=x]


/SCANNOW        Natychmiast skanuje wszystkie chronione pliki systemowe.
/SCANONCE       Skanuje wszystkie chronione pliki systemowe przy następnym
                rozruchu.
/SCANBOOT       Skanuje wszystkie chronione pliki systemowe przy każdym
                rozruchu.
/REVERT         Przywraca ustawienie domyślne skanowania.
/PURGECACHE     Przeczyszcza bufor plików.
/CACHESIZE=x    Ustawia rozmiar buforu plików.
```

Rysunek 5. *Pomoc programu sfc.exe w konsoli.*

Na Zdjęciu 2 widać, że program nie rozpoznał systemu operacyjnego skanowanego komputera. Nie przeszkadza mu to jednak w pracy – nawet w przypadku nieodnalezienia kluczy MD5.

Na kolejnym Zdjęciu 3 można zobaczyć, że Rkhunter po zakończonym skanowaniu wyświetla informacje o ilości przeskanowanych plików, ilości podejrzanych plików i aplikacji (w przypadku, gdy je wykryje) oraz o czasie skanowania.

Opisane powyżej aplikacje dla Windows oraz Unix/Linux podczas skanowania systemu korzystają z techniki zwanej *cross-check*, która polega na porównywaniu listy plików zwracanej przez system operacyjny z tym, co na naszym dysku faktycznie się znajduje. W przypadku, gdy rootkit zainfekuje system, potrafi się on skutecznie maskować i niestety nie zawsze metoda ta pozwala na jego wykrycie.

W ramach projektu *Strider* autorstwa Microsoftu powstała aplikacja Ghostbuster, która podchodzi do tematu wykrywania rootkitów nieco inaczej. Program (niestety, na razie nie upubliczniony) porównuje listę plików w zainfekowanym systemie z listą plików ze zdrowego systemu. Porównanie takie pozwala na wykrycie plików (oraz uruchamianych przez nie procesów), których w systemie nie powinno być. Wymogiem wykorzystania tej aplikacji jest jej uruchomienie w niezainfekowanym systemie (aby mieć możliwość wiarygodnego porównania). Aby tego dokonać, możemy skorzystać z programu BartPE i z jego pomocą zbudować bootowalnego CD z systemem Windows oraz programami do wykrywania rootkitów. Strider Ghostbuster jest jeszcze niedostępny, ale program Rootkit Revealer firmy Sysinternals wykorzystuje bardzo podobne mechanizmy, można więc skorzystać właśnie z niego.

W sieci dostępna jest cała gama przeróżnych programów pozwalających na znalezienie, zidentyfikowanie i często usunięcie rootkita – jak chociażby RootKit Unhooker, Sophos Antirootkit, UnHackMe, RootKit Hook Analyzer, IceSword, Helios, DarkSpy, F-Secure BlackLight czy polskie Gmer oraz System Virginity Verifier (ten ostatni autorstwa Joanny Rutkowskiej).

Użytkownicy systemów uniksowych także mają możliwość uruchomienia aplikacji chkrootkit czy rkhunter z bootowalnej płyty CD.

W sieci można znaleźć także co najmniej kilka bootowalnych dystrybucji Linuksa zawierających programy chkrootkit oraz rkhunter. Jedną z nich jest InSeRT (*Inside Security Rescue Toolkit*), którą można pobrać ze strony *http://www.inside-security.de*. Kolejna dystrybucja to GRML (*http://grml.org*), bazująca na Knoppiksie i wyposażona w blisko 2500 pakietów, wśród których znajduje się między innymi chkrootkit.

Sprzęt widmo

Do wykrycia rootkita w systemie można również użyć specjalnie zaprojektowanego sprzętu. Niestety, z racji braku możliwości zakupu i praktycznego wykorzystania tego typu urządzeń ograniczę się do ich ogólnego opisu. Urządzenie o nazwie Tribble powstało na potrzeby prowadzenia śledztwa w przypadkach cyfrowych przestępstw. W jego projektowaniu brali udział Joe Grand z Grand Idea Studio oraz Brian Carrier z Digital-Evidence. Zbudowano je na bazie procesora Intel IQ80303 wyposażonego między innymi w mostek *PCI-to-PCI*, pozwalający na transfer danych z prędkościami do 528MB/s. Instaluje się je w serwerze lub komputerze, na którym istnieje podejrzenie ataku, w celu zapisania zawartości pamięci RAM do późniejszej analizy. Karta PCI zainstalowana w systemie po uruchomieniu procedury zapisu pamięci dokonuje zrzutu zawartości pamięci RAM oraz rejestrów CPU. Zapisaną zawartość pamięci można więc analizować pod kątem przeróżnych kryteriów, między innymi przeprowadzając testy na obecność rootkitów.

Kolejne urządzenie o podobnych możliwościach to RAM Capture Tool, wyprodukowany przez BBN Technologies Inc. Na temat tego urządzenia można powiedzieć tyle, że pracuje również na szynie PCI, lecz szczegółowe informacje na jego temat nie są ogólnie dostępne.

Działania prewencyjne

Działalność rootkitów w systemie jest przez nie same maskowana

Dodanie wpisów w rejestrze

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\pe386
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\pe386\Security
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\pe386\Imagepath="\??\%windir%\System32:lzx32.sys"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\pe386\Start="1"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\pe386\Group="Base"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\pe386\Extparam=""
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\pe386\Security\Security="(binary registry data)"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\pe386\Errorcontrol="0"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\pe386\Type="1"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\pe386\Displayname="Win23 lzx files loader"

po zainstalowaniu się. Chcąc zadbać o sprawność systemu, możemy posłużyć się narzędziem o nazwie Tripwire w celu wykrycia prób modyfikacji plików systemowych. Jest to aplikacja z rodzaju IDS, która pozwala na wykrycie działalności intruza w systemie poprzez kontrolę integralności plików systemowych. Sprawdza ona, czy pliki nie zostały zmodyfikowane, podmienione na inne – często właśnie zainfekowane – wersje, czy też usunięte.

Tripwire tworzy bazę danych zawierającą informacje na temat atrybutów plików i katalogów (łącznie z ich sygnaturami MD5), którą można zapisać na jakimś nośniku w celu późniejszego odczytu dla dokonania porównania.

Dla zapewnienia maksymalnego stopnia pewności wyników porównywania, Tripwire należy zainstalować w systemie jak najszybciej – najlepiej zaraz po zainstalowaniu systemu operacyjnego. Dla systemów Unix/Linux aplikacja jest darmowa, niestety dla systemów Windows dostępna jest tylko wersja komercyjna.

W celu sprawdzenia, czy nasz system nie został zainfekowany rootkitem, możemy się posłużyć także innymi narzędziami. Zainfekowany system, w którym działa już rootkit, jest przez niego modyfikowany w taki sposób by programy antywirusowe czy antyrootkitowe nie wykryły go. Z pomocą przyjść mogą narzędzia wbudowane w system. W przypadku Windows warto tu wymienić dwa z nich.

Windows Signature Verification (*sigverif.exe)* to program, który dba o kompletność i integralność systemu. Pozwala na przywracanie usuniętych przez użytkowników plików, kontrolę spójności całości systemu, sprawdza, czy pliki wykonywalne **.exe*, **.dll* oraz sterowniki posiadają podpis cyfrowy, a także weryfikuje podpisy/sygnatury pliku z posiadanymi bazami danych.

W przypadku wykrycia zmian w podpisanym pliku lub pojawienia się pliku, który nie jest rozpoznawany (w naszym przypadku będzie to pojawienie się pliku rootkita w systemie), wyświetlana jest informacja.

System File Checker (*sfc.exe*) to aplikacja działająca w linii poleceń. Służy do kontroli chronionych plików systemowych. W przypadku wykrycia zmienionego pliku *System File Checker* pyta, czy ma przywrócić oryginalną wersję pliku z płyty instalacyjnej.

Uruchomienie programu z parametrem */scanboot* spowoduje sprawdzanie wszystkich chronionych plików systemowych przy każdym rozruchu. (Uwaga! Może to spowodować znaczne wydłużenie czasu rozruchu systemu.) Jest to zawsze jakaś forma ochrony i weryfikacji tego, czy w systemie pojawiły się zmiany mogące być efektem działania rootkita bądź innego złośliwego programu.

W celu obrony przed atakami hakerów powstały programy określane mianem HIPS (*Host Intrusion Prevention System*). Ponieważ z założenia spełniają one rolę systemu zapobiegania atakom, częściowo pomagają chronić system także przed rootkitami. Przykładami takich narzędzi dla systemów Windows są *ProcessGuard i AntiHook*. Obie aplikacje pozwalają zablokować możliwość uruchamiania nowych programów, zabezpieczają pamięć RAM, blokują możliwość instalacji niechcianych programów, kontrolują uruchamiane aplikacje.

Wprawdzie nie można takim programom ufać całkowicie, jednak spełniają one swoje zadania i pozwalają czuć się odrobinę pewniej. Dla Linuksa istnieje aplikacja o podobnym działaniu, nazywająca się LIDS (*Linux Intrusion Detection System*). Program ten jest rozszerzeniem dla jądra Linuksa, implementującym wiele narzędzi, których normalnie nie znajdziemy w jądrze. Obsługuje między innymi mechanizm obowiązkowej kontroli dostępu *(Mandatory Access Control* – MAC), zawiera detektor skanowania portów, zapewnia ochronę plików oraz procesów.

Podsumowanie

W dzisiejszych czasach komputery są stałym składnikiem naszego świata – czy to prywatnego, czy zawodowego. Ich obecność widać w każdym domu, instytucji, firmie – po prostu wszędzie. Wszystko to powoduje, że ryzyko zainfekowania komputera złośliwym kodem znacznie wzrosło w stosunku do lat ubiegłych.

Ilość wirusów oraz innego rodzaju malware, między innymi rootkitów, urosła do takiego stopnia, że niełatwo się przed nimi bronić. Powstają coraz to nowe aplikacje do ich wykrywania i dezaktywowania, jednak autorzy kodu rootkitów także udoskonalają swoje *dzieła*, więc walka nieustannie trwa.

Jak na razie nie zanotowano żadnej wielkiej epidemii rootkitów, lecz czy można być pewnym, że takowa nie wystąpi? Wiele wskazuje na to, że sytuacja nie będzie się wyraźnie poprawiać. Możemy mieć tylko nadzieję, że powstaną systemy operacyjne odporne na tego typu zagrożenia lub programy odpowiednio zabezpieczające obecne systemy. Odpowiedź na tytułowe pytanie, czy można się skutecznie bronić przed rootkitami, jest bardzo trudna i tak naprawdę robiąc to, co opisałem w tym artykule możemy tylko zminimalizować prawdopodobieństwo dostania się do naszego komputera nieproszonego, utrudniającego nam życie gościa. ●

O autorze

Grzegorz Błoński z wykształcenia jest informatykiem, certyfikowanym specjalistą IBM. Pracuje w dużej firmie o zasięgu światowym. Zajmuje się administracją i bezpieczeństwem sieciowym.Należy do międzynarodowych organizacji ISOC oraz ISACA zajmujących się szeroko pojętym bezpieczeństwem IT.
Kontakt z autorem: *mancymonek@wp.pl*