Ukryte zagrożenie: alternatywne strumienie danych

bezpieczeństwa, administratorzy często nie doceniają długości, jakie przeszliby wyrafinowani hakerzy, by ukryć swoje ślady. Proste pomyłki i odskocznia od scenariusza, wyrafinowany haker z bardziej skoncentrowanymi celami patrzy na naruszenie systemu perymetru jako szansę na dalszy postęp w sieci lub ustanowienie nowej anonimowej bazy, z której można zaatakować inne cele.

Aby osiągnąć to zadanie, zaawansowany haker potrzebuje czasu i zasobów, aby zainstalować tak zwany zestaw rootów lub narzędzia hakerskie, za pomocą których może wykonywać kolejne ataki. W ten sposób pojawia się potrzeba ukrycia narzędzi jego handlu i uniemożliwienie administratorowi systemów wykrywania różnych aplikacji hakerskich, które może wykonywać w naruszonym systemie.

Popularną metodą stosowaną w systemach Windows jest użycie alternatywnych strumieni danych (ADS). Stosunkowo mało znaną funkcją kompatybilności z NTFS, ADS jest możliwość przenoszenia danych plików do istniejących plików bez wpływu na ich funkcjonalność, rozmiar lub wyświetlanie tradycyjnym narzędziom przeglądania plików, takim jak dir lub Windows Explorer. Znalezione we wszystkich wersjach systemu plików NTFS, ADS, tam, gdzie pierwotnie stworzono, aby umożliwić kompatybilność z hierarchicznym systemem plików systemu Macintosh, HFS; gdzie informacja o pliku jest czasami dzielona na osobne zasoby. Alternatywne strumienie danych mogą być używane zgodnie z prawem przez różne programy, w tym natywny system operacyjny Windows do przechowywania informacji o plikach, takich jak atrybuty i tymczasowe przechowywanie.

Co zaskakujące, alternatywne strumienie danych są niezwykle łatwe do wykonania i wymagają niewielkiej lub żadnej umiejętności ze strony hakera. Typowe polecenia DOS, takie jak "type", służą do tworzenia ADS. Polecenia te są używane w połączeniu z przekierowaniem [>] i dwukropkiem [:] do rozwidlenia jednego pliku do drugiego.

Na przykład: polecenie

 "Wpisz c: \ anyfile.exe> ​​c: \ winnt \ system32 \ calc.exe: anyfile.exe"

rozwiąże standardowy program Windows Kalkulator z ADS "anyfile.exe."

Alarmujące pliki z reklamami są prawie niemożliwe do wykrycia przy użyciu rodzimych technik przeglądania plików, takich jak wiersz poleceń lub Eksplorator Windows. W naszym przykładzie rozmiar pliku calc.exe będzie wyświetlany jako oryginalny rozmiar 90k niezależnie od rozmiaru pliku ADF anyfile.exe. Jedynym wskazaniem, że plik został zmieniony, jest znacznik czasu modyfikacji, który może być względnie niewinny.

Po wstrzyknięciu ADS można wykonać za pomocą tradycyjnych poleceń, takich jak typ, lub rozpocząć lub pisać w typowych językach skryptowych, takich jak VB lub Perl. Po uruchomieniu plik wykonywalny ADS wydaje się działać jako oryginalny plik - wygląda niewykrywalny, aby przetwarzać przeglądarki, takie jak Menedżer zadań Windows. Dzięki tej metodzie nie tylko można ukryć plik, ale także ukryć wykonanie nielegalnego procesu.

Niestety, jest praktycznie niemożliwe, aby natywnie chronić system przed ukrytymi plikami ADS, jeśli używasz systemu plików NTFS. Używanie alternatywnych strumieni danych nie jest funkcją, którą można wyłączyć i obecnie nie ma możliwości ograniczenia tej możliwości do plików, do których użytkownik ma już dostęp. Darmowe programy takie jak lads.exe autorstwa Franka Heyne'a (www.heysoft.de) i criticalADS by CrucialSecurity mogą być używane do ręcznego audytu twoich plików pod kątem obecności alternatywnych strumieni danych. Alternatywnie akcja przeniesienia pliku do innego systemu plików, który nie obsługuje reklam ADS, automatycznie niszczy wszelkie alternatywne strumienie danych.

Ostatecznie tylko aplikacja kontrolująca pliki stron trzecich może skutecznie utrzymać integralność partycji NTFS przed nieautoryzowanymi alternatywnymi strumieniami danych. Niedawno nazwane jako "Intrusion Prevention Systems" lub "Intrusion Detection Systems", aplikacje bezpieczeństwa, takie jak eTrust Access Control firmy Computer Associates, od lat są używane w wysokiej jakości sieciach rządowych do sprawdzania integralności plików używanych w najbezpieczniejszych środowiska. Oprócz podwyższonego poziomu kontroli i kontroli dostępu, te aplikacje zwykle tworzą bazę danych MD5 z sumami kontrolnymi plików, które służą do sprawdzania wiarygodności pliku. Techniki wtrysku plików, takie jak Alternatywne strumienie danych, uruchamiają akcję, dzięki której plik jest uznawany za niezaufany, a zatem uniemożliwiony lub jeszcze lepszy, uniemożliwiając jego zmianę w pierwszej kolejności.

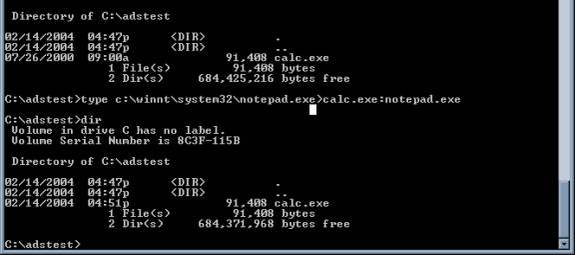
Inną dobrą aplikacją do integrowania plików jest Tripwire for Servers firmy Tripwire Inc. Tripwire od początku lat dziewięćdziesiątych koncentruje się na zarządzaniu integralnością plików i wykonuje olbrzymią pracę polegającą na zapewnieniu rygorystycznych zabezpieczeń przed nieautoryzowanymi zmianami plików.

Przykład ADS

Aby w pełni zrozumieć konsekwencje alternatywnych strumieni danych, poniżej opisano tworzenie i wykonywanie ADS przy użyciu standardowych programów Windows 2000 na partycji NTFS 5.0.

Rysunek 1 pokazuje plik wykonywalny standardowego kalkulatora programów Windows, calc.exe, o oryginalnym rozmiarze 90 KB i datowniku datowanym na 7/26/2000.



  
Rysunek 2

Następnie dodajemy alternatywny strumień danych do programu calc.exe z innym standardowym programem Windows, notepad.exe, jak pokazano na rysunku 2.

**Rysunek 3 pokazuje, że podczas gdy notepad.exe ma rozmiar 50 KB, rozmiar pliku calc.exe nie zmienił się z pierwotnego 90 KB. Widzimy jednak, że zmieniony został datownik daty modyfikacji.**