PORADNIKI

Alternatywne Strumienie Danych w NTFS

Co to jest NTFS?

Jest to skrót od *New Technology File System*

Co to jest Alternatywny Strumień Danych (ADS) ?

W NTFS, plik składa się z różnych strumieni danych. Jedne strumień przechowuje informacje bezpieczeństwa (prawa dostępu i inne takie rzeczy), inny przetrzymuje "dane rzeczywiste" jakich oczekujesz w pliku. Może być inny strumień z łaczem informacyjnym zamiast strumienia danych rzeczywistych, jesli plik w rzeczywistości jest linkiem.I mogą być alternatywne strumienie danych, przechowujące dane w ten sam sposób do standardowe strumienie danych

Co jest nie tak z alternatywnymi strumieniami danych?

Powiem tak: Nic, one działają jak oczekujemy i tak jak są udokumentowane (Microsoft udokumentował tą cechę). Ale jest cośzłego: Są one całkowicie ukryte. Możesz mieć plik z 1 bajtem w oficjalnym głónym strumieniu danych i setki MB w jednym lub wielu alternatywnych strumieni danych. To co pokazują polecenie dir, menadżer plików czy Explorer to rozmiar tego pliku. 1 bajta!

Oznacza to, że użytkownik może ukryć sporo danych zawartych w alternatywnych strumieni i nikt nie będzie wiedział?

Tak jest

Ale użytkownik nie potrzebuje pewnych specjalnych przywilejów korzystać alternatywne strumienie danych?

Nie. Nawet gość może stworzyć taki strumień w każdym pliku gdzie ma zapisany dostęp.

Jak ktoś tworzy ADS?

Możesz to zrobić w wierszu poleceń, jak notepad visible.txt:hidden.txt. Stworzysz ukryty strumień hidden.txt w pliku visible.txt. Nie ma znaczenia czy plik istnieje czy nie

Jak skopiować dane do ADS?

type atextfile -> visible.txt:hidden2.txt
Stworzy to inny ukryty strumień hidden2.txt w pliku visible.txt

Jak skopiować dane tekstowe z ADS do "normalnego" pliku?

more < visible.txt:hidden2.txt > newfile.txt
Tworzy plik newfile.txt z ukrytego strumienia hidden2.txt w pliku visible.txt

Jak można skopiowć dane binarne z ADS do "normalnego" pliku?

cat visible.txt:hidden.exe >hack.exe
Tworzy się plik hack.exe z ukrytego strumienia hidden.exe w pliku visible.txt (cat jest narzędziem z Ressource Kit)

Jak można usunąć ADS?

Załóżmy ,że wiesz gdzie jest plik important.exe z umieszczonym w nim ADS. Plik jest bardzo ważny a ADS bardzo niebezpieczny. Musisz przejść do głównego strumienia i usunąć ADS. Załóżmy, że nie ma napędu FAT w twojej sieci, w przeciwnym razie możesz przenieść plik do tego napędu a potem przesunąć go z powrotem. Wszystko co trzeba zrobić to:

```
ren important.exe temp.exe
cat temp.exe > important.exe
del temp.exe
```

Metoda ta nie działa kiedy ADS jest dołączony do katalogu. Jeśli musisz usunąć, na przykład c:\Windows:harmful.ee bez reisntalacji Windowsa, możesz użyć tej sztuczki

1. Otwórz ADS z Notatnikiem:
   C:\NT4Tools\notepad.exe c:\Windows:harmful.exe
2. Usuń całą zawartosć ADS
3. Zamknij Notatnik. Zostaniesz zapytany czy chcesz zapisać zmiany
4. Odpowiedz TAK
5. Notatnik powie ci,że plik jest pusty i że usunie go

Zrobione, ADS zniknął

Czy można dodać ADS do wpisu katalogu zamiast pliku?

Tak, to działa w ten sam sposób

Jakie możliwości stwarza Microsoft aby sprawdzić czy ADS znajduje się na moich dyskach NTFS?

A czy sądzisz, że coś ich to obchodzi?

Ale jeśli suma dostępnej i używanej przestrzeni na dysku twardym jest mniejsza niż jej rozmiar, chciałbym znać sposób sprawdzenia czu jest alternatywny strumień danych na moich dyskach NTFS!

Możesz przenieść wszystkie pliki na napę FAT i wrócić do dysku NTFS. W ten sposób wszystkie ADS'y zostaną usunięte ponieważ FAT nie wie jak zapisywać takie dane

OK, ale to nie jest praktyczne. A może chcę podejrzeć dane zanim jes usunę!

Jest narzędzie lini poleceń zwane LADS (List Alternate Data Streams), które skanuje cały dysk lub podany katalog. Listuje nazwy i rozmiar wszystkich ADS'ów jakie znajdzie

Jakich uprawnień potrzebuję aby uruchomić LADS?

Program jest narzędziem dla administratorów. Administrator normalnie ma konieczne uprawnienia. Komunikat błędu "Odmowa dostępu" nigdy nie powinien się pojawić. Jeśli jest, upewnij się ,że konto ma stosowne uprawnienia!

Wersja LADS w wersji 2.10 i wyższe obliczają inną sumę rozmiaru pliku katalogu niż wersja 2.0 .Dlaczego?

Wersj 2.10 jest zoptymalizowana dla szybszego wykonywania. Jeśli to możliwe, nie każdy plik będzie skanowany. Jednyną wadą jest brak możliwości na znajdowanie rozmiaru każdego nagłówka pliku, co jest pomijane teraz przy obliczaniu sumy użytej przestrzeni.

Czy mogę używać LADS z bootowalnej dyskietki DOS?

Program używa kilku funkcji API, daltego musi być uruchamiany pod Windowsem

Jak LADS wykrywa ADS?

W NTFS, każdy strumień pliku ma nagłówek. LADS odczytuje wszystkie te nagłówki i pokazuje tylko te , które należą do ADS

Kiedy klikam dwukrotnie na LADS.exe aby go zainstalować, widzę czarne okno DOS podczas 10 mikrosekund i nie mogę go potem znaleźć

LADS jest programem wiersza poleceń, nie ma nic do intsalacji

Jak używać właściwie LADS?

1. Otwórz okno poleceń
2. Przejdź do katalogu z LADS
3. Wpisz "LADS" i naciśnij ENTER z klawiatury
4. Przeczytaj plik Readme po więcej informacji