PAULA JANUSZKIEWICZ

# Omijanie uprawnień dostępu do plików

Stopień trudności

Systemy Windows znane są z mocno rozbudowanego zarządzania dostępem do plików. Niniejszy artykuł ma na celu pokazanie jednej z ciekawszych metod uzyskiwania dostępu do plików, z pominięciem podstawowych mechanizmów zabezpieczeń, jakimi są listy Access Control List.

Mimo tego, że artykuł obejmuje tematykę przeznaczoną raczej dla administratorów niż programistów, na wstępie chciałabym zaznaczyć, że w niektórych miejscach pozwoliłam sobie na opisanie poszczególnych funkcji systemowych. Inaczej po prostu się nie da. Zasadniczym celem artykułu jest wykazanie, że istnieje wiele *wbudowanych* metod pozwalających na uzyskanie dostępu do plików nawet, jeżeli użytkownik nie znajduje się na liście uprawnionych kont systemowych.

## Take ownership

Najprostsza metoda uzyskania dostępu do plików wymaga uprawnień *Take ownership* - niezależnie od tego, czy obiektem występującym o przejęcie pliku na własność jest Administrator (konto to ma domyślne uprawnienia *Take ownership of files or other objects*), czy zwykły użytkownik. Uściślając zagadnienie, kiedy obiekt (np. plik, folder) jest tworzony, osoba tworząca jest przez system operacyjny uznana za właściciela. W standardowym funkcjonowaniu, konto użytkownika posiada uprawnienia do obiektów w folderach prywatnych danego użytkownika, czyli jest ich właścicielem (w większości przypadków właścicielem elementów systemowych jest wirtualne konto *TrustedInstaller* np. w Windows 7). Przejęcia na własność może dokonać konto Administrator, bądź też inny użytkownik z uprawieniami *Take ownership*. Bieżący właściciel obiektu, użytkownikA może przekazać uprawnienia do obiektu innemu użytkownikowi (dodać go do listy potencjalnych właścicieli). UżytkownikB musi zdecydować się na przejęcie na własność, inaczej nie będzie właścicielem obiektu. Właściciel obiektu może w praktyce dowolnie ustawiać uprawnienia do niego. Oznacza to, że mając uprawnienie do zostania właścicielem, Administrator może sięgnąć do pliku, do którego chwilę wcześniej nie miał żadnych uprawień. W systemach Windows Vista, Windows Server 2008 nieco się to zmieniło (powstał nowy Security Identifier: OWNER_RIGHT, mogący zabronić zmiany uprawnień właścicielowi do jego

UWAGA: Istnieją w przyrodzie programy, które nie do końca szanują określone przez Administratora reguły dostępu do plików, np. Total Commander. Dobrym przykładem jest Junction (dowiązanie) Documents and Settings w Windows Vista i Windows 7 (aby wyświetlić to dowiązanie należy włączyć wyświetlanie ukrytych folderów i plików systemowych). Folder oznaczony jest symbolem kłódki i przy próbie wejścia domyślnie w Windows Explorerze otrzyma się komunikat z informacją o braku dostępu (można oczywiście przejąć go na własność, ale nie w tym rzecz). W Total Commanderze – ten sam folder przekieruje użytkownika bezpośrednio do miejsca przeznaczenia dowiązania, czyli do folderu %SystemDrive%\Users. W tym temacie odsyłam do: *http://blogs.technet.com/plwit/archive/2009/01/14/symlink-czyli-mklink-w-windows-server-2008.aspx.*

### Z ARTYKUŁU DOWIESZ SIĘ

jakie są metody omijania uprawnień do plików w systemie Windows,

co to jest BackupRead (), BackupWrite(),

jak używać narzędzia robocopy omijając uprawnienia do plików.

### CO POWINIENEŚ WIEDZIEĆ

jak działają Access Control List's w systemie Windows,

co to są prawa systemowe,

co to jest kontekst bezpieczeństwa w systemie.

własnego obiektu), ale idea pozostała ta sama. Przykład 1 oraz Przykład 2 ukazują podstawowe sposoby przejmowania na własność w systemach Windows.

### Przykład 1

Przejęcia na własność np. dla folderu, można dokonać wybierając jego Właściwości, na zakładce Security kliknąć Edit, z zakładki Owner wybrać Edit i określić właściciela (Rysunek 1).

### Przykład 2

Przejęcia na własność można dokonać również z wiersza poleceń przy wykorzystaniu `takeown.exe`, wbudowanego w system (Rysunek 2). Podano dwa przykłady: próba przejęcia na własność z uprawnieniami użytkownika (1) oraz z uprawnieniami Administratora (2). Parametr /F określa miejsce docelowe działania polecenia, /R określa wszystkie obiekty wewnątrz folderu *Dst*, /A przyznaje Administratorowi uprawnienia do obiektów (zamiast bieżącego użytkownika).

Przejmowanie zasobów na własność, opiera się o uprawnienia zdefiniowane w ACL. Działa więc jedynie w systemie operacyjnym, który rozumie ACL i całe funkcjonowanie opiera na tychże listach.

## Dostęp Offline

W kolejnej metodzie dostępu schodzi się już nieco poniżej poziomu, na którym operują listy ACL. Wszelkie ataki offline bazują na omijaniu list ACL poprzez np. przepięcie dysku do innego komputera. W wielu sytuacjach płyta DVD z systemem Windows Vista uratowała niejednemu pechowcowi cały informatyczny dorobek, właśnie poprzez fakt, że wszelkie uprawnienia ACL przy uruchomieniu systemu z płyty CD/DVD są po prostu pomijane. A co gdyby móc uzyskać dostęp do danych pomijając ACL oraz sięgać do systemu online? W końcu ACL to nie żadna świętość.

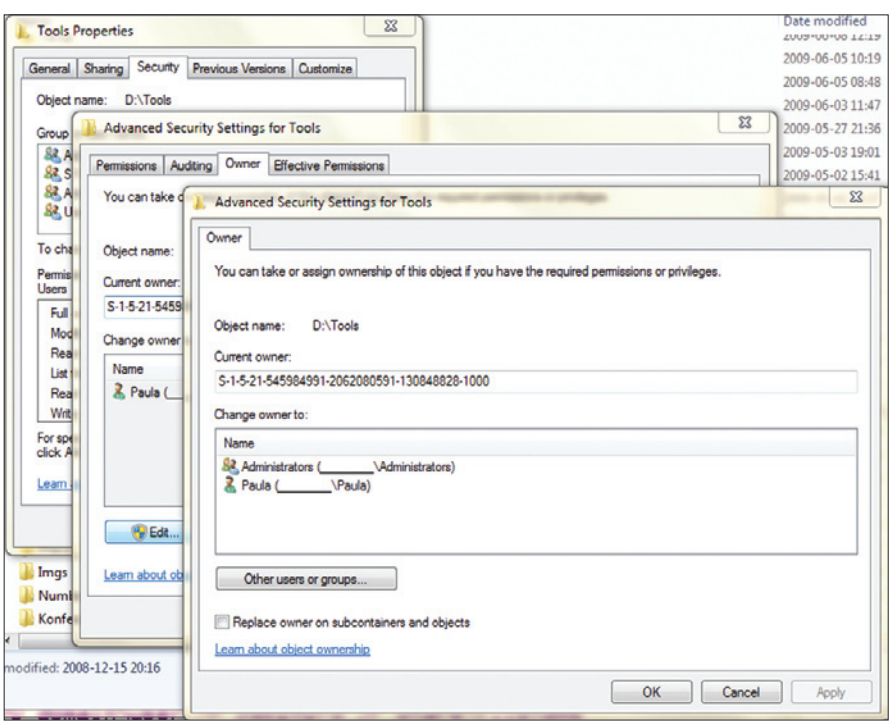
## Odczyt zawartości sektorów na dysku

Odczyt zawartości sektorów na dysku jest kolejną metodą dostępu przy ominięciu list ACL, między innymi za pomocą programów typu WinHex (Rysunek 3). Założenie jest proste: ACL nie funkcjonują na tym poziomie – zupełnie inna technologia, zupełnie inna koncepcja. W tym przypadku najlepiej sprawdziłyby się rozwiązania typu BitLocker (czy inne alternatywne metody niskopoziomowego szyfrowania).

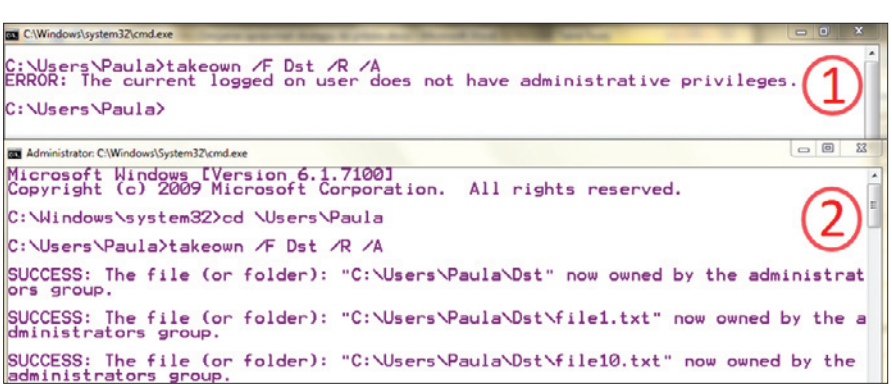
Wadą tego rozwiązania jest fakt, iż aby móc uzyskać dostęp do pożądanego dysku, należy także uzyskać do niego fizyczny dostęp (np. w scenariuszu, gdy wielu użytkowników pracuje na tym samym komputerze w trybie zmiennym). Ponadto, dostęp taki wymaga zazwyczaj praw administratora, który zazwyczaj do danych może sięgnąć kilkoma innymi metodami.

## Usługi na prawach Local System

Istnieje także standardowy mechanizm odwoływania się do określonych zasobów przez dedykowaną usługę systemową. Jest to jedynie pośrednie *ominięcie* ACL, ponieważ usługa działa po prostu na koncie o zwiększonych uprawnieniach. Jeżeli taka usługa tworzona jest w niecnych celach warto pamiętać o nadaniu jej pseudo rozsądnej nazwy w stylu: *COM+ Manager*, aby zmniejszyć prawdopodobieństwo jej wykrycia. Do utworzenia usługi potrzebne są uprawnienia administratora. Usługę tworzy się np. przy wykorzystaniu poleceń *Srvinstw.exe* – wersja z GUI, *Sc.exe* – wersja konsolowa (Microsoft KB251192). W ogólnym założeniu, celem jest utworzenie usługi systemowej, która pracując na uprawnieniach *Local System* (wbudowanych w system uprawnień administratorskich), będzie realizowała




**Rysunek 1.** *Określanie właściciela obiektu*




**Rysunek 2.** *Przejmowanie na własność przy wykorzystaniu polecenia takeown.exe*