Bezpieczeństwo systemów informatycznych

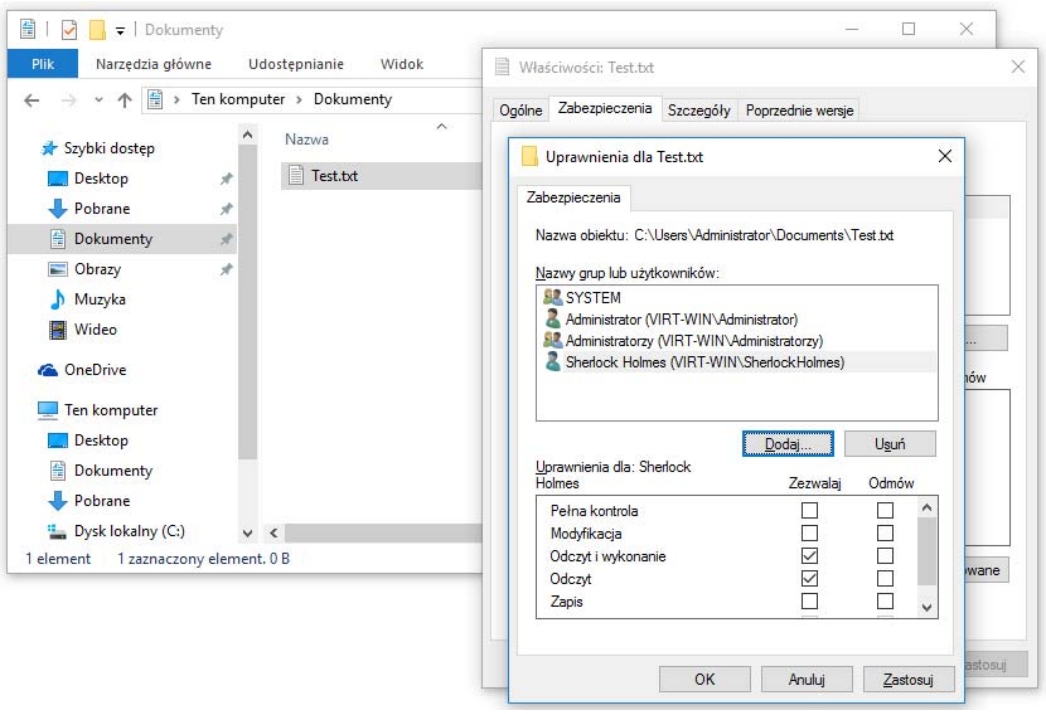
ĆWICZENIE: Windows NTFS

cz. 1: p. 1.1-1.2

1. System plików

1.1 Prawa dostępu

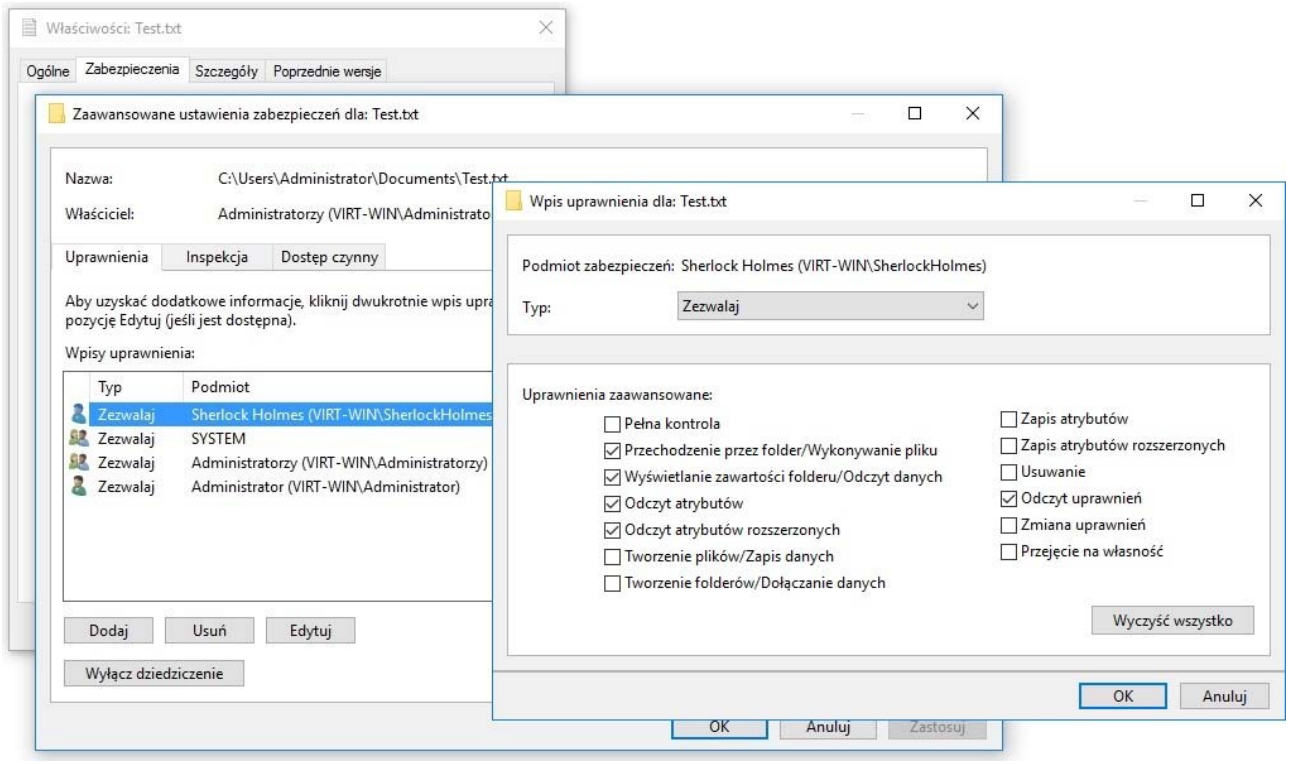
System plików NTFS umożliwia związanie z każdym zasobem plikowym (w tym: katalogiem) list kontroli dostępu ACL (*Access Control List*). Dostęp do prostych ustawień ACL pliku (katalogu) jest możliwy z poziomu np. Eksploratora Windows w opcji Właściwości (menu Plik lub kontekstowe):



Ciekawą własnością środowiska Windows jest możliwość operowania (również na liście ACL) grupami o zawartości dynamicznej (*wirtualnymi*), np. Użytkownicy uwierzytelnieni, Twórca-Właściciel. Ponadto możliwe jest oddzielne przypisywanie uprawnień na liście ACL (*zezwolenia*) i odbieranie ich (*odmowy*), przy czym odmowy mają priorytet w określaniu uprawnień efektywnych (*czynnych*) podmiotu. Uprawnienia do katalogów mogą być dziedziczone w głąb. Dziedziczenie można wyłączyć na dowolnym poziomie zagłębienia.

Widoczne powyżej uprawnienia proste są jedynie zgrupowanymi w jedną nazwę podzbiorami uprawnień szczegółowych.

Rozszerzone listy ACL są dostępne po wyborze ustawień Zaawansowanych:



Do zarządzania prawami dostępu w systemie Windows można również użyć programu icacls. Polecenie to pozwala m.in. wyszukiwać i odczytywać uprawnienia z list ACL plików i katalogów (również rekurencyjnie) wg nazwy użytkownika lub jego SID, nadawać, zmieniać i usuwać nadane wpisy ACL, resetować listę ACL (przywracać dziedziczenie z nadrzędnego katalogu), przypisywać własność obiektu użytkownikowi, czy podmieniać SID istniejącego wpisu. Przykładowo polecenie:

```
icacls *.txt
```

poda listę bieżących uprawnień ACL do wskazanych plików. Natomiast:

```
icacls *.txt /grant "Sherlock Holmes":r
```

zmieni te uprawnienia przyznając wybranemu użytkownikowi prawo odczytu.
W bardziej interesującym przypadku możemy operować na kilku prawach:

```
icacls . /grant *S-1-5-21-356853-282454-172693-1000:(w,d,wdac)
```

Ponadto poleceniem tym można zapisać istniejące wpisy ACL do plików:

```
icacls .\* /save aclfile /t
```

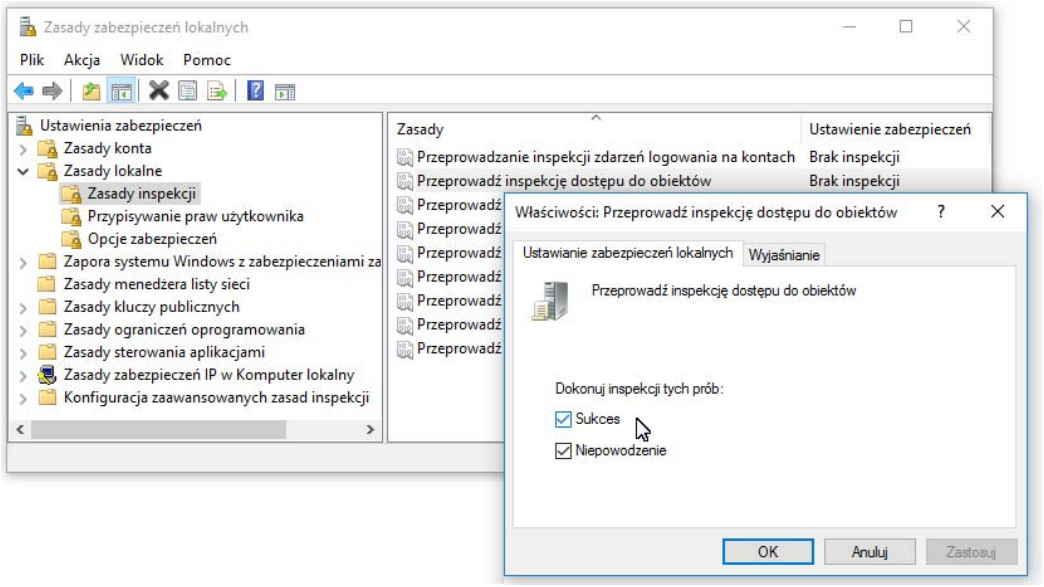
a następnie przywrócić je dla wszystkich zapisanych w ten sposób wcześniej plików:

```
icacls .\ /restore aclfile
```

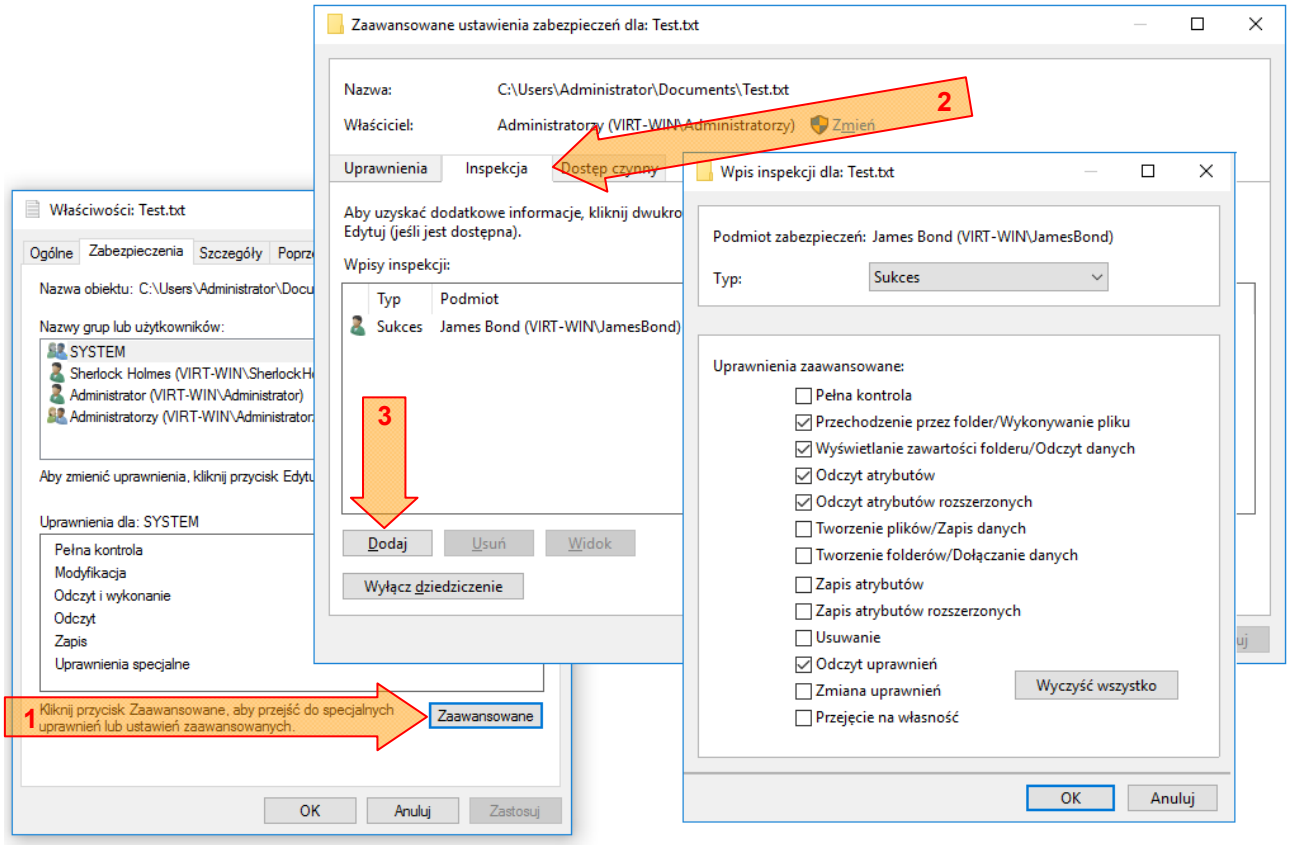
Poleceniem tym można też ustawiać poziom integralności obiektów w systemie plików.

1.2 Inspekcja dostępu do plików

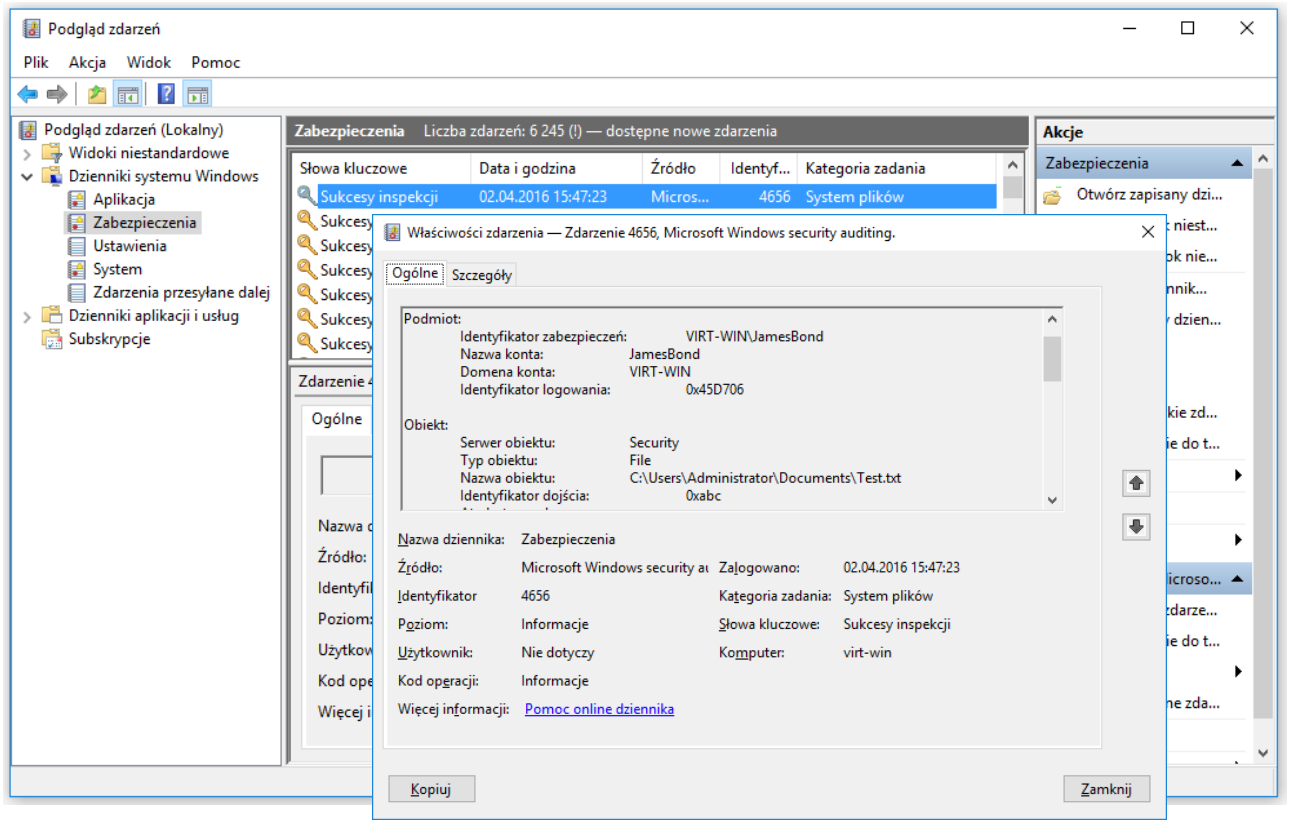
System operacyjny umożliwia rejestrowanie operacji dostępu do zasobów systemu plików, zarówno operacji udanych, jak i nieudanych. W celu uaktywnienia tej rejestracji należy najpierw włączyć inspekcję dostępu do obiektów:



Następnie, dla wybranych obiektów systemu plików należy w zaawansowanych opcjach zabezpieczeń zaznaczyć operacje mające podlegać rejestracji:

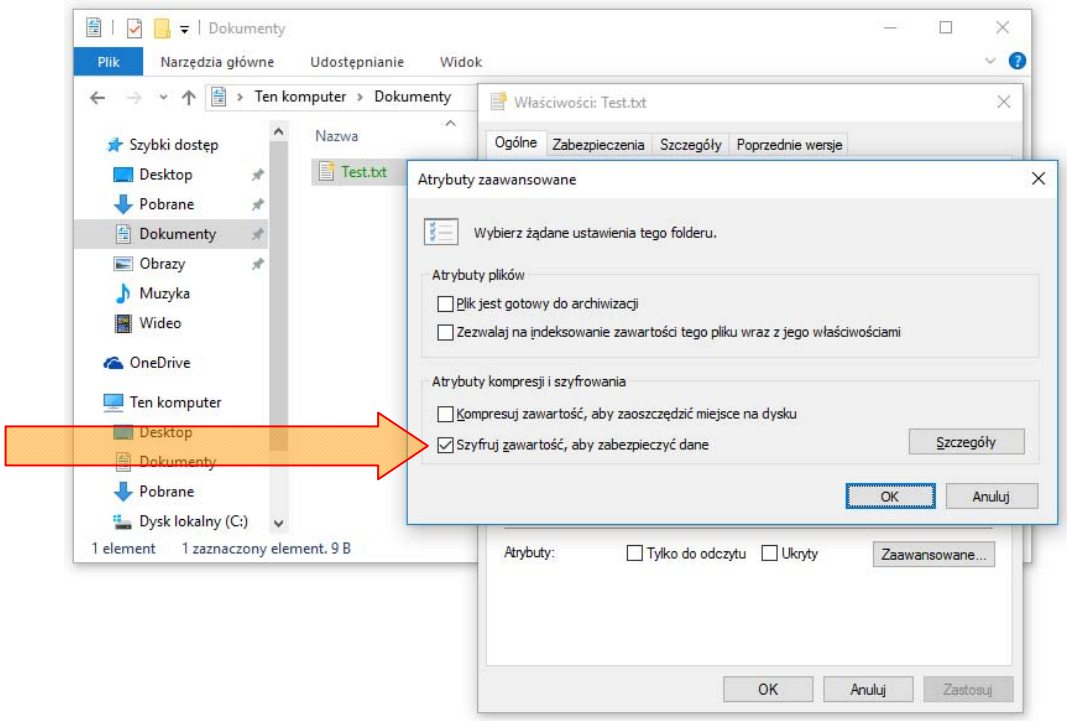


Rejestrowane operacje dostępu można przeglądać w aplikacji Podgląd zdarzeń:



1.3 Szyfrowanie

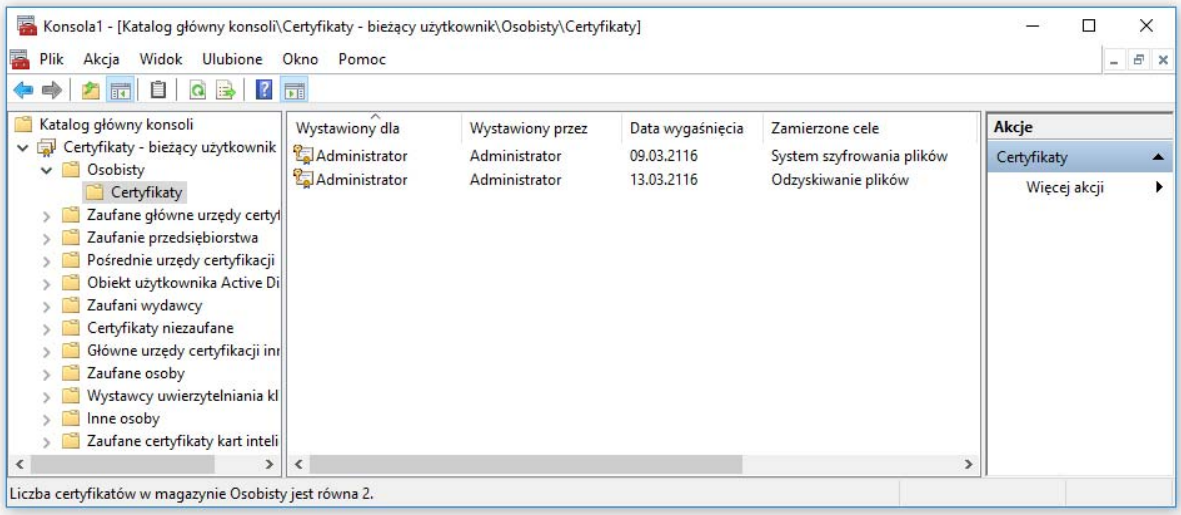
Mechanizm EFS (ang. *Encrypting File System*) umożliwia ochronę kryptograficzną zasobów plikowych w systemie plików NTFS metodą szyfrowania symetrycznego (algorytmem AES, 3DES lub DESX). Próba dostępu do zawartości zaszyfrowanego pliku (katalogu) przez użytkowników niepowołanych powoduje wygenerowanie przez system operacyjny błędu odmowy dostępu.



Operacje związane z dostępem do zaszyfrowanych plików wykonuje usługa *Local Security Authority* (LSA), całkowicie transparentnie dla użytkownika.

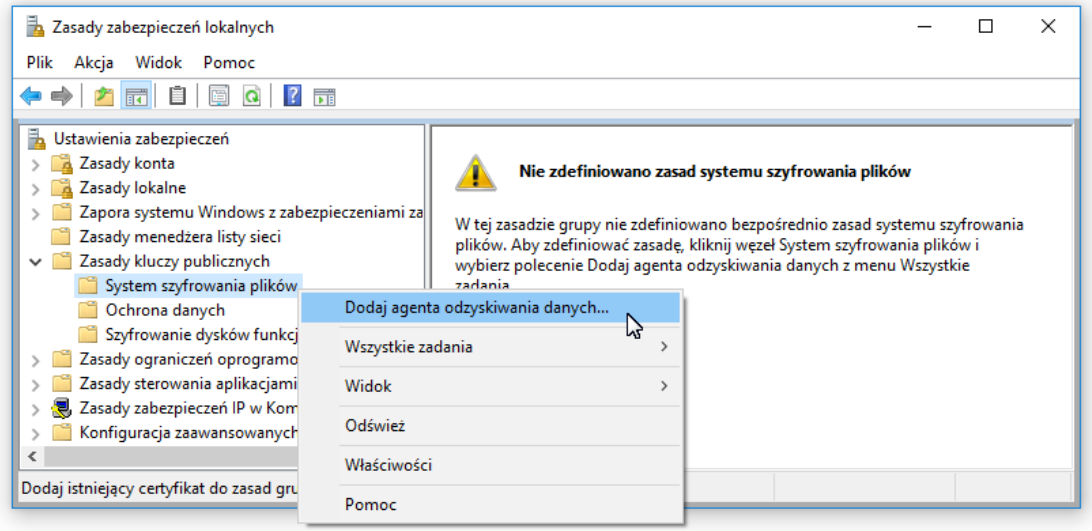
Użyty do szyfrowania pliku jednorazowy klucz symetryczny FEK (*File Encryption Key*) zapisywany jest w nagłówku EFS zaszyfrowanego pliku. Klucz ten jest z kolei zaszyfrowany kluczem publicznym (algorytm RSA) właściciela pliku, przechowywanym w certyfikacie EFS użytkownika. Klucz szyfrowania FEK może być zachowany w pliku w wielu kopiach – oprócz kopii dla właściciela nagłówek przechowuje też kopię klucza FEK dla każdego użytkownika, któremu przydzielono dostęp do zaszyfrowanego pliku oraz dla każdego zdefiniowanego agenta usługi odzyskiwania plików DRA (ang. *Data Recovery Agent*).

Certyfikaty kluczy publicznych używanych do szyfrowania kluczy FEK są widoczne w aplikacji Microsoft Management Console (program mmc). Po uruchomieniu konsoli należy z menu Plik wybrać opcję Dodaj/Usuń przystawkę (np. klawiszem ^M), a następnie dodać przystawkę Certyfikaty – bieżący użytkownik:



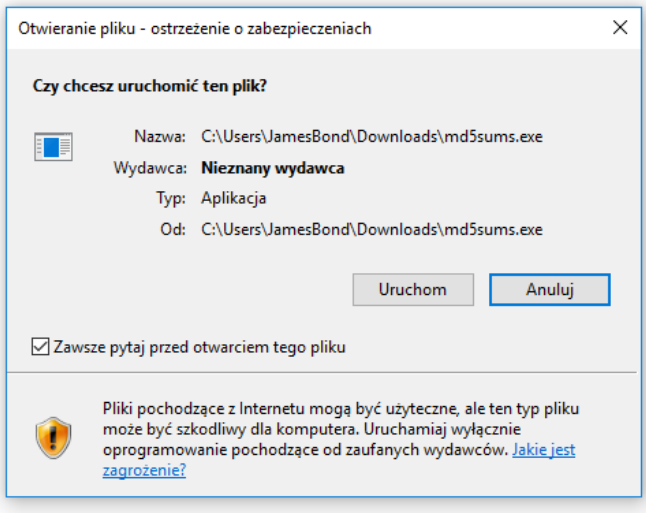
1.4 Agent odzyskiwania plików – DRA

Agent odzyskiwania plików jest użytkownikiem który może wykonywać kopie zapasowe plików (np. systemowym narzędziem Kopia zapasowa). Aby zdefiniować nowego agenta odzyskiwania w lokalnym systemie operacyjnym, można posłużyć się programem Zasady zabezpieczeń lokalnych lub Zasady grupy:



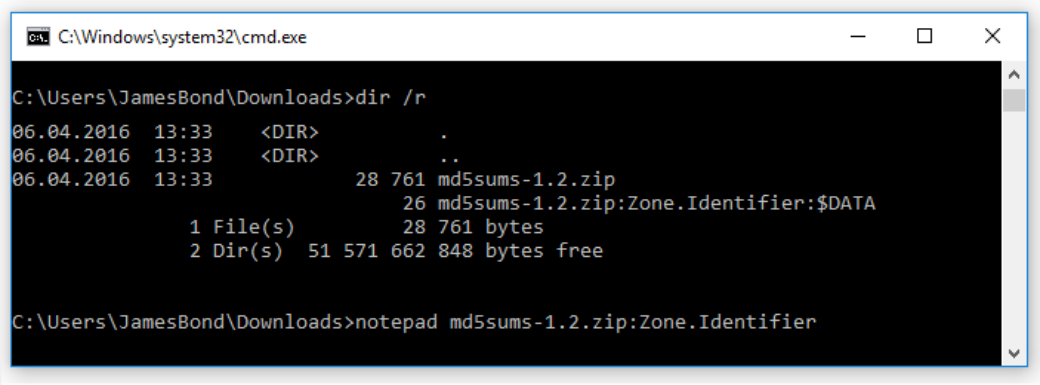
1.5 Strumienie alternatywne ADS

Mechanizm alternatywnych strumieni danych ADS (ang. *Alternate Data Streams*) w NTFS został zaadaptowany z systemu plików HFS (MacOS), gdzie służy do przechowywania metadanych. System Windows aktualnie wykorzystuje strumienie alternatywne w zasadzie tylko do przechowywania informacji o tzw. strefie internetowej, z której pobrany został plik zapisany następnie w lokalnym systemie plików. Na podstawie owej strefy, Eksplorator Windows określa poziom ostrzeżeń przy rozpoczęciu przetwarzania pobranego pliku (np. przy uruchomieniu programu wykonywalnego):



Informacja ta umieszczana jest w strumieniu :Zone.Identifier pobranego pliku. Jest to strumień tekstowy zawierający w sekcji `[ZoneTransfer]` deklarację parametru `ZoneId`.

Strumienie ujawnia polecenie `dir /r`, np.:



Strumienie ADS identyfikuje przyrostek :$DATA podawany na listingu z tego polecenia.

Jednym z nielicznych narzędzi systemu Windows, które pozwalają odczytać strumienie ADS jest Notatnik (notepad). Brak zarządzania strumieniami alternatywnymi przez system operacyjny wprowadza ogromne ryzyko potencjalnego wykorzystania strumieni jako doskonałej kryjówki złośliwego lub niechcianego oprogramowania.

Wykorzystane zasoby:

icacls (http://technet.microsoft.com/en-us/library/cc753525.aspx)

🕮 Dodatkowe informacje i narzędzia:

NTFS access control (http://support.microsoft.com/kb/308419)
EFS technet magazine (http://technet.microsoft.com/en-us/magazine/2006.05.howitworks.aspx)
EFS technet library (http://technet.microsoft.com/en-us/library/cc780166(WS.10).aspx)
EventID database (https://www.eventid.net)

🗒 Problemy do analizy:

- Jakie uprawnienia kryją się pod nazwą „Uprawnienia specjalne” widoczną wśród prostych ACL?
- Jak wyznaczane są czynne uprawnienia dostępu do zasobów NTFS? Które operacje autoryzacji – zezwolenia czy odmowy – posiadają priorytet podczas kontroli dostępu? Które uprawnienia – odziedziczone czy jawnie nadane mają priorytet?
- Jak w Windows można zmienić uprawnienia dla kilku plików jednocześnie?
- Czy można w jakiś sposób przekopiować listę ACL jednego pliku do drugiego?
- Co oznacza uprawnienie WDAC (dostępne w poleceniu icacls)?
- Na czym polega działanie funkcji Bypass Traverse Checking w NTFS?
- Jak szyfrowany jest plik w systemie NTFS: metodą symetryczną czy asymetryczną? Jakim kluczem? Gdzie ten klucz jest przechowywany i jak jest zabezpieczony?
- Co zawierają certyfikaty EFS użytkowników?
- Jak umożliwić współdzielenie zaszyfrowanego pliku?
- Do czego służy systemowe narzędzie rekeywiz?