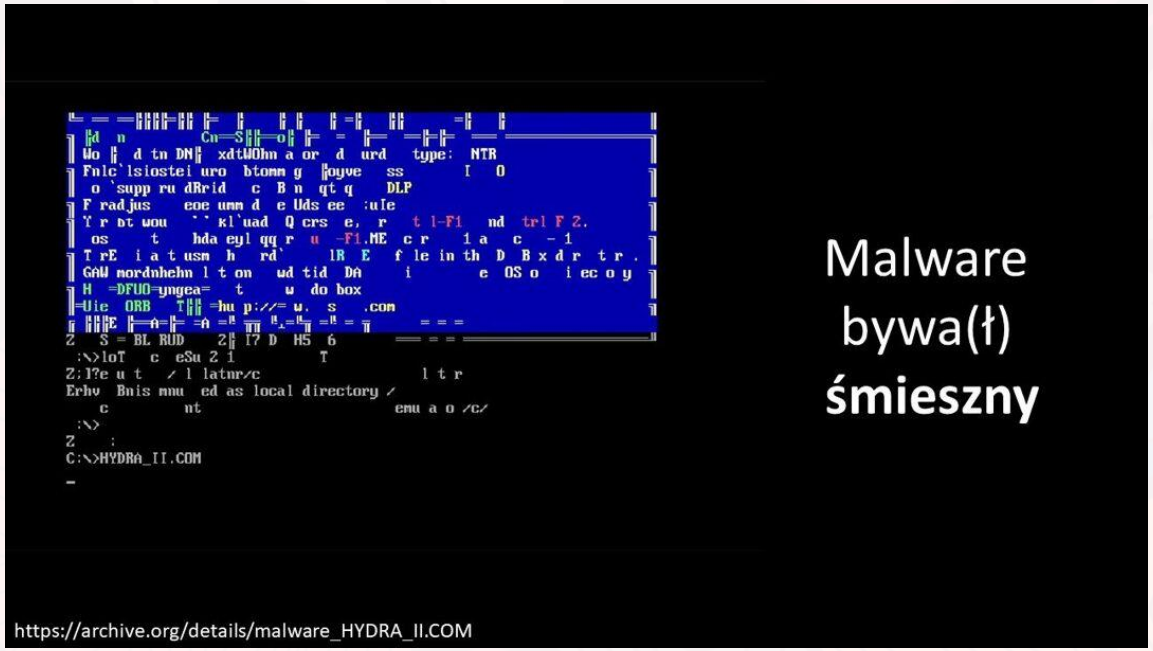

CZEGO NIE WIESZ O ZŁOŚLIWYM OPROGRAMOWANIU

Nie każde złośliwe oprogramowanie od razu niszczy lub kradnie Twoje dane. Jeżeli popatrzymy na starsze przykłady malware'u - często zobaczymy, że były to zabawne programy pokazujące kunszt twórców. Stanowiły pokaz umiejętności programowania i prezentowały niezwykłe możliwości systemu.

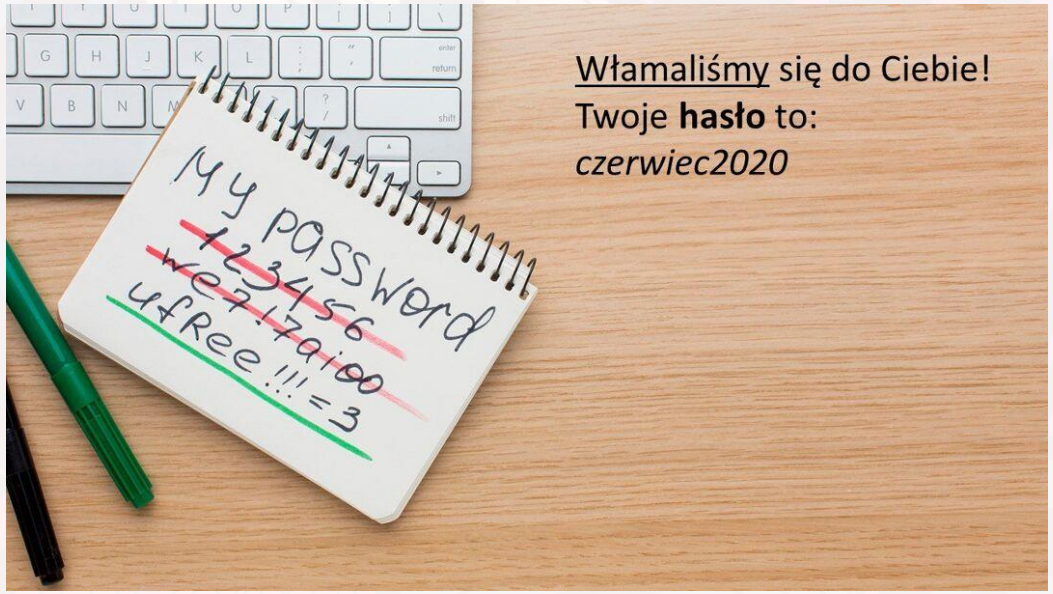


Ale to już przeszłość. W dzisiejszych czasach chodzi głównie o zysk - jak zarobić na tych, którzy uruchomili niebezpieczne oprogramowanie. Widok taki jak tutaj - może więc przestraszyć - zwłaszcza jeżeli jesteś prezesem dużej firmy. No bo wyobraź sobie, że przychodzi do Ciebie księgowa i informuje Cię że wszystkie dane finansowe znikły. Albo mówiąc bardziej szczegółowo - zostały zaszyfrowane.

Teraz taki komunikat może być **przerażający**

https://avlab.pl/aktualizacja-3-podpowiadamy-jak-zabezpieczyc-komputery-przed-ransomware-wannacry/

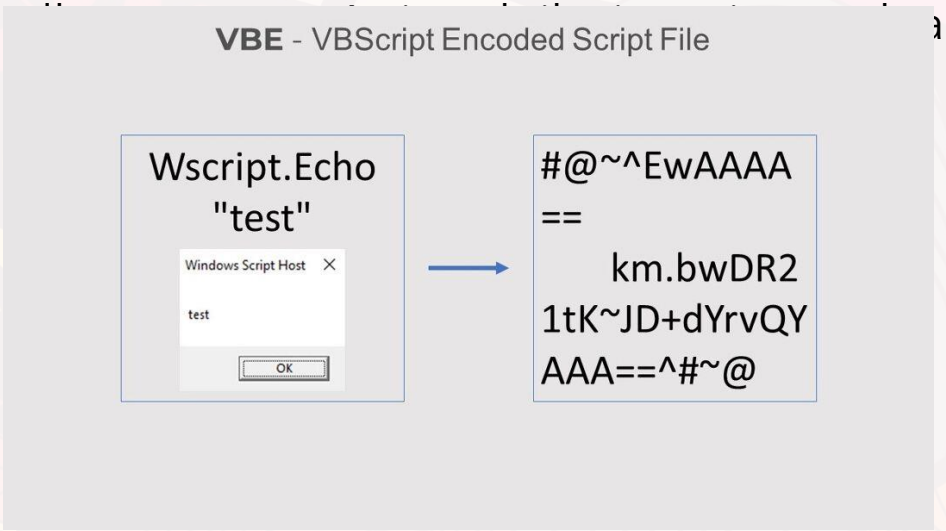
SCAM, próba oszustwa. Bo jeśli przestępca wyśle takiego maila do miliona użytkowników, to zapewne znajdzie się jakiś procent, który nie będzie pewny swoich poczynań i wpłaci odpowiednią kaucję



Jeżeli pracujesz w dużej korporacji, to pewno od czasu do czasu bierzesz udział w szkoleniach z bezpieczeństwa. Słyszysz tam, że pliki **exe**, pliki **js** czy **vbs** mogą być niebezpieczne. Że nie powinieneś klikać w nieznane Ci odnośniki - bo mogą zawierać niebezpieczne dane.

VBS to język skryptowy stworzony przez Microsoft, stanowiący część rodziny języków Visual Basic. Z językami skryptowymi wiąże się jednak problem piractwa. Bo użytkownik końcowy, nie otrzymuje skompilowanego pliku exe - ale cały kod źródłowy aplikacji, który może otworzyć i przeczytać w dowolnym edytorze tekstu.

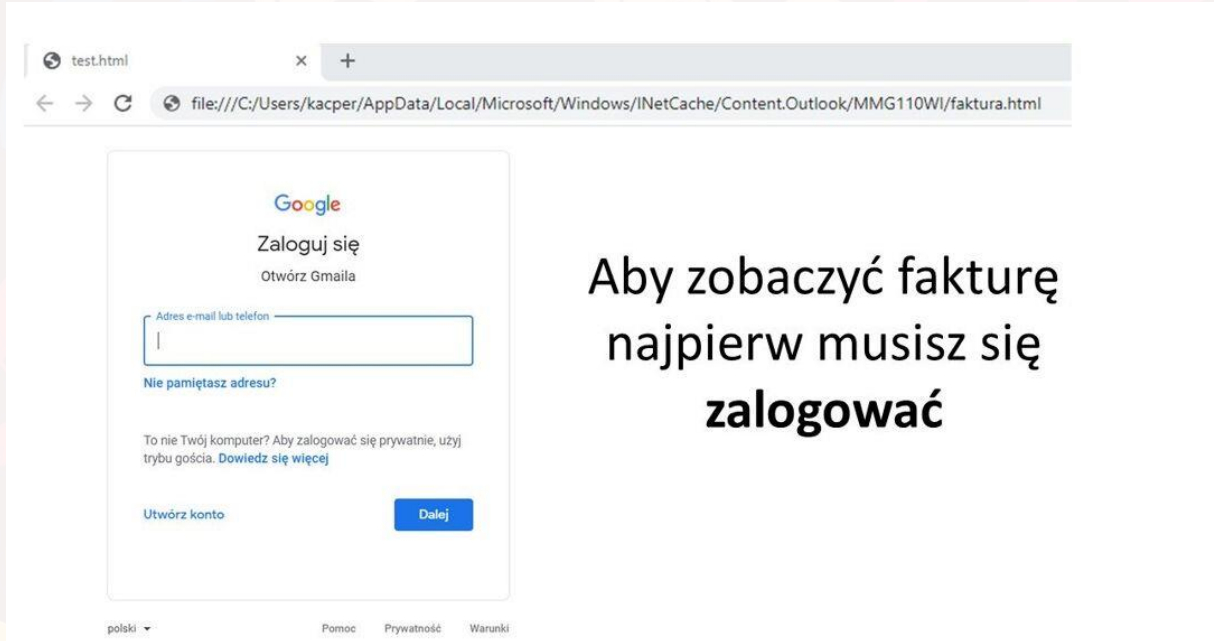
Z punktu widzenia programistów, którzy żyją z tworzenia kodu źródłowego - mogło to stanowić problem. No bo taki kod można dowolnie kopiować i dystrybuować bez płacenia za niego. Postanowiono więc rozwiązać ten problem i zaobfuskować plik, który trafia do użytkownika. Czyli zamieniamy go na postać, która



i zupełnie

Po lewej stronie prosty program, wyświetlający okienko z napisem test - korzystając z funkcji echo. Po prawej stronie dokładnie **ten sam** program - ale poddany procedurze **obfuskacji**.

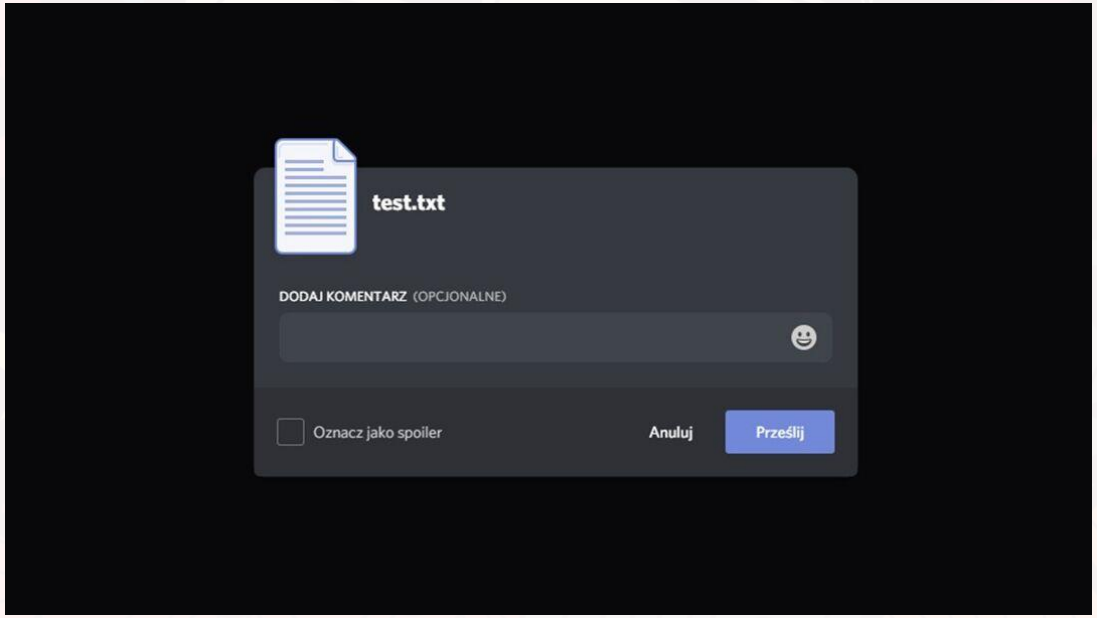
Złośliwe mogą być też proste pliki **HTML**. Tutaj otrzymałeś fakturę od gazowni. Prosta sprawa - trzeba otworzyć załącznik, skopiować numer rachunku i wysłać przelew. Klikasz więc w plik i otwiera się przeglądarka.

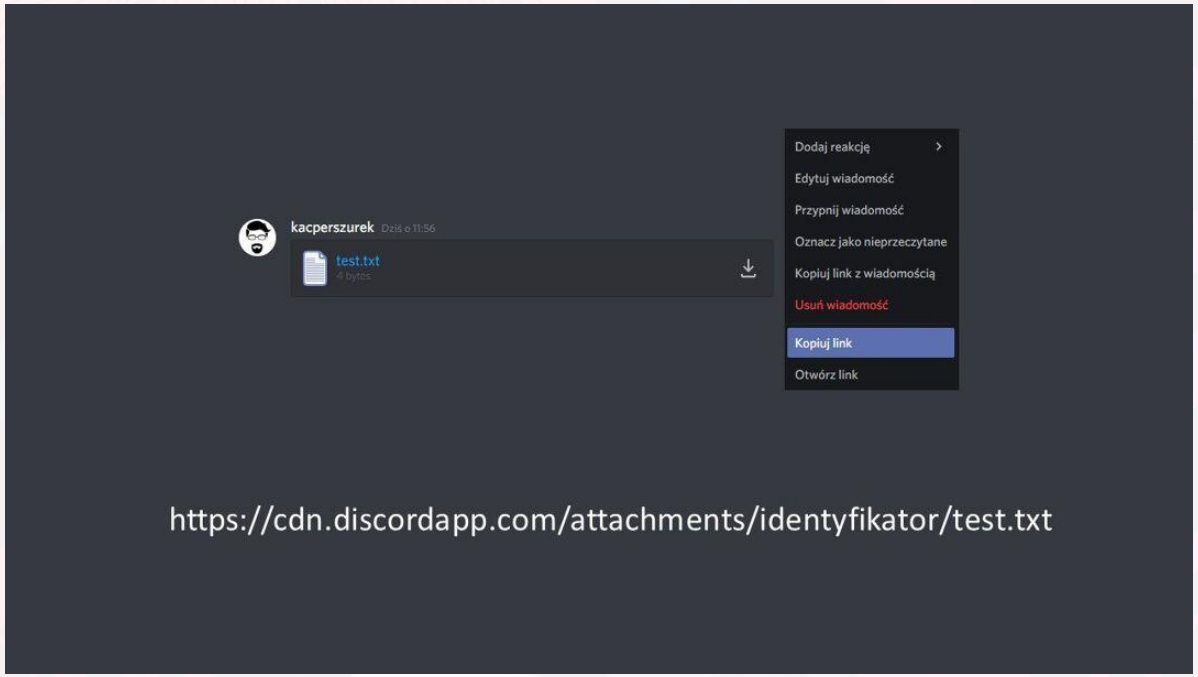


Kolejne pytanie - o logowanie. Normalna rzecz - otworzyło się nowe okno przeglądarki, więc nie jestem zalogowany na swoją skrzynkę mailową. Ile osób zauważy, że to oszustwo? Że tak naprawdę nie jesteś na stronie Gmaila? Że obok paska adresu nie ma zielonej kłódeczki? Ile osób wie, że wpisując w to okno cokolwiek - wysyłamy te dane przestępcom?

Ale nie zawsze malware jest wysyłany przez email. Czasami możemy pobrać złośliwe oprogramowanie ze strony internetowej - zwłaszcza jeżeli poszukujemy nielegalnych wersji oprogramowania, darmowych filmów czy gier. Jeżeli masz stronę internetową to wiesz - że potrzebna jest do tego domena i **serwer**.
Dzięki temu użytkownicy mogą wyświetlać nasz sklep i blog. Tak samo jest w przypadku złośliwych plików - muszą się one znajdować gdzieś fizycznie, na jakimś serwerze - aby można je było ściągnąć.

Discord to bezpłatna aplikacja służąca do rozmów głosowych i komunikacji za pomocą wiadomości tekstowych. Popularna głównie wśród młodszych użytkowników, którzy grają w różne gry. Dostępna w formie aplikacji na telefon, ale także programu na system Windows.
Użytkownicy mogą tam rozmawiać ze sobą za pomocą **kanałów**. Można też korzystać z prywatnych wiadomości. Oprócz tekstu i emotek oprogramowanie pozwala na przesyłanie **plików** do innych osób.



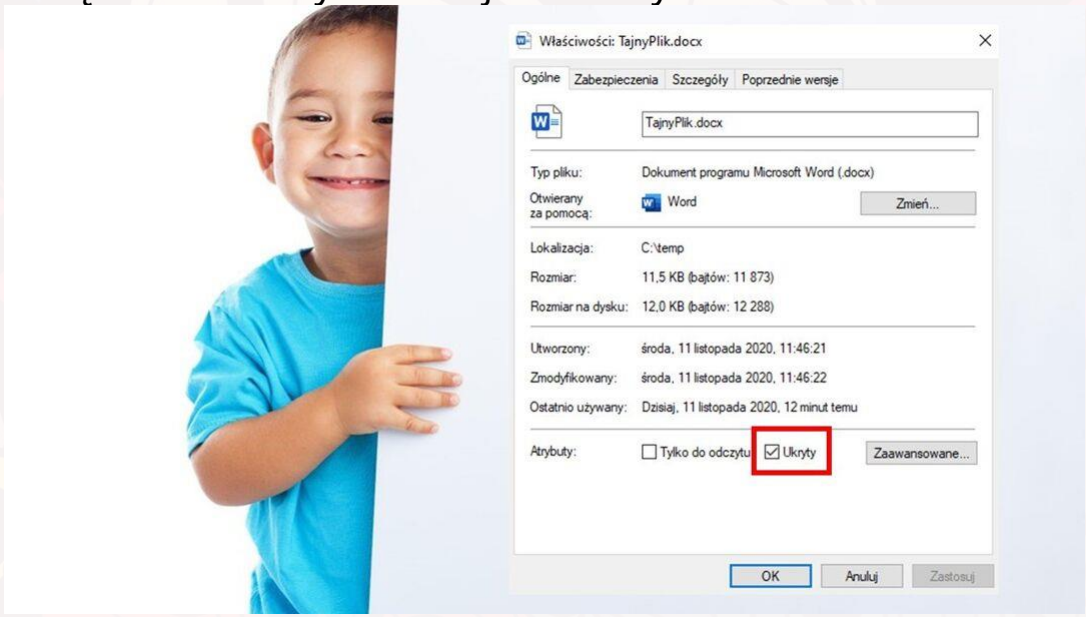


W tle generuje się unikalny odnośnik. Każdy kto zna **identyfikator** - może za jego pomocą pobrać plik i zapisać na swoim dysku.

Czy już widzisz schemat?

Twórcy malware'u mogą wykorzystać tą usługę do przechowywania swoich plików. Oczywiście są one po jakimś czasie **blokowane** i usuwane - ale dalej - przez jakiś czas przestępcy mogą z nich korzystać za darmo - bez żadnych kosztów. Co więcej, ta domena nie może zostać **zablokowana** przez twórców antywirusów. Bo należy do **legalnej** firmy i większość osób korzysta z niej w prawidłowy sposób.

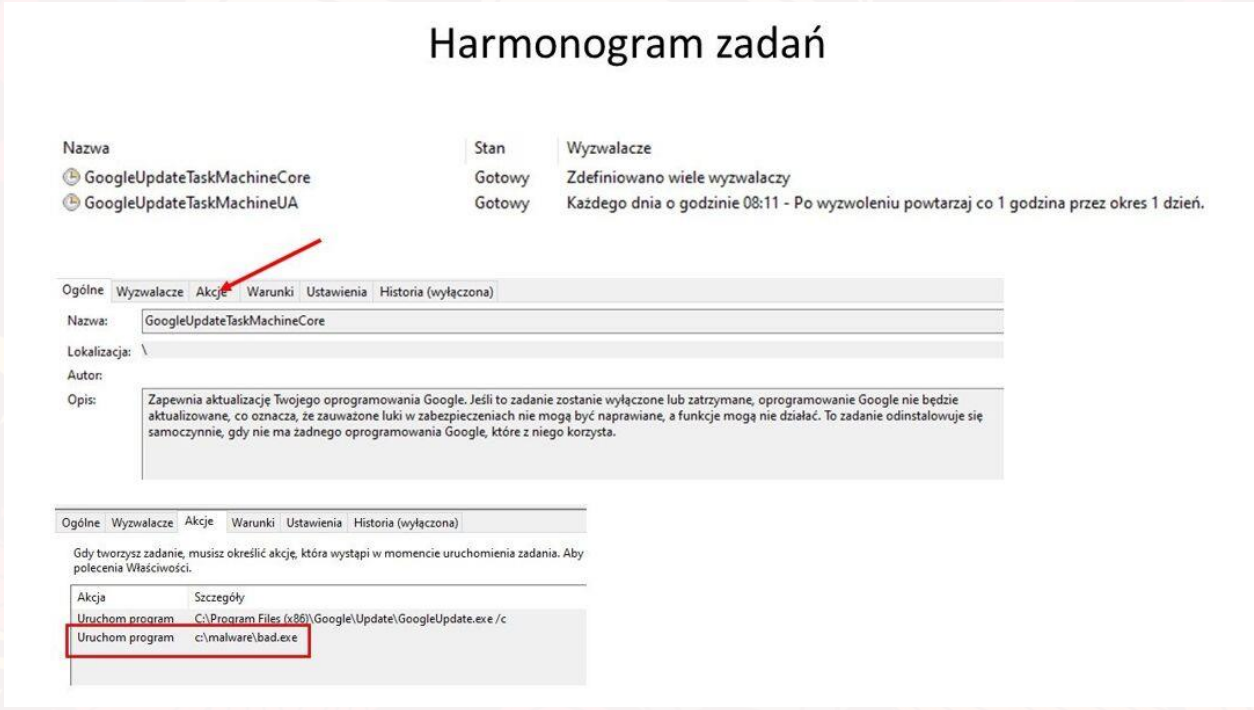
No dobrze - złośliwe oprogramowanie pojawiło się już na Twoim dysku. Teraz musi się ukryć przed Twoim wzorkiem - tak aby jak najdłużej pozostało aktywne bez wykrycia. Jak wygląda taka zabawa w "chowanego"?
W systemie Windows - pliki mogą mieć nadane atrybuty. Jednym z takich atrybutów jest wartość ukryty. Wtedy taki plik nie wyświetla się w niektórych miejscach systemu.



W eksploratorze dla przykładu musimy zaznaczyć odpowiednią opcję, aby móc widzieć takie pliki ponownie. No ale nie oszukujmy się, ta metoda to *nic skomplikowanego*.

No dobrze - czy wiesz, że Windows posiada harmonogram zadań? Umożliwia on planowanie automatycznie wykonywanych zadań. Ten mechanizm można dla przykładu wykorzystać do aktualizacji oprogramowania.

Korzystasz z Chroma? Podczas instalacji automatycznie definiowane jest nowe zadanie nazwane GoogleUpdateTaskMachineCore. Jak możemy wyczytać z opisu: "zapewnia ono aktualizacje Twojego oprogramowania Google".



ADS tłumaczymy jako **Alternate Data Stream**. Pozwala on na dodanie dodatkowych danych do pliku - równocześnie nie zmieniając oryginalnych danych. Możemy więc **ukryć** dane - tak jak na tym przykładzie.

W pliku plik.txt znajduje się zawartość nic ciekawego. Widzimy to, wyświetlając zawartość tego pliku przy pomocy komendy more.

Przy pomocy ADS chowamy tam dodatkowe dane o nazwie ukryte. To właśnie tam zapisujemy wartość tajne dane. Możemy ją później odczytać - ponownie korzystając z komendy more.

Tym razem oprócz nazwy pliku, po dwukropku podajemy identyfikator ADS. Kolejny sposób na ukrycie danych - bo, o ile nie znasz nazwy ADS, nie możesz ich wyświetlić. A poznanie identyfikatorów ADS nie jest takie proste - zwłaszcza, jeżeli nie wiesz, że coś takiego w ogóle istnieje.