MiscDev 001

by gynvael.coldwind//vx

001. Własny toolset

Cel

Cel główny:
- chcemy zmodyfikować lekko regedit.exe, tak aby odzyskać dostęp do rejestru
- rozkodować plik SECRET.TXT (mamy histogram oryginału!)

Cel

Cel drugorzędny:
Chcemy stworzyć kilka przydatnych funkcji oraz narzędzi, które będziemy używać w przyszłości:
Funkcje do operacji na plikach:
- wczytanie całego pliku do pamięci (text, bin)
- zapisanie fragmentu pamięci jako plik
- wczytanie całego pliku pod podany adres
- wczytanie fragmentu pliku pod podany adres
- wypisanie fragmentu pamięci jako hex/ascii

Narzędzia:
- wypisanie wszystkich stringów z danego pliku
- wypisanie (fragmentu) pliku jako hex/ascii
- histogram znaków w pliku

Założenia

portable

re-usable

secure
(później)

stable
(później)

Część pierwsza

rozkodować plik SECRET.TXT

histogram znaków w pliku

wczytanie całego pliku do pamięci (text, bin)
wczytanie całego pliku pod podany adres*
wczytanie fragmentu pliku pod podany adres*

Część pierwsza

? stabliność ? security ?

Część druga

uruchomić regedit.exe

wypisanie wszystkich stringów z danego pliku
wypisanie (fragmentu) pliku jako hex/ascii

zapisanie fragmentu pamięci jako plik
wypisanie fragmentu pamięci jako hex/ascii

Część druga

? stabliność ? security ?

Podsumowanie

Inne przydatne narzędzia do stworzenia we własnym zakresie

sleep
rip out
fuzz
byte diff
xor / add / sub / rotate

Dziękuje za uwagę :)

http://re.coldwind.pl/
http://gynvael.coldwind.pl/