

Mateusz „krzywy” Krzywicki

Inżynieria Wsteczna w praktyce Zabezpieczenia aplikacji

Inżynieria Wsteczna

- Co to jest?
- Co możemy zrobić?

Kto „rewersuje”?

- Analitycy zagrożeń w firmach AV
- Kontrolerzy jakości, bezpieczeństwa
- Pasjonaci
- Crackerzy

Kto powinien „reversować”?

- Programiści

Co „reversować”?

- CrackMe
- KeygenMe
- UnpackMe
- DebugMe
- ReverseMe

Jak to wygląda?

- Pokaz podstawowych technik crackerskich.
- CrackMe
- 2x UnpackMe

Rady dla programistów

- Trial – zapomnijcie o nim
- Demo – brak funkcji zapisu (brak!)
- Antydebugi, packery, protectory i utrudniacze życia

Najlepsze zabezpieczenia?

- Wszystkie które wymagają uwierzytelnienia na serwerach producentów. (np. steam, gry online, UBI DRM)
- Ring zero i niżej (VM)

(Niestety obie metody są zawodne do tego stopnia, że nie warto z nich korzystać.)

Nie da się?



Gdzie szukać wiedzy?

- Po drugiej stronie barykady – u crackerów
- Na forach
- IRC
- Książki? Neeee. Przestarzałe.

Dziękuję za uwagę

- Poproszę kawę :D