Ukážka analýzy malware

Ladislav Bačo

Computer Security Incident Response Team Slovakia

17. máj 2016

Úvod

- rýchla ukážka analýzy PE vzorky
- prerekvizity
- ciele prednášky

Analýza malware

- základná statická analýza
- behaviorálna analýza
- dynamická analýza
- pokročilá statická analýza – reverzné inžinierstvo

Základná statická analýza

- *môže byť vzorka nebezpečná?*
- základné informácie o vzorke bez jej spustenia
  - sekcie
  - importy, exporty
  - resources
  - reťazce
  - *hash* $\rightarrow$ *VirusTotal*
  - entropia
- *(Ukážka)*

Behaviorálna analýza

- *čo robí vzorka za normálnych okolností?*
- spustenie vzorky v bezpečnom prostredí
- simulovanie reálneho prostredia
  - virtuálne PC
  - virtuálny Internet
- *(Ukážka)*
- problém: skrytá funkcionalita

Dynamická analýza

- *ako funguje vzorka?*
- debuggovanie vzorky v bezpečnom prostredí
- simulovanie reálneho prostredia
  - úprava flagov a registrov
- antidebug ochrany
- *(Ukážka)*

Reverzné inžinierstvo

- *čo všetko dokáže vzorka robiť? ako to robí?*
- disassemblovanie/dekompilovanie zdrojového kódu
- pochopenie významu kódu
  - obfuskovaný kód
- *(Ukážka)*

Použité (a ďalšie užitočné) (free) nástroje

- Wireshark
- VirtualBox
  - virtualizované systémy používajú sieťový adaptér len pre hostiteľa
- Windows 7 (kontrolované spúšťanie malvéru)
  - Far Manager s vlastným User Menu
  - Hiew 32 Demo
  - PSPad
  - PEiD
  - ResourceHacker
  - SysInternals Suite
    - Strings
    - ProcessMonitor
    - ProcessExplorer
    - Autoruns
  - NirLauncher + Nirsoft Utilities
    - DNSQuerySniffer
    - HTTPQuerySniffer
  - RegShot
  - OllyDbg
  - Ida Free, Ida Demo
- Remnux distro (simulácia Internetu, obsahuje tiež analytické nástroje na statickú analýzu a reverzné inžinierstvo)
  - InetSim
  - DnsMasq

Otázky, diskusia.

Kontakt

Mgr. Ladislav Bačo
Oddelenie NIKI
CSIRT.SK
WWW.CSIRT.GOV.SK

ladislav.baco@csirt.gov.sk