

Z každého rožku trošku

Peter Košinár

kosinar[zavináč]eset.sk

Šifra sem, šifra tam

- Nie vždy máme všetko naservírované na striebornom podnose.
- Aj jednoduchá substitúcia spraví z PE či ELF fajlu nezrozumiteľný mix.
- Najčastejšie jednoduché 1-, 2-, 4-, 8- bajtové substitúcie.
- XOR, ADD (SUB), ROL (ROR)
- Občas špeciálne triky kvôli stringom (koncová nula, ...)
- Štatistická analýza vie byť extra užitočná.
- Programy sú plné núl, debug-verzie tiež 0xCC-čiek.

Base64

- Reprezentácia postupnosti pomocou 64-znakovej sady (A-Za-z0-9+/) a podľa potreby ešte jedného extra znaku (=).
- 3 bajty ($= 3 \cdot 8$ bitov) $\Rightarrow$ 4 znaky ($4 \cdot 6$ bitov)
- Vymyslené najmä kvôli e-mailom.
- Extra populárne, aj keď ho veľakrát netreba.
- Variácie zvyčajne v posledných dvoch hodnotách, ale aj alfanumerická časť môže byť prehádzaná.
- Ďalšie variácie na podobnú tému – Base32, Ascii85, ...

Encoding

- Nie všetko, čo vyzerá divne binárne, je skutočne šifrované 😊
- Existuje veľa foriem zápisu znakov, encodingov:
 - ASCII – 8 bitov na znak
 - Codepages – 8 bitov na znak, dolná polovica ako ASCII, horná špecifická pre danú sadu.
 - Unicode (UCS-2) – 16 bitov na znak, `wchar_t`
 - Unicode (UTF-8) – 1-4 bajty (ľahko rozšíriteľné na 1-6)
 - Môžu, ale nemusia byť označené!
- Uhádnuť encoding vie občas dosť pomôcť – aj programátor je zvyčajne len človek a chybové hlásenia sa hodia.

Formáty

- Slušné formáty sa dajú rozoznávať podľa nejakej značky (začiatok súboru, občas koniec súboru, ...)
- Položky majú buď fixnú dĺžku, alebo je dĺžka niekde nablízku.
- Existujú aj polygloti – súbor môže naraz sedieť na viac formátov.
- „file“ pozná formátov pomerne dosť – tak zvyčajne poradí.
- Ak nie, dá sa stále skúsiť niečo „uhádnuť“.

Steganografia

- V súbore sa toho môže skrývať viac, ako je na prvý pohľad zrejmé.
- Aj v nevinnom .jpg súbore môže byť niekde skrytý exáč 😊
- Zvyčajne obrázky resp. audio/videoformáty: malá zmena nie je vidieť ani počuť.
- Nízke bity, každý n-tý, ...

Ďakujem za pozornosť

Peter Košinár

kosinar[zavináč]eset.sk