SSTIC 06 - Rump Sessions

Metasm

Raphaël Rigo
Yoann Guillot

France Telecom R&D

C’est quoi ?

- Assembleur / Désassembleur modulaire
- Full Ruby : pas de dépendances, multi platerforme
- Principalement fait pour être intégré, scripté
- GPL
- Encore en version alpha

Ca fait quoi ?

- Pour l'instant : Intel et MIPS
- Désassembleur ELF et PE
- En cours : "moteur" de polymorphisme (shellcodes)
- Intégration dans Metasploit 3 prévue : plus de shellcode en hexa

Demo

Demo