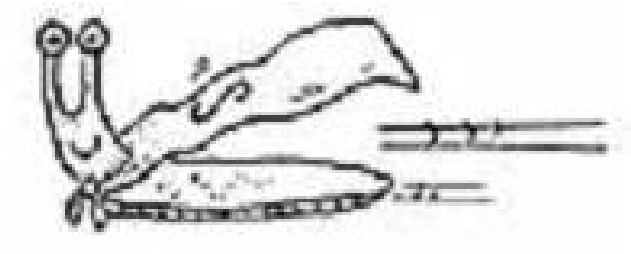
SSLug



rstack.org

valgasu@rstack.org

Programme pour Internet Explorer type "SSL Man-in-the-Middle Inside". Cela pourrait être simplement un spyware, un malware, ...

+ Injection de code pour l'API Hooking
  * OpenProcess
  * VirtualAllocEx
  * WriteProcessMemory
  * CreateRemoteThread

+ API Hooking avec redirection via un JMP
  * Sauvegarde les premières instructions
  * Patch l'API avec un JMP vers notre code
  * Appel les instructions sauvées et l'API

+ API Hookées pour les connexions de SSLug
  * HttpOpenRequest, HttpSendRequest : gestion de la connexion à notre serveur MiM, désactive les cookies, le cache et la redirection, ajoute les bons champs HTTP (Host, Cookie)
  * InternetReadFile, InternetReadFileEx, InternetCloseHandle : gestion des cookies

+ API Hookées pour les certificats
  * CertVerifyCertificateChainPolicy : valide notre certificat auto-signé

+ API Hookées pour les certificats
  * InternetShowSecurityInfoByURL : utilisé par IE quand vous cliquez sur le cadenas, vous pouvez alors spécifier l'URL du site original pour récupérer et afficher le véritable certificat.

+ Demo ?