Autor: Ruxandra F. Olimid
Departamentul de Informatică, Universitatea din București

- Laboratorul 9 -

Analiză de scripturi

Disclaimer: Pe parcursul acestui curs/laborator vi se vor prezenta diverse noțiuni de securitate informatică, cu scopul de a învăța cum să securizați sistemele. Toate noțiunile și exercițiile sunt prezentate în scop didactic, chiar dacă uneori se presupune să gândiți ca un adversar. Nu folosiți aceste tehnici în scopuri malițioase! Acestea pot avea consecințe legale în cazul comiterii unor infracțiuni, pentru care **deveniți pe deplin răspunzători**!

A. *Analiză statică*

Analiza statică presupune examinarea unui fișier prin diverse metode fără a îl executa. În acest sens ne putem uita la proprietățile fișierului, la numele acestuia, la string-urile din interior, la rapoartele unor sisteme de antivirus/anti malware sau la codul sursă (dacă se poate).

B. *Analiza dinamică*

Analiza dinamică presupune examinarea unui fișier prin executarea acestuia. Anumite exemplare de malware au un efect vizual care permit o clasificare rapidă, în schimb altele folosesc diverse tehnici pentru a se ascunde. Pentru exercițiile din laborator este suficientă o analiză dinamică de comportament, care nu presupune folosirea unui debugger.

Folosiți analiza statică și dinamică pentru următoarele exerciții. Arhivele cu exerciții folosesc parola **infected**. Analiza sample-urilor este recomandată pe sistemul de operare Windows. Dezactivați sistemele antivirus de pe mașina de analiză!

1. Analizați fișierul ***sample1.js*** folosind *Node JS* (puteți folosi un tool online [1]). Răspundeți la următoarele întrebări:
   a. Ce face acest cod? Justificați.
   b. Cum ați ajuns la această concluzie?
   c. Care este mesajul ascuns?
   d. Cine a realizat acest cod (în acest format)?

Important! Următoarele exerciții se vor rezolva **fără Node JS**. Ele vor putea fi analizate prin intermediul unui editor de text (spre exemplu *Notepad / Notepad++*) pentru analiza statică și vor putea fi rulate direct în mașina virtuală/pe PC-ul dvs pentru analiza dinamică.

Hint: Link-urile de la referințe vă pot fi de folos.

2. Analizați fișierul ***sample2.js*** și răspundeți la următoarele întrebări:

a. Ce face acest cod? Justificați!
b. Putem să considerăm că acest fișier este malware?
c. Cine a realizat acest cod?

3. Analizați fișierul ***sample3.js*** și răspundeți la următoarele întrebări:

a. Ce face acest cod? Justificați!
b. Explicați conținutul de tipul '\x$$'. Ce sunt aceste valori?
c. În urma unei analize dinamice observăm un comportament asemănător cu primul sample. Care este diferența dintre cele două sample-uri?

4. Folosind analiza statică, dinamică și tool-ul online *VirusTotal* [2], analizați fișierul ***sample4.js*** și răspundeți la următoarele întrebări:

a. Ce face acest script?
b. Cum putem extrage payload-ul fără să rulăm scriptul (doar din analiză statică)?
c. Putem considera acest script că este malware?
d. Căutați/Încărcați acest fișier pe *VirusTotal* [2]. Ce observați? În urma raportului de pe *VirusTotal* cum încadrați acest sample până la urmă (malware/benign)?
e. Folosiți tool-ul [3] pentru a obfusca scriptul. Salvați rezultatul într-un fișier javascript și încărcați acest fișier pe VirusTotal [2]. Ce observații notabile puteți face? Explicați!

Referințe bibliografice

1. Node.js Online Compiler & Interpreter - Replit. Accesibil la: https://replit.com/languages/nodejs.
2. VirusTotal. Accesibil la: https://www.virustotal.com/gui/home/upload.

3. BeautifyConverter JavaScript. Accesibil la: https://www.beautifyconverter.com/javascript-obfuscator.php.