

Ministerul Educației și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

Departamentul Ingineria Software și Automatică

Raport la

Lucrarea de laborator Nr. 5

Disciplina: Tehnici de inginerie inversa

**Efectuat:** st. gr. SI-211: Chihai Adrian

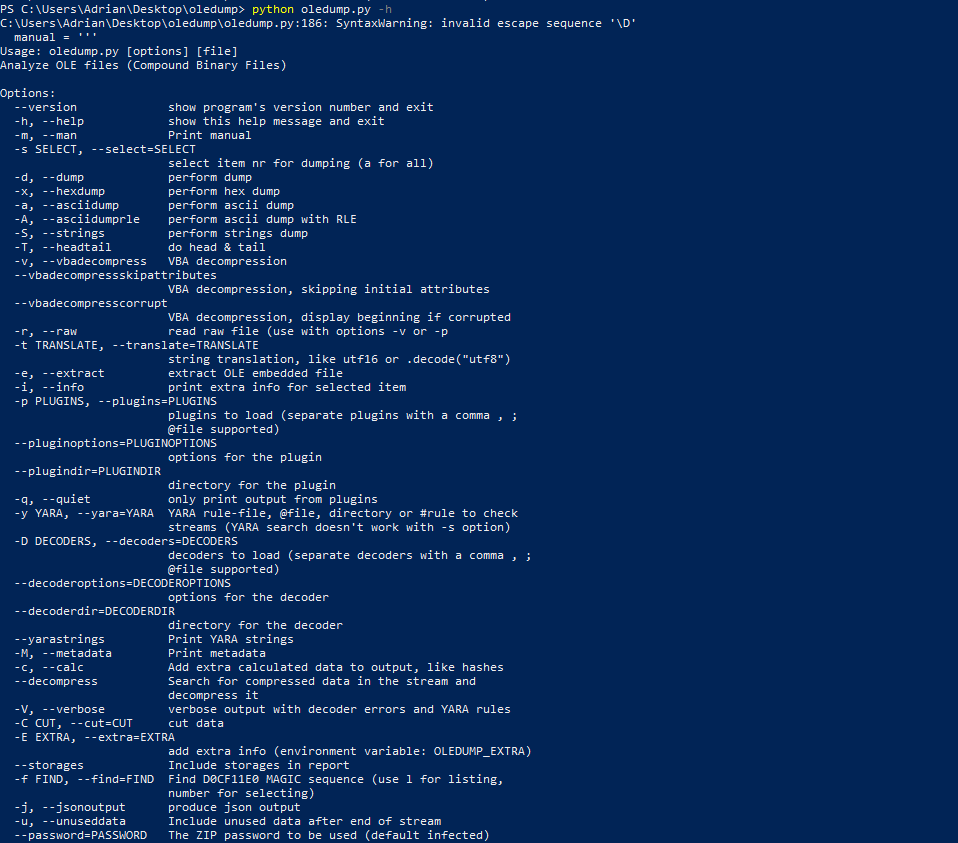
**Verificat:** Catanoi Maxim

**Chișinău 2024**

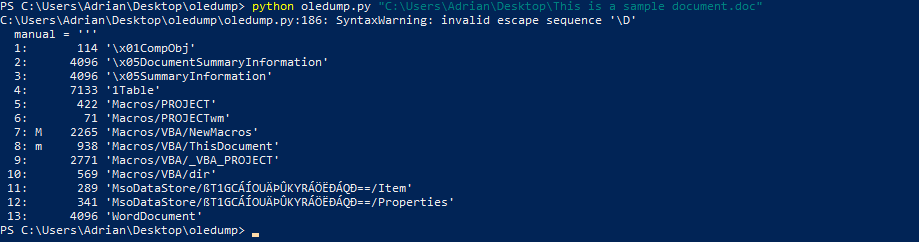
**Etapele de îndeplinire a laboratorului:**

* **Document 1**

Inițial am folosit biblioteca oledump.py pentru a putea găsi macro-urile din documentele word, mai jos este meniul help al acestei biblioteci.

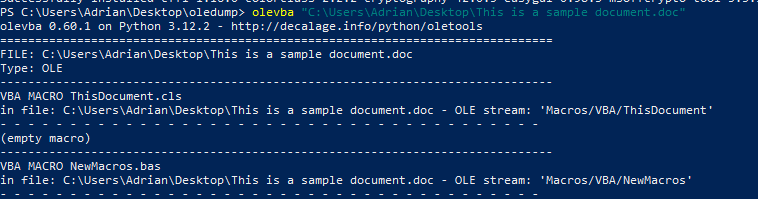


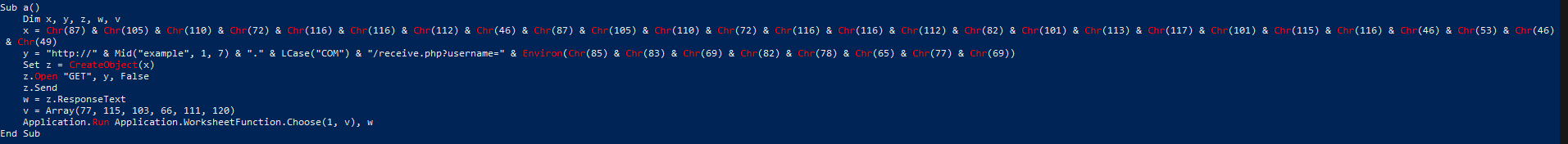
Scanarea primului document, cu ajutorul acestei biblioteci am găsit că conține macrouri pe care le-am selectat pentru vizualizare, dar nu am obținut un cod citibil de om, după care am găsit biblioteca olevba pe care am folosit-o mai departe.



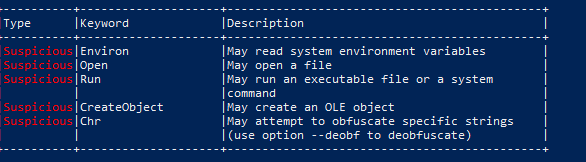
Cu ajutorul bibliotecii olevba am primit imediat după scanarea documentului mai multe detalii despre el.

Vedem denumirea NewMacros, pe care am găsit-o și cu ajutorul oledump, dar aici am primit și un cod în VBA.

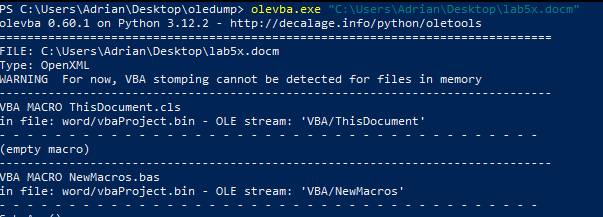


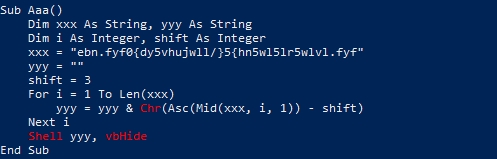
Aici avem subrutina a care este un macro.

* Inițial sunt create 2 șiruri:
  + - Primul șir creează un string care e format din concatenarea mai multor caracter din **ASCII**, iar la final se obitne **“WinHttp.WinHttpRequest.5.1”**
    - Variabila **y** stochează un URL format dintr-o combinație de șiruri literale și funcții VBA. În acest caz, URL-ul este construit astfel încât să includă o parte statică **("http://example.COM/receive.php?username=")** și un nume de utilizator preluat din variabila de mediu **USERNAME** a sistemului de operare (obținut cu ajutorul funcției **Environ**). Astfel, variabila **y** reprezintă URL-ul final utilizat pentru cererea GET.
  + Variabila **z** creează un obiect cu ajutorul variabilei **x** care conține un șir specific **HTTP** de tip **GET** către URL-ul stocat în variabila **y**, iar codul asteaptă răspuns de la server pentru a continua.
  + Variabila **w** primește răspunsul de la server și îl stochează.
  + Variabila **v** este un vector care stochează indexuri pentru a apela valori specifice în cadrul aplicației.
* **Application.Run** apelează indexul 1 din vectorul **v** în funcție de răspunsul primit de la variabila **w**



* **Document 2**





Subrutina Aaa este un ciclu pentru criptarea unui șir cu un anumit număr de peremutări, aici fiind 3, astfel stringul inițial xxx, fiecare caracter va fi convertit în codul său ASCII după care va fi modificat cu elementul din spatele său cu 3 poziții, vbHide probabil este folosit pentru a ascunde fereastra Shell de utilizator, shell-ul fiind apelat de această subrutină iar primește argument variabila yyy.

Am scris codul în java, astfel putem observa cum șirul inițial este afectat de către aceste peremutări și cum cum este transformat. Acesta fiind un algoritm simplu care este transcris din VBA.

**Concluzie**

În cadrul laboratorului de Tehnici de Inginerie Inversă, am explorat procesul de analiză a macro-urilor în documentele Word utilizând biblioteci precum oledump.py și olevba. Prin intermediul acestor instrumente, am identificat și inspectat macro-uri, obținând detalii precum codul VBA asociat. Am evidențiat o subrutină specifică (Aaa) care efectuează criptarea unui șir prin permutări și apelarea unui shell, evidențiind astfel tehnici de ascundere și manipulare a codului.