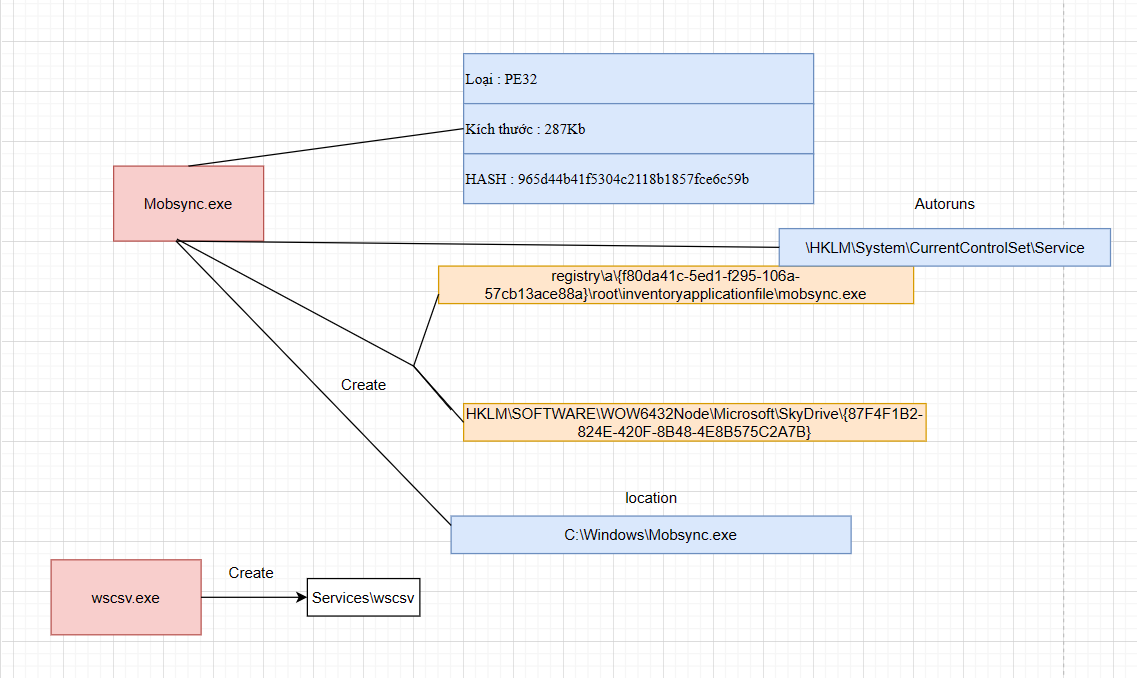
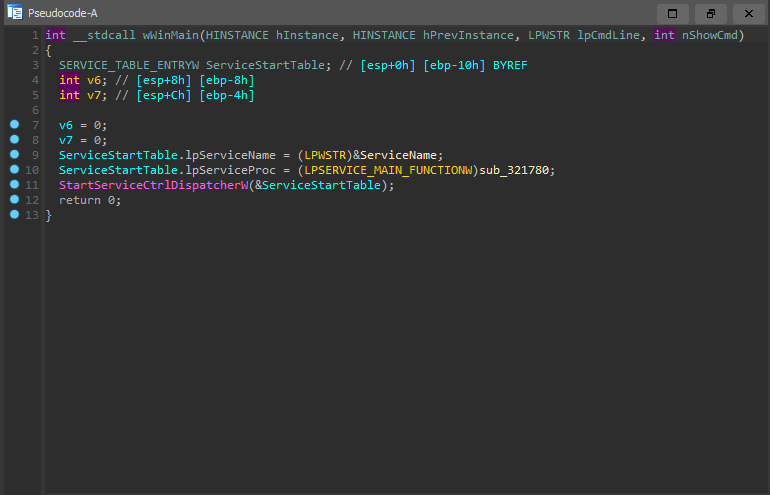
I Thông tin cơ bản



II. Khả năng Persistent

Phân tích mẫu wscsv.exe chúng ta thấy nó createService trong hệ thống để có thể persistent và call tới hàm sub\_321780

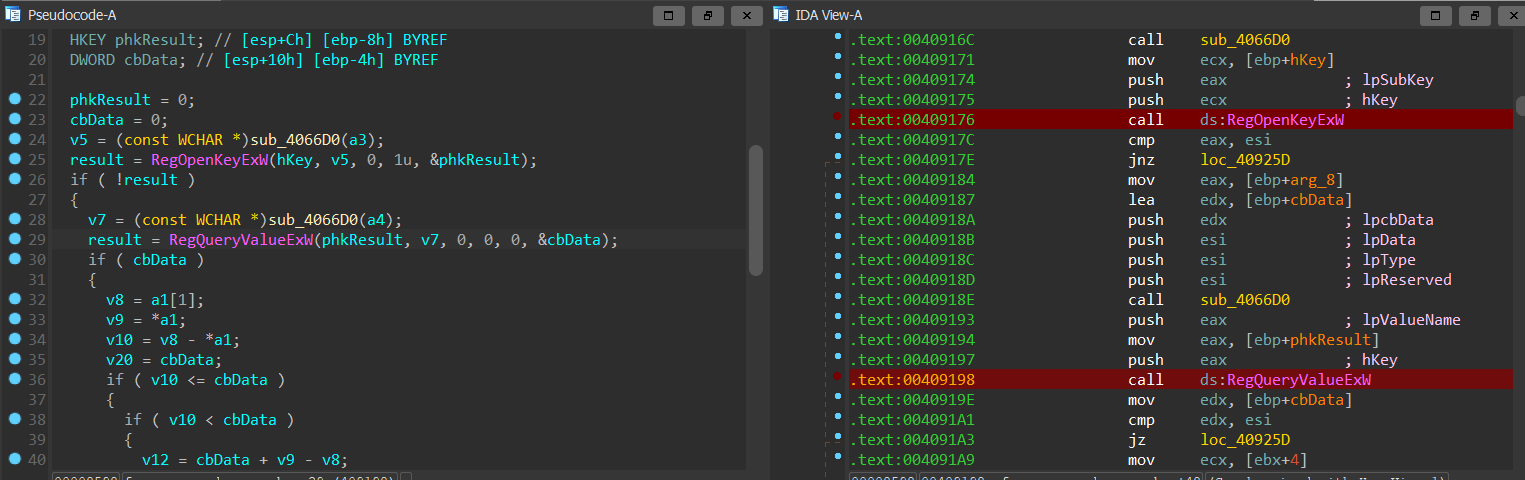


Khi đi sâu vào hàm sub\_321780 nó làm rất nhiều việc đến setup service và trong đó có 1 đoạn code khá là đáng chú ý . Nó sẽ CreateProcess là mẫu Mobsync.exe và run mẫu đó



III. Phân tích chi tiết

Chúng ta sẽ tập trung phân tích những chức năng quan trọng của mẫu mobsync.exe và lược bỏ những đoạn không cần thiết . Mẫu sẽ không connect trực tiếp tới C&C mà mã hóa thông qua registry rồi mới connect



Chúng ta có thể thấy ở đây nó tạo key:

HKLM\SOFTWARE\WOW6432Node\Microsoft\SkyDrive\{87F4F1B2-824E-420F-8B48-4E8B575C2A7B}

Nó còn open đến rất nhiều key như :

Path

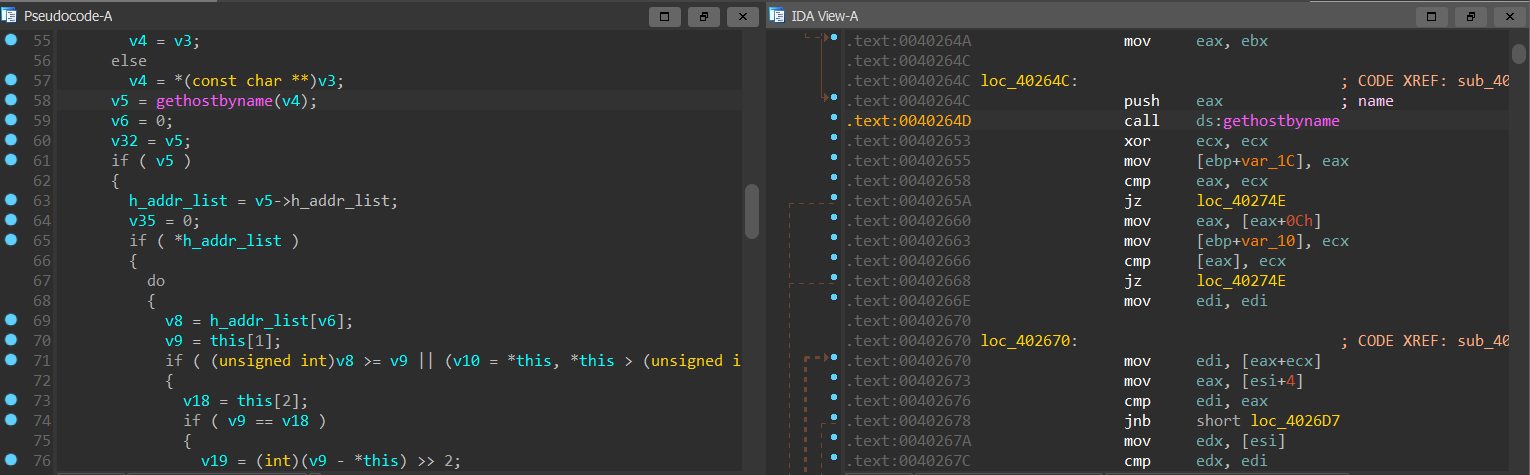
HKLM\System\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-1866265027-1870850910-1579135973-1000

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap

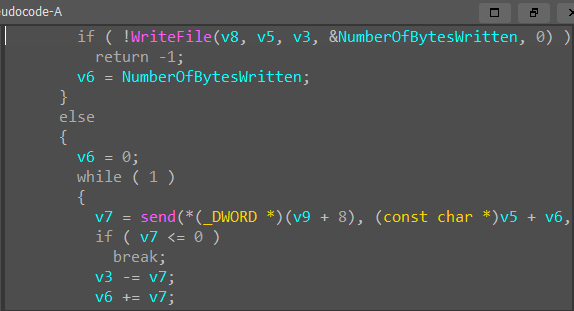
HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap

HKCU\SOFTWARE\Microsoft\SkyDrive\{87F4F1B2-824E-420F-8B48-4E8B575C2A7B}

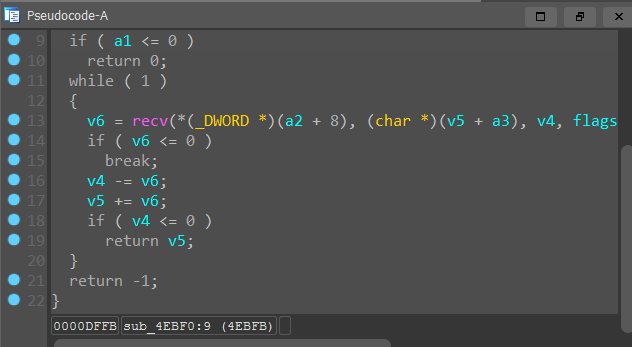
Vì số lượng key open là rất lớn nên chúng ta lấy những key đặc trưng



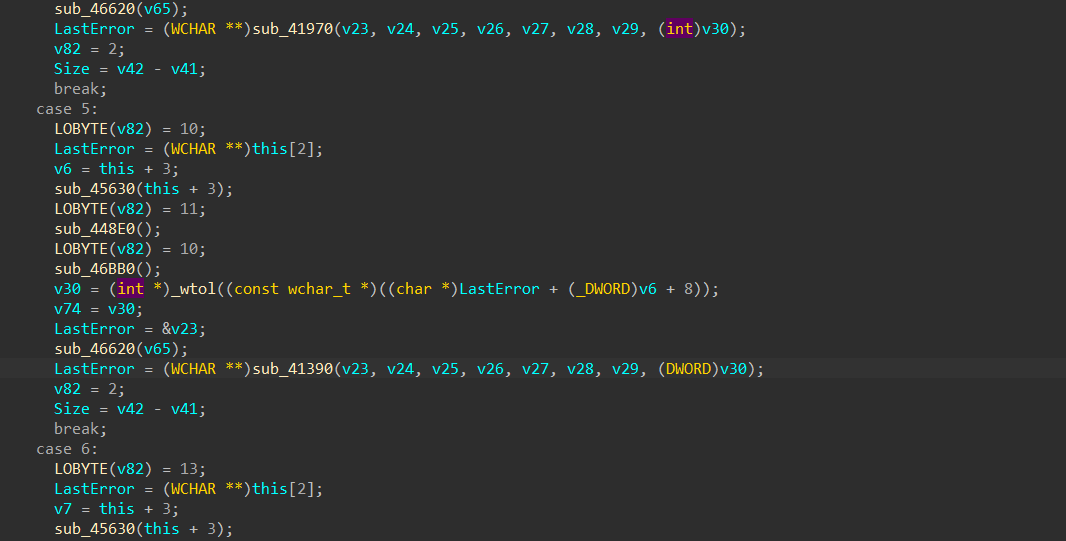
Chúng ta có thể thấy nó call gethostbyname



Chúng ta có thể thấy nó writefile và send đi



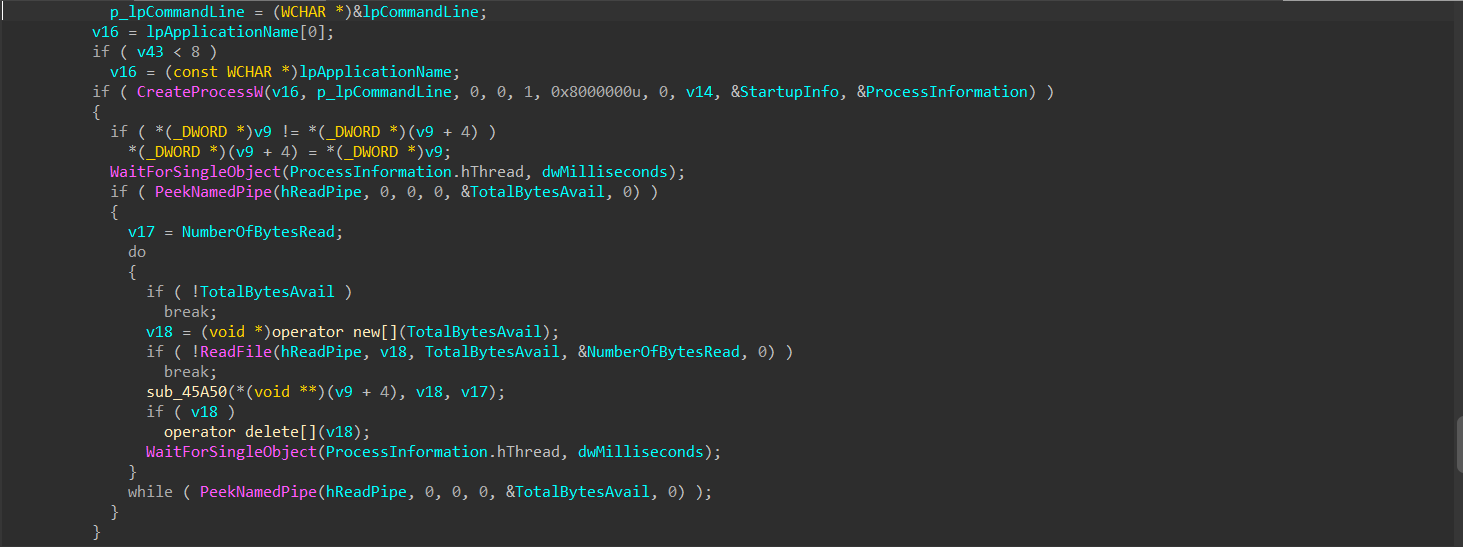
Nó nhận tín hiệu từ C&C và thực thi ứng với tín hiệu recv



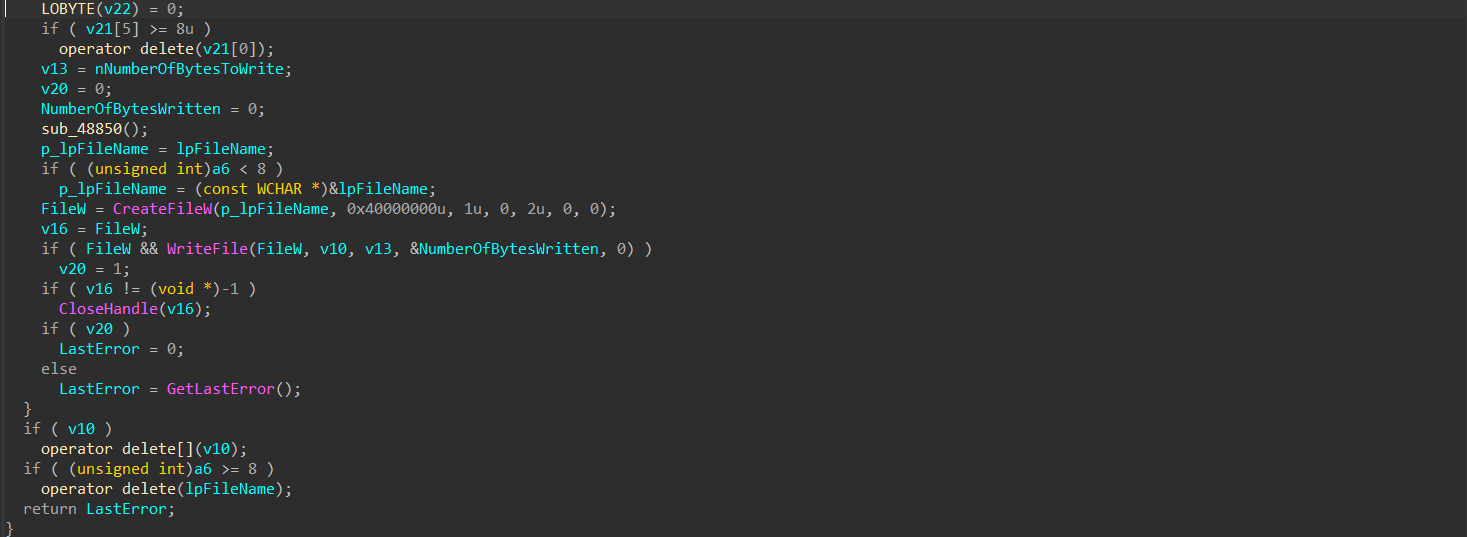
ứng với các option sẽ có những mục mà những mã độc có sử dụng RAT hay làm



Option này là copy file

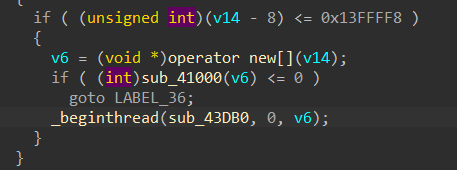


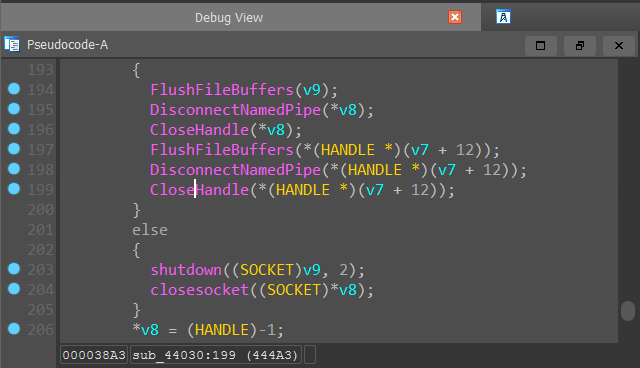
Option này là remote command



Optione này là writefile

Những optine này được thực hiện thông qua 1 thread





Cuối cùng là close socket

IV.IOC

- Wscsv.exe:

MD5 : de08c8e2e7e3f5956e3727ea3c6260de

- Mobsync.exe:

MD5 : 965d44b41f5304c2118b1857fce6c59b

- C&C:

IP:

-23.32.77.164

-8.241.144.125

-152.195.38.75

-20.198.162.78

alive.innielmes[.]com

route.rnouarrette[.]com