DG’hAck 2023

REVERSE - WRONGSOMEWHERE

50 POINTS

SAM NZONGANI

Reverse - wrongsomewhere

Description

Un nouveau ransomware se propage sur internet.

Trop de vieilles dames se font arnaquer par celui-ci, il est temps d'agir !

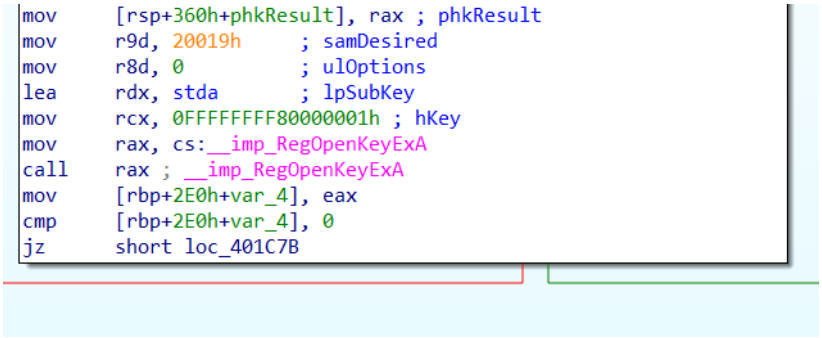
Une des victimes nous a accordé l'accès à distance à sa machine, veuillez enquêter et trouver la clé pour déchiffrer les fichiers.

Solution

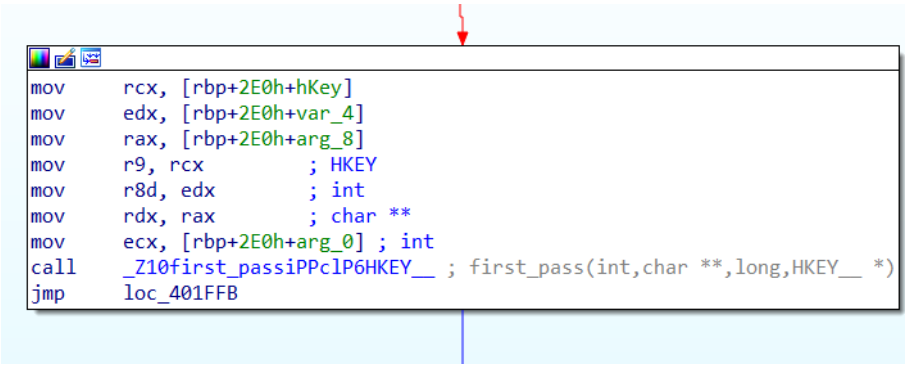
On a accès à une machine victime du ransomware.

Dessus on trouve plusieurs fichiers chiffrés dont un nommé **flag**. On commence par ouvrir l'exécutable avec notre désassembleur préféré (IDA).

La fonction main commence par appeler **RegOpenKeyExA** de l'API Windows.



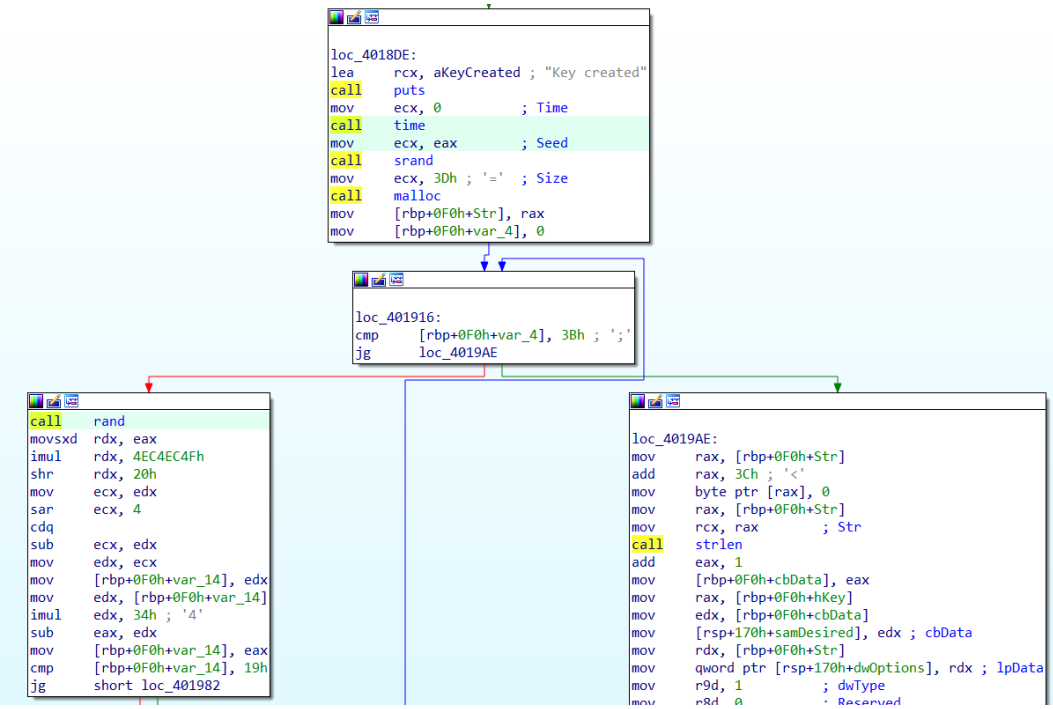
Si elle échoue (valeur de retour non nulle), ce bloc est exécuté:



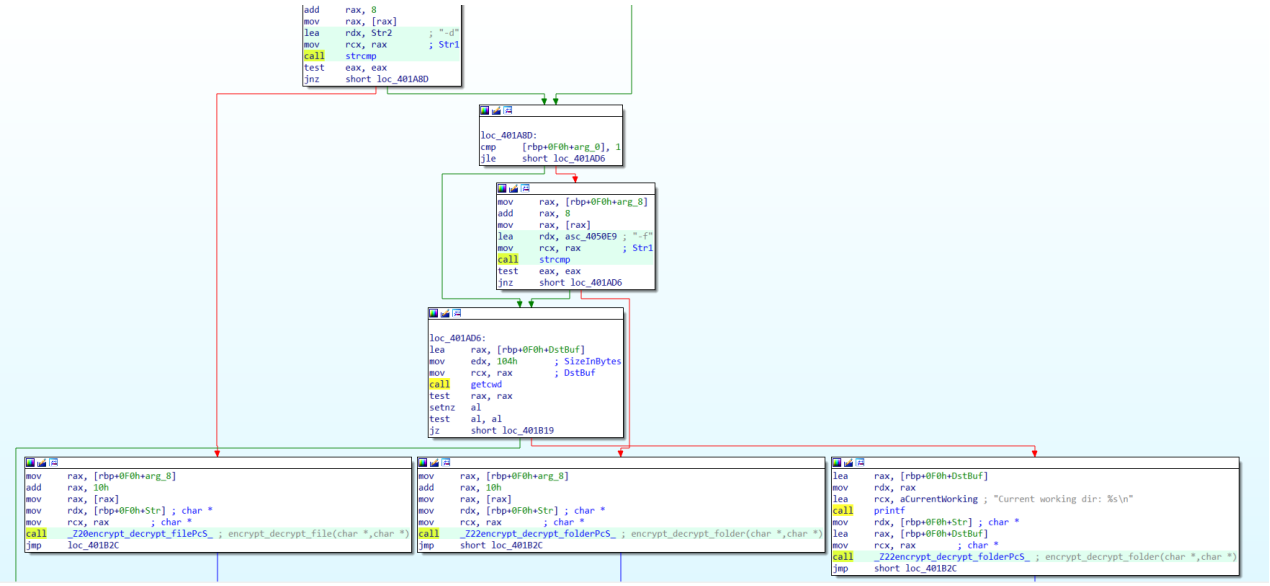
La fonction **first_pass** fait 2 choses:

- elle génère une clé
- elle chiffre les documents du dossier spécifié

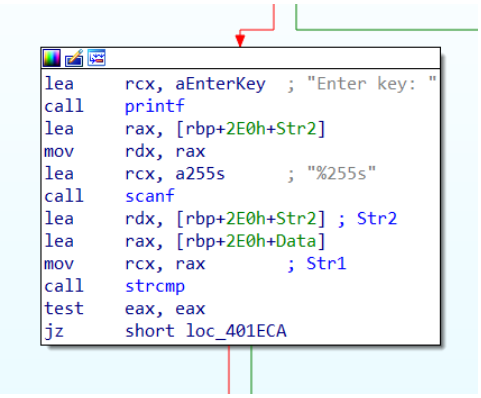
La génération de clé se fait dans une boucle qui utilise des nombres aléatoires avec **rand**. On voit que le seed utilisé est la valeur de retour de la fonction **time**. Elle permet d'obtenir le temps écoulé depuis le premier janvier 1970 à 00:00:00.



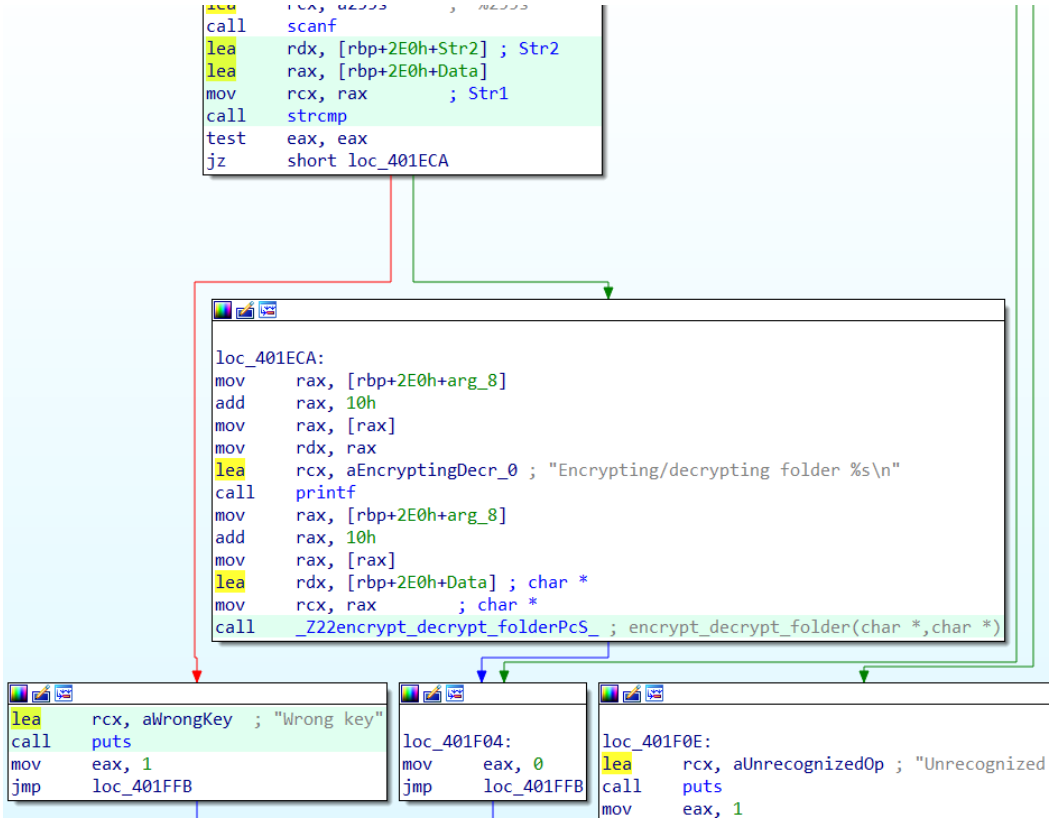
Une fois la clé générée le programme parse des options (-d et -f) avec **strcmp** et appel la fonction **encrypt_decrypt_folder** pour chiffrer/déchiffrer les documents du dossier spécifié.



Si on revient à la fonction **main**, dans le cas où l'appel à **RegOpenKeyExA** réussi le programme parse des options avec **strcmp** comme dans **first_pass** et demande d'entrer la clé.



La valeur donnée est comparée à la véritable clef (générer dans **first_pass** et si elle est correcte le dossier spécifié est chiffré/déchiffré.

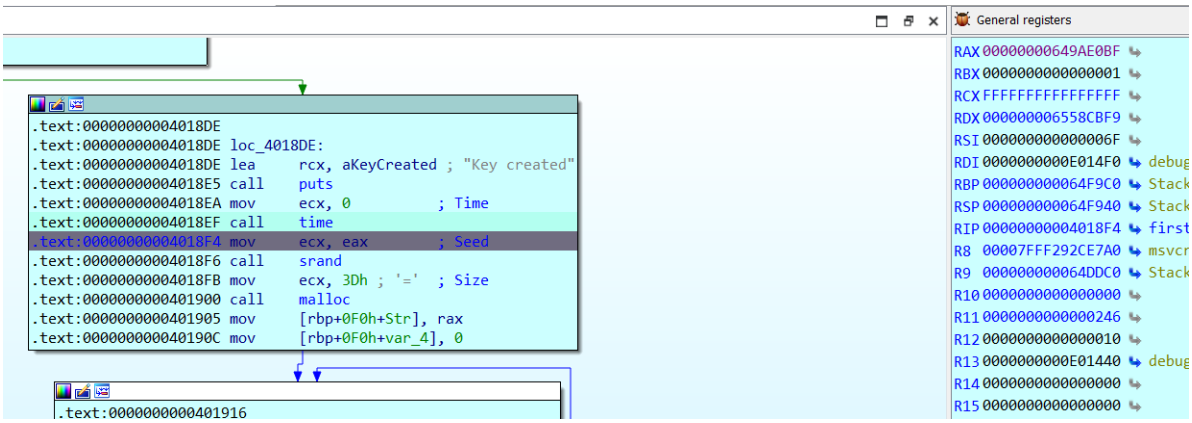


Résumons:

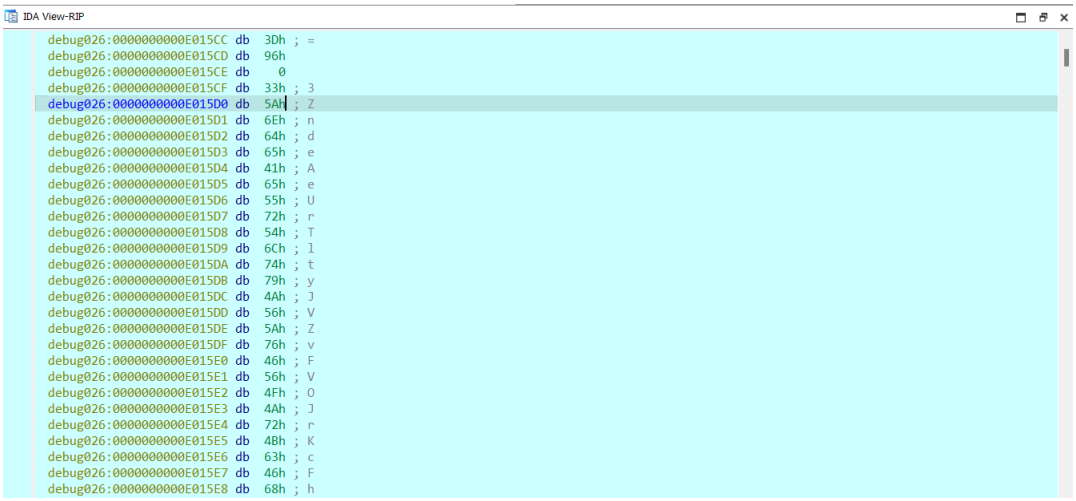
- La première fois que le programme est utilisé **RegOpenKeyExA** échoue, une clé est générée et le dossier est chiffré
- Lors des utilisations suivantes la clé est déjà présente dans le registre Windows, une clé est demandée puis comparée à la vraie clé. Si elle est correcte les documents sont déchiffrés

On a vu que le seed utilisé pour générer la clé est la valeur de retour de **time**. Sur la machine infectée on voit que le fichier **flag** a été modifié (chiffré) pour la dernière fois le 27 juin 2023 à 15:14:39. Sur internet on peut simuler **time** avec cette date et la valeur renvoyée est 1687871679 (0x649AE0BF).

En plaçant un breakpoint après l'appel à **time** on peut modifier la valeur de retour (dans le registre RAX) par 0x649AE0BF.



En mettant un autre breakpoint après la boucle de génération de la clé on peut la voir stockée dans RAX.



Clé: ZndeAeUrTltyJVZvFVOJrKcFhkIhqljzryWPdUQpakaGPjiyBniXvenYwMvU

Il ne reste qu'à exécuter le malware sur la machine infectée avec cette clé !

DGHACK{R4nS0mW4r3s_4r3_4_Cr1m3_D0_n0t_Us3_Th1s_0n3_F0r_3v1l}