le cnam

SEC102 - TP02

Registre UserAssist sur Windows

Date	Version	Description	Auteurs
18/02/2023	1	Retranscription collective des informations présentées en cours	Bartel Cantin Bialas Alexis Dufourt Marvin Faussurier Marc N'Guessan Jérémy

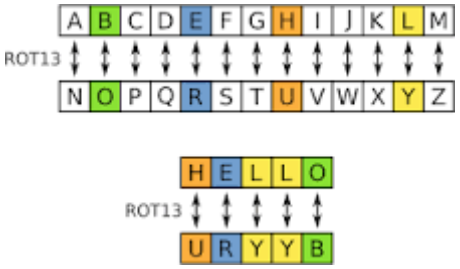
Sommaire :

Contexte

Le registre UserAssist de Windows contient des informations sur les programmes qui ont été exécutés sur un ordinateur. Il est utilisé par Windows pour afficher les raccourcis récemment utilisés dans le menu Démarrer et le menu Exécuter. Les informations stockées dans le registre UserAssist peuvent être utilisées pour comprendre l'activité d'un utilisateur sur l'ordinateur, ce qui peut être utile dans certaines situations. Le registre UserAssist peut être utilisé par des programmes malveillants pour collecter des informations sur l'utilisation du système ou masquer des activités malveillantes. C'est pourquoi, il est important de l'analyser pour trouver des preuves numériques lors d'enquêtes sur des activités suspectes sur un système Windows. Lors de la rédaction de cette étude; le registre UserAssist était encore présent; et encodé en ROT13 sur la dernière version de Windows : 22H2.

Chiffrement

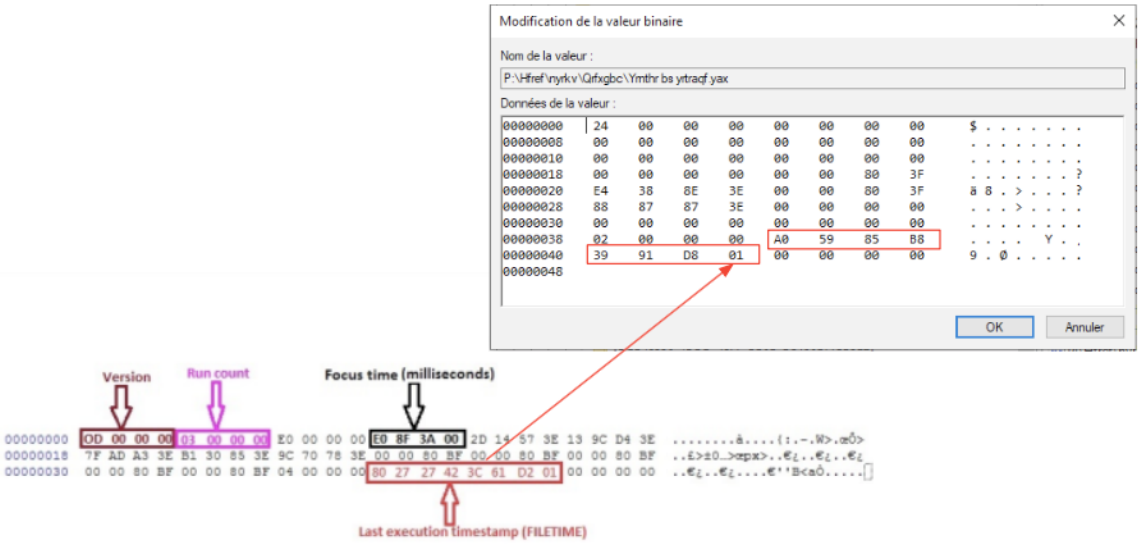
Le chiffrement ROT13 est une technique de chiffrement par substitution qui consiste à décaler chaque lettre de l'alphabet de 13 positions. C’est un dérivé du code césar. Il s'agit d'une méthode de chiffrement simple et souvent utilisée pour cacher des informations. Bien que ce chiffrement soit facile à mettre en œuvre, il est facilement déchiffrable, car le ROT13 est simplement l'inverse de lui-même. Ainsi, si l'on applique une seconde fois le chiffrement ROT13 au texte chiffré, on obtient le texte clair initial. Cette méthode de chiffrement est donc considérée comme une technique de chiffrement faible et ne doit pas être utilisée pour les communications confidentielles. ROT13 est souvent utilisé sur des forums pour cacher des spoilers ou des blagues. Pour réaliser cette étude; un code Python développé pour l’occasion est disponible en annexe.



Fonctionnement de ROT13

Contenu

Le Registre contient des informations auxquelles Windows fait référence en permanence durant son fonctionnement, telles que le profil de chaque utilisateur, les applications installées sur l'ordinateur et les types de documents pouvant être créés, les paramètres de feuille de propriétés pour les dossiers et les icônes d'application, le matériel présent sur le système et les ports utilisés.



Conclusion

En conclusion, le registre UserAssist de Windows est un élément clé pour comprendre l'activité d'un utilisateur sur un système Windows. Cependant, il peut également être utilisé à des fins malveillantes, ce qui en fait un élément important de la recherche de preuves numériques lors d'enquêtes sur des activités suspectes. La raison du chiffrement de ce registre en ROT13 n’est pas clairement établie. Le chiffrement ROT13 est une méthode simple de chiffrement par substitution, mais elle est considérée comme une technique de chiffrement faible et ne doit pas être utilisée pour des communications confidentielles. Bien que facilement déchiffrable, le ROT13 est souvent utilisé pour cacher des spoilers ou des blagues sur les forums. Dans l'ensemble, une compréhension approfondie du registre UserAssist et des techniques de chiffrement est essentielle pour les professionnels de la sécurité informatique et les enquêteurs numériques.

Glossaire

Registre UserAssist : un registre de Windows qui contient des informations sur les programmes qui ont été exécutés sur un ordinateur. Il est utilisé par Windows pour afficher les raccourcis récemment utilisés dans le menu Démarrer et le menu Exécuter.

Chiffrement : la conversion d'un texte en clair en un texte chiffré, qui ne peut être compris que par le destinataire autorisé.

ROT13 : une technique de chiffrement par substitution qui consiste à décaler chaque lettre de l'alphabet de 13 positions. C’est un dérivé du code césar.

Chiffrement par substitution : une méthode de chiffrement qui remplace chaque lettre du texte en clair par une autre lettre, un chiffre ou un symbole.

Code César : une technique de chiffrement par substitution qui consiste à décaler chaque lettre de l'alphabet d'un nombre fixe de positions.

Chiffrement faible : une méthode de chiffrement qui peut être facilement déchiffrée ou cassée avec des méthodes connues.

Communications confidentielles : des communications qui doivent être protégées et ne doivent être accessibles qu'à des personnes autorisées.

Preuves numériques : des éléments de preuve numériques tels que des fichiers de journaux, des enregistrements de données et des métadonnées qui peuvent être utilisés pour prouver l'existence ou l'absence d'activités sur un système informatique.

Activités suspectes : des activités qui sont potentiellement malveillantes ou qui sont en contradiction avec les politiques de sécurité ou les procédures opérationnelles standard.

Annexe

```python
# UNICODE Characters: https://en.wikipedia.org/wiki/List_of_Unicode_characters

# a to z  => 97 to 122
# A to Z  => 65 to 90
# print(ord('a')) // 97
# print(chr(97)) // a

sentence = input('Enter a sentence: ')
key = 13

def encrypt(message, nb):
    result = ''
    for letter in message:
        if letter.islower():
            result += chr(((ord(letter) + nb -97) % 26) + 97)
        elif letter.isupper():
            result += chr(((ord(letter) + nb - 65) % 26) + 65)
        else:
            result += letter
    return result

def decrypt(message, nb):
    return encrypt(message, (nb * -1))

encrypted_sentence = encrypt(sentence, key)
print(encrypted_sentence )

decrypted_sentence = decrypt(encrypted_sentence, key)
print(decrypted_sentence)
```