LA STENOGRAPHIE

Matthieu IZAC – BTS SIO1 – 2022/2023

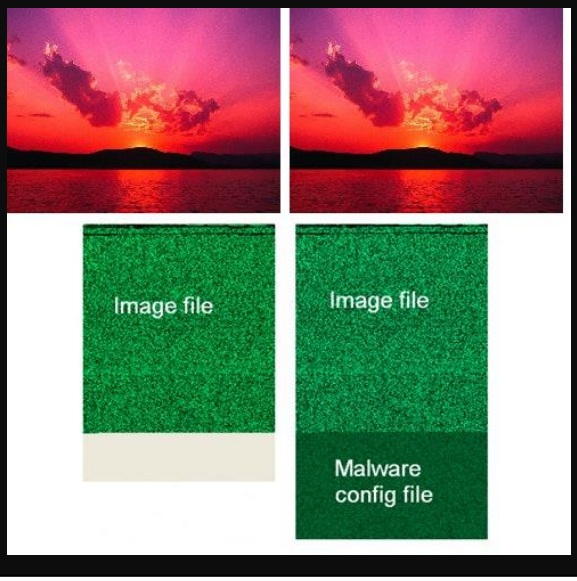
SOMMAIRE

Qu'est-ce qu'est la sténographie ?

Le mot sténographie a été utilisé pour la première fois en 1499 par le cryptographe allemand Johannes Trithemus, ce mot vient en fait du grec ancien, en associant les mots *steganos* (caché, protégé, couvert) et *graphein* (écrire). La sténographie est une forme de dissimulation d'information qui a pour but de transmettre un ou des message(s) de manière inaperçue au sein d'un autre message. L'information utile est cachée au premier abord, mais non protégée pour celui qui sait où regarder. On peut opposer la sténographie a la cryptographie qui lui dissimule un message et qui ne le rend pas visible pour toute personne n'ayant pas la clé tandis que la sténographie quant à elle peut révéler son message a tout le monde tant que l'on sait comment et où le trouver, cependant on peut combiner sténographie et cryptographie pour plus de sécurité.

Quelle est l'utilité de la sténographie ?

La sténographie peut être utilisée pour dissimuler quasiment tout type de contenu numérique comme par exemple du texte des images des vidéos ou encore du contenu audio ces contenus peuvent etre cachés de la même manière dans tout type de contenu numérique. La sténographie peut être utilisé par les pirates car en effet, il peut utiliser un contenu qui a l'air totalement inoffensif pour l'utiliser comme une sorte de protection sur sa victime et dissimulé dedans des codes malveillants amenant des malwares sur la machine de la victime.



Exemple d'utilisation de la sténographie pour dissimuler un malware

src :https://www.nomios.fr/actualite/steganographie/#:~:text=La%20st%C3%A9ganographie%20est%20une%20forme,pour%20qui%20sait%20o%C3%B9%20regarder.

Mais la sténographie ne sert pas qu'à dissimuler des malwares il peut comme dit précédemment se contenter de cacher des textes dans une image. Exemple avec l'utilisation de QuickStego. :

Texte dissimuler trouver grace a l'application QuickStego

Comment fonctionne la sténographie ?

Les fichiers media numériques se constituent en fait d'un ensemble de données extrêmement complexes ce que l'on voit est différent de ce que notre ordinateur lui voit.

Ce que l'on voit :

Ce que l'ordinateur voit :

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   42 4D 3C 00 00 00 00 00 00 00 36 00 00 00 28 00   BM<.......6...(.
00000010   00 00 01 00 00 00 01 00 00 00 01 00 18 00 00 00   ................
00000020   00 00 06 00 00 00 12 0B 00 00 12 0B 00 00 00 00   ................
00000030   00 00 00 00 00 00 AC 8C 6F 59 00 00               ......¬Œoy..
```

Ce qui se trouve au-dessus c'est le code machine en hexadécimal qui représente seulement un pixel de la photo encore au-dessus. Cet élément représente R-111 G-140 B-172 qui est la couleur du pixel si on change la valeur de celui-ci par R-112 G-141 B-173 on verra cela :

A l'œil nu aucun changement mais la machine quant a elle verra ca :

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   42 4D 3C 00 00 00 00 00 00 00 36 00 00 00 28 00   BM<.......6...(.
00000010   00 00 01 00 00 00 01 00 00 00 01 00 18 00 00 00   ................
00000020   00 00 06 00 00 00 12 0B 00 00 12 0B 00 00 00 00   ................
00000030   00 00 00 00 00 00 AC 8C 6F 0E 00 00               ......¬Œo...
```

La modification d'un seul pixel fait apparaitre ce qui semble être la même image cependant le code machine responsable de la production de l'image est bel et bien différent. C'est comme ça que les utilisateurs malveillants dissimule des codes malveillants sans éveiller aucun soupçon.

Conclusion

En somme, la sténographie nous montre que c'est que lorsque des fichiers ou des contenus numériques semblent amicaux ou même inoffensifs c'est que c'est souvent l'inverse qui se produit. Il faut être méfiant et ne pas télécharger n'importe quoi car la moindre erreur suffit à un pirate pour installer un logiciel malveillant.