Virus RSA-4096

Un point sur deux familles de ransomwares qui peuvent prétexter confusion, en effet, ces deux familles utilisent les mêmes messages d'instructions.
Il s'agit de :

- TeslaCrypt
- CryptXXX – une nouvelle famille apparue il y a quelques jours.

Tous les deux ont leur messages d'instructions qui débutent par :
All of your files were protected by a strong encryption with RSA-4096

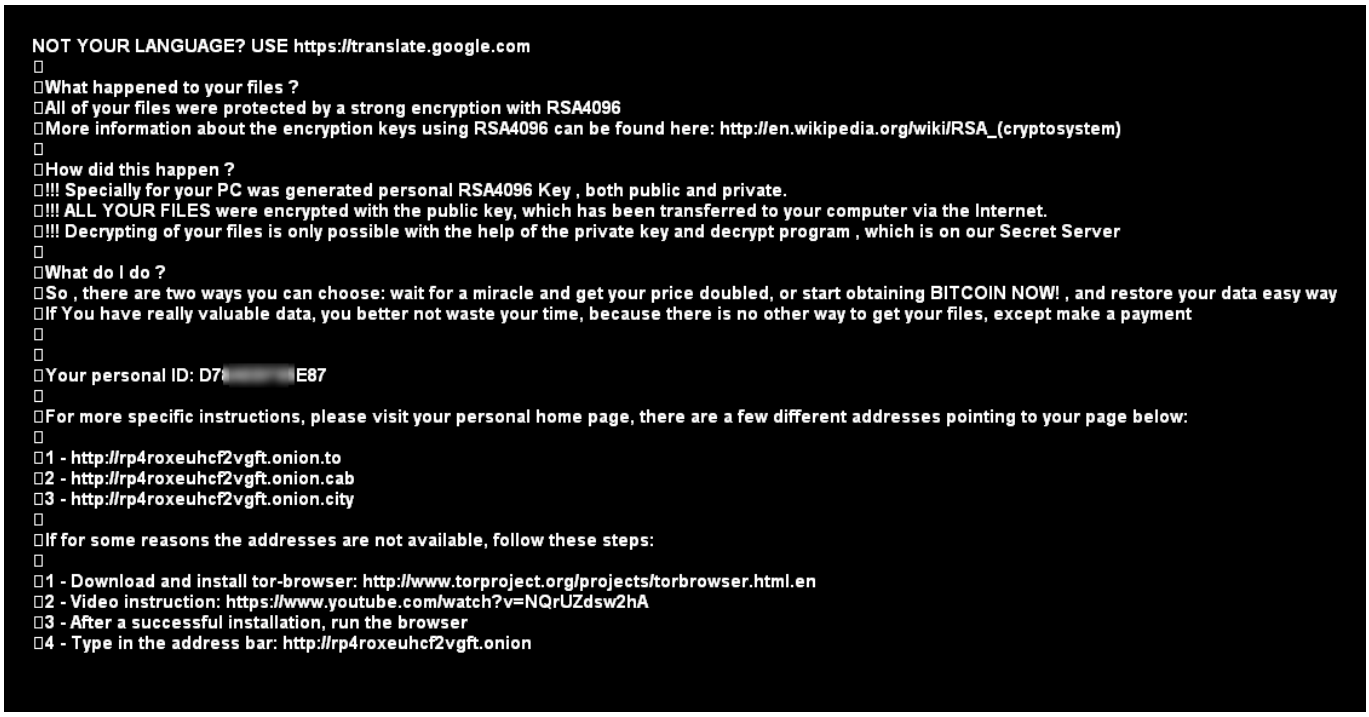
Il y a tout de même des différences entres les deux familles.
TeslaCrypt utilise des noms de fichiers d'instructions qui changent régulièrement et contenu des lettres aléatoires, ex : {RecOveR}-xxxx, RECOVERxxxx

Les versions HTML sont identiques, par contre les versions textes et images comportent pour TeslaCrypt, des lettres aléatoires, comme le montre la capture d'écran ci-dessous :

côté virus RSA-4096 CryptXXX, les noms des fichiers instructions sont :

de_crypt_readme.bmp
de_crypt_readme.txt
de_crypt_readme.html

Je ne sais pas encore s'ils vont changer régulièrement, cette famille étant nouvelles.
On obtient ceci qui semble être le fichier instructions des premières vagues TeslaCrypt



et en version 2.0, plus facile à identifier avec des couleurs :

La réutilisation de fichiers d’instructions ou extensions peut semer la confusion chez les internautes qui pensent avoir affaire à tel ou tel ransomware et qui vont donc pas forcément suivre les bonnes procédures.

Les subtilités des différences étant difficiles à voir si on est pas dans le « bain » des ransomwares.

Un résumé rapide de ces familles.

TeslaCrypt – RSA-4096

Je ne vais pas m'étendre, tout a été à peu près dit sur la page lors du pic de la campagne :

- how_recover/help_recover_instructions : TeslaCrypt extension .micro et .mp3
- Récupération/Décrypter fichiers .vvv (ransomware TeslaCrypt)

Seules les variantes .vvv et antérieures peuvent voir les fichiers récupérés par factorisation.
Les variantes futures (après février 2016), .mp3, .micro et actuellement .jpg ont corrigé ce problème, les fichiers ne peuvent être récupérés par ces attaques.

Côté technique, TeslaCrypt RSA-4096 se charge par une clef Run qui lance un .exe qui se trouve en général dans le dossier Documents.
Exemple :

```
HKU\S-1-5-21-2568215945-4132293836-1244343729-1000\...\Run: [hostslertmutxtk] => C:\Windows\SYSTEM32\CMD.EXE /C START "" "C:\Users\VincentPC\Documents\fsudgkjcqavn.exe"
```

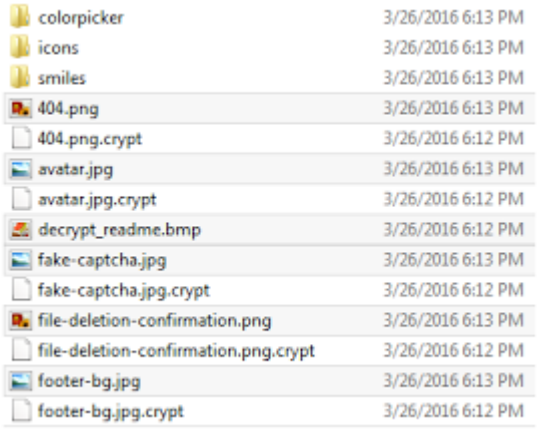
Les FAQ de suppression TeslaCrypt :

- Supprimer TeslaCrypt (supprimer-trojan)
- Supprimer TeslaCrypt (supprimer-virus.com)

TeslaCrypt en vidéo :

CryptXXX – .crypz – Virus RSA-4096

Il s'agit donc d'une nouvelle variante.
D'après les analyses effectuées, le groupe derrière ce ransomware est le groupe Reveton, un ransomware « virus gendarmerie » très actif de 2013 à 2015.
Les fichiers touchés par ce ransomware RSA 4096 voit leurs extensions modifiées en .crypz



CryptXXX en vidéo :

Enfin tout comme le malware Reveton par le passé, cette variante RSA 4096 charge une DLL via rundll32.exe et créé une clef Run pour lancer celle-ci au démarrage de la session Windows.
La suppression de la clef et de la DLL rend ce rançongiciel inactif.

J'imagine que les futures variantes de CryptXXX vont voir leur propre message d'instructions.
Côté récupération des documents .crypt – à priori, pour le moment, il n'y a pas de solution connue pour récupérer les documents de ce virus RSA-4096.

Les FAQ de suppression CryptXXX (Ransomware RSA 4096) :

- Supprimer le ransomware rsa-4096 – extension .crypt (supprimer-trojan.com)

- Supprimer Virus RSA 4096 (supprimer-virus.com)

Ce Malware RSA 4096 embarque des fonctionnalités de vol de mot de passe, en cas d'infection, pensez à changer vos mots de passe après désinfection.

Conclusion

Les ransomwares continuent leurs progressions, chaque groupe de cybercriminels sort sa famille, tout comme en 2012/2013 on pouvait voir apparaître régulièrement de nouveaux « virus gendarmerie » et encore avant cela, le même phénomène pour les rogues/scarewares.
On notera aussi les copycat, généralement attribué à des groupes moins professionnel, dernièrement AutLocky, un ransomware écrit en langage Autoit qui tente de se faire passer pour le fameux ransomware Locky.

Côté sécurité, lire le sujet Sécuriser Windows et pensez à effectuer des sauvegardes des documents importants.