

Satana, un ransomware pire que Petya



Le nouveau rançomware Satana cumule chiffrement des fichiers et remplacement du secteur d'amorçage du disque.

```
You had bad luck. There was encrypting of all your files in a FS bootkit virus
<!SATANA!>
To decrypt you need send on this E-mail: banetnata@mail.com
your private code: 7Ea61278DFBAD65AE31E707FFE019711 and pay on
a Bitcoin Wallet: XsrR2he2Z20un5ysGWhJ1uweZRP96XEoX total 0,5 btc
After that during 1 - 2 days the software will be sent to you - decryptor -
and the necessary instructions. All changes in hardware configurations of
your computer can make the decryption of your files absolutely impossible!
Decryption of your files is possible only on your PC!
Recovery is possible during 7 days, after which the program - decryptor -
can not ask for the necessary signature from a public certificate server.
Please contact via e-mail, which you can find as yet in the form of a text
document in a folder with encrypted files, as well as in the name of all
encrypted files. If you do not appreciate your files we recommend you format
all your disks and reinstall the system. Read carefully this warning as it is
no longer able to see at startup of the computer. We remind once again- it is
all serious! Do not touch the configuration of your computer!
E-mail: banetnata@mail.com - this is our mail
CODE: 7Ea61278DFBAD65AE31E707FFE019711 this is code; you must send
BTC: XsrR2he2Z20un5ysGWhJ1uweZRP96XEoX here need to pay 0,5 bitcoins
How to pay on the Bitcoin wallet you can easily find on the Internet.
Enter your unlock code, obtained by E-mail here and press "ENTER" to
continue the normal download on your computer. Good luck! May God help you!
<!SATANA!>
```

Une nouvelle génération de ransomware est en train d'émerger. Satana, nom du nouveau malware, combine chiffrement des fichiers et écriture de code sur le secteur d'amorçage du disque, le MBR. Deux techniques inspirées de Petya et Mischa, note Malewarebytes qui constate la croissance du nouvel agent satanique ces dernières semaines.

« *Satana fonctionne en deux modes*, note la société de sécurité sur son blog. *Le premier se comporte comme Petya, un fichier exécutable (sous Windows, NDLR) [et] écrit au début du disque infecté un module de bas niveau, un bootloader avec un noyau personnalisé. Le deuxième mode se comporte comme un ransomware typique et chiffre les fichiers un par un (tout comme Mischa).* » Mais à la différence que les deux modes ne sont pas exploités alternativement mais bien appliqués ensemble, l'un après l'autre, pour s'attaquer à leurs victimes.

Payer ne garantit rien chez Satana

Malwarebytes ne le précise pas mais le mode de propagation de Satana reste probablement classique. A savoir par e-mail (et éventuellement d'un expéditeur en recherche de travail avec des liens vers les fichiers infectieux comme dans le cas de la première version de Petya). Une fois le MBR remplacé, le malware s'attaque au chiffrement des fichiers du disque (et des éventuels volumes reliés à l'ordinateur) et attend patiemment que le système soit redémarré. Quand c'est le cas, un message s'affiche sur l'écran expliquant la démarche à suivre pour récupérer l'accès à son PC, à savoir le paiement d'une rançon de 0,5 bitcoin (plus de 300 euros au cours du jour).

Si l'utilisateur parvient néanmoins à remplacer le MBR par un fichier d'amorçage sain (une manipulation manuelle qui est loin d'être à la portée de tout le monde), il se heurtera aux fichiers chiffrés sur le disque. Lesquels ont été renommés avec, en en-tête du nom, un e-mail aléatoirement choisi parmi ceux de l'équipe des développeurs de Satana, selon l'expert en sécurité (Gricakova@techmail.com, dans l'exemple présenté). Et les méthodes de chiffrement semblent suffisamment avancées pour rendre les fichiers piégés définitivement irrécupérables. D'autant que Malewarebytes pointe un bug pour le moins problématique pour la victime. De par le mécanisme de chiffrement/déchiffrement des fichiers, en cas de déconnexion au serveur de commandes et contrôle (C&C), la clé de décryptage (qui est la même que pour le cryptage) est perdue. Brisant tout espoir de la victime à pouvoir récupérer ses données (sauf à avoir fait préalablement des sauvegardes). « *Même les victimes qui paient peuvent ne pas récupérer leurs fichiers si elles (ou le C&C) sont hors ligne lorsque le chiffrement arrive* », prévient la société de sécurité.

Du code en cours de perfectionnement

Ce n'est pas la seule bizarrerie que remarque le chercheur Hasherezade, auteur du billet. Il constate également que, le ransomware affiche toute la procédure de son déploiement, y compris la progression du chiffrement des fichiers. « *Habituellement les auteurs de logiciels malveillants ne veulent pas laisser le code de débogage dans leur produit final* », écrit le chercheur. Lequel conclut que Satana est probablement encore en cours de développement et contient des failles. « *Le code d'attaque de bas niveau semble inachevée - mais les auteurs montrent un intérêt dans le développement du produit dans ce sens et nous pouvons nous attendre que la prochaine version sera améliorée.* » Une nouvelle génération de rançongiciel est bien en marche.

Article original de Christophe Lagane



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique;
- Formations et conférences en cybercriminalité;
- Formation de C.I.L. (Correspondants Informatique et Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Satana, un ransomware pire que Petya