Synthèse

Une tendance émergeante a été observée dans le paysage cybercriminel au cours de l'année passée : la mise à disposition de plateformes de location de rançongiciel[1]. Connue sous le nom de *Ransomware as a Service* ou « RaaS », cette pratique se développe à grande vitesse.

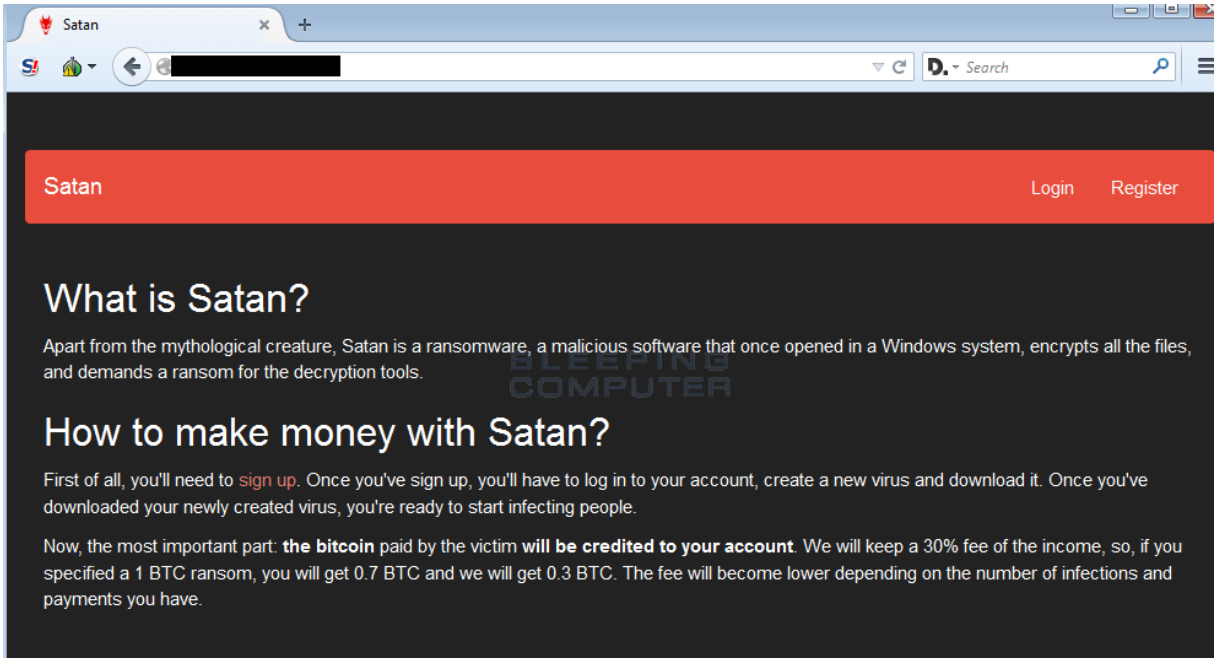
Une tendance toutefois bousculée par un phénomène nouveau : la gratuité et la collaboration autour de ces outils. La découverte de plusieurs sites sur le darknet distribuant des rançongiciels gratuits, les gains étant partagé entre l'utilisateur et les créateurs du logiciel malveillant, semble peser en faveur d'un changement de paradigme. Plusieurs cas similaires ont été reportés sur des forums spécialisés sur le *clearnet*[2].

École traditionnelle

Le RaaS, depuis plus d'une année, était initialement proposé sous une forme « traditionnelle », location du ransomware pour une modique somme (comparée aux hypothétiques bénéfices) payée en cryptomonnaies[3]. L'utilisateur s'occupe alors de la distribution du malware, il peut suivre l'évolution de ses activités sur un tableau de bord et via un accès aux serveurs de commande & contrôle (C2). L'utilisateur ayant loué ce « service » récupère l'ensemble des sommes extorquées.

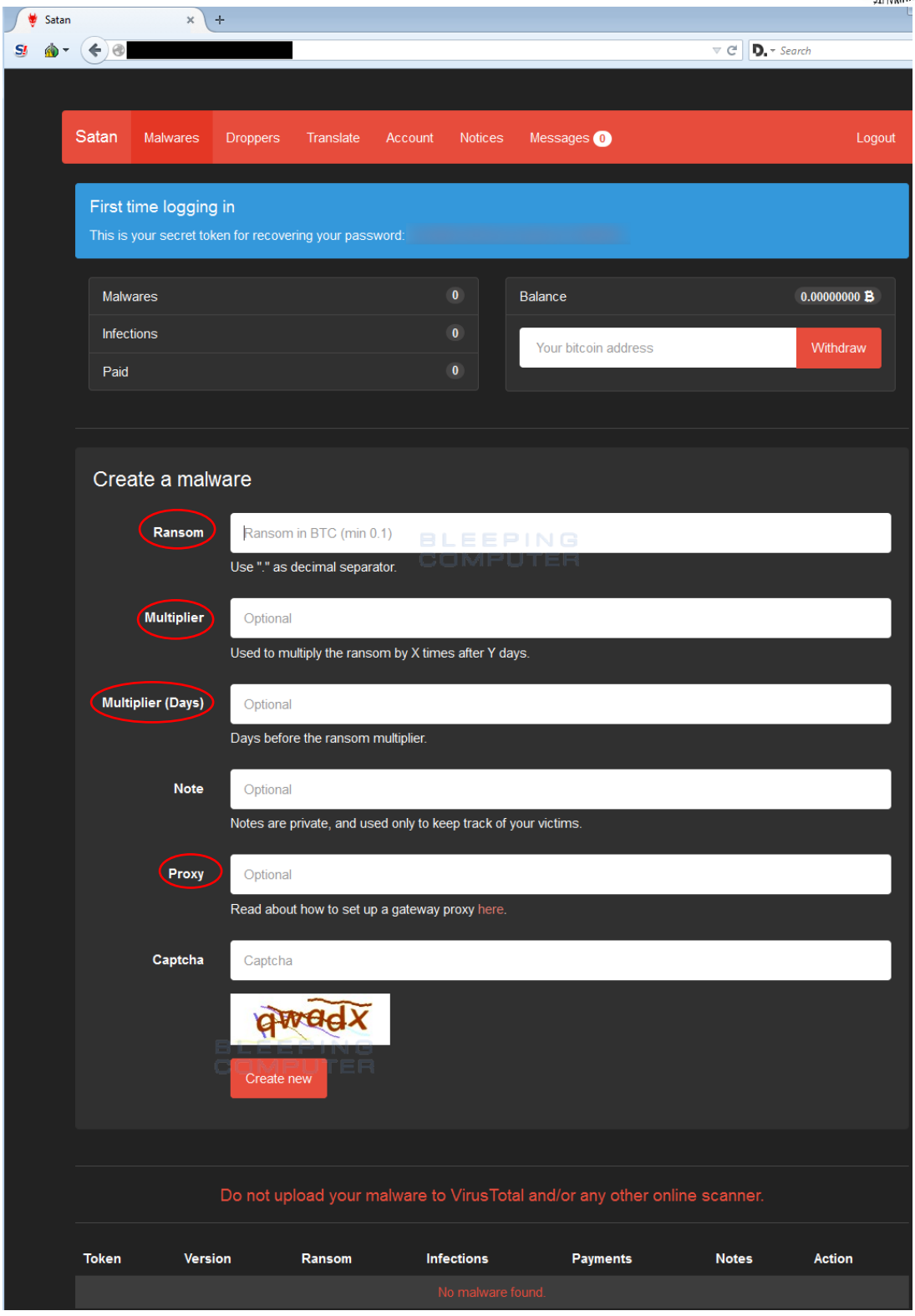
Plusieurs cas ont été recensés sur le darknet tor à ce jour :

Satan (hors-ligne)



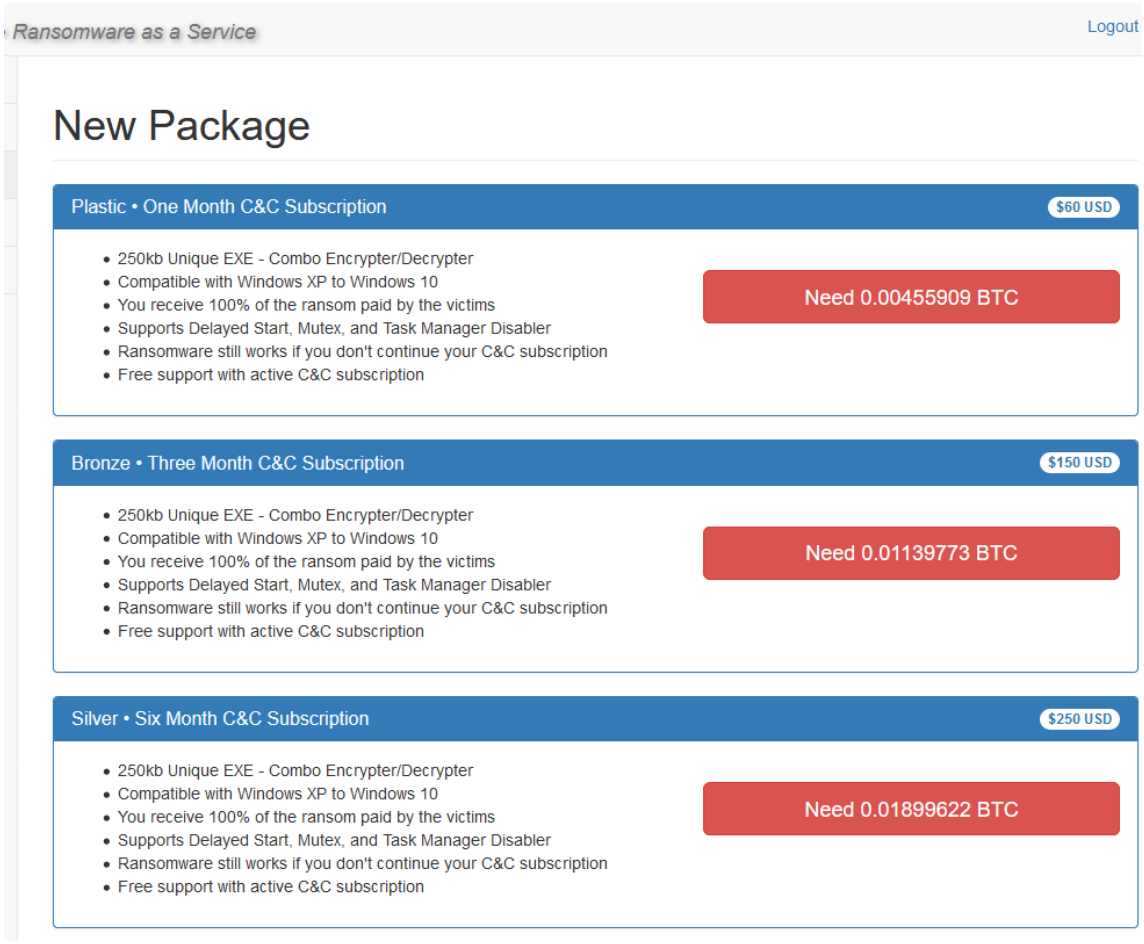
Capture d'écran de la page d'accueil de Satan

[1] Logiciel informatique malveillant, prenant en otage les données et demandant une rançon en échange.
[2] Le web traditionnel, référencé, auquel on accède avec les outils classiques (Chrome, Mozilla, etc.). En opposition avec les darknets.
[3] Bitcoin très majoritairement



Page de configuration du rançongiciel **SATAN**, il est possible de configurer précisément certains éléments

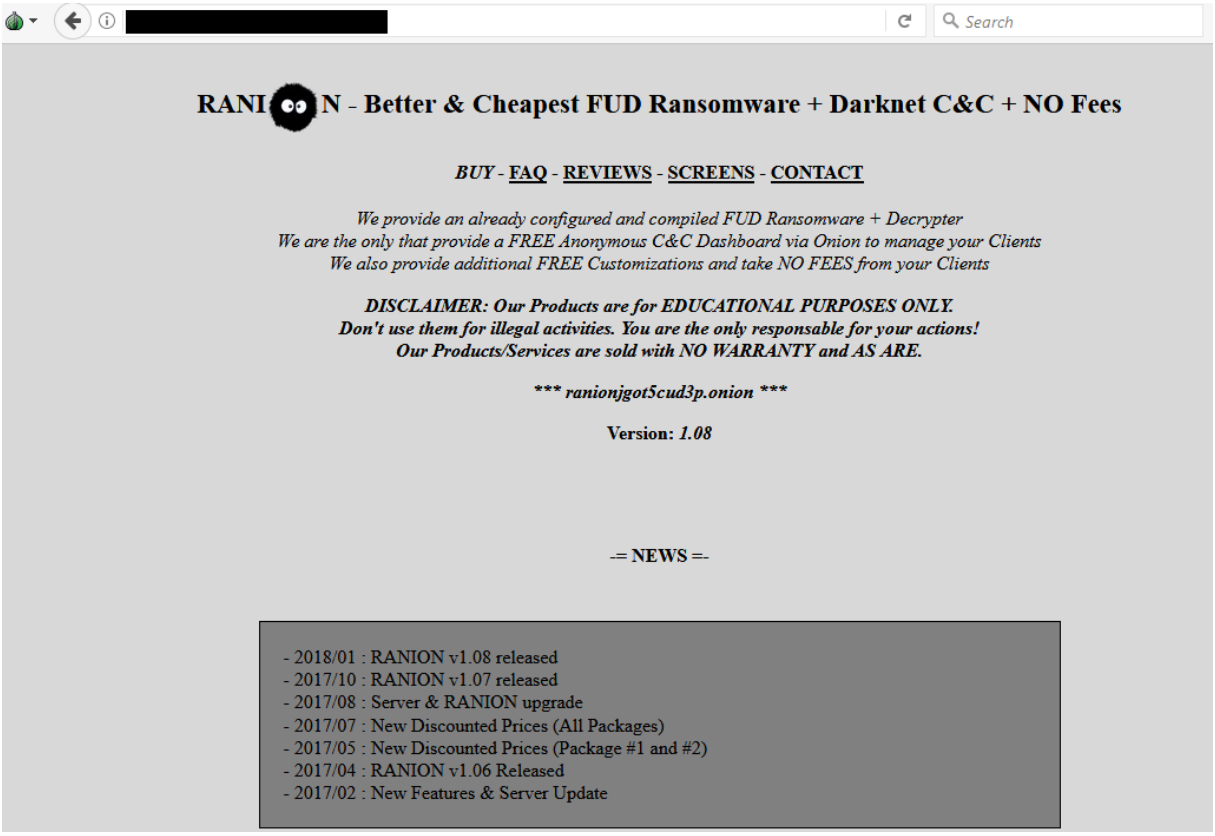
RaaSberry (en ligne)



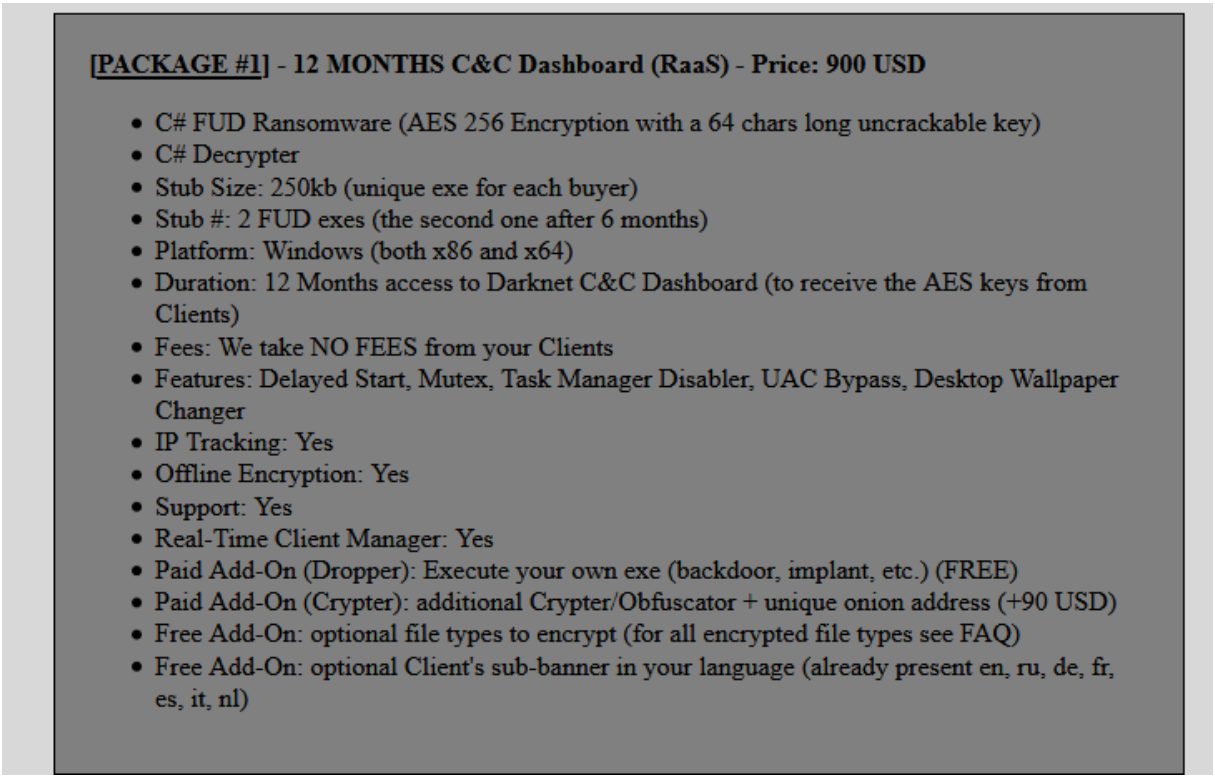
Les différents packages disponibles (prix entre 42€ et 176€)

Les différents packages disponibles (prix entre 282€ et 460€)

Ranion (en ligne)



Page d'accueil du rançongiciel, dernière mise-à-jour du maliciel en janvier 2018.



Exemple de package #1 avec tous les éléments inclus ($900)

[PACKAGE #2] - 6 MONTHS C&C Dashboard (RaaS) - Price: 490 USD

- C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
- C# Decrypter
- Stub Size: 250kb (unique exe for each buyer)
- Stub #: 1 FUD exe
- Platform: Windows (both x86 and x64)
- Duration: 6 Months access to Darknet C&C Dashboard (to receive the AES keys from Clients)
- Fees: We take NO FEES from your Clients
- Features: Delayed Start, Mutex, Task Manager Disabler, UAC Bypass, Desktop Wallpaper Changer
- IP Tracking: Yes
- Offline Encryption: Yes
- Support: Yes
- Real-Time Client Manager: Yes
- Paid Add-On (Dropper): Execute your own exe (backdoor, implant, etc.) (+90 USD)
- Paid Add-On (Crypter): additional Crypter/Obfuscator + unique onion address (+90 USD)
- Free Add-On: optional file types to encrypt (for all encrypted file types see FAQ)
- Free Add-On: optional Client's sub-banner in your language (already present en, ru, de, fr, es, it, nl)

[PACKAGE #3] - 1 MONTH C&C Dashboard (RaaS) - Price: 120 USD

- C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
- C# Decrypter
- Stub Size: 250kb (unique exe for each buyer)
- Stub #: 1 FUD exe
- Platform: Windows (both x86 and x64)
- Duration: 1 Month access to Darknet C&C Dashboard (to receive the AES keys from Clients)
- Fees: We take NO FEES from your Clients
- Features: Delayed Start, Mutex, Task Manager Disabler, UAC Bypass, Desktop Wallpaper Changer
- IP Tracking: Yes
- Offline Encryption: No
- Support: No
- Real-Time Client Manager: No
- Paid Add-On (Dropper): Execute your own exe (backdoor, implant, etc.) (NOT AVAILABLE)
- Paid Add-On (Crypter): additional Crypter/Obfuscator + unique onion address (+90 USD)
- Free Add-On: optional file types to encrypt (for all encrypted file types see FAQ)
- Free Add-On: optional Client's sub-banner in your language (already present en, ru, de, fr, es, it, nl)

Intended to Test our Service

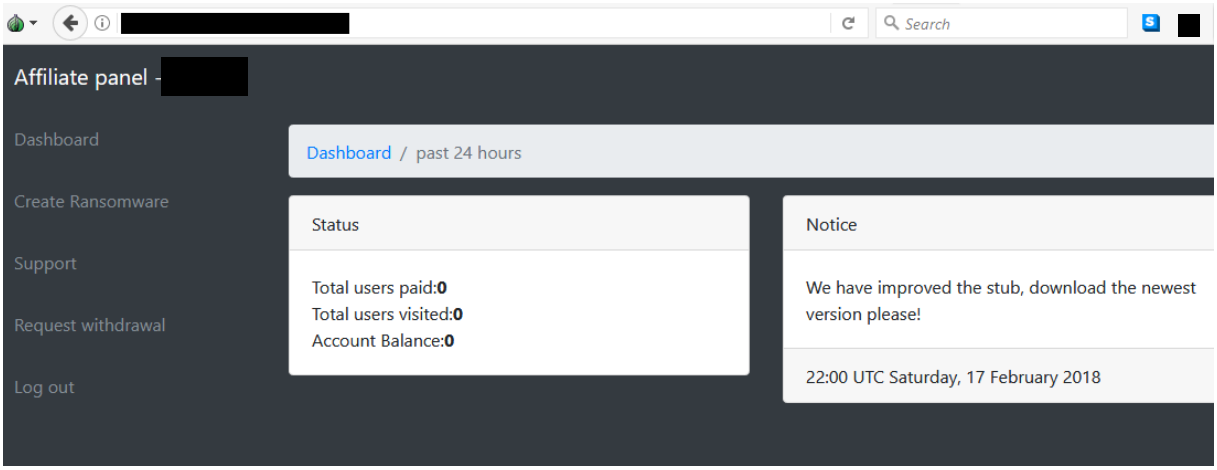
Exemple des packages #2 et #3

- Nouvelle école

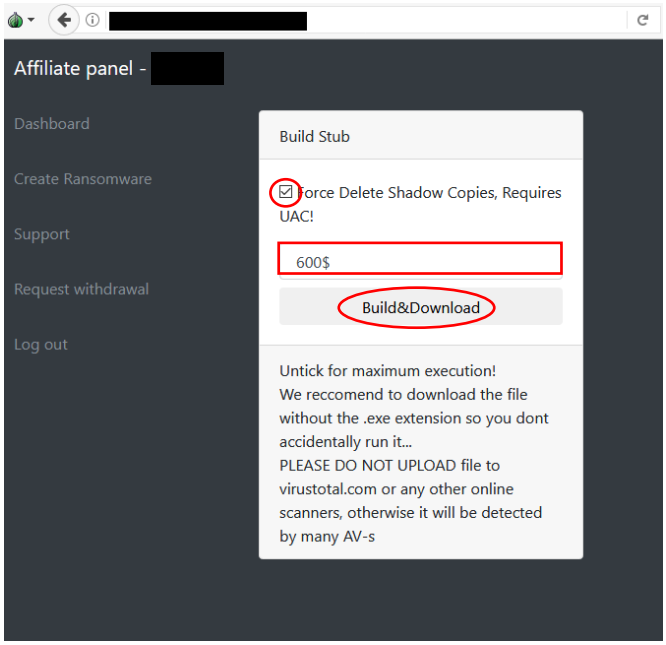
Depuis le début de l'année 2018, un nouveau modèle économique est apparu. Ces dernières semaines, au moins trois RaaS ont été mis à disposition de manière gratuite.

Le modèle économique proposé n'étant plus de louer le rançongiciel mais de le paramétrer et de le télécharger gratuitement. L'infection se fait toujours par l'utilisateur mais cette fois les bénéfices engrangés sous forme de rançons sont versées sur le(s) portefeuille(s) des créateurs du maliciel. Le partage des gains est généralement annoncé comme étant 70% pour l'utilisateur et 30% pour les développeurs.

Saturn (en ligne)



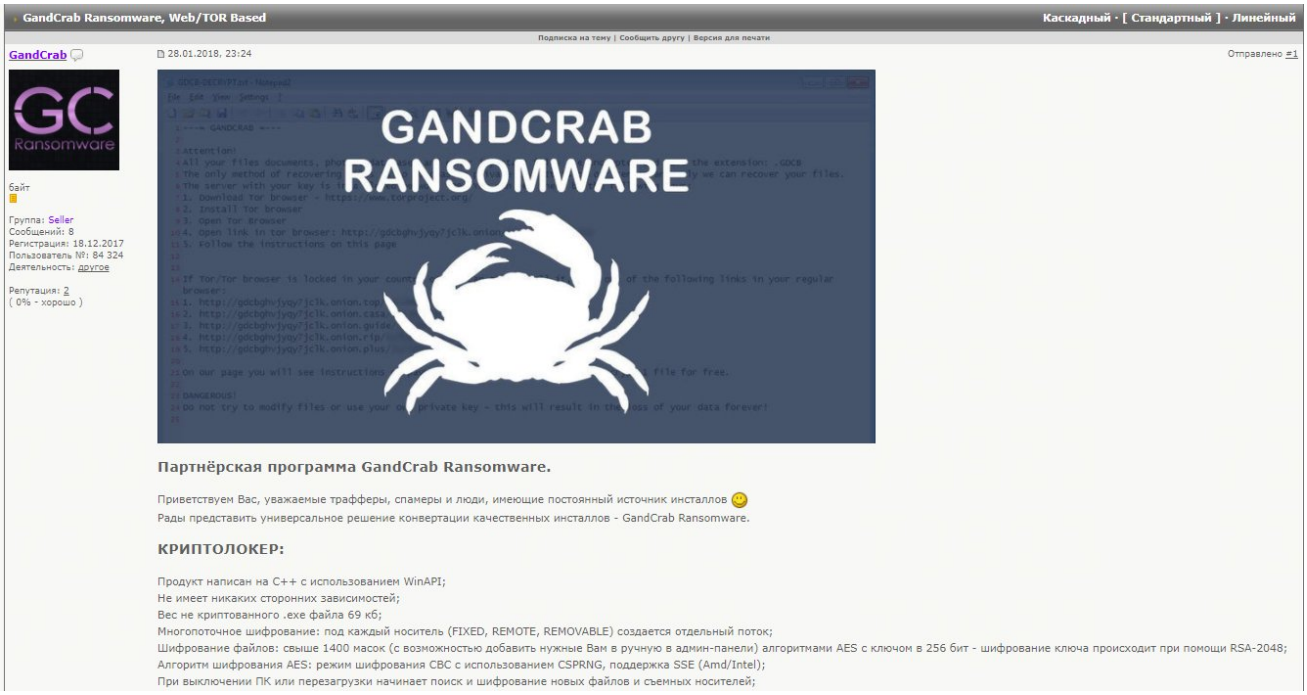
Le tableau de bord du RaaS Saturn



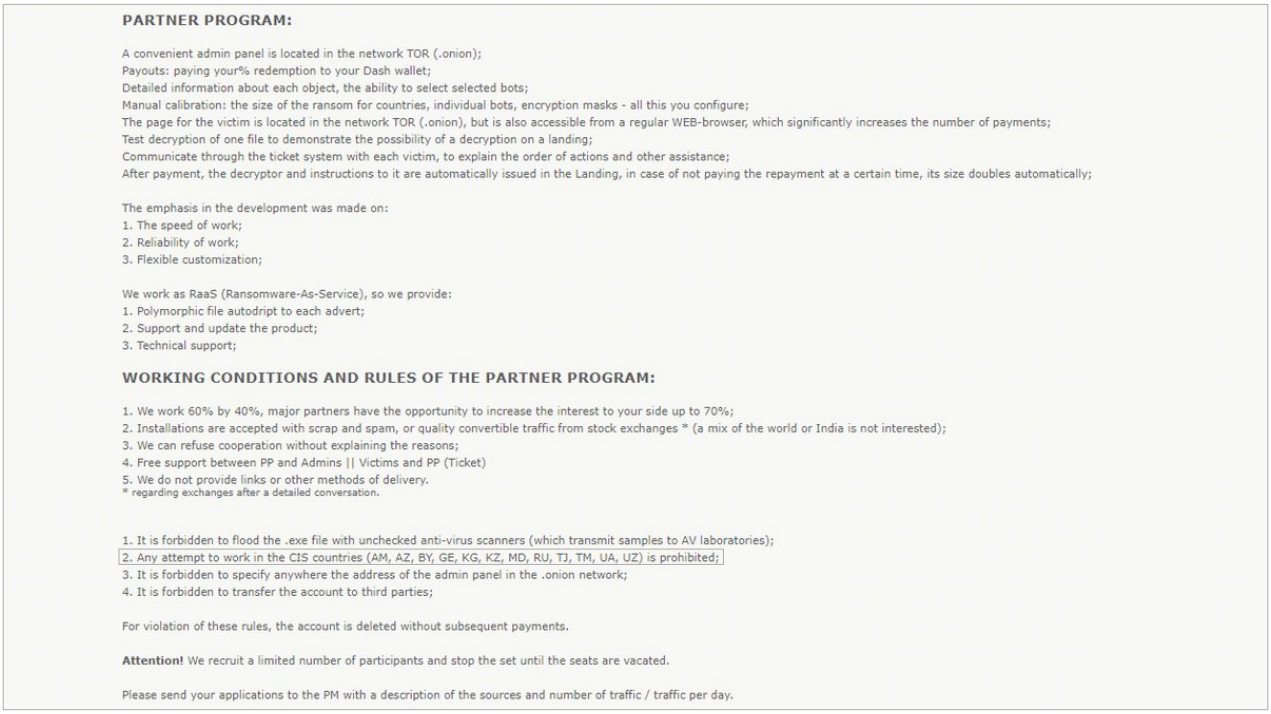
Possibilité de forcer la suppression des « Shadow copies », choix du montant de la rançon (de 300 à 800$) et téléchargement du rançongiciel

GandCrab (V2.0 en ligne)

Un chercheur en sécurité a repéré début février une proposition de RaaS gratuit sur le célèbre forum de hacking « exploit.in ». Il s'agissait du très populaire rançongiciel « GandCrab ». L'offre, formulée en russe et en anglais, propose un fonctionnement comme explicité précédemment avec le partage des gains entre utilisateurs et développeurs.



Introduction du rançongiciel



Proposition formulée en anglais. Il faut noter l'interdiction d'attaquer les membres du CIS (Common wealth of Independent states) donc de l'ex-URSS

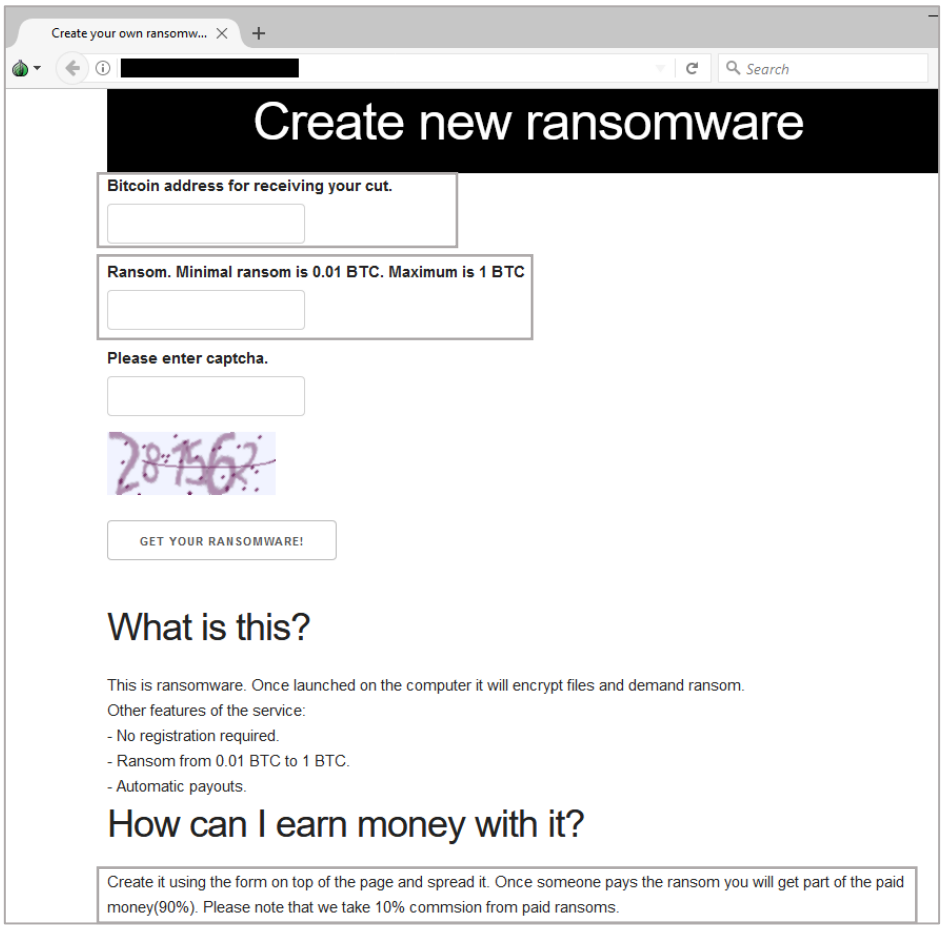
05/03/2018 : Un outil de déchiffrement a été mis en ligne pour les victimes du ransomware GANDCRAB. Cet outil est disponible sur le site www.nomoreransom.org. Cet outil a été développé par la police roumaine, sous la supervision du Bureau du Procureur Général (DIICOT) et en collaboration avec l'entreprise de sécurité informatique Bitdefender et Europol.

07/03/2018 : Un nouvelle version du rançongiciel (**GandCrab V2.0**) est découverte. Sa page de paiement étant accessible sur le darknet. Celle-ci indique une demande d'environ $550 dans la crypto-monnaie « **Dash** ».

On observe la rapidité d'adaptation du milieu criminel : dès lors que leur outil a été rendu inoffensif, ces derniers ont immédiatement développé une nouvelle version de leur maliciel.

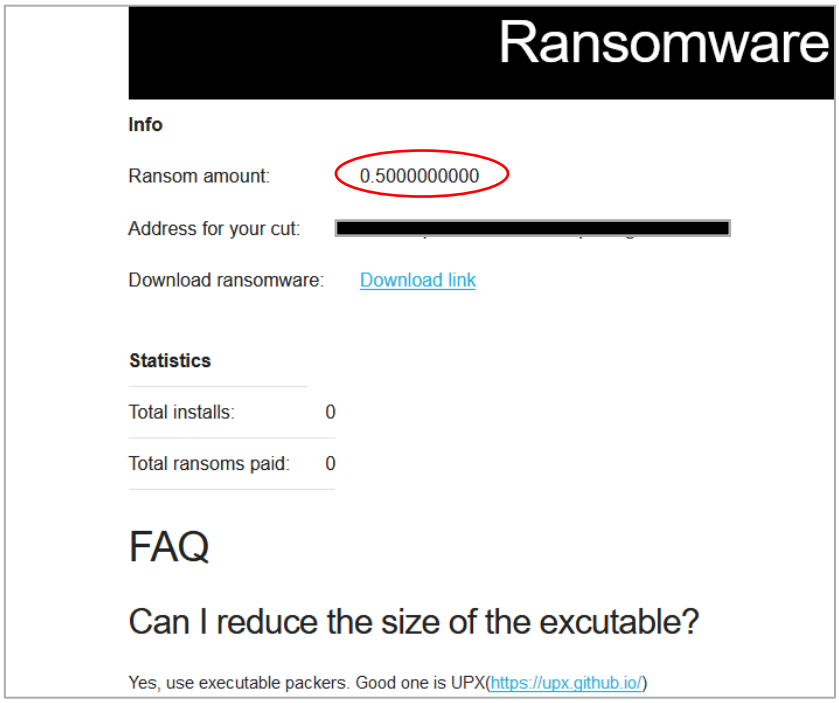
Unnamed Ransomware (en ligne)

Ce RaaS est le plus récent de tous : il propose un fonctionnement quasiment similaire aux précédents exemples mais avec une augmentation des gains de l'utilisateur (90%-10%). Toutefois, suite aux investigations d'un chercheur indépendant[4], cet exemple semblerait être une arnaque (un *scam*). En effet, selon ce chercheur il ne serait pas possible de récupérer les fonds ou de gérer le C&C.



La page d'accueil du RaaS, aucun besoin de s'inscrire pour télécharger le maliciel. Les commissions sont plus avantageuses que les autres offres présentes sur le marché, pour rendre celle-ci plus attirante ?

[4] *Krypt3ia*, source : voir annexes



Une fois une adresse Bitcoin insérée et le choix de la rançon effectuée, il est possible de télécharger le ransomware.

Conclusion

Ce changement de paradigme dans le fonctionnement des RaaS intervient dans un contexte plus général où le cryptojacking[5] devient de plus en plus courant.
Les nombreux mineurs (cryptominers) alimentés par des botnets[6] ont fait leur apparition en 2017 et présentent l'avantage d'être plus simples d'utilisation et ne nécessitent qu'une infrastructure allégée.
Ces innovations (ransomware gratuit et augmentation des cryptominers) coïncident temporellement, ce qui pourrait être vu comme une possible explication aux chamboulements du secteur criminel lié aux crypto-monnaies.

La première conséquence possible est un **affaiblissement du « milieu RaaS »** en raison des multiples **arnaques** susceptibles d'apparaître. De nombreux acteurs peuvent être tentés, derrière une annonce alléchante, de ne pas reverser les fonds aux utilisateurs. Ce non-respect des règles du jeu peut amener à une implosion des acteurs majeurs, n'ayant plus de succès, parasités par la mauvaise réputation d'autres escrocs.

La deuxième conséquence envisageable est une **augmentation conséquente de la cybercriminalité** par l'usage de rançongiciels. La mise en place de ce dispositif de RaaS simplifie l'utilisation de tels logiciels malveillants par des populations peu compétentes en informatique. Il suffit désormais de se rendre sur une page du Darknet (aisément trouvable), de s'inscrire en quelques clics pour télécharger le rançongiciel **gratuitement**.

C'est donc une tendance dangereuse qui fait son apparition depuis le début de l'année 2018 : la sensibilisation et la prévention du grand public restent les premières réponses.

Éléments supplémentaires

Toutes les souches obtenues ont été soumises à la plateforme EMAS d'Europol en attente d'une analyse long terme locale.
2 souches ont ainsi pu être analysées (**Saturn** et **Unnamed Ransomware**). Les rapports d'EMAS indiquent bien une activité type de ransomware.

Sources

Krypt3ia (chercheur en sécurité indépendant)
https://krypt3ia.wordpress.com/2018/02/19/create-new-ransomware-darknet-site-ransomware-scheme/

Bleeping Computer (média spécialisé)
https://www.bleepingcomputer.com/news/security/new-saturn-raas-lets-everyone-become-a-ransomware-distributor-for-free/

[5] Utiliser la puissance de calcul de victimes afin de miner des cryptomonnaies. Nécessite moins de moyens (infrastructure, logistique, etc.)
[6] Réseaux d'ordinateurs zombies