

- Synthèse

Une tendance émergente a été observée dans le paysage cybercriminel au cours de l'année passée : la mise à disposition de plateformes de location de rançongiciel¹. Connue sous le nom de *Ransomware as a Service* ou « **RaaS** », cette pratique se développe à grande vitesse.

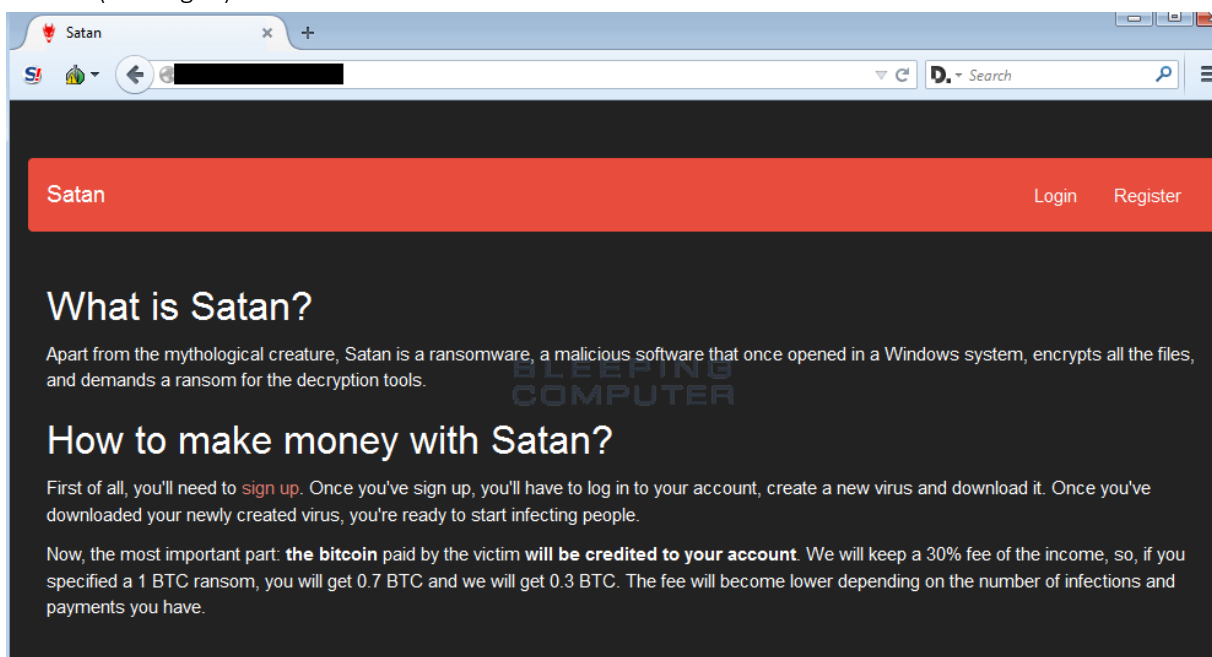
Une tendance toutefois bousculée par un phénomène nouveau : la gratuité et la collaboration autour de ces outils. La découverte de plusieurs sites sur le darknet distribuant des rançongiciels gratuits, les gains étant partagé entre l'utilisateur et les créateurs du logiciel malveillant, semble peser 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 cryptomonnaies³. 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)

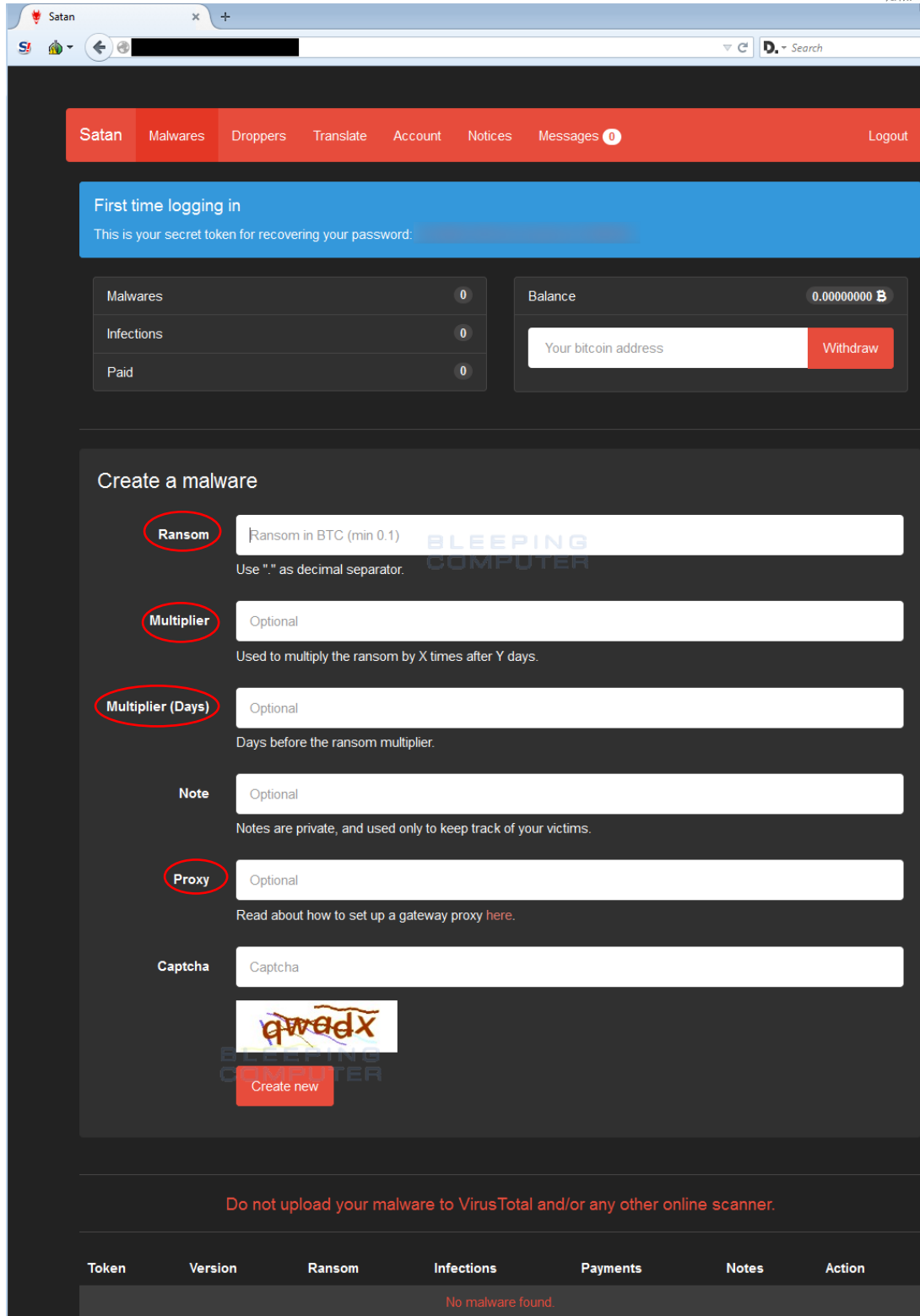


Capture d'écran de la page d'accueil de Satan

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



Satan Malwares Droppers Translate Account Notices Messages 1 Logout

First time logging in
This is your secret token for recovering your password: [REDACTED]

Malwares	0
Infections	0
Paid	0

Balance 0.00000000 B

Your bitcoin address

Create a malware


Ransom
Use "." as decimal separator.

Multiplier
Used to multiply the ransom by X times after Y days.

Multiplier (Days)
Days before the ransom multiplier.

Note
Notes are private, and used only to keep track of your victims.

Proxy
Read about how to set up a gateway proxy [here](#).

Captcha


Do not upload your malware to VirusTotal and/or any other online scanner.

Token	Version	Ransom	Infections	Payments	Notes	Action
No malware found.						

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

RaaSberry (en ligne)

Ransomware as a Service Logout

New Package

Plastic • One Month C&C Subscription \$60 USD

- 250kb Unique EXE - Combo Encrypter/Decrypter
- Compatible with Windows XP to Windows 10
- You receive 100% of the ransom paid by the victims
- Supports Delayed Start, Mutex, and Task Manager Disabler
- Ransomware still works if you don't continue your C&C subscription
- Free support with active C&C subscription

Need 0.00455909 BTC

Bronze • Three Month C&C Subscription \$150 USD

- 250kb Unique EXE - Combo Encrypter/Decrypter
- Compatible with Windows XP to Windows 10
- You receive 100% of the ransom paid by the victims
- Supports Delayed Start, Mutex, and Task Manager Disabler
- Ransomware still works if you don't continue your C&C subscription
- Free support with active C&C subscription

Need 0.01139773 BTC

Silver • Six Month C&C Subscription \$250 USD

- 250kb Unique EXE - Combo Encrypter/Decrypter
- Compatible with Windows XP to Windows 10
- You receive 100% of the ransom paid by the victims
- Supports Delayed Start, Mutex, and Task Manager Disabler
- Ransomware still works if you don't continue your C&C subscription
- Free support with active C&C subscription

Need 0.01899622 BTC

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

Gold • One Year C&C Subscription \$400 USD

- 250kb Unique EXE - Combo Encrypter/Decrypter
- Compatible with Windows XP to Windows 10
- You receive 100% of the ransom paid by the victims
- Supports Delayed Start, Mutex, and Task Manager Disabler
- Ransomware still works if you don't continue your C&C subscription
- Free support with active C&C subscription

Need 0.03039396 BTC

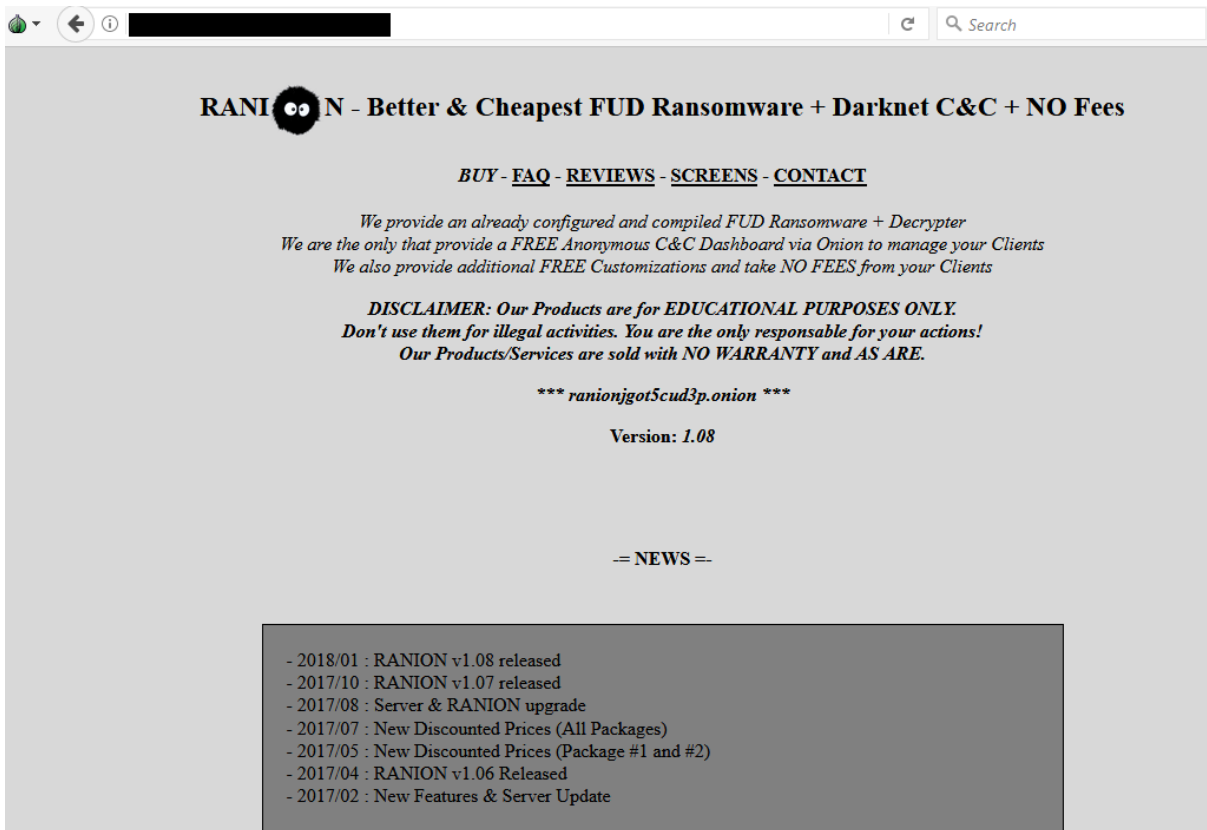
Platinum • Three Year C&C Subscription \$650 USD

- 250kb Unique EXE - Combo Encrypter/Decrypter
- Compatible with Windows XP to Windows 10
- You receive 100% of the ransom paid by the victims
- Supports Delayed Start, Mutex, and Task Manager Disabler
- Ransomware still works if you don't continue your C&C subscription
- Free support with active C&C subscription

Need 0.04939018 BTC

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

Ranion (en ligne)



RANION - Better & Cheapest FUD Ransomware + Darknet C&C + NO Fees

BUY - FAQ - REVIEWS - SCREENS - CONTACT

*We provide an already configured and compiled FUD Ransomware + Decrypter
We are the only that provide a FREE Anonymous C&C Dashboard via Onion to manage your Clients
We also provide additional FREE Customizations and take NO FEES from your Clients*

**DISCLAIMER: Our Products are for EDUCATIONAL PURPOSES ONLY.
Don't use them for illegal activities. You are the only responsible for your actions!
Our Products/Services are sold with NO WARRANTY and AS ARE.**

*** ranionjgot5cud3p.onion ***

Version: 1.08

-- NEWS --

- 2018/01 : RANION v1.08 released
- 2017/10 : RANION v1.07 released
- 2017/08 : Server & RANION upgrade
- 2017/07 : New Discounted Prices (All Packages)
- 2017/05 : New Discounted Prices (Package #1 and #2)
- 2017/04 : RANION v1.06 Released
- 2017/02 : New Features & Server Update

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

[PACKAGE #1] - 12 MONTHS C&C Dashboard (RaaS) - Price: 900 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 #: 2 FUD exes (the second one after 6 months)
- Platform: Windows (both x86 and x64)
- Duration: 12 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.) (FREE)
- 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)

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

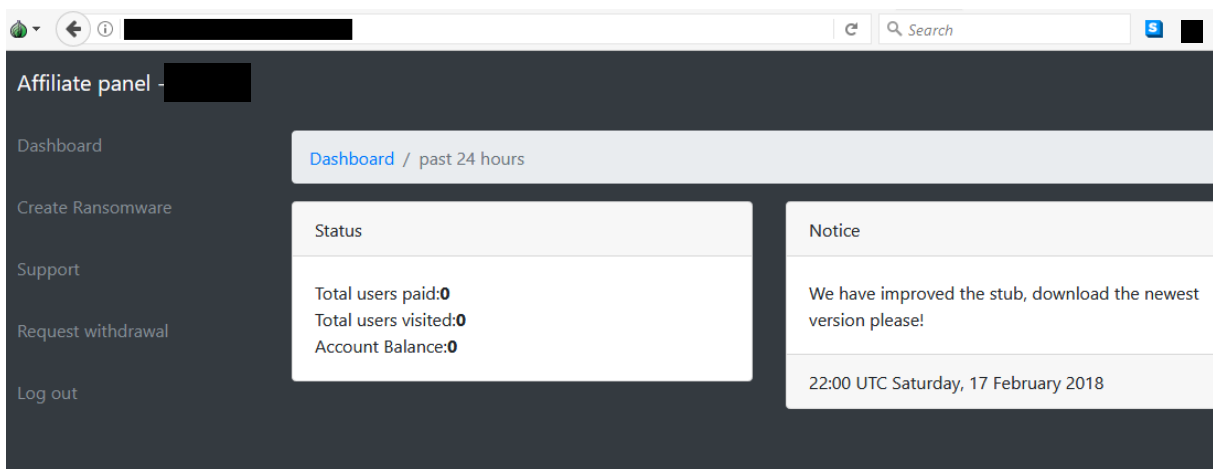
Exemple des packages #2 et #3

- Nouvelle école

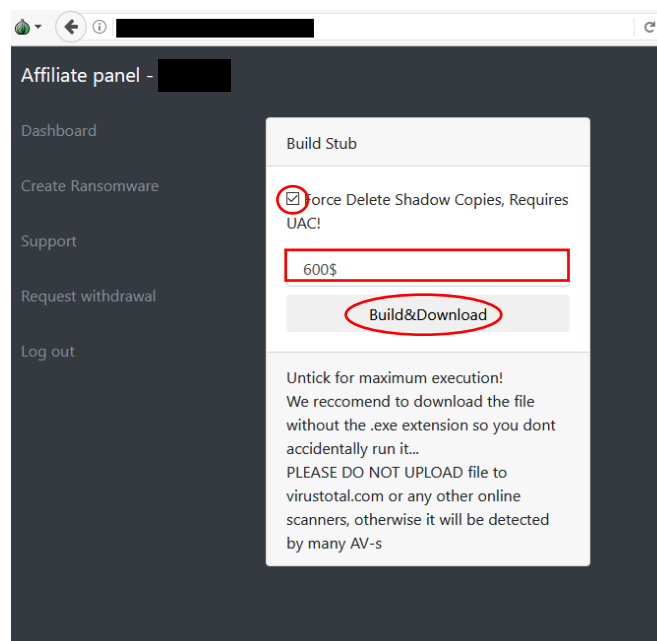
Depuis le début de l'année 2018, un nouveau modèle économique est apparu. Ces dernières semaines, au moins trois RaaS ont été mis à disposition de manière gratuite.

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 malicieux. 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.

Партнёрская программа GandCrab Ransomware.

Приветствуем Вас, уважаемые трафферы, спамеры и люди, имеющие постоянный источник инсталлов 😊
 Рады представить универсальное решение конвертации качественных инсталлов - GandCrab Ransomware.

КРИПТОЛОКЕР:

Продукт написан на C++ с использованием WinAPI;
 Не имеет никаких сторонних зависимостей;
 Вес не криптованного .exe файла 69 кб;
 Многопоточное шифрование: под каждый носитель (FIXED, REMOTE, REMOVABLE) создается отдельный поток;
 Шифрование файлов: свыше 1400 масок (с возможностью добавить нужные Вам в ручную в админ-панели) алгоритмами AES с ключом в 256 бит - шифрование ключа происходит при помощи RSA-2048;
 Алгоритм шифрования AES: режим шифрования CBC с использованием CSPRNG, поддержка SSE (Amd/Intel);
 При выключении ПК или перезагрузки начинается поиск и шифрование новых файлов и съемных носителей;

Introduction du rançongiciel

PARTNER PROGRAM:

A convenient admin panel is located in the network TOR (.onion);
 Payouts: paying your% redemption to your Dash wallet;
 Detailed information about each object, the ability to select selected bots;
 Manual calibration: the size of the ransom for countries, individual bots, encryption masks - all this you configure;
 The page for the victim is located in the network TOR (.onion), but is also accessible from a regular WEB-browser, which significantly increases the number of payments;
 Test decryption of one file to demonstrate the possibility of a decryption on a landing;
 Communicate through the ticket system with each victim, to explain the order of actions and other assistance;
 After payment, the decryptor and instructions to it are automatically issued in the Landing, in case of not paying the repayment at a certain time, its size doubles automatically;

The emphasis in the development was made on:

1. The speed of work;
2. Reliability of work;
3. Flexible customization;

We work as RaaS (Ransomware-As-Service), so we provide:

1. Polymorphic file autodript to each advert;
2. Support and update the product;
3. Technical support;

WORKING CONDITIONS AND RULES OF THE PARTNER PROGRAM:

1. We work 60% by 40%, major partners have the opportunity to increase the interest to your side up to 70%;
2. Installations are accepted with scrap and spam, or quality convertible traffic from stock exchanges * (a mix of the world or India is not interested);
3. We can refuse cooperation without explaining the reasons;
4. Free support between PP and Admins | Victims and PP (Ticket)
5. We do not provide links or other methods of delivery.
 * regarding exchanges after a detailed conversation.

1. It is forbidden to flood the .exe file with unchecked anti-virus scanners (which transmit samples to AV laboratories);
2. Any attempt to work in the CIS countries (AM, AZ, BY, GE, KG, KZ, MD, RU, TJ, TH, UA, UZ) is prohibited;
3. It is forbidden to specify anywhere the address of the admin panel in the .onion network;
4. It is forbidden to transfer the account to third parties;

For violation of these rules, the account is deleted without subsequent payments.

Attention! We recruit a limited number of participants and stop the set until the seats are vacated.

Please send your applications to the PM with a description of the sources and number of traffic / traffic per day.

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

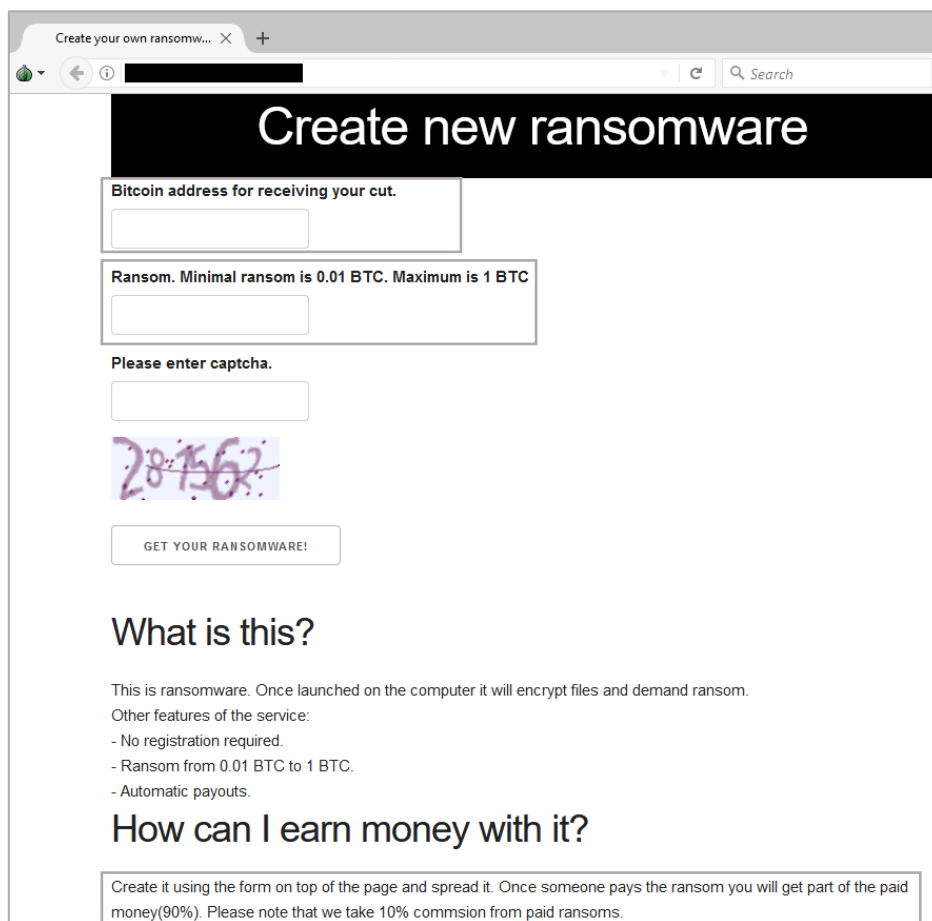
05/03/2018 : Un outil de déchiffrement a été mis en ligne pour les victimes du ransomware GANDCRAB. Cet outil est disponible sur le site www.nomoreransom.org. Cet outil a été développé par la police roumaine, sous la supervision du Bureau du Procureur Général (DIICOT) et en collaboration avec l'entreprise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

07/03/2018 : Une 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 indépendant⁴, 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

Ransomware

Info

Ransom amount: 0.5000000000

Address for your cut: [REDACTED]

Download ransomware: [Download link](#)

Statistics

Total installs: 0

Total ransoms paid: 0

FAQ

Can I reduce the size of the executable?

Yes, use executable packers. Good one is UPX(<https://upx.github.io/>)

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 cryptojacking⁵ devient de plus en plus courant.

Les nombreux mineurs (cryptominers) alimentés par des botnets⁶ 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