Différents ransomware

Le ransomware **Locker**: Bloque les fonctions de base de l’ordinateur.

Le ransomware **Crypto** : chiffre les données importantes (documents, photos etc…)

* Locky :

**Fonctionnement :** Lorsque la victime ouvre la pièce jointe de son mail (une facture en format .txt), le logiciel Word va demander à l’utilisateur d’activer les macros pour lire le texte. Le ransomware chiffre ensuite tous les fichiers et supprime les sauvegardes Windows (shadow copies).

**Date d’apparition :** 2016

**Rançon :** 400$

**Victime :** représentent environ 16% des ransomwares

**Moyen d’infection :** pièce jointe (document, format .doc) par mail envoyé grâce à un botnet.

**Moyen de réparation :**

* Paiement d’une rançon en Bitcoin puis installation du déchiffreur « Locky »
* Perte des données, formatage complet des disques durs infectés.



* WannaCry :

**Fonctionnement :**  Ce ransomware profite d’une faille de sécurité (EternalBlue) dans le système d’exploitation Windows. Cette faille a été découverte deux mois avant l’apparition de WannaCry, mais certains utilisateurs n’ont pas eu le temps de mettre à jour leur OS. Le ransomware s’est donc installé sur Windows en installant DoublePulsar en tant que backdoor. Il modifie également les volumes système pour gêner les antivirus. Il est considéré comme le plus grand piratage à rançon de l’histoire d’Internet.

**Date d’apparition :** mai 2017

**Victime :** 330 000 utilisateurs Windows, Renault, Vodafone, gouvernement russe et allemand etc…

**Rançon :** 600$

**Moyen d’infection :** faille de sécurité EternalBlue exploitée par la NSA mais volée par le groupe de pirates informatiques Shadow Brokers. Et pièce jointe (document, format .doc) par mail envoyé grâce à un botnet.

**Moyen de réparation :**

* Paiement d’une rançon en Bitcoin n’a que très rarement fonctionné sur ce Ransomware.
* Perte des données, formatage complet des disques durs infectés.
* Utilisation du logiciel français Wanakiwi qui fonctionne dans 10% des cas.



* PETYA :

**Fonctionnement :** Il chiffre la table de fichiers maitres (MFT) de l’ordinateur de la victime. La particularité de Petya est qu’il cible l’ensemble du disque, empêchant ainsi l’ordinateur de démarrer. Il infecte ensuite le master boot record (MBR), attend une heure puis force l’ordinateur à redémarrer pour ensuite chiffrer la table MFT.

**Date d’apparition :** mars 2016

**Rançon :** 300 $

**Victime :** SNCF, BNP Paribas etc…

**Moyen d’infection :** pièce jointe (document, format .doc) par mail envoyé grâce à un botnet.

**Moyen de réparation** :

* Paiement d’une rançon en Bitcoin
* Perte des données, formatage complet des disques durs infectés.
* PEYTA attend une heure avant de se lancer. S’il est détecté avant, éteindre l’ordinateur, se déconnecter du réseau et contacter le CAD.

Une image contenant texte, capture d’écran, menu, rouge

Description générée automatiquement

* ZCRYPTOR :

**Fonctionnement :** Il fonctionne comme les autres hormis qu’il infecte également tous les drivers et les stockages externes (clés USB, disques durs etc..). Sur les supports externes, il se camoufle et attend de contaminer une autre machine.

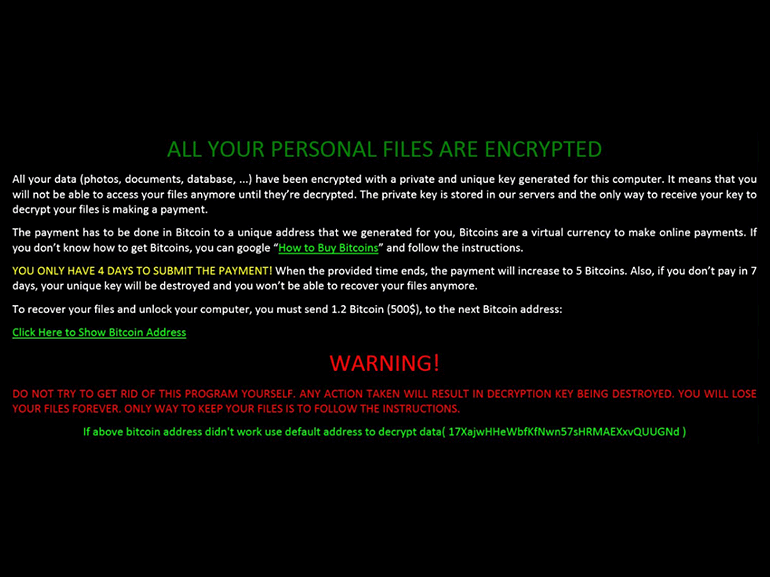
**Date d’apparition :** mai 2016

**Rançon :** 500$ à 2500$ dollars (augmente avec le temps).

**Moyen d’infection :** pièce jointe (document, format .doc) par mail envoyé grâce à un botnet.

**Moyen de réparation :**

* A l’avance, désactiver l’autoplay sur les clés USB.
* Paiement d’une rançon en Bitcoin
* Perte des données, formatage complet des disques durs infectés.



* nRansom (nRansom.exe) :

**Fonctionnement :** La particularité de nRansom est qu’il ne demande pas une rançon, mais 10 photos de soi nu, envoyés par mail, qui seront revendus sur le Deep Web. Ce ransomware est assez inoffensif car il ne chiffre pas le disque dur mais bloque l’écran. Le code de déverrouillage est « 12345 » mais ne fonctionne pas. L’intérêt de ce ransomware est plutôt de souligner l’inventivité et la diversité que peut avoir une demande de rançon via un malware.

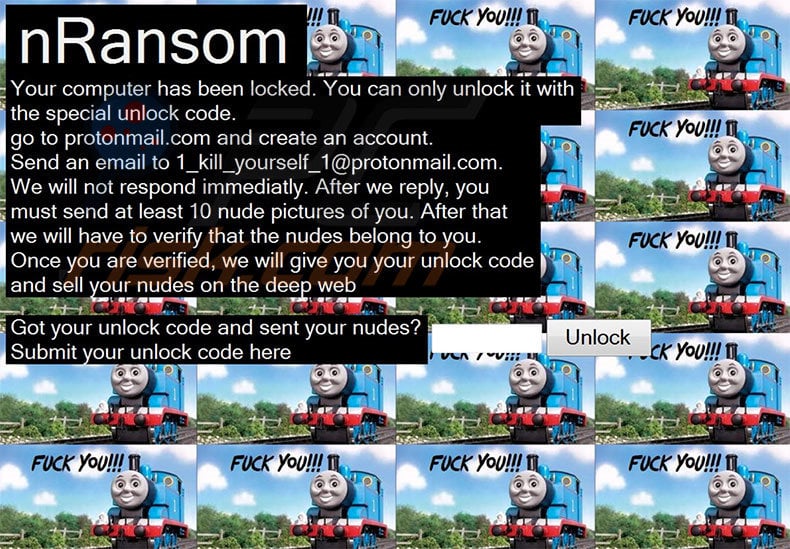
**Date d’apparition :** 2017

**Rançon :** 10 « nudes »

**Moyen d’infection :** mails, pièces jointes, téléchargement (ne touche que les utilisateurs Windows car fichier .exe).

**Moyen de réparation :**

* Diminuer l’écran et fin des tâches sur le process. Ctrl + Alt + Maj + F4



Musique d’arrière-plan : called your-mom-gay.mp3

* RAA (JS/RANSOM-DLL) :

**Fonctionnement :** Contrairement aux autres ransomware, RAA écrit en JS car Windows n’affiche pas les extensions .js par défaut. La victime se fait donc avoir plus facilement et a plus de confiance envers le fichier qu’elle vient de recevoir sur sa boîte mail. Le ransomware chiffre les données, envoie un message afin de détourner l’attention de l’utilisateur. En bonus, il installe également un extracteur de mdp (Pony stealer) afin de récupérer plus d’informations sur la victime, même si celle-ci paye la rançon. Les fichiers touchés par l’extension. locked sont les suivants : .doc, .xls, .rtf, .pdf, .dbf, .jpg, .dwg, .cdr, .psd, .cd, .mdb, .png, .lcd, .zip, .rar, .csv. Il supprime également les sauvegardes Windows Shadow Copy Services (VSS)

**Date d’apparition :**

**Rançon :** 250$

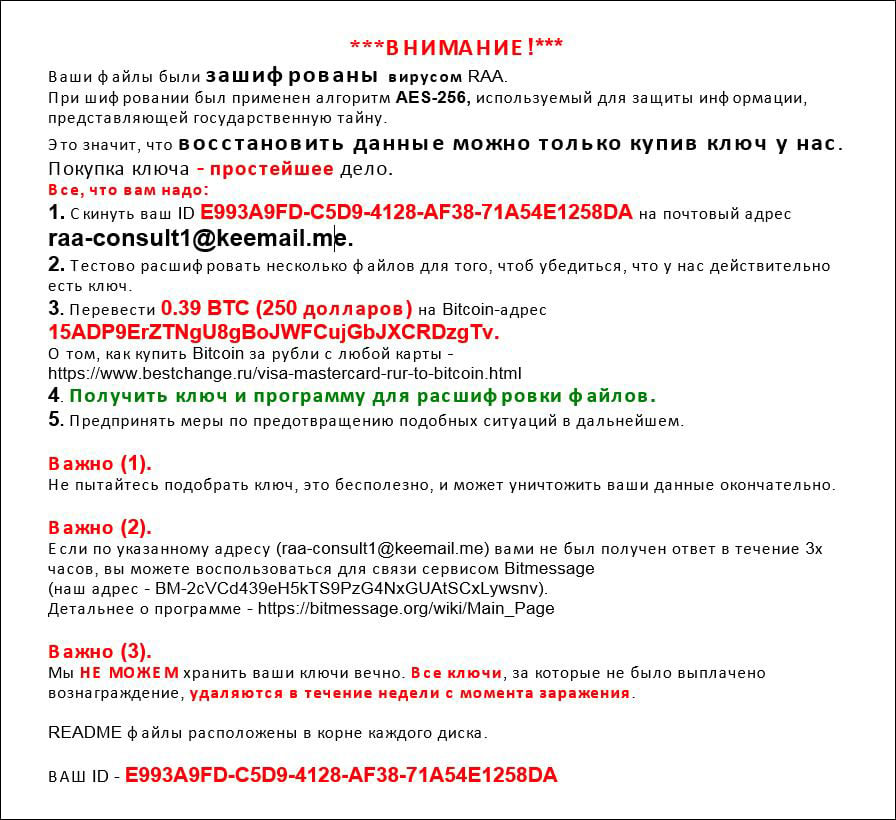
**Répartition :**

**Moyen d’infection :**

**Moyen de réparation :**

* Aucun moyen actuel afin de décrypter les fichiers sans avoir la clef.
* Avant l’infection, désactiver Windows Script Host si vous n’utilisez pas ces scripts.

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows Script Host\Settings\Enabled



* Ryuk :

**Fonctionnement :** Ryuk est un ransomware complexe qui vise des victimes importantes avec des demandes de rançons très élevées. Avant 2021, Il n’était pas automatique et nécessitait un accès via une latéralisation manuelle, ce qui impliquait du temps de la part du Hacker. Sa particularité est qu’il ne chiffre pas uniquement les données, mais récupère énormément d’informations en restant invisible avant de se lancer. Il exploite des vulnérabilités afin de se propager. Cela peut être des failles dans des logiciels (Adobe Flash Player ou Java), dans des OS (failles dans le service Remote Desktop Protocol RDP). Une fois installer il désactive les protections, les antivirus et les pare-feu via des techniques d’obfuscation et de modification de code. Il modifie les attributs de ses fichiers ainsi que les clés de registre afin de rester caché et assurer son lancement et sa persistance. Il utilise Powershell afin de récupérer des informations que les groupes, le réseau, les processus en cours d’exécution, décrypter des mdp simple via une bibliothèque de mots clés etc… En bonus, il supprime les VSS afin d’empêcher les restaurations Windows. Il chiffre les données avec les algorithmes RSA-2048 et AES 256. Et les fichiers cryptés de démarquent d’une extension .RYK

**Date d’apparition :** 2018

**Rançon :**  100 000$ à un record à 12,5 millions$

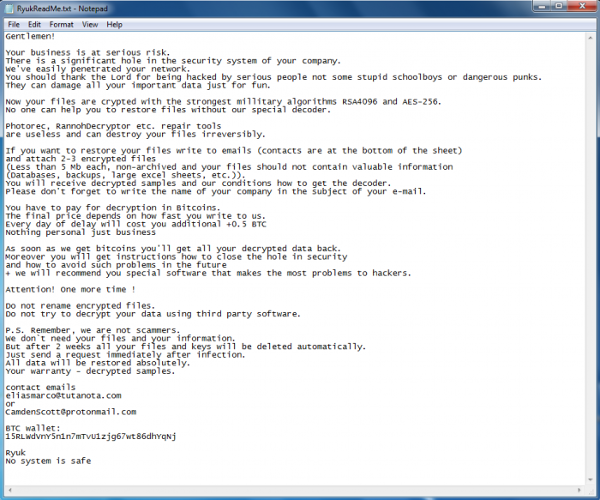
**Victime :** grosse entreprise, hôpitaux américains

**Répartition :** 75% des attaques du secteur de la santé en 2020

**Moyen d’infection :** mail, ingénierie sociale, phishing etc…

**Moyen de réparation :**

* Payer ou perdre ses données…
* A l’avance, vérifier que son OS ne soit pas infecté par des malwares (TrickBot, BazarLoader, Emotet) qui facilitent l’insertion d’un ransomware



Résumer des moyens d’éviter un ransomware :

* Désactiver l’autoplay sur les clés USB.
* Désactiver les Macros sur Word
* Sauvegarde externe régulière des fichiers

Collectifs Hacker intéressants : WizardSpider / UNC1878 / FIN6

Source :

Etude des Ransomware : Vecteur d’attaque, fonctionnement, économie et réponse légal / Leutrim Bisini

-avast

Kasperky

[CERTFR-2020-CTI-011.pdf (ssi.gouv.fr)](https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-011.pdf)

[nRansom Joke Locker Demands Nude Pics as Payment. (bleepingcomputer.com)](https://www.bleepingcomputer.com/news/security/nransom-joke-locker-demands-nude-pics-as-payment-/)