ROUZEE Julien
LOPEZ Paul

INFO910:
Ransomware

TABLE DES MATIÈRES

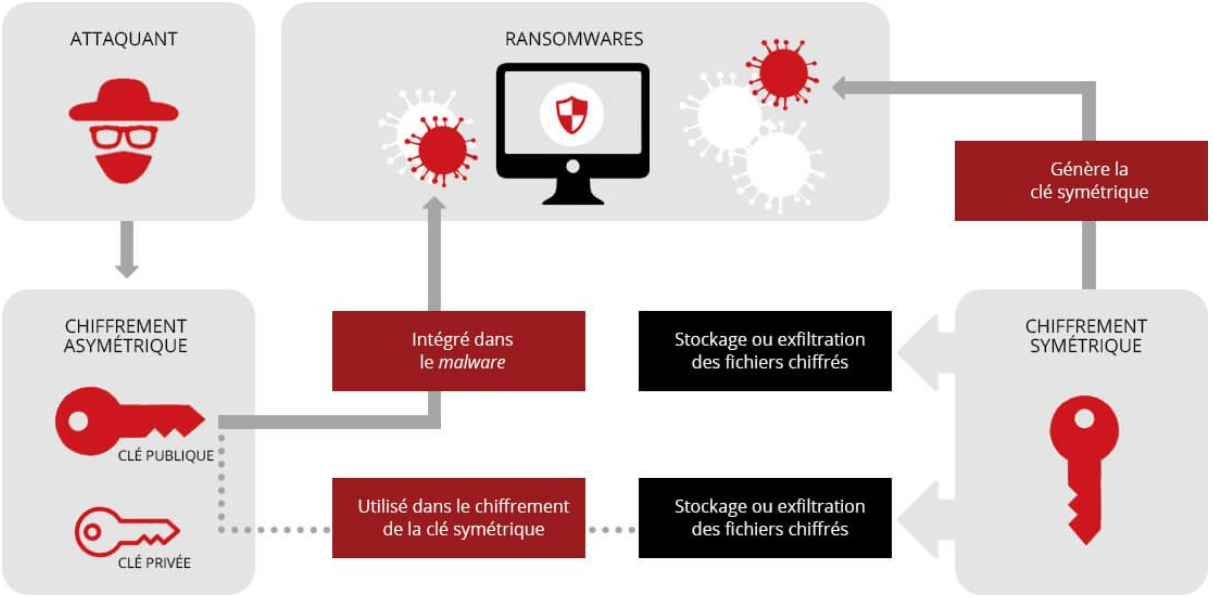
Introduction

Un ransomware (rançongiciel en français) est un logiciel rançonneur qui a pour but de récupérer des données personnelles, de chiffrer ces données puis de demander au propriétaire d'envoyer de l'argent en échange de la clé qui permettra de déchiffrer les données. Ceci est l'utilisation la plus courante du ransomware mais il est aussi possible de bloquer l'accès de tout utilisateur à une machine et d'échanger de l'argent contre une clé qui permettra de débloquer cette machine. En 2012 McAfee rapporte avoir enregistré 120 000 nouveaux échantillons de ce genre de virus au deuxième trimestre 2012 (soit 4 fois plus qu'à la même période l'année précédente.) Depuis l'utilisation de ces virus n'a fait que d'augmenter, entre 2016 et 2017 on peut enregistrer une augmentation de 36% d'utilisation de ces virus.

Qu'est-ce qu'un ransomware ?

Mode opératoire :

Un ransomware se propage de la même manière qu'un cheval de Troie. Il pénètre le système grâce à un email-malicieux, ou alors par malvertising.
Cette méthode consiste à utiliser des publicités en ligne pour distribuer des malwares et qui nécessite peu ou pas d'interactions avec les utilisateurs. Alors qu'ils surfent sur le Web, y compris sur des sites légitimes, les utilisateurs peuvent être renvoyés vers des serveurs criminels sans avoir même cliqué sur une seule publicité. Ces serveurs répertorient des informations concernant les ordinateurs des victimes et leur emplacement, puis ils sélectionnent les malwares les plus susceptibles de les infecter.



Pour faire simple:

1. Le cybercriminel génère une paire de clés et place la clé publique dans le malware.
2. Le malware génère une clé symétrique aléatoire et chiffre les données de la victime. Un **chiffrement hybride** va être effectué où la clé publique va être utilisée pour chiffrer la clé symétrique.
3. Ce chiffrement va donner un ciphertext asymétrique ainsi qu'un ciphertext symétrique des données de la victime.
4. Un message est envoyé à la victime incluant le ciphertext asymétrique et la marche à suivre pour payer la rançon. La victime renvoie le ciphertext asymétrique et la rançon (en e-monnaie) au cybercriminel.
5. Celui-ci reçoit le paiement, déchiffre le ciphertext asymétrique avec sa clé privée et envoie la clé symétrique à la victime. La victime peut donc déchiffrer ses données cryptées avec cette clé.

Une fois propagé, il y a 3 types de ransomware :

Scareware

Un faux logiciel de sécurité ouvre une fenêtre, vous informant qu'un malware a été détecté et que la seule manière de s'en débarrasser est de passer à la caisse. Si vous ne faites rien, vous continuerez sûrement à être bombardé de messages similaires, mais, dans l'absolu, vos fichiers resteront en sécurité. En soit, à par énormément de messages, rien de grave.

Verrouilleurs d'écran

Ce malware a pour but de bloquer l'accès d'une machine, il changera le shell par défaut dans la base de registre Windows (où il changera le Master Boot Record). Lorsque vous démarrez votre ordinateur, votre écran est entièrement recouvert par une fenêtre comportant souvent des éléments de mise en page semblables à ceux d'une institution gouvernementale, telle que le FBI ou le ministère de la justice, qui vous informe qu'une activité illégale a été détectée sur votre ordinateur et que vous devez payer une amende.

Ransomwares chiffreurs

Les plus dangereux, ils exécutent une charge active (La charge symbolise les données utiles transportées par un protocole). Par exemple un exécutable qui va chiffrer les fichiers de l'utilisateur depuis son disque dur. Une fois ceci fait, vos fichiers sont cryptés et vous ne pourrez plus les utiliser. Il existe des ransomwares sophistiqués qui utilisent des algorithmes de chiffrement hybride sur les données de la victime, ceci permet d'avoir une clef symétrique aléatoire et une clé publique fixée. Ainsi, l'auteur du ransomware est le seul connaissant la clé privée permettant de déchiffrer les documents.

Dans les 3 cas, le but est d'extorquer de l'argent, la victime payera un programme pour chiffrer ses fichiers ou un simple code qui retire tous les verrous appliqués à ses documents. plusieurs moyens de paiement sont possibles (virement bancaire, sms surtaxé, achats de monnaie virtuelle, paypal etc). La rançon est depuis 2017 souvent aux alentours de 550 dollars.

Histoire :

1989 :

Premier logiciel de ransomware, PC Cyborg Trojan, consistait à envoyer un payload avertissant l'utilisateur qu'une certaine licence d'un certain logiciel aurait expiré, en chiffrant des fichiers sur le disque dur et en demandant 189$ à ces victimes. Toutefois les chercheurs ont découvert que le chiffrement était réalisé symétriquement (ce qui signifie que la clé de chiffrement est la même que la clé de déchiffrement). Etant donné que pour chiffrer le contenu, le logiciel devait transporter la clé de chiffrement. Cela rendait cette première version obsolète car les victimes pouvaient ne pas payer la rançon.

1996 :

L'utilisation du chiffrement de clé publique pour les ransomware a été introduite par Adam L. Young et Moti Yung. Ils proposent un POC d'un ransomware utilisant les algorithmes RSA et TEA (Tiny Encryption Algorithm) pour effectuer un chiffrement hybride des données de la victime. Ce POC a été réalisé dans le but d'attaquer un Macintosh SE/30.
Le virus ne contient que la clé de chiffrement. L'attaquant conserve la clé privée de déchiffrement correspondantes.

2006:

Des ransomware comme GPcode ont commencé à utiliser des schémas de chiffrement RSA à 660 bits.

2008:

Amélioration de GPcode, il utilise désormais des schéma de chiffrement RSA a 1024 bits, considéré comme suffisamment grand pour être incassable (sans utiliser une puissance de calcul considérable).

2013 :

Les ransomwares redeviennent populaires avec la popularité du Bitcoin. Un ransomware a été utilisé de nombreuses pour soutirer des sommes en cryptomonnaies, le CryptoLocker. Il

visait principalement des machines sous Windows. Les cybercriminels derrière CryptoLocker auraient amassé plus de 27 millions de dollars selon ZDNet.

CryptoLocker a ensuite été utilisé comme base pour développer de nouveaux ransomwares de plus en plus performant.

Quelques exemples notables d'attaque au ransomware

Reveton :

En 2012, le ransomware appelé Reveton a commencé à se faire connaître.

Il se transmettait grâce aux méthodes Trojan. Une fois installé sur la machine, Reveton s'installe lui-même sous forme de fichier .dll qui se lance à chaque lancement de Windows et qui ne peut être arrêté par le gestionnaire de tâches.

Une fois exécuté, toutes les applications et fonctionnalités afficheront une page web avec de fausses accusations comme des téléchargements illégaux. Une demande de rançon est affichée pour débloquer la machine. Le paiement se faisait d'abord sous un système de e-paiement (MoneyPack) qui plus tard sera remplacé par le bitcoin. Les rançons allaient de 100$ à 200$ avec une deadline.

Cette méthode est la version classique de Reveton, il y a eu des versions où au lieu de bloquer les applications, les données sont cryptées.

WannaCry :

En mai 2017, une attaque au ransomware WannaCry s'est répandue sur internet utilisant une faille appelée EternalBlue.

Sans rentrer dans les détails techniques, EternalBlue est une faille dans les systèmes Microsoft repérée par la NSA. Cette dernière n'a pas informé Microsoft de cette faille pendant 5 ans jusqu'à qu'il soit trop tard. Cette faille venait du Server Message Block (SMB) protocole.
Une fois la faille connue, Microsoft a mis à disposition des patchs de sécurité pour se défendre face à ce ransomware. Cependant de nombreux utilisateurs n'avaient pas installé les mises à jour et l'attaque a continué à se répandre.

WannaCry est un ransomware de type "cryptoworm". Comme la plupart des ransomwares, il crypte les données et demande une rançon en Bitcoin. Il est surnommé "ver" car il dispose d'un mécanisme de transport qui lui permet de se répandre lui-même. Il scanne les systèmes vulnérables et exploite la faille EternalBlue pour accéder à ce nouveau système et ainsi de suite.

Les conséquences de cette attaque ont été plus de 230.000 machines infectées dans 150 pays différents avec des rançons à hauteur de 300$ par machine.

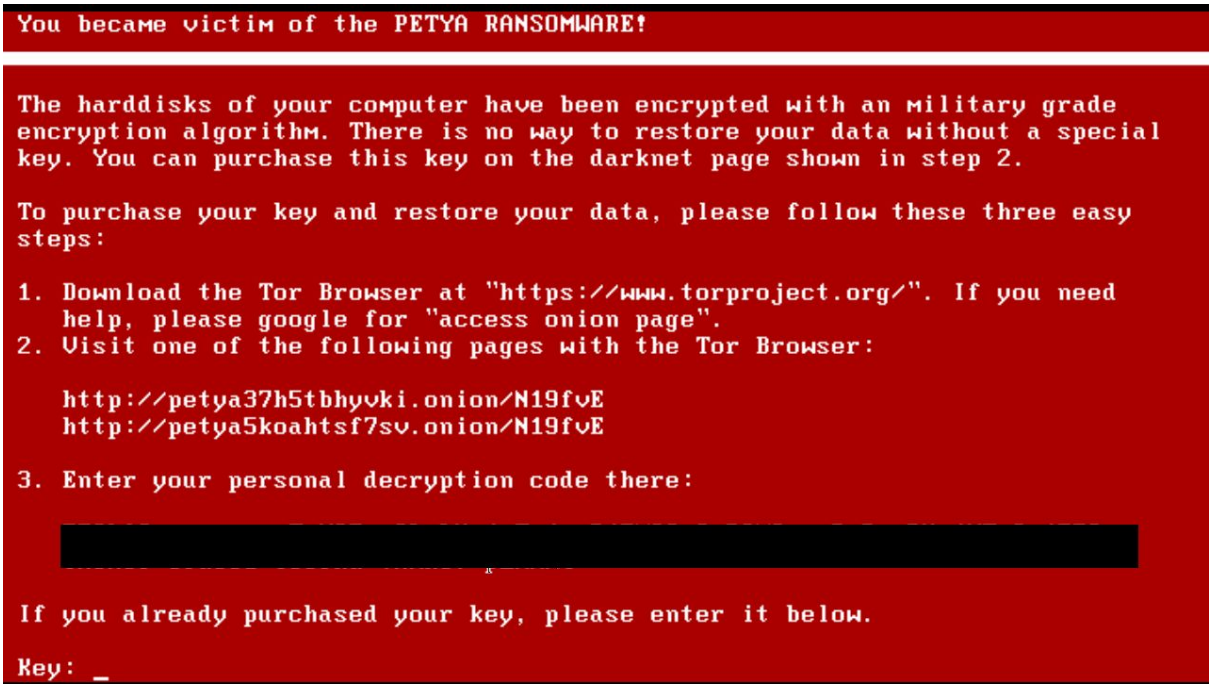
L'originaire présumé de ce ransomware est le groupe Lazarus, un groupe de cybercriminel koréen.

Petya :

Le ransomware Petya a été découvert en mars 2016. Il se démarque par sa cible à infecter dans la machine, le MBR (Master Boot Record) qui correspond au premier secteur adressable d'un disque dur dans un partitionnement Intel.

Il installe un payload qui chiffre les fichiers NTFS la prochaine fois que la machine est booté. Cela résultait dans un blocage du lancement de Windows jusqu'à ce que la rançon soit payée.
Il a été constaté que malgré la nouveauté dans le type d'attaque, il y en a eu moins que d'autres ransomwares à cette époque (CryptoLock par exemple).

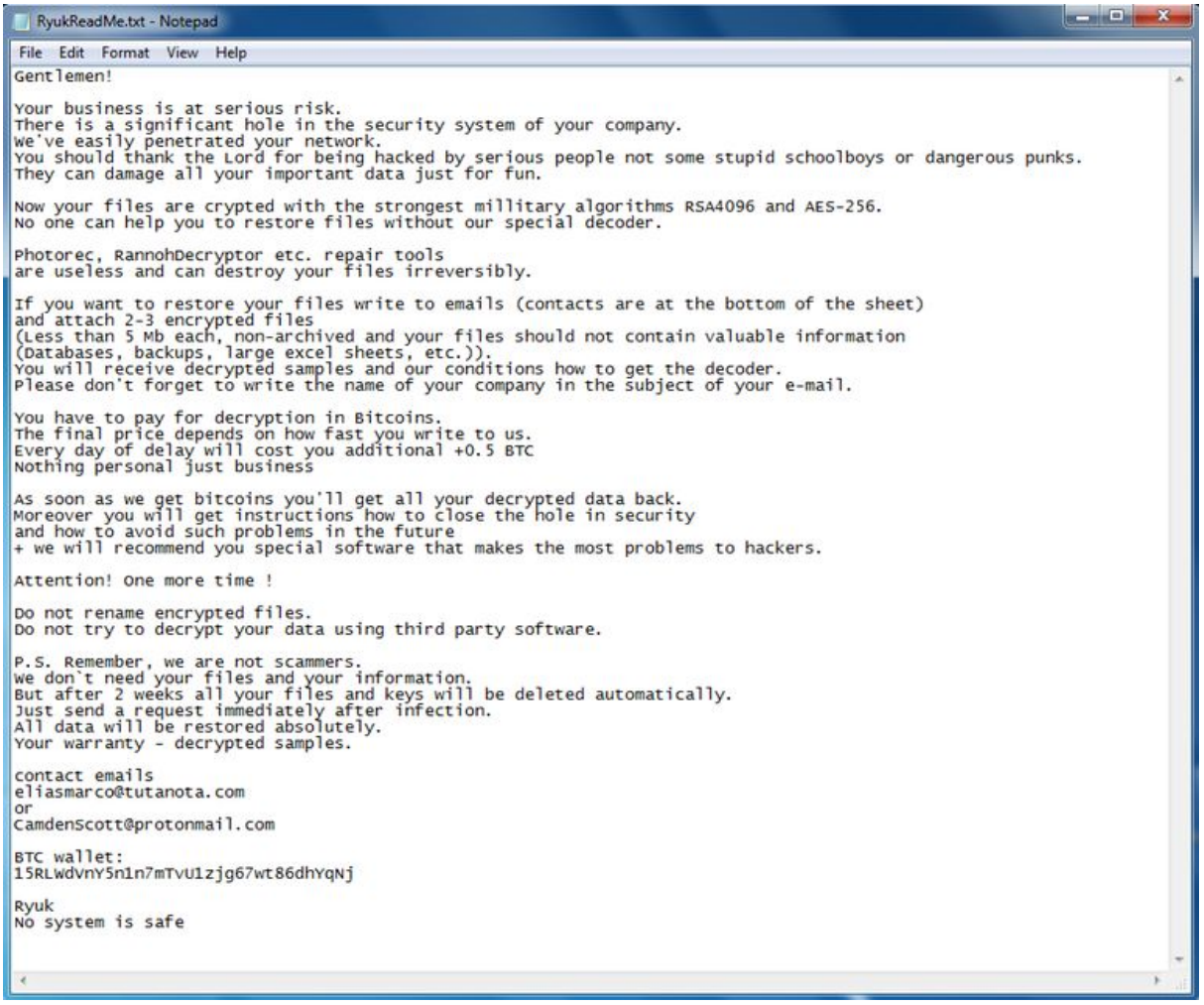
En juin 2017, une version améliorée de Petya est découverte. Elle est utilisée pour des cyberattaques de masse et dans ce cas, contre l'Ukraine. De nombreux pays ont aussi été affectés.
Cette nouvelle version utilisait la faille EternalBlue comme WannaCry mais était faite de manière à ce que le système soit débloqué dès que la rançon est payée.



Ryuk :

Le plus récent est le ransomware Ryuk qui, en août 2019, a été utilisé contre des grandes entreprises américaines et a permis aux cybercriminels de amasser 640.000$ en moins de deux semaines.

Ce ransomware chiffre les stockages et les centres de données des victimes et demandent des rançons conséquentes (50 Bitcoins).
Le résultat de cette attaque est au lancement de votre machine, un parmi deux messages:
Le premier, très poli où il est spécifié qu'une faille dans la sécurité de l'entreprise a été détectée ce qui a mené à un chiffrement de toutes les données qui pourront être récupérées contre une certaine somme.



Le deuxième message est beaucoup plus simple. Juste une demande de rançon car les données de la machine ont été chiffrées.

Il a été découvert que la technique de chiffrement utilisée par le ransomware Ryuk est similaire au ransomware Hermès. Ce dernier utilise les algorithmes de chiffrement AES.
Ryuk s'en est inspiré à tel point que des références à Hermès sont présentes dans le code source.

Comment lutter ?

Des anti-virus ont fournis une solution pour certains ransomwares :

Crypto-verrouilleur	Société ayant fourni une solution (partielle ou complète)
Amnesia	Emsisoft
BTCware	Avast
Cry9, Cry128 et Crpton	Emsisoft
Jaff	Kaspersky Lab[38]
LambdaLocker	Avast[39]
MacRansom	Trend Micro[40]
Mole	Organisme polonais Cert-pl (en)
NemucodAES	Emsisoft[41]

Prévention :

Très important: faire des sauvegardes régulières de ses données, et les stocker hors ligne.
Une fois infecté, déconnecter les appareils infectés des réseaux partagés, avec ou sans fil.

Soyons clairs : il n'existe pas encore de déchiffreurs pour toutes les familles de ransomwares, car les ransomwares utilisent généralement des algorithmes de chiffrement sophistiqués et très avancés. Cependant il existe des déchiffreurs gratuits permettant de récupérer ces données (ne marche pas à tous les coups).

Télécharger une solution de sécurité connue pour ses capacités de remédiation et en lançant une analyse pour éliminer la menace.Vous ne retrouverez peut-être pas vos fichiers, mais vous aurez au moins l'assurance de vous être débarrassé de l'infection.

Contre un ransomware verrouilleur d'écran, une restauration complète du système sera peut-être nécessaire.

Une fois désinfecté, changer ses mots de passe après avoir nettoyé le réseau ;

Qui peut créer un ransomware ?

Aujourd'hui il est très facile d'acquérir un logiciel de type ransomware. Pirates propose des logiciels permettant d'acquérir un ransomware, il est possible de le personnaliser. Ensuite vous obtiendrez un fichier .exe, cachez ce fichier dans une image ou autre, et pour finir il ne vous restera plus qu'à infecté des machines avec votre ransomware caché dans un fichier. Bien sûr le pirate proposant ce genre de service prend 50% du montant de votre rançon.

Voici un ransomware Builder permettant de créer son ransomware en le personnalisant simplement.

Conclusion

Nous avons pu voir que les ransomwares représentent une menace grandissante. En effet, ces 10 dernières années les dégâts causés par ces malware en font une priorité pour les entreprises.
Cette évolution s'explique par le développement des outils numériques et ainsi des accès à un réseau. La situation sanitaire a accentué ces vulnérabilités avec le télétravail et des entreprises pas à jour dans leurs protocoles de sécurité en faisant des cibles idéales pour ce type d'attaque.
De plus, il devient de plus en plus facile de se procurer son propre ransomware (darkweb, programme de création de ransomware …).

C'est un sujet qui nous a beaucoup intéressé car nous ne connaissions pas l'étendue des ransomwares et la menace qu'ils représentent actuellement.
Comprendre le fonctionnement d'un ransomware parait simple au premier abord mais quand on creuse un peu et que l'on s'intéresse à certains ransomwares, on se rend très vite compte de la complexité des différents processus (infection, chiffrement, propagation …).

Sources

https://www.altospam.com/glossaire/ransomware.php

https://www.kaspersky.fr/resource-center/definitions/what-is-ransomware

https://en.wikipedia.org/wiki/Ransomware

https://www.zdnet.fr/actualites/ryuk-un-ransomware-qui-coute-tres-cher-aux-entreprises-39872615.htm

https://www.avast.com/fr-fr/c-petya