SIMPLY SECURE

Ransomware
Risques et solutions

G DATA analyse le phénomène et présente ses protections

G DATA Software AG | 2017

Table des matières

Évolution des Ransomware

L'attaque par ransomware est un Business model cybercriminel. Il empêche l'accès aux données, applications ou au système d'exploitation d'un utilisateur à l'aide de logiciels malveillants et en propose le déblocage contre le paiement d'une rançon (en anglais : ransom).

Les cas de Ransomware ont été très nombreux ces dernières années avec un pic en 2016 et deux attaques significatives en 2017. Les Ransomware ont recours aux mêmes mécanismes d'infection utilisés par les autres programmes malveillants. La différence la plus notable comparée aux autres types de malware réside dans la visibilité de l'attaque. La plupart des autres programmes malveillants se dissimulent en arrière-plan afin de pouvoir réaliser leurs actions à l'insu de la personne infectée. Ici c'est différent : lors d'une infection, les conséquences c'est-à-dire les dommages résultants de l'infection sont perceptibles tout de suite.

Une histoire ancienne, des évolutions régulières

Les récentes attaques de ransomware, Wannacry et Petna, qui ont défrayé la chronique durant les mois de juin et juillet 2017 ne doivent pas faire oublier que ce type d'attaque n'est pas récent.
Le premier cas connu de Ransomware nous ramène en 1989. Un cheval de Troie nommé *AIDS* a été diffusé sur une disquette lors d'une conférence WHO sur le thème du sida et contenait supposément des informations sur cette maladie. Après la lecture de la disquette, la table d'allocation des fichiers était chiffrée sur le système de la victime. Pour le déblocage, la somme de $189 était exigée et devait être envoyée à une boîte aux lettres au Panama. Cette ancienne attaque avec paiement par courrier postal reste anecdotique. Dans leur format actuel, qui repose sur la diffusion du code par Internet et le paiement numérique de la rançon, les ransomware sont beaucoup plus récents.

GPCoder, le premier d'une longue lignée

C'est en 2005 que *GPCoder* se diffuse. Il chiffre photos, bases de données et documents et demande le versement d'une rançon pour le déchiffrement. *GPCoder* est passé par de nombreuses phases de développement, qui ont amélioré autant la fonctionnalité que la qualité du Ransomware.

Fin 2013, ce sont les programmes malveillants de la famille *CryptoLocker* qui apparaissent. Les données sur le disque dur sont alors chiffrées. La clé nécessaire au déchiffrement est envoyée à l'attaquant à la fin du processus de chiffrement et supprimée sur le système de la victime. Le paiement se réalise en Bitcoin – une monnaie virtuelle qui assure l'anonymat de la transaction. La rançon demandée dans le cadre d'une attaque non ciblée se situe en moyenne autour de 300 $.

Petya, le système est attaqué

En mars 2016, G DATA Software détecte et analyse Petya, un nouveau type de ransomware qui a la particularité de chiffrer le secteur de démarrage du système (MBR). Alors que seuls les fichiers étaient ciblés auparavant, ce nouveau code s'attaque au système en lui-même. Petya est utilisé en juin 2016 dans la campagne Golden Eye. Elle cible principalement les entreprises allemandes.

En janvier 2017, un autre ransomware particulier est détecté et analysé par G DATA. Spora est le premier ransomware à intégrer des fonctions de diffusion de type « vers ». Autrement dit, alors que les codes malveillants précédents restaient cantonnés au poste infecté et aux partages réseau qui y étaient

connectés, Spora est capable de se répandre sur d'autres postes à travers les supports de stockage amovibles.

Des attaques au retentissement mondial

Les nouvelles capacités de diffusion des ransomware sont les éléments déclencheurs des attaques massives qui ont lieu en mai et juin 2017. La première vague commence avec le code Wannacry, le 12 mai. En 12 heures elle touche près de 100 000 systèmes en utilisant une faille dans le protocole de communication SMB de Windows. Une faille pourtant connue et pour laquelle un patch est disponible depuis quelques semaines. L'arrêt miraculeux de cette campagne est dû à un chercheur qui, par l'enregistrement du domaine interrogé par le code malveillant, va désactiver l'exécution du code sur les systèmes infectés.

La deuxième attaque massive basée sur un ransomware survient quelques semaines plus tard, le 27 juin 2017. Cette attaque, dont la charge virale appelée « Petna » s'inspire en partie du code Petya, cible les entreprises ukrainiennes par l'infection du serveur de mise à jour du logiciel financier MeDOC[1]. Mais l'impact de cette attaque sera plus global compte tenu des interconnexions de réseau dans les grands groupes internationaux. Toutefois, le processus de paiement sous-dimensionné et l'impossibilité de déchiffrer des fichiers posent des questions de la finalité de cette attaque[2]…

Les raisons du succès

La hausse des cas est liée à plusieurs facteurs :

- Le modèle est simple et lucratif. L'investissement dans la diffusion du programme malveillant est minime. Le retour sur investissement est très rapide et sans grand investissement.
- Le déroulement du paiement par Bitcoins est anonyme.
- Le risque d'être pris en faute est faible.

En outre, il existe également l'offre Ransomware-as-a-Service (RaaS). Les attaquants ne doivent pas nécessairement avoir de compétences en programmation ou disposées d'une infrastructure pour mettre en place ce type d'attaque. Ils peuvent acheter la conception du Ransomware et sa diffusion comme un service.

Vecteurs d'infection

Jusqu'aux attaques récentes, la majorité des Ransomware était diffusée à travers les emails. Les codes malveillants étaient camouflés dans des factures (par exemple avec *Locky*)[3], ou si des entreprises étaient ciblées, en tant qu'email de candidature au format PDF (par exemple avec *Petya*)[4]. Ces emails intègrent une pièce jointe malveillante qui contient le « downloader ». Ce programme se connecte à Internet et télécharge à partir d'un serveur de commande la dernière version du code malveillant (appelé « charge utile »).

L'autre vecteur de diffusion également utilisé est le « Drive-by », ou l'infection du système par la navigation. Les attaquants intègrent des kits exploits dans des sites Internet mal protégés, ou créent

[1] https://www.gdatasoftware.com/blog/2017/06/29840-petya-is-back-again
[2] https://www.gdatasoftware.com/blog/2017/07/29859-who-is-behind-petna
[3] https://blog.gdatasoftware.com/2016/02/25209-encryption-trojan-locky-what-you-need-to-know-about-the-ransomware
[4] https://blog.gdatasoftware.com/2016/03/28213-ransomware-petya-encrypts-hard-drives
https://blog.gdatasoftware.com/2016/03/28226-ransomware-petya-a-technical-review

également leurs propres pages web infectées. Ces kits exploits ciblent des vulnérabilités dans le système de l'utilisateur. Par ces failles, l'installation de logiciels malveillants est possible et se fait à l'insu de l'internaute. Un comportement prétendu « sûr » lors de la navigation ne protège pas des infections, car les attaques peuvent également venir de sites Internet légitimes compromis. Sur ceux-ci, les kits exploits sont souvent intégrés dans des bannières publicitaires nuisibles (Malvertising).

Avec l'arrivée de Spora, Wannacry et Petna, de nouvelles méthodes de diffusion ont vu le jour. La plus avancée a été utilisée par Petna. En plus d'exploiter les vulnérabilités EternalBlue et EternalRomance (deux failles qui ont fuité des serveurs de la NSA !), Petna détourne les outils d'administration WMI et psexec de Windows. Des éléments du célèbre outil Mimikatz[5] ont aussi été utilisés.

> *CryptoDefense + CryptorBit* se font passer pour des mises à jour Adobe Flash
> *Synolocker* utilise les vulnérabilités dans Synology Diskstation Manager
> *UmbreCrypt* utilise en autre les Terminal Services hackés comme vecteur d'infection

La solution G DATA Anti-Ransomware

Le Ransomware est un type de malware qu'il est possible de reconnaître et de bloquer avec les protections existantes telles que le pare-feu, le filtrage Internet, les signatures antivirus ou encore la surveillance comportementale. Mais G DATA a également développé G DATA Anti-Ransomware afin de réagir encore plus spécifiquement aux activités des Ransomware et protéger contre les menaces telles que *Locky, CryptoLocker, TeslaCrypt, Petya, CTBLocker*, etc.

G DATA Anti-Ransomware travaille indépendamment des signatures et utilise la procédure de reconnaissance heuristique pour une protection proactive. Ainsi, les chevaux de Troie de chiffrement, même encore inconnus, sont reconnus en temps et en heure par leurs activités et leurs attributs typiques. Par exemple, on peut déceler :

- La prise de contact sur le serveur de contrôle. Certains types de Ransomware ne sont actifs que lorsqu'ils ont reçu des fichiers nécessaires à leur fonctionnement provenant de ce serveur pilote. Sans ce contact, ils restent inactifs.
- La mise hors service et la suppression de sauvegardes du système d'exploitation (copies fantômes).
- L'utilisation de procédure pour une suppression sécurisée des fichiers. Si les fichiers ne sont pas supprimés d'une façon sécurisée, alors ils peuvent être restaurés.
- Le chiffrement de nombreux fichiers dans un laps de temps court.
- Après un accès en écriture, le type des fichiers et l'entropie de ceux-ci se modifient.
- La modification de l'extension des fichiers (par ex : de .docx en .locky)

[5] https://twitter.com/gentilkiwi/status/879855038713274369

- La création et la consignation d'une note d'extorsion (Ransom Note) par les attaquants.

> *Exemple du Ransomware Teslacrypt :*
> *Dans la plupart des cas, les programmes malveillants de la famille Teslacrypt ciblent les PC des victimes par des infections Drive-by en passant par des sites Internet compromis. L'antivirus utilise le filtrage d'URL, l'analyse du flux http et la protection anti-exploit comme premiers remparts. Si ces protections sont contournées et que le code est exécuté, il va alors contacter son serveur de contrôle, s'ancrer dans le système et modifier les paramètres du système d'exploitation. Ces actions sont généralement détectées et bloquées par l'analyse comportementale. Si ces barrières sont également franchies, alors Teslacrypt se prépare au chiffrement en commençant par supprimer les copies fantômes. Les fichiers sont ensuite chiffrés et des notes d'information (Ransom Notes) déposées dans les dossiers correspondants. G DATA AntiRansomware est capable de détecter et de bloquer l'ensemble de ces actions et ainsi arrêter immédiatement l'attaque.*

Aussitôt que l'heuristique reconnaît des modifications caractéristiques aux chevaux de Troie de chiffrement, les processus concernés sont arrêtés. Les programmes malveillants mis en cause sont envoyés en quarantaine.

La technologie de blocage de ransomware de G DATA est démontrée en vidéo ici :

Attaque sans la solution G DATA installée : https://www.youtube.com/watch?v=OtMJ7eG1LNI

Attaque bloquée par G DATA : https://www.youtube.com/watch?v=5C6-nGUvdlI

Optimiser le niveau de protection de son réseau

L'infection par Ransomware n'est pas une fatalité. Avec de bons outils et de bonnes pratiques, il est possible de protéger efficacement son réseau contre ces attaques.

- Utilisation d'une solution de sécurité Endpoint multicouche à administration centralisée.
  - Être équipé d'un antivirus ne suffit pas. Filtrage web, pare-feu ou encore sauvegarde sont nécessaires à une protection efficace.
  - L'administration centralisée permet également de s'assurer que les protections sont à jour sur tous les postes du réseau.
- Filtrage Antispam et antivirus sur la passerelle de messagerie.
- Désactivation de l'exécution automatique des macros dans les logiciels de bureautique.
- Sauvegardes régulières des données.
- Mises à jour régulières des programmes installés et des systèmes d'exploitation des clients du réseau.
  - Les failles de sécurité sont des portes d'entrée pour les malware
  - La mise en place d'un système de gestion centralisé des correctifs est un plus.
- Limitation des droits administrateurs sur les postes et dans le réseau.