G DATA Anti-Ransomware

G DATA SecurityLabs

G DATA SecurityLabs

Introduction aux Ransomware 2

Evolution des Ransomware 2

Un peu d'histoire 2

Screenlocker – l'accès à l'ordinateur est bloqué 2

Cryptolocker – les données sont chiffrées 3

Causes et origines de l'augmentation des activités liées aux Ransomware 4

Vecteurs d'infection 4

Bilan 5

G DATA Anti-Ransomware 5

Optimiser le niveau de protection de son réseau d'entreprise 6

Introduction aux Ransomware

Evolution des Ransomware

Le 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 significatif en 2016. 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.

Un peu d'histoire

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. Mais, 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 boite aux lettres au Panama.

Screenlocker – l'accès à l'ordinateur est bloqué

Depuis 2012, les Ransomware ont le vent en poupe ! Un logiciel malveillant nommé *Reveton* interrompait le lancement du système avec un écran verrouillé. L'accès au système n'était consenti que sous condition du paiement d'un montant défini. L'attaque reposait généralement sur une tromperie : la police (ou une autre autorité) aurait bloqué l'ordinateur, car l'utilisateur aurait eu accès à du contenu illégal, par exemple des copies pirates ou du matériel pédopornographique. L'identité d'une organisation comme l'Hadopi (Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet), ou une autorité judiciaire (police, gendarmerie, etc.) était usurpée pour effrayer la cible de l'attaque. La SACEM, Microsoft ou encore le FBI était d'autres entités usurpées. En France, *Reveton* était sous le nom de « virus gendarmerie ».

Reveton était relativement facile à supprimer. Seul le démarrage du système d'exploitation était modifié, et non les données sur le disque dur. Les modifications de la procédure de lancement étaient relativement simples à restaurer. Et les données pouvaient au moins être sauvées en connectant le

disque dur à un autre ordinateur. G DATA EU Ransomware Cleaner[1] supprime *Reveton* et autres bloqueurs de systèmes/screenlocker.

Cryptolocker – les données sont chiffrées

GPCoder se diffuse en 2005 et chiffre des photos, des bases de données et d'autres types de données importantes 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, les programmes malveillants de la famille *CryptoLocker* 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. Pour pouvoir effectuer le déchiffrement et restaurer l'accès aux documents personnels, il ne reste alors plus d'autre choix que de payer la somme demandée par les attaquants.

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 $[2]. La famille du code malveillant *CryptoLocker* a été impactée en août 2014 par l'arrestation de ses créateurs et la déconnexion (takedown) des serveurs de chiffrement[3]. L'analyse de ces serveurs a permis de récupérer des données et de trouver des moyens de déchiffrement. *CryptoLocker* a marqué de son nom toute une catégorie de Ransomware qui est toujours utilisée, bien que le premier de cette catégorie ne soit plus actif. Les logiciels malveillants suivants, qui se font passer pour *CryptoLocker* sont des successeurs (par exemple : *TorrentLocker* ou *PClock*).

Le nombre de familles de Ransomware qui chiffrent des données augmente constamment. De 2014 à 2015, ce nombre double d'environ 15 à 30. A l'heure actuelle, nous comptons plus de 200 familles de Ransomware différentes. Mais il n'y a pas que le nombre de familles qui augmente, la diffusion de ces Ransomware augmente elle aussi. Le nombre d'infections par Locky ou Cryptowall sont arrivés respectivement aux places 3 et 8 du top 10 des programmes malveillants les plus fréquents[4].

Le panel de types de données concernées par ces attaques a également été élargi de façon conséquente. Le nombre d'extensions de fichiers ciblées ne cesse d'augmenter. On recense :

- Média (Images, fichiers audio et vidéo)
- Documents, fichiers Office
- E-Mails
- Profil et état d'enregistrement de jeux
- Codes source de programmes et sites Internet
- Bases de données
- Archives et sauvegardes
- Machines virtuelles

[1] https://www.gdata.de/securitylabs/tipps-tricks/g-data-eu-ransomware-cleaner. L'outil G DATA EU-Ransomware-Cleaner est un produit émanant de la coopération de recherche en 2013 entre 28 partenaires venant de 14 pays de l'Union Européenne sous le nom d'ACDC. L'outil est également disponible sur le site de l'union eco.

[2] http://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/

[3] http://www.bbc.com/news/technology-28661463

[4] http://news.softpedia.com/news/ransomware-reaches-the-malware-top-3-for-the-first-time-509552.shtml

Causes et origines de l'augmentation des activités liées aux Ransomware

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 disposer 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

Les Ransomware n'ont pas de vecteurs de diffusion spécifiques comparés aux autres types de malware.

La majorité des Ransomware est envoyée par spams. Les emails sont camouflés dans des factures (par exemple avec *Locky*)[5], ou si des entreprises sont ciblées, en tant qu'email de candidature au format PDF (par exemple avec *Petya*)[6]. Les 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 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 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).

A côté de ces vecteurs de diffusion courants, les Ransomware comme par exemple *Samsam* attaquent des serveurs insuffisamment protégés par l'exploitation de vulnérabilités ou l'attaque par force brute de mots de passe faibles. Les Ransomware se diffusent également dans les vulnérabilités des programmes de prise de contrôle à distance de l'ordinateur. Ces vecteurs d'infection touchent en premier lieu les utilisateurs dans les entreprises.

> *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

Des Ransomware spécialisés dans les réseaux d'entreprises ne se contentent pas - après intrusion - de chiffrer des données sur les postes locaux. Ils chiffrent également les partages réseaux. Dans le cadre

[5] https://blog.gdatasoftware.com/2016/02/25209-encryption-trojan-locky-what-you-need-to-know-about-the-ransomware
[6] https://blog.gdatasoftware.com/2016/03/28213-ransomware-petya-encrypts-hard-drives
https://blog.gdatasoftware.com/2016/03/28226-ransomware-petya-a-technical-review

d'une attaque ciblée, les attaquants essayent de voler les données d'un compte administrateur. Ils peuvent ainsi chiffrer tous les partages et prendre en otage le réseau entier.

Les attaquants ne reculent pas devant des infrastructures critiques. Par exemple, en 2016, l'établissement Hollywood Presbyterian Hospital a été paralysé grâce au logiciel malveillant *Locky* et la somme de $17.000 extorquée[7].

Bilan

Les Ransomware sont des modèles très rentables. L'étude[8] d'une seule adresse Bitcoin en relation avec *CryptoLocker,* a montré des transactions à hauteur de 1 100 000 $ (1 226 Bitcoins), répartis sur 771 rançons extorquées en un seul jour !

Pour les victimes, il n'existe normalement aucune chance de restaurer les données chiffrées – sauf par le paiement de la rançon. Mais il n'existe également aucune garantie de recevoir la clé de déchiffrement des données après le paiement.

Dans certains cas, des chercheurs réussissent à concevoir un outil de déchiffrement, soit par retro-ingénierie du code malveillant, soit par analyse des serveurs dans le cas d'une action judiciaire. Mais sur les 200 familles de Ransomware recensées par Hunter Team[9], 80 de ces familles[10] ne permettront pas de restaurer les données. Dans ce cas, seule une sauvegarde permettra de récupérer les données.

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.

[7] https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/
[8] http://miki.it/pdf/thesis.pdf
[9] https://id-ransomware.malwarehunterteam.com/index.php?lang=fr_FR
[10] https://twitter.com/demonslay335/status/759462184141328385

- Après un accès écriture, le type des fichiers et l'entropie de ceux-ci se modifient.
- La modification de la terminaison des fichiers (par ex: de .docx en .locky)
- 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.

Optimiser le niveau de protection de son réseau d'entreprise

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

- Utilisation d'une solution de sécurité Endpoint multicouche à administration centralisée.
  - Etre 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'entrées 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.