© depositphotos, zephyr18

Les ransomwares: la bourse ou la vie

Nous avons déjà tous entendu l'histoire d'un ami ou d'un collègue qui s'est retrouvé devant son ordinateur avec un message lui disant que toutes ses données ont été cryptées et qu'il n'a que quelques heures pour payer une rançon. Ce type d'attaques s'appelle un ransomware (rançongiciel en français) et affole autant les particuliers que les gouvernements, car elles sont devenues l'arme de prédilection du cybercrime.

Steven Meyer

C'est peut-être difficile à imaginer, mais le premier ransomware de l'histoire est apparu il y a 30 ans. Il contaminait les ordinateurs par disquette puis demandait une rançon de $ 189 payable à une boîte aux lettres au Panama.

Depuis le monde a changé: plus de 88% de la population suisse est connectée à internet et la majorité de notre vie s'est digitalisée. Que ce soit dans notre environnement privé ou professionnel, nous utilisons des ordinateurs pour stocker nos documents, faire nos achats, exécuter nos payements et garder les souvenirs qui nous sont chers.

Les criminels ont eux aussi évolué et se sont digitalisés. Les attaques sur les systèmes informatiques sont passées, en quelques années, de jeunes hackeurs qui essaient de découvrir les nouvelles technologies au crime organisé et à la mafia qui en ont fait leur business le plus rentable.

Historiquement, les criminels s'intéressaient à voler des informations dans les entreprises: les brèches de confidentialité sont coûteuses pour les victimes et l'espionnage industriel est très rentable une fois les données dans les mains des concurrents. Mais les grandes entreprises se protégeant de mieux en mieux, les cibles faciles sont devenues les privés et les PME. Les criminels ont donc dû trou-

ver une façon de rentabiliser un hack d'un ordinateur privé, d'un ordinateur qui n'a rien de confidentiel et qui n'a de valeur que pour son propriétaire.

C'est à ce moment-là que les criminels ont eu une nouvelle idée: voler les données et les revendre au propriétaire. Ils ont donc ressorti de leur arsenal des années 80 le ransomware.

Les technologies qui ont créé les ransomwares

Bien évidemment, il n'est plus envisageable de hacker un ordinateur avec une disquette et de demander un paiement via une boîte aux lettres. Grâce aux nouvelles technologies, il est maintenant possible d'industrialiser le processus de distribution, d'infection et de paiement. Trois ingrédients essentiels permettent à ces attaques de faire son œuvre destructrice.

Les monnaies intraçables

Pour commencer, il faut remplacer le moyen de paiement par une méthode offrant de l'anonymat. En 2006, les criminels demandaient aux victimes de payer via des formulaires sur des sites web ou avec des cartes iTunes, mais très vite ils ont découvert la limite de ces méthodes de transaction et les forces de l'ordre bloquaient très rapidement les transferts. Quelques années plus tard, la blockchain est venue à la rescousse des hackeurs en leur apportant le bitcoin, cette monnaie anonyme et digitale permettant de faire le transfert d'argent rapide à travers le monde à moindres frais sans que ce soit facilement traçable ou révocable.

Les algorithmes cryptographiques

Le premier ransomware de 1989 remplaçait simplement un fichier de configuration perturbant ainsi le fonctionnement normal du système d'exploitation. Mais ce genre d'attaque est complètement inefficace sur un système moderne. Effacer ou détruire les données n'est pas une option non plus, car il n'y aurait pas moyen de les retourner une fois la rançon payée. La meilleure solution que les hackeurs ont trouvée était donc de crypter les données, afin qu'eux seuls puissent les restaurer une fois la rançon versée. Mais crypter correctement des données n'est pas banal et les premiers ransomwares cryptographiques contenaient beaucoup de bugs qui permettaient aux victimes de récupérer leurs données sans payer. Vers le milieu des années 2000, les hackeurs se sont donc tournés vers des librairies et programmes cryptographiques créés par des professionnels, qui sont finalement devenus open source, afin que leur code fonctionne correctement et que seule la possession de la clef secrète permettait de récupérer les informations.

Les serveurs anonymes

Le ransomware doit pouvoir communiquer avec un serveur pour lui transmettre la clef secrète de cryptage, et permettre à la victime de communiquer avec le hackeur afin de recevoir la clef de décryptage. Mais ces communications restaient très risquées sur l'open web (l'internet que nous utilisons tous les jours) et les forces de l'ordre pouvaient saisir le serveur et le nom de domaine des hackeurs, interrompant ainsi l'opération d'escroquerie. En 2014, le projet TOR, qui est spécialisé dans les connexions anonymes à internet, a lancé un nouveau projet: le TOR hidden service. Ce service permet non seulement de cacher l'identité de la personne qui visite un site web, mais aussi de cacher l'identité (l'adresse IP) du service web en question. Grâce à cet outil, les serveurs des hackeurs deviennent anonymes, ces derniers agissant dès lors en toute impunité sans risquer de se faire découvrir par la police.

C'est grâce à ces trois ingrédients principaux que les ransomwares sont devenus si efficaces et populaires auprès des hackeurs.

Les ransomwares ont continué à évoluer pendant les dernières années. Il y a dix ans, ils ne cryptaient que le dossier «Mes documents» sur l'ordinateur local. Maintenant ils cryptent tous les documents et images se trouvant sur le système et le réseau, se propagent d'un ordinateur à l'autre, et détruisent même les backups afin d'empêcher une restauration sans payer.

Les finances derrière ce fléau

L'efficacité des ransomwares a surpris tout le monde et les hackeurs eux-mêmes. Eux, qui pensaient avoir trouvé une façon de rentabiliser leurs attaques sur les PME et les privés, se sont rendu compte que c'était parfois même plus rentable d'utiliser un ransomware que des attaques traditionnelles sur les infrastructures d'entreprises ou de gouvernements. Certes, un hackeur pourrait probablement se faire plus d'argent en vendant des secrets de

RECOMMANDATIONS

Depuis le début de l'année 2019, de nombreuses PME et grandes entreprises en Suisse et à l'étranger ont signalé que leurs données avaient été chiffrées et rendues inaccessibles par des chevaux de Troie appelés rançongiciels.

En raison des menaces actuelles, MELANI tient à mettre en garde une nouvelle fois les entreprises suisses contre les rançongiciels et leur recommande de prendre au plus vite les mesures suivantes:

- Veillez à effectuer régulièrement des sauvegardes de vos données, par exemple sur un disque dur externe. Procédez selon un plan de rotation (sauvegardes quotidiennes, hebdomadaires, mensuelles [méthode grand-père – père – fils], minimum de deux générations). Après la sauvegarde, veillez à déconnecter physiquement de l'ordinateur le support contenant les données sauvegardées, sans quoi ces données pourront également être verrouillées et rendues inutilisables en cas d'infection de l'ordinateur par un rançongiciel.
- Si vous utilisez une solution de sauvegarde en nuage, assurez-vous qu'elle propose au moins deux générations, de manière analogue à une sauvegarde classique. L'accès à ces sauvegardes doit être tout particulièrement protégé, par exemple avec un deuxième facteur d'authentification.
- Il convient de toujours garder à jour son système d'exploitation et toutes les applications (p.ex. Adobe Reader, Adobe Flash, Java, etc.) installées sur sa machine de manière automatique lorsque cela est possible.
- Protégez toutes les ressources accessibles depuis internet (par ex. serveur de terminal, RAS, accès VPN, etc.) avec un deuxième facteur d'authentification.
- Bloquez la réception de courriels contenant des fichiers dangereux sur votre passerelle de messagerie, ceci comprend également les fichiers Office avec macros. Vous trouverez des informations détaillées sur la page suivante, en bas:

www.melani.admin.ch/rancongiciels

production à un concurrent, mais ce genre d'opération demande beaucoup plus d'effort et de travail qu'un ransomware.

Actuellement, toutes les 14 secondes une compagnie se fait attaquer par un ransomware et d'ici fin 2019, les hackeurs auront escroqué plus de $ 11 milliards à travers cet outil. Ceci représente une augmentation de plus de 300% d'année en année.

Le prix à payer pour une rançon varie. Dans la majorité des cas, le hackeur qui demande la rançon n'est pas celui qui a écrit le programme. En effet, il existe des milliers de familles de ransomware que des hackeurs peuvent acheter pour ensuite les utiliser pour infecter leurs victimes. C'est donc au hackeur de décider quel est le prix qu'il va exiger à la victime de payer pour libérer ses documents. Ce montant commence à une centaine de dollars et peut monter jusqu'à près de 10 millions. En moyenne, un ransomware demande à une PME (qui représente 71% des victimes) $ 116 000.

La première question que se pose une victime lorsqu'elle découvre que ses données sont en otage est si elle va devoir payer ou non. Et cette décision dépend de beaucoup de facteurs et engendre de nombreuses conséquences.

Tout d'abord, il faut savoir si les données sont récupérables sans payer: est-ce que la victime à un backup récent. Sans ce backup, elle sera probablement obligée de payer si elle veut pouvoir continuer à travailler sur ses données. Dans certains cas, ce n'est pas nécessaire, mais les dommages pour une société de devoir recommencer à zéro sont conséquents et risquent même de la mettre en faillite. Et même lorsqu'une compagnie a un backup, faire la restauration des données peut s'avérer plus cher que la rançon. Rien qu'en 2019, nous avons vu plusieurs cas intéressants: Norsk Hydro a refusé de payer la rançon et la facture pour rétablir ses systèmes est montée à plus de $ 57 millions. La ville de Baltimore a également refusé de payer $ 57 000 et la facture de rétablissement ascende maintenant les $ 18 millions. D'autres villes comme Riviera Beach (Floride) ont décidé de payer une rançon de $ 600 000. Et dans la grande majorité des cas, fort heureusement, les hackeurs libèrent les données une fois la rançon payée. Pour l'instant…

Mais il reste quand même la question morale lorsqu'on paye, car en payant, on encourage les hackeurs à continuer. En tant que ville, pouvons-nous donner l'argent des contribuables à des criminels? Est-ce qu'une ONG ou une œuvre de charité peut utiliser l'argent des donateurs pour payer un criminel? En plus, dans certains cas, les hackeurs se trouvent dans des pays avec lesquels il est illégal de «faire des affaires», notamment la Corée du Nord. Il y a, en effet, de nombreux ransomwares qui émanent de la Corée du Nord dont certains sont soutenus par le gouvernement lui-même.

Dans certains cas, il est possible de négocier avec les hackeurs pour diminuer la rançon. Si cela devait vous arriver, il faut absolument tenter de négocier. La majorité des ransomwares ont une hotline (si, si, comme un vrai business avec une permanence 24/7 et dans une ou plusieurs langues) avec laquelle on peut discuter. L'expérience démontre que de telles négociations peuvent réduire la rançon d'environ 30%.

Les vecteurs d'attaque

Plus de 90% des cyberattaques commencent par un e-mail. Souvent, il s'agit de documents Office ou PDF qui vont introduire un code malveillant dans l'ordinateur, ou encore des liens vers des sites web qui vont ensuite télécharger le ransomware. Mais il existe de nombreux vecteurs d'infection: tels que des ordinateurs ou firewalls mal configurés qui laissent une porte ouverte permettant au hackeur d'entrer, ou bien encore des ordinateurs pas mis à jour qui ont des vulnérabilités facilement utilisables pour infecter la machine. Certains sites web grand public peuvent avoir des publicités malveillantes qui déploient le ransomware à tous les visiteurs, ou encore des clefs USB, ordinateurs personnels, smartphones qui peuvent être utilisés pour propager le virus, etc. Les hackeurs sont très créatifs et trouvent régulièrement de nouvelles méthodes d'infection.

Connaître le vecteur d'infection est très important, car, non seulement cela permet d'expliquer à d'autres les méthodes et techniques des hackeurs, mais surtout cela permet à la victime de fermer la brèche afin de ne pas se refaire infecter une nouvelle fois de manière identique.

Ce n'est pas une fatalité

Il existe, fort heureusement, des méthodes pour se protéger et se prémunir d'un ransomware. Avoir un bon antivirus (investir de l'argent peut s'avérer très rentable) permet de détecter et bloquer un ransomware. Les plus récents utilisent de l'intelligence artificielle et des moteurs spécialement développés contre ce type d'attaque afin d'empêcher le cryptage. Une bonne protection des e-mails (communément appelé antispam) permet de bloquer l'attaque avant même que celle-ci n'arrive sur votre ordinateur grâce à des outils de sandboxing et de désarmement; et un bon firewall peut empêcher le ransomware de communiquer avec l'extérieur et donc avec le hackeur. Bien évidemment il faut faire un backup. Celui-ci ne permet pas de prémunir l'attaque, mais permet, lorsqu'il fonctionne correctement, de récupérer ses données sans payer de rançon.

Avec les ransomwares, il n'y a plus personne qui est à l'abri des hackeurs, car ces derniers ont trouvé une façon de vous revendre les données que vous avez créées et de vous redonner accès à des appareils que vous avez achetés. Les victimes sont aujourd'hui autant les privés, les PME, les multinationales que les centres médicaux ou les gouvernements. Et plus notre société et notre environnement se digitalise, plus les hackeurs verront une opportunité pour nous attaquer: nous verrons bientôt des maisons domotisées se faire prendre en otage, le chauffage coupé en plein hiver, des voitures qui ne démarrent plus avant des rendez-vous importants et peut-être même des stimulateurs cardiaques qui menacent d'une crise cardiaque si la rançon n'est pas payée.

C'est donc une responsabilité commune des constructeurs de matériels, développeurs de solutions, administrateurs de systèmes informatiques, directeurs d'entreprises et utilisateurs d'ordinateurs de s'assurer d'avoir suivi les meilleures pratiques afin de ne pas être de prochaines victimes. ■

STEVEN MEYER

Expert reconnu et référent suisse en cybersécurité auprès de nombreuses institutions, médias et entreprises, il est aussi le co-fondateur de ZENData, un des leaders romands dans les solutions, audits et formations en protection digitale.