Une prise d'otage de vos données ou ransomware
Une rançon en échange de vos données informatiques

Un ransomware, ou rançongiciel, est un 'virus' dont l'objectif est de prendre en otage vos données en échange d'une rançon. Les ransomwares se propagent le plus souvent par email sous forme d'un exécutable présent dans une pièce jointe. Si par malheur vous exécutez ce programme ce dernier va infecter votre ordinateur et se propager sur le réseau local. Très rapidement tous les fichiers importants présents sur l'ordinateur infecté vont être chiffrés (on parle souvent de 'cryptage' par abus de langage) et devenir inexploitables. Vous devrez payer une rançon aux 'pirates' pour pouvoir récupérer vos données, mais rien n'est garanti...

Le phénomène n'est pas nouveau, les ransomwares existent depuis 1989. Il en existe de tous types, dont le principe est de soutirer de l'argent en échange d'un accès à son propre ordinateur ou à ses propres données ! Certains d'entre eux, comme "Reveton", se font également passer pour des autorités gouvernementales, type FBI, et vous annoncent que vous devez payer une amende pour récupérer vos données... Les "Winwebsec" sont également une forme de ransomware, il s'agit de faux antivirus que l'on vous propose de télécharger à partir d'une fenêtre de navigateur vous faisant croire lors d'un surf que votre pc est infecté.

Cependant depuis quelques mois, les ransomwares sont de plus en plus présents et surtout extrêmement perfectionnés. Certains d'entre eux, dont les plus dangereux "CryptoLocker" (et ses variantes) et la famille des "ACCDFISA", chiffrent les données à tel point qu'il est actuellement impossible de les déchiffrer sans la clef. CryptoLocker a infecté environ 234 000 utilisateurs dans le monde, il est considéré par le CERT US comme étant très dangereux: http://www.us-cert.gov/ncas/alerts/TA13-309A .

Certaines versions de ransomwares sont capables de chiffrer non seulement les fichiers locaux, mais également les fichiers stockés, les clés USB, les disques durs externes et les fichiers partagés. Les sauvegardes externalisées peuvent aussi être compromises si elles synchronisent parfaitement les données locales, il est donc important d'utiliser une sauvegarde intégrant du versioning [Cf. Conseil 1].

Cas 1 : Principe de fonctionnement et détails de CryptoLocker

CryptoLocker est essentiellement diffusé par des emails de phishing. Les emails en question apparaissent comme des notifications ou des pseudos factures provenant d'UPS, DHL, FedEx ou de banques américaines. Ces emails comportent le plus souvent une pièce jointe au format ZIP renfermant un programme exécutable qu'il ne faut surtout pas lancer sans l'avoir analysé [Cf. Conseil 7]. Pour tromper l'utilisateur, le fichier comporte souvent une double extension, permettant de cacher l'extension principale (un fichier nommé "facture.pdf" peut ainsi être un exécutable, car son vrai nom est: "facture.pdf.exe" mais votre système vous cache sa vraie extension [Cf. Conseil 8]). D'autre part, le programme incorpore l'icône par défaut qui reprend l'apparence de l'icône utilisée pour le type de fichier correspondant à l'extension fictive. Dans notre exemple précédant, l'icône de présentation de l'exécutable reprendrait l'icône habituellement utilisée pour les fichiers PDF.

Pour chiffrer vos fichiers, CryptoLocker génère une biclef RSA sur 2048 bits, la clef privée sera envoyée sur le serveur du pirate pour permettre un déchiffrement ultérieur, la clef publique est quant à elle utilisée pour chiffrer les photos, les vidéos et les documents présents sur votre disque et sur les lecteurs partagés directement comme lecteur externe. Le chiffrement est fait avec l'algorithme AES-256 assurant une parfaite étanchéité contre le décryptage brut-force. Après chiffrement des données, CryptoLocker vous laisse 72 à 100 heures pour envoyer la rançon (généralement autour de $300), passé ce délai le montant sera très significativement augmenté (*10 env).

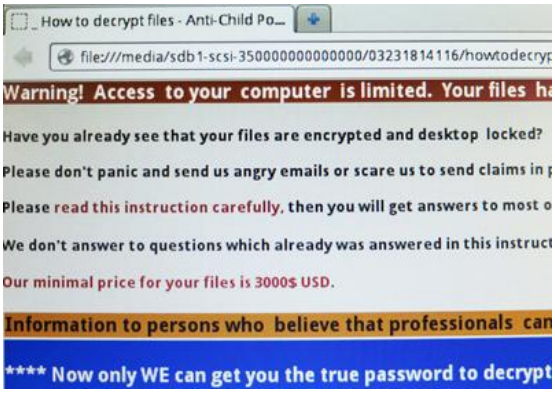
Bien que démantelé début juin 2014 par le FBI, le botnet "Gameover Zeus" qui utilisait la technologie P2P pour construire un botnet d'ordinateurs zombies et servant de base à la propagation du malware CryptoLocker, vient de renaitre en utilisant la technique dite de "fast-flux hosting" sous le nom: "Try Again Zeus" : http://blog.emsisoft.com/2014/07/11/gameover-zeus-decides-to-try-again/ .

D'autre part des imitations comme "CryptoLocker 2.0", "CryptoDefense", "CryptoWall" et "CryptorBit" sont également très dangereuses et toujours actives. L'architecture, le moyen de propagation, les langages utilisés et/ou les moyens de chiffrement diffèrent légèrement d'un programme à l'autre, mais le principe général reste le même. Certains ransomwares comportaient quelques imperfections permettant un décryptage, mais ils ont été rapidement corrigés.

Vous trouverez plus de détails sur CryptoLocker sur le site : http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

Cas 2 : Les ACCDFISA, un autre type de ransomware

Les ransomwares de type ACCDFISA pour : "Anti Cyber Crime Department of Federal Internet Security Agency" se font passer pour une organisation gouvernementale d'où leur nom et indiquent qu'ils ont bloqué vos fichiers parce que vous avez soi-disant des données pédophiles sur votre pc ! Un des plus dangereux est "Anti-child Porn Spam Protection 2.0" que nous allons détailler.



Contrairement à la plupart des logiciels malveillants, "Anti-child Porn Spam Protection 2.0" n'utilise pas les attaques de phishing pour se propager et infecter le système cible. La propagation de ce malware se fait par l'intermédiaire du protocole RDP [Cf. Conseil 4], le plus souvent détecté suite à des "scans sauvages" de vos IP et des attaques de type brut-force via le protocole d'accès à distance RDP avec des comptes bien précis couramment utilisés comme notamment : 123, adm, admin, Administrator, backup, Guest, scanner, support, test, user, ... ou par l'intermédiaire d'une faille de sécurité présente sur le système distant [Cf. Conseil 3].

Dans le cas d' "Anti-child Porn Spam Protection 2.0" les fichiers sont chiffrés en AES-128 à l'aide d'une version customisée du logiciel de compression WinRAR en mode auto-extractible. Un premier chiffrement des données est fait à l'aide d'une clef symétrique combinant une chaîne de 50 caractères générée aléatoirement et d'une chaîne statique. La chaîne aléatoire est temporairement stockée dans un fichier local, envoyée sur le serveur des pirates pour permettre un déchiffrement et enfin supprimée à l'aide d'une routine intégrée de type 'broyeur' rendant la récupération du fichier d'origine impossible. Après cette première phase de chiffrement, un second mot de passe comportant entre 80 et 114 caractères est généré pour chiffrer une seconde fois les fichiers. Cette seconde clef est conservée en local et pourrait éventuellement permettre un déchiffrage, mais la récupération de la première clef est quasi impossible.

Les pirates qui se cachent derrière ce ransomware réclament entre $3000 et $4000 minimum en précisant clairement que ce ne sera jamais moins même si vous n'avez besoin que d'un seul fichier.

Plus de détails sur les ransomwares de la famille ACCDFISA sur le site : http://blog.emsisoft.com/2012/04/11/the-accdfisa-malware-family-ransomware-targetting-windows-servers/

Comment éviter de se faire infecter ?

Maintenant que nous avons mis en évidence les désastres que peuvent causer ce type de 'virus', voici quelques conseils pour éviter d'en subir les frais. Étant donné que dans la plupart des cas, le mal arrive par un email, l'idéal est de ne pas recevoir le message infecté. D'où l'importance d'avoir un bon antivirus en amont capable de détecter les virus intégrés dans les fichiers joints [Cf. Conseil 2], mais également sur votre poste pour éviter les contaminations par d'autres moyens. Mais comme aucun système n'est infaillible, le plus important est d'avoir une sauvegarde, cela arrive donc en tête de notre liste de conseils. La population concernée est indiquée entre crochets.

Conseil 1 : [Administrateur] Utiliser un service de sauvegarde gérant le versioning, de préférence externalisé pour limiter les risques de propagation de malware par le réseau. Il est important de pouvoir revenir sur d'anciennes versions d'un fichier.

Conseil 2 : [Administrateur] Être équipé d'un bon antivirus, réalisant des mises à jour très régulièrement et positionné si possible en amont de votre serveur de messagerie. A titre indicatif, ALTOSPAM intègre 5 antivirus en série, et procède automatiquement à une vérification des pièces jointes suspectes auprès de son partenaire VirusTotal, cela garantit à ses clients une protection de très haut niveau contre ces ransomwares. Détails sur: http://www.altospam.com/actualite/2014/02/la-forteresse-daltospam-les-malwares/

Il semble que certaines versions de ransomwares soient également envoyées par mail dans des pièces jointes au format "ZIP chiffré" pour lesquels le correspondant vous donnera le mot de passe dans le corps du mail. Attention, dans ce cas, les antivirus ne peuvent pas faire leur travail, soyez d'autant plus vigilants !

Conseil 3 : [Administrateur] Avoir son système et ses applications à jour. Les mises à jour de sécurité doivent être appliquées au plus tôt sur les systèmes d'exploitation. Certains ransomwares exploitent des failles Microsoft par exemple.

Conseil 4 : [Administrateur] Éviter tout accès distant non utile. RDP (Remote Desktop Protocol) utilisé notamment par "Anti-child Porn Spam Protection 2.0" est un protocole qui permet à un utilisateur de se connecter à distance sur un ordinateur, le port utilisé par défaut est TCP/3389. Si un compte est compromis, l'accès à votre réseau sera aisé.

- L'accès ne doit pas être possible depuis Internet, s'il est nécessaire modifier le port par défaut et/ou limiter l'accès à certaines IP spécifiques,

- vérifier les comptes possédant des droits d'accès au bureau à distance et ne conserver que ceux réellement utiles, tous n'ont pas nécessairement besoin de cet accès. Supprimer tous les comptes inutiles, comme "guest", "test", "user", ...

- les mots de passe utilisateur doivent tous être suffisamment robustes (avec minuscules, majuscules, chiffres, signes et faire au moins 12 caractères), surtout pour les comptes possédant des droits d'accès à distance.

Conseil 5 : [Administrateur] Sensibilisez vos utilisateurs aux problématiques de sécurité et à ce type de risque, notamment en communiquant les conseils ci-dessous précédés de la mention [Utilisateurs].

Conseil 6 : [Utilisateurs] Être vigilant concernant les liens présents dans les emails, ne pas cliquer inopinément. Vérifier toujours par exemple que l'URL écrite correspond bien à l'adresse de redirection et que le site est correctement orthographié.

Conseil 7 : [Utilisateurs] Être très vigilant et suspicieux vis à vis des pièces jointes, y compris ceux de vos interlocuteurs connus (qui ont pu se faire pirater leur compte). Faire très attention aux fichiers ZIP présents dans les emails; tester l'archive à l'aide d'un analyseur multi-scanners en ligne comme http://www.virustotal.com (scan automatique intégré à Altospam)

Conseil 8 : [Utilisateurs] Pour éviter tout abus lié aux extensions des fichiers, nous vous conseillons de configurer votre explorateur de fichiers avec l'affichage systématique des extensions. Pour cela, dans votre explorateur de fichiers, cliquez sur : Organiser / Options des dossiers / Affichage / Décocher : Masque les extensions des fichiers dont le type est connu.

Mais que faire en cas d'infection ?

Surtout ne pas payer la rançon, pour plusieurs raisons : d'une part il ne faut jamais céder au chantage et, malgré la rançon, il n'existe évidemment aucune garantie de récupérer vos données après avoir payé. D'après les forums certains utilisateurs confirment avoir payé sans recevoir la clef de déchiffrement, d'autres indiquent que tous les fichiers n'ont pas pu être déchiffrés.

1. Débrancher immédiatement le câble réseau et déconnecter tous les réseaux,

2. Porter plainte auprès d'un ESCI (Enquêteur Spécialisé sur la Criminalité Informatique) de votre SRPJ local (Service Régional de Police Judiciaire),

3. Supprimer le malware : demander à un professionnel ou rechercher sur Internet des outils ou procédures pour supprimer le virus,

4. Modifier tous vos mots de passe, sur votre système, votre réseau, mais également tous vos mots de passe en ligne si possible,

5. Vérifier l'ensemble de votre parc informatique, comprendre comment le malware est entré et faire le nécessaire pour sécuriser votre entreprise.

Si vous décidiez de céder au chantage et de payer la rançon, dans ce cas ne supprimez rien, ne touchez à rien sur le PC infecté, ne lancez pas d'antivirus, vous risqueriez de compromettre la procédure de déchiffrement.

Si un de ces malwares est détecté sur votre poste, mais que vos données ne sont pas encore chiffrées, surtout ne redémarrez pas votre poste, il existe des outils capables de l'éradiquer, en voici une liste concernant CryptoLocker : https://www.us-cert.gov/ncas/alerts/TA14-150A

En conclusion, quelle est la valeur de vos données ? Votre entreprise survivrait-elle si elle perdait l'ensemble de ses données informatiques du jour au lendemain ? Que pourriez-vous faire pour sécuriser d'avantage vos données et celles de votre entreprise ?

Attention, il existe aussi désormais des ransomwares sous Android alors, même avec votre téléphone soyez prudent !