الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي
خ ا م

LETTRE D'INFORMATION : BON A SAVOIR (N°15)

Génération Ransomware 2016 : Le top 6 des derniers nés et comment vous en protéger

Qu'est-ce qu'un ransomware ?

Le ransomware (ou rançongiciel en français) correspond à une catégorie particulière de logiciels malveillants qui en cas d'infection, bloquent tout ou partie de votre ordinateur et réclament le paiement d'une rançon dans un délai imparti généralement en bitcoins (monnaie électronique).

En clair, non seulement votre ordinateur est pris en otage mais surtout, le paiement de la rançon ne garantit en rien la récupération saine et sauve de votre machine et de son précieux contenu.

Dans la majorité des cas, les données passées aux mains de l'attaquant sont perdues de manière irréversible.

Les différents visages du ransomware

Il y a deux types de ransomwares :

Les ransomwares classiques dit « policiers » qui se figent votre navigateur (appelés Browlock) ou paralysent entièrement votre ordinateur.

La deuxième catégorie de plus en plus répandue et probablement la plus néfaste est celle des « Crypto-ransomwares » ou « cryptowares ». Le logiciel malveillant va chiffrer les documents contenus sur votre ordinateur les rendant illisibles sans la clé de déchiffrement détenue par le pirate qui exige alors une rançon en échange de cette clé.

Les modes d'infection des ransomwares :

- Un e-mail frauduleux (dans lequel se trouve une pièce jointe infectée),
- Un site internet compromis ou malveillant,
- Une installation de logiciel de source non fiable,
- Les réseaux sociaux (qui facilitent le social engineering),

Les derniers nés de la génération ransomware :

Locky n'épargne personne

Locky est un crypto-ransomware qui fait beaucoup parler de lui depuis le mois de février. Il se répand actuellement comme une traînée de poudre dans toute l'Europe, principalement au travers de macros malicieuses dans un document Word, généralement transmis à la victime lorsque cette dernière télécharge la pièce jointe d'un email malveillant. Il chiffre les fichiers sur le poste de travail et parfois sur un réseau entier.

Par ailleurs, il évolue chaque semaine en utilisant de nouvelles méthodes de propagation. Par exemple, certains groupes favorisent la propagation du malware en payant des individus spécialistes en exploitation de failles de sécurité. Ces derniers utilisent des vulnérabilités, notamment 0day, pour prendre le contrôle de l'ordinateur et installer Locky sur le poste.

CTB Locker, un nouvel adversaire sur mesure

CTB-Locker est également un crypto-ransomware découvert en février de cette année et cible toutes les versions de Windows sans exception (à partir de Windows XP). Le ransomware se propage principalement par email piégé, mais aussi via des sites webs compromis ou malveillants. Les campagnes d'emails frauduleux en question sont efficaces car elles ciblent un groupe d'utilisateurs particulier pour lequel les messages sont personnalisés (dans la langue de l'utilisateur notamment) et donc plus percutants qu'un email standardisé et envoyé en masse.

Une fois exécuté, il parcourt en silence dans l'arrière-plan de votre machine, l'ensemble des disques durs et des partages réseaux, s'empare d'une liste de fichiers (documents office, images, textes etc.) et les place dans une archive chiffrée protégé par mot de passe.

Afin de ne pas être détecté par les experts sécurité des entreprises, CTB-Locker est doté d'un mécanisme d'anti-debugging, qui lui permet de repérer et donc de ne pas s'exécuter sur les machines virtuelles utilisées par les experts en sécurité pour analyser les malwares. Enfin, le ransomware démontre une versatilité inquiétante, avec plusieurs variantes détectées à son actif dont la dernière, une variante serveur découverte par un de nos experts Stormshield.

TeslaCrypt, le ransomware qui cache bien son jeu

Le ransomware analyse votre ordinateur, sur l'ensemble de vos lettres de lecteurs, à la recherche de vos fichiers de données. Il ignore Windows lui-même et les applications pour permettre à l'ordinateur de continuer à fonctionner afin d'aller sur Internet et payer la rançon.

Les fichiers de données sont chiffrés en utilisant un chiffrement AES. Le chiffrement AES étant l'un des plus robustes, il assure au hacker un contrôle total sur les fichiers sans aucune chance pour la victime de pouvoir récupérer ses fichiers en clair. Certaines versions de ce malware ciblent particulièrement les PC des gamers. Son mode d'infection est multiple mais se fait en grande majorité par des emails ou des exploits kits.

Petya, encore plus agressif que Locky

Ce ransomware est encore plus agressif que Locky puisqu'en plus de chiffrer les fichiers, Petya va lui chiffrer les premiers secteurs du disque système ; empêchant alors le système d'exploitation de l'ordinateur de se charger. Il rend donc totalement inutilisable l'appareil ciblé. Cette agressivité démontre encore une fois l'aspect lucratif de ce type de malwares. Le prétexte utilisé pour infiltrer les disques durs est, par exemple, un CV envoyé par email au département des ressources humaines d'une entreprise. Si le réseau est infecté, l'ordinateur est totalement inutilisable. Tant que la rançon n'est pas payée, avec une issue qui reste incertaine, les informations de l'entreprise sont condamnées.

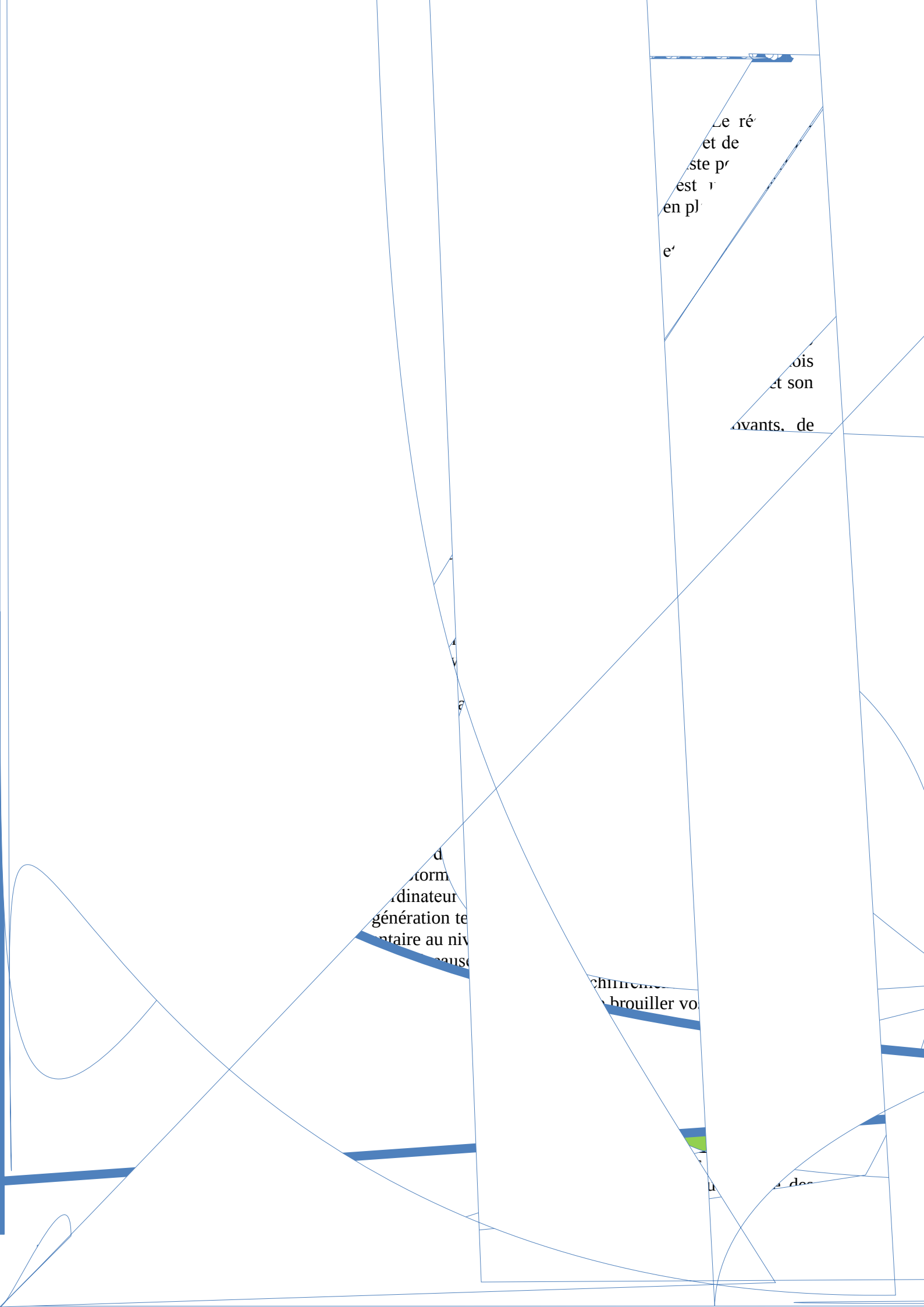
Samsam déterre le Hash de guerre

La particularité de ce nouveau cryptoware est l'utilisation de la technique dite « Pass the Hash », qui constitue un réel danger pour la sécurité des réseaux d'entreprise. Les pirates informatiques utilisent cette technique pour contourner les systèmes d'authentification au serveur et accéder aux informations confidentielles et aux applications critiques. Il permet à l'attaquant, qui a réussi à compromettre un poste de travail ciblé, d'étendre son emprise sur l'ensemble des machines et du système informatique d'une entreprise. Ce mécanisme ne pouvant pas être bloqué par un anti-virus, les entreprises doivent prendre conscience de la gravité de ce type d'attaque et changer d'attitude face aux risques encourus par leur infrastructure IT.

Samsam a récemment bloqué MedStar Health, une organisation gérant une dizaine d'hôpitaux dans le Maryland et l'état de Washington Au total, 45 bitcoins ont été demandés pour déverrouiller tous les systèmes affectés, soit environ 18.500 $.

Cerber, la dernière bête noire de la communauté cybersécurité

Cerber est ce qu'on appelle un Ransomware As A Service (RaaS), bien que ce ne soit pas le seul, c'est une tendance qui pointe le bout de son nez et qui va en s'intensifiant. Désormais,



n'ont plus besoin de mules pour convertir ou « blanchir » l'argent sale obtenu grâce aux ransomwares.

- Le côté obscur du Web est de plus en plus organisé et spécialisé. Voyez-le comme « l'industrialisation des malwares ». Plutôt que d'avoir une seule équipe s'occupant de tous les développements, il existe maintenant différents groupes se focalisant uniquement sur certaines techniques (botnets, vente de failles, chiffrement, etc.). Les forums parallèles et les marchés noirs en ligne fournissent les outils nécessaires aux cybercriminels pour développer des ransomwares. Ces outils incluent de nombreux kits « Do It Yourself » qui permettent de créer son propre malware, même sans connaissances techniques spécifiques, comme le cas du cryptoware Power Locker.

Bogdan Botezatu, Analyste Senior en E-menaces chez Bitdefender souligne : « *Nous voyons de plus en plus d'infections par des ransomwares. Les ransomwares sont hautement polymorphes et les cybercriminels les modifient régulièrement pour échapper à toute détection.* »

Menaces de sécurité sur PC : les ransomwares gardent la tête du classement

Le paysage des menaces de sécurité ciblant les utilisateurs de PC se décompose en deux catégories :

- Les menaces financières, qui regroupent les « outils malveillants » qui ont pour objectif de dérober/soutirer de l'argent ou des informations concernant des comptes bancaires. Par exemple des trojans bancaires comme Dyreza et des ransomwares comme CTB Locker et Cryptowall.
- Les services malveillants, qui se focalisent sur les moyens qui permettent aux outils cités ci-dessus de faire effet. Nous pouvons y inclure : les downloaders (Upatre, Dalexis), les botnets (Pushdo, Ursnif), les proxys, les kits d'exploits.

Bien que la tendance du ransomware ne soit pas nouvelle, elle a atteint des sommets en février dernier et reste en pôle position ces derniers mois. Pour ce qui est de la catégorie des services malwares, celle-ci reste d'actualité, rendant difficile l'identification et la mise en avant de certaines tendances. Cependant, l'état actuel des services malwares peut être résumé comme suit :

- Les cybercriminels peuvent trouver et acheter sur Internet un grand nombre d'outils qui leur sont nécessaires pour lancer leur propre campagne malveillante.
  Les transactions sont généralement réalisées via Ukash, Bitcoin, Webmoney ou d'autres monnaies difficiles à suivre.
- Upatre et Dalexis sont les plus gros downloaders du marché noir actuel. Ils peuvent permettre le téléchargement de n'importe quel type de malware sur votre ordinateur, du malware dérobant des mots de passe au trojan bancaire, en passant par le ransomware.
- Les moyens les plus communs pour diffuser des malwares sont l'envoi de spams, les campagnes de phishing, les fausses publicités et les drive-by-downloads (téléchargement automatique à la visite d'une page Web). Il est intéressant de noter que la plupart de ces méthodes de diffusion n'exploitent pas les vulnérabilités, mais la bonne vieille méthode de l'ingénierie sociale, en jouant sur la curiosité de la victime.

Menaces de sécurité mobile : les ransomware à l'attaque des tablettes et smartphones

Les tendances pour les ransomwares et les FakeAV observées sur les appareils Android. Notez qu'Android reste la plateforme mobile la plus ciblée, en grande partie à cause de sa popularité (plus de 1,6 million d'applications disponibles pour plus d'un milliard d'utilisateurs).

Pour illustrer ces propos, en juin 2015 une nouvelle vague de ransomwares Android est apparue sous la forme d'une fausse mise à jour Flash Player, via plus de 15 000 e-mails de spam envoyés sur 3 jours. Le ransomware, identifié comme Android.Trojan.SLocker.DZ, demandait aux utilisateurs de payer 450 euros pour « débloquer » l'appareil contaminé. Le prix pouvait même tripler si l'utilisateur essayait de débloquer l'appareil de force.

Ransomware vs. sécurité de l'Internet des Objets (IoT)

L'aspect inquiétant de cette évolution des ransomwares mobiles est l'impact qu'elle pourrait avoir sur la sécurité de l'Internet des Objets. Vu son périmètre et ses plusieurs niveaux de connexions – application, endpoint, réseau, cloud – s'il n'est pas protégé à chaque niveau, l'Internet des Objets pourrait fournir aux développeurs de ransomwares un large choix de vecteurs et vulnérabilités dont ils peuvent tirer profit pour propager leurs malwares.

http://www.linformaticien.com/actualites/partenaires/articletype/articleview/articleid/38103/selon-bitdefender-les-ransomwares-dominent-le-paysage-actuel-des-menaces-et-cela-va-continuer.aspx

Rançongiciels, la nouvelle arme fatale des cyberpirates

Sécurité informatiqueLes prises d'otages numériques, avec demande de rançon, se multiplient. Payer est souvent la seule solution

Grâce à un mode opératoire ingénieux, baptisé «rançongiciel», les pirates informatiques soutirent des rançons.

Locky, Cryptolocker, Synolocker, Cryptowall, TeslaCrypt, Petya… Si vous n'êtes pas un spécialiste de la sécurité informatique, ces noms barbares ne vous disent probablement rien. Et pourtant, ils représentent la nouvelle menace qui pèse sur vos ordinateurs. Depuis quelques années, en effet, un nouveau type de logiciel malveillant a le vent en poupe: les rançongiciels – un néologisme 2.0 dérivé du mot «ransomware» dans la langue de Shakespeare. Ces virus prennent, à distance, le contrôle de PC, tablettes ou smartphones et bloquent l'ensemble de leurs données. Pour les récupérer, les propriétaires légitimes sont sommés de payer une rançon dans un délai très court, dans une monnaie virtuelle et non traçable comme les bitcoins.

Selon une étude d'Intel Security-McAffe, datant de mars 2016, ce type d'attaque a augmenté de 26% au dernier trimestre 2015, par rapport à l'année précédente. Un constat partagé par la centrale d'enregistrement et d'analyse suisse pour la sûreté de l'information (Melani) qui, dans un communiqué publié le 3 décembre 2015, alerte sur une «recrudescence» des infections de ce type.

Les PME ne sont pas préparées

«Les demandes de rançons après un piratage sont en plein essor dans le monde et en Suisse, résume Ilia Kolochenko, CEO et fondateur de l'entreprise genevoise High-Tech Bridge, spécialisée dans la sécurité informatique. C'est devenu une véritable industrie.»

De fait, les exemples se multiplient – proches de nous. En avril 2016 par exemple, Ralph Eberhard, patron de la gérance Immogeste basée à Genève, témoigne dans le journal L*e Temps* avoir dû payer 1800 francs à des hackers. Le même mois, un peu plus loin d'ici, dans le Béarn, le PDG d'une entreprise raconte peu ou prou la même histoire, dans le journal *La République des Pyrénées*.

En effet, à chaque fois le scénario est identique. Un matin, en allumant leurs ordinateurs, les salariés voient s'afficher sur leur moniteur un message martial, généralement rouge sur fond noir, qui dit en substance: «Tous les fichiers de votre disque dur ont été cryptés. Pour les déchiffrer et les récupérer, vous devez nous payer.» La plupart du temps, les montants exigés ne s'avèrent pas dissuasifs: de quelques centaines de francs pour des particuliers à quelques

milliers pour les PME. Mais parfois les sommes demandées sont astronomiques. En février 2016, un ransomware a infecté un hôpital de Los Angeles, bloquant l'ensemble des données médicales des patients. Pour remettre le système d'information d'aplomb, les pirates ont réclamé 9000 bitcoins, soit l'équivalent de 3,6 millions de dollars!

«Auparavant, les hackers s'attaquaient à de grosses entreprises, afin de toucher le jackpot, rappelle Ilia Kolochenko. Aujourd'hui, ils se recentrent sur les PME et les particuliers, parce qu'ils ont compris que même si les sommes obtenues sont moindres, l'activité se révèle moins risquée et plus facile. Si vous attaquez une grande banque, vous devez d'abord déjouer une sécurité informatique de premier plan. Et si vous y parvenez, vous pouvez être certain qu'elle ne vous lâchera jamais. Elle vous traquera pendant des années s'il le faut. A l'inverse, les particuliers et les PME ne sont absolument pas préparés à ce type d'attaque et en plus ne disposent pas des moyens nécessaires pour retrouver les auteurs.» Selon un rapport de Symantec publié en avril 2016, 57% de ces attaques ciblent des entreprises de moins de 250 salariés.

Mais comment ces logiciels malveillants se diffusent-ils? «Ces chevaux de Troie accèdent à l'ordinateur par le biais de courriels infectés ou de sites Internet piratés», explique la centrale Melani. Concrètement, «les hackers possèdent des robots informatiques, les botnets, qui scrollent l'ensemble des pages Internet – un peu comme Google – à la recherche de failles connues, explique Ilia Kolochenko. Lorsqu'une vulnérabilité est découverte, le virus s'installe et attend sa victime, en affichant par exemple un nouveau lien. Lorsque quelqu'un clique sur ce dernier, le virus passe sur son ordinateur et crypte l'ensemble des données.»

Faut-il payer la rançon ou pas?

Face à cette situation, la centrale Melani recommande de «ne pas céder à l'extorsion car, en payant la rançon, vous participez au financement de l'activité des criminels et leur permettez d'améliorer l'efficacité de leurs prochaines attaques. De plus, il n'existe aucune garantie que les criminels respecteront leur engagement et vous enverront réellement la clé vous permettant de récupérer vos données.»

En pratique, les choses s'avèrent plus compliquées, notamment pour les PME qui, privées de leurs fichiers clients, voient toute leur activité bloquée. «Si vous êtes infectés, il n'existe pas 3000 solutions, reconnaît Ilia Kolochenko. La première consiste à faire des recherches sur Internet, afin de savoir s'il existe déjà une clef de décryptage contre le rançongiciel. Malheureusement, c'est rarement le cas. La seconde, c'est payer. Si vous vous adressez à une entreprise comme la nôtre, nous finirons par remonter jusqu'au coupable et nous parviendrons peut-être à récupérer vos données. Mais cela va prendre beaucoup de temps. Même si cela peut paraître immoral, c'est moins coûteux pour une PME de régler la rançon que de lancer des investigations.» (24 heures)

http://www.24heures.ch/vivre/Rancongiciels-la-nouvelle-arme-fatale-des-cyberpirates/story/21034490

Le ransomware est un modèle économique criminel, et non un problème de malware

L'Unité 42 publie sa dernière analyse en date sur les ransomware, qui représentent l'une des cybermenaces les plus sérieuses auxquelles sont aujourd'hui confrontées les entreprises aux quatre coins du monde.

Véritable modèle économique, le ransomware, ou rançongiciel, se révèle extrêmement efficace pour enrichir les cybercriminels tout en causant un préjudice opérationnel significatif aux entités touchées. Il ne fait pas de distinction entre ses victimes, sévit partout dans le

monde et frappe les principaux marchés verticaux. Petites structures, grandes entreprises, particuliers : tous sont des cibles potentielles.
Si les rançongiciels existent, sous diverses formes, depuis plusieurs décennies, les criminels en ont perfectionné les principaux aspects au cours de ces trois dernières années. Résultat : les nouvelles familles de malware se sont multipliées, rendant cette technique particulièrement redoutable, et de nouveaux acteurs prennent aujourd'hui part à ces procédés très lucratifs.
Pour mener à bien une attaque de ce type, un pirate doit se conformer à la procédure suivante :
1. Prendre le contrôle d'un système ou d'un équipement.
2. Empêcher le propriétaire de l'équipement contrôlé d'y avoir accès, en partie ou en totalité.
3. L'avertir que l'accès à son équipement lui sera restitué, moyennant le versement d'une rançon, et lui préciser les modalités de règlement de celle-ci.
4. Accepter le paiement effectué par le propriétaire de l'équipement.
5. Restituer au propriétaire un accès intégral à son équipement une fois le paiement perçu.
Si le pirate néglige l'une de ces étapes, il ne parviendra pas à ses fins. Bien que le concept de ransomware existe depuis plusieurs décennies, la technologie et les techniques requises pour s'acquitter de ces cinq étapes à grande échelle étaient encore inaccessibles il y a quelques années. La déferlante d'attaques imputables à l'exploitation de cette procédure a eu des répercussions sur les entreprises du monde entier qui, pour nombre d'entre elles, n'étaient pas préparées à les esquiver.
L'Unit42 retrace l'historique des ransomware et la façon dont des pirates s'y sont pris, plusieurs années durant, pour peaufiner ce modèle économique. Nous analysons également les perspectives de ce type d'attaques, à l'aune des évolutions ci-après.

1. Multiplication des plates-formes

Les rançongiciels ont d'ores et déjà migré de Windows à Android, et un cas sous Mac OS X a été recensé. Aucun système n'est à l'abri de ce genre d'attaques, et tout équipement susceptible d'être détourné pour faire l'objet d'une demande de rançon sera une cible à l'avenir.
Ce phénomène s'affirmera encore avec l'essor de l'Internet des objets (IoT). Si un pirate est en mesure d'infecter un réfrigérateur connecté à Internet, peut-être est-il plus délicat de monnayer cette intrusion. Pourtant, le modèle économique du ransomware peut s'appliquer à ce cas de figure, et plus largement, à partir du moment où le pirate est en mesure de s'acquitter des cinq étapes citées pour mener à bien ce type d'attaque. Une fois le réfrigérateur infecté, le pirate en question pourrait parfaitement désactiver à distance le circuit de refroidissement et ne le réactiver qu'en contrepartie d'un petit pécule versé par la victime.

2. Rançons très élevées

Dans le cadre d'attaques monosystèmes de type ransomware, des rançons allant de 200 à 500 $ sont exigées, mais les montants peuvent être nettement plus élevés. Si des pirates réalisent avoir compromis un système stockant de précieuses informations, et que l'entité infectée a les moyens de payer, ils reverront à la hausse le montant de leurs exigences. Nous avons d'ores et déjà constaté ce phénomène avec plusieurs attaques ultra-médiatisées dirigées contre des hôpitaux en 2016 : les rançons acquittées dépassaient largement les 10 000 $.

3. Attaques ciblées avec demande de rançon

Une intrusion ciblée sur un réseau s'avère intéressante pour un pirate à plus d'un titre. La revente ou l'exploitation d'informations dérobées est une technique usuelle, mais qui nécessite souvent une infrastructure « back-end » supplémentaire et des préparatifs pour pouvoir les monnayer. Les attaques ciblées avec ransomware représentent un réel potentiel pour ces pirates susceptibles de ne pas savoir comment autrement monétiser leur intrusion. Une fois le réseau infiltré, rien ne les empêche d'isoler des fichiers très lucratifs, bases de données et systèmes de sauvegarde, puis de crypter simultanément l'ensemble de ces données.

De telles attaques, qui font appel au logiciel malveillant SamSa, ont d'ores et déjà été observées et se sont révélées très rentables pour les adversaires les exécutant.
http://www.globalsecuritymag.fr/Le-ransomware-est-un-modele,20160601,62556.html

Le cyber-kidnapping, nouvelle arme des hackers

Bien plus efficace que le phishing, le "rançongiciel" kidnappe l'ordinateur de la victime et l'oblige à payer une rançon pour le débloquer.

La traque aura duré plus d'un an. La police espagnole annonce, le 13 février, avoir arrêté onze personnes soupçonnées d'être des membres d'un des réseaux les plus sophistiqués en matière de cybercriminalité.

Les pirates, des Russes, des Ukrainiens et des Géorgiens, avaient créé un "super-virus", nommé Reveton, spécialisé dans le cyber-kidnapping. Ce logiciel malveillant est capable de s'infiltrer dans un n'importe quel ordinateur. Il bloque alors l'accès au PC et aux données stockées dans la machine. Lorsque l'utilisateur veut utiliser son ordinateur, un message s'affiche et demande à son propriétaire de payer une rançon, comme pour un vrai kidnapping, entre 100 et 200 euros, pour le débloquer.

Ces virus font partie de la catégorie des "rançongiciel", ou "ransomware" en anglais. Et ils sont devenus l'arme préférée des cybercriminels.

Le subterfuge parfait

Selon le rapport annuel sur la cybercriminalité de Symantec, chaque seconde, 18 internautes sont victimes de piratage dans le monde, soit plus d'un million et demi de personnes chaque jour. Et le cyber-kidnapping prend une place de plus en plus importante.

L'éditeur d'antivirus McAfee a déjà enregistré 120.000 virus de ce genre en 2012, soit quatre fois plus qu'un an auparavant, rapporte Slate. Car le "ransomware" est bien plus efficace que le phishing, dont le but est d'obtenir de la victime ses coordonnées bancaires afin de vider son compte.

Des experts en sécurité informatique américains ont d'ailleurs récemment estimé que le cyber-kidnapping rapporte plus de 5 millions de dollars par an. Une estimation qui n'est que la partie visible de l'iceberg. "Seules 3% des personnes infectées paient la rançon, mais ce nombre est en augmentation", souligne Candid Wueest de Symantec. "Et comme il s'agit d'une somme relativement faible, les victimes ne portent pas plainte pour éviter la paperasse." Les hackers ne sont donc pas inquiétés et peuvent récolter jusqu'à 30.000 euros par jour, selon Symantec.

"Le cas de Reveton est particulièrement intéressant", raconte Pierre Siaut, expert en sécurité à TrendMicro, au "Nouvel Observateur", qui a participé à la traque des hackers à l'origine de Reveton. "Ce virus affiche un message qui ressemblait en tout point à ceux envoyés par la police : le logo, les références aux articles de loi nationale, le type d'amendes."

Pour la victime, le subterfuge est total et la tentation de payer la rançon bien plus forte. "Reveton est tellement perfectionné qu'il arrive même à identifier la langue du propriétaire de l'ordinateur et donc son pays. Ce qui lui permet de créer un message plus vrai que nature avec des références très précises à la législation du pays de l'utilisateur."

Selon la police, l'organisation à l'origine de Reveton aurait réussi à extorquer des millions d'euros dans plus de 30 pays, principalement européens. Europol, l'agence de police européenne, estime qu'au moins 20.000 personnes auraient été victimes de Reveton en Europe.

Traquer les hackers

Dans un cas classique de cyber-kidnapping, la rançon est, le plus souvent, réclamée en argent virtuel. L'internaute doit alors convertir ses euros en monnaie virtuelle via des services comme Ukash, pour ensuite entrer un code dans son ordinateur bloqué. La machine ne

bougera pas d'un iota, mais l'argent sera automatiquement transféré jusqu'au pirate qui ira le blanchir sur un site de casino ou de poker en ligne où il joue quelques minutes avant de se retirer en empochant de véritables euros.
"Dans le cas de Reveton, le message demandait de payer avec des coupons", explique Pierre Siaut. "La victime allait l'acheter dans une station-service et n'avait plus qu'à rentrer le code pour payer." Selon l'expert en sécurité, c'est ce qui a rendu la traque des hackers à l'origine de Reveton si difficile. "Les coupons sont pratiquement impossibles à tracer sur internet."
Pierre Siaut confie alors qu'il a fallu détecter les traces laissées par Reveton et les hackers plutôt que de suivre la piste de l'argent. "On a découvert que les hackers avaient piraté les bases de données des sites informations. Ils ont alors récupéré les adresses mails des abonnés et envoyé de fausses publicités qui amenaient sur de faux site." Ensuite, Reveton, caché entre les lignes de codes du faux site, n'avaient plus qu'à utiliser les vulnérabilités présentes dans les navigateurs internet pour s'installer sur l'ordinateur de la victime.
Les pirates auraient aussi réussi à cibler les internautes susceptibles d'avoir des activités illégales sur internet, comme la visite un pédopornographique. "Cela rendait la menace d'une amende plus crédible pour l'utilisateur" relève Europol.
"Ces arrestations, ce sont le résultat de plusieurs mois de recherches, d'investigations, d'analyses pour aider la police. On avait une équipe dédiée", termine Pierre Siaut. Et le pire, c'est que Reveton est toujours en activité. "On a pas pu l'abattre totalement." Europol a, pour l'instant, détecté pas moins de 48 mutations de Reveton en activité
http://o.nouvelobs.com/high-tech/hacker-ouvert/20130214.OBS8969/le-cyber-kidnapping-nouvelle-arme-des-hackers.html

Le piratage informatique sous forme de rançon en plein essor dans le monde

L es pirates informatiques redoublent d'efforts pour transformer leurs aptitudes techniques en monnaie sonnante et trébuchante grâce à des logiciels extorqueurs. Au dernier trimestre 2015, ces campagnes ont bondi d'un quart dans le monde, selon un rapport d'Intel Security publié ce mardi 22 mars.
Le nombre de campagnes menées par "ransomware" ou "rançongiciels", des logiciels qui piègent vos données afin d'exiger une rançon, a augmenté de 26% au dernier trimestre 2015 par rapport au précédent, note le rapport d'Intel Security publié ce mardi 22 mars.

Jusqu'à 325 millions de dollars extorqués

Le principe ? Un logiciel bloque le démarrage de votre ordinateur. Ensuite, il demande une rançon afin de les débloquer. Une méthode utilisée par les pirates pour extorquer de l'argent à l'utilisateur de l'appareil en échange du code de déblocage des données. Des attaques qui peuvent être très lucratives. D'après les auteurs du rapport, une seule campagne a ainsi rapporté 325 millions de dollars. Sans donner d'estimation du montant total extorqué, le rapport a dénombré quelque six millions de tentatives d'installation de ces logiciels malveillants. Même Apple, d'ordinaire assez épargné par les virus, a été touché il y a peu (voir vidéo ci-dessous).
Steve Grobman, responsable technique chez Intel Security, a identifié plusieurs facteurs à l'essor de cette pratique : facilité d'accès au logiciel malveillant disponible gratuitement, réseaux criminels offrant cette prestation, difficultés de remonter jusqu'aux auteurs qui se dissimulent sur la toile. "En de nombreux points, c'est un modèle entrepreneurial plus lucratif que les formes traditionnelles de cybercrime". Steve Grobman souligne que ces attaques visaient désormais d'autres cibles que de simples usagers, comme des hôpitaux, des écoles ou des postes de police.

Un profil de victime

Ces victimes sont choisies, selon lui, "parce qu'elles ne disposent pas des protections informatiques que l'on peut voir chez des banques ou des sous-traitants de la défense" et qu'elles possèdent des données pouvant être prises "en otage". Les rançongiciels existent depuis plusieurs années mais les techniques se sont affinées, les rendant plus exploitables. A noter par ailleurs que ces arnaques fonctionnent également car l'utilisateur se sent piégé et obligé de payer.

"Peu de risque d'arrestation"

Traquer les auteurs est aussi beaucoup plus compliqué en cas de paiement en bitcoins, monnaie virtuelle qui ne nécessite pas de passer par le système bancaire. Il y a "peu de risque d'arrestation, donc (ces campagnes) sont devenues assez populaires", relève Intel. Le mois dernier, le Centre médical presbytérien d'Hollywood, à Los Angeles, a versé 17 000 dollars en bitcoins à des pirates informatiques qui avaient pris le contrôle de ses ordinateurs pendant plus d'une semaine.

Les rouages du piratage informatique

Selon M. Grobman, la meilleure protection contre ces attaques est de sauvegarder les données en plusieurs endroits pour pouvoir les récupérer en cas de besoin et d'utiliser des logiciels permettant de détecter les emails des pirates. "Le principal problème est qu'en payant la rançon, vous encouragez les cybercriminels et cela va faire apparaître une nouvelle génération de rançongiciels" prévient-il.

http://www.midilibre.fr/2016/03/23/le-piratage-informatique-en-plein-essor-dans-le-monde,1305190.php

Le racket à l'ère du numérique

Payer ses impôts, ses factures, ses amendes par internet est chose commune. Les ransomwares (ou rançongiciels) surfent sur la vague du télépaiement associée à la peur du gendarme : et ça marche !

Une recette à l'origine japonaise

Pourquoi braquer une banque alors que l'on peut organiser tranquillement un chantage à échelle internationale du fond de son canapé ? Né au Japon en 2010, le ransomware a fait ses preuves avec le premier virus de ce type le Kenzero. Ce virus visait les internautes qui téléchargeaient des jeux pornographiques (Hentaï). Ressemblant à l'écran d'une installation de jeu, l'utilisateur remplissait des champs de données personnelles, pendant qu'à son insu, le virus téléchargeait ces détails et l'historique de ce dernier. C'est alors que l'internaute recevait un email lui demandant 1500 yen (11€) contre le retrait de la page de son historique publiée sur un site leur appartenant, le site étant enregistré au nom d'une société fantôme.

Puis, le prix des amendes se sont envolés. Une variante de ce virus proposait un règlement à l'amiable via le paiement d'une amende forfaitaire de 465€, sans quoi une procédure judiciaire serait engagée : les japonais ont payé.

Un nouveau créneau pour le crime organisé.

Soudain, votre ordinateur laisse apparaître une fenêtre, affublée de logos pseudo officiels, vous invitant à vous acquitter de la modique somme allant de 50€ à 400€. L'écran se fige et moult redémarrages en « mode sans échec » n'y changent rien. La seule option qui vous est offerte pour reprendre le contrôle de votre ordinateur est le paiement et pour le prouver vous êtes censé rentré le code de la carte achetée au bureau de tabac du montant de l'amende. Bien évidemment, vous pourrez vous acharner à saisir tous les combinaisons de codes possibles, cela restera sans effet. Le virus devra être enlevé par un logiciel adapté.

On estime les bénéfices de cette « plaisanterie » à 33 000$/jour, même si sur 5700 ordinateurs contaminés par jour, seuls 2.9% des victimes paieront. En 2012, cette arnaque aurait rapporté plus de 2 millions de dollars.L'argent ainsi collecté sera blanchi via les casinos en ligne. Selon toute probabilité, cette ingénieuse arnaque vient de l'Est : toutes les pistes pointent vers les mafias russe et ukrainienne.

La mondialisation du phénomène « Ransomware »

La conquête de nouveaux marchés est à l'ordre du jour. Jusqu'alors, les Etats-Unis, le Canada, et l'Europe étaient les cibles privilégiées. Aujourd'hui, les marchés asiatiques, africains et de certains pays émergents, comme le Brésil, sont dans la ligne de mire de ces organisations criminelles.

Les Madwares : l'avenir des ransomwares

Pour connaître les futures cibles des ransomwares, il suffit d'observer les tendances du marché des nouvelles technologies. Les cybercriminels s'adaptent à la demande.

Les appareils mobiles sont en pleine expansion : tablettes, smartphones, GPS, appareils divers de domotique, les télévisions connectées via une box internet, équipements médicaux (appareils cardiaques), le Cloud

Ces appareils mobiles représentent de nouvelles opportunités pour les cybercriminels En effet, ces dispositifs comptent de nombreuses brèches. Par exemple, il n'existe pas de certificat de sécurité (SSL) adapté pour les activités internet à partir d'un téléphone mobile.

Ainsi, le ransomware devient « Mobile Adware » : Madware.

Se glissant subrepticement lors de téléchargement de nouvelles App, ce nouveau virus recueille de multiples informations précieuses : des informations de géolocalisation et d'identification du matériel utilisé.

Les Madware ont augmenté de 210% ces neuf derniers mois : l'extorsion numérique a de beaux jours devant elle.

http://www.crime-expertise.org/braquage-2-0/

Le boom des logiciels de demande de rançon

Les « rançongiciels » cryptent les données d'un utilisateur et exigent de l'argent pour les déverrouiller.

Les « rançongiciels » (« ransomware ») sont la nouvelle arme des hackers pour mettre la main sur des fonds et des informations personnelles de clients d'une société. Aux côtés des traditionnels logiciels malveillants ou la technique de « harponnage » - des mails frauduleux envoyés à des cadres dirigeants pour demander des transferts de fonds vers un compte externe -, les attaques de ce type sont en forte progression, selon une étude de l'assureur britannique Beazley, fondée sur ses propres clients. Lors de ces attaques, les hackers prennent le contrôle d'un ordinateur, d'un smartphone ou d'une tablette, cryptent les données, puis réclament de l'argent en échange du déblocage. *« Sur le premier semestre 2016, il y a eu deux fois plus d'attaques de ce type traitées par Beazley que sur toute l'année 2015 »*, un chiffre qui avait déjà doublé par rapport à 2014, souligne l'assureur.

Cette recrudescence a conduit Europol, l'organe chargé de coordonner les polices européennes, à lancer un site Web dédié au mois de juillet, en collaboration avec la police néerlandaise et des entreprises spécialisées en cybersécurité. Le portail No More Ransom propose des conseils et des outils pour éviter ces attaques, mais surtout il aide les victimes à retrouver les données piratées. Les fichiers cryptés par un « rançongiciel » peuvent être téléchargés dans le service Crypto Sheriff, qui tentera de les déverrouiller grâce aux 160.000 clefs de déchiffrement que contient sa base de données.

Les petites institutions financières visées

Si le secteur de la santé reste le plus touché par les piratages informatiques de toutes sortes, les services financiers ne sont pas épargnés. Notamment les petites institutions financières, premières cibles des hackers : les banques et coopératives de crédit dont le chiffre d'affaires annuel est inférieur à 35 millions de dollars constituent 81 % des actes de piratage informatique dans les services financiers au premier semestre 2016, selon l'étude Beazley. Une tendance en forte hausse, puisque ces établissements ne concernaient que 54 % des cas pour l'année 2015.

« Ces petites institutions financières détiennent des informations personnelles de valeur et ne disposent généralement pas de systèmes de sécurité informatique à la hauteur de ceux de leurs homologues de grande taille, ce qui en fait des cibles de choix », explique l'assureur, spécialisé dans les interventions en cas de violation de données personnelles. Plus globalement, les hackers ont redoublé leurs attaques contre les services financiers durant cette période : les piratages informatiques représentent 43 % des violations de données - loin devant les cas de divulgation non intentionnelle (27 %) -, contre 27 % pour l'année 2015.

http://www.lesechos.fr/journal20160916/lec2_finance_et_marches/0211219429616-le-boom-des-logiciels-de-demande-de-rancon-2027846.php

Ransomware : une menace en forte croissance

Les attaques par Ransomware coûtent de plus en plus cher aux entreprises. Les dommages générés à la fois pour le paiement de la rançon et/ou pour la récupération des données corrompues se chiffrent en centaines de millions de dollars. Pour faire le point sur la situation, Malwarebytes a mené une vaste enquête.

Au mois de juin 2016, Malwarebytes a mené une enquête auprès de 165 entreprises aux Etats-Unis et 125 dans plusieurs pays européens. Au total 540 questionnaires ont été complétés autour d'une nouvelle forme d'attaques : les ransomware ou rançongiciels. Il en ressort que 39% des entreprises interrogées ont été victimes d'une attaque de ce type durant les 12 derniers mois. Si l'on y ajoute tous les types d'attaques (déni de service, tentatives d'intrusion, malwares …) on arrive au chiffre de 79% aux Etats-Unis et plus de 65% en Allemagne. Concernant les rançongiciels, les différences sont importantes en termes de secteur d'activité et de pays. Sans surprise, ce sont les secteurs financiers et de la santé qui subissent le plus d'attaques. La Grande-Bretagne étant la première place financière d'Europe, 54% des entreprises britanniques ont été victimes d'une tentative d'attaque contre seulement 18% en Allemagne.

Prise de conscience mais peu d'actions

La confiance quant à la possibilité d'écarter un ransomware sans dommage varie également selon les pays. Les 2/3 des responsables sécurité canadiens ou allemands sont plutôt ou très confiants quant à la possibilité de stopper l'attaque. A contrario, ils ne sont que 37% à partager ce sentiment aux USA. Il en va de même pour la confiance selon le type d'attaque.

2/3 des responsables pensent pouvoir stopper les attaques par phishing, les infiltrations de malware via le web ou la messagerie. En revanche, ils sont à peine plus de la moitié à affirmer pouvoir contrer une attaque de ransomware. Notons d'ailleurs que cette prise de conscience est surtout américaine. En effet, dans les pays d'Europe, les décideurs sécurité semblent bien moins concernés par ces produits pourtant très dangereux. En effet, ils ne sont que 32% au Canada et 12% en Allemagne à se sentir concernés ou extrêmement concernés par ce type d'attaques.

Un autre paradoxe concerne la formation des utilisateurs et l'implémentation de technologies. Bien que les responsables sécurité américains considèrent à 60% qu'il s'agit d'une priorité

élevée voire très élevée contre 19% pour les Allemands, ils sont en même temps à la traîne pour la mise en place de ces actions de formation et d'installation des technologies.
Dans une seconde partie, nous détaillerons, les principaux vecteurs d'infection, les montants moyens réclamés et obtenus par les pirates ainsi que les différentes techniques devant être utilisées pour combattre ces menaces.
http://www.linformaticien.com/actualites/partenaires/articletype/articleview/articleid/41712/ransomware-une-menace-en-forte-croissance.aspx

Cryptolocker : une prise d'otages en 2.0

Qu'est-ce que le Cryptolocker ?
Le CryptoLocker est un logiciel malveillant dit « rançongiciel » (ransomware) qui se propage par courrier électronique à l'ouverture d'une pièce jointe, d'un fichier zippé. En très peu de temps des dizaines de milliers de données sont « prises en otages et rançonnées ».
Plusieurs mairies en France se sont vues crypter leurs dossiers en une fraction de seconde, au Royaume-Uni les ordinateurs d'universités et d'étudiants ont ainsi été complètement cryptés.
A l'ouverture d'une pièce jointe, certains documents des disques internes ou accessibles par le réseau sont transformés en chiffres. Les pirates proposent de rendre les données après le paiement d'une rançon dans un délai imparti, au-delà duquel les documents sont définitivement perdus (généralement 72 heures).
Comment fonctionne le CryptoLocker ?
C'est un code malveillant classique qui se copie dans le dossier temporaire au moment du lancement.
La persistance du code est assurée par l'ajout de deux clés de registre dans le profil de l'utilisateur courant.
Une fois la persistance établie sur la machine de la victime, le rançongiciel va utiliser son algorithme de génération de noms de domaine (détaillé dans la section suivante) pour identifier le ou les serveurs de contrôle et de commande avec lesquels il va pouvoir communiquer. Lorsque le serveur a été identifié, CryptoLocker demande au serveur de contrôler et de commander la génération d'un couple de clés RSA 2048 bits.
L'une d'elle est stockée sur le serveur, l'autre est envoyée au logiciel malveillant pour chiffrer les données jugées importantes (fiches de paies, analyses techniques, délibérations, images, jeux, musiques, cours, etc.)
A l'issue, une fenêtre s'affiche pour indiquer à la victime la marche à suivre pour payer la rançon.
Cette fenêtre utilise parfois les identifiants graphiques de l'État (police ou gendarmerie nationales).
La clé de déchiffrement ne peut être reçue qu'après paiement.
Les montants de la rançon oscillent entre 100 et 500 dollars. La rançon peut dans certains cas être acquittée en bitcoins.
Comment éviter d'être rançonné ?

- Vérifiez l'émetteur des courriers reçus avant de les ouvrir.
- Soyez vigilants lors de l'ouverture des pièces jointes de vos courriels, tout particulièrement si ces dernières sont compressées (zippées) et si elles contiennent des fichiers exécutables.
- Dotez-vous d'un anti-virus avec une licence à jour. Vérifiez que sa base anti-virale s'actualise quotidiennement.
- Faites des sauvegardes régulières de vos documents sensibles.

http://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Cryptolocker-une-prise-d-otages-en-2.0

La prise d'otage 2.0 est née : les Cryptolockers font des dégâts

La prise d'otage 2.0 est née. Le Cryptolocker est un logiciel malveillant qui se présente sous diverses formes et qui s'avère très perturbant pour ses victimes, surtout pour les non initiés. La récupération de données cryptées peut ainsi être un vrai chemin de croix pour certains.

CryptoLocker : qu'est-ce que c'est ?

Le Cryptolocker ou Cryptographic locker, est un logiciel malveillant qui attaque votre ordinateur, tablette ou smartphone. Il s'agit très précisément d'un ransomware (un rançongiciel en français), qui se propage dans tout le système. Il est très facile d'être victime du CryptoLocker dans la mesure où il se niche notamment dans les pièces jointes et autres fichiers zippés. Certes, il est de coutume de faire appel à la vigilance de chacun, mais certains utilisateurs sont encore peu familiers avec le web et ignorent les dangers de cet univers très spécifique, ce qui en fait des proies faciles. S'il existe plusieurs déclinaison du CrytpoLocker, le concept reste sensiblement le même. Une fois propagé, le virus crypte vos données. Vous recevez alors un message vous indiquant de donner de l'argent, plusieurs centaines d'euros, via Bitcoin. Une fois cette rançon payée, vous devez pouvoir récupérer toutes vos données. Si vous ne souhaitez pas payer, vous pouvez tenter vous-même de réparer ou faire appel à un professionnel de la récupération de données.

Quels sont les différents CrytoLocker ?

On trouve plusieurs cryptolockers dont TeslaCrypt, CryptoFortress ou encore Locky. TeslaCrypt est un logiciel escroc qui utilise un cryptage AES et qui cible tout particulièrement les joueurs de jeux vidéo. CryptoFortress, quant à lui, infiltre votre système via de faux pop-ups de téléchargement voire de faux mails. Il crypte divers types de fichiers tels que les .wma, .rar, .jpeg et autres .ai. Le virus Locky figure parmi les plus virulents des CryptoLockers. Souvent niché dans un .doc en pièce jointe d'un mail de spam, il se diffuse ensuite dans tout le système et transforme les documents en .locky. Nous aurions également pu citer SimpleLocker ou encore CryptoWall.

Quid de la récupération de données cryptées?

Comme évoqué précédemment, certains choisissent de payer la rançon demandée. Or, rien ne peut réellement leur assurer que le paiement de la rançon leur permettra de retrouver tous les documents. Il y a fort à parier qu'une nouvelle rançon peut être parfois demandée pour décrypter tous les fichiers. Pour ne pas payer, il est possible d'utiliser un antivirus et un antimalware. Bien sûr, pour cela, il faut avoir un minimum de connaissances en matière d'informatique. Pour certains, cela s'avérera trop compliqué. Dans ce cas, afin d'être certain que la récupération de données se fera dans les règles de l'art et que l'ordinateur, ou tout autre support, sera à nouveau utilisable, il est plus que conseillé de s'adresser à un spécialiste de la récupération de données cryptées. Les professionnels maîtrisent la manière dont agissent les CryptoLockers et savent ainsi contrer les attaques. En outre, au regard des rançons demandées par les CryptoLockers, il est certainement préférable de s'adresser un professionnel plutôt que de rentrer dans le jeu de ces créateurs de virus.

http://www.lesnewsdunet.com/lesactus/prise-dotage-2-0-nee-cryptolockers-degats.html

Petya, un nouveau ransomware qui en veut à vos fichiers (et votre porte-monnaie) !

Parmi les nombreux malwares et autres virus pouvant nuire à votre ordinateur et à ses données, certains ont davantage le vent en poupe. Actuellement, ce sont les ransomwares qui semblent plébiscités. Et il y en a un nouveau dans la nature, Petya. Celui-ci sévit via Dropbox, et il en veut, comme les autres, à vos fichiers (et à votre porte-monnaie) !

Publicité

C'est, une fois encore, via une pièce jointe, via Dropbox, que Petya s'invite sur votre machine. Une fois en place, il crypte immédiatement l'intégralité du contenu de la mémoire, rendant tout votre ordinateur inutilisable. Pour récupérer la main (et vos précieuses données), il vous faut alors payer la rançon exigée : 0,99 bitcoins (environ 370€) sous sept jours, sans quoi le montant sera doublé.

En provenance d'Allemagne, ce nouveau ransomware se cache sous la forme d'un lien vers un dossier Dropbox inséré dans un email de candidature. Dans le dossier sont censés se trouver un CV et une photo. Résultat de l'opération, de nombreux services de ressources humaines de sociétés allemandes ont été infectés.

Dropbox a évidemment fait immédiatement supprimer ce dossier mais, vous vous en doutez, les hackers ont eu tôt fait de trouver une parade pour continuer de répandre leur création. D'après plusieurs sites spécialisés, Petya est bien « inarrêtable » pour le moment. La seule protection possible reste la vigilance : ne cliquez pas sur des liens d'une provenance inconnue et faites des sauvegardes régulières de vos données !

http://fr.ubergizmo.com/2016/04/03/petya-nouveau-ransomware.html

20 000 prises d'otage chaque jour en Europe

Depuis un an, les attaques de type « rançongiciels » – des virus qui bloquent et cryptent l'accès à d'importants fichiers informatiques ou l'accès à l'ordinateur même – se développent à un rythme soutenu. Les pirates offrent de rétablir l'accès contre le versement d'une certaine somme d'argent. Mais payer la rançon ne fait qu'empirer les choses.

En Europe, 20 000 prises d'otage ont lieu chaque jour – et Bernard, patron d'une petite entreprise spécialisée dans la vente de vins en ligne, vient juste d'en être victime.

Il a 42 ans et sort d'une grande école ; une carrière d'ingénieur dans une entreprise du CAC 40 avant de péter un cable et envoyer balader la chaîne hiérarchique. La volonté d'être son propre patron et de prendre du plaisir à se lever tous les matins, pour faire partager sa passion, son amour, pour les très bons vins Français – de préférence accompagnés d'excellents fromages du terroir.

Alors, Bernard quitte le CAC 40 et lance sa petite entreprise. Il se met à vendre les vins de son excellente cave personnelle – et, le succès grandissant, embauche quelques employés pour gérer son stock, servant à la fois de conseiller, de fournisseur, de traiteur pour des clients fortunés aux quatre coins du monde. Ses clients – principalement chinois et japonais – viennent de son ancien carnet d'adresse. Et le plaisir de conseiller à son ancien patron des vins de merde et de pourtant l'écouter pérorrer sur l'excellence des vins conseillés, « parole de connaisseur ».

Mais un jour, Bernard est pris en otage.

Ni par des braqueurs, ni par des terroristes, ni par des hommes armés jusqu'aux dents, ni par des fondamentalistes religieux. Ces ravisseurs d'un nouveau genre sont cachés derrière un écran d'ordinateur et cryptent et vérouillent à distance toutes les bases de données de Bernard.

20 000 victimes par jour

Impossible d'accéder à son carnet d'adresse, aux commandes des clients ou même de savoir quelles bouteilles se trouvent dans son entrepôt – Bernard perd ses yeux, ses mains, ses oreilles, à cause d'un clic malheureux sur la bannière publicitaire d'un site de *streaming* (visionnage de vidéo en ligne). « Tout ça pour voir le dernier épisode de Glee » … Et, presque au même moment, à l'autre bout de la planète, plusieurs cliniques australiennes, dont celle du médecin généraliste Munira Butt, sont victimes du même logiciel, et de la même demande de rançon. 3 000 € pour débloquer l'accès aux fichiers des patients ; outil de travail indispensable pour connaître les antécédents médicaux et assurer la prise en charge de ses patients.

A quelques kilomètres de là, et au même moment, une compagnie d'assurance et un club de golf du Queensland se font prendre en otage par le même groupe de pirates. La police conseille de ne jamais payer la rançon – et c'est l'attitude que le Dr Butt a décidé d'adopter. Mais les gérants de la compagnie d'assurance et du club de golf, eux, ont décidé de se soumettre aux demandes de leur ravisseur. « Au moment de l'attaque, les victimes sont souvent vulnérables psychologiquement » m'écrit un policier spécialisé dans la cybercriminalité. « Ils ne comprennent pas ce qui arrive et n'ont pas le réflexe d'appeler la police qui, de toute façon, ne pourra rien faire. Ils sont complètement démunis. Alors, ils paient. »

20 000 attaques de ce type ont lieu chaque jour en Europe selon Symantec, éditeur de logiciels de sécurité informatique. Et le profil des victimes n'est jamais le même. Ils peuvent être étudiant, PDG, chômeur, ingénieur, employé de caisse – et les rançons demandées varient entre 40 et 4000 €. Au début, ces attaques ne visaient que les entreprises mais très vite, les pirates ont étendu leur sphère d'action aux particuliers – et ceux qui paient sont nombreux, car la pression est forte. Pression économique : paralyser le site web d'une entreprise a des répercussions immédiates sur ses ventes, sur sa réputation – comme s'il y avait une honte à être victime d'une cyberattaque. 71 % des petites et moyennes entreprises ne s'en relèveraient jamais d'après le CLUSIF (Club de la sécurité de l'information Français) – mais les grandes entreprises françaises du CAC 40, assaillies elles aussi quotidiennement, ne réagissent pas différemment.

Une rançon de 3000 €

Pression psychologique : pour accentuer l'état de détresse dans lequel se trouve la victime, les pirates peuvent également activer la webcam de l'ordinateur infecté pour faire croire à une surveillance en temps réel. Parfois, à ce moment, le téléphone sonne. Un individu – doté parfois d'un fort accent africain, parlant parfois un Français parfait – se fait passer pour un enquéteur du FBI, de l'OCLCTIC ou de la Gendarmerie. Et fait croire à la victime qu'il est sous surveillance policière pour téléchargement illégal ou consultation de sites pédopornographiques. On lui propose de payer une amende discrète – et, même si la victime est innocente, le seul fait de penser que leur entourage pourrait apprendre qu'ils sont sous le coup d'une surveillance policière pour pédophilie suffit à faire paniquer pas mal de monde.

Il y a quelques mois, Symantec a repéré un groupe de pirates ayant installé des rançongiciels sur plus de 400 000 ordinateurs en seulement 18 jours.

Bernard a fini par payer ce qu'on lui demandait. 3000 € – une somme considérable pour une petite entreprise de 4 employés qui ne fait que vendre du vin. Puiser l'argent dans le compte de son entreprise aurait contraint Bernard à fermer boutique. Mais les pirates savaient qu'il possédait les ressources nécessaires – un tour sur Linkedin pour consulter son parcours professionnel et le type de projet sur lequel il travaillait, quelques coups de fil pour connaître le salaire moyen proposé à ce niveau de responsabilité, son train de vie analysé via ses photos

Facebook, ses habitudes de consommation scrutées … Les pirates savaient qu'il pourrait payer. Et Bernard a payé. Mais les pirates ne lui ont jamais donné les clés de déchiffrement.
Heureusement, Bernard avait quelques sauvegardes sur une clé USB et connaissait personnellement la plupart de ses clients – mais les pertes engendrées l'ont quand même poussé à licencier le plus jeune de ses employés.

Mise en ligne d'un site d'inormation spécialisé

Pour aider les utilisateurs à mieux prévenir les risques liés aux virus informatiques et en particulier les rançongiciels, les animateurs du wiki botnets.fr ont lancé Lundi 17 décembre un site d'information: http://stopransomware.fr/.
Les rançongiciels sont une catégorie particulière de logiciels malveillants qui bloquent l'ordinateur des victimes et réclament le paiement d'une rançon. Il ne faut jamais payer la rançon réclamée. Le site stopransomware.fr regroupe un ensemble d'informations pour sensibiliser les usagers et aider les victimes à se protéger contre ces risques, voire à nettoyer leurs ordinateurs lorsqu'un tel virus les a touchés.
Quelques idées importantes à retenir:

- La Gendarmerie nationale, la Police nationale ou même encore l'ANSSI et la SACEM n'ont pas le droit de bloquer votre ordinateur à distance. Ils ne vous réclameront jamais le paiement d'une amende en bloquant votre ordinateur.
- Aucune autorité officielle ne demande le règlement d'une amende par un moyen de paiement tel que Paysafecard, Ukash, MoneyPak, WesternUnion etc.
- Si vous êtes victime d'un rançongiciel, la seule solution est de nettoyer son ordinateur. En outre, il est fort probable que d'autres virus informatiques, plus discrets aient été installés à votre insu.

Il existe différents types de raçongiciels, dont voici une présentation rapide.

Les rançongiciels policiers

Depuis le milieu de l'année 2011, leurs auteurs utilisent les logos de services d'enquête pour réclamer le paiement d'une amende. D'autres encore se font passer pour des solutions de sécurité.
Si vous voulez en savoir plus sur les variétés des rançongiciels policiers, vous pouvez consulter la rubrique correspondante du Wiki botnets.fr ou encore visualiser les copies d'écrans des rançongiciels connus s'attaquant à des internautes français.

Les chiffreurs

Un autre type de rançongiciels agit en chiffrant les documents de l'utilisateur: l'accès aux documents est impossible tant que vous n'avez pas la clef de déchiffrement. Ces variantes réclament une somme d'argent en échange de cette clef. Cela se fait en général via un fichier texte laissé sur le bureau.
Malheureusement, pour cette variante, il est quasiment impossible de déchiffrer les documents: Ne payez jamais, les auteurs de logiciels malveillants ne donnent jamais les clefs de déchiffrement.

Bloqueurs par publicité

Une variante plus récente des rançongiciels consiste à bloquer l'ordinateur et invite la victime à cliquer sur des publicités. L'auteur du virus touche bien entendu des revenus à chaque clic.
http://christopherchriv.blog.lemonde.fr/2012/12/18/20-000-prises-dotage-chaque-jour-en-europe/

Europol annonce le démantèlement d'un réseau de développeurs de virus

L'unité européenne d'Europol dédiée au combat contre le cybercrime annonce avoir mis la main sur un réseau versé dans le développement et la diffusion de ransomware

(rançongiciels). Ce type de virus fait, en règle générale, croire à une victime que son poste est effectivement infecté et demande ensuite une somme d'argent afin de pouvoir le nettoyer.
L'EC3, l'unité chargée de la lutte contre la cybercriminalité annonce être parvenue à démanteler un réseau de personnes spécialisées dans la création, le développement et la diffusion à échelle internationale de logiciels malveillants de type ransomware. Europol précise que le malware baptisé Reveton a infecté des dizaines de milliers de postes à travers le monde.
Ces pratiques auraient permis à ce réseau de générer environ « *un million d'euros par an* », précise l'organisme dans un communiqué. Europol ajoute que 11 arrestations ont permis notamment de mettre la main sur la clé de voûte de ce réseau, à savoir un développeur russe de 27 ans accusé d'avoir mis au point ce logiciel malveillant.
Pour rappel, un ransomware ou rançongiciel est un programme qui, une fois installé sur un poste, tente d'induire en erreur son propriétaire. Le malware explique alors que ledit poste est infecté et demande à l'utilisateur d'installer un nouveau programme payant afin de le nettoyer. Un procédé dangereux pour la victime puisque si elle décide d'y répondre, elle devra communiquer ses données bancaires alors qu'elle ne sera pas pour autant débarrassée du virus.
De son côté, la police espagnole, ayant activement participé à « l'opération Ransom » précise que six citoyens russes, deux ukrainiens et deux géorgiens ont également été arrêtés. Leur matériel informatique a été confisqué et les forces de l'ordre ajoutent avoir saisi des fausses cartes de crédit.
Le réseau de pirates utilisait en effet des systèmes virtuels de paiement, de la monnaie virtuelle et faisait transiter ses gains via des différents portails de jeux en ligne ou des passerelles de paiement électronique pour blanchir son argent. L'argent était ensuite acheminé vers la Russie
http://www.clubic.com/antivirus-securite-informatique/actualite-541314-europol.html

5,25 milliards de fichiers pris en otage par CryptoWall

Le cheval de Troie CryptoWall, un malware de cryptographie utilisé par les pirates pour chiffrer les fichiers des ordinateurs infectés et pour demander des rançons aux propriétaires de fichiers contre la clef de déverrouillage, tiendrait en otage la quantité astronomique de 5,25 milliards de fichiers, selon Dell SecureWorks.
Le business du ransomware est-il en train de péricliter ? C'est ce que laissent penser les derniers chiffres de Dell SecureWorks qui suggèrent que CryptoWall, le malware leader du genre sur le marché en ce moment, n'aurait pas été aussi rentable que son prédécesseur de triste mémoire, le fameux CryptoLocker, même s'il a réussi à infecter un nombre important d'ordinateurs et s'il a pu prendre en otage la quantité stupéfiante de 5,25 milliards de fichiers.
En décembre 2013, c'est Dell SecureWorks qui avait déjà fourni les chiffres, souvent repris depuis, montrant le succès du terrible CryptoLocker de CryptoWall, lequel avait semé la panique après sa première apparition en septembre dernier. En 100 jours, CryptoLocker avait réussi à infecter quelque 250 000 systèmes avant que son réseau ne soit neutralisé par l'opération Tovar démarrée en mai. Le nombre exact de victimes qui ont finalement payé pour pouvoir déchiffrer leurs données reste inconnu, mais Dell avait estimé ce nombre à environ 0,4 %. Mais, celui-ci est sans doute un peu inférieur dans la mesure où les systèmes de protection se sont adaptés à la menace. La division sécurité du texan estime aujourd'hui que CryptoLocker a probablement rapporté 3 millions de dollars environ de rançons aux pirates, soit trois fois plus que le 1,1 million de dollars qu'aurait réussi à soutirer CryptoWall. Pourtant, entre le début du mois de mars 2014, date de son apparition, et le 24 août dernier, CryptoWall a tout de même réussi à infecter au moins 625 000 systèmes. « L'impact de cette

famille de logiciels malveillants est moins important, même si CryptoWall a réussi à infecter une quantité impressionnante de fichiers. Les obstacles techniques rencontrés par les utilisateurs pour acheter des bitcoins ont probablement aussi contribué à cette baisse », a déclaré Keith Jarvis, un chercheur de Dell SecureWorks, qui a essayé d'expliquer le phénomène. « Par ailleurs, il est probable que les opérateurs de CryptoWall ne disposent pas de système de « cash out » et de blanchiment aussi sophistiqué que celui dont dispose l'équipe de Gameover Zeus [qui a distribué CryptoLocker] et qu'ils ne peuvent pas traiter les gros volumes de cartes prépayées ».

CryptoWall, plus efficace, mais moins rentable que CryptoLocker

« Reste que, CryptoWall est tout de même parvenu à crypter la quantité astronomique de 5,25 milliards de fichiers », a indiqué l'entreprise. La majorité des 1683 victimes identifiées par Dell SecureWorks aurait déboursé la modique somme de 500 dollars environ pour recevoir la fameuse clef de déverrouillage. Cependant, selon Dell SecureWorks, toutes les victimes n'ont pas payé la même rançon : certaines - 399 selon l'entreprise de sécurité - auraient déboursé 1000 dollars, et l'une d'elles aurait versé une rançon de 10 000 dollars. On ne sait pas vraiment si Dell SecureWorks a pu identifier les serveurs de paiement : il y a quelques semaines, l'entreprise de sécurité PhishMe avait réussi à tracer des portefeuilles Bitcoins dont le solde atteignait plus de 700 000 dollars en valeur. Enfin, s'il a eu moins de succès que CryptLocker, CryptoWall (également connu sous le nom CryptoDefense) a toutefois réussi à infecter des ordinateurs partout dans le monde, avec un impact très variable selon le pays. D'après la liste établie par Dell SecureWorks, 253 521 ordinateurs ont été infectés aux États-Unis (40,6 % du total), 66 590 au Vietnam (10,7 %), 40 258 au Royaume-Uni (6,4 %), 32 579 au Canada (5,2 %), 22 582 en Inde (5,2 %), et 19 562 en Australie (3.1 %).

La conclusion de tout cela c'est que le ransomware est probablement un business en perte de vitesse. Ce type de malware infecte encore beaucoup de systèmes, mais le nombre de victimes acceptant de payer le prix fort pour obtenir la clef de décryptage baisse. Probablement, les gens pensent que le paiement d'une rançon ne changera rien (souvent les pirates n'envoient aucune clef de déchiffrement en retour), ils se protègent avec des sauvegardes et certains ne savent pas comment acheter des Bitcoins, monnaie utilisée pour payer les rançons. Mais avant d'apprécier ces bonnes nouvelles, il est important aussi de se rappeler l'énergie incroyable qu'il a fallu déployer pour contrer les ravages de CryptoLocker, le prédécesseur de CryptoWall. De nombreux organismes et de nombreuses entreprises de sécurité avaient consacré des mois de travail pour trouver une solution. Entre temps, le malware avait allégé ses victimes de 3 millions de dollars...

http://www.lemondeinformatique.fr/actualites/lire-5-25-milliards-de-fichiers-pris-en-otage-par-cryptowall-58469.html

Ransomware : des pirates s'excusent pour leur arnaque et livrent l'antidote

Les ransomwares sont de plus en plus répandus ces derniers temps. Ces programmes malveillants infectent vos appareils et vous demandent par la suite une rançon, donc une somme d'argent, pour que tout fonctionne à nouveau. Des pirates, amateurs de ce genre d'arnaque, se sont excusés et ont livré l'antidote de leur ransomware.

Pour ceux qui ne connaissent pas les ransomwares, petite explication. Il s'agit en fait de logiciels qui prennent en otage les utilisateurs en cryptant leur ordinateur. Face à un utilisateur démuni, les pirates demandent alors une rançon en échange de la « libération » de l'ordinateur.

Face à de tels logiciels, il n'y a pas 100 000 solutions. Soit on paie pour pouvoir utiliser à nouveau sa machine, soit on attend et on espère qu'un antidote soit trouvé. Enfin, ça c'est

pour les cas généraux. Car on apprend aujourd'hui que dans certains cas, il suffit de demander gentiment aux pirates de donner l'antidote.
En effet, le site Bleeping Computer nous raconte qu'un chercheur en sécurité de la société ESET a contacté les pirates à l'origine du ransomware TeslaCrypt.
Le chercheur a en effet constaté un ralentissement de l'activité des pirates qui visaient principalement les joueurs. Non, il ne s'agit pas de ceux qui pullulent sur les sites pornos. Il s'est alors fait passer pour une victime du ransomware et a tout simplement contacté les responsables de TeslaCrypt via le site de paiement des rançons. Là, il leur a sans complexe demandé s'il pouvaient publier la clé de déchiffrage.
Et là, surprise ! Non seulement les pirates ont fourni l'antidote au chercheur en expliquant que TeslaCrypt était clos, mais ils se sont en plus excusés en ajoutant « nous sommes désolés ! ».
Suite à cela, le chercheur a pu mettre au point un outil de décryptage qui déverrouille toutes les versions de TeslaCrypt. Une histoire complètement dingue mais qui nous a bien fait rire.
http://www.phonandroid.com/ransomware-pirates-excusent-arnaque-livrent-antidote.html

Un nouveau rançongiciel nommé locky arrive en France

Locky est un logiciel malveillant dit « rançongiciel » (ransomware) qui se propage par courrier électronique à l'ouverture d'une pièce jointe, d'un fichier zippé.

Le principe

Des cyberescrocs envoient par courrier électronique (mail) une pièce jointe contenant le virus locky. Une fois cette dernière ouverte :

- tous les fichiers du destinataire,
- tous les périphériques branchés (clés usb, disque durs externes, etc.),
- tous les répertoires partagés sur un réseau

sont rendus inaccessibles (cryptés) et leurs extensions modifiées en .locky , .mp3 ou .xxx
Ces données, désormais chiffrées, ne peuvent plus être récupérées et les cyberescrocs vous demandent une rançon pour les débloquer.

Les bons réflexes

- je vérifie l'origine du message électronique ;
- en cas de doute, je n'ouvre pas la pièce jointe et je m'assure auprès de la personne qui me l'a envoyée qu'il s'agit bien de son document;
- je me tiens au courant de l'actualité, par exemple de faux messages FREE circulent;
- je pense à maintenir mes équipements à jour (logiciels, antivirus, etc.);
- je fais des sauvegardes régulières de mes documents sensibles.
- Si j'ai ouvert la pièce jointe :
- je coupe l'accès à internet (je débranche le câble ethernet ou je désactive le wifi) ;
- je ne réponds pas aux sollicitations du cyberescroc.

Votre vigilance est importante, elle peut prévenir la perte de vos données.
http://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Un-nouveau-rancongiciel-nomme-locky-arrive-en-France

Bulletin d'alerte du CERT-FR

Objet : Campagne de messages électroniques non sollicités de type Locky

1 - Risque(s)

Installation d'un logiciel malveillant de type Locky.

2 - Systèmes affectés

Tous les systèmes d'exploitation Windows peuvent être victimes de ce logiciel malveillant.

3 - Résumé

Depuis la mi-février 2016, le CERT-FR constate à l'échelle nationale une vague de pourriels dont le taux de blocage par les passerelles anti-pourriel est relativement faible. Ces pourriels ont pour objectif la diffusion du rançongiciel Locky.
Un rançongiciel est un programme malveillant qui chiffre les données du poste compromis. Il va également cibler les partages de fichiers accessibles depuis le compte utilisateur dont la session est compromise. Celui-ci est exécuté, dans le cas présent, par une action de l'utilisateur. La victime est ensuite invitée à verser de l'argent afin que l'attaquant déchiffre les fichiers ciblés.
Dans le cadre de cette campagne, et d'après les échantillons que le CERT-FR a observés, la diffusion de Locky s'effectue par l'intermédiaire d'un pourriel dans lequel se trouve une pièce jointe au format doc. Ce document Microsoft Office contient un texte illisible ainsi qu'un message indiquant la nécessité d'activer les macros pour l'affichage correct du message. Macro dont l'objectif est la récupération puis l'exécution du malware. L'exécution de ce dernier entraine le chiffrement des données et les fichiers sont renommés avec l'extension ".locky".
Il est intéressant de noter que le message eléctronique a pour sujet "ATTN: Invoice J-<8 chiffres>" et la pièce jointe pour nom "invoice_J-<8 mêmes chiffres>". Cette caractéristique peut permettre le blocage ou la mise en place d'alertes via les serveurs mandataires.
À l'aide les échantillons remontés, le CERT-FR a constaté que les URLs de téléchargement du binaire Locky sont les suivantes :

4 - Solution

Mesures préventives

Le CERT-FR recommande de sensibiliser les utilisateurs aux risques associés aux messages électroniques pour éviter l'ouverture de pièces jointes. Il convient en effet de ne pas cliquer sans vérification préalable sur les liens de messages et les pièces jointes. Les utilisateurs ne doivent pas ouvrir des messages électroniques de provenance inconnue, d'apparence inhabituelle ou frauduleuse. Plus généralement, il convient de mettre à jour les postes utilisateurs, notamment le système d'exploitation et les applications exposées sur Internet (lecteur PDF, lecteur messagerie, navigateurs et greffons) dans le cas où le code malveillant (ou une variante) exploiterait une vulnérabilité logicielle.
Le CERT-FR recommande de configurer sur les postes de travail les restrictions logicielles pour empêcher l'exécution de code à partir d'une liste noire de répertoires :

- Si la solution utilisée est AppLocker, les règles de blocage suivantes doivent être définies :
  - OSDRIVE\Users*\AppData\
  - OSDRIVE\Windows\Temp\
- Si les restrictions logicielles (SRP) sont utilisées, les règles de blocage suivantes doivent être définies :
  - UserProfile\AppData
  - SystemRoot\Temp

Il est important de vérifier que le service "Application Identity" (AppIDSvc) est paramétré en démarrage automatique sur l'ensemble des postes pour que les restrictions logicielles soient opérantes (ce mode de démarrage peut être paramétré à travers une politique de groupe sur le domaine Windows). Si des dysfonctionnements sont rencontrés suite au déploiement de ces règles de blocage, il est nécessaire d'identifier les applications légitimes situées dans ces répertoires, et de définir des règles en liste blanche afin d'autoriser leur exécution.
Le CERT-FR recommande également de mettre à jour les logiciels antivirus du parc informatique (postes utilisateurs, passerelle de messagerie, etc.). Le code malveillant étant polymorphe, les éditeurs antivirus ont besoin de publier des signatures en constante évolution.

Par ailleurs, il convient d'envoyer dès que possible un exemplaire du code malveillant à votre éditeur de logiciel antivirus si la variante n'est pas détectée par ce dernier.
Enfin, le CERT-FR recommande d'effectuer des sauvegardes saines et régulières des systèmes et des données (postes de travail, serveurs) puis de vérifier qu'elles se sont correctement déroulées. Les sauvegardes antérieures ne doivent pas être écrasées (cas où une version chiffrée aurait été sauvegardée). Les sauvegardes doivent être réalisées en priorité sur les serveurs hébergeant des données critiques pour le fonctionnement de l'entité. Celles-ci doivent être stockées sur des supports de données isolés du réseau en production.

Mesures réactives

Si le code malveillant est découvert sur vos systèmes, le CERT-FR recommande de déconnecter immédiatement du réseau les machines identifiées comme compromises. L'objectif est de bloquer la poursuite du chiffrement et la destruction des documents partagés. Le CERT-FR recommande aussi d'alerter le responsable sécurité ou le service informatique au plus tôt. Le temps de revenir à une situation normale, le CERT-FR recommande également de positionner les permissions des dossiers partagés en LECTURE SEULE afin d'empêcher la destruction des fichiers sur les partages. Les personnels pourront continuer de travailler localement et mettre à jour ultérieurement le partage. Aussi, le CERT-FR recommande de prendre le temps de sauvegarder les fichiers importants sur des supports de données isolés. Ces fichiers peuvent être altérés ou encore être infectés. Il convient donc de les traiter comme tels. De plus, les sauvegardes antérieures doivent être préservées d'écrasement par des sauvegardes plus récentes.
Le CERT-FR recommande également de bloquer sur le serveur mandataire l'accès aux domaines ou URLs identifiés dans le message malveillant. L'objectif est de prévenir toute nouvelle compromission sur le même site. En complément, le CERT-FR recommande de rechercher et supprimer les messages malveillants similaires dans les boîtes de messagerie des utilisateurs. Par ailleurs, le CERT-FR recommande la réinstallation complète du poste et la restauration d'une sauvegarde réputée saine des données de l'utilisateur. De plus, dans le cadre de l'utilisation de profils itinérants, il convient de supprimer la copie serveur du profil afin de prévenir la propagation des codes malveillants par ce biais.
Enfin, les fichiers chiffrés peuvent être conservés par la victime au cas où dans le futur, un moyen de recouvrement des données originales serait découvert.
Cette alerte sera maintenue tant que le volume de message électronique constaté sera considéré significatif par le CERT-FR.
http://www.cert.ssi.gouv.fr/site/CERTFR-2016-ALE-001/index.html

Un hôpital de Los Angeles paie une rançon en bitcoins

Un hôpital de Los Angeles a versé 17 000 dollars en monnaie virtuelle à des pirates informatiques qui avaient pris le contrôle de ses ordinateurs pendant plus d'une semaine, ont indiqué les autorités jeudi.
Le Centre médical Presbytarien d'Hollywood a indiqué dans un communiqué qu'il avait versé plus tôt ce mois-ci une rançon de 40 bitcoins, l'équivalent de 17 000 dollars, pour pouvoir accéder de nouveau à son système informatique.
Le directeur général de l'hôpital, Allen Stefanek, a précisé dans une lettre aux employés que des problèmes pour accéder aux données numériques de l'hôpital avaient été constatées le 5 février et qu'une enquête avait alors été lancée.
«Le virus informatique a bloqué l'accès à certains systèmes informatiques et nous empêchait de partager des communications électroniques», a expliqué M. Stefanek.

«La manière la plus rapide et efficace de restaurer nos systèmes et fonctionnalités administratives était de payer une rançon et d'obtenir un code de décryptage», a-t-il ajouté.
Il a souligné que l'accès informatique avait été rétabli lundi et qu'il n'y avait aucune preuve que des données personnelles de patients ou d'employés aient été dérobées par les pirates.
Les autorités ont déclaré au Los Angeles Times que la rançon avait été payée avant que les forces de l'ordre n'aient été alertées sur cette affaire, sur laquelle enquête à présent la police fédérale (FBI).
Les «rançongiciels» («ransomware» en anglais) sont un type d'attaque informatique qui se multiplie à travers le monde: elles ont doublé en 2014 d'après la dernière étude en la matière de la société de sécurité informatique Symantec.
Ces logiciels malveillants prennent le contrôle des PC, tablettes et téléphones intelligents et les auteurs de ces attaques réclament ensuite de l'argent à leur utilisateur.
Le bitcoin est une forme de monnaie numérique particulièrement prisée des pirates informatiques pour collecter des fonds de façon anonyme et difficilement traçable.
http://affaires.lapresse.ca/economie/hors-cote/201602/18/01-4952078-un-hopital-de-los-angeles-paie-une-rancon-en-bitcoins.php

Infectée par un cryptolocker, la police du Massachusetts paie 500$ de rançon

Le police de la ville de Tewksbury, dans le Massachusetts, victime d'un cryptolocker, a du régler 500$ pour déchiffrer les fichiers conservés sur un serveur afin de remettre ses équipes au travail.
Un Département de police du Massachusetts, celui de la ville de Tewksbury, a du verser 500 $ à un cyberpirate pour débloquer les fichiers chiffrés avec un cryptolocker, le ransomware qui verrouille les disques durs jusqu'à ce que les propriétaires paient une rançon. Après plusieurs jours d'essais infructueux, les services informatiques de la police de Tewksbury ont réalisé qu'ils ne pouvaient pas casser le chiffrement et payé la rançon pour obtenir la clef privée permettant d'accéder aux données.
« Ils ont rendu inopérant le logiciel que nous utilisons pour assurer le fonctionnement du Département de la police », a déclaré le chef de la police, Timothy Sheehan, au journal Tewksbury Town Crier. L'incident est survenu à la fin de l'année dernière, l'infection a démarré le 7 décembre sur un poste de travail.

Une attaque très ciblée

Les attaquants ont exploré le réseau jusqu'à corrompre le serveur principal du Département. Les services de Police sauvegardent leurs fichiers sur un disque dur externe qui a également été touché par le ransomware, de sorte qu'ils avaient le choix de payer 500 $ ou de perdre toutes les données.
La police de l'État et le FBI se sont penchés sur cette affaire, tout comme Delphi Technology Solutions et Stroz Friedberg, des sociétés spécialisées dans la police scientifique. Aucune des deux n'a réussi à casser le cryptage de sorte que le Département a payé, indique le journal local. Stroz Friedberg a converti les 500 $ de la rançon en bitcoins avant de l'envoyer de la part du Département de police.

Payer ou pas

Les applications affectées concernaient la répartition des tâches assignées aux différents agents, la gestion des documents, la main courante avec les arrestations et la conservation des appels au commissariat. La même mésaventure s'est déjà produite en 2013 dans un autre service de police à Swansea, toujours dans le Massachusetts ; 750$ avaient alors été réglés pour débloquer le système.

De nombreux experts estiment que les victimes auraient du refuser de payer, surtout s'ils s'agit des forces de l'ordre, mais après avoir examiné l'alternative, c'est-à-dire ne jamais revoir ses données, de nombreuses entreprises préfèrent payer afin de recommencer à travailler.
http://www.lemondeinformatique.fr/actualites/lire-infectee-par-un-cryptolocker-la-police-du-massachusetts-paie-500$-de-rancon-60783.html

Attaqué par un ransomware, faut-il payer la rançon ?

Début février, dans la nuit du 4 au 5 exactement, le Hollywood Presbyterian Medical Center (HPMC), un hôpital de Los Angeles aux USA, a fait l'objet d'une attaque virale via un virus de type ransomware (rançongiciel). Tout le Système d'Information Hospitalier (SIH) est devenu hors d'usage. Les pirates demandaient initialement, d'après les premiers journaux, plus de 3,6 millions de dollars à payer en Bitcoins, cette monnaie virtuelle difficile à tracer, pour fournir la clé de déchiffrement des données.
Un hôpital moderne dont les processus de soins sont pleinement informatisés (niveau 6 ou 7 sur l'échelle EMR de l'HIMSS) peut se retrouver en grande fragilité pour assurer sa mission auprès des patients lors d'un incident informatique majeur. Les équipes médicales peuvent continuer à travailler mais elles le feront dans le cadre d'un Plan de Reprise d'Activité, si il existe, avec un passage forcé par l'âge de pierre, disons plutôt un retour au papier et aux crayons façon années 90. Cela n'étant pas sans risque pour les patients.
D'autre part dans le cadre d'un piratage, si le virus a pu chiffrer nos données, qu'a t-il pu faire d'autre ? Pour un expert en sécurité, la réponse est très anxiogène : Tout est envisageable ! Les bonnes pratiques et l'expérience nous conseillent de tout nettoyer par formatage. Les postes, les serveurs et les équipements infectés. Imaginez alors la complexité du chantier lorsque l'on parle de l'ensemble d'un SIH !
Il aura fallu dix jours à peu près pour que l'hôpital décide de payer une rançon négociée à 17 000 $ (15 000 € environ). Dix jours de cauchemar pour cet établissement d'environ 400 lits.
La question qui est aujourd'hui sur toutes les lèvres est la suivante : est-ce que Monsieur Stefanek, le PDG du HPMC, a eu raison de payer cette rançon pour débloquer son SIH ?
Une grande majorité des experts en sécurité vous diront qu'il n'aurait jamais dû accepter, la raison que nous évoquons tous à ce sujet c'est que si l'on paye on alimente ce système et les futures attaques seront encore plus évoluées et sans doute plus dramatiques.
Certes cela est juste mais il faut aussi peser le rapport « bénéfices / risques ». Un hôpital ne peut pas rester bloqué dans une situation à hauts risques pour ses patients. 15 000 € dans cet exemple, est-ce si cher eu égard à ce que peut coûter une aggravation médicale liée à une erreur voire pire, un décès ?
La question à se poser, l'analyse à faire pour l'HPMC, c'est pourquoi est-ce arrivé ? Pourquoi l'établissement n'a pas pu restaurer son Système d'Information Hospitalier dans l'état stable le plus récent, précédent l'attaque ? Il n'était sans doute pas prêt, comme beaucoup d'autres établissements de santé partout dans le monde, y-compris chez nous en France.
Dans cet exemple c'est un hôpital qui n'a pas eu de chance (d'après le FBI il n'était pas spécifiquement ciblé). Depuis 2013 nous avons référencé des dizaines d'attaques de ce type, dont plusieurs en milieu hospitalier. Dans une très grande majorité des cas une déconnexion du poste utilisé pour l'attaque, suivi d'une restauration complète des systèmes infectés à suffit. En quelques heures seulement, parce que les outils et le savoir-faire étaient au rendez-vous.
http://www.om-conseil.fr/vous-avez-ete-attaque-par-un-ransomware-faut-il-payer-la-rancon/