Cellule de traitement du renseignement financier

Lettre d'Information

DES ACTUALITES INTERNATIONALES

DANS LE DOMAINE DE LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCEMENT DU TERRORISME

VOLUME N°50 JUIN 2016

Génération Ransomware 2016 :

Le top 6 des derniers nés et comment vous en protéger

La vague de ransomwares qui déferle actuellement sur le monde informatique risque de faire chavirer la politique sécurité de plus d'une entreprise. Toujours plus nombreux et virulents, la météo des ransomwares est loin d'être maussade. Alors, pour garder la tête hors de l'eau, Stormshield surfe sur l'actualité et dresse le profil des six derniers ransomwares pour mieux comprendre la dynamique du phénomène avec en prime, le gilet de sauvetage offert contre Locky et ses amis, CTB-Locker, TeslaCrypt, Petya, SamSam.

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

Nous avons publié un article détaillé en anglais sur le cryptoware TeslaCrypt apparu en février 2016: https://thisissecurity.net/2016/03/02/lets-ride-with-teslacrypt/

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, les fraudeurs peuvent acheter le logiciel malveillant et l'opérer à volonté. Le réseau de malfaiteurs ne se limite donc plus à un cercle d'experts de la programmation et de l'écriture de logiciels. Avec, les innovations fulgurantes du ransomware, la société assiste petit à petit à l'éclatement et l'amplification du marché noir de la criminalité. C'est une véritable commercialisation généralisée et organisée de cette criminalité qui se met en place.

Des conseils indispensables pour vous protéger des ransomwares :

- Tenez à jour votre ordinateur (du système d'exploitation, logiciels et plugins)
- Réaliser des sauvegardes de vos fichiers les plus importants
- Ne cliquez pas sur les liens provenant de sources inconnues

Vers une génération « Super Cryptoware »

On peut s'attendre sans nul doute non seulement à une recrudescence de l'apparition de nouveaux ransomwares mais aussi à une métamorphose toujours plus complexe dans les mois à venir du visage des cryptowares. Le phénomène ransomware ne fait que commencer et son évolution sera au cœur de l'actualité pour encore longtemps. Pour en savoir plus, lisez les tendances cybersécurité 2016.

L'une de ces évolutions à surveiller concerne les modes toujours plus innovants, de propagation des ransomwares. A titre d'illustration, on note que Locky et Cerber utilisent parfois l'exploitation d'une vulnérabilité 0day pour se répandre ; un canal beaucoup plus impactant en terme de volume que l'email. Cette tendance montre que le caractère très lucratif du ransomware incite les attaquants redoubler de malice pour atteindre le plus de victimes possibles. Alors que le profil des pirates se diversifie, ils gagnent donc également en puissance à travers la génération ransomware.

Non, un antivirus n'est pas suffisant

Parce que les pirates élaborent des scénarios d'attaque et des malwares toujours plus complexes et intelligents, l'installation d'un antivirus n'est désormais plus assez efficace pour protéger le poste de travail. En effet, les malwares déjouent aisément le système d'analyse de signature et une identification proactive de comportements malicieux comme le propose Stormshield Endpoint Security, est maintenant indispensable pour contrer les nouvelles menaces connues comme inconnues. Ainsi, la technologie Stormshield Endpoint Security permet de maîtriser l'ensemble des ransomwares présentés dans cet article et pour la majorité de les bloquer avant même qu'ils ne soient identifiés par la communauté cybersécurité. Pour comprendre les différences avec votre antivirus classique, découvrez notre infographie ici.

Pensez au garde-fou pour votre réseau

Dans certains cas comme celui de Locky, le poste de travail n'est pas votre seul point de ralliement pour vous prémunir des dangers d'un ransomware.

En effet, si une protection comme Stormshield Endpoint Security empêche le logiciel malveillant de s'exécuter sur votre ordinateur et/ou l'exploitation de la vulnérabilité (via un exploit kit), un pare-feu nouvelle génération tel que Stormshield Network Security apporte une couche de protection complémentaire au niveau du serveur.

Ainsi, si votre PC est infecté par Locky à cause d'un anti-virus peu performant, Stormshield Network Security empêchera le ransomware d'obtenir la clé de chiffrement auprès du serveur sur Internet et donc de chiffrer vos documents. Sans possibilité de brouiller vos documents, le ransomware ne pourra pas donc mettre sa menace de rançon à exécution.

Liens : https://www.stormshield.eu/fr/endpoint-security-2/the-2016-ransomware-generation-top-6-of-the-last-born-progeny-and-how-you-can-protect-yourself/

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.

Liens : http://christo-pherchriv.blog.lemonde.fr/2012/12/18/20-000-prises-dotage-chaque-jour-en-europe/

Victimes de hackers,l'hôpital verse une rançon en bitcoin

Amériques. Le centre médical presbytérien d'Hollywood a été paralysé pendant une semaine à la suite d'une cyberattaque. Une rançon de 17.000 dollars en bitcoins a finalement été versée aux pirates pour débloquer le plus vite possible le système informatique de l'hôpital.

C'est une affaire de piraterie d'un nouveau temps. Le paiement d'une rançon de 17.000 dollars "a été le moyen le plus rapide et efficace" d'avoir de nouveau accès aux systèmes affectés du Centre médical presbytérien de Hollywood, a déclaré Allan Stefanek, le président du centre. Le contrôle des systèmes informatiques de l'hôpital, paralysés après une cyberattaque, a été rétabli lundi dernier.

La paralysie a duré une semaine entière ! Les pirates ont verrouillé tous les systèmes de l'hôpital en cryptant certains fichiers. Evidemment, les hackers étaient les seuls à détenir la clé permettant de décrypter tout le système.

Ces professionnels du hacking n'ont pas encore été identifiés mais selon une source locale contactée par le site CSO Online, les pirates ont réclamé, à l'origine, une rançon de 9.000 bitcoins, une monnaie virtuelle et anonyme, soit 3,6 millions de dollars. Le FBI et la police de Los Angeles ont été saisis de l'enquête.

Allan Stefanek a tenu à préciser dans son communiqué que cette cyberattaque n'a eu aucune conséquence sur les soins faits aux patients. Certains d'entre eux ont, tout de même, été transférés dans un hôpital voisin. avec AFP le 18 février 2016

Liens : http://lci.tf1.fr/monde/amerique/etats-unis-l-hopital-a-verse-17-000-dollars-de-rancon-aux-hackers-8717081.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. Publié le 18 février 2016

Liens : http://affaires.lapresse.ca/economie/hors-cote/201602/18/01-4952078-un-hopital-de-los-angeles-paie-une-rancon-en-bitcoins.php

Le bitcoin, monnaie d'échange du cybercrime

LOS ANGELES (Etats-Unis) – Le Hollywood Presbyterian Medical Center, un hôpital de Los Angeles a été obligé de payer une rançon de 17 000 dollars en bitcoins pour récupérer ses données et celles de ses patients.

Un hôpital victime d'un acte de ***« ransomware »*** **–** ce type d'attaque informatique qui chiffre les données contenues sur un disque dur et les rend illisibles – cela s'est passé ces jours derniers à Los Angeles, rapporte **une chaîne de télévision locale appartenant au réseau NBC**. Le FBI et la police de Los Angeles (**LAPD**) mènent l'enquête.

Pendant plus d'une semaine le réseau du Hollywood Presbyterian Medical Center a été paralysé par une attaque informatique. Fiches d'admission, dossiers médicaux des quelque 900 patients alors traités dans l'établissement, des données extrêmement sensibles ont été dérobées par les pirates.

Bitcoin et cybercriminalité

Certains ont beau claironné haut et fort que le **bitcoin,** cette monnaie électronique décentralisée apparue en 2008, n'est pas utilisée plus souvent qu'à leur tour par les cybercriminels, et encore moins par les terroristes, c'est bien en bitcoins, que ceux-ci ont exigé que soit payée la rançon réclamée à l'établissement hospitalier.

Ils demandaient au départ la modique somme de 3,4 millions de dollars. Il semble qu'ils n'aient obtenu au final *« que »* l'équivalent de 17 000 dollars. Contre la garantie, qui reste dans de pareils cas à la discrétion des cybercriminels, de débloquer le système informatique de l'hôpital. Quant à la divulgation, toujours techniquement possible, des données médicales des patients, c'est une toute autre histoire…18 février 2016

Liens : http://www.newzilla.net/2016/02/18/un-hopital-de-los-angeles-oblige-de-payer-une-rancon-de-17-000-dollars-en-bitcoins-pour-recuperer-ses-donnees-et-celles-de-ses-patients/

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) !

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 !

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

Russie : le bitcoin désormais interdit

Ainsi en a décidé le parquet général de Russie. L'usage du bitcoin comme de toute autre monnaie virtuelle est dorénavant prohibé sur tout le territoire de la Fédération. Le parquet général a justifié sa décision par la potentielle utilisation à des fins délictueuses ou criminelles des monnaies virtuelles, notamment pour le blanchiment d'argent sale. Il a également fait remarquer que les bitcoins n'ont strictement aucune contrepartie réelle et que les personnes en acquérant le faisaient à leurs risques et périls. En effet, les détenteurs de monnaie virtuelle ne disposent d'aucun moyen juridique de défendre leurs intérêts face aux escrocs pullulant sur internet.

Cependant, le plus dur reste à faire, soit parvenir à faire appliquer cette interdiction. Le parquet fédéral et la banque centrale de Russie planchent dès à présent sur la mise au point de méthodes efficaces de lutte contre la circulation des monnaies virtuelles.

Avant la Russie, la Chine, la Thaïlande et la Finlande se sont déjà engagés sur la voie de la prohibition des bitcoins et autres succédanés de monnaies.

Liens : http://www.medias-presse.info/russie-le-bitcoin-desormais-interdit/6219

Cybercriminality

Un nouveau rançongiciel nommé locky arrive en France Un nouveau rançongiciel nommé locky arrive en France 4 mars 2016 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 ; je le signale aux autorités via la plateforme de signalement « Pharos » (nouvelle fenêtre) external link Votre vigilance est importante, elle peut prévenir la perte de vos données. Publié par : pintejp | mars 7, 2016. Jean-Paul Pinte, expert en cybercriminalité depuis 2006.

Liens : https://cybercriminalite.wordpress.com/2016/03/07/un-nouveau-rancongiciel-nomme-locky-arrive-en-france-un-nouveau-rancongiciel-nomme-locky-arrive-en-france-4-mars-2016-locky-est-un-logiciel-malveillant-dit-rancongiciel-ransomware-q/

Vous avez été 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.

Mais pour vous, qu'en est-il de votre organisation ?

Liens : http://www.om-conseil.fr/vous-avez-ete-attaque-par-un-ransomware-faut-il-payer-la-rancon/

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. 20 mai 2016

Liens : http://www.phonandroid.com/ransomware-pirates-excusent-arnaque-livrent-antidote.html

Les monnaies virtuelles et non traçables

alimentent-elles le financement de la cybercriminalité?

Le bitcoin est utilisé dans la majorité des demandes de rançons (rançongiciels) de piratage informatique à destination des entreprises et des particuliers. Le point avec Solange Ghernaouti de l'Unil, experte en cybersécurité.

Les demandes de rançons après un piratage se multiplient contre les entreprises et les particuliers. Un logiciel malveillant (maliciel) s'immisce dans l'ordinateur et crypte toutes les données informatiques. Alors que la traque classique des policiers pour démasquer les criminels passe par l'analyse des flux financiers, le recours à l'utilisation d'une monnaie virtuelle, comme le bitcoin, efface toute traçabilité.
L'interview complète de Solange Ghernaouti, professeur à l'Unil et experte internationale en cybersécurité, est à lire dans l'édition de mercredi de L'Agefi. 10.05.2016

Liens : http://www.agefi.com/ageficom/news/detail-ageficom/edition/online/article/le-bitcoin-est-utilise-dans-la-majorite-des-demandes-de-rancons-rancongiciels-de-piratage-informatique-a-destination-des-entreprises-et-des-particuliers-le-point-avec-solange-ghernaouti-de-426341.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...

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

Baromètre des menaces DNS : les domaines de ransomware ont vu leur nombre multiplié par 35

Infoblox , le spécialiste du contrôle du réseau, publie le baromètre Infoblox des menaces DNS pour le premier trimestre 2016, faisant ressortir une multiplication par 35 du nombre des nouveaux domaines de ransomware observés par rapport au quatrième trimestre 2015. Cette augmentation spectaculaire a contribué à propulser à un niveau record l'indice global des menaces qui mesure la création d'infrastructures DNS malveillantes (malwares, kits d'exploitation de vulnérabilité, phishing, etc.).

Qu'est-ce qu'une attaque par ransomware ?

Une attaque de ransomware consiste à infecter une machine par un malware pour crypter les données, puis à exiger le paiement d'une rançon en échange de la clé de décryptage. Selon Rod Rasmussen, vice-président cybersécurité d'Infoblox, « la menace du ransomware connaît un formidable bouleversement : il ne s'agit plus de quelques acteurs qui extorquaient un maigre butin à des particuliers mais d'attaques massives, à l'échelle industrielle contre des entreprises de toutes tailles et de tous secteurs, y compris de grands groupes. Notre baromètre des menaces montre que les cybercriminels se ruent pour profiter de cette opportunité. »

Le FBI a révélé récemment que les victimes de ransomware aux Etats-Unis ont déclaré 209 millions de dollars de pertes au premier trimestre 2016, contre 24 millions pour l'ensemble de l'année 2015. Parmi les attaques de grande ampleur survenues au cours de ce trimestre figurent notamment celles lancées en février contre le Hollywood Presbyterian Medical Center de Los Angeles et, en mars, contre MedStar Health à Washington.

Nombre record de nouveaux domaines malveillants

Le baromètre Infoblox des menaces DNS a atteint le niveau record de 137 au 1er trimestre 2016, soit une hausse de 7 % par rapport au chiffre déjà élevé de 128 enregistré au dernier trimestre, battant le précédent record de 133 établi au 2ème trimestre 2015. Le baromètre Infoblox des menaces DNS mesure la création d'infrastructures DNS malveillantes, qu'il s'agisse de l'enregistrement de nouveaux domaines ou du piratage de domaines ou d'hôtes légitimes existants. L'indice de référence est 100, correspondant à la moyenne des résultats sur 8 trimestres pour les années 2013 et 2014.

Cinq nouveaux pays en tête de liste des domaines malveillants

Les Etats-Unis demeurent le principal pays hébergeant des domaines malveillants nouvellement créés ou exploités, représentant 41 % des ob-

servations, une proportion en net recul par rapport à leur domination écrasante (72 %) au trimestre précédent. Cinq autres pays présentent un fort regain d'activité :

Portugal17 %

Russie12 %

Pays-Bas10 %

Royaume-Uni8 %

Islande6 %

L'Allemagne, qui avait enregistré au quatrième trimestre près de 20 % des nouveaux domaines malveillants et des infrastructures associées, est quasiment sortie de la liste, chutant à moins de 2 %.

« Les cybercriminels ne se privent pas de la possibilité d'exploiter une infrastructure sophistiquée, et tous les pays figurant dans la liste ce trimestre répondent à cette condition », commente Lars Harvey, vice-président stratégie de sécurité d'Infoblox. « Cependant, la répartition géographique montre que, tels des blattes fuyant la lumière, cela ne dérange pas les cybercriminels de changer de cibles. »

Les kits d'exploitation demeurent la menace numéro un

Les kits d'exploitation – des outils à louer qui facilitent la tâche des cybercriminels en automatisant la création et la diffusion de malwares – demeurent la menace numéro un, représentant un peu plus de la moitié de l'indice général. A l'instar des trimestres antérieurs, Angler reste le kit le plus utilisé mais un nouveau prétendant revient du diable vauvert : les observations de Neutrino ont ainsi progressé de 300 %.

Angler est réputé pour avoir inauguré la technique de masquage de domaine, destinée à contrer les stratégies de blocage sur la base de la réputation, et pour infiltrer des URL malveillantes dans des réseaux publicitaires légitimes, dirigeant les visiteurs vers des sites web qui leur injectent un malware même s'ils ne cliquent pas sur des liens infectés. Les diverses occurrences des récentes campagnes Neutrino observées infectent les systèmes des victimes avec différentes versions de ransomware telles que Locky, Teslacrypt, Cryptolocker2 et Kovter. juin 2016.

Liens : http://www.globalsecuritymag.fr/Barometre-des-menaces-DNS-les,20160601,62564.html

Kaspersky Lab a développé un outil contre le ransomware Crypt XXX

Kaspersky Lab propose gratuitement RannohDecryptor pour déchiffrer et récupérer les données des victimes du ransomware Crypt XXX.

Les cybercriminels engrangent 30 millions de dollars tous les 100 jours avec le ransomware Cryptolocker. Et ce type de logiciel malveillant ne cesse de proliférer. L'un des derniers en date est le ransomware Crypt XXX. Il se propage via des spams contenant des pièces jointes ou des liens vers des sites infectés. Le logiciel chiffre les fichiers du système via RSA-4096, un algorithme de chiffrement fort qui ajoute une extension .crypt à leur nom. L'objectif : voler des données, verrouiller l'accès à des fichiers... Les victimes sont informées du piratage et doivent souvent payer une rançon en Bitcoins.

Mais Kaspersky Lab est parvenue à trouver une parade pour qu'une victime récupère ses données sans avoir à débourser. RannohDecryptor détecte l'Angler exploit kit (un composant que les cybercriminels utilisent pour actionner leurs malwares) utilisé par Crypt XXX dès le début de l'infection. Pour déchiffrer les fichiers corrompus, il aura besoin d'une version originale non chiffrée d'au moins un fichier touché par Crypt XXX. D'où l'intérêt de sauvegarder régulièrement ses données.

Pour développer cet outil, l'entreprise précise dans son communiqué qu'elle a exploité une maladresse des hackers : *« les criminels se targuaient d'utiliser RSA-4096, ce qui nous a permis de développer un outil de déchiffrement ».*

Fedor Sinitsyn, Senior Malware Analyst chez Kaspersky Lab, n'a cependant pas souhaité en dire plus concernant l'exploitation de cette erreur et sur le fonctionnement détaillé de RannohDecryptor: *« Nous préférons ne pas divulguer de détails à ce propos afin de ne pas fournir trop d'informations susceptibles d'aider les cybercriminels. Cependant, nous pouvons confirmer que si les développeurs de ransomwares mettent au point une formule de chiffrement forte, il est alors impossible de décrypter les fichiers. Il existe néanmoins des cas où ils font des erreurs, et c'est ce qui nous permet de récupérer des fichiers cryptés. »*

Pas de solution miracle

Plus de 50 familles de ransomwares circulent et l'algorithme

universel qui permet de bloquer ou contrôler les attaques n'existe pas. Même si d'autres solutions s'offrent à l'utilisateur comme le précise Fedor Sinitsyn : *« Cet outil ne fonctionne que pour CRYPTXXX mais il existe beaucoup d'autres outils ransomwares de décryptage disponibles, à la fois de Kaspersky et d'autres sources. En raison de la façon dont chaque programme de ransomware est écrit, chacun d'entre eux nécessite une solution de décryptage séparée. »*
Avant d'installer une solution de sécurité, quelques gestes simples à adopter permettent de se prémunir face à cette menace potentielle: sauvegarder régulièrement ses données, installer les mises à jour critiques de ses navigateurs et systèmes d'exploitation. 09 mai 2016.
Liens : http://www.linformaticien.com/actualites/id/40432/kaspersky-lab-a-developpe-un-outil-contre-le-ransomware-crypt-xxx.aspx

Immeuble Ahmed FRANCIS. 16306 BEN AKNOUN - ALGER

Téléphone : +213 (0)21 59 53 10 / Fax : (0)21 59 51 96
www.mf.gov.dz