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°49 JUIN 2016

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

Les 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 tentaives d'installation de ces logiciels malveillants. Même Apple, d'ordinaire assez épargné par les virus, a été touché il y a peu

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.

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.

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

This story can fit 75-125 words.

Your headline is an important part of the newsletter and should be considered carefully.

In a few words, it should accurately represent the contents of the story and draw readers into the story. Develop the headline before you write the story. This way, the headline will help you keep the story focused.

Examples of possible headlines include Product Wins Industry Award, New Product Can Save You Time!, Membership Drive Exceeds Goals, and New Office Opens Near You.

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

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.

> **"Pourquoi** braquer une banque alors **que l'on peut** organiser **"tranquillement** un chantage à échelle internationale du fond de son canapé ?

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.

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

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.

L'éditeur d'antivirus McAfee a déjà enregistré 120.000 virus de ce genre en 2012

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 pédo-pornographique. "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.

Liens : http://o.nouvelobs.com/high-tech/hacker-ouvert/20130214.OBS8969/le-cyber-kidnapping-nouvelle-arme-des-hackers.html

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.

Liens : http://www.clubic.com/antivirus-securite-informatique/actualite-541314-europol.html

Comment devenir une mule financière ?

Pour les criminels, Internet est devenu un maillon essentiel de leur chaîne de blanchiment d'argent. Ainsi, ils peuvent construire des réseaux d'agents aux quatre coins du globe prêts à opérer contre rétributions dans ce processus.

L'argent blanchi grâce à des mules financières

Comme pour le trafic de drogue, les cybercriminels ont également leurs mules. Dans ce cas, il ne s'agit pas de transporter de la drogue, mais de l'argent afin de complexifier la traçabilité des flux de blanchiment. La mule se voit confier une somme d'argent qu'elle doit remettre à un certain endroit, une autre banque ou un service de transfert international d'argent en échange d'une rétribution financière. A noter que ce type d'activité n'est pas anodine car elle est bien entendu pénalement répréhensible.

Des mules financières recrutées grâce aux spams

Internet est aujourd'hui un canal incontournable lorsque l'on recherche un nouvel emploi. Ce n'est donc pas étonnant que les cybercriminels utilisent également ce même principe pour recruter des mules via des pseudo-emplois habillés de revenus alléchants. Ainsi, pour la recherche de mules financières, ils utilisent aujourd'hui très souvent de larges campagnes d'envois de spams.

Inutile de chercher à obtenir une information quelconque sur l'expéditeur originel par ce biais. Dans un email, le format de l'expéditeur peut être modifié très facilement et permettre d'utiliser des adresses totalement valables comme celle du londonstockexchange.com par exemple. C'est néanmoins pas important dans le cas de ces emails car les différentes adresses de réponse sont sans lien avec ces expéditeurs et utilisent des messageries publiques distinctes comme gmail ou aol.com par exemple.

Difficile de croire à un vrai emploi

Au vu des nombreux éléments incohérents tant sur la forme que le contenu de tels emails, la véracité de telles propositions d'emploi est donc facilement contestable. Il s'avère néanmoins que, comme pour la combinaison *spam* + *phishing*, de telles campagnes obtiennent la postulation passive ou volontaire de personnes dans le besoins … avec le risque qu'elles se retrouvent bien seules devant le juge.

Liens : https://www.ledecodeur.ch/2012/11/18/comment-devenir-une-mule-financiere/

Les "rançongiciels" ou quand des pirates kidnappent vos données informatiques

High-Tech. Une nouvelle forme de piratage informatique sévit actuellement sur le web. Les pirates prennent en otage en quelque sorte des données informatiques, pour ensuite demander une rançon en échange afin de les récupérer.

Valerie Goss conseille les couples dont le mariage bat de l'aile. Un jour, cette Californienne allume machinalement son ordinateur et se rend compte que la totalité de ses données ont été "prises en otages" par des pirates qui exigent une rançon en bitcoins (système de paiement sur Internet). A l'aide d'un codage baptisé "ransomware" ou "rançongiciel", les cyberdélinquants sont parvenus à encrypter les données de Mme Goss, lui en interdisant l'accès. Les pirates lui demandent alors 500 dollars en bitcoins, une monnaie virtuelle très difficile à pister, en échange du sésame qui lui permettra de récupérer ses dossiers. Et ils préviennent : si elle ne paye pas dans les 24 heures, la rançon montera à 1.000 dollars..

"J'étais sous le choc. J'avais l'impression qu'on m'avait détroussée", raconte la thérapeute. Son fils entreprend alors des recherches sur internet et constate qu'un quart des victimes de ce genre d'arnaques ne revoient jamais leurs données, même quand elles payent. Valerie Goss refuse de payer. A la place, elle s'achète un nouvel ordinateur qu'elle dote d'un logiciel de sécurité renforcé. Elle n'a bien sûr jamais revu ses données "kidnappées", mais elle a sans doute bien fait de ne pas céder aux pirates, estiment certains analystes..

Un Americain sur trois prêt à payer

Les "rançongiciels" n'ont rien de nouveau, mais ils connaissent un véritable engouement, relève M. Kleczynski. D'autant que les pirates ciblent désormais aussi les smartphones, et surtout les modèles qui fonctionnent sous Android. Et les Etats-Unis sont l'un des terrains de chasse favoris des "ravisseurs de données", parce que les Américains stockent plus que quiconque leurs données personnelles sur leurs ordinateurs et leurs téléphones..

Une étude publiée l'an dernier par Lookout révélait d'ailleurs qu'un Américain sur trois serait prêt à payer pour récupérer ses photos, contacts et autres dossiers stockés sur son smartphone si ces données étaient prises en otages. Pour se prémunir contre ce genre de déboires, les informaticiens conseillent aux internautes de faire attention aux liens sur lesquels ils cliquent et de mettre à jour régulièrement leurs logiciels de protection. Autre mesure : toujours dupliquer les données stockées sur l'ordinateur et garder des copies sur le "cloud" (informatique dématérialisée), et sur des supports qui ne sont pas ou peu connectés à internet. 27 février 2015.

Liens : http://lci.tf1.fr/high-tech/les-rancongiciels-ou-quand-des-pirates-kidnappent-les-donnees-8571085.html

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. juin 2016.
Liens : http://www.globalsecuritymag.fr/Le-ransomware-est-un-modele,20160601,62556.html

La prise d'otage 2.0 est née :

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.

Les Cryptolockers font des dégâts

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. 26 mai 2016.

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

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.

Caption describing picture or graphic.

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.

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

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
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 tri-

mestre 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).Créé: 30.04.2016.

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

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'il s'agit des forces de l'ordre, mais après avoir examiné native, l'alternative, c'est-à-dire ne jamais revoir ses données, de nombreuses entreprises préfèrent payer afin de recommencer à travailler.

Liens : http://www.lemondeinformatique.fr/actualites/lire-infectee-par-un-cryptolocker-la-police-du-massachusetts-paie-500$-de-rancon-60783.html

Immeuble Ahmed FRANCIS. 16306 BEN AKNOUN - ALGER

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