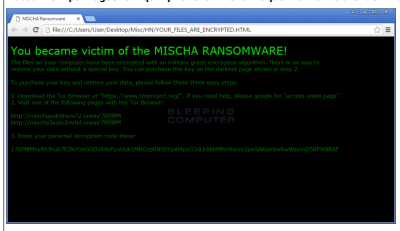
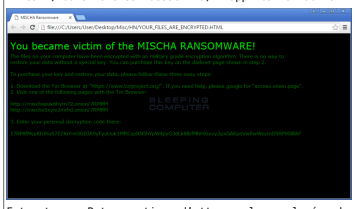
Mischa, le ransomware successeur de Petya

Mischa, le ransomware successeur de Petya

Apparu au mois de mars, le ransomware Petya a ouvert une nouvelle voie dans le développement des ransomwares. Il s'agissait du premier cas d'un malware qui allait au-delà du chiffrement des fichiers sur les disques locaux et partagés et qui préférait s'attaquer à la table de fichiers principale



Ceci étant dit, Petya n'était pas infaillible et les chercheurs ont été rapidement en mesure de créer un outil de restauration de certains des fichiers chiffrés par ce malware. Les individus malintentionnés n'ont pas perdu leur temps et ils ont trouvé le moyen de contourner une autre lacune de Petya : sa dépendance vis-à-vis de la volonté de la victime qui doit octroyer au malware les autorisations d'administrateur pour accéder à la table de fichiers principale (MFT).
Un nouveau programme d'installation de Petya a été détecté la semaine dernière. Celui-ci utilise un scénario de réserve. Si le malware n'obtient pas les autorisations d'administrateur au lancement, c'est un autre ransomware qui sera installé sur la machine infectée, en l'occurrence Mischa.
D'après les explications de Lawrence Abrams, de chez Bleeping Computer, les autorisations d'administrateur indispensables au fonctionnement de Petya figurent dans le manifeste de la version originale. Dans les commentaires envoyés à Threatpost, Lawrence Abrams explique « qu'avant l'exécution du code, Windows affiche la boîte de dialogue UAC qui sollicite ces autorisations. Si le service UAC est désactivé, l'application est exécutée automatiquement avec [les autorisations d'administrateur]. Si l'utilisateur clique sur « No » dans la fenêtre UAC, l'application n'est pas exécutée et, par conséquent, l'installation de Petya n'a pas lieu ».
Pour les exploitants de Petya, ces échecs représentent un gaspillage de ressources d'après Lawrence Abrams. Pour rectifier le tir, ils ont empaqueté un autre ransomware avec le programme d'installation. Il s'agit de Mischa qui sera exécuté si l'option « Petya » n'a pas pu être mise en œuvre.
Le manifeste de la nouvelle version indique que le fonctionnement requiert les données du compte utilisateur. Dans ce cas, Windows autorise le lancement de l'application sans afficher d'avertissement UAC. Comme l'explique Lawrence Abrams, « au lancement du programme d'installation, il sollicite les autorisations d'administrateur conformément à ses paramètres. La boîte de dialogue UAC s'affiche et si l'utilisateur choisit « Yes », ou si UAC est désactivé, l'application obtient les autorisations d'administrateur et installe Petya. Dans le cas contraire, c'est Mischa qui sera installé. Cette méthode est très intelligente ».



Entre temps, Petya continue d'attaquer les employées des services des ressources humaines allemands à l'aide de messages non sollicités qui contiennent des liens vers un fichier malveillant dans le cloud. Au début, les individus malintentionnés utilisaient Dropbox, mais depuis le blocage des liens Dropbox malveillants, ils se sont rabattus sur le service allemand TelekomCloud. Le fichier exécutable se dissimule sous les traits d'un fichier PDF qui serait un prétendu CV d'un candidat à un poste libre. Il contient même une photo.
« Lorsque l'utilisateur télécharge le fichier exécutable, l'icône PDF s'affiche, ce qui laisse penser qu'il s'agit bien d'un CV au format PDF » explique Lawrence Abrams. Toutefois, lorsque ce fichier est ouvert, il tente d'installer Petya. Et si cela ne marche pas, il installe le ransomware Mischa.
Le comportement de Mischa est identique à celui des autres ransomwares standard. Il analyse le disque local à la recherche de fichiers portant certaines extensions. Il chiffre les fichiers à l'aide d'une clé AES et ajoute à leur nom une extension de 4 caractères, par exemple 7GP3. Lawrence Abrams explique que « lorsque Mischa chiffre le fichier, il conserve la clé de chiffrement à la fin du fichier obtenu. Il convient de noter qu'il ne chiffre pas uniquement les fichiers traditionnels dans ce genre d'attaque (PNG, JPG, DOCX, etc.), mais également les fichiers EXE. »
Une fois qu'il a chiffré les fichiers, Mischa exige le versement d'une rançon de 1,93 bitcoins (environ 875 dollars américains) pour le déchiffrement. La somme doit être payée via le site Tor. Il n'existe pas encore d'outil de déchiffrement pour ce ransomware. « Nous conseillons aux victimes de vérifier avant tout la conservation des clichés instantanés à l'aide de Shadow Explorer. Ils pourraient être utile pour restaurer une ancienne version des fichiers chiffrés » conclut Lawrence Abrams.

Article du Kaspersky Lab

Réagissez à cet article

Source : *Petya possède un suppléant : Mischa – Securelist*

Forte hausse des applications Android malveillantes

Forte hausse des applications Android malveillantes

Les applications Android malveillantes et les ransomwares dominent le paysage des menaces au 1er trimestre 2016.

La société Proofpoint a publie son Rapport trimestriel sur les menaces, qui analyse les menaces, les tendances et les transformations observées au sein de notre clientèle et sur le marché de la sécurité dans son ensemble au cours des trois derniers mois. Chaque jour, plus d'un milliard de courriels sont analysés, des centaines de millions de publications sur les réseaux sociaux et plus de 150 millions d'échantillons de malwares afin de protéger les utilisateurs, les données et les marques contre les menaces avancées. On apprend, entre autres, que 98 % des applications mobiles malveillantes examinées au 1er trimestre 2016 ont ciblé des appareils Android. Cela demeure vrai en dépit de la découverte médiatisée d'un cheval de Troie pour iOS et de la présence persistante d'applications iOS ou officieuses dangereuses. Les applications Android malveillantes sont de plus en plus nombreuses.

75 % des attaques de phishing véhiculées par des e-mails imposteurs comportent une adresse «répondre à » usurpée afin de faire croire aux destinataires que l'expéditeur est une personne représentant une autorité. Ce type de menaces est de plus en plus mature et spécialisé, et c'est l'un des principaux ciblant les entreprises aujourd'hui, qui leur auraient coûté 2,6 milliards de dollars au cours des deux dernièresannées selon les estimations.

Applications Android malveillantes

Les ransomwares se sont hissés aux premiers rangs des malwares privilégiés par les cybercriminels. Au 1er trimestre, 24 % des attaques par e-mail reposant sur des pièces jointes contenaient le nouveau ransomware Locky. Seul le malware Dridex a été plus fréquent.

L'e-mail reste le principal vecteur de menaces : le volume de messages malveillants a fortement augmenté au 1er trimestre 2016, de 66 % par rapport au 4ème trimestre 2015 et de plus de 800 % comparé au 1er trimestre 2015. Dridex représente 74 % des pièces jointes malveillantes.

Chaque grande marque analysée a augmenté ses publications sur les réseaux sociaux d'au moins 30 %. L'accroissement du volume des contenus générés par les marques et leurs fans va de pair une accentuation des risques. Les entreprises sont constamment confrontées au défi de protéger la réputation de leurs marques et d'empêcher le spam, la pornographie et un langage grossier de polluer leur message.

Les failles de Java et Flash Player continuent de rapporter gros aux cybercriminels. Angler est le kit d'exploitation de vulnérabilités le plus utilisé, représentant 60 % du trafic total imputable à ce type d'outil. Les kits Neutrino et RIG sont également en progression, respectivement de 86 % et 136 %. (ProofPoint)… [Lire la suite]

Article de Damien BANCAL

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

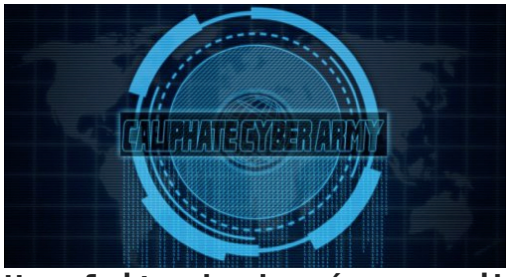
Réagissez à cet article

Source : *Forte hausse des applications Android malveillantes – Data Security BreachData Security Breach*

La France visée par une nouvelle cyberattaque de l’EI

La France visée par une nouvelle cyberattaque de l’EI

Les équipes CybelAngel ont repéré lundi 16 mai une base de coordonnées de citoyens français et américains publiée sur le site justepaste.it. L'utilisateur à l'origine de la publication se revendique de la Caliphate Cyber Army (#CCA).



Une fuite de données sensibles mais accessibles depuis 6 mois

Le message commence par une représentation de la basmala, un verset leitmotiv du Coran à la gloire de Dieu. Des mots-dièse "CCA #CyberCaliphate #UCC" et un logo de la Caliphate Cyber Army viennent compléter la revendication introductive.

Vient ensuite une liste de 77 emails, mots de passe, numéros de téléphone, adresses, comptes Paypal et soldes de compte Paypal. La liste concerne 38 adresses françaises, 31 américaines, 6 australiennes, 1 philippine et 1 néerlandaise. Les coordonnées semblent être uniquement personnelles et non professionnelles.

Après analyse, il semblerait que les données exposées ici étaient déjà présentes sur le Dark Web avant cette publication. En effet, un message publié le 12 janvier dernier sur le site pastebin.com reprenait 35 paires d'emails/mots de passe correspondant exactement à ceux publiés le 16 mai par la Cyber Caliphate Army. A l'aune de cette troublante similarité entre le 12 janvier et le 16 mai, la CCA reprendrait à son compte des adresses en libre accès sur le Dark Web ; ce qui ne serait pas la première fois.

Une Cyber Armée aux attaques peu techniques mais à fort impact médiatique

La Cyber Caliphate Army est issue de la volonté de l'Etat Islamique de projeter son action dans l'espace virtuel en 2014. Elle est dans un premier temps dirigée, et probablement entièrement constituée par Junaid Hussain, un hacker anglais.

De son lancement pendant l'été 2014 jusqu'à l'assassinat de Hussain par un drône américain en août 2015, la CCA a revendiqué une série de cyberattaques peu sophistiquées mais très médiatiques : plusieurs défacements de comptes Twitter du Commandement Central des Armées américaines (CENTCOM), de Newsweek, de chaînes de télévisions américaines, l'arrêt des retransmissions des 11 chaînes de TV5 Monde (action dont la parenté est mise en doute par de nombreux experts).

Cette nouvelle fuite souligne les faiblesses de la Cyber Armée du Califat

Depuis la mort de Husain, la CCA a mené des actions nettement moins symboliques : des défacements indiscriminés de milliers de sites et des actions à la parenté douteuse dont des fermetures de systèmes informatiques revendiquées ex-post et des diffusions de données en réalité déjà en ligne, comme celle détectée ce 16 mai par CybelAngel.

Face à ce potentiel de nuisance visiblement réduit, 4 groupuscules d'hacktivistes islamistes dont la Cyber Caliphate Army ont proclamé leur union en un United Cyber Caliphate en avril ainsi que nous vous le rapportions la semaine dernière. Quelques semaines plus tard, le groupuscule Cyber Caliphate Army revendique pourtant en son nom propre une action et ne mentionne le United Cyber Caliphate qu'en un hashtag UCC. Il semblerait que l'intégration des différents groupes hacktivistes islamistes prenne plus de temps que prévu.

Article de CybelAngel Analyst Team

Réagissez à cet article

Source : *La France visée par une nouvelle cyberattaque de l'EI*

Un vague massive de spams JavaScript distribue le ransomware Locky

Un vague massive de spams JavaScript distribue le ransomware Locky

---

Les pays européens sont aujourd'hui victimes d'une vague de spams essayant d'exécuter un code JavaScript installant le redoutable ransomware Locky.

Au cours de la semaine écoulée, un grand nombre d'ordinateurs à travers l'Europe – et d'autres endroits dans le monde dont les Etats-Unis et le Canada – ont été touchés par une campagne massive de spams transportant des pièces jointes JavaScript malveillantes qui installent le ransomware Locky. Les pièces jointes sont généralement des fichiers d'archives .zip qui contiennent .js ou fichiers .jse intérieur. Ces fichiers s'exécutent directement sous Windows sans avoir besoin d'applications supplémentaires.

L'éditeur spécialisé dans la sécurité ESET a observé un pic dans les détections de JS / Danger.ScriptAttachment, un téléchargeur malware écrit en JavaScript qui a démarré le 22 mai et a atteint son sommet le 25 mai. JS / Danger.ScriptAttachment permet de télécharger divers programmes malveillants à l'insu des internautes, mais il a récemment été adapté pour distribuer Locky, un programme malveillant répandu qui utilise un chiffrement fort pour crypter les fichiers des utilisateurs. Cependant, il est très rare que des gens envoient des applications légitimes écrites en JavaScript par email. Les utilisateurs devraient éviter d'ouvrir ce type de fichiers.

La France touchée à 36%

De nombreux pays en Europe ont été touchés. Les taux de détection les plus élevés ont été observés au Luxembourg (67%), en République tchèque (60%), en Autriche (57%), aux Pays-Bas (54%), au Royaume Unie (51%) et en France 36%. Les données de télémétrie de l'éditeur ont également montré des taux de détection importants pour cette menace au Canada et aux États-Unis. Bien que Locky n'a pas de défauts connus qui permettraient aux utilisateurs de déchiffrer leurs fichiers gratuitement, les chercheurs en sécurité de Bitdefender ont développé un outil gratuit qui peut prévenir les infections Locky. L'outil trompe le ransomware en lui indiquant que l'ordinateur est déjà infecté.
L'utilisation de fichiers JavaScript pour distribuer Locky a commencé un peu plus tôt cette année, ce qui a incité Microsoft à publier une alerte à ce sujet en avril dernier.
Article de Lucas Mearian/ IDG NS (adaptation SL)

Réagissez à cet article

Source : *Un vague massive de spams JavaScript distribue le ransomware Locky – Le Monde Informatique*

L’adoption de l’analyse comportementale appelée à s’étendre

L’adoption de l’analyse comportementale appelée à s’étendre

Selon Gartner, les entreprises se tournent de plus en plus vers l'analyse comportementale pour améliorer la détection des incidents et renforcer l'efficacité de leurs SOC. De quoi pousser à une inéluctable consolidation du marché.

L'analyse comportementale – des utilisateurs comme des flux réseau ou des entités connectées à l'infrastructure – a fait une entrée remarquée sur le marché de la sécurité l'an passé. Mais selon Gartner, les solutions isolées actuellement proposées vont être rapidement appelées à s'intégrer, au point d'encourager à une consolidation des acteurs.

Dans une note d'analyse, Avivah Litan et Eric Ahlm résument la situation : « les besoins des acheteurs pour détecter les brèches de tout type vont pousser à la consolidation des systèmes de détection basés sur le comportement, tels que les systèmes d'analyse du comportement des utilisateurs et des entités (UEBA), de détection et de réponse sur les points de terminaison (EDR), et d'analyse du trafic réseau (NTA) ».

Des catégories bien distinctes

Dans la première catégorie, le cabinet mentionne par exemple Securonix, LightCyber, Exabeam et Gurucul. Le premier étant notamment utilisé par HP au sein du système de gestion des informations et des événements de sécurité (SIEM) ArcSight. Pour l'EDR, il prend pour exemples Hexis et Ziften, mais pourrait également évoquer SentinelOne, notamment. En matière de NTA, le cabinet fait référence à SS8 et Niara, mais il faut également compter avec Vectra Networks ou encore Darktrace, entre autres.

Mais voilà, comme le relèvent les deux analystes, les acheteurs de solutions de sécurité ne veulent pas seulement détecter les brèches, « mais aussi y répondre rapidement et efficacement ». S'il le fallait, l'édition 2016 de RSA Conference a fait la démonstration de cette tendance. Ce besoin doit conduire à une « collision du marché entre systèmes de détection basés sur le comportement et systèmes d'orchestration et de réaction ». Et cela parce que ni UEBA, ni EDR, ni NTA ne semble en mesure d'apporter, seul, une réponse complète aux besoins des entreprises.

Des capacités différentes

Ainsi, Avivah Litan et Eric Ahlm soulignent que la première catégorie est efficace pour identifier des compromissions de comptes utilisateurs ou des acteurs internes malveillants, mais peut montrer ses limites dans la détection des incidents impliquant des logiciels malveillants. De son côté, « l'EDR peut être efficace pour trouver les comportements mauvais sur un hôte et identifier les objets malicieux », mais plus faible lorsqu'il s'agit de mettre le doigt sur une menace interne. Enfin, les outils de NTA « peuvent être capables de trouver les conséquences de deux types d'événements, mais n'ont pas les données relatives aux utilisateurs ou aux hôtes nécessaires pour confirmer l'incident ».

Analyse comportementale : la clé de la sécurité ?

D'autres outils peuvent venir en outre compléter l'édifice, qu'il s'agisse des SIEM ou des systèmes de gestion du renseignement sur les menaces comme ceux d'Anomali, de ThreatConnect ou encore de ThreatQuotient. Au final, pour les analystes de Gartner, le marché s'avère « bruyant, chaotique et encombré », pollué notamment par des discours marketing qui s'articulent « autour des mêmes thèmes clés tels que analytique, machine learning, automatisation, et autres termes similaires, bien que leur application de ces fonctionnalités soit largement différente en ce qui concerne ce qu'ils peuvent faire dans leurs rôles spécifiques ». Bref, la confusion règne.

Des performances à démontrer

Et cela d'autant plus que, selon Gartner, les spécialistes de l'analytique appliquée à la sécurité peinent encore à faire la démonstration de la valeur de leurs solutions. Lors d'échanges, ceux-ci cherchent surtout à se différentier en évoquant l'étendue ou le volume de leurs échantillons de données, le framework analytique utilisé ou encore la technologie analytique employée – apprentissage machine, deep learning, et intelligence artificielle sont là largement mis à contribution. Las, si le cabinet voit là des « facteurs importants et des sujets de discussions divertissants », tous « échouent à constituer un différentiateur majeur » car, pour Avivah Litan et Eric Alhm, « les éditeurs devraient d'abord se concentrer sur la manière dont le recours à l'analytique rend leur technologie meilleure en termes de résultats, de manière mesurable. Par exemple, dans quelle mesure trouver des attaques inconnues est plus efficace en pourcentage avec l'analytique que chercher à trouver un logiciel malveillant inconnu sans ».

Une inéluctable consolidation

Pour autant, les deux analystes ne contestent pas la valeur intrinsèque que l'analytique apporte à la détection de brèches. Mais ils soulignent l'importance des étapes suivant la détection. D'où la convergence anticipée entre acteurs de la détection basée sur l'analytique et de l'orchestration/réaction. Et c'est peut-être là que le SIEM est appelé à jouer une nouvelle carte, pour dépasser des limites bien connues. Dès lors, pour Gartner, les acteurs de détection devaient « soit prévoir de nouer formellement des partenariats avec des acteurs du SIEM […] ou se préparer à reprendre des fonctions clés du SIEM ».

Le cabinet s'attend donc clairement à une consolidation prochaine de systèmes de détection de menaces basés sur les comportements, mais il n'exclue pas l'émergence de solutions de type plateforme dédiées à l'investigation et à la réponse aux incidents. Des solutions sur lesquelles les composant de détection et de réponse viendraient se greffer. Et n'est-ce pas justement ce que cherche à proposer un Phantom Cyber ?

Article de Valéry Marchive

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *L'adoption de l'analyse comportementale appelée à s'étendre*

Les six choses à faire pour éviter 95% des attaques informatiques

Les six choses à faire pour éviter 95% des attaques informatiques

La cybersécurité est essentielle, d'accord, mais par où commencer ? Pour vous aider à faire le premier pas, nous avons identifier 6 principes clés qui, lorsqu'ils sont suivis, peuvent éviter la grande majorité des attaques.

1/ FAIRE DE LA SÉCURITÉ UN PROCESS (CE N'EST PAS UN PRODUIT)

« Je dois protéger mon entreprise ? Certes. Quel produit faut-il que j'achète ? » La réflexion peut sembler naturelle. Après tout, autant faire appel à des professionnels. Le problème, c'est qu'on ne sécurise pas son entreprise en signant un chèque. La cybersécurité est avant tout une façon de penser, et passe par une organisation, par la mise en place de règles et méthodes. Elle implique de connaître son système d'information sur le bout des doigts pour en cartographier la surface d'attaque, de savoir tout ce qui est connecté (et ce qui ne doit pas l'être). Elle implique aussi de déterminer quels sont les services et les données qui sont réellement cruciaux au fonctionnement de la structure pour s'assurer que l'on concentre ses forces là où elles doivent l'être, sans s'évertuer à défendre plus que nécessaire des ressources non critiques. *« La sécurité est une composante au service du coeur de métier,* explique Eric Filiol, directeur du laboratoire de virologie et de #cryptologie opérationnelles de l'école d'ingénieurs ESIEA. *Il faut comprendre son métier et ce qui est critique. »* La stratégie doit être sensée pour que les ressources engagées (financières, humaines, temporelles) soient utilisées au mieux.

2/ PATCHER, PATCHER, PATCHER

Les révélations sur les méthodes de la NSA ou les gros titres sur les attaques contre des opérateurs d'importance vitale qui s'étalent sur des mois voire des années peuvent laisser penser que les hackers exploitent systématiquement des failles complexes et jamais référencées (appelées « zero days ») pour s'infiltrer dans un SI. Rien n'est moins vrai. Ces zero days ne sont utilisés qu'extrêmement rarement et seulement pour les cibles les plus importantes. La très grande majorité des attaques ciblent au contraire des failles bien connues et pour lesquelles existent déjà des correctifs de sécurité, souvent depuis des années. C'est pourquoi il est capital de faire systématiquement ces mises à jour (aussi bien pour le système d'exploitation que les frameworks ou les applications), et de concevoir son SI autour de cette nécessité. *« Il faut savoir que les criminels font du reserve engineering sur les patchs dès leur sortie pour exploiter les failles qu'ils corrigent. Auparavant cela leur prenait des mois, aujourd'hui ce ne sont plus que des heures,* détaille Thomas Tschersich, director of IT security chez Deutsche Telekom.*Et ils automatisent ensuite le processus pour toucher de très nombreuses cibles. »* Et ce besoin reste le même dans le cas d'un environnement de production industriel qui se doit d'être opérationnel 365 jours par an. La perception selon laquelle les environnements industriels sont fondamentalement différents des environnements de bureau est fausse et contribue à renforcer leur vulnérabilité.

3/ NE PAS SE CROIRE NON CONCERNÉ

Si les réseaux industriels sont de plus en plus visés par des attaques informatiques, c'est parce qu'ils y sont particulièrement vulnérables. La faute à l'évolution dramatique de la connectivité à Internet au cours des 20 dernières années. Lors de leur conception, il était assumé que ces systèmes ne couraient pas de risques car ils n'étaient pas visibles. Quand bien même ce fut jamais vrai, ce n'est définitivement plus le cas. Des services gratuits comme shodan.io permettent depuis des années de chercher parmi des centaines de milliers de systèmes ouverts, connectés à Internet sans aucune protection. Cela va de simples caméras de surveillance (résidentielles ou industrielles) jusqu'aux ICS qui supervisent le parc machine, que les opérateurs laissent sans protection car ils veulent pouvoir en prendre facilement le contrôle à distance. *« Il y a beaucoup de négligence et de mauvaises pratiques,* assène Frédéric Planchon, PDG de FPC Ingénierie. *Cela laisse des portes ouvertes à des malwares qui ne sont normalement pas si nocifs. »* Peu importe la taille de votre installation ou la nature de votre activité, si vous êtes vulnérables, vous serez tôt ou tard attaqué. Et ce même lorsqu'il n'y a rien à en obtenir, car de nombreux hackers agissent simplement « pour le sport ».

4/ PROTÉGER SES DONNÉES

La meilleure façon de garantir la sécurité de ses données, que ce soit contre le vol ou contre des attaques de type ransomwares, c'est de prendre les mesures adéquates en amont. Cela passe par deux axes clés : le chiffrement et la sauvegarde. Le chiffrement garantit que seuls les individus autorisés peuvent accéder aux données, même si le canal de communication ou le support de stockage est compromis. Ainsi, même en cas de vol, les dégâts restent minimaux. De son côté, la sauvegarde évite la perte de données, qu'elle soit dûe à un accident ou à un acte de malveillance. Une politique de sauvegarde rigoureuse et régulière peut faire la différence entre « plus de peur que de mal » et « la clé sous la porte ».

5/ FORMER SES TROUPES

Une vaste majorité d'attaques ont un point commun : l'erreur humaine. Un collaborateur qui ouvre le mauvais email ou clique sur le mauvais lien. Un autre qui perd son appareil ou sa clé USB. Un troisième qui laisse traîner ses identifiants de connexion (ex. post-it sur l'écran) ou les communique par erreur/inattention… La sécurité n'est pas innée, elle s'enseigne. Il est impératif de former les équipes aux bonnes pratiques à adopter et de les sensibiliser aux conséquences que la négligence peut avoir. Les rendre personnellement responsables de la protection de leurs données et appareils au travers de mesures simples peut suffire à largement diminuer les accidents.

6/ SÉCURISER AUSSI LES ACCÈS PHYSIQUES

Une #attaque informatique n'est pas forcément menée depuis l'autre bout du monde. Il faut donc s'assurer en premier lieu que le périmètre de l'entreprise est sécurisé pour limiter les accès non autorisés en interne. Car le « social engineering », qui consiste à obtenir accès à un système en trompant son interlocuteur, est au coeur de nombreuses attaques. Il suffit parfois de mettre un uniforme de réparateur, de prendre une boîte à outils et de demander poliment l'accès à un local technique pour qu'on vous ouvre. Ou de mettre un costume et de se tenir devant une porte les bras chargés de documents. *« Nous appelons ça les attaques 'femme de ménage', et cela permet de prendre le contrôle d'un serveur en 5 secondes, »* explique Eric Filiol. Autre exemple, lorsque le réseau Wi-Fi interne d'une usine, non protégé car l'accès au bâtiment est restreint, peut aussi être capté depuis le parking… Les cas de figure sont nombreux et leur exploitation bien documentée. Ces éléments doivent donc systématiquement être pris en compte.

Article de Julien BERGOUNHOUX

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Cybersécurité : Les six choses à faire pour éviter 95% des attaques*

La France adopte son arsenal anti-hackers

La France adopte son arsenal anti-hackers

La loi de programmation militaire a placé le secteur financier en première ligne des 12 opérateurs d'importance vitale, soumis à de nouvelles règles de sécurité.

C'est un test d'envergure pour les banques françaises. L'Etat a placé le secteur financier en première ligne des douze secteurs d'importance vitale qui devront adopter les nouvelles règles en matière de cybersécurité, arrêtées par la loi de programmation militaire de 2013.
Ce choix n'est pas dû à une recrudescence des cyber-risque dans le secteur, assure la puissance publique – en l'occurrence, c'est Bercy qui a fait l'objet de l'attaque la plus grave ayant jamais visé une administration en France en 2011. *« Le niveau de sécurité du secteur financier est jugé satisfaisant,* indique Yves Jussot, coordinateur sectoriel à l'Agence nationale de la sécurité des systèmes d'information (Anssi). *Cependant la menace évolue vite et de façon continue, en particulier avec le développement du numérique. »*
Considérées comme *« pionnières »* dans l'identification des menaces informatiques et de lutte contre les cyberfraudes, les banques fixeront la barre des nouvelles exigences en matière de protection, qui s'appliqueront aux autres secteurs vitaux comme l'énergie, aux transports, en passant par la santé. Définies par un arrêté d'ici au 1er juillet, celles-ci promettent d'être élevées. Des règles renforcées en matière d'administration des systèmes sont par exemple définies pour cantonner davantage les flux de données.
Surtout, l'Etat voit son pouvoir renforcé en matière de contrôle. L'Anssi, rattachée au secrétaire général de la Défense et de la sécurité nationale, pourra mener des audits réguliers, et des amendes pourront être délivrées pour infraction à la sécurité informatique ou non-application de la réglementation. Les incidents qui pouvaient jusqu'à présent ne pas être déclarés devront être notifiés et, en cas d'attaque majeure, l'Anssi pourra prendre la main sur les systèmes. L'Etat a pris soin de travailler de concert avec les banques, au travers du Forum des compétences, qui regroupe les experts informatiques des banques et des assurances. Restera la question des moyens. *« La course à la transformation digitale entre banques impose d'aller vite et d'y allouer des moyens. La mise à niveau des systèmes informatiques peut ne pas suivre et ne pas être prioritaire »*, note un expert en cybersécurité…[Suite de l'article original de Anne RIF et Véronique CHOCRON]

Réagissez à cet article

Source : *La France adopte son arsenal anti-hackers, Banque – Assurances*

Augmentation de 30% des

demande de rançon informatique en 3 mois

	**Augmentation de 30% des demande de rançon informatique en 3 mois**

Le #ransomware a dépassé les attaques de type APT (menaces persistantes avancées) pour devenir le principal sujet d'actualité du trimestre. 2900 nouvelles variantes de malwares au cours de ces 92 jours.

Selon le rapport de Kaspersky Lab sur les malwares au premier trimestre, les experts de la société ont détecté 2900 nouvelles variantes de malwares au cours de cette période, soit une augmentation de 14 % par rapport au trimestre précédent. 15 000 variantes de ransomware sont ainsi dorénavant recensés.

Un nombre qui va sans cesse croissant.
Pourquoi ? Comme j'ai pu vous en parler, plusieurs kits dédiés aux ransomwares sont commercialisés dans le blackmarket. Autant dire qu'il devient malheureusement très simple de fabriquer son arme de maître chanteur 2.0.
Au premier trimestre 2016, les solutions de sécurité de l'éditeur d'antivirus ont empêché 372 602 attaques de ransomware contre leurs utilisateurs, dont 17 % ciblant les entreprises. Le nombre d'utilisateurs attaqués a augmenté de 30 % par rapport au 4ème trimestre 2015. Un chiffre à prendre avec des pincettes, les ransomwares restant très difficiles à détecter dans leurs premiéres apparitions.

Locky , l'un des ransomwares les plus médiatisés et répandus au 1er trimestre
Le ransomware Locky est apparu, par exemple, dans 114 pays. Celui-ci était toujours actif début mai. Un autre ransomware nommé Petya est intéressant du point de vue technique en raison de sa capacité, non seulement à crypter les données stockées sur un ordinateur, mais aussi à écraser le secteur d'amorce (MBR) du disque dur, ce qui empêche le démarrage du système d'exploitation sur les machines infectées.
Les trois familles de ransomware les plus détectées au 1er trimestre ont été Teslacrypt (58,4 %), CTB-Locker (23,5 %) et Cryptowall (3,4 %). Toutes les trois se propagent principalement par des spams comportant des pièces jointes malveillantes ou des liens vers des pages web infectées. « Une fois le ransomware infiltré dans le système de l'utilisateur, il est pratiquement impossible de s'en débarrasser sans perdre des données personnelles. » confirme Aleks Gostev, expert de sécurité en chef au sein de l'équipe GReAT (Global Research & Analysis Team) de KL.

Une autre raison explique la croissance des attaques de ransomware : les utilisateurs ne s'estiment pas en mesure de combattre cette menace. Les entreprises et les particuliers n'ont pas conscience des contre-mesures technologiques pouvant les aider à prévenir une infection et le verrouillage des fichiers ou des systèmes, et négligent les règles de sécurité informatique de base, une situation dont profitent les cybercriminels entre autres. Bref, trop d'entreprise se contente d'un ou deux logiciels de sécurité, se pensant sécurisées et non concernées. L'éducation du personnel devrait pourtant être la priorité des priorités… [Lire la suite]

Article de Damien BANCAL

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybersécurité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Ransomware: +30% d'attaques en 3 mois – Data Security BreachData Security Breach*

Un gros botnet détourne des requêtes de recherche

Un gros botnet détourne des requêtes de recherche

Depuis septembre 2014, un botnet a pu compter près d'un million de zombies pour faire gonfler des revenus publicitaires de cybercriminels.

Actif depuis mi-septembre 2014, un botnet est parvenu à prendre le contrôle de près d'un million d'ordinateurs dans le monde. L'agent infectieux est un malware intégré dans un fichier d'installation modifié de type MSI pour Windows.
Botnet-Redirector.Paco-carte-BitdefenderCes fichiers corrompus sont associés à des programmes tels que WinRAR, YouTube Downloader, Connectify, Start8 et KMSPico. Après installation sur la machine prise pour cible, le nuisible dénommé Redirector.Paco s'appuie sur un fichier PAC (Proxy auto-config) pour rediriger des requêtes de recherches sur Google, Bing ou Yahoo.
Au gré de quelques modifications dans la base de registre, le trafic sera redirigé vers des publicités contextuelles permettant de générer des revenus ici frauduleux grâce au programme AdSense pour les recherches de Google.
Les opérateurs du botnet détournent les recherches vers un autre moteur de recherche personnalisé spécifiquement conçu qui affiche ses propres résultats, et détournent par la même occasion des revenus publicitaires… [Lire la suite]
Article de Jérôme GARAY

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Un gros botnet détourne des requêtes de recherche*

Le GCHQ aide Apple à corriger une faille de sécurité sur MacOSX

Le GCHQ aide Apple à corriger une faille de sécurité sur MacOSX

Dans ses derniers correctifs pour MacOSX, Apple signale que plusieurs failles de corruption de mémoire ont été corrigées grâce à l'aide du CESG, l'équivalent britannique de l'Anssi rattaché au GCHQ.

Si les choses se passent plutôt mal entre le FBI et Apple, le constructeur semble entretenir des rapports bien plus cordiaux avec le GCHQ britannique. Celui-ci a en effet été crédité dans une note de patch pour avoir aisé à la correction de failles de sécurité au sein de MacOSX. Deux failles ont ainsi été corrigées à l'aide du CESG, l'une permettant une corruption de mémoire au niveau du kernel de Mac OSX et une autre au sein des technologies de gestion des ports Firewire. Celles-ci permettaient à un attaquant d'exécuter du code potentiellement malveillant sur la machine visée.

Ce n'est pas la première fois que le CESG est crédité pour avoir débusqué des failles au sein de logiciels et les avoir communiqué à l'éditeur. L'organisme est souvent présenté comme un équivalent britannique de l'Anssi, mais est de fait rattaché aux services du GCHQ, l'équivalent britannique de la NSA. Une position qui laisserait croire que celui-ci aurait plutôt tendance à garder les vulnérabilités découvertes par ses équipes pour ses activités d'espionnage informatique.

La collaboration entre les forces de l'ordre et les acteurs de l'IT est à géométrie variable. Si Apple semble travailler en bonne intelligence avec le CESG, ses rapports sont nettement moins apaisés avec le FBI. Aux États Unis, le FBI est d'ailleurs critiqué par les développeurs de Tor pour son refus de communiquer l'une des failles ayant été utilisées dans le démantèlement du réseau de pédopornographie Playpen. Le GCHQ tout comme le FBI ou la NSA ne donnent que peu d'information sur les raisons qui les poussent à dévoiler les failles qu'ils connaissent aux éditeurs des logiciels ou matériels affectés. Mais Apple ne crache pas dans la soupe et a profité du tuyau pour combler les deux failles signalées par le CESG… [Lire la suite]

Article de ZDNet

Réagissez à cet article

Source : *Le GCHQ aide Apple à corriger une faille de sécurité sur MacOSX – ZDNet*