Sécurité informatique des collectivités : Toujours plus avec moins…

	Sécurité informatique des collectivités : Toujours plus avec moins…

Les collectivités et leurs groupements, notamment les communautés de communes, peinent encore à prendre en compte tous les aspects de la sécurité des systèmes d'information, à en croire le rapport 2016 du Club de la sécurité de l'information Français (Clusif). Alors qu'elles se numérisent de plus en plus, les collectivités vont devoir maintenir voire accentuer leurs efforts dans un contexte budgétairement contraint.

Dans l'édition 2016 de son rapport sur les « Menaces informatiques et pratiques de sécurité en France » (Mips), le Club de la sécurité de l'information Français (Clusif) se penche de nouveau sur les collectivités (1). De plus en plus nombreuses à recourir à des services dématérialisés, celles-ci auront à charge de « maintenir » leurs « efforts » pour « assurer la sécurité de leur système d'information et des informations qui leur sont confiées », selon les auteurs de ce document de plus de cent pages. Le tout dans un contexte budgétaire restreint. Globalement, alors que le sentiment de dépendance à l'égard du numérique s'enracine, la sécurité des systèmes d'information est « efficiente dès lors que les moyens organisationnels, humains et financiers sont clairement attribués » et que la direction est fortement impliquée, indique le rapport. Cependant, sur la base des 203 collectivités interrogées, il est fait état de grandes disparités entre les échelons territoriaux, où les communautés de communes sont à la peine.

Stagnation des budgets malgré la numérisation en cours

Publié tous les deux ans, le « Mips » délivre un bilan approfondi des usages en matière de sécurité de l'information ; et inclut dans son édition 2016 (comme tous les 4 ans) les collectivités territoriales de grande taille. Autrement dit les communes de plus de 30.000 habitants, les intercommunalités (communautés de communes, d'agglomération, communautés urbaines ou encore les métropoles) et enfin les régions et les départements (regroupés par le rapport sous le terme de conseils territoriaux).

Côté résultats, si une grande partie des collectivités interrogées a confié un sentiment toujours croissant de « dépendance » vis-à-vis de l'informatique (75% contre 68% en 2012), les budgets qui y sont liés tendent pourtant à baisser et restent très disparates (avec un rapport de 1 à 100 entre les plus petits et les plus importants). Ainsi, près de 54% des collectivités ont un budget informatique inférieur à 100.000 euros en 2016, contre 45% en 2012. En moyenne, les conseils territoriaux sont les mieux dotés avec 5,8 millions d'euros, pour un million d'euros dans les intercommunalités et 800.000 euros dans les villes.

Dans ce total, la part de la sécurité est difficilement évaluable et demeure au mieux constante (67% des cas) ou diminue (28% des collectivités contre 14% en 2012 y consacrent moins de 1% de leur budget informatique). Enfin, si augmentations il y a, elles servent avant tout à mettre en place des solutions de sécurité (25%), même si des efforts importants sont effectués en matière organisationnelle (11%) et en sensibilisation (9%).

Pas de politique de sécurité sans personnels qualifiés

Bien que majeur, l'aspect financier n'occupe que la deuxième place des principaux freins pour les collectivités (à 45%), pour qui l'absence de personnels qualifiés semble être le véritable problème (à 47%), accru par un manque avoué de connaissance (38%). En conséquence, les contraintes organisationnelles (29%) et les réticences de la direction générale, des métiers ou des utilisateurs (24%) ferment la marche.

Malgré tout, l'étude montre que les collectivités sont de plus en plus nombreuses à formaliser leur politique de sécurité (PSI), en particulier les villes (54% contre 43% en 2012) et les conseils territoriaux (52% contre 35%). A l'inverse, les communautés de communes sont à la peine (un peu plus de 2 sur 10).

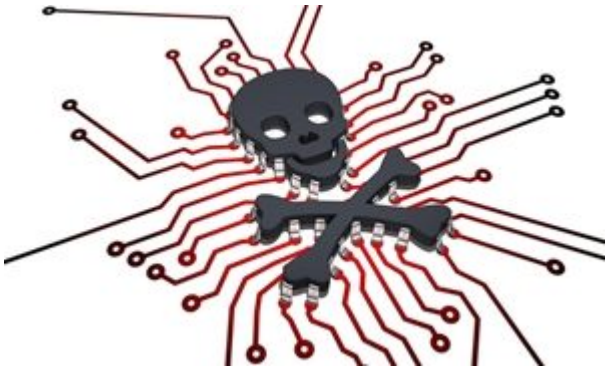
Concrètement, les DSI (directions des systèmes d'information) gèrent les politiques de sécurité dans 65% des cas, alors que les directions générales des services tendent à se désengager (impliquées dans 54% des cas, contre 80% en 2012). Dans 21% des cas, des élus y ont contribué. Enfin, on notera que la présence d'un responsable de la sécurité des systèmes d'information (RSSI) « serait une condition sine qua none pour disposer d'une PSI ». Par ailleurs de plus en plus nombreux (+3 points, à 35%), les RSSI voient cependant leur fonction se diluer, avec 39% de personnel dédié en 2016 contre 62% en 2012 dans les villes, pour ne citer qu'elles. Enfin, ils sont bien souvent rattachés à la DGS (dans les communautés de communes notamment) ou à la DSI (dans les régions ou les départements par exemple) – selon une règle qui veut que « plus la collectivité est petite et plus les fonctions sont cumulées par le comité de direction »…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Sécurité informatique : les collectivités encouragées à maintenir leurs efforts – Localtis.info – Caisse des Dépôts

---

Des serveurs Linux attaqués par le ransomware Fairware



Des serveurs Linux attaqués par le ransomware Fairware

Des exploitants de serveurs Linux signalent des attaques qui entraînent la disparition du dossier Internet du serveur et la non disponibilité des sites pendant une durée indéterminée.

Les participants aux forums de BleepingComputer se plaignent également de l'attaque : d'après la description fournie par une des victimes, cela ressemble plus à une attaque via force brute contre SSH. Notons qu'à chaque fois, le dossier Internet est supprimé et il ne reste que le fichier read_me qui contient un lien vers une page Pastebin où apparaît la demande de rançon.
Les individus malintentionnés promettent de rendre les fichiers contre 2 bitcoins et expliquent que le serveur de la victime a été infecté par le ransomware Fairware. Toutefois, à en croire Lawrence Abrams de chez Bleeping Computer, cette affirmation pourrait ne pas être tout à fait exacte.
« Si l'attaquant télécharge un programme ou un script pour réaliser « l'attaque », il s'agit alors bel et bien d'un [ransomware]. Malheureusement, nous ne disposons pas pour l'instant des informations suffisantes. Tous les rapports montrent que les serveurs ont été compromis, mais je n'ai pas encore eu l'occasion de le vérifier » a déclaré l'expert.
La demande de rançon contient l'adresse d'un portefeuille Bitcoin. La victime est invitée à réaliser le paiement dans les deux semaines, sans quoi les individus malintentionnés menacent d'écouler les fichiers sur le côté. Le message publié sur Pastebin possède le contenu suivant : « Nous sommes les seuls au monde qui pouvons vous rendre vos fichiers . Après l'attaque contre votre serveur, les fichiers ont été chiffrés et envoyés vers un serveur que nous contrôlons. »
Le message contient également une adresse email pour l'assistance technique, mais il est interdit à l'utilisateur d'y envoyer un message uniquement pour confirmer si les attaquants possèdent bien les fichiers perdus. Lawrence Abrams affirme que pour l'instant, il ne sait pas ce que les attaquants font avec les fichiers. Vu que les fichiers sont supprimés, il serait plus logique pour les conserver de les archiver et de les charger sur un serveur et non pas de les chiffrer et de gérer des clés individuelles.
En général, les ransomwares sont diffusés via l'exploitation de vulnérabilités ou par la victime elle-même qui est amenée, par la ruse, à exécuter le malware. Dans le cas qui nous occupe, rien ne trahit ce genre d'activité. Une des victimes indiquait sur le forum de Bleeping Computer que son serveur Linux avait été épargné en grande partie par l'attaque et que les fichiers de la base de données avaient été préservés. Ce commentaire indiquait également que les individus malintentionnés avaient laissé le fichier read_me dans le dossier racine.
La suppression de fichiers et le refus de confirmer leur vol sont des comportements inhabituels pour des individus malintentionnés qui travaillent avec des ransomwares. « Il est tout à fait possible qu'il s'agisse d'une escroquerie, mais dans ce cas c'est un mauvais business pour les attaquants » explique Lawrence Abrams. « Si l'escroc ne respecte pas sa promesse après le paiement de la rançon, il aura mauvaise réputation et plus personne ne le paiera. »
Toutefois, le message sur l'infection via le ransomware et la menace de publier les données volées sont en mesure de confondre la victime et de l'amener à répondre aux exigences des attaquants. Fairware n'est pas la première cybercampagne accompagnée d'une telle menace. L'année dernière, les exploitants du ransomware Chimera, avaient adopté une astuce similaire, même si leur malware n'était pas en mesure de voler les fichiers ou de les publier sur Internet.
Lawrence Abrams explique que les victimes de ransomwares devraient s'abstenir de payer la rançon, mais si elles décident d'agir ainsi, elles doivent au moins confirmer que le bénéficiaire du paiement possède bien les fichiers.
Article original de Securelist

Réagissez à cet article

Original de l’article mis en page : Fairware attaque des serveurs Linux – Securelist

---

Cybersécurité et Cyberdéfense : leviers de l’intelligence économique

La transition numérique en Afrique étroitement liée à l’intelligence économique

---

La numérisation de la société africaine s'accélère : la part du numérique dans les services, les produits, les métiers ne cesse de croître. Réussir la transition numérique est devenu un enjeu continental. Vecteur d'innovation et de croissance, la numérisation présente aussi des risques pour l'Etat, les acteurs économiques et les citoyens. La cybercriminalité, l'espionnage, la propagande, le sabotage ou l'exploitation excessive de données personnelles menacent la confiance et la sécurité dans le numérique et appellent une réponse collective.

Le second pilier de l'intelligence économique est par définition la sécurité du patrimoine immatériel. Composante indispensable au développement. Le problème est que ce patrimoine est de plus en plus numérisé en Afrique comme partout dans le monde. A cela il faut rajouter le fait que la technologie est injectée à forte dose dans les entreprises pour améliorer la croissance et la compétitivité. Il y va de même pour les Etats.
Dans ce contexte, l'utilisation, l'accès et l'exploitation de la technologie est en forte croissance. Ce qui a pour implication d'exposer les données stratégiques. Il faut alors disposer de mécanismes efficaces pour protéger ce patrimoine. « La cybersécurité est la prévention des risques de sécurité et de sûreté liés à l'emploi des technologies de l'information. Elle est à ce titre un volet de « l'intelligence des risques » elle-même composante de l'intelligence économique. » Bernard Besson.
De nouveaux crimes, risques, infractions et menaces sont apparus dans le cyberespace africain : utilisations criminelles d'internet (cybercriminalité), espionnage politique, économique et industrielle, attaques contre les infrastructures critiques de la finance, des transports, de l'énergie et des communications à des fins de spéculation, de sabotage et de terrorisme.
Émanant de groupes étatiques ou non-étatiques, les cyberattaques n'ont aucune contrainte de distances, de frontières et même d'espaces ; peuvent être complètement anonymes ; ne nécessitent plus de coûts et de moyens importants et peuvent présenter de très faibles risques pour l'attaquant…[lire la suite]

Denis Jacopini anime des **conférences et des formations** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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.

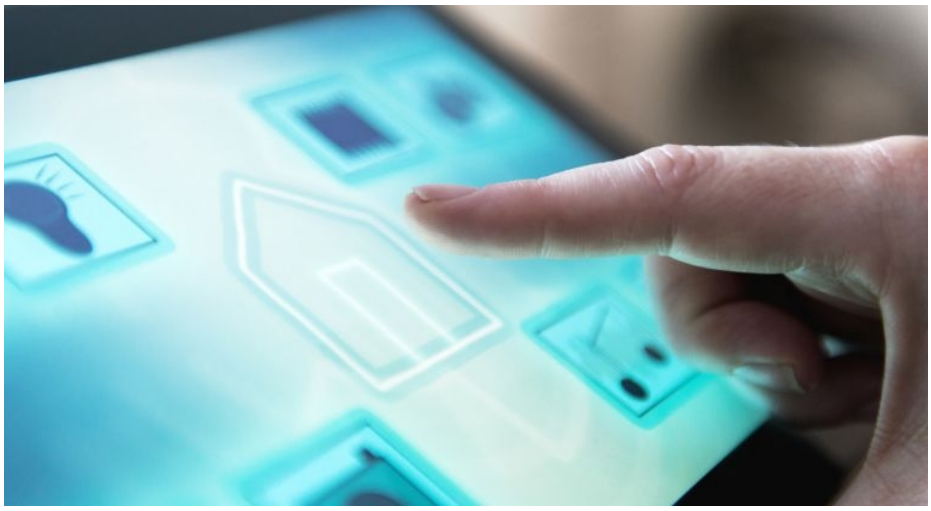
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cybersécurité et Cyberdéfense : leviers de l’intelligence économique. »

Jusqu’où les Objets connectés sont les maillons faibles de la cybersécurité ?



Jusqu’où les Objets connectés sont les maillons faibles de la cybersécurité ?

La Chine s'impose parmi les principaux pays créateurs d'objets quotidiens connectés à l'internet, mais elle génère ainsi de gigantesques failles sécuritaires exploitables par des pirates informatiques, a prévenu mardi John McAfee, créateur américain du logiciel antivirus portant son nom.

S'exprimant devant une conférence spécialisée à Pékin, M. McAfee a cité des précédents, dans lesquels des pirates sont parvenus à distance à prendre le contrôle de coffre-forts, de systèmes de chauffage, mais aussi d'ordinateurs de bord d'automobiles ou d'aéroplanes.

« La Chine prend la tête des progrès sur les objets intelligents, depuis les réfrigérateurs jusqu'aux thermostats, et c'est le maillon faible de la cybersécurité », a-t-il martelé, disant vouloir « lever un drapeau rouge » d'avertissement.
« Il y a tellement plus de ces objets, et plus vous en connectez ensemble, plus les risques de piratage augmentent », a encore souligné John McAfee.
L'excentrique septuagénaire avait fait fortune aux débuts d'internet dans les années 1990, après avoir mis au point un logiciel antivirus qui porte son nom et est maintenant la propriété d'Intel.
Plombé par la crise financière de 2008, il avait défrayé la chronique en 2012 après la mort de son voisin au Belize, pays où il vivait à l'époque et qu'il avait fui après l'ouverture d'une enquête de la police locale.
M. McAfee a livré à Pékin un discours au ton sombre et inquiétant, à l'heure où sa nouvelle société MGT Capital se prépare à lancer de nouveaux produits de cybersécurité d'ici la fin de l'année.
« Notre espèce n'a jamais été confrontée jusqu'ici à une menace de cette ampleur. Et pour l'essentiel, nous n'en prenons pas conscience », a-t-il averti.
« Vous pouvez penser que j'exagère, que je tombe dans l'alarmisme. Mais je compte parmi mes amis beaucoup de +hackers+ (pirates) qui ont les capacités de faire d'énormes dégâts si l'envie leur en prend », a-t-il ajouté.
A l'instar de Xiaomi, fabricant de smartphones ayant élargi son offre dans l'électroménager « intelligent », nombre d'entreprises chinoises intègrent désormais une connexion wi-fi à des produits variés, des autocuiseurs pour riz aux purificateurs d'air, permettant aux usagers de les allumer à distance depuis leur téléphone.
De telles connexions créent de graves failles qui accentuent les vulnérabilités de leurs réseaux, selon John McAfee.
Dans un entretien avec des journalistes à Pékin, l'Américain a cependant noté « n'avoir entendu parler d'aucune » attaque informatique de grande ampleur en Chine sur l'année passée, tandis que les Etats-Unis en enregistraient « des centaines ».

Original de l'article mis en page : Objets connectés : le créateur de l'antivirus McAfee met en garde la Chine contre les failles de sécurité | La Provence

---

Position du CERT-FR (Computer Emergency Response Team de

l’ANSSI) vis à vis de Pokemon Go

Position du CERT-ER (Computer Emergency Response Team de l’ANSSI) vis à vis de Pokemon Go

Cyber-risques liés à l'installation et l'usage de l'application Pokémon GoLancé courant juillet par la société Niantic, le jeu Pokémon Go est depuis devenu un phénomène de société, au point d'être installé sur plus de 75 millions de terminaux mobiles dans le monde. Certains acteurs malveillants ont rapidement tenté d'exploiter la popularité du jeu à des fins criminelles. Certaines précautions s'imposent donc avant de pouvoir tenter de capturer un Dracaufeu ou un Lippoutou sans porter atteinte à la sécurité de son ordiphone.

Cyber-risques liés à l'installation et l'usage de l'application Pokémon Go

Lancé courant juillet par la société Niantic, le jeu Pokémon Go est depuis devenu un phénomène de société, au point d'être installé sur plus de 75 millions de terminaux mobiles dans le monde. Certains acteurs malveillants ont rapidement tenté d'exploiter la popularité du jeu à des fins criminelles. Certaines précautions s'imposent donc avant de pouvoir tenter de capturer un Dracaufeu ou un Lippoutou sans porter atteinte à la sécurité de son ordiphone.

Applications malveillantes

Des sociétés spécialisées en sécurité informatique ont mis en évidence la présence de nombreuses fausses applications se faisant passer pour une version officielle du jeu. Ces applications sont susceptibles de naviguer sur des sites pornographiques pour simuler des clics sur des bannières publicitaires, de bloquer l'accès au terminal et de ne le libérer qu'en contrepartie d'une rançon, ou bien même d'installer d'autres codes malveillants. Au vu du nombre d'applications concernées (plus de 215 au 15 juillet 2016), cette technique semble très populaire, en particulier dans les pays où le jeu n'est pas encore disponible via les sites officiels.

Niveau de permissions demandées par l'application

La version initiale du jeu sur iOS présentait un problème au niveau de la gestion des permissions. En effet, le processus d'enregistrement d'un compte Pokemon Go à l'aide d'un compte Google exigeait un accès complet au profil Google de l'utilisateur.
Suite à la prise de conscience de ce problème, la société Niantic a rapidement réagi en précisant qu'il s'agissait d'une erreur lors du développement. Elle propose désormais une mise à jour pour limiter le niveau d'accès requis au profil Google de l'utilisateur. A noter que la version Android du jeu ne semble pas avoir été affectée par ce problème.
Dans le doute, il est toujours possible de révoquer cet accès en se rendant sur la page de gestion des applications autorisées à accéder à son compte Google.

Collecte de données personnelles

De par son fonctionnement, l'application collecte en permanence de nombreuses données personnelles qui sont ensuite transmises au développeur du jeu, par exemple les informations d'identité liées au compte Google ou la position du joueur obtenue par GPS. Certaines indications visuelles (nom de rue, panneaux, etc) présentes sur les photos prises avec l'application peuvent aussi fournir des indications sur la position actuelle du joueur. La désactivation du mode « réalité augmentée » lors de la phase de capture permet de se prémunir de ce type de risques (et accessoirement, de réduire l'utilisation de la batterie de l'ordiphone).

Pokemons et BYOD

Il peut être tentant d'utiliser un ordiphone professionnel pour augmenter les chances de capture d'un Ronflex. Même s'il est souvent délicat de répondre par la négative à une requête émanant d'un VIP, il semble peu opportun de déployer ce type d'application dans un environnement professionnel, en raison des différents risques évoqués précédemment.

Recommandations

Le CERT-FR recommande de n'installer que la version originale du jeu présente sur les boutiques d'Apple et de Google. En complément, il convient de désactiver la possibilité d'installer une application téléchargée depuis un site tiers (sous Android, paramètre « Sources inconnues » du menu « Sécurité »).
Il est également conseillé de vérifier les permissions demandées par l'application. La version originale du jeu nécessite uniquement :
• d'accéder à l'appareil photo pour les fonctionnalités de réalité augmentée ;
• de rechercher des comptes déjà présents sur l'appareil ;
• de localiser l'utilisateur grâce au GPS ou aux points d'accès Wi-Fi ;
• d'enregistrer localement des fichiers sur le téléphone.
Toute autre permission peut sembler suspecte et mettre en évidence la présence sur l'ordiphone d'une version altérée de l'application.
Le CERT-FR suggère de mettre en place un cloisonnement entre l'identité réelle du joueur et celle de dresseur Pokémon. Pour cela, il est possible d'ouvrir un compte directement auprès du Club des dresseurs Pokémon [8] ou bien de créer une adresse Gmail dédiée à cet usage.
Enfin, le CERT-FR déconseille de pratiquer cette activité dans des lieux où le geo-tagging du joueur pourrait avoir des conséquences (lieu de travail, sites sensibles, etc) [9]…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Bulletin d'actualité CERTFR-2016-ACT-031

Déchiffrement des

communication numériques (Telegram et autres). Où en est-on ?

Déchiffrement des communication numériques (Telegram et autres). Où en est-on ?

Ce mardi 23 Août, Bernard Cazeneuve se réunissait avec son homologue allemand pour discuter d'une initiative européenne contre le chiffrement des données, afin de lutter contre le terrorisme. Une initiative qui ne fait pas l'unanimité.

Une initiative européenne contre les chiffrements trop forts ?

Face au terrorisme international et sachant que les messageries instantanées visées par le projet de loi sont majoritairement américaines, Bernard Cazeneuve s'en remet à une initiative européenne. L'idée serait d'étendre aux services de messageries et d'appels sur internet, les mêmes règles de sécurité et de confidentialité destinées jusque-là, aux opérateurs télécom. Le ministre a ainsi fermement déclaré vouloir obliger les services en ligne «*non coopératifs*» à «*retirer des contenus illicites ou déchiffrer des messages dans le cadre d'enquêtes judiciaires, que leur siège soit en Europe ou non*».

Conscient de la polémique qui entoure ce projet de loi, le ministre a précisé que l'utilisation des données déchiffrées ne servirait que dans le cadre « *judiciaire* ». Ce qui voudrait dire qu'elles ne seraient pas utilisées par les services secrets, comme le redoutent beaucoup de personnes. Se voulant rassurant, il a insisté « *Il n'a bien sûr, jamais été question de remettre en cause le principe du chiffrement des échanges* ». Le 16 septembre prochain, le projet de loi contre le chiffrement des données sera discuté lors du sommet des chefs d'états européens.

…[lire la suite]

Original de l'article mis en page : Une initiative franco-allemande contre le chiffrement numérique

Le logiciel de téléchargement Transmission à nouveau piraté

Le logiciel de téléchargement Transmission à nouveau piraté

Le Net Expert vous avait déjà informé en juillet dernier de cet type d'attaque dont avait été victime la sphère Apple. Apparemment la leçon n'a pas servi. Même méthode, même punition.

Pour la deuxième fois en moins de six mois, la version Mac du logiciel Transmission a été corrompue, a révélé mardi 30 août l'entreprise de sécurité informatique Eset. Ce client BitTorrent gratuit, qui permet de télécharger des fichiers (vidéo, sons…) est l'un des plus utilisés.
Cette fois l'éditeur propose une procédure à suivre si vous avez été piégé en téléchargeant la version 2.92 du logiciel entre le 28 et le 29 août. Si vous avez un doute, n'hésitez pas à suivre cette procédure.
Comme l'explique l'équipe de Transmission sur son site, des pirates se sont introduits dans ses serveurs et ont remplacé le logiciel par une version modifiée contenant un *malware* baptisé « OSX/Keydnap ». Ce logiciel malveillant permet, selon Eset, de dérober des mots de passe et d'installer une porte dérobée sur les ordinateurs touchés, permettant d'y avoir accès en permanence.

Un précédent avec un logiciel de racket

Tous les utilisateurs de Transmission ne sont pas concernés : seules les personnes ayant téléchargé la version 2.92 du logiciel entre le 28 et le 29 août risquent d'avoir par la même occasion installé le malware sur leur ordinateur. Ni Eset, ni Transmission n'ont précisé combien de personnes cela représentait. L'équipe du logiciel souligne toutefois que les mises à jour automatiques ne comprenaient pas ce malware.
Transmission dit avoir « *immédiatement* » supprimé la version piratée de son serveur après avoir découvert son existence, « *soit moins de vingt-quatre heures après que le fichier a été mis en ligne* ». Son site a publiéune marche à suivre pour les personnes ayant téléchargé le logiciel corrompu.
En mars, Transmission avait été victime du même type de piratage : le logiciel avait été remplacé sur le site par un *ransomware*, un logiciel de racket qui verrouille l'accès aux fichiers de sa victime et exige de l'argent en échange du déblocage de l'ordinateur.
Source : Le Monde

Réagissez à cet article

Original de l’article mis en page : Le logiciel de téléchargement Transmission à nouveau piraté

Alerte : Un canular sur Facebook qui diffuse de fausses informations terroristes

Alerte : Un canular sur Facebook qui diffuse de fausses informations terroristes

---

Les chercheurs ESET ont découvert une arnaque qui cible les utilisateurs de Facebook. D'abord répandu en République Tchèque et en Slovaquie, elle pourrait se propager dans d'autres pays

Les utilisateurs de Facebook en République Tchèque et en Slovaquie font face à une vague de fausses informations sur une attaque meurtrière à Prague. Quand l'utilisateur clique sur le canular, il est redirigé vers une page Internet de phishing qui essaye de le tromper en l'incitant à partager ses identifiants Facebook.

« D'après ce que nous savons à propos de cette campagne, l'attaque pourrait se propager dans plusieurs autres pays » met en garde Lukáš Štefanko, Malware Researcher chez ESET.

Cette prétendue attaque terroriste est facile à discréditer car la photo publiée ne ressemble pas à Prague, ni à aucune autre ville d'Europe. Malgré cela, l'arnaque se diffuse rapidement. « Les utilisateurs de Facebook partagent fréquemment des histoires sans les avoir lues. Les campagnes d'arnaques, si elles font appel à l'émotion, réussissent étonnamment bien à cause de notre empathie naturelle » commente Lukáš Štefanko.

Peu après le lancement de la campagne, Facebook a commencé à stopper les pages de phishing utilisées dans cette campagne. Les solutions de sécurité ESET sont conçues pour bloquer les pages Internet de phishing liées à ce type d'escroquerie ainsi que d'autres domaines enregistrés par cette même personne.

« Au cours des dernières semaines, il y a eu 84 domaines enregistrés par la même personne. La plupart d'entre eux possède une fonction de phishing, tandis que d'autres pourraient être utilisées à l'avenir lors d'une attaque à plus grande échelle » ajoute Lukáš Štefanko.

Voici les recommandations des experts ESET pour ceux qui pensent avoir été escroqué en partageant leurs identifiants Facebook :

– Changez votre mot de passe Facebook et utilisez les deux facteurs d'authentification fournis par Facebook

– Si vous avez utilisé le même mot de passe pour plusieurs services, changez-le partout – et mettez un terme à cette pratique très dangereuse.

Denis JACOPINI vous recommande les outils de protection suivants :

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

Original de l’article mis en page : Boîte de réception – denis.jacopini@gmail.com – Gmail

L’un des outils préférés des cybercriminels mis à mal par un coup de filet ?

L’un des outils préférés des cybercriminels mis à mal par un coup de filet ?

Karspersky publie aujourd'hui sur son blog un compte rendu d'une enquête des autorités russes à laquelle ils ont collaboré. Celle-ci a permis l'arrestation en juin d'un groupe de 50 cybercriminels, baptisés Lurk, qui opéraient notamment l'Angler exploit kit.

L'Angler Exploit Kit connaissait ces dernières années une popularité redoublée. Ce couteau suisse du cybercriminel était une plateforme utilisée pour infecter les machines de victimes : en l'installant sur un serveur et en amenant la cible à se connecter à ce serveur via un navigateur par exemple, le cybercriminel pouvait avoir recours à tout un éventail d'exploits fournis par les créateurs du kit pour tenter d'infecter la machine de la victime.

Simple à utiliser, évolutif et souvent à jour avec les derniers exploits et dernières vulnérabilités découvertes, l'Angler Exploit Kit dominait naturellement le marché. Mais en juin 2016, l'utilisation de cet outil par les cybercriminels a soudainement chuté sans véritable explication.

De nombreux observateurs avaient néanmoins fait le lien entre l'arrestation d'un groupe de 50 cybercriminels par les autorités russes et la soudaine disparition de l'Angler Kit. Dans une longue note de blog, Ruslan Stoyanov, dirigeant de l'unité investigation chez Kaspersky confirme cette théorie et détaille les 5 années passées sur la piste de ce groupe de cybercriminels de haute volée qui avaient été baptisés « Lurk ».

Le nom du groupe Lurk vient du premier malware repéré par Kaspersky en 2011. Celui-ci se présentait sous la forme d'un malware bancaire sophistiqué, qui visait principalement les logiciels bancaires afin de procéder à des virements frauduleux en direction des cybercriminels. Swift a connu plusieurs versions et évolutions, allant parfois jusqu'à fonctionner entièrement in memory pour éviter la détection.

Le malware Lurk se présentait comme un logiciel modulaire, pouvant embarquer plusieurs modules capables de réaliser des actions différentes, mais toujours orientées vers le vol de données bancaires et l'émission de virements frauduleux depuis les machines infectées.

Une petite PME sans histoire

« Avec le temps, nous avons réalisé que nous étions face à un groupe d'au moins 15 personnes. (…) Cette équipe était en mesure de mettre en place le cycle complet de développement d'un malware : à la fois sa conception, mais aussi la diffusion et la monétisation, à l'instar d'une petite entreprise de développement logiciel » explique Ruslan Stoyanov. Et le groupe Lurk avait également un autre atout de taille dans sa poche : exploitant leur renommée parmi les cybercriminels russophones, ils avaient commencé à louer les services de leur plateforme d'exploit, baptisée Angler Kit.

Cet exploit kit était à l'origine utilisé pour diffuser le malware bancaire Lurk, mais face aux mesures de sécurisation mises en place par de nombreuses banques, les revenus déclinants du groupe les ont forcés à diversifier leur activité. Les premières détections d'Angler Kit remontent à 2013, mais ce kit vendu en Saas par les cybercriminels du groupe Lurk a rapidement gagné en popularité.

Les créateurs du Blackhole kit ont été arrêtés en 2013, ce qui a laissé au nouveau programme du groupe Lurk un boulevard pour devenir le nouvel exploit kit préféré des cybercriminels. Dès le mois de mai 2015, celui-ci dominait largement le marché. Angler Kit pouvait être loué par d'autre groupe de cybercriminels qui s'en servaient pour diffuser différents types de malwares allant du ransomware au traditionnel trojan bancaire.

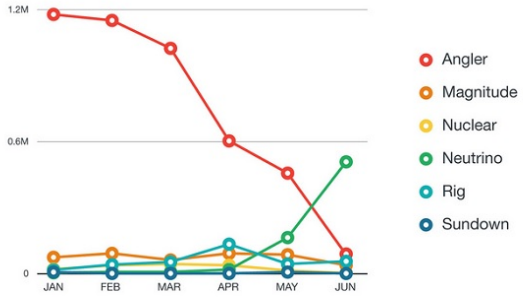


Figure 3: Number of times exploit-kit-hosting URLs were accessed in the first half of 2016

Mais le 7 juin, les autorités russes sont parvenues à arrêter les cybercriminels cachés derrière ce système. Kaspersky explique avoir collaboré avec les autorités afin de mener cette investigation, notamment via de l'échange d'informations compilées par la société sur le groupe. Un processus qui semble avoir été long et difficile, mais qui aura finalement porté ses fruits : l'Angler Kit est hors service et peut maintenant laisser la place… au nouvel exploit kit à la mode.

Selon les données récentes compilées par la société Trend Micro, l'exploit kit Neutrino aurait maintenant le vent en poupe et profiterait le plus de la retraite anticipée de son concurrent. Un de coffré, dix de retrouvés ?

Article original de Louis Adam

Réagissez à cet article

Original de l’article mis en page : L’un des outils préférés des cybercriminels mis à mal par un coup de filet ? – ZDNet

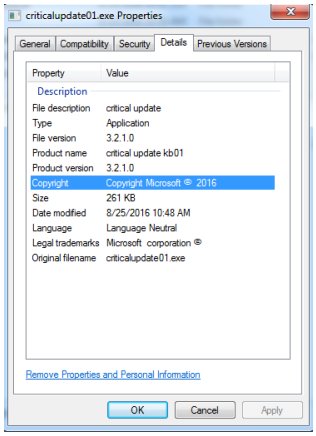
---

Alerte : Fantom, un nouveau ransomware qui sévit sous Windows 10

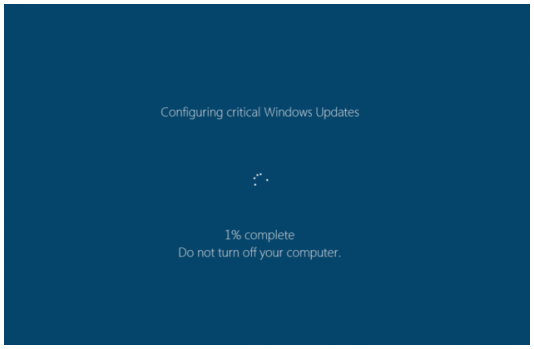
Alerte : Fantom, un nouveau ransomware qui sévit sous Windows 10

Windows 10 lance automatiquement ses mises à jour, ainsi que tous les utilisateurs que ça importunent le savent. Une bonne opportunité pour les cybercriminels de sévir tranquillement.

C'est ainsi qu'un nouveau ransomware a été découvert par un analyste de chez AVG Technologies.
Un premier exécutable maquille ses propriétés afin de faire croire qu'il provient de Microsoft et qu'il s'agit d'une mise à jour critique.



Une fois ce malware installé, il en télécharge un autre dans le répertoire AppDataLocalTemp, sous le nom WindowsUpdate.exe. Puis il l'exécute.
Pour l'utilisateur, c'est une mise à jour qui s'est déclenchée, tant l'écran de cette seconde partie du malware est bien faite, avec les polices de Microsoft bien imitées.



L'utilisateur n'est pas surpris de voir que son disque dur tourne, tourne… Une 'expérience utilisateur' qu'il doit régulièrement supporter…
Sauf que là, le disque tourne parce que le malware en crypte toutes les données. Le méfait accomplit, un autre écran apparaît, moins habituel, avec une invitation à contacter les cybercriminels par mail, pour finalement devoir payer une rançon afin de récupérer les données.
Utilisateurs de Windows 10, la prochaine fois que vous verrez un écran de mise à jour, croisez les doigts !

Article original de fredericmazue

Denis JACOPINI vous recommande le logiciel de sécurité suivant :

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

Original de l’article mis en page : Fantom : un nouveau ransomware qui sévit sous Windows 10 | Programmez!