Le Bénin, capitale de la cyber-arnaque en Afrique de l’Ouest

	Le Bénin, capitale de la cyber-arnaque en Afrique de l’Ouest

Au Bénin, les cybercriminels sont habituellement connus sous le nom de « Gaymans. » Les premières méthodes d'escroquerie concernaient les réseaux de jeunes se faisant passer pour des homosexuels, pour appâter des personnes de la même orientation sexuelle dans les pays occidentaux, d'où le nom de « Gayman » donné à la plupart des cybercriminels opérant à partir du Bénin.

Le phénomène fait son apparition dans les années 2000 et se caractérise essentiellement par des arnaques en ligne par des individus sans connaissance particulière en informatique, mais avec de solides atouts en psychologie.

Pour Nicaise Dangnibo, le directeur de l''Office central de répression de la cybercriminalité (OCRC), une unité spéciale de la police béninoise, « le phénomène a pris ses racines à partir du Nigeria, l'un des tout premiers pays d'Afrique de l'Ouest confrontés au phénomène de la cybercriminalité. »

Avec les premières mesures de rétorsion mises en place par les autorités nigérianes, les cybercriminels se sont massivement délocalisés au Bénin et en Côte d'Ivoire.

Ces derniers copiaient sur Internet des photos de jeunes hommes « beaux et musclés » à la recherche de l'âme soeur.

Les méthodes d'escroquerie se sont ensuite diversifiées, pour s'étendre au love chat, au porno-chantage, puis à des montages complexes de fausses affaires.

"Internet a certes révolutionné le monde au point qu'il serait difficile d'imaginer un autre monde sans internet ; mais, autant les coupeurs de routes existent et pourtant nous circulons sur nos routes, autant les flibustiers existent et pourtant nous naviguons sur les eaux ; autant les cybercriminels existeront toujours et nous allons toujours surfer sur le net."

Pierre Dovonou Lokossou

Gestionnaire de projets technologiques

Selon Pierre Dovonou Lokossou, gestionnaire de projets technologiques, « la première arnaque via l'Internet au Bénin a eu lieu deux ans après l'arrivée du web dans le pays. Il s'agissait d'un Nigérian se prénommant Christopher qui avait escroqué un pasteur américain (Jim), en se faisant livrer 40 ordinateurs, 10 imprimantes et un millier de bibles, en échange d'un chèque délivré par une banque fictive ».

Pierre Dovonou Lokossou raconte qu'à cette époque, « la plupart des mails indésirables (spams) provenant du Bénin étaient en anglais. La répression des actes de cybercriminalité au Nigéria avait vite fait de déverser au Bénin et dans la sous-région de jeunes Nigérians qui pouvaient désormais poursuivre en toute impunité leurs sales besognes… »

« Par la suite, ajoute-t-il, de l'anglais, les spams ont commencé à être rédigés dans un français approximatif, signe qu'avec le séjour de ces cybercriminels anglophones au Bénin, l'apprentissage de la langue française a été mis à contribution. »

Mais actuellement, à en croire le gestionnaire de projets, « le phénomène a pris de l'ampleur dans toute la sous-région ouest-africaine ». « Aussi bien des Béninois que des Togolais et des Burkinabè, des Nigériens et des Ivoiriens s'adonnent à cœur joie à ce cyber-banditisme », précise-t-il.

Offres de vente

Il s'agit le plus souvent de propositions de prêts, voire de dons ou d'offres de vente assez diversifiées diffusées sur des sites internet, ou parfois envoyées sous forme de spams aux internautes.

Les offres de vente vont des appareils électroménagers aux métaux précieux en passant par les téléphones portables, les ordinateurs, les véhicules, voire les animaux ou les domaines fonciers.

Une étudiante en Relations internationales, Adidjath Kitoyi, raconte avoir été contactée en 2012 sur le réseau social Facebook par « une Suissesse âgée de 83 ans atteinte d'un cancer au stade très avancé » qui souhaitait lui céder « une fortune héritée de ses parents et qui se trouve dans les coffres d'une banque à Genève ».

Appâtée, Adidjath s'était empressée d'envoyer à une adresse indiquée (qui se révèlera inexistante) tous les documents administratifs réclamés par son interlocuteur avant d'effectuer à l'attention d'un « intermédiaire » basé en Côte d'Ivoire un transfert de 150 000 FCFA représentant « les frais de dossiers ».

Par la suite, il ne lui était plus possible de communiquer avec la Suissesse donatrice, ni avec l'intermédiaire en Côte d'Ivoire.

La mésaventure d'Adidjath Kitoyi n'est qu'un cas parmi des centaines, voire des milliers d'autres victimes des cybercriminels.

Pierre Dovonou Lokossou distingue trois catégories de cybercriminels.

« La première est celle de ces jeunes qui n'ont pas un emploi légal connu et qui ne fréquentent que les cybercentres ou qui sont toujours avec leur ordinateur portatif et qui ont un train de vie largement au-dessus de la moyenne. Ils changent souvent de motos ou de voitures. Ils peuvent disparaître du quartier pendant des mois et réapparaître pour faire croire aux gens qu'ils étaient en France ou à Abidjan, alors qu'ils étaient en prison ou en cavale; la deuxième catégorie est celle des jeunes qui vont, soit au collège, soit à l'université, ou qui ont un emploi, mais s'adonnent à la cybercriminalité et à divers autres actes d'escroquerie; la troisième catégorie comporte les jeunes qui sont embauchés souvent par les cyber-bandits de la première ou deuxième catégorie et qui jouent le rôle d'assistants. Ce sont eux qui vont récupérer l'argent à la banque, qui jouent le rôle de secrétaire, d'avocat, de notaire pour confirmer au téléphone que le patron ou "son client" est quelqu'un de "bonne foi"…

Dispositif législatif

De 1997 à ce jour, ce qui n'était alors qu'un cas isolé à l'époque s'est mué en un cas d'école. De 2005 à 2010 notamment, le nombre de jeunes quittant les bancs au profit des cybercafés a considérablement augmenté.

Aujourd'hui encore, le phénomène est palpable et les nombreuses descentes de la police ne découragent pas les malfaiteurs.

A la sous-direction des crimes économiques et financiers de la police béninoise (ex-Brigade économique et financière-BEF), la cellule de lutte contre la cybercriminalité a déjà eu à effectuer plusieurs arrestations.

De source proche de ce service de police, quelques-uns des auteurs de ces forfaits via le web croupissent en prison.

La loi portant lutte contre la corruption, adoptée en 2011, qui y consacre tout son chapitre XV (« Des infractions cybernétiques, informatiques et de leur répression »), condamne fermement la cybercriminalité.

L'article 124 dispose notamment : « Quiconque a procédé à la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, est puni d'un emprisonnement d'un an à cinq ans et d'une amende de deux millions de francs CFA à vingt millions. »

Mais du dispositif législatif à la réalité sur le terrain, semble exister un grand fossé.

La note d'alerte de l'ambassade de France au Bénin citée plus haut est sans ambages :

Toutefois, des réflexions existent sur le plan local en faveur de la lutte contre la cybercriminalité.

En 2010, le professeur agrégé de droit, Joseph Djogbénou, concluait ainsi une étude intitulée « la cybercriminalité : enjeux et défis pour le Bénin » :

« Le cybermonde appelle la cybercriminalité. A la lumière de l'ensemble de ces considérations, la réponse nationale devra répondre à une double exigence de cohérence. En premier lieu, elle doit, et il ne saurait en être autrement, tenir compte de la convention de Budapest avec laquelle elle doit nécessairement être compatible. En second lieu, elle doit forcément s'inscrire dans un environnement régional propice. La situation est donc mûre (à notre sens) pour un instrument régional en la matière. Toutefois, il faut sur ce sujet un changement d'approche. En effet, l'examen des travaux réalisés jusqu'ici montre que la cybercriminalité n'est pas traitée de façon spécifique, mais comme un aspect particulier de la criminalité organisée. Ici encore c'est aux experts béninois et africains de mettre en exergue la nécessité et l'exigence d'une approche spécifique de la question. C'est à ce prix que l'Afrique parviendra à s'arrimer à la révolution post-industrielle en cours. »

Pour sa part, le gestionnaire de projets technologiques, Pierre Dovonou Lokossou appelle à éviter le piège de la résignation : « Internet a certes révolutionné le monde au point qu'il serait difficile d'imaginer un autre monde sans internet ; mais, autant les coupeurs de routes existent et pourtant nous circulons sur nos routes, autant les flibustiers existent et pourtant nous naviguons sur les eaux ; autant les cybercriminels existeront toujours et nous allons toujours surfer sur le net. »

Le plus urgent, selon lui, « c'est que nos autorités prennent le taureau par les cornes pour freiner de façon drastique ce fléau qui n'honore pas le Bénin et la sous-région ouest-africaine. »

Article original de Virgile Ahissou

Réagissez à cet article

Original de l’article mis en page : Le Bénin, capitale de la cyber-arnaque en Afrique de l’Ouest – SciDev.Net Afrique Sub-Saharienne

---

Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

Locky, TeslaCrypt, Cryptolocker, Cryptowall… Depuis plusieurs mois, les rançongiciels (« ransomware »), ces virus informatiques qui rendent illisibles les données d'un utilisateur puis lui réclament une somme d'argent afin de les déverrouiller, sont une préoccupation croissante des autorités. Le commissaire François-Xavier Masson, chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, une unité de la police spécialisée dans la criminalité informatique, explique au Monde les dangers de cette menace.

Combien y a-t-il d'attaques par rançongiciel en France ?
On ne le sait pas avec précision, nous n'avons pas fait d'étude précise à ce sujet. Statistiquement, le rançongiciel ne correspond pas à une infraction pénale précise et il recoupe parfois l'intrusion dans un système automatisé de traitement de données. Il faudrait affiner le cadre car nous avons besoin de connaître l'état de la menace.
Avez-vous quand même une idée de l'évolution du phénomène ?
L'extorsion numérique est clairement à la hausse, c'est la grande tendance en termes de cybercriminalité depuis 2013. Tout le monde est ciblé : les particuliers, les entreprises, même l'Etat. Les attaques gagnent en sophistication et en intensité. Il y a aussi une industrialisation et une professionnalisation. La criminalité informatique est une criminalité de masse : d'un simple clic on peut atteindre des millions de machines. Désormais, il n'y a plus besoin de vous mettre un couteau sous la gorge ou de kidnapper vos enfants, on s'en prend à vos données.
Les victimes ont-elles le réflexe de porter plainte ?
Certaines victimes paient sans porter plainte. Ce calcul est fait par les entreprises qui estiment que c'est plus pratique de payer la rançon – dont le montant n'est pas toujours très élevé, de l'ordre de quelques bitcoins ou dizaines de bitcoins – et qu'en portant plainte, elles terniront leur image et ne récupéreront pas nécessairement leurs données. Elles pensent aussi que payer la rançon coûtera moins cher que de payer une entreprise pour nettoyer leurs réseaux informatiques et installer des protections plus solides. C'est une vision de court terme. Nous recommandons de ne pas payer la rançon afin de ne pas alimenter le système. Si l'on arrête de payer les rançons, les criminels y réfléchiront à deux fois. C'est la même doctrine qu'en matière de criminalité organisée.
Qu'est-ce qui pousse à porter plainte ?
Chaque cas est unique mais généralement, c'est parce que c'est la politique de l'entreprise ou parce que le montant de la rançon est trop élevé.
Qui sont les victimes ?
Il s'agit beaucoup de petites et moyennes entreprises, par exemple des cabinets de notaires, d'avocats, d'architectes, qui ont des failles dans leur système informatique, qui n'ont pas fait les investissements nécessaires ou ne connaissent pas forcément le sujet. Les cybercriminels vont toujours profiter des systèmes informatiques vulnérables.
Quel est votre rôle dans la lutte contre les rançongiciels ?
La première mission, c'est bien sûr l'enquête. Mais nous avons aussi un rôle de prévention : on dit que la sécurité a un coût mais celui-ci est toujours inférieur à celui d'une réparation après un piratage. Enfin, de plus en plus, nous offrons des solutions de remédiation : nous proposons des synergies avec des entreprises privées, des éditeurs antivirus. On développe des partenariats avec ceux qui sont capables de développer des solutions. Si on peut désinfecter les machines nous-mêmes, on le propose, mais une fois que c'est chiffré, cela devient très compliqué : je n'ai pas d'exemple de rançongiciel qu'on ait réussi à déverrouiller.
Quel rapport entretenez-vous avec les entreprises ?
On ne peut pas faire l'économie de partenariats avec le secteur privé. Nous pourrions développer nos propres logiciels mais ce serait trop long et coûteux. Il y a des entreprises qui ont des compétences et la volonté d'aider les services de police.
Parvenez-vous, dans vos enquêtes, à identifier les responsables ?
On se heurte très rapidement à la difficulté de remonter vers l'origine de l'attaque. Les rançongiciels sont développés par des gens dont c'est le métier, et leur activité dépasse les frontières. On a des idées pour les attaques les plus abouties, ça vient plutôt des pays de l'Est. Mais pas tous.
Parvenez-vous à collaborer avec vos homologues à l'étranger ?
Oui, c'est tout l'intérêt d'être un office central, nous sommes le point de contact avec nos confrères internationaux. Il y a beaucoup de réunions thématiques, sous l'égide de l'Office européen de police (Europol), des pays qui mettent en commun leurs éléments et décrivent l'état d'avancement de leurs enquêtes. C'est indispensable de mettre en commun, de combiner, d'échanger des informations. Il peut y avoir des équipes d'enquête communes, même si ça ne nous est pas encore arrivé sur le rançongiciel.
De plus en plus d'enquêteurs se penchent sur le bitcoin – dont l'historique des transactions est public – comme outil d'enquête. Est-ce aussi le cas chez vous ?
C'est une chose sur laquelle on travaille et qui nous intéresse beaucoup. S'il y a paiement en bitcoin, il peut y avoir la possibilité de remonter jusqu'aux auteurs. C'est aussi pour cela que l'on demande aux gens de porter plainte même lorsqu'ils ont payé.
Article original de Martin Untersinger

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 : Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

Deux hommes ont volé 1,7 million d’euros en piratant des distributeurs de billet

Deux hommes ont volé 1,7 million d’euros en piratant des distributeurs de billet

---

Sans utiliser la moindre carte de crédit, deux hommes ont volé 1,7 millions d'euros à la First Commercial Bank de Taïwan.

Les « casses du siècles » deviennent de plus en plus cocasses et subtiles à l'ère du tout numérique. Chaque mois ou presque, on peut trouver un exemple de vol de banque, qui mêle développement logiciel et matériel. Cette fois le crime n'implique pas le vol ou la copie de cartes de crédit : à Taïwan, deux pirates ont réussi à retirer l'argent de 30 distributeurs sans se faire prendre. La somme volée s'élève à 70 millions de dollars taïwanais.
Leur méthode était particulièrement rodée. En moins de 10 minutes, les voleurs ont exécuté un programme dans le système du distributeur de billet qui, bien gentiment, a offert ses devises sans demander de compte. Le logiciel a ensuite pris soin d'effacer toute trace du larcin. Et les voleurs sont repartis, à 30 reprises, avec le gros lot. Les enquêteurs ne savent toujours pas comment les pirates ont fait pour déployer leur code aussi rapidement sur les distributeurs, ni quel moyen a été utilisé pour se connecter aux machines – un smartphone est évoqué.

LES VOLEURS SONT REPARTIS, À 30 REPRISES, AVEC LE GROS LOT
Les deux hommes seraient des étrangers : l'un d'eux a été identifié comme étant un citoyen russe qui s'est enfui de l'île dimanche et est recherché par Interpol. L'identité et la nationalité de l'autre homme ne sont pas connues. En attendant les experts de la compagnie allemande qui fournit les distributeurs à la banque taïwanaise qui a été prise pour cible, la décision de bloquer tous les distributeurs du même fournisseur a été prise par les autorités. 400 distributeurs de billet ont donc été rendus inactifs.
Article original de Julien Cadot

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

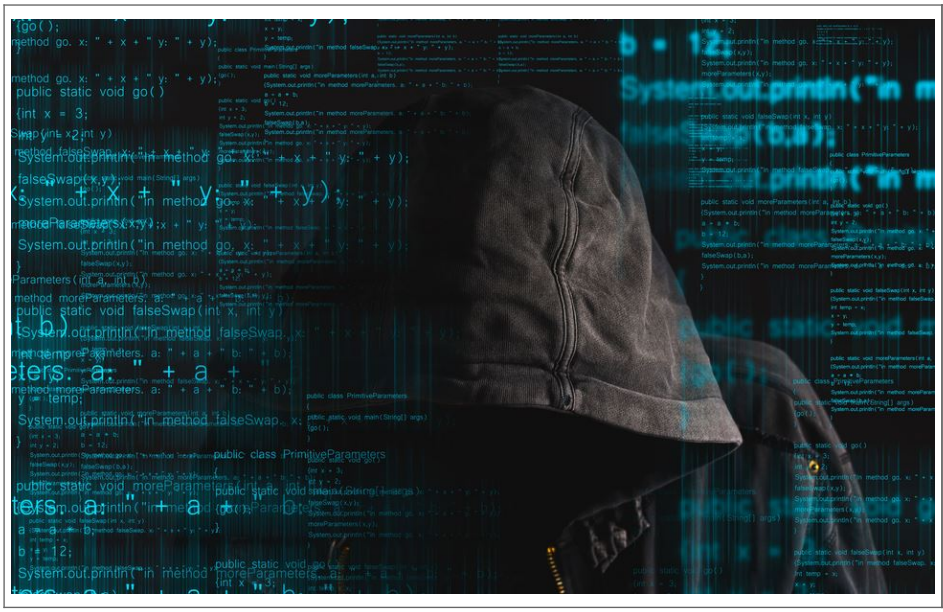
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Deux hommes ont volé 1,7 million d’euros en piratant des distributeurs de billet – Tech – Numerama

---

Un cousin du malware Furtim cible les énergéticiens européens



Un cousin du malware Furtim cible les énergéticiens européens

---

SentinelOne a découvert une variante du malware Furtim qui vise les sociétés européennes dans le domaine de l'énergie.

En mai dernier, des chercheurs la société EnSilo ont découvert un malware baptisé Furtim qui devait son nom à une obsession virant à la paranoïa de ne pas être détecté par les outils de sécurité. De la préparation à son installation jusqu'à son implémentation, le malware scrute, analyse et bloque tout ce qui touche de près ou de loin à la sécurité IT.

Il semble que ce malware revienne sous une autre forme pour s'attaquer au système industriel des entreprises énergétiques européennes. Des chercheurs de SentinelOne l'ont détecté au sein du réseau d'un énergéticien européen. Cette menace a un nom, SFG, et a été trouvée à la fois par une remontée d'information des logiciels de SentinelOne, mais aussi sur des forums privés. Les experts ont travaillé sur les échantillons pour comprendre son fonctionnement. Les résultats de cette analyse montrent que le comportement, la sophistication et la furtivité du malware sont l'œuvre d'un Etat ou pour le moins d'une organisation soutenue par un gouvernement. Les experts penchent pour une initiative provenant de l'Europe de l'Est.

Jusqu'au sabotage du réseau énergétique

Dans le détail, le cousin de Furtim s'appuie sur les mêmes exploits pour éviter d'être repéré par les outils de sécurité (antivirus, firewall next gen, solution endpoint, sandboxing). Plusieurs développeurs de haut niveau ont mis la main à la pâte pour perfectionner SFG. L'objectif est multiple, extraire des données ou faire tomber le réseau d'énergie, sans laisser de traces. Le malware affecte toutes les versions de Windows, précise SentinelOne dans un blog. Il situe ses débuts au mois de mai dernier et il est encore actif.

Ce n'est pas la première fois que les entreprises énergétiques sont visées par des malwares ayant pour ambition le sabotage du réseau. On pense bien évidemment au premier virus qui visait les SCADA, Stuxnet. Mais plus récemment, l'Ukraine a été victime d'une panne de courant provoquée par une cyberattaque s'appuyant sur le malware Blackenergy. Ce type de menaces est pris très au sérieux par les gouvernements au point de forcer les entreprises à remonter leurs niveaux de sécurité. En France, l'ANSSI peaufine les arrêtés sectoriels sur la sécurité des OIV (opérateurs d'importance vitale) notamment dans le domaine de l'énergie.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l'article mis en page : Malware : un cousin de Furtim cible les énergéticiens européens

Un concessionnaire Lamborghini de Mulhouse piraté

Un concessionnaire Lamborghini de Mulhouse piraté

Le vol de données peut souvent cacher des arnaques et attaques informatiques plus vicieuses encore. Exemple avec le piratage d'un concessionnaire de Lamborghini de l'Est de la France.

Derrière un piratage informatique, 99 fois sur 100, se cache le vol des données que le malveillant à pu rencontrer dans son infiltration. Des données qui se retrouvent, dans l'heure, quand ce n'est pas dans les minutes qui suivent la pénétration du site dans des forums et autres boutiques dédiés à l'achat et revente d'informations subtilisées.Un concessionnaire de Lamborghini, à Mulhouse, vient d'en faire les frais.

Une fois les contenus dérobés exploités (phishing, escroqueries…) le pirate s'en débarrasse en les diffusant sur la toile. C'est ce qui vient d'arriver à un concessionnaire automobile de l'Est de la France. Ici, nous ne parlons pas de la voiture de monsieur et madame tout le monde, mais de Lamborghini.

Prend son site web par dessus la jambe et finir piraté !

Le concessionnaire se retrouve avec l'ensemble des pousses bouton de la planète aux fesses. De petits pirates en mal de reconnaissance qui profitent d'une idiote injection SQL aussi grosse que l'ego surdimensionné de ces « piratins ». Bilan, le premier pirate a vidé le site, revendu/exploité les données. Il a ensuite tout balancé sur la toile. Les « suiveurs » se sont jetés sur la faille et les données. J'ai pu constater des identifiants de connexion (logins, mots de passe) ou encore des adresses électroniques lâchées en pâture. Des courriels internes (webmaster, responsables du site…).

Article original 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

Original de l'article mis en page : ZATAZ Un concessionnaire Lamborghini de Mulhouse piraté – ZATAZ

Le malware Nymaim s’attaque désormais aux institutions financières du Brésil

Le malware Nymaim s’attaque désormais aux institutions financières du Brésil

Après avoir contaminé l'Europe et l'Amérique du Nord en 2013, le malware Nymaim refait surface 3 ans plus tard et se propage désormais via une campagne de spearphising intensive, en utilisant un document Microsoft Word comme pièce jointe infectée

Lors de la découverte de la souche originale de Nymaim en 2013, notamment avec ses techniques de code modulaire (chaîne d'abattage et d'évasion), nous avions pu remarquer que plus de 2,8 millions d'infections s'étaient propagées. Sur le premier semestre 2016, ESET a de nouveau observé une augmentation significative de détections du malware Nymaim.

Infectant principalement la Pologne (54%), l'Allemagne (16%) et les Etats-Unis (12%), cette mutation du malware Nymaim a été détectée comme appartenant à la catégorie *Win32/TrojanDownloader.Nymaim.BA.* Elle utilise le spearphishing et une pièce jointe (type Word.doc) contenant une macro malveillante. Utilisée pour contourner les paramètres de sécurité par défaut de Microsoft Word via les techniques d'ingénierie sociale, l'approche est très dangereuse dans les versions anglaises de MS Word.

« Grâce à ses techniques d'évasion sophistiquées, l'anti-VM, l'anti-débogage et les flux de contrôle, cette fusée à deux étages sert à livrer le ransomware comme charge utile finale. Ce code que l'on peut nommer « Trojan modulaire » est impressionnant par sa faculté à voler les informations d'authentification de sites de banque électroniques dans les formulaires typiques en contournant la protection SSL. Ce code malveillant a évolué de façon à fournir des logiciels espions », explique Cassius de Oliveira Puodzius, Security Researcher chez ESET en Amérique Latine.

En avril 2016, la version précitée a été rejointe par une variante hybride de Nymaim (Gozi) qui avait pour cible les institutions financières d'Amérique du Nord, mais également en Amérique latine et principalement au Brésil. Cette variante fournit aux cybercriminels le contrôle à distance des ordinateurs compromis plutôt que de chiffrer les fichiers ou bloquer la machine – comme cela se fait habituellement.

En raison des similitudes entre les cibles visées dans chaque pays et les taux de détection, nous pouvons affirmer que les institutions financières restent au centre de cette campagne.

« L'étude complète de cette menace est toujours en cours. Toutefois, si vous pensez que votre ordinateur ou votre réseau a été compromis, nous vous recommandons de vérifier que les adresses IP et les URL que nous avons partagées dans l'article complet de WeLiveSecurity ne se trouvent pas dans votre pare-feu et dans le journal de votre proxy. Nous vous conseillons de mettre en place une stratégie de prévention en ajoutant une liste noire des des adresses IP contactées par ce malware au pare-feu et les URL à un proxy, aussi longtemps que votre réseau prendra en charge ce type de filtrage », conclut Cassius de Oliveira Puodzius.

Pour lire l'intégralité du rapport et ainsi obtenir des informations complémentaires sur le malware Nymaim, cliquez ici.

Réagissez à cet article

Eleanor, nouvelle menace sur la planète Mac

Eleanor, nouvelle menace sur la planète Mac

Alors que beaucoup d'utilisateurs de Mac se montrent parfois négligents en matière de sécurité, les équipes de BitDefender ont détecté un nouveau backdoor baptisé Eleanor qui ciblent les Mac et qui peut causer d'importants dégâts sur les machines. En effet, il offre la possibilité aux pirates de prendre le contrôle d'une machine à distance.

Le backdoor Eleanor à l'assaut des Mac

Comme souvent, c'est l'éditeur BitDefender qui a identifié la nouvelle menace qui pèse sur les Mac. Eh oui, même si les dangers sont généralement moindres sur Mac que sur PC, voilà que ceux qui ont choisi les ordinateurs d'Apple doivent se montrer vigilants.

En effet, dès lors que ce backdoor silencieux est parvenu à infecter une machine, il a la capacité de permettre à un attaquant de prendre le contrôle du Mac à distance. Ainsi, les hackers peuvent s'en servir pour voler des données présentes sur la machine piratée, télécharger des applis frauduleuses ou même pour détourner la webcam, une pratique de plus en plus courante.

Reste que l'infection du Mac ne se produit pas toute seule et qu'elle est l'une des conséquences du téléchargement de l'application malveillante Easy Doc Converter. En effet, lors du démarrage d'OS X, cette appli va installer sur le Mac trois composantes : un service Tor, un service web capable de faire tourner PHP et un logiciel dédié. Autrement dit le matériel indispensable pour que s'installe, sur Mac, un backdoor silencieux comme Eleanor.

L'intégralité des Mac concernée par Eleanor ?

Si BitDefender a tenu à alerter sur sa découverte, il semblerait tout de même que tous les Mac ne soient pas tous concernés par cette menace.

En effet, parce que le logiciel Easy Doc Converter n'est pas signé numériquement avec un certificat approuvé par Apple, les risques d'infection sont réduits. D'ailleurs, la marque à la pomme a tenu à le préciser en rappelant que tous les Mac dotés de la protection Gatekeeper n'avaient rien à craindre.

Article original de Jérôme DAJOUX

Réagissez à cet article

Original de l’article mis en page : Eleanor, nouvelle menace sur la planète Mac

---

Selon Denis Jacopini, le Darknet s’apparente à un marché noir

Selon Denis Jacopini, le Darknet s’apparente à un marché noir

---

Bernard Debré, médecin et député LR de Paris, dénonce la simplicité avec laquelle on pourrait acheter des produits stupéfiants sur internet. Denis Jacopini, spécialiste en Protection des données personnelles, cybercriminalité, informatique légale et Sécurité de l'information alerte ceux qui veulent faire un tour sur le côté dark d'Internet.
Interview du 29 juin 2016

https://soundcloud.com/sputnik_fr/denis-jacopini-le-darknet-sapparente-a-un-marche-noir

Pourquoi d'après vous le gouvernement se penche si peu sur le darknet et préfère faire passer loi renseignement qui concerne surtout le coté ouvert d'Internet ?
Qu'est ce que le public doit savoir sur le darknet ?

Est qu'il y a un nombre estimé de personnes qui utilisent le darknet?
12 millions de sites internet pour 1,5 millions à travers le monde.

Quels sont les dangers du darknet?

Des experts disent que bientot le darknet sera le refuge de la liberté d'expression, pensez vous que c'est possible que bientot le public « normal » va passer plus de temps sur le darknet que sur le net ouvert ?

Denis JACOPINI répond à ces questions dans cet interview.
Cliquez sur le cercle orange pour faire play

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

La fraude au Président n’arrive pas qu’aux autres

La fraude au Président n’arrive pas qu’aux autres

Des millions d'euros envolés dans une escroquerie aux faux virements bancaires. Une entreprise Dunkerquoise découvre qu'elle vient de perdre plus de neuf millions d'euros dans la manipulation de ses informations bancaires.

Qu'ils sont fatigants ces gens qui savent toujours tout. Il y a quelques semaines, lors d'une conférence que m'avait demandé une collectivité locale, un responsable d'un bailleur social m'expliquait qu'il ne fallait pas trop exagérer sur les risques de piratage informatique, de fuites de données… J'expliquais alors comment des malveillants s'attaquaient aussi aux locataires de logements sociaux. Le monsieur expliquait alors, pour conforter ses dires « ***depuis que j'ai un antivirus et le firewall incorporé*** […] ***je n'ai plus jamais eu d'ennui avec mon ordinateur portable***« . Le monsieur travaillait pour un bailleur social de la région de Dunkerque (Nord de la France – 59). Et c'est justement à Dunkerque, chez un bailleur social, *Le Cottage social des Flandres*, qu'une nouvelle affaire de fraude au président vient de toucher la banlieue de la cité de Jean-Bart. Une manipulation des informations bancaires qui coûte 25% du chiffre d'affaires de la victime.

23 versements de 400.000 euros

Alors, cela n'arrive qu'aux autres ? L'entreprise Dunkerquoise n'est pas une structure à la Nestlé, Michelin, Total, Le Printemps. 140 employés, 6.000 locataires et un quelques 40 millions d'euros de chiffre d'affaires. Bref, une petite entreprise comme il en existe des dizaines de milliers en France. Le genre d'entité économique qui pense que les pirates informatiques, les escrocs ne s'intéresseront pas à elles. Erreur grave ! Pour *Le Cottage social des Flandres*, les professionnels de la Fraude au Président, la fraude au FoVI, se repartis avec 23 virements de plus de 400.000 euros. Bilan, 9,8 millions d'euros envolés dans les caisses d'une banque basée en Slovaquie. Autant dire que revoir l'argent revenir à la maison est peine perdue. D'autant plus que la fraude a couru du 7 avril au 23 mai. Piratage qui n'aura été découvert qu'un mois plus tard, au départ en vacances d'un dès comptable. Bref, en manquement évident de sérieux, et cela dans toutes les strates stratégiques de l'entreprise. Surtout à la lecture de la Voix du Nord : un responsable explique que l'arnaque était tellement bien montée que la société n'y a vu que du feu, et plus grave encore « ***On a les reins solides, on va pouvoir faire face***. » Après tout, 9,8 millions d'euros « ne » représente que 25% du CA de cette société (Sic !).

Méthode rodée mais simple à contrer

Un exploit que cette fraude ? Les adeptes du social engineering (l'étude de l'environnement d'une cible avant de s'attaquer à son univers informatique) savent très bien que non. Dans l'affaire Dunkerquoise, un compte mail piraté aurait permis le début de cette fraude au président. Détail troublant, les courriels arrivaient ailleurs que sur une adresse type adresse@Cottages.fr ? Car si piratage il y a eu, c'est l'ensemble des services couplés au domaine qui ont pu être corrompu. A moins que le responsable usurpé utilisait un gMail, Yahoo! ou tout autre compte webmail. Toujours est-il que le pirate a mis la main sur une adresse officielle et a pu ainsi manipuler les employés.

Parce que pour éviter un FoVI, c'est aussi simple que de protéger son argent personnel, normal. C'est d'ailleurs très certainement là où le bât blesse. Ce n'est pas mon argent, donc j'en prends soin, mais pas trop. Penser que cela n'arrive qu'aux autres est une grande erreur. Éduquer vos personnels, éduquez-vous, patrons, dirigeants…

Pour éviter un FoVI, contrôler ses informations bancaires

N'autoriser le transfert d'argent qu'après applications de mesures décidées en interne, et quelle que soit l'urgence de la demande de manipulation des informations bancaires. D'abord, la somme d'argent. Plafonner le montant. Si ce montant dépasse le chiffre convenu, obligation d'en référer à la hiérarchie. Un élément qui doit obligatoirement faire « tiquer » dans les bureaux : la demande d'un second transfert, d'une nouvelle modification des Le mot-clé principal « informations bancaires » n'apparait pas dans le titre SEO de la page par la même personne, même entité, doit également être indiquée à la hiérarchie. « ***Paulo, c'est normal de faire 23 versements de 400.000 euros en 2 mois ?*** » – « ***Oui ! Le boss achète des chouquettes en Slovénie. Il me l'a dit par mail !***« . La validation de transfert doit se faire par, au moins, deux personnes différentes, dont un supérieur hiérarchique.

Article original 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

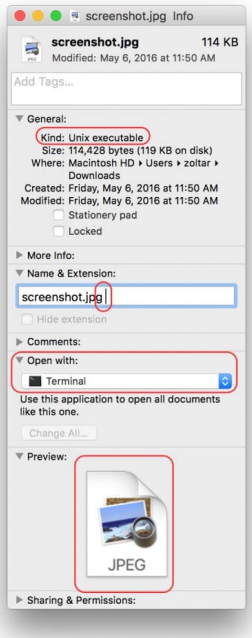
Réagissez à cet article

Original de l'article mis en page : ZATAZ Informations bancaires : la fraude au Président n'arrive pas qu'aux autres – ZATAZ

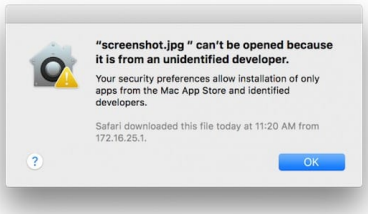
Alerte sur Apple, le Trousseau d’accès mis en défaut par un nouveau malware

	Alerte sur Apple, le Trousseau d’accès mis en défaut par un nouveau malware

Faut-il y voir la rançon du succès des Mac ? Toujours est-il qu'OSX/Keydnap est le deuxième malware de la semaine sur OS X, après Backdoor.MAC.Eleanor. Découvert par ESET, ce nouveau logiciel malveillant est pour le moment d'origine inconnue, mais on connait son mode de fonctionnement.
Téléchargé en pièce jointe ou depuis un site interlope, Keydnap se présente sous une forme bien innocente : une archive ZIP qui contient ce qui ressemble à une image (.jpg) ou un document texte (.txt). Sauf que le suffixe du document contient une espace, ce qui lance un Terminal, et non Aperçu ou TextEdit comme on peut s'y attendre.



En cliquant sur le document, un mécanisme se met en place qui fait prendre des vessies pour des lanternes. L'application attendue s'ouvre et présente le document qui va bien… sauf que dans l'intervalle, le fichier aura ouvert un Terminal (l'icône du Terminal apparait brièvement dans le dock avant d'être remplacée par celle de l'application standard). Une fois l'exécutable lancé, Gatekeeper prévient que le fichier provient d'un développeur non enregistré et qu'il ne peut pas ouvrir le document :



Ce message d'alerte intervient si et seulement si Gatekeeper n'autorise que les applications provenant du Mac App Store et des développeurs identifiés. Sur OS X El Capitan, on peut choisir de lancer une app téléchargée depuis « n'importe où », mais plus sous macOS Sierra.
Une fois lancé, le malware crée une porte dérobée et remplace le contenu de l'exécutable par un leurre téléchargé sur internet ou intégré dans le code du logiciel malveillant – il peut s'agir du document effectivement attendu, comme une image :

La porte dérobée créée par Keydnap est persistante, même si on multiplie les redémarrages du Mac. Il demandera aussi le mot de passe de la session, déguisé sous la forme d'icloudsyncd. Une fois en possession de cette information, il transforme le Mac en open-bar : l'objectif du malware est de récupérer les informations du Trousseau d'accès, qui contient les identifiants et mots de passe de vos logiciels et services en ligne.
À la lumière de cette nouvelle affaire, on comprend mieux pourquoi Apple exige maintenant des logiciels signés sur macOS Sierra.
Merci à Mickaël Bazoge pour son enquête et son article

Réagissez à cet article

Original de l’article mis en page : Nouveau malware sur OS X : OSX/Keydnap détrousse le Trousseau d’accès | MacGeneration