cddb.ch/Bulletin Cybersécurité et Menaces Internet #010 – 18 mai 2012

Sommaire

1. Pour les plus pressés

Le vol de données du prestataire de solutions de paiement électronique Global Payments serait plus étendu qu'annoncé initialement, le nombre d'enregistrements de cartes de crédits subtilisé étant désormais estimé à 7 millions[1]. Verizon a publié son rapport Data Breach Investigations Report 2012, il peut être téléchargé gratuitement[2]. OpenDNS, fournisseur de services DNS avancés propose désormais le chiffrement de trafic DNS pour ses utilisateurs. Le service est gratuit pour les particuliers[3].

Une fois de plus, les utilisateurs possédant l'extension Flash installée dans leur machine sont cordialement invités à la mettre à jour au plus vite[4]. Le correctif de la faille de sécurité PHP permettant l'accès au code source des scripts via un simple paramètre (faille rendue publique par erreur dans le système de notification de bugs il y a deux semaines[5]) n'a pas servi à grand-chose : les chercheurs qui avaient identifié la vulnérabilité originale ont rapidement annoncé que le correctif était inopérant. L'éditeur annonce la disponibilité très prochaine d'un nouveau correctif[6]. En attendant, un patch virtuel peut être appliqué via les pare-feux applicatifs[7]. 23 failles de sécurité ont été corrigées durant le dernier Patch Tuesday de Microsoft[8].

Symantec a publié son dix-septième rapport Internet Security Threat Report, il peut être téléchargé gratuitement[9]. On y apprend en particulier que les attaques utilisant les applications web comme vecteur ont augmenté de 36% en 2011 par rapport à 2010. La régie publicitaire OpenX (concurrent directe de la plateforme Google AdSense) affichant des publicités sur les sites web de ses affiliés serait vulnérable aux attaques de type CSRF. La vulnérabilité est activement exploitée par des pirates en vue de détourner les clics des internautes[10].

La présence de publicités sur le site de l'encyclopédie Wikipedia serait le signe d'une très probable infection de la machine par un programme frauduleux[11]. Après avoir banni à ses citoyens l'accès vers diverses plateformes de services telles que Pirate Bay ou Pastebin, les sites gouvernementaux indiens sont désormais la cible principale des campagnes de déni de service du groupe Anonymous[12]. La mise en œuvre du programme de sécurisation des applications « SDL » (Security Development Lifecycle, conçu par Microsoft) auprès des administrations indiennes pourra peut être réduire l'impact de cette nouvelle campagne d'attaques[13]...

L'équivalent britannique du préposé à la protection des données a condamné la commune de Barnet (banlieue londonienne) à une amende de 105'000 francs (70'000 livres) suite à la perte d'un dossier comportant les données personnelles de quinze mineurs. La perte a eu lieu lors du cambriolage d'un collaborateur. Détail ironique : l'ordinateur volé était entièrement chiffré par cryptographie mais le collaborateur avait joint les versions imprimées des fichiers[14] dans la sacoche.

Un tribunal finlandais a innocenté le propriétaire d'un réseau wifi ouvert depuis lequel des infractions à la propriété intellectuelle avaient été constatées. La société d'édition avait tenté de faire condamner le propriétaire du modem-routeur, pourtant reconnu comme n'étant pas l'auteur des téléchargements[15]. On notera que la Finlande est l'un des rares pays dans lequel l'exploitation d'un wifi domestique sans protection cryptographique ne sera prochainement plus punissable par la loi[16][ndlr: voir commentaire en (a)].

1: http://online.wsj.com/article/SB10001424052702303877604577382522160414052.html
2 : http://www.verizonbusiness.com/Products/security/dbir/
3 : https://www.opendns.com/technology/dnscrypt/
4 : http://www.symantec.com/connect/blogs/targeted-attacks-using-confusion-cve-2012-0779
5 : https://threatpost.com/en_us/blogs/serious-remote-php-bug-accidentally-disclosed-050312
6 : https://threatpost.com/en_us/blogs/php-group-set-release-another-patch-cve-2012-1823-flaw-050812
7 : http://blog.sucuri.net/2012/05/php-cgi-vulnerability-exploited-in-the-wild.html
8 : https://blogs.technet.com/b/srd/archive/2012/05/08/ms12-034-duqu-ten-cve-s-and-removing-keyboard-layout-file-attack-surface.aspx
9 : http://www.symantec.com/threatreport/
10 : http://www.infosecstuff.com/openx-csrf-vulnerability-being-actively-exploited/
11 : http://www.theregister.co.uk/2012/05/17/wikipedia_click_fraud_malware_warning/
12 : http://www.theregister.co.uk/2012/05/18/anonymous_ddos_india_sites/
13 : https://www.microsoft.com/en-us/download/details.aspx?id=29857
14 : http://www.theregister.co.uk/2012/05/17/ico_fines_barnet/
15 : http://arstechnica.com/tech-policy/2012/05/finnish-court-rules-open-wifi-network-owner-not-liable-for-infringement/
16 : http://www.techdirt.com/blog/wireless/articles/20100611/1234429783.shtml

(a) : [ndlr : cette décision est une claque adressée au lobby finlandais des fournisseurs d'accès et d'équipements réseaux, qui restent les bénéficiaires économiques directs d'une phobie largement véhiculée aux consommateurs. Ces derniers sont en effet fréquemment convaincus qu'un réseau sans-fil les mènera directement à la case prison si un inconnu s'y connecte pour commettre des crimes informatiques tels que le téléchargement illégal de films et musiques, de fichiers à caractère pédophile ou la commission d'actes de piratage informatique contre des entreprises. La conséquence immédiate de cette phobie étant l'absence quasi-généralisée de réseaux wifi proposés en libre accès dans les villes, petites ou grandes, ou mis à disposition de communautés (partages d'accès au sein d'immeubles et/ou associations), contraignant les touristes et citoyens à passer par des bornes payantes exploitées par les opérateurs dominants].

2. En bref

86% des applications web conçues sur mesure exposent l'organisation à une intrusion
Un représentant de Fortify, division de HP dédiée à l'analyse automatisée de code source d'applications, a annoncé la semaine dernière qu'environ 86% des applications web conçues sur mesure pour des entreprises contiennent des failles de sécurité de sévérité haute ou supérieure. L'éditeur explique cette prévalence élevée par une population de clients « testeurs » particulièrement réduite dans le cas des applications web conçues sur mesure. L'éditeur précise également que les vulnérabilités observées dans les applications web commerciales ont diminué en quantité ces deux dernières années alors que leur sévérité marginale a augmenté. « Il est primordial pour les organisations de bien comprendre que les applications web conçues et développées sur mesure constituent aujourd'hui une cible de premier choix pour des pirates informatiques. » (Fortify)
-- http://www.computing.co.uk/ctg/news/2173851/custom-built-web-applications-vulnerable-attack

Atlassian confirme une faille de sécurité critique dans son produit Confluence
L'éditeur du système de gestion de contenu et d'Intranets d'entreprise Confluence a confirmé jeudi dernier l'existence d'une faille de sécurité de sévérité critique. La vulnérabilité affecte toutes les versions antérieures à 4.2 et permet de déclencher l'arrêt pur et simple de la plateforme au moyen d'une requête XML, sans authentification préalable. Ce type de faille constitue un excellent cas d'école lorsqu'il s'agit de clairement distinguer les attaques de déni de service distribué (paralysie du système suite à un accroissement illégitime de la demande) et les attaques de déni de service non-distribuées (paralysie du système suite à une sollicitation frauduleuse).
-- https://confluence.atlassian.com/display/DOC/Confluence+Security+Advisory+2012-05-17#ConfluenceSecurityAdvisory2012-05-17-RiskMitigation

Elcomsoft ajoute l'extraction via iCloud à son outil d'investigation de mobiles iPhone
Elcomsoft, éditeur du produit d'investigation d'appareils mobiles Phone Password Breaker, a ajouté une nouvelle fonctionnalité permettant l'extraction transversale des données résidant dans la plateforme Apple de sauvegarde de données en ligne, iCloud. En cas d'obtention de l'identifiant d'un utilisateur (par exemple suite à l'extraction des données du téléphone), l'outil est capable d'extraire une copie intégrale des données du compte, étendant ainsi l'extraction à la totalité des terminaux de l'utilisateur (téléphones, tablettes, ordinateurs fixes et portables). Pour l'instant, l'éditeur annonce ne vendre sa solution qu'aux autorités de police et sociétés d'investigation numérique reconnues…
-- http://www.theregister.co.uk/2012/05/17/elcomsoft_data_retrieval_tool/

3. OpenDNS : ajout de filtrage dynamique anti-Flashback et chiffrement de requêtes DNS

OpenDNS, organisation proposant un service DNS de sécurité accrue et gratuit pour les particuliers, a récemment mis en place deux nouvelles fonctionnalités : un filtre Flashback et le chiffrement DNS.

La première fonctionnalité est un filtrage transparent pour les clients infectés par le cheval de Troie Flashback[1]. Lorsque la machine est infectée, Flashback tente quotidiennement de joindre l'un des serveurs maîtres afin de collecter d'éventuelles nouvelles instructions. L'adresse internet du serveur de contrôle est modifiée automatiquement chaque jour. Flashback intègre cet algorithme pour calculer le nom du serveur à joindre. Le filtre mis en place par OpenDNS suit l'évolution de cet algorithme et intercepte simplement les tentatives de résolution des machines clientes en retournant l'adresse de boucle locale (la machine pointe alors sur elle-même).

L'éditeur avait déjà utilisé ce mécanisme de protection à plusieurs reprises pour d'autres chevaux de Troie, ce qui a permis dans de nombreux cas de réduire les conséquences d'une infection de la machine de l'utilisateur. L'on notera toutefois que les pirates, ne manquant pas d'ingéniosité, ont anticipé une telle contremesure en dotant Flashback d'un mécanisme de repli (contre-contremesure) pour obtenir l'adresse du serveur de contrôle via des requêtes Twitter[2].

La seconde protection, elle aussi très demandée des internautes, est le chiffrement des requêtes DNS par DNScrypt pour les machines Windows (la version pour ordinateurs Mac existe depuis décembre 2011). Ce chiffrement adresse essentiellement deux menaces : premièrement, il empêche la collecte étendue de données de trafic par les fournisseurs d'accès zélés ou collaborant avec des gouvernements intrusifs. En second lieu, il empêche un pirate de modifier les résultats DNS via de simples interceptions de trafic, une attaque très courante par exemple dans les réseaux wifi publics, d'hôtels ou de congrès. Le chiffrement peut être activé via l'installation du client DNSCrypt fourni gratuitement sur le site d'OpenDNS[3].

1 : https://blog.opendns.com/2012/04/11/flashback-much-ado-about-something
2 : http://news.drweb.com/?i=2410&c=5&lng=en&p=0
3 : https://www.opendns.com/technology/dnscrypt/

4. Chiffres et statistiques (source : Verizon data breach investigations report 2012)

L'échantillon du rapport pour l'année 2011 est composé de 855 cas d'intrusion informatique survenus durant l'année 2011. Dans le cas d'incidents de vol de données, 174 millions d'enregistrements ont été compromis.

Dans 79% des cas, l'organisation victime de l'intrusion n'a pas été directement ciblée mais ses systèmes présentaient des vulnérabilités facilement exploitables. Les organisations compromises ont, dans 92% des cas, eu connaissance de l'intrusion suite à l'intervention d'un tiers et l'investigation de l'incident a révélé dans 97% des cas que l'intrusion n'aurait pas été possible si des contrôles fondamentaux (référentiels de type Top XX) avaient été mis en œuvre. Parmi les victimes qui exploitaient des applications sujettes à certification selon la norme PCI-DSS, 96% d'entre-elles n'avaient pas entrepris la démarche de certification.

Dans 75% des cas d'intrusion, l'attaquant a investi de quelques minutes à quelques heures pour identifier la brèche et l'exploiter. Dans le cas des grandes organisations, il a fallu, pour 43% des intrusions, moins de cinq minutes à l'attaquant pour identifier la brèche. Dans 83% des cas d'intrusion, entre quelques semaines et plusieurs mois se sont écoulés entre l'exploitation et la découverte de l'incident. Dans le cas des grandes organisations, il leur a fallu de plusieurs mois à plusieurs années (48% des cas) pour remarquer l'incident. Dans 55% des cas d'intrusion, il a fallu à l'organisation de plusieurs jours à plusieurs semaines pour rétablir la confiance dans son infrastructure.

1 : http://www.verizonbusiness.com/Products/security/dbir/

5. Code de conduite « anti-botnets » pour les fournisseurs d'accès et grandes entreprises

L'OTA (Online Trust Alliance), une initiative dont les principaux éditeurs et fournisseurs d'accès Internet américains sont membres, a publié un ensemble de recommandations destinées à faciliter la lutte contre la prolifération de botnets (*réseaux de zombies*) dans les structures informatiques de grande taille et auprès des fournisseurs d'accès Internet.

L'*Anti-Botnet Code of Conduct*[1] recommande aux organisations concernées la mise en œuvre d'au moins une activité dans chacun des cinq processus globaux suivants: sensibilisation des utilisateurs, détection des systèmes infectés, notification des propriétaires de systèmes infectés, nettoyage des systèmes infectés et collaboration entre fournisseurs adjacents. L'ensemble des recommandations pour la lutte contre la prolifération de botnets est aujourd'hui formalisé sous la forme d'une RFC (rfc6561)[2].

De nombreux experts s'accordent aujourd'hui sur la place centrale qu'occupent les fournisseurs d'accès, et autres entreprises opérant de grands réseaux informatiques, dans la lutte contre la prolifération de réseaux de zombies. Il a été jusqu'ici particulièrement difficile de convaincre ces organisations de collaborer [ndlr : une situation s'expliquant probablement par l'absence d'arguments motivants tels que l'éthique, la déontologie, la protection des consommateurs et le soutien passif des activités criminelles de structures organisées].

Toutefois, le renouvellement continu et particulièrement créatif des techniques d'infection, couplé à une compréhension accrue des opportunités d'exploiter de nombreux sites web vulnérables, induit aujourd'hui une prolifération de machines infectées telle qu'il en résulte un manque à gagner important pour plusieurs acteurs majeurs du web (p.ex. : fraude et détournement de clics sur les publicités, vente de « faux » logiciels) et des coûts particulièrement élevés pour les fournisseurs (détournement abusif de la bande passante), les institutions financières (coûts de la fraude à la carte bancaire et vol d'identité) et les réseaux informatiques majeurs, tels que ceux des universités[3]. L'argument strictement financier ainsi formulé pourrait changer la donne et désormais convaincre les acteurs concernés d'entamer une collaboration efficiente…

1 :
http://www.otalliance.org/resources/botnets/20120322%20WG7%20Final%20Report%20for%20CSRIC%20III.pdf
2 : https://www.ietf.org/rfc/rfc6561.txt
3 : http://www.macworld.co.uk/mac/news/?newsid=3355474

6. [Analyse] Retour sur Flashback ou comment retenir la leçon de "petit deviendra grand"

Avec plus de 800'000 systèmes Mac infectés en moins de deux mois et de nombreuses apparitions en grandes lettres sur les magazines spécialisés, FlashBack aura peut-être réussi là où d'autres avaient échoué jusque-là : démontrer aux utilisateurs de systèmes Mac OS que leur machine pouvait elle aussi être directement concernée par la prolifération massive et accélérée d'un cheval de Troie. Réflexion sur l'évolution de Flashback.

L'analyse attentive du virage récemment entamé par les créateurs de FlashBack révèle des éléments intéressants pour la compréhension des menaces présentes sur Internet. FlashBack, rappelons-le [cf. bulletin #009] a été identifié le 30 septembre 2011[1]. La menace fut immédiatement qualifiée de basse par les éditeurs d'antivirus, un choix pertinent vu que l'infection n'était pas automatique : un clic de l'utilisateur devait être obtenu (via ingénierie sociale) pour déclencher son installation.

Vingt jours après la première détection, une troisième variante du cheval de Troie était identifiée (la seconde variante apportait l'exécution en mode privilégié[2]). Cette troisième variante, en plus d'améliorer le canal de communication avec le centre de contrôle, désactivait définitivement le mécanisme de mises à jour des produits Apple installés dans la machine. Dès lors, même lorsque l'éditeur publie une nouvelle mise à jour, la machine ne l'installe pas. L'éditeur F-Secure place aussitôt la barre de risque à « moyen » et quelques rares éditeurs d'analyses technologiques s'intéresseront désormais au sujet plus en détail[3].

Durant les six mois suivants, les créateurs de Flashback ont affiné trois aspects : le protocole de communication, le mécanisme d'infection et les contremesures anti-détection. Par exemple, la septième version de Flashback (Février 2012) intègre un algorithme d'allocation dynamique (au jour près) de l'adresse du centre de contrôle, des détecteurs de solutions antivirus ainsi que les codes d'exploitation de plusieurs vulnérabilités, déjà corrigées par leur éditeur respectif[4].

Le 2 avril 2012, la onzième version de Flashback apparaît dans le réseau. L'avancée technologique est évidente : l'infection s'effectue désormais via l'exploitation d'une vulnérabilité de classe critique (exécution de code arbitraire) présente dans l'extension Java, annoncée au public deux mois auparavant.

Le choix d'exploiter cette vulnérabilité plutôt qu'une autre était particulièrement astucieux pour deux raisons. Premièrement, Apple est réputé imposer un délai moyen de deux mois à ses utilisateurs pour élaborer un correctif de sécurité visant une technologie que l'éditeur ne maîtrise pas. En instrumentant cette vulnérabilité, les créateurs se sont offert une fenêtre d'ouverture sur une communauté intimement convaincue que ces systèmes sont invulnérables aux attaques informatiques et qui considère par extension qu'il est inutile d'y installer un outil de protection. Les détails de la vulnérabilité n'avaient pas été rendus publics au moment de la mise à disposition du correctif de sécurité par l'éditeur[5], laissant supposer qu'ils étaient soit bien connectés à la communauté, soit qu'ils étaient en mesure d'opérer une rétro-ingénierie du correctif de sécurité pour en extraire les détails de la faille.

Deuxième point essentiel : l'extension Java est automatiquement activée lorsque l'internaute navigue sur le web. Il suffisait dès lors aux pirates de placer des routines d'infection sur des sites web publics et vulnérables. Une complication ? Non. Car une fois encore, le tapis s'est déroulé devant eux : plusieurs dizaines de milliers de sites utilisent actuellement des versions vulnérables des produits Joomla et WordPress, deux solutions de gestion de contenu très appréciées des entreprises souhaitant publier des contenus à moindre frais tout en ignorant qu'ils doivent être hautement surveillés. Les pirates n'hésiteront bien entendu pas à disséminer des scripts infectieux[6] sur ces sites vulnérables. En moins de trois jours, le phénomène devient alors suffisamment spectaculaire pour être relayé au grand public : 800'000 hôtes infectés sont recensés.

Ainsi posé, le contexte offrait aux créateurs de Flashback un moyen de propagation à moindre coût, silencieux et de portée globale. En d'autres termes : le Saint-Graal pour des éditeurs de chevaux de Troie, surtout lorsque l'on a compris que la fonction première de Flashback est d'intercepter les publicités affichées dans les navigateurs et de rediriger les clics des internautes vers des régies sous contrôle.

Il est estimé que les créateurs de Flashback auraient pu, durant la période de haute propagation, amasser en moyenne la coquette somme de 10'000 dollars par jour[7]. « Auraient » car les investigations sur les machines infectées ont récemment relevé que moins de 2% du parc infecté incluait le composant d'interception de clics publicitaires[8]. On ne sait pas s'il s'agit d'un bête oubli des pirates ou s'ils voulaient simplement rester plus discrets. Cette estimation exclut toutefois les éventuels revenus générés par d'autres activités telles que la sous-location du réseau ou l'utilisation/ revente d'informations collectées sur les systèmes infectés…

Une activité très probablement rentable (tout dépend du coût de la vie au lieu à partir duquel les pirates opèrent), lorsque l'on réalise avec recul que les créateurs ont disposé de plus d'un semestre pour continuer d'affiner leurs connaissances et successivement publier de nouvelles versions plus performantes de leur création…

1 : http://www.intego.com/mac-security-blog/intego-security-memo-september-26-2011-mac-flashback-trojan-horse-masquerades-as-flash-player-installer-package/
2 : https://www.f-secure.com/v-descs/trojan-downloader_osx_flashback_b.shtml
3 : http://arstechnica.com/apple/news/2011/10/variation-on-mac-malware-disables-built-in-os-x-malware-protections.ars
4 : http://arstechnica.com/apple/news/2012/02/flashback-mac-trojan-is-back-with-new-and-improved-exploit-strategy.ars
5 : http://www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html
6 : https://www.securelist.com/en/analysis/204792227/The_anatomy_of_Flashfake_Part_1
7 : http://www.symantec.com/connect/blogs/osxflashbackk-motivation-behind-malware
8 : http://www.darkreading.com/security-services/167801101/security/attacks-breaches/240000601/flashback-botnet-click-fraud-operation-could-have-been-more-profitable.html

FIN/#010.

BIENTOT 100 ABONNES! VOTRE PARTICIPATION EST LA BIENVENUE:
> Avez-vous apprécié le format de ce bulletin ?
> Souhaitez-vous qu'un sujet particulier soit traité ?
> Avez-vous des recommandations d'amélioration ou des corrections à communiquer ?
--> écrivez à mailing@cddb.ch ou commentez sur le blog : http://cddb.ch

Conditions et tarifs:
- Inscription : envoyer un email avec sujet "inscription texte" ou "inscription PDF" à cddb-mailing@nxtg.net
- Désinscription: envoyer un email avec sujet "désinscription" à cddb-unmailing@nxtg.net
- Le bulletin est publié sur http://cddb.ch 1 à 2 semaines après sa diffusion par email
- Tarif: gratuit
Données sur les abonnements et abonnés:
- Mesures de confidentialité: best effort, liste d'abonnés stockée sur conteneur chiffré, envois en copie carbone
- Eléments conservés: uniquement adresse email et date d'inscription/désinscription
- Diffusion: aucune (sauf cas de force majeure ou distraction exceptionnelle)
- Suppression: sur demande, par email à cddb-mailing@nxtg.net
- Tiers identifiés: fournisseurs d'accès (envoi des bulletins en clair, par courrier électronique)

