Attaque par Phishing

Une banque Suédoise la Nordea a fait l'objet d'une attaque par Phishing
Selon ces sources 250 clients de son service en ligne ont été victimes de phishing, avec vol d'argent.
Le mail envoyé aux clients de cette banque reproduisait exactement l'apparence d'un mail de la banque Nordea, dans la pièce jointe annoncée comme un antispam se cachait un cheval de Troie, nommé Haxdoor.
Lorsqu'il était activé, ce parasite dirigeait les clients vers une fausse page, identique à la page de la banque Nordea, ce qui permettait aux pirates de récupérer les mots de passe des clients.
Au mois de Mai 2006 les banques suivantes ont fait l'objet d'une attaque : BNP Paribas, CCF, CIC et la Société générale, suivies quelques semaines plus tard par le Crédit mutuel et Le Crédit Lyonnais.

Attaque Serveur Racine

Ce mardi 6 Février trois serveurs de noms de domaine (DNS) ont fait l'objet d'une attaque massive sans toutefois occasionner de gêne pour les internautes.
Cette attaque a été confirmée par le département américain de la Sécurité intérieure, car il surveillait un trafic "anormal" sur le Web.
A savoir que ces serveurs de base au nombre de 13, sont la colonne vertébrale de l'Internet, ils traduisent les noms des sites web en adresse IP. Le risque c'est que si une partie des serveurs est touchée, les sites web ne peuvent plus répondre, et les e-mails ne peuvent être livrés correctement
Depuis la dernière attaque de ce type en Octobre 2002, le réseau DNS se veut donc très résistant, car en 2002 les treize serveurs avaient tous subit la même agression.
Afin d'éviter le même scénario l'infrastructure a été répartie sur la planète, de manière à ne pas exposer toutes les serveurs racines.

Attaque sur la VoIp

Des pirates s'attaquent, sur une technologie à la mode la téléphonie via Internet ou VoIP (voix sur IP), à l'aide de robots qui composent des milliers d'appels en quelque seconde.
Le but est de récupérer les données personnelles de l'internaute pour cela ils utilisent plusieurs techniques
- La première technique concerne le Vishing (contraction de VoIP et de phishing) : un message téléphonique vous demande de téléphoner à un service clientèle pour une mise à jour en ligne le message vous invite à fournir vos identifiants en les saisissant sur le clavier de téléphone.
Des cas ont été repérés aux Etats-Unis, au Canada et en Angleterre.
- Une autre technique, le Spit (Spam over IpTelephony) comme le spam le but c'est de saturer la messagerie vocale
Il existe aussi le Spim (Spam over Instant Messaging), équivalent du spam classique les messages publicitaires sont adressés via une messagerie instantanée.
Pour les experts en sécurité, le pire est à venir car de plus en plus de personnes vont utiliser la VoIP.

Nouvelle attaque par phishing

Le phishing, technique pour récupérer les données personnelle, a encore frappé envers une banque, cette fois c'est le Crédit Agricole qui fut attaqué.
Comme toutes les banques, le Crédit Agricole rappelle qu'il ne demande jamais des informations personnelles par courrier électronique.
Les filtres anti-phishing implantés dans les récents navigateurs commencent à détecter ce type d'attaque.

Faille des curseurs animés

Le problème de la sécurité n'épargne personne même les meilleurs.
Le navigateur Firefox considéré comme l'un des plus sur, est touché par la faille des curseurs animés, car il utilise le même module que Windows pour la gestion des curseurs animés

Le problème de cette faille, c'est qu'un pirate peut aussi bien accéder au système comme à tous les fichiers du disque dur; contrairement au navigateur Internet Explorer fonctionnant sous Vista car celui-ci fonctionne dans un mode “ protégé ” c'est à dire avec des accès réduits, lui interdisant de modifier les fichiers systèmes de Vista

Heureusement, Microsoft a prévu de mettre un correctif qui règle ce problème sur n'importe quel navigateur - pensez à faire une mise à jour de votre système
De leur côté, les programmeurs de Mozilla vont prochainement mettre à disposition un patch

Attaque contre l'Estonie

Les sites gouvernementaux de l'Estonie subissent des attaques virulentes de la part de pirates apparemment d'origine Russe, car il existe une communauté russe dans cette région.
Mais à l'heure actuelle rien ne prouve l'origine de cette attaque, car un pirate peut utiliser des ordinateurs zombies pour effectuer cette tâche.
Selon les autorités estionniennes, le départ de cette vague d'attaque viendrait du déplacement d'une statue soviétique du centre de la ville de Tallinn vers une autre ville

Alerte chez Symantec

Faille importante dans les programmes de Symantec, éditeur de logiciel de sécurité, il s'agit :
- Du pare-feu Norton Personal Firewall 2004
- De la suite Norton Internet Security 2004
La faille est due à un contrôle ActiveX qui peut détourner ces programmes à des fins malveillantes
Si l'internaute tombe sur un site piégé, un pirate pourrait installer du code malsain et prendre le contrôle de l'ordinateur
Un correctif est disponible via la mise à jour automatique LiveUpdate
A savoir, les autres produits de l'éditeur ne sont pas concernés

juin

Coup de filet sur Internet

L'OCLTIC (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication) a déjoué une attaque par phishing dont le but était de pirater des comptes bancaires.
Ces pirates utilisaient sur Internet les services de transfert d'argent de la Western Union, spécialiste des transferts de fonds via des mandats postaux, pour effectuer leurs délits.
Pour rappel cette société avait, en avril dernier participé à une campagne de sensibilisation sur les dangers du phishing.
L'argent était détourné vers l'Ukraine et la Russie, le préjudice financier se monte au minimum à 400 000 euros.
Selon les sources policières ces pirates font partie d'un réseau international qui serait à l'origine de cette manœuvre, mais ce mardi la police française a interpellé une cinquantaine de personnes.
Des actions similaires ont eu lieu en Europe sous l'égide d'Europe.

Attaque du Pentagone

Selon un rapport Américian entre 2005 et 2006 : 844 tentatives ont été notifiées ; plusieurs attaques ont lieu chaque jour sur leurs serveurs, mais rares sont celles qui réussissent.
Cette fois, la citadelle Pentagone a tremblé en subissant une attaque informatique sur ces ordinateurs, les pirates ont réussis à pénétrer le système de mails avec comme conséquence 1 500 ordinateurs déconnectés du réseau suite à cette intrusion.
Les autorités mentionnent qu'aucune donnée classée et relative à des opérations militaires n'aurait été chapardée.

Attaque sur les sites italiens

Depuis le 15 juin, les sites en .it (sitesWeb italien) sont victimes d'une attaque de masse, cela concerne plusieurs milliers de sites de toutes catégories : Automobiles, sport, tourisme...
Les pirates ont infecté les pages d'accueil par un code malveillant qui lance le téléchargement de logiciels de type malware et keylogger, dans le but de récupérer des données personnelles
Cette infection est totalement transparente pour l'internaute

Failles dans Yahoo Messenger

Yahoo vient de sortir une nouvelle version de Yahoo Messenger car la version précédente de son programme (version 8.1.0.249) comportait deux failles de sécurité dans les contrôles activeX
Un pirate informatique pouvait prendre le contrôle de la machine ou injecter du code malveillant
Selon les experts en sécurité, cette faille est considérée comme extrêmement critique

Juillet

FBI + CIPAV

C'est après l'arrestation d'un étudiant Américain envoyant des mails alarmistes sur un compte du réseaux communautaire MySpace, qu'est apparu pour la première fois auprès du public la preuve de l'utilisation légale de logiciel espion. Au mois de juin, la justice Américaine accorde au FBI d'utiliser leur programme CIPAV (Computer & Internet Protocol Address)
Ce dernier permet de collecter toutes les informations sur un internaute.

Crédit Mutuel-CIC : alerte au pharming

Mise en garde du Crédit Mutuel-CIC envers ses clients contre un acte de piratage : le Pharming
Cette technique utilise un cheval de Troie pour rediriger les clients vers un faux site imitant le site cic.fr, qui demande de saisir leur identifiant et leur mot de passe dans le but de récupérer ces coordonnées bancaires
Plusieurs établissements bancaires : le Crédit Lyonnais, BNP Paribas, la Société Générale, Crédit Agricole ont déjà subi de telles attaques.
Si vous recevez un mail de votre soit disante banque : ne répondez pas à ces mails et ne cliquez pas sur un lien hypertexte qui vous dirigerez vers un faux site

PDF spammé

Après le spam texte, puis le spam image voici qu'une nouvelle technique fait son apparition le spam au format PDF
Ceci afin d'échapper aux filtres car le message n'est plus dans le titre, image ou texte mais dans une pièce jointe au format .pdf
Ainsi il peut duper n'importe quel utilisateur
En dehors du désagrément qu'occasionne le spam, un fichier pdf est plus lourd qu'un fichier texte cela va entraîné une augmentation du trafic Internet

Les Captcha piratés

Les Captcha sont des images avec une séries de lettres et chiffres qui servent à valider le compte d'un internaute lors d'une inscription
Ces images sont censées empêcher les robots de récupérer les adresses mails dont le but sera d'inonder les messageries de spam.
Mais cette sécurité a été mis à mal par un cheval de Troie HotLan.a, celui-ci pourrait envoyer des spams depuis les comptes de Yahoo et Hotmail

Client de Free spammé

Les clients du FAI Free reçoivent actuellement un mail avec comme objet "Suspension de compte"
Voici le contenu du mail :
"Cher(e) client(e).
Merci de lire attentivement ce courrier. Il contient des informations essentielles, destinées à faciliter l'utilisation de votre compte Freebox et le recours à ses différents services.
Free.fr A l'honneur de vous annoncer qu'elle a enfin mis à votre disposition un système de sécurité total. Pour en savoir plus et souscrire a ce programme Veuillez cliquer sur le lien ci-dessous."
En cliquant sur ce lien, un pirate pourra récupérer votre identifiant et mot de passe de connexion

Août

L'antre du Monstre infiltré

Le site Internet leader sur le marché de l'emploi Monster, c'est fait attaquer ses serveurs par un groupe de pirates.
Ces derniers ont installé un cheval de Troie (Infostealer.Monstres) sur les machines de Monster.
Ce troyen a envoyé un mail avec une fausse offre d'emploi dans le but de récupérer les données personnelles des utilisateurs du site en remplissant un formulaire : leurs noms, adresses mail, numéro de téléphone...
Ensuite le virus Banker.c s'installe pour voler le numéro bancaire, mot de passe...

Free : Nouvelle attaque par phishing

Attention si vous êtes client chez le FAI Free, car si vous avez reçu un mail vous incitant à cliquez sur un lien du type security.free.fr, celui-ci peut être dangereux car il va vous conduire sur un site ressemblant à celui de Free
Comme dans toute pratique de phishing, le pirate informatique tentera de récupérer vos données privées : login - mot de passe...

Le mail comporte comme intitulé :
Objet : problème technique
Contenu
Cher(e) client(e) Merci de lire attentivement ce courrier. Il contient des informations essentielles, destinées à faciliter l'utilisation de votre compte Freebox et le recours à ses différents services. Free.fr A l'honneur de vous annoncer qu'elle a enfin mis à votre disposition un système de sécurité total. Pour en savoir plus et souscrire a ce programme Veuillez cliquer sur le lien ci-dessous"

L'e-mail est signé service@freebox.free.fr

Froideur chez Télé2

Une faille sur le site web de l'opérateur de télécommunications Télé2, a permis à des pirates informatiques de récupérer des données confidentielles de citoyens Norvégiens (environ 60 000 personnes soit 1,3% de la population totale du pays scandinave) en obtenant le numéro personnel d'identification, une série de 11 chiffres, utilisé dans beaucoup de services norvégien

Avec ce numéro, les pirates peuvent l'utiliser pour passer des commandes, détourner l'identité des personnes par un changement d'adresse et ainsi, détourner le courrier du destinataire
Maintes fois alertés par la vulnérabilité de son site, cette fois et devant le fait accompli, l'opérateur a annoncé qu'il allait renforcer la sécurité de son site

Des cookies mal digérés par les hackers

Lorsque vous utilisez les liens hypertextes, l'ouverture d'une page web peut de façon transparente installer un cookie sur votre ordinateur.
Ce qui permettra au site de connaitre vos goûts, vos habitudes d'internaute, en retour ils pourront vous envoyer des publicités.
Réuni en congrès à Las Vegas du 28 juillet au 2 août dédiée à la sécurité informatique BlackHat, des hackers et experts en sécurité informatique ont démontré la facilité d'accéder et de récupérer le contenu des cookies.
En exploitant cette faille, un pirate en récupérant les données personnelles du cookie, peut prendre le contrôle d'une page personnelle, voler les mots de passe puis accéder à distance à un ordinateur, ou lui insérer du code malveillant
Les sites de mise en réseau comme MySpace sont vulnérable mais d'autres le sont tout autant Google, facebook...
Par cette mise en garde, les sites vulnérables pourrait proposer comme solution de crypter leurs cookies
Contre le piratage de Hot spot Wifi, une technique pour se prémunir contre le vol de données : utiliser une connexion sécurisée SSL.

Septembre

PDF (Pas De Faille) malheureusement si !!

Attention faille très critique pour les documents au format PDF sous Windows XP SP2
L'ouverture avec Internet Explorer 7 d'un document .PDF autorise l'exécution de code malicieux pour les versions :
- Adobe Reader 7
- Adobe Reader 8.0
- Adobe Reader 8.1

Le simple fait d'ouvrir un document PDF infecté par le virus ou naviguer sur un site web proposant ce type de document suffit pour compromettre le système d'exploitation Windows XP
Par contre le système Windows Vista, ne serait pas concerné par cette vulnérabilité
La faille est confirmé par l'équipe de la société Adobe
Dans l'attente d'un correctif, la solution proposée est simpliste :
Eviter absolument d'ouvrir ce type de document

Faille dans le programme Wordpress

Découverte d'une vulnérabilité dans le logiciel de création de blog Wordpress version antérieure à la 2.2.3 et pour Wordpress MU antérieure à la version 1.2.5a, cette faille peut permettre à un pirate informatique d'effectuer des attaques de type cross-site scripting ou des injection SQL
Ces failles sont considérées par les experts en sécurité comme moyennement critique
La solution la plus judicieuse, c'est de mettre à jour le logiciel Wordpress

Attention aux hameçons

Depuis ce mois de septembre, nombres de sites sont la cible du phishing
- AOL
- Paypal
- FREE
- Kaspersky
- La Poste Suisse
- Voila.

La technique du phishing ultra connu, consiste à envoyer un faux mail pour inciter les internautes à cliquer sur un lien hypertexte qui les renvois vers de faux sites afin de récupérer tous types d'informations personnelles sur l'internaute
Deux pistes facilement repérable pour les novices :
- Le contenu du message dans un Français approximatif
- Le lien interne au message qui peut inciter l'internaute à cliquer dessus

Des enchères gourmandes

Ils s'avèrent que les cookies des clients du site d'enchère eBay peuvent être intercepter par des pirates informatiques en exploitant des failles
Avec les renseignements contenus dans les cookies, les pirates peuvent sans problème prendre l'identité du client et faire des achats, faire des enchères à la place du client
Attention à tous messages contenants un lien pour accéder au site d'eBay

Cyber-bataille sur le Net

Après le Pentagone qui a subit au mois de juin une attaque de masse sur ces serveurs
C'est au tour des nations suivantes : l'Allemagne - la Grande Bretagne - la France - la Nouvelle Zelande, de subir les assauts de leurs systèmes de sécurité
Selon une source du Financial Times les attaques du Pentagone, serait le fait de pirates chinois
D'autres sources comme The Guardian ou le Monde dénoncent ces cyberattaques venant de Chine
Le porte-parole du ministère des affaires étrangères Jiang Yu a démenti ces accusations qui sont sans fondement.