SÉCURITÉ INFORMATIQUE

numéro 20 juin 1998

SÉCURITÉ DES SYSTÈMES D'INFORMATION

éditorial

Peter Pan et le Capitaine Crochet

Pourquoi en informatique parle-t-on de pirates et de piratage? Peut-on sérieusement imaginer, en contemplant son moniteur de 17 pouces, l'irruption vociférante de brutes avinées, sabrant tous ceux qui leur résistent et n'épargnant le capitaine que le temps de lui rôtir les orteils pour lui faire avouer la cache de sa cassette à doublons? Les Anglo-Saxons seraient-ils plus prosaïques? Certes non, leurs «hackers» (du verbe «to hack»: hacher, tailler en pièces…) évoquent eux aussi les mers chaudes et la flibuste.

Qu'en est-il en réalité ? Celui qui menace la sécurité et l'intégrité de nos systèmes d'information est le plus souvent un cérébral et un solitaire. Au soleil, au rhum et au vent du large, il préfère la lueur glauque des écrans cathodiques, le Coca-Cola et la fumée d'un joint. Plutôt que de faire la tournée des tavernes avec ses complices, il s'en tient à distance et n'échange avec eux que des signaux cabalistiques. Si ses attaques sont moins spectaculaires que celles de Barbe-Noire, elles n'en sont pas moins dangereuses. Elles le sont d'autant plus, qu'homme de l'ombre, il entre en catimini aux heures où la vigilance s'émousse et, son forfait accompli, ressort en s'efforçant d'effacer les traces de son passage.

Pour vous décrire la menace que ces pirates font peser sur nos systèmes et nos réseaux, nous avons demandé le concours des services spécialisés du ministère de l'Intérieur. Ils ont pour mission de traquer la délinquance informatique sous toutes ses formes, et, parmi les cas concrets qu'ils nous dévoilent, certains ont causé des troubles sérieux dans des laboratoires. Réfléchissons donc sur ce que chacun d'entre nous (directeur d'unité, administrateur système, simple utilisateur…) doit faire pour protéger ses outils et ses données. Empressons-nous ensuite de mettre en pratique toutes les consignes de sécurité en gardant toujours à l'esprit que :

le piratage, cela n'arrive pas qu'aux autres.

Philippe Schreiber
Fonctionnaire de Défense

Le CNRS renouvelle son accord de licence avec AVP

La difficulté d'effectuer des mises à jour régulièrement a, jusqu'à présent, constitué le point le plus faible de la protection contre les virus. AVP (logiciel antivirus pour PC), outre qu'il est parmi les meilleurs, d'après *Virus-Bulletin* de mai 1998, pour la détection des fichiers contaminés, offre une mise à jour de la base des signatures, hebdomadaire et facile à faire.

Les personnels CNRS peuvent obtenir des licences d'utilisation en envoyant une demande à robert.longeon@cnrs-dir.fr. stipulant le nom du laboratoire bénéficiaire.

La délinquance informatique: où en est-on?

Le piratage, ça n'existe pas qu'à la télé !

Pas une semaine ne se passe sans qu'un reportage ne vienne relater les terribles menaces qui planent sur Internet, avec, à l'appui, l'interview de X, petit génie de l'informatique qui, à neuf ans, hackait la NASA pour la première fois, et déclare, sous l'œil affolé du journaliste, pouvoir faire fondre les processeurs des super-calculateurs du Pentagone. Difficile dans ces conditions de débrouiller le vrai de l'exagération, de se forger une idée objective sur les dangers qui pèsent véritablement sur les réseaux. A vrai dire, entre les alertes aux faux virus qui se multiplient et les statistiques discordantes sur la « sinistralité informatique » – fondées le plus souvent sur des extrapolations hardies et des projections fantaisistes –, il n'est pas surprenant qu'un grand nombre d'utilisateurs abordent le problème de la sécurité informatique avec circonspection. Après tout, ce marché-là n'a rien de virtuel, et il ne s'agirait pas de tomber dans le panneau d'une «cybertrouille» fomentée par d'habiles marchands et amplifiée aussitôt par certains journalistes en quête de sensationnel.

Il s'agit donc ici – à travers l'expérience récente du ministère de l'Intérieur dans la lutte contre la délinquance informatique – d'apporter un éclairage sur les attaques qui menacent véritablement nos systèmes informatiques et celles dont il faut relativiser la portée. Nous détaillerons également le déroulement de ce type d'investigations, afin de convaincre ceux qui ne le seraient pas encore qu'il est possible de remonter jusqu'aux auteurs des piratages, à condition d'avoir mis en place au préalable les outils adaptés.

Pour des raisons évidentes, les exemples qui émaillent cet article ne sont jamais nominatifs. S'ils sont tous récents, ils ne sont pas forcément issus du milieu de la recherche, partant du principe qu'il y a toujours quelque enseignement à tirer des infortunes vécues par les administrateurs réseaux...

..... suite page 2 ...

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

suite de la page 1

Les intrusions

Si, légalement, la peine encourue pour une simple tentative d'intrusion sur un système informatique est de 100 000 F et un an de prison (*cf.* tableau), à ce jour personne n'a jamais été inquiété pour avoir tenté sans succès de fracturer un verrou informatique. Et pour cause: plusieurs centaines d'attaques sont recensées quotidiennement sur le seul site du ministère de l'Intérieur. Impossible donc de ne pas crouler sous le nombre, ni d'ailleurs de faire le tri entre les véritables attaques et les simples erreurs de manipulation. Les investigations ne concernent donc que les intrusions qui ont abouti – soit 900 sites environ en France pour 1997 –, dont le ministère a pu avoir connaissance, ce qui correspond globalement à 10 000 ordinateurs visités indûment. A ces statistiques s'ajoute bien sûr le chiffre noir des piratages dont nous n'aurons jamais connaissance soit qu'ils soient suffisamment discrets pour passer totalement inaperçus, soit qu'ils n'aient été portés à la connaissance d'aucune autorité; chiffre sur lequel il n'est pas nécessaire d'extrapoler: la partie émergée de l'iceberg est suffisamment éloquente pour donner matière à réflexion.

Les pirates ont-ils un truc ?

Levons tout de suite une interrogation fondamentale: comment procèdent les pirates pour pénétrer sur les systèmes?

Encore une fois, il faut tordre le cou à l'image galvaudée du piratage «high-tech » qui mettrait en œuvre des failles encore inconnues pour transpercer un «firewall» solide et bien configuré. Les méthodes utilisées par les pirates sont beaucoup plus prosaïques. La plus utilisée pour pénétrer sur les machines qui ne disposent pas de protection particulière reste la récupération du fichier de mots de passe par l'intermédiaire d'une faille classique du système d'exploitation. Les pirates ont ensuite tout leur temps pour casser le «etc/passwd » une fois qu'il a été rapatrié sur leur propre ordinateur. C'est simple et efficace: tous les outils étant à disposition sur Internet pour effectuer ce type d'attaque (*cf.* http://www.rootshell.com ou http://www.dhp.com/~fyodor/sploits all.html), la meilleure parade est comme souvent la plus simple: elle consiste à attribuer automatiquement aux utilisateurs des mots de passe solides. En effet, partant du principe qu'il suffit au pirate de parvenir à cracker un seul mot de passe pour s'introduire dans le système, il paraît illusoire de s'en remettre totalement à la bonne volonté des utilisateurs...

L'autre technique consiste à dérober le mot de passe de l'un des utilisateurs habituels du système. Le plus souvent ce mot de passe est subtilisé alors que l'utilisateur se connecte depuis une machine elle-même piratée et piégée par un «sniffer». Le risque est maximal dans deux cas: lorsque la connexion s'effectue depuis un site «ouvert» du type université, salon–forum ou cybercafé, par exemple, ainsi que lorsque les connexions s'effectuent depuis l'étranger. Ce dernier cas est particulièrement préoccupant: en effet, en 1997, il a été possible de relier dans 50% des cas les piratages depuis l'étranger avec le déplacement d'un utilisateur hors de nos frontières. Il ne s'agit évidemment pas de suspecter les organismes d'accueil de piéger les accès qu'ils peuvent mettre à disposition. Lorsque les enquêtes permettent de le déterminer, il s'avère le plus souvent que les sites sont eux-mêmes piratés à leur insu, ou, plus inquiétant encore, qu'une entité capable d'intercepter les transmissions satellitaires (*cf.* encadré «Le système échelon») a subtilisé les trames dans lesquelles les mots de passe circulent en clair. Dans ce cas, la seule parade efficace est d'utiliser, lors des déplacements à l'étranger, des procédures de connexions qui sont invalidées dès la fin de session. Bien sûr ces techniques sont un peu délicates à mettre en œuvre les premières fois, mais elles existent dans des versions basiques, c'est-à-dire uniquement logicielles, pour des coûts raisonnables. Une fois encore, ces procédures n'ont de sens que si elles sont appliquées par tous.

Enfin, il n'est pas rare que le code d'accès utilisé par les pirates ait tout bonnement été fourni – indirectement – par l'utilisateur lui-même. Ce dernier, soucieux de faciliter le travail d'un collègue lui aura «prêté» son accès, le collègue l'aura confié à son fils, lequel l'aura montré à son copain de classe, qui se le sera lui-même fait subtiliser par son frère, pirate accompli, qui se chargera de le répandre dans la communauté des hackers...

Que cherchent les pirates ?

Il faut différencier deux types d'attaques: celles qui visent un site unique et celles dont l'objectif est clairement de s'approprier le contrôle du maximum de machines. Essayons d'analyser les deux processus et de comprendre les motivations des auteurs.

Quand les pirates construisent leur toile...

Les affaires de piratages multisites traitées par notre service en 1997-1998 présentent des similarités étonnantes, les auteurs ayant laissé presque systématiquement le même type de traces.

- Mise en place d'un programme «sniffer» qui permet de capturer les trames réseau afin de dérober les procédures de connexions vers les sites en relation avec celui qui est piraté.

- Mise en place d'un cheval de Troie permettant aux auteurs de se reconnecter à loisir avec les privilèges «root» sur les ordinateurs attaqués sans utiliser les procédures classiques, afin d'échapper à la vigilance des responsables système.

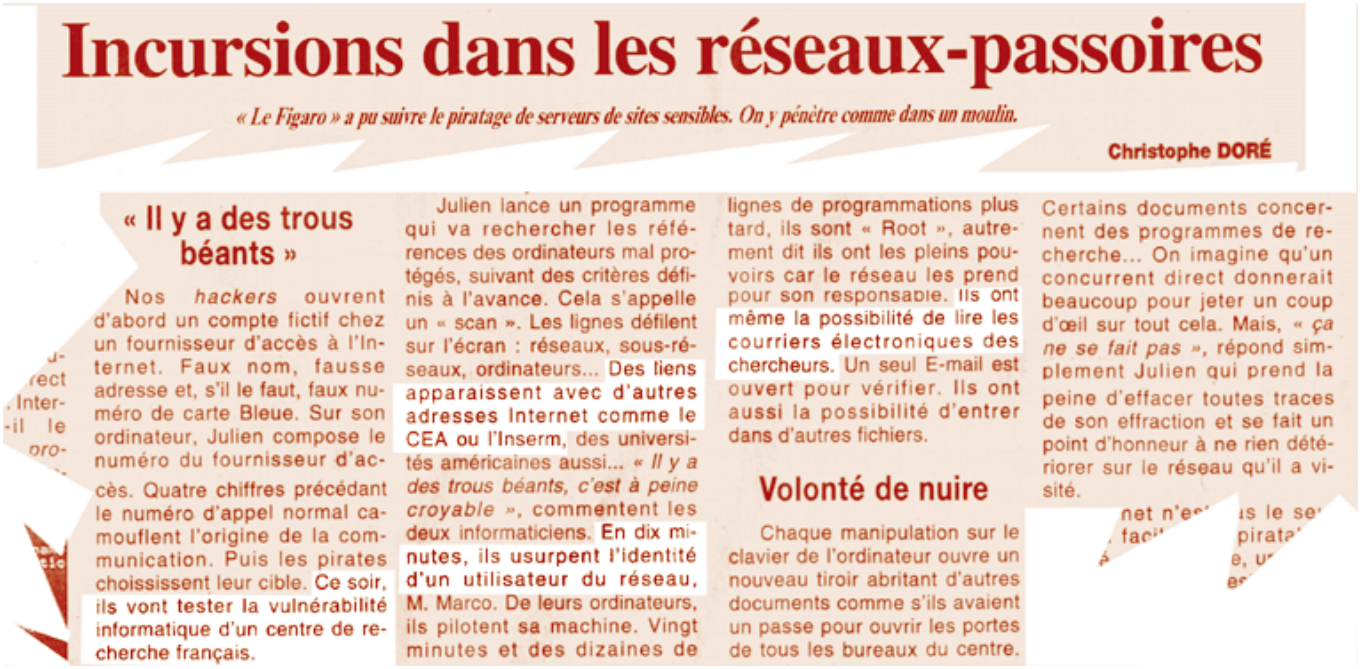
- Dépôt d'une boîte à outil de piratage. Cet ensemble de logiciels, habilement dissimulé dans des répertoires anodins, a servi au pirate pour obtenir les droits «root» sur le système. Il contient également des modules qui sont utilisés pour effacer automatiquement certaines traces des différents fichiers d'accounting du système.

- Dépôt d'un client IRC dénommé «eggdrop». Ce programme de communication permet, outre la création et la gestion de canaux de discussion sur les IRC, le téléchargement de fichiers et les connexions de types «telnet» sans utiliser les ports «FTP, telnet, ou rlogin » traditionnels, c'est-à-dire en échappant aux principaux outils de détection d'intrusions.

La particularité du logiciel «eggdrop» est de créer un réseau virtuel (le «botnet») constitué par l'ensemble des sites sur lesquels les «eggdrop» ont été déposés. Les pirates peuvent alors à loisir rebondir sur toutes les machines qui hébergent un «eggdrop » intégré au «botnet» sans risque de se faire repérer. Cette fonctionnalité est utilisée par les pirates pour transformer les disques durs des sites visités en une vaste zone de stockage de fichiers, essentiellement des images licencieuses, des jeux et des utilitaires piratés. Pour que le «botnet» vive, un certain nombre de machines doivent continuellement rester accessibles, d'où la nécessité pour les pirates d'agrandir le «botnet» au fur et à mesure de la découverte des piratages...

Certains responsables ont tendance à tolérer ce type d'intrusions, considérant que le préjudice subi ne contrebalance pas le temps passé à essayer de détecter ce type d'intrusions. Il faut donc insister sur deux points: d'une part, la nature des fichiers déposés est souvent délictueuse: programmes sans licence ou interdits de diffusion en France, images à caractère pédophile..., ce qui porte incontestablement atteinte à la crédibilité de l'institution visée et risque de l'entraîner dans des suites judiciaires fâcheuses. D'autre part, le système dispose alors d'une porte dérobée excessivement difficile à surveiller et qui est contrôlée par un individu extérieur à l'établissement ayant tout loisir pour en diffuser les clés à qui bon lui semble. Si par ailleurs le système est correctement sécurisé, les utilisateurs continueront à entreposer en confiance le fruit de leur travail sur les disques, y compris le plus sensible.

Il faut également constater que l'époque des pirates respectueux des codes de bonne conduite et autre «netiquette » est bien révolue:



Incursions dans les réseaux-passoires

« Le Figaro » a pu suivre le piratage de serveurs de sites sensibles. On y pénètre comme dans un moulin.

Christophe DORÉ

« Il y a des trous béants »

Nos *hackers* ouvrent d'abord un compte fictif chez un fournisseur d'accès à l'Internet. Faux nom, fausse adresse et, s'il le faut, faux numéro de carte Bleue. Sur son ordinateur, Julien compose le numéro du fournisseur d'accès. Quatre chiffres précédant le numéro d'appel normal camouflent l'origine de la communication. Puis les pirates choisissent leur cible. Ce soir, ils vont tester la vulnérabilité informatique d'un centre de recherche français.

Julien lance un programme qui va rechercher les références des ordinateurs mal protégés, suivant des critères définis à l'avance. Cela s'appelle un « scan ». Les lignes défilent sur l'écran : réseaux, sous-réseaux, ordinateurs... Des liens apparaissent avec d'autres adresses Internet comme le CEA ou l'Inserm, des universités américaines aussi... *« Il y a des trous béants, c'est à peine croyable »*, commentent les deux informaticiens. En dix minutes, ils usurpent l'identité d'un utilisateur du réseau, M. Marco. De leurs ordinateurs, ils pilotent sa machine. Vingt minutes et des dizaines de lignes de programmations plus tard, ils sont « Root », autrement dit ils ont les pleins pouvoirs car le réseau les prend pour son responsable. Ils ont même la possibilité de lire les courriers électroniques des chercheurs. Un seul E-mail est ouvert pour vérifier. Ils ont aussi la possibilité d'entrer dans d'autres fichiers.

Volonté de nuire

Chaque manipulation sur le clavier de l'ordinateur ouvre un nouveau tiroir abritant d'autres documents comme s'ils avaient un passe pour ouvrir les portes de tous les bureaux du centre.

Certains documents concernent des programmes de recherche... On imagine qu'un concurrent direct donnerait beaucoup pour jeter un coup d'œil sur tout cela. Mais, *« ça ne se fait pas »*, répond simplement Julien qui prend la peine d'effacer toutes traces de son effraction et se fait un point d'honneur à ne rien détériorer sur le réseau qu'il a visité.

Article du *Figaro* du 20 mars 1998 paru sous la plume de Christophe Doré.

il n'est pas rare de voir le contenu d'un répertoire de travail totalement effacé pour laisser place à «DukeNukem3D» ou «Samantha.jpg»...
Le profil de ces pirates est sans surprise : âgés de 15 à 22 ans, souvent étudiants médiocres, voire autodidactes sortis du système scolaire, ce sont le plus souvent des adolescents curieux, naïfs, et surtout fascinés par le réseau et ses trésors cachés. A première vue, pas de quoi réveiller un contre-espion sur les accords de «patrimoine en péril». A y regarder de plus près, la menace n'est pas si anodine, car certains ont vite fait de vouloir mettre à profit leur savoir-faire.

... et monnayent leurs talents !

En 1997, cinq organismes ont rapporté avoir été contactés par de jeunes garçons proposant de leur vendre des informations dérobées sur les réseaux français dans les domaines de l'industrie et de la recherche. L'un des pirates a présenté à l'appui de ses dires les fichiers de mots de passe de plus de 70 ordinateurs répartis sur 13 sites du même groupe industriel!
Récemment, un groupe industriel français travaillant dans le domaine de l'électronique high-tech s'est vu proposer par un pirate 11 CD-Rom supportant la quasi-totalité des données volées sur les disques durs d'une société concurrente. Hélas ! – pour le pirate –, sa triste offre ne risquait pas de rencontrer beaucoup d'écho : l'entreprise piratée n'était autre qu'une filiale américaine du groupe à qui il tentait de vendre les données!
Courant juillet 1997, un pirate est repéré dans un laboratoire d'Orsay où il s'est introduit afin de se livrer à son occupation favorite : l'exploration des réseaux. L'individu est bien connu des services de police, c'est l'un des pirates les plus actifs de la scène française, catalogué depuis longtemps comme une sorte de «taggeur» Internet, évacuant sur le réseau et ses utilisateurs ses griefs envers notre société. Contre toute attente, l'enquête révélera que ce piratage ne devait rien au hasard. L'auteur, dont la notoriété dépasse largement nos frontières, avait été contacté quelques mois auparavant par un ressortissant d'un pays étranger afin qu'il obtienne des accès vers un organisme de recherche, très bien protégé celui-là. Le marché – de dupe très certainement – était d'échanger l'accès contre un emploi à vie chez le commanditaire.
Pour parvenir à ses fins, notre pirate a tout d'abord recherché un laboratoire entretenant des relations étroites avec la cible qui lui avait été désignée. Il s'y est introduit de nuit, déjouant facilement les mesures de sécurité mises en place. Il se procura un premier accès au réseau en utilisant un compte shell laissé ouvert par mégarde sur l'une des machines, et disposa aussitôt un sniffer. Il revint régulièrement dans le laboratoire pour «relever ses filets» et ne tarda pas à trouver ce qu'il était venu chercher.
Son entreprise a si bien réussi que le site sensible, dont le pirate a ainsi obtenu les accès, a été visité indûment durant les mois suivants à plus de 300 reprises ! Pour l'anecdote, si l'auteur du piratage est actuellement sous les verrous, le commanditaire de l'opération ne sera probablement jamais formellement identifié. Quant au site principalement victime, il a préféré ne pas porter plainte...

Le casse électronique

Cela nous amène au deuxième cas, celui de l'attaque ciblée sur un site précis. Il s'agit généralement de piratages pratiqués avec un souci de discrétion maximal, qui ne sont détectés le plus souvent que grâce à un heureux concours de circonstances. Il est difficile d'évoquer les enquêtes en cours sur le sujet puisqu'elles sont toutes couvertes par le secret de l'instruction ; néanmoins il est bon de noter que quatre d'entre elles, à forte connotation «espionnage scientifique», concernent des laboratoires CNRS.
Un point d'accès incontournable sur l'intelligence économique et la guerre de l'information : http://www.infowar.com.

Vent d'Est sur la cyber-criminalité

Une affaire récente, largement médiatisée, illustre bien cette forme de délinquance ; il s'agit du piratage de la Citibank de New York depuis Saint-Pétersbourg en 1994 attribué à la mafia russe.
En 1991, il existait 785 gangs spécialisés dans le crime organisé en ex-Union soviétique ; en mars 1996, la police d'Etat russe en a identifié 5700 ; aujourd'hui les statistiques officielles en recensent près de 8 000 qui contrôleraient plus de 40% du PNB de la Russie pour un chiffre d'affaires estimé à 100 milliards de dollars annuels selon la Douma. Parmi ces groupes criminels, certains apparaissent comme les plus performants du crime cybernétique sur Internet. Ils sont essentiellement composés de scientifiques et d'informaticiens spécialisés ayant appartenu au «KGB» ou au complexe politico-militaire de l'ancienne Union soviétique.
Le 4 mars 1995, Vladimir Levin, informaticien russe de 24 ans, diplômé de l'université de Saint-Pétersbourg, était interpellé à Londres pour le «casse électronique» de la Citibank de New York.

Des perquisitions menées à Saint-Pétersbourg chez des individus proches du pirate permettaient de récupérer d'importants stocks d'armes, confirmant ainsi que le groupe Levin serait une tentacule informatique de la mafia russe.
Levin était extradé aux Etats-Unis en septembre 1997 pour y être jugé. Le département américain de la Justice l'accusait d'avoir, avec la complicité d'un Russe travaillant dans l'agence new-yorkaise, transféré 400 000 dollars de la Citibank vers des comptes en Israël, en Finlande, en Allemagne et en Hollande.
Il était condamné, par un jugement rendu le 24 février 1998, à trois ans de prison assortis d'une amende de 240 000 dollars.
Par ailleurs, l'enquête avait permis de mettre à jour plusieurs plans organisés de piratage. L'un d'eux visait une grande banque située dans l'est de la France. En janvier 1996, un groupe de quatre à cinq mathématiciens russes, recrutés par un ressortissant allemand, devait s'infiltrer dans le réseau informatique de l'agence bancaire ciblée, dans le but de réaliser des opérations frauduleuses d'importance.
L'enquête révélait qu'un complice des pirates avait déjà approché une employée travaillant dans l'agence en question. Celle-ci était immédiatement mise à l'écart par le service d'inspection de la banque.
Cependant, la police russe précise que, en dépit de l'arrestation et de la condamnation de Levin, de nombreux membres influents de ce groupe sont encore actifs. Elle est convaincue que leurs actions de transferts de fonds illicites et de blanchiment d'argent via les réseaux informatiques se poursuivent...

Que fait la police ?

Quatre services spécialisés traitent les affaires d'intrusions informatiques :

- La Brigade centrale de répression de la criminalité informatique (BCRCI – compétence nationale);
- Le Service d'enquêtes aux fraudes aux technologies de l'Information (SEFTI - compétence Paris + petite couronne) ;
- Les brigades spécialisées de Gendarmerie (compétence nationale) ;
- La Direction de la surveillance du territoire (DST)

La DST est saisie lorsque les piratages ont une connotation d'espionnage scientifique ou industriel, c'est-à-dire lorsque les sites visés sont sensibles ou lorsque les attaques proviennent de l'étranger. La DST présente la particularité de traiter, hors du cadre judiciaire classique, des enquêtes dites «de sécurité». Ces enquêtes informelles s'effectuent à la demande des victimes et en collaboration avec elles, en dehors de tout dépôt de plainte. Elles ont pour objectif principal de remonter aussi rapidement que possible la chaîne du piratage afin que tous les sites impliqués puissent prendre les mesures indispensables de conservation des traces. Lorsqu'il ressort que les auteurs sont susceptibles d'être identifiés, la victime est orientée vers le service de police *ad hoc* si elle souhaite porter plainte.
Si les enquêtes sur les piratages extensifs aboutissent le plus souvent à l'interpellation d'un groupe de jeunes pirates, il en va bien autrement pour les attaques ciblées souvent caractérisées par le soin qu'apportent les pirates à dissimuler toutes traces de leur passage.
L'expérience a montré que deux conditions devaient être réunies pour que l'enquête puisse véritablement déboucher:

- que l'intrusion soit découverte rapidement, c'est-à-dire si possible alors que le pirate est encore actif,
- que l'un des sites attaqués soit en mesure, dès qu'il a détecté l'intrusion, d'enregistrer l'intégralité du trafic réseau pendant un laps de temps suffisant.

Cela implique bien sûr de prendre certaines mesures avant que l'incident ne se déclenche. Certains sites ont mis en place, en plus des outils classiques de sécurisation comme «tcp-wrapper», des logiciels permettant la détection **automatique** d'un comportement anormal du système. Le principe est simple: dès que le pirate installe son «sniffer», son « client IRC», ou modifie un fichier système, l'administrateur est avisé et peut prendre des mesures.
La réaction la plus efficace est alors, lorsque la sensibilité de la machine attaquée le permet, de tolérer quelque temps la présence de l'intrus et d'installer un logiciel «sniffe» du type «tcp-dump» ou «snoop» afin de récupérer l'ensemble des trames réseaux. Il est indispensable d'avoir prévu un support adapté afin de pouvoir archiver les données qui peuvent rapidement devenir encombrantes...

Que risquent les pirates ?

A ce jour, les décisions de justice concernant les intrusions informatiques sont rares (*cf.* http://www.legalis.net/jnet/index.htm et http://grolier.fr/cyberlexnet). Elles concernent essentiellement des piratages ludiques et les sanctions prises ont logiquement été modérées: faibles amendes assorties parfois de quelques mois de prison avec sursis.
Il faut toutefois prendre note d'une décision du TGI de Paris du 8 décembre 1997. Dans cette affaire classique, les auteurs étaient poursuivis pour avoir accédé frauduleusement à un système automatisé de données (SID), et avoir divulgué à un tiers des informations avec une intention de nuire. **La cour a considéré que, « en l'absence de mise en place d'un système de protection ou de manifestation de volonté, par les dirigeants de l'entreprise, de restreindre l'accès au SID », l'accès aux ordinateurs s'était effectué sans fraude et que, de ce fait, le délit n'était pas constitué.**
Les enquêtes relatives aux piratages d'envergure internationale sont encore en cours d'instruction. Les premiers jugements concernant ces types d'affaires ne devraient pas intervenir avant fin 1998. Cette relative lenteur de traitement s'explique par le caractère nouveau de la menace et la nécessité de mettre en place, au fil des enquêtes, les coopérations internationales. Différents projets sont actuellement à l'étude, notam-

suite page 6

Les dangers du Surf

Si le comportement de votre ordinateur est déroutant, ne suspectez pas tout de suite votre collègue de bureau d'avoir reconfiguré la machine en votre absence. Ce peut aussi bien être les conséquences de votre dernière balade sur le Web.
Plus les «browsers» (Netscape ou Internet Explorer) offrent de fonctionnalités, plus ils ouvrent de brèches sur les systèmes. Un site piégé pourra, par exemple, par l'intermédiaire d'une applet Java ou ActiveX, modifier l'un de vos fichiers ou formater le disque dur. Pour tester si votre configuration est correctement sécurisée une bonne adresse : http://www.digicrime.com; à visiter de préférence après avoir effectué une bonne sauvegarde…

Une bonne nouvelle: jusqu'à présent la meilleure parade était de désactiver Java ou activeX. Maintenant certains logiciels permettent de bloquer sélectivement certaines applets Java, ce qui offre un bon compromis: confort de navigation-sécurité.

Les pirates se servent également des informations que nous abandonnons en parcourant leurs sites. Ils peuvent s'en servir pour attaquer ensuite plus effacement, ou usurper les identités dérobées pour envoyer des courriers falsifiés ou des «mail-bombs».
Deux sites intéressants sur le sujet: http://www.cnil.fr/traces/demonst/demo.htm et http://195.146.194.176/europe/mysite/htm/menu/menulight/impertinencelight.html. ■ GR

Principes généraux de sécurité et de bon usage des moyens informatiques

Réglementation : synthèse de la législation en vigueur

Atteinte au Système de traitement automatisé de données (STAD)

Infractions	Protection	Peines encourues	
		Emprison-nement	Amendes
Accès au maintien frauduleux dans un STAD	Art. 323-1 al. 1 NCP	1 an	100 000 F
Atteinte involontaire au fonctionnement d'un STAD avec modification de données ou altération du fonctionnement (même si les dommages causés ne sont pas volontaires lors d'un accès au maintien frauduleux)	Art. 323-1 al.2 NCP	2 ans	200 000 F
Atteinte volontaire avec le fait d'entraver ou de fausser	Art. 323-2 NCP	3 ans	300 000 F
Manipulation frauduleuse (introduction, suppression, modification) de données dans un STAD	Art.323-3 NCP	3 ans	300 000 F

Atteinte au matériel informatique

Infractions	Protection	Peines encourues	
		Emprison-nement	Amendes
Vol de matériel (soustraction frauduleuse de la chose d'autrui)	Art. 311-1 NCP	3 ans	300 000 F
Vol aggravé (accompagné de circonstances aggravantes, prévues aux articles 311-4 et suivants du NCP)	Art. 311-1 NCP	5 ans	500 000 F
Destructions, dégradations, détériorations sans danger pour les personnes (pénalités aggravées pour certains biens ou certaines circonstances)	Art. 322-1 al. NCP Art. 322-2 al. NCP Art. 322-3 al. NCP	2 à 5 ans	2 000 000 F à 5 000 000 F
Destructions, dégradations, détériorations dangereuses pour les personnes (manquement à une obligation de sécurité)	Art. 322-5 NCP	1 à 2 ans	100 000 F à 200 000 F

Loi relative à l'informatique, aux fichiers et aux libertés du 6/01/1978

Infractions	Protection	Peines encourues	
		Emprison-nement	Amendes
Création de fichiers clandestins (fichiers privés non déclarés à la CNIL ou fichiers publics non autorisés)	Art. 41	6 mois à 3 ans	2 000 F à 200 000 F
Enregistrement ou conversation illicite d'informations nominatives	Art. 42	1 à 5 ans	20 000 F à 2 000 000 F
Divulgation illicite (non intentionnelle) d'informations nominatives	Art. 43		2 000 F à 20 000 F
Divulgation illicite (intentionnelle) d'informations nominatives. L'obligation de sécurité est pénalement sanctionnée	Art. 43	2 à 6 mois	2 000 F à 20 000 F
Détournement de finalité d'informations nominatives (utilisation des informations à d'autres fins que celles prévues)	Art. 44	1 à 5 ans	20 000 F à 2 000 000 F
Collectes d'informations nominatives sans avoir informé les personnes interrogées		10 jours à 1 mois	2 500 F à 5 000 F
Entrave à l'action de contrôle de la Commission nationale de l'informatique et des libertés		10 jours à 1 mois	2 500 F à 5 000 F
Entrave au droit d'accès ou de rectification des intéressés		10 jours à 1 mois	2 500 F à 5 000 F

Atteinte au logiciel

Infractions Contrefaçon (reproduction non autorisée, sauf copie de sauvegarde par utilisateur)
Protection Art. L 335-3 CPI
Peines encourues
Emprisonnement 2 ans
Amendes 1 000 000 F

Infractions Les personnes morales peuvent être déclarées responsables pénalement
Protection Art. L 335-2 à 4 CPI
Peines encourues
Amendes Peine pouvant aller jusqu'à la fermeture de l'établissement ou de l'entreprise

Dispositions générales

Infractions Participation à un regroupement en vue de la préparation d'une action frauduleuse punie par les articles 323-1 à 323-3 du NCP
Protection Art. 323-4 NCP
Peines encourues
Emprisonnement 1 à 3 ans
Amendes 300 000 F

Infractions Participation à un regroupement en vue de la préparation d'une action frauduleuse punie par les articles 323-1 à 323-3 du NCP
Protection Art. 323-4 NCP
Peines encourues
Emprisonnement 1 à 3 an s
Amendes 100 000 F à 300 000 F

Infractions Tentative des délits prévus par les articles 323-1 à 323-3 du NCP
Protection Art. 323-4 NCP
Peines encourues
Emprisonnement 1 à 3 ans
Amendes 100 000 F à 300 000 F

CPI : Code de la propriété intellectuelle
NCP : Nouveau code pénal

suite de la page 4

ment au niveau du G7/P8, afin de rendre plus efficace les investigations transfrontalières.

Que nous réserve l'avenir ?

L'accession du plus grand nombre à Internet aura probablement des conséquences directes sur le type de délinquance qui se développera sur le réseau. De plus en plus, le Net devient une sorte de défouloir sur lequel chacun peut, sans trop de risques, exprimer à sa manière ses mécontentements et ses frustrations.

Ainsi le premier trimestre 1998 a été marqué par l'explosion d'attaques d'un nouveau type. Le but n'est plus de visiter discrètement un site, mais au contraire de l'empêcher de fonctionner normalement par tous les moyens. Les pirates se regroupent généralement sous une bannière évocatrice, les «Warlords», les «DarkFlood» ou les «SpammX», et attaquent des nuits durant les sites qui, le plus souvent pour des raisons obscures, ont eu le malheur d'attirer leurs foudres. Les assauts, qui proviennent de multiples machines disséminées sur des domaines souvent eux-mêmes piratés, sont particulièrement difficiles à endiguer.

Il semble donc indispensable que les sites les plus ouverts prennent dès à présent les mesures les plus basiques afin de se prémunir de ce type d'attaques dont le préjudice n'a rien de virtuel...

Restons positifs : l'avenir proche, c'est aussi l'avènement d'une nouvelle génération d'outils de sécurité informatique «intelligents», qui ne se contenteront plus de tenter de bloquer et de détecter les intrusions, mais qui prendront également d'eux-mêmes les contre-mesures adaptées suivant les attaques ; les responsables système pourront enfin passer des nuits paisibles...

Gilles Romain
Ministère de l'Intérieur
Courriel : gilles.romain@wanadoo.fr

Le Parlement européen s'intéresse à «Echelon»

En décembre 1997, le Parlement européen publiait, sur l'initiative du député britannique Glynn Ford, le rapport «Evaluation des techniques de contrôle politique» qui depuis ne cesse de faire des vagues en Europe. Ce rapport dénonce le système d'interception des transmissions hertziennes mis en place par les Etats-Unis dès 1948 pour recueillir le maximum d'informations sur l'Union soviétique et ses alliés.

Ce n'est pas l'existence d'un outil perfectionné d'interception qui inquiète le Parlement européen, mais plutôt l'absence de contrôle qui caractérise aujourd'hui l'utilisation de ce système. En effet, à ce jour, les données collectées sur les cinq continents par le système Echelon sont acheminées à Fort Mead aux USA où elles sont traitées par la NSA (National Security Agency) qui est la plus importante agence de renseignement américaine en terme d'effectif ou de budget. Si la NSA affirme que les informations ainsi obtenues concernent prioritairement le grand banditisme, la lutte anti-terroriste et la prolifération des armements, on a du mal à croire que le système n'est pas également intensivement exploité dans les programmes d'espionnage économique et autre veille concurrentielle. Cela gêne d'autant plus le Parlement européen que seuls cinq pays bénéficient des informations recueillies et triées par la NSA : l'Angleterre, le Canada, la Nouvelle-Zélande et l'Australie. ■ GR

Quid du chiffrement ?

La législation dans le domaine du chiffrement évolue dans le sens d'une plus grande souplesse d'utilisation. Les arrêtés et les décrets d'application de la loi de 1996 sur les télécommunications ont été promulgués en mars 1998. Ils instaurent le principe de la simple déclaration auprès du SCSSI (Service Central pour la Sécurité des Systèmes d'Information) pour un chiffrement à clés de 40 bits, et d'autorisation préalable pour un chiffrement avec des clés de taille supérieure.

En pratique, si une institution souhaite aujourd'hui chiffrer avec des clés de 40 bits, elle peut soit le faire avec l'un des logiciels ayant obtenu une autorisation générale d'utilisation (environ 100 produits à ce jour, dont ceux qui équipent les firewalls), soit déclarer le logiciel qu'elle a choisi auprès du SCSSI.

Si cette institution désire utiliser des clés de plus de 40 bits, deux solutions vont s'offrir à elle : la demande classique d'autorisation auprès du SCSSI, ou l'utilisation d'un logiciel de chiffrement agréé avec des clés générées par un organisme tiers de confiance. À ce jour, seul le SCSSI est apte à délivrer ces clés, mais plusieurs autres organismes sont en cours d'agrément pour fournir le même service.

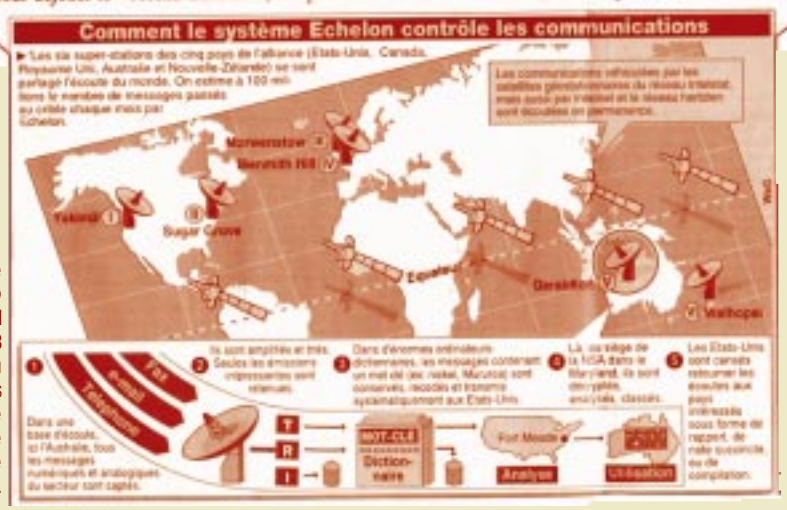
Il semble que le seuil des 40 bits doive rapidement être porté à 56 bits.

ATTENTION

Plusieurs organismes publics ont subi récemment les foudres du SCSSI pour avoir mis à disposition sur leur serveur des logiciels de chiffrement dont la diffusion est strictement interdite (PGP 5.0 notamment). Selon les textes, ils encourent une peine pouvant aller jusqu'à trois ans d'emprisonnement et 500 000 F d'amende si ce moyen a servi à dissimuler la préparation ou la commission d'un crime ou d'un délit. ■ GR

Ces « grandes oreilles » qui espionnent l'Europe

vesti pour déjouer le « réseau Echelon », un système d'écoutes industrielles, financé par les Etats-Unis et la Gra



Article du *Figaro* du 10 avril 1998 paru sous la plume de Christophe Doré.

SÉCURITÉ INFORMATIQUE
numéro 20 juin 1998
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité d'information. Gratuit.
Périodicité : 5 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
ROBERT LONGEON
Centre national de la recherche scientifique
Service du Fonctionnaire de Défense
c/o IDRIS - BP 167. 91403 Orsay Cedex
Tél. 01 69 35 84 87
Courriel : robert.longeon@cnrs-dir.fr
http://www.cnrs.fr:Infosecu

ISSN 1257-8819
Commission paritaire n° 3105 ADEP

Conseil et coordination : CNRS - MIST - Jacqueline Leclère • Conception et réalisation : La Souris 01 45 21 09 61