puis le programme teste des groupes de signes moins naturels ; l'exploration peut durer des mois, voire des années. Cependant Nau est chanceux. Vers 5 heures, le prénom «Nancy» est identifié : le compte administrateur est accessible!

Nau est ravi. Il crée une fenêtre de dialogue entre lui et le système d'exploitation de l'ordinateur, d'où il dispose des mêmes pouvoirs que l'administrateur. Puis il renforce sa position en transférant un programme *Root kit* pour la discrétion et un programme *Sniffer* sur l'ordinateur de sa nouvelle victime : toute saisie et toute connexion seront enregistrées par le programme *Sniffer* dans un fichier dissimulé. Le programme *Root kit* permet également de créer un chemin d'accès supplémentaire que Nau baptise «revanche» ; mot de passe «MoRtSurCf».

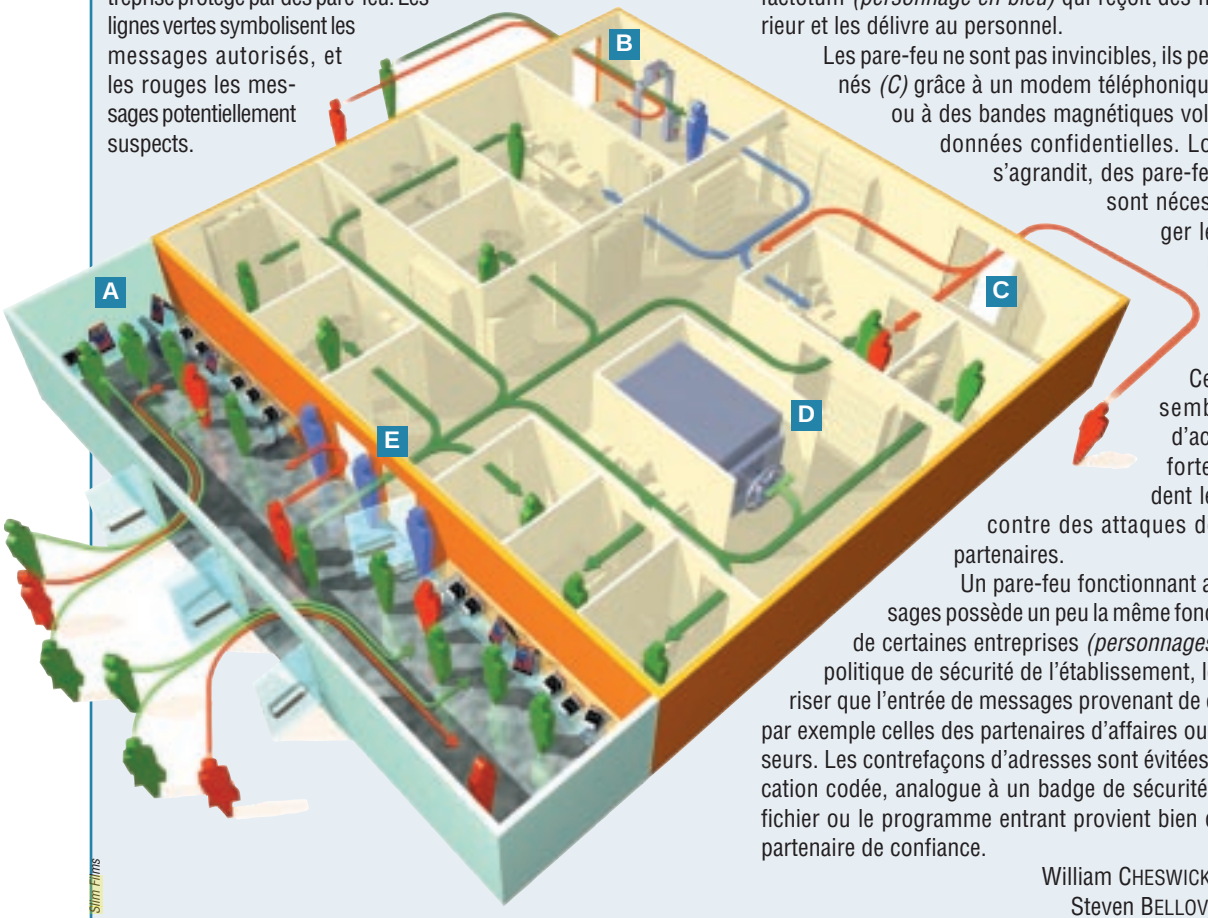
Nau termine sa nuit en déterminant que le compte administrateur auquel il a accédé est connecté sur l'ordinateur picasso du réseau boucanum.fr. Grâce au programme *Root kit*, l'utilisateur normal de l'ordinateur picasso ne remarquera pas que son ordinateur est maintenant commandé par quelqu'un d'autre. Surcouf ne détecte qu'une tentative d'intrusion dans boucanum.fr à partir du réseau Internet. Ce nouvel incident l'inquiète, mais, faute d'informations suffisantes, il ne peut rien faire.

Deux nuits plus tard, Nau se connecte sur l'ordinateur picasso et examine les comptes rendus du programme *Sniffer*. Toutes les informations concernant le trafic interne du réseau sont codées, mais le programme *Sniffer* a enregistré la connexion de quelqu'un, de l'ordinateur picasso sur un autre ordinateur du nom de fantasia.

Les pare-feu

Aucun réseau informatique relié au réseau Internet n'est invulnérable, mais des protections peuvent être installées. La première ligne de défense est le pare-feu, dont les deux types le plus fréquemment utilisés agissent soit au niveau des messages transmis, soit au niveau des logiciels. Le premier fonctionne sur une machine nommée routeur. Il examine dans chaque message entrant ou sortant les adresses de la source et de la destination, qu'il compare à des règles d'accès. Les messages autorisés sont transmis, les autres sont bloqués. Le second examine les adresses et le contenu des messages. Plus lent qu'un filtre de messages, il permet toutefois une politique de sécurité plus raffinée.

L'illustration représente un réseau informatique d'entreprise protégé par des pare-feu. Les lignes vertes symbolisent les messages autorisés, et les rouges les messages potentiellement suspects.



Slim Films

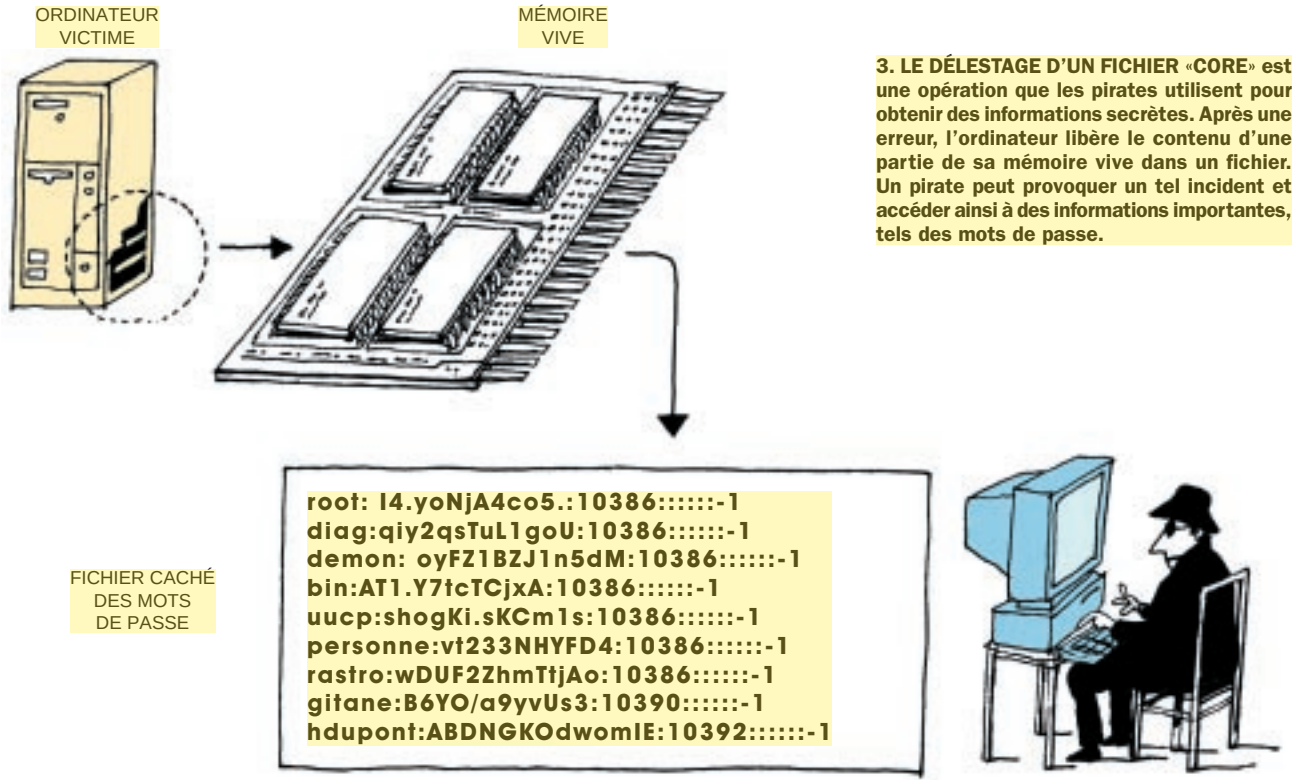
À l'extérieur du pare-feu *(en orange)*, l'entreprise possède un réseau accessible au public, qui permet aux clients d'envoyer des courriers électroniques vers l'entreprise ou de naviguer sur ses différents sites informatiques. Cette zone *(A)* est analogue à l'espace d'accueil réservé au public que l'on trouve à l'entrée de certains établissements : aucune information confidentielle n'y est présente.

Un pare-feu fonctionnant au niveau des logiciels ressemble aux salles de police des aéroports *(B)* : les courriers électroniques sont inspectés. Les programmes reçus par le réseau Internet, qui peuvent contenir des instructions néfastes, sont envoyés sur un serveur mandataire, puis à un programme mandataire qui fonctionne en toute sécurité sur le réseau. Un programme mandataire est l'analogue du factotum *(personnage en bleu)* qui reçoit des messages de l'extérieur et les délivre au personnel.

Les pare-feu ne sont pas invincibles, ils peuvent être contournés *(C)* grâce à un modem téléphonique, à des disquettes ou à des bandes magnétiques volées, contenant des données confidentielles. Lorsque l'entreprise s'agrandit, des pare-feu supplémentaires sont nécessaires pour protéger les systèmes informatiques de services importants, tel celui de la comptabilité. Ces protections ressemblent à la porte d'acier d'une chambre forte *(D)* ; elles défendent les systèmes vitaux contre des attaques de l'intérieur ou de partenaires.

Un pare-feu fonctionnant au niveau des messages possède un peu la même fonction que les gardes de certaines entreprises *(personnages en bleu)*. Selon la politique de sécurité de l'établissement, le filtre peut n'autoriser que l'entrée de messages provenant de certaines adresses, par exemple celles des partenaires d'affaires ou celles des fournisseurs. Les contrefaçons d'adresses sont évitées par une authentification codée, analogue à un badge de sécurité, qui assure que le fichier ou le programme entrant provient bien d'une adresse d'un partenaire de confiance.

William CHESWICK, Laboratoires *Bell*
Steven BELLOVIN, *AT&T Research*



3. LE DÉLESTAGE D'UN FICHIER «CORE» est une opération que les pirates utilisent pour obtenir des informations secrètes. Après une erreur, l'ordinateur libère le contenu d'une partie de sa mémoire vive dans un fichier. Un pirate peut provoquer un tel incident et accéder ainsi à des informations importantes, tels des mots de passe.

Nau passe maintenant à l'abordage d'une nouvelle zone du réseau.

Cet ordinateur fantasia est une station de travail de type SPARC, utilisée pour la création d'animations en images de synthèse, peut-être des génériques pour la télévision. C'est certainement un serveur auquel accèdent de nombreux autres ordinateurs. Nau cherche un fichier de mots de passe. Peut-être en trouvera-t-il certains valables sur d'autres ordinateurs à l'intérieur du réseau de la société.

Il localise ce fichier, mais n'y trouve que des «x» : l'information est probablement dissimulée ailleurs. Peu importe : utilisant le protocole de transfert de fichiers, Nau provoque une erreur qui oblige fantasia à transférer une partie de sa mémoire vive dans le compte que Nau s'est créé. Cette procédure est un «délestage de fichier core» *(voir la figure 3)*, qui permet normalement aux programmeurs de découvrir des indices lors d'une panne de programme. Des mots de passe codés sont parfois stockés dans la mémoire vive. Lors d'une connexion, l'ordinateur code le mot de passe saisi par l'utilisateur et le compare aux mots de passe déjà codés du fichier caché. Lorsque les deux coïncident, la connexion est autorisée. Grâce au délestage, Nau récupère le fichier de mots de passe codés. Il lance son programme de recherche de mots de passe : il va falloir patienter...

Impatient, Nau élabore déjà sa prochaine manœuvre. Avec un système d'exploitation *Unix*, lorsqu'un programme fournit trop de données à un espace de mémoire temporaire, nommé tampon, les informations en excès dépassent la capacité du tampon et s'écoulent dans d'autres zones de la mémoire de l'ordinateur. Nau utilise ces dépassements de capacité *(voir la figure 5)* pour introduire dans la station de travail SPARC un programme grâce auquel il peut exécuter d'autres commandes et d'autres programmes. Ravi de son dernier forfait, Nau installe un autre programme *Sniffer* et un autre *Root kit*. Ce dernier ne masquera son œuvre qu'une fois activé ; le forban efface donc les traces de ses premières activités.

Une dernière chose à faire encore. Quelqu'un est-il autorisé à se connecter sur fantasia à partir du réseau Internet? D'une simple commande qui affiche l'enregistrement de toutes les connexions sur fantasia, Nau constate que des utilisateurs prénommés nancy et vangogh sont récemment entrés sur fantasia par le réseau à partir du site pemmican.fr, qui se situe en dehors du pare-feu de la Société *Boucaniers*. Au matin, Nau s'effondre, terrassé par le sommeil, mais satisfait : bientôt, il vaincra la Société *Boucaniers*.

La mise à mort

Le lendemain soir, Nau se présente sous une fausse adresse informatique chez pemmican.fr. Puis, en testant des signaux de synchronisation sur pemmican.fr, il détermine la valeur de temporisation qu'utilise pemmican.fr et falsifie sa propre origine. Il installe alors un programme *Sniffer* sur pemmican.fr et un interpréteur sécurisé pour se connecter en toute sécurité sur fantasia. Une commande lui fournit la liste des connexions actives à l'intérieur du réseau de la Société *Boucaniers*, où il découvre un nouvel ordinateur : «admin.boucanier.fr». L'ordinateur de Surcouf?

Parallèlement, Nau essaie chaque nouveau mot de passe et le nom d'utilisateur associé, découverts par son programme de recherche sur les ordinateurs du site boucanier.fr. Hélas, aucun ne fonctionne ailleurs que sur fantasia, qu'il a déjà conquis.

Cependant, cette déconvenue est largement compensée par fantasia, qui lui fournit l'enregistrement de ce qu'a tapé l'utilisateur vangogh lorsqu'il a mis à jour la page Internet de la société. Nau y trouve le mot de passe nécessaire au piratage de la page Internet de la Société *Boucaniers*. Par ailleurs, son programme *Sniffer* installé sur l'ordinateur picasso lui indique qu'une certaine Nancy a utilisé cet ordinateur pour se connecter par une porte dérobée sur le compte administrateur d'admin.boucanier.fr, dissimulée derrière un programme *Root kit*.

Il se glisse juste derrière elle et essaie de se connecter sur tous les ordinateurs de boucanier.fr. Hélas, Surcouf a été prudent : sur le réseau boucanier.fr, même les pouvoirs d'administrateur n'autorisent pas l'accès à d'autres ordinateurs sans nouveaux mots de passe. Nau est bloqué. Il retourne à l'assaut du site Internet. De son propre ordinateur, il installe une nouvelle version du site spécialement préparée.

La quarantaine de Java

Le langage Java est utilisé par les programmeurs pour écrire de petits programmes, ou appliquettes, qui peuvent être récupérés sur le réseau Internet ou sur d'autres réseaux d'ordinateurs. Un individu peut toutefois créer une appliquette malveillante qui efface des fichiers, vole des données ou injecte un virus. Cependant, le langage Java a prévu une sécurité : il s'agit d'un ensemble de logiciels, nommé machine virtuelle Java, indispensable à l'exécution de n'importe quelle appliquette.

Lorsqu'un utilisateur récupère une appliquette *(A)*, par exemple un programme de gestion bancaire, la machine virtuelle empêche l'accès au disque dur, au réseau et à d'autres ressources vitales. L'appliquette se trouve alors en une sorte de quarantaine, d'où elle ne peut provoquer aucun dommage. L'appliquette n'est libérée que lorsque la machine virtuelle a vérifié qu'elle provenait d'une source de confiance.

En premier lieu, un vérificateur de code détermine si l'appliquette est écrite dans une syntaxe Java correcte *(B)*. Quand ce n'est pas le cas, le programme ne pourra pas être utilisé. Ensuite, la machine virtuelle recherche une signature numérique, associée à l'appliquette qui identifie la personne ou l'organisme créateur et révèle toute altération. En cas de signature invérifiable, l'appliquette restera en quarantaine. Le programme fonctionnera, mais ne pourra ni lire ni écrire des fichiers sur le disque dur.

Lorsque la signature de l'appliquette est reconnue *(C)*, la machine virtuelle détermine quel type d'accès donner au programme : lecture de n'importe quel fichier du disque dur ou restrictions à certaines zones.

James GOSLING, *Sun Microsystems*