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

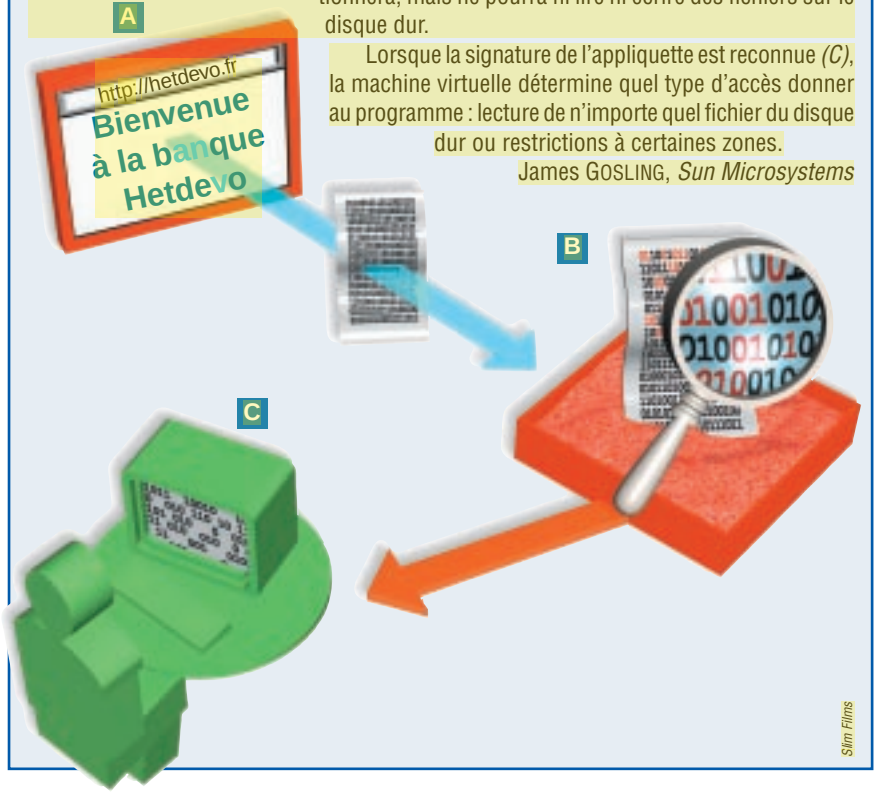
Le langage Java est utilisé par les programmeurs pour écrire de petits programmes, ou appliquettes, qui peuvent être récupérés sur le réseau Internet ou sur d'autres réseaux d'ordinateurs. Un individu peut toutefois créer une appliquette malveillante qui efface des fichiers, vole des données ou injecte 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*



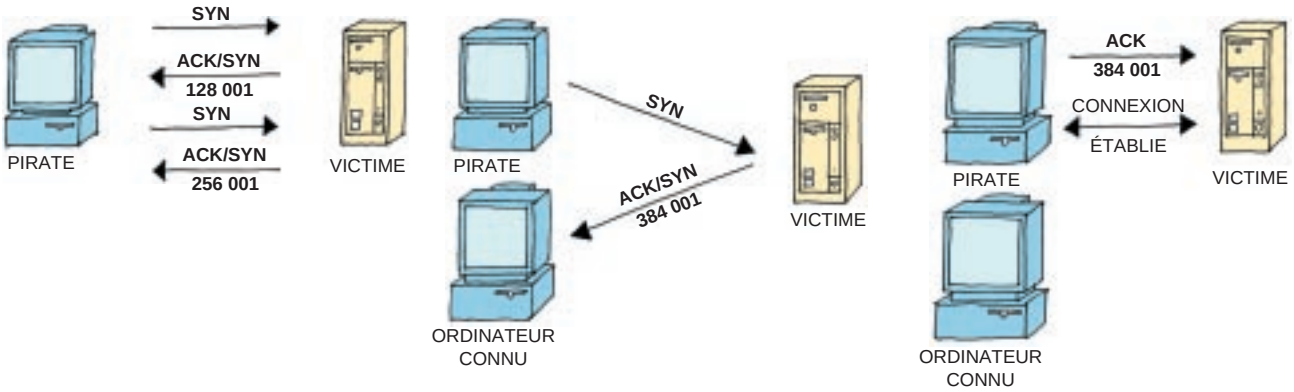
Aujourd'hui, Surcouf travaille tard, il étudie les comptes rendus où apparaît un nombre inhabituel de connexions par le système commercial. Que s'est-il passé ? L'aide de l'administratrice du système de pemmican.fr, une collègue qui lui est redevable, l'aidera sûrement.

La sonnerie du téléphone retient Surcouf au moment de partir. Un client se plaint de la séquence pornographique affichée sur le site Internet de la Société *Boucaniers*. Après vérification, Surcouf débranche rapidement le câble Ethernet, le cordon ombilical qui relie la société au réseau Internet.

Nau enrage de voir son chef-d'œuvre d'obscénité détruit aussi vite. Il s'inquiète également d'avoir laissé autant de traces derrière lui : il se connecte par modem sur l'ordinateur picasso – un accès qu'ignore Surcouf – et reformate complètement le disque dur de l'ordinateur d'administration du système. Le système de la société est hors service. Surcouf ne rassemblera aucun indice. Surcouf redémarre rapidement l'ordinateur d'administration, mais c'est trop tard : il devra complètement réinstaller les logiciels. Cependant, Nau ignore qu'un programme de détection *Etherpeek*, installé sur un des ordinateurs du réseau, a enregistré ses activités...

Nau est irrité : il noie boucanier.fr sous un flot de données. Peu après, Surcouf reçoit la plainte d'une représentante de la société qui n'arrive pas à se connecter sur le serveur de courrier électronique.

Le lendemain, Surcouf, exténué, demande au directeur technique de la Société *Boucaniers* l'autorisation de nettoyer complètement tous les ordinateurs du réseau et de changer les mots de passe. Cependant, une telle mesure, bien que prudente, nécessiterait l'arrêt du système pour plusieurs jours. Le directeur refuse.



4. UNE ESCROQUERIE INTERNET permet au pirate de falsifier son identité. Il teste d'abord sa victime en lui envoyant de multiples signaux de synchronisation (SYN) pour obtenir, en réponse, un double signal d'accord et de synchronisation (ACK/SYN), et une valeur de temporisation *(à gauche)* caractéristique d'un système d'exploitation. Cette valeur augmente ici de 128 000 à chaque échange. Le pirate envoie ensuite de nombreux signaux de synchronisation dont un est identique à celui d'un ordinateur connu de la victime, qui transmet alors un double signal d'accord et de synchronisation à cet ordinateur autorisé *(au centre)*. Le pirate ne reçoit pas cette réponse, mais poursuit la correspondance. Il délivre un signal d'accord avec la valeur de temporisation correcte : la communication entre son ordinateur et sa victime est établie *(à droite)*. Le piratage commence

5. LE DÉPASSEMENT DE CAPACITÉ D'UN TAMPON est une faiblesse de certains programmes, par exemple ceux écrits en langage de programmation C et qui fonctionnent sur un système d'exploitation comme Unix. Le pirate exécute un programme en C sur l'ordinateur victime *(a)*. Le programme stocke tout d'abord des données dans un espace de stockage temporaire, nommé tampon *(b)*, puis souhaiterait déplacer des données de l'emplacement 1 vers le 2 et vers le 3 *(c)*. Cependant, le pirate oblige le programme à accepter des données en excès : certaines informations s'infiltrent directement dans l'emplacement 4 *(d)*. Le pirate en profite pour installer son propre code *(e)* et bénéficie ainsi des possibilités étendues de l'ordinateur de sa victime.