Date: Mercredi 20 octobre 2004 à 19:29:35
Sujet: 3 Sécurité et Hacking

Kevin Mitnik, le plus grand des HACKERS

L'histore de Kevin Mitnik, un des grands hackers de l'histoire.

C'était le meilleur hacker du monde, il se faisait appeler le CONDOR et il a joué un grand role dans l'histoire du hacking. Kevin Mitnick est une légende dans l'univers du Net et surtout de la securité informatique. Il a fait toutes sortes de piratages. D'abord, adolescent, il aurait détourné le service des renseignements téléphoniques américain basé sur le même principe que notre 12 National. Quand un abonné appelait pour s'informer sur un numéro de téléphone, il tombait sur Mitnick ou sur un de ses complices qui répliquait : "La personne que vous recherchez est-elle blanche ou noire, Monsieur ? Car nous tenons deux répertoires distincts." On lui attribue aussi l'une des premières passes à l'encontre du Pentagone, il y retournera par la suite une bonne centaine de fois. L'un des jeux du CONDOR était aussi de se balader dans les systèmes téléphoniques américains pour y déconnecter le téléphone de ses ennemis ou pour "simplement" changer leur nom d'abonné en James Bond. Lors de sa cavale, il s'est attribué des numéros de téléphone, un bon millier, dont les trois derniers chiffres finissaient par 007. Pour finir dans ce qui est connu, Mitnick aurait déjoué les barrières du laboratoire de mise à feu de la NASA à Pasadena ; du réseau de l'Université de Leeds en Angleterre ; de l'unité centrale de la défense aérienne américaine, dans le Colorado et surtout le système de localisation d'appels du FBI. Et c'est ici que la traque commence, le Fédéral Bureau of Investigation n'a pas apprécié d'être visité de la sorte. Pour vous donner une idée, un visiteur qui accède dans un immeuble du FBI, est fouillé, aucun document ne peut ni rentrer, ni sortir, même pas un rouleau de papier toilette, alors imaginez un mec qui se promène dans toutes les machines et diffuse en libre accès les documents qu'il a piqué. Cette cavale durait depuis trois ans, jusqu'à ce jour de décembre 1994, ou, par défit, il s'attaqua aux ordinateurs de Tsutomu Shimomura. Le CONDOR souhaitai faire un tour à cet ancien ami passé à l'ennemi.

Tsutomu Shimomura est un autre grand Hacker de l'histoire. Mais cet américain de 30 ans est passé du coté de la securité informatique comme le font beaucoup d'autres Hacker. Il a développé toute une gamme d'outils capables de détourner les systèmes téléphoniques cellulaires, mais aussi toute une série de programmes permettant de piéger à coup sur n'importe quel pirate. Il s'est taillé une excellente réputation. Le FBI, l'Us Air Force ou encore l'Agence de Sécurité Nationale, le NSA, font partie de ses clients.

Plus le système est protégé plus on s'amuse. Alors jouons...

Le 26 décembre, Shimomura est chez lui, il se prépare à partir en vacances, quand il reçoit un appel de ses collègues du Centre de calcul de San Diego. Quelqu'un s'est introduit la nuit

précédente dans les ordinateurs installés dans sa maison de vacances, à Del Mar, et a "volé" des centaines de documents et de logiciels. Le hacker a exploité une faille notoire dans l'architecture du réseau Internet, faisant croire à l'ordinateur de Tsutomu Shimomura que le message venait d'une source autorisée - en l'occurrence, un ordinateur de la Loyola University de Chicago utilisé comme "passerelle". Habile, certes, mais le pirate ne s'est toutefois pas aperçu que Shimomura a programmé des firewalls d'un genre particulier, ces derniers envoient toutes les heures une copie de leur index à un autre ordinateur - ce qui a produit une alerte automatique. Un mois plus tard, Shimomura reçoit un deuxième coup de fil. L'opérateur d'un service commercial d'accès à Internet, le W.e.l.l. ("Whole Earth Lectronic Link") de Sausalito, l'informe que les documents volés à Del Mar ont été déposés dans son ordinateur par un inconnu. Dans ces documents, entre autres, les feuilles de salaires de Shimamoura, des contrats et surtout tous ses mots de passe.

Tsutomu Shimomura et une petite équipe du Centre de calcul s'installent alors à Sausalito, branchent une série de portables sur le réseau interne du W.e.l.l., mettent en place un système de surveillance, et commencent à observer l'activité du pirate - Dorénavant chaque frappes de ce dernier s'affichent sur leurs écrans. Le 17 janvier, ils l'observent alors qu'il infiltre le système de Motorola, il accède à l'ordinateur censé protéger le réseau interne et dérobe, le logiciel de sécurité. Il semblerait, mais personne ne pourra le prouver, que c'est à partir de cette passe, que le FBI aura accès au décryptage des communications entre mobiles.

Quelques jours plus tard, Tsutomu et ses associés détectent le vol de 20 000 numéros de cartes de crédit appartenant aux clients de Netcom, un des principaux fournisseurs d'accès à Internet, basé à San José. Ils s'y déplacent et recommencent la traque. Mitnick, connaît son affaire, ses appels passent par trois villes : Denver, Minneapolis, et Raleigh. Ce n'est qu'en comparant longuement les registres des compagnies téléphoniques à ceux de Netcom que Shimomura et ses collègues acquièrent la conviction que le pirate se trouve à Raleigh. Le hacker utilise un téléphone cellulaire pour se connecter à plusieurs points d'accès de Netcom afin d'éviter d'être localisé.

A Raleigh, les appels semblent entrer par un central de la compagnie téléphonique GTE, dont les listings en renvoient toutefois l'origine chez une autre compagnie : SPRINT. Grâce à une brillante manipulation des logiciels du réseau, GTE pensait que les appels venaient de Sprint, et vice versa. Aucune des deux compagnies n'avaient donc de données sur l'utilisateur du téléphone - ni ne lui a jamais envoyé de facture d'ailleurs ! Le numéro identifié, pendant deux jours Shimomura parcours les rues de Raleigh avec une antenne de détection, et localise enfin l'appartement où habite Kevin Mitnick. Selon d'autre dire, c'est ici qu'apparaît l'une des premières utilisations du système TEMPEST. A deux heures du matin, le 15 février 1995, le FBI et Shimomura investissent le nid du

Condor. "Salut Tsutomu ! Félicitations", aurait dit MITNICK. Ceux qui l'ont rencontré ou ont étudié ses agissements le décrivent comme un jeune homme d'une intelligence limitée, spécialisée, très réservé et méfiant. Un perdant doué d'un talent extraordinaire sur ordinateur, le seul endroit où il excellait. Les gens avaient peur de lui, comme d'un magicien un peu fou. Non sans raison : les talents techniques de Mitnick avaient de quoi faire trembler la planète. Mais jamais il n'a essayé de tirer un profit de ce qu'il savait, ni effacé ou altéré les mémoires informatiques qu'il parvenait à percer. Il n'a d'ailleurs jamais utilisé les numéros de cartes de crédit qu'il ait eu en sa possession. Il faisait ça pour la beauté du geste, pour défier ceux qui sont en charge de la sécurité informatique.
"Kevin se moquait des grosses entreprises comme du FBI, et c'est pour ça qu'il a fini par représenter une menace" : a déclaré son ex-femme. " Il leur a prouvé qu'ils étaient vulnérables, et eux ne voulaient surtout pas que ça se sache." Le Condor en cage, le doute plane toujours...

Kevin Mitnick a écopé d'une peine de trente-cinq ans de prison. Il ne peut téléphoner qu'à son avocat, sa mère et sa grand-mère. Pourquoi une telle méfiance ? On craint qu'il amorce un virus, en appelant un autre numéro quelque part dans le monde. Un numéro qui enclencherait une bombe informatique pré-programmée.

En décembre 1997, les amis du Condor, le groupe Pants/Hagis ont menacé les systèmes informatiques de la planète d'une infection virale de leur cru. Ils demandaient la libération du hacker emprisonné à Los Angeles. Le message d'avertissement est apparu très brièvement sur le moteur de recherche Yahoo, ainsi que quelques semaines plus tard, sur le site de l'Unicef, de l'Unesco, du F.B.I. et de l'U.S. air force.