Cybercriminalité: de l'artisanat à l'art de la guerre

La cybercriminalité a connu un virage stratégique en 2004 avec des méthodes de vol, de racket et de chantage de plus en plus élaborées et efficaces. C'est la conclusion du panorama de la cybercriminalité 2004 dressé par le Clusif (Club de la sécurité des systèmes d'information français).

Le Club dégage deux tendances majeures: la volonté d'enrichissement, notamment à travers les spywares, les robots et les rackets, la destabilisation économique à travers la multiplication des vols de données et codes sources et les attaques concurrentielles. Aujourd'hui, les cyber-escrocs n'utilisent plus de méthodes artisanales pour entourlouper les internautes particuliers. Ils sont désormais devenus de véritables professionnels s'attaquant aux grandes entreprises grâce à des outils de plus en plus efficaces. Le moteur reste néanmoins toujours le même: l'appât du gain. Le Clusif a donc identifié deux méthodes de racket sur Internet: le vol de données et le chantage. L'année 2004 s'est en effet illustrée par trois affaires majeures de vol de données rappelle le Clusif. En février, Microsoft annonçait le vol de 13,5 millions de lignes de code de Windows 2000 et NT4, et sa mise à disposition sur les réseaux. Ce vol a remis en question toutes les procédures de sécurité qui entourent la protection des codes sources des produits de la firme, des joyaux inestimables pour Microsoft. C'est tout un système, fort complexe, qu'il a fallu revoir. Vol du code de Windows: enquête et inquiétude Vol du code Windows: première faille mise à jour Vol du code Windows: Microsoft menace pour limiter l'hémorragie USA : arrêté pour avoir vendu du code source Windows En mai 2004, c'est une partie du code source de l'IOS de Cisco qui se retrouve dans la nature. Le code source partiellement dérobé concerne la version 12.3 d'IOS, le système d'exploitation qui équipe les gros routeurs de la gamme 7000 de Cisco ou encore les commutateurs Catalyst 6000. La version volée daterait de 1996. Une partie du code source Cisco IOS aurait été volé Vol du code IOS: Cisco prend la menace au sérieux Cisco minimise le vol de son code source IOS Du code Cisco pirate en vente sur le Net: la filière Ukraine? Enfin, en novembre, c'est la banque américaine Wells Fargo qui se faisait dérober des données clients. Un de leur sous-traitant avait été délesté de trois portables et d'une station de travail. Ces PC contiendraient les noms, adresses, numéros de prêts et cartes de sécurité sociales de centaines de clients. Vols répétés chez Cisco Systems & Wells Fargo Dans toutes ces affaires, on s'aperçoit que les données sont la plupart du temps dérobées par des mafias qui les revendent ensuite en ligne ou aux plus offrants selon les cas. Mais le vol de données n'est qu'une arme parmi d'autres. Les cyberescrocs utilisent désormais de plus en plus le chantage et le racket. En clair, ils menacent les entreprises de paralyser leurs système d'information en ligne si elles ne payent pas de rançons. Les exemples sont déjà nombreux: Softbank s'est vu réclamer 28 millions de dollars contre la non divulgation de données personnelles de 4,5 millions de clients. Google a été menacé de paralysie s'il ne payait pas 100.000 dollars etc... Pire, ces maîtres-chanteurs s'attaquent aussi aux employés comme les secrétaires en exigeant des petites sommes que ces salariés préfèrent payer plutôt que d'avertir leurs directions. Il faut dire que ces escrocs ont les moyens de leurs ambitions. Les outils d'attaque sont désormais connus, faciles à utiliser et largement disponibles sur la Toile, souligne le Clusif. Pour paralyser un site il suffit de le bombarder de requêtes. Ces attaques par deni de service distribué (DDoS) sont générées par des armées de PC infectés (machines zombies) par des virus ou des chevaux de Trois programmés pour « faire

tomber » un site. Ces réseaux de robots (botnet) se développent à très grande vitesse. Un réseau russe de pirates/maître chanteurs démantelé Des entreprises soumises au chantage du spam Il y a donc de quoi être inquiet car ces phénomènes devraient encore prendre de l'ampleur. Une seule solution pour se protéger selon le Clusif: limiter l'information mise en ligne. Soit un sacré retour en arrière!