

CYBERCRIMINALITE

Des recettes qui battent les revenus de la criminalité classique

"Les recettes de la cybercriminalité ont atteint les 200 milliards de dollars en 2006. Sachant que ce cumul d'argent sale était de l'ordre de 16 milliards de dollars en 2002, le chiffre a été multiplié par 12,5 en 4 ans. A partir de 2002, elles sont devenues supérieures aux revenus de la criminalité classique sous toutes ses formes y compris le trafic de drogue", c'est ce qu'a précisé Rachid Bencheraiet du service-conseil en sécurité chargé de la gouvernance et la gestion des risques dans le groupe LGS inc.IBM, dans une conférence intitulée "les nouveaux visages de la cybercriminalité", tenue jeudi dernier au centre culturel français de Constantine. Il constatera également que même le nombre des crimes classiques a dû fléchir devant le fléau de la cybercriminalité.

Le conférencier a défini la cybercriminalité comme étant le non-respect ou la violation des lois moyennant des outils informatiques. Il classe les pirates du net en dix catégories à commencer par les script-kiddies ou newbies (les enfants scripteurs) qui sont des initiés de la cybernétique motivés par leur ego et emmenés par la maîtrise de la pointe informatique. Ils représentent la catégorie la moins dangereuse. Les hackers sont réputés également comme les chevaliers de la toile. Ces chapeaux blancs se

prennent pour des connaisseurs des systèmes de protection et peuvent détruire n'importe quelle structure d'exploitation. Les collaborateurs indelicats sont les plus méchants dans la mesure où ils monnayent leur collaboration au profit de ceux qui ont besoin de renseignements relevant des secrets de leurs employeurs. Ils peuvent être des employés ou consultants à l'intérieur d'une entreprise. Ils sont les plus nombreux avec 80 % des flibustiers. La team est une équipe ou une secte constituée de pirates paranoïaques. Leur objectif est de mettre le désordre pour le simple plaisir. Ces groupes commencent, indique le communicant, à se déployer de manière vertigineuse en Algérie. Soldiers de fortune (les soldats du profit) sont des mercenaires dont le seul souci reste l'argent et restent les plus activistes. Leurs besoins les poussent même à travailler pour les intérêts politiques de certains Etats délinquants. L'exemple des Marocains qui ont attaqué un réseau d'institutions bancaires d'Israël est bel et bien révélateur. Le crime international organisé qui est structuré sur Internet par la mafia du web est motivé par la collecte d'un maximum d'argent via des sites pornographiques. Donc, son cheval de bataille est la traite des blanches. Les entreprises qui s'attaquent aux intérêts des concurrents recrutent

des pirates à cet effet, enfin, les structures paraétatiques, les Etats et les structures professionnelles.

Les USA sont les plus délinquants

Les Etats-Unis d'Amérique sont le pays le plus délinquant. Les Américains sont en effet derrière le scandale de l'année 2006. Sous prétexte de la lutte antiterroriste, et sur une réquisition administrative sans l'aval d'un juge, les instances fédérales américaines ont violé le réseau Swift, une coopérative interbancaire internationale qui contrôle les transactions bancaires et les transferts d'argent estimés à 6000 milliards USD par jour dans 7800 établissements implantés à travers 200 pays dans le monde. L'alibi était de traquer "terrorist finance tracking programme" (la trajectoire du financement du terrorisme). La demande paraissait légitime. Est-ce qu'il y a des comptes qui servent les réseaux terroristes ? Cependant, l'objectif réel est de savoir qui fait quoi à travers le monde ? Certains Etats comme la France et la Belgique ont demandé la levée de cette réquisition, mais... en vain !

"Seuls les moyens ont été adaptés aux NTIC"

L'ingénieur Bencheraiet qui a fait une parabole entre les formes de la criminalité classique et la cybercriminalité a conclu que même si cette dernière a développé d'autres visages et pris d'autres proportions, seuls les moyens ont été adaptés aux nouvelles technologies de l'information et de la communication et cette cybercriminalité calque exactement le crime classique. Primo, les racketteurs de la toile se proposent pour protéger des systèmes informatiques d'entreprises sous la menace de détruire ces structures qui craignent de voir leur image de marque entachée. Comme c'est le cas dans le racket classique opéré par des gangs dans les villes américaines, italiennes ou russes, "tu me donnes tant et je te laisse tranquille", a simulé le conférencier.

Secundo, l'extorsion en ligne moyennant la diffusion d'images pornographiques et de secrets qui mettent en péril les intérêts des victimes de ces prédateurs des temps modernes. Le chantage exercé sur des sites commerciaux dont les pertes causées par des pirates sur les ventes en ligne peut être préjudiciable sur le plan comptable de ces sites. Ils préfèrent payer et ça marche pour ces criminels. Ce sont de véritables masters qui comme les dealers qui rabattent des enfants pour qu'ils travaillent pour eux. Moyennant des ordinateurs mal protégés, ils s'attaquent aux institutions sans que ces internautes exploités le sachent. L'ingénierie sociale consiste en le vol par des imposteurs d'identités par le biais d'une communication tous azimuts sur la toile pour soutirer des informations à des victimes potentielles, leurs identités, numéros de comptes bancaires et autres mots de passe utiles pour les exploiter à leur profit. Autrement dit, ils se procurent de fausses identités volées à des personnes "crédules" en donnant l'apparence officielle à leurs emails, une banque ou un représentant d'une marque commerciale pour lui soutirer de l'argent. Le vol de cartes de crédit n'est pas le vol classique de la carte physique. Ces voleurs attaquent les bases de données des sites commerciaux et s'approprient des codes de ces cartes pour transférer l'argent. Les faux courtiers en bourse qui proposent des actions n'ont aucune valeur mise à la vente en ligne.

Les motivations de ces flibustiers du net s'articulent, selon M.Bencheraiet, autour de trois points essentiels qui se rejoignent, l'argent, la connaissance et l'ego en l'occurrence. Il y a beaucoup d'argent sur Internet, ce qui ne laisse personne indifférent et bien évidemment les criminels. Ceux, menés par leur ego veulent flatter le rideau et exprimer leur maîtrise des technologies de l'information et de la communication. Enfin, la recherche de la connaissance est l'apanage des hackers. "Je

connais le système et je peux le détruire", c'est ce qui motive le plus ces pirates.

Il est à signaler que l'évolution de l'impact de la cybercriminalité a évolué très rapidement depuis l'année 2000. Selon le schéma exposés par M.Bencheraiet, illustrant les étapes de la maturation de la menace en fonction de son impact, elle a évolué à de simples scénarios montés par des scripteurs avec des outils informatiques pour le plaisir, à des actions visant la dégradation de sites Web en 2002, en passant à un stade de pratiques méchantes en 2004 pour se structurer en criminalité au sens propre du mot en 2006. Le pactole engrangé par les réseaux de la cybercriminalité durant cette année indique à bien des égards son ampleur.

Le conférencier s'est étalé dans sa communication sur des exemples de nouvelles images de la cybercriminalité. Il a parlé du phénomène du "Spam nigérian" qui est une nouvelle forme d'escroquerie. Il a émergé l'année dernière au Nigeria et commence à prendre des proportions alarmantes dans le monde entier. Les pirates diffusent des lettres sur le net en disant qu'elles ont hérité d'une fortune estimée à des millions de dollars qui est dissimulée dans un coffre chez une structure de consigne privée. Et qu'ils sont à la recherche de l'aide pour sortir de leur pays d'origine proposant un pourcentage de la cagnotte. La cause étant des contraintes politiques ou autres. Ces pirates exigent de leurs victimes potentielles de l'argent pour accomplir certaines procédures administratives avant de l'inviter à aller dans ce pays pour le même motif. "Ça peut être rigolo, mais ça marche !" affirme le conférencier en indiquant que ces histoires finissent le plus souvent par la mort de la victime car une fois elle atteint l'adresse de ce présumé héritier, il la délèste de tous ses objets de valeur et la tue. Il a raconté l'histoire d'une femme canadienne qui s'est dirigée vers sa banque pour l'accomplisse-

ment du transfert. Ensuite, la banque a pris le relais dans les négociations bien sûr à la charge de cette femme qui a tout perdu à la fin. Le pirate a exigé au milieu de la procédure 15 000 dollars, transférés par la banque à son propre compte. Il a évoqué aussi "les Botnets", là où il y a, selon lui, énormément d'argent et où les pirates envoient des chevaux troyens des plus furtifs, et donc, difficiles à détecter. Et de faire allusion à la menace dite "OD" que ceux qui veillent à la gestion des risques dans les entreprises ne peuvent en aucun cas la détecter. Ils soupçonnent l'existence sans pour autant savoir si elle existe réellement.

Un avenir des plus certains

Le communicant a avoué que l'avenir offre des perspectives plus favorables à la cybercriminalité. C'est un éldorado qui échappe à tout contrôle de par l'absence de législation commune et adaptée aux NTIC dans le monde, l'absence du comportement sécuritaire dont le crime a toujours un pas en avant sur la protection et également la méconnaissance des méandres d'Internet. Un avenir qui sera, d'après ses dires, axé sur trois choses qui sont la mobilité, étant un marché florissant avec 2 milliards d'utilisateurs en 2005 et qui peuvent atteindre les 3 milliards en 2010, avec les services qu'elle propose comme les MMS, le Bluetooth et les modems Wi-Fi dans la mesure où tout manager organisé synchronise certainement son téléphone cellulaire avec son ordinateur ce qui oppose son entreprise à toutes les infections possibles. La RFID (Radio Frequency Identification) est l'intégration des tags dans les passeports à identification biométrique et aussi leur substitution aux codes des marchandises. Ces étiquettes magnétiques permettent la localisation de tout ce qui bouge et n'offrent aucune garantie de sécurité pour les usagers. Et de surcroît ouvrent la porte à toute manipulation.

Lyas Hallas

SUR DECISION
DU WALI D'ALGERLes salles des fêtes
vont être fermées

La wilaya d'Alger a sommé les gérants de salles des fêtes installées dans les communes relevant des 13 circonscriptions administratives de la wilaya d'arrêter leurs activités. Les décisions de fermeture ont été signifiées il y a quelques jours et des scellés ont été apposés dans la majorité des salles pour non-conformité des locaux et l'absence de documents autorisant l'activité.

Pour protester contre ces décisions jugées "arbitraires", les gérants de salles des fêtes, organisés en association sous l'égide de l'Union générale des commerçants et artisans algériens, se sont regroupés hier au siège de l'UGCAA. Les présents ont fait part de leur mécontentement quant à cette situation en déplorant la décision de la wilaya par le biais d'une correspondance qu'ils ont adressée au chef du gouvernement. Ils exigent l'annulation des décisions de fermeture ainsi que la révision du décret exécutif 207-05 du 04 juin 2006. Les arguments cités dans les décisions de fermeture ont été rejetés par l'ensemble des gérants présents lors de ce regroupement qui crient à l'arbitraire et qui considèrent, surtout, que l'administration a outrepassé ses prérogatives. Ils estiment aussi que cette mesure pénalise et les propriétaires qu'elle met au chômage et les clients, c'est-à-dire les familles qui ont pris des réservations aux fins d'organiser leurs fêtes (mariages, circonscriptions, fiançailles). En plus, pour avoir la conformité exigée, il faudrait se diriger vers la Direction de l'urbanisme de la wilaya qui refuse selon les concernés la délivrance de cette attestation.

I. T.

BEJAIA

Un énorme cachalot s'échoue près de Boulimat

Un cachalot d'une quinzaine de mètres a échoué, vendredi dernier, au lieu-dit Aach El Vas, à quelques centaines de mètres de la coquette plage de Boulimat, située sur la côte-ouest du littoral de Béjaïa.

Le cétacé, vraisemblablement désorienté par les courants, a été retrouvé par les citoyens, rejeté par la mer et emprisonné dans un amas de rochers.

Au moment où nous mettons sous presse, aucune opération d'évacuation de cette énorme espèce marine n'a été engagée soit par les autorités municipales, soit par la Protection civile.

"Nous n'avons aucun moyen pour faire dégager cet animal de cet endroit, c'est à l'APC de le prendre en charge. Il faut de gros engins pour l'extraire de ces rochers", nous dira un responsable

de la Protection civile de la wilaya de Béjaïa, interrogé à cet effet. Il est à noter que si les autorités locales n'arrivent pas à prendre de mesures ou à extraire le corps de ce cachalot, ce paradisiaque site touristique de la région peut provoquer une impitoyable pollution qui risque de faire des victimes.

Kamel Gaci