La cybercriminalité

La criminalité se développe aujourd'hui sur un terrain moins risqué et plus fertile que celui du monde réel car l'anonymat y est pratiquement assuré pour qui sait s'y prendre et le dispositif policier s'il n'est pas inexistant est très insuffisant pour surveiller le milliard d'individus qui se retrouvent sur le net. Pourtant cet espace virtuel est devenu aussi indispensable à l'économie des entreprises et aux relations entre le citoyen et son administration que le téléphone et le courrier papier.

Le monde devient instable et dangereux. Les échanges se mondialisent et ne connaissent, sur la toile, pas de frontières. Dans ce monde virtuel où tout est à craindre, les amis de nos amis peuvent être nos pires ennemis et les clients de nos partenaires peuvent être nos concurrents. La montée du terrorisme et une situation économique très perturbée engendrent un impérieux besoin de sécurité.

Connaître les menaces qui pèsent sur les systèmes d'information, comprendre les mesures de sécurité à mettre en place et déjà un premier pas est franchi vers un monde Internet plus sûr, un monde où l'économie et la culture pourront se développer harmonieusement, malgré les pièges et les coups de boutoirs des hackers qui foisonnent sur la toile.

Les vulnérabilités

Prenons comme exemple parmi tant d'autres, une vulnérabilité qui a fait beaucoup parler d'elle dans les milieux des bases de données. Cette vulnérabilité pourtant connue, et pour laquelle il existait un correctif depuis six mois, qui affectait les serveurs MS SQL a été exploitée par le ver Slammer, à partir du 25 janvier 2004.

Moins de dix minutes après la première injection de ce ver quelque part sur le net, plusieurs dizaines de milliers de serveurs MS SQL ont été contaminés autour de la planète entraînant un sérieux ralentissement des transactions sur la toile.

Cet événement est intéressant à plus d'un titre. Outre la vitesse fulgurante de propagation de ce ver, on a remarqué que le correctif de l'éditeur qui corrigeait cette faille connue n'avait pas été implémenté sur la plupart des serveurs MS SQL. Si la faille était connue par les experts en base de données, elle l'était aussi par les hackers et ceux-ci ne sont donc pas restés bien longtemps inactifs.

Des logiciels plus vulnérables qu'avant ?

Tout logiciel peut présenter des vulnérabilités qui sont autant de portes ouvertes dans la sécurité des systèmes d'information et par lesquelles les hackers vont s'engouffrer. Un logiciel est une oeuvre souvent très complexe et ses auteurs ne sont pas à l'abri de commettre des erreurs au cours du développement et de la maintenance du produit.

Les CERT sont des organismes à qui vous pouvez vous adresser pour décrire des vulnérabilités trouvées et des attaques subies. Les CERT répertoriaient quelques dizaines de vulnérabilités il y a dix ans et en signalent plusieurs milliers aujourd'hui.

Les logiciels sont-ils alors aujourd'hui plus sujets aux vulnérabilités qu'il y a dix ans ? Non, mais malgré tous les efforts méritoires fournis par les entreprises pour former leurs développeurs à écrire du code sans failles, comme le nombre d'instructions qui composent les logiciels, même en langage évolué, ne cesse de croître, la complexité suit. La probabilité de trouver des erreurs augmente également.

Le cycle de vie d'une vulnérabilité

Une vulnérabilité ne reste pas méconnue bien longtemps. Le nombre de sites attaqués, suite à une vulnérabilité trouvée dans un logiciel présente un cycle de vie particulier.

Au début peu de sites sont concernés par les attaques car peu de monde a entendu parler de la vulnérabilité. Après quelques jours, parfois quelques heures, suite à la publicité faite sur le trou de sécurité trouvé, le nombre de sites touchés par des attaques croit brusquement pour se stabiliser quand le correctif est disponible. Mais le nombre de sites attaqués ne tombe pas à zéro car le correctif n'est pas appliqué sur tous les sites qui présentent cette vulnérabilité. Les attaques se perpétuent encore longtemps après la disponibilité du correctif. Le nombre d'attaques finit par décroître, mais c'est surtout du au fait que les attaquants se tournent vers l'exploitation de nouvelles vulnérabilités pour lesquelles il n'y pas encore de correctif.

Les attaques qui se déchaînent entre la publication de la vulnérabilité et la fourniture de son correctif appelées les « zero day attacks » peuvent faire très mal sur des systèmes d'information incapables de se protéger !

Quelle cible, Microsoft ou UNIX ?

On dit habituellement que les vulnérabilités affectent essentiellement les logiciels de Microsoft. Il n'en est rien. Les logiciels sous les différents UNIX et autres systèmes d'exploitation ne sont pas épargnés. D'ailleurs, d'après les CERT, 45% des vulnérabilités sont trouvées sous UNIX et « seulement » 16% sous Windows. Ainsi, côté vulnérabilités, le navigateur Firefox n'est pas la réponse à Internet

Explorer ; le serveur Web Apache n'est pas la réponse à Internet Information Server et Thunderbird n'est pas la réponse à Outlook ! On ne peut donc que vivre dangereusement.

Des vulnérabilités qu'on n'attendait pas

Des vulnérabilités sont découvertes même aux endroits où on ne supposait vraiment pas pouvoir en trouver. Ainsi une banale image JPEG, intentionnellement mal formée peut permettre à un hacker de prendre le contrôle de votre poste de travail suite à une vulnérabilité qui affecte les logiciels Microsoft Office que vous utilisez pour l'interpréter.

Mais pouvez-vous vous passer de lire des images quand vous naviguez sur la toile, quand vous écrivez des documents sous Word ou quand vous développez une présentation sous PowerPoint ?

Un humoriste a fait remarquer que si les voitures présentaient les mêmes défauts que les logiciels, personne n'oserait rouler avec. L'informatique est omniprésente, il faut bien utiliser des logiciels, alors surtout, ne pas négliger de placer des solutions de sécurité et d'installer les correctifs aussitôt qu'ils sont disponibles chez l'éditeur qui a votre confiance.

Les menaces

On distingue les menaces d'origine interne et celles d'origine externe. Les menaces internes sont celles provenant des utilisateurs situés dans votre réseau, les menaces d'origine externe viennent des utilisateurs situés en dehors de votre système d'information. Ce sont celles dont on se méfie le plus, mais c'est une erreur. Au moins 60% des attaques réussies proviennent de l'intérieur d'un réseau.

Les menaces internes

Les menaces d'origine interne sont induites par la maladresse des utilisateurs, par leur méconnaissance des outils qu'ils utilisent mais aussi hélas par leur malveillance.

C'est par exemple un fichier pourtant classé confidentiel, qui se retrouve publié par la presse alors qu'il contient des informations nominatives ou diffamatoires, avec toutes les conséquences pénales ou civiles que cette menace peut entraîner pour l'employé et aussi pour le dirigeant de l'entreprise qui n'a pas su assumer sa responsabilité de protéger l'information qu'il détient.

C'est le téléchargement d'outils logiciels « craqués » dont l'utilisation est illicite car sans licence ou de fichiers ou pages Web délictuelles. En France, par exemple la consultation de pages Web pédophiles ou racistes est un délit pénal et la loi réprime aussi le dirigeant de l'entreprise qui n'a pas pris les mesures de contrôle indispensables pour réguler l'utilisation du Web par ses employés.

Les menaces portent aussi sur la perte de productivité voire même de marchés, suite à la saturation de la bande passante par un employé qui télécharge des fichiers de très grosse taille, sans prendre conscience de la gêne causée aux autres usagers.

Mais c'est aussi des actes de malveillance perpétrés par des utilisateurs de l'intérieur et les protections périmétriques mises autour du réseau pour faire face aux menaces venant de l'extérieur sont évidemment inopérantes.

Les menaces externes

Sans négliger les simples tentatives de malveillance gratuite qui ne constituent pas les menaces les plus inquiétantes, les menaces d'origine externe peuvent être à caractère stratégique, idéologique ou terroriste. Savez-vous que nos échanges d'informations ont été depuis plusieurs années, à notre insu, captés et analysés par un gigantesque dispositif de grandes oreilles, le réseau Echelon, réparti sur plusieurs pays, en particulier les USA, le Canada, la Grande Bretagne, l'Australie, la Nouvelle Zélande, avec radars d'écoute, satellites, et batteries d'ordinateurs parmi les plus puissants du monde pour analyser les informations captées ?

Difficile d'échapper à ce réseau d'espionnage électronique et informatique dont le but avoué était de lutter contre le terrorisme et les narcotrafiquants mais qui a aussi servi de stations d'écoutes pour favoriser l'économie des pays qui hébergeaient ces grandes oreilles. Ceci constitue une menace réelle pour nos économies nationales.

Cette menace est toujours actuelle, et avec moins de moyens mais beaucoup de compétences, la mafia et les terroristes sont aussi à l'écoute des échanges et utilisent le réseau public pour organiser leurs actions ou paralyser les nôtres.

Les codes source des éditeurs de logiciels parmi les plus renommés sont volés et analysés pour en découvrir les vulnérabilités. L'armée américaine, et d'autres armées, disposeraient même d'équipes de hackers dotées de grands moyens pour infiltrer ou attaquer les infrastructures informatiques ennemies. Mission impossible, pensez-vous ? Dans l'industrie, qui sont nos amis et qui sont nos ennemis ?

Les menaces évoluent très vite et deviennent de plus en plus complexes à contrer. Nous n'en sommes plus, comme il y a 20 ans, à essayer de découvrir des mots de passe pour pénétrer dans un réseau. Aujourd'hui on s'offre des services de

hackers particulièrement efficaces ou on loue du temps machine sur des réseaux d'attaque aussi nombreux que volatiles.

Mais si le niveau de menaces est de plus en plus élevé, les connaissances requises pour lancer des attaques sont de plus en plus basiques parce que les outils pour attaquer sont de plus en plus conviviaux. D'après une enquête menée par le FBI, les attaques en 2006 aux USA, sur 313 entreprises qui ont répondu, ont coûté aux victimes une somme estimée à 52 millions de dollars et de nombreuses entreprises ne se sont pas relevées des attaques subies.

Les inquiétudes

Face à ces menaces, quelles sont les inquiétudes majeures ressenties par les entreprises ? Ce sont bien sûr les vers et les virus qui sont toujours médiatisés jusqu'à faire la une des journaux télévisés et qui constituent une menace réelle. Ce sont les SPAM qui encombrent les boîtes aux lettres et entraînent une perte considérable d'heures de travail passées à les supprimer. Ce sont encore les informations confidentielles qui s'envolent dans la nature avec les fichiers clients, les conflits internes et les secrets de fabrication, et qui se retrouvent chez les concurrents, chez les clients et dans le grand public.

C'est le réseau de l'entreprise qui tombe suite à une attaque par déni de service distribué. Et l'arrivée du sans fil, de la téléphonie sous IP, des applications peer to peer, des services Web et des smartphones / PDA n'a pas fini de justifier les inquiétudes légitimes des entreprises.

Quelques type de menaces

Classons les menaces les plus présentes en commençant par la plus médiatisée : le virus. Un virus s'attache à un logiciel porteur qui le véhicule et qui doit être exécuté pour que le code malfaisant qui l'infecte puisse agir et infecter d'autres logiciels.

La menace la plus rusée est le ver, qui diffère du virus parce qu'il n'a pas besoin d'être hébergé par un programme infecté pour arriver jusque chez vous sur votre système d'information. Le ver est autonome et pénètre dans votre réseau et sur votre poste de travail sans que vous n'ayez à exécuter la moindre action malheureuse, ni commettre la moindre maladresse (autre que celle d'être connecté au réseau !). Le ver arrive chez vous par le réseau, le plus souvent en passant par une faille d'un logiciel de votre poste de travail.

La menace la plus sournoise est sans aucun doute le cheval de Troie. C'est un logiciel qui ne cause pas de dégâts apparents mais qui au contraire se fait oublier et vous observe, capte vos informations et les envoie à son destinataire qui alors peut en faire un usage dommageable. Le cheval de Troie peut observer les frappes des touches de votre clavier, et vous aurez beau chiffrer votre information, lui la reçoit en clair. Il peut se situer au niveau de la fenêtre d'accueil par laquelle vous entrez votre mot de passe ou votre code PIN, ou être tapi dans votre système de fichiers où il scrute vos informations pour éventuellement les dévoiler.

La menace la plus répandue est sans doute le macro virus, variante des virus, qui, s'il est présent chez vous, a de grandes chances d'infecter tous les fichiers que vos fichiers Office ouvrent.

Et enfin la menace la plus imparable est le dépassement de buffer. Si le programme que vous utilisez présente ce type de vulnérabilité, une information entrée dans votre programme peut entraîner l'écrasement de ses instructions par des instructions conçues par le pirate et entrées en tant que données. Alors, ce n'est plus votre programme qui s'exécute mais les instructions entrées par le hacker qui peut prendre ainsi le contrôle de votre poste de travail.

Mais les menaces ne seraient pas grand chose s'il n'y avait aussi les attaques qui sont une concrétisation de ces menaces et quand ces attaques exploitent les vulnérabilités de vos programmes, il est difficile de les arrêter avant qu'elles n'aient atteint leur but !

Les attaques

Les attaques sur les systèmes d'information, qu'elles soient brutales ou feutrées, menacent aujourd'hui chacun de nous pour peu que nous soyons, ou que notre système d'information soit connectés. Une récente étude de Sophos indique qu'un poste de travail connecté à l'Internet, sans protection efficace, a 50% de (mal)chance d'être infecté au bout de 10 minutes et la quasi-certitude d'être infecté au bout d'une heure. Les attaques ciblent particulièrement les applications les plus utilisées sur le net que sont le Web et la messagerie, et les plus redoutables sont formées par une combinaison savamment dosée de plusieurs attaques.

Nous avons déjà évoqué l'action des CERT pour répertorier les vulnérabilités. Les CERT répertorient également les attaques depuis une vingtaine d'années et montrent que celles-ci augmentent de manière quasi exponentielle et dépassent cette année les 500.000. Une attaque peut cibler un seul poste de travail ou plusieurs dizaines de milliers de réseaux.

Qui sont les agresseurs ?

Il y a quelques années, la motivation des attaquants, était simple : nuire et détruire, souvent par défit, par pur plaisir ou simplement par vengeance. Aujourd'hui leur but principal est de soutirer de l'argent et les nouvelles attaques qui s'annoncent sont encore plus inquiétantes. Elles commencent dans le monde virtuel et se poursuivent dans le monde réel où elles retrouvent les victimes rencontrées sur le net, et s'en prennent à leur vertu ou à leur vie.

L'image de l'adolescent féru de nouvelles technologies, dans sa chambre encombrée de bandes dessinées, de documentations techniques et de canettes de coca, et qui mène des attaques au hasard, depuis son PC ou son MAC hors d'âge, pour prouver à ses copains et ses copines à quel point il est redoutable n'est plus de mise.

Une étude récente indique que seulement 10% des attaques sont menées par des hackers en herbe qui recherchent la notoriété, 60% par la petite cybercriminalité et 30%, les plus dangereuses, sont des attaques de grande ampleur perpétrées par des organismes mafieux, parfois officiels. Aujourd'hui les hackers redoutables sont plutôt des professionnels qui ciblent leur victime et combinent le « social engineering » et les outils sophistiqués qu'ils conçoivent pour leur usage personnel.

Les attaquants vont jouer sur la peur, l'incertitude et le doute, c'est dire que les piliers du commerce électronique se trouvent menacés par cette criminalité qui se regroupe en mafias organisées.

Les grandes familles d'infection

Les virus et les vers

Si les virus et les vers sont partout, ils ne constituent pas pour autant la seule cause d'infection. En 2004 un nouveau type de virus a réalisé la plus violente attaque que le cyber monde ait connu. Mydoom est arrivé par la messagerie. Si la messagerie ne suffisait pas pour l'infection, Mydoom se donnait une deuxième chance en passant par le logiciel « peer to peer » Kazaa.

Le but de ce virus n'était pas de vous nuire directement mais d'utiliser votre poste de travail comme base d'attaque, à une date programmée, vers le Web de la société SCO en Californie. Il était programmé pour envoyer des milliers de sollicitations à partir de centaines de milliers de PC infectés, dans le but de constituer un déni de service distribué.

Le code source de Mydoom étant connu, on remplace le nom de domaine sco.com par le nom de votre domaine, et c'est vous qui êtes menacé.

Les virus évoluent. En juillet 2001, le virus Code Red s'était installé sur 250 000 systèmes autour du monde en 9 heures. En janvier 2004, Slammer a mis 10 minutes pour infecter plusieurs dizaines de milliers de serveurs. Les virus et vers deviennent polymorphes en changeant de signature pour échapper aux anti-virus. Ils s'en prennent d'ailleurs parfois en priorité à l'antivirus qui les traque, puis à votre navigateur pour vous isoler et vous empêcher de trouver de l'aide sur la toile.

Les chevaux de Troie

D'après une étude de Sophos, les vers et virus ne constituent que 35% des infections. 62% sont constituées par des chevaux de Troie qui sont des logiciels qui se font oublier, une fois qu'ils ont infecté votre poste de travail mais qui écoutent ce que vous faites. Le but, pour les moins nocifs, est de connaître vos habitudes d'achat sur la toile, mais certains cherchent à connaître vos mots de passe, vos codes d'accès et vos coordonnées bancaires.

Les adawares, les spywares et les rootkits

Quand vous passez un programme d'éradication de spywares sur votre PC pour la première fois, vous êtes étonnés du nombre de programmes espions qu'il y trouve. Les adawares et les spywares sont deux variantes de logiciels espions qui résident sur votre poste de travail et qui diffèrent par leur finalité.

Les adawares s'intéressent plutôt à vos habitudes, aux pages Web que vous consultez, par exemple, afin de mieux cerner votre personnalité. Parfois vous êtes surpris de voir passer sur une page Web, une bannière publicitaire particulièrement ciblée sur vos préoccupations du moment. Vous avez acheté sur la toile un appareil photo numérique ? Deux jours après, sur une page Web qui n'a rien à voir avec votre achat, vous voyez passer une bannière qui vous propose d'acquérir une mémoire supplémentaire adaptée à votre achat pour en augmenter la capacité.

Le but des spywares, moins défendable, est de vous espionner, souvent pour capturer votre mot de passe ou votre code PIN.

Et pour cacher le tout, il y a les rootkits qui rendent furtifs les logiciels qu'ils accompagnent, en jouant sur les paramètres systèmes. La découverte et l'éradication des logiciels indésirables sont alors beaucoup plus problématiques.

Les attaques qui portent sur votre crédulité

Canulars ou tentatives de fraude, la messagerie nous réserve bien des surprises, voyons deux d'entre elles :

Le hoax

Le hoax ou canular joue sur la naïveté qui réside en chacun d'entre nous, même chez les plus méfiants. On peut vous mettre en garde contre un virus particulièrement dangereux et on vous indique comment l'éradiquer en supprimant la cause : un programme résidant sur votre disque. Mais ce programme est en fait un programme système parfaitement honnête et de plus nécessaire pour la bonne marche de votre système. Quand vous l'avez effacé, vous n'avez plus qu'à tout réinstaller.

Un autre exemple de hoax vous prend par les sentiments. La petite Noélie, 9 ans est atteinte de leucémie et a besoin d'une greffe de moelle osseuse avant la fin du mois. Sauvez là, utilisez vos listes de messagerie pour trouver le donneur avec le bon groupe sanguin introuvable. Que cette chaîne de solidarité est belle et que la demande est louable ! Si ce n'est que Noélie a 9 ans depuis plus de quinze ans et n'a jamais existé.

On peut aussi ruiner un marché honnête en signalant que dans des cinémas de telle ville, on a trouvé sur les sièges, des aiguilles infectées par le virus du sida ou alors vous raconter, en général par courriel, l'histoire de la banane tueuse, contaminée par une bactérie ravageuse, ou encore vous avertir que le chat de votre voisine a contracté le H5N1.

Un site, fort bien fait, répertorie les hoax www.hoaxbuster.com et propose même un moteur de recherche de hoax par mots clés. A consulter impérativement avant de commettre une bêtise.

La fraude nigériane

Qu'elle vienne par courriel du Nigeria, des Philippines ou d'ailleurs, avec la fraude nigériane ou carambouille, la chasse aux pigeons est ouverte. Le pigeon, c'est vous, et l'agresseur est toujours quelqu'un en grand danger dans son pays d'origine mais détenteur d'une énorme somme d'argent, qui vous propose de l'aider à faire transférer cette somme vers un pays plus calme, en passant par votre compte en banque, et moyennant bien sûr pour vous une commission conséquente.

Le business Model étant, vous vous en doutez, non pas de vous offrir de l'argent mais de vous en soutirer en exploitant par exemple les coordonnées bancaires que vous aurez transmises.

Les attaques sur le Web

La défiguration ou defacing

Le Web est souvent la première image institutionnelle qui présente l'entreprise et le premier contact que prend un client alors il faut soigner particulièrement sa page d'introduction. C'est pour cela que les attaques sur cette page intéressent les hackers.

Exploiter un défaut de protection en écriture pour accéder directement au serveur qui héberge les pages Web d'une entreprise, et en modifier le contenu est fort excitant pour l'attaquant. Les réussites sont parfois croustillantes pour le grand public et catastrophiques pour les victimes.

On parle ainsi d'un site Web d'un grand voyagiste qui vendait des billets en ligne et dont la page de garde montrait un avion montant dans un ciel sans nuages vers des destinations de rêve. Après défiguration, cette même page montrait l'avion en flamme. Commanderiez-vous alors des billets en ligne sur ce site ?

On parle aussi d'un site consacré à l'habillement de luxe et qui montrait un magnifique manteau de vison porté par une superbe créature. Après défiguration du site, la page montrait un bébé vison, tirant la créature par la manche de son manteau, qui s'écriait en larmes : « ils ont écorché ma maman ! »

Citons aussi un site qui donnait des conseils juridiques avec un bouton poussoir pour entrer en contact avec un conseiller, et dont la défiguration, avait dédoublé le bouton avec la légende « si vous êtes blanc, cliquez sur ce bouton, si vous êtes noir cliquez sur celui ci ».

Même le site de Microsoft, même le site de la CIA ont subit les ravages de la défiguration. Un beau matin, ce pourrait être le vôtre.

Le déni de service distribué

Plus que tout autre applicatif, le serveur Web va être la cible d'attaques en déni de service distribué qui consistent à lui envoyer des centaines de milliers de sollicitations pour saturer sa bande passante et le mettre hors d'état de servir ses pages Web à ceux qui en ont besoin.

Que faire pour empêcher cette attaque ? Si vous pouvez protéger un site Web contre des agressions, vous ne pouvez pas empêcher qu'on le sollicite et il est facile d'envoyer un nombre incroyable de requêtes vers un site Web cible. Le virus Slammer l'a fait en janvier 2003 et les botnets aujourd'hui nous en donnent facilement la possibilité, moyennant finance.

Les attaques sur la messagerie

La messagerie est, avec le Web, l'outil le plus utilisé sur les réseaux, donc le plus attaqué. Du hoax au SPAM en passant par le mass mailing et le mail bombing, on rencontre un choix d'attaques qui ne cesse de se diversifier.

Le SPAM ou pollupostage

Plus vous êtes présent sur l'Internet et plus vous recevez des SPAM.

De petite gêne à ses débuts parce qu'il était rare, le SPAM est devenu un véritable fléau qui fait hélas de cet outil merveilleux d'efficacité qu'est la messagerie, un vecteur de perte de temps et encombre nos boîtes aux lettres.

La CNIL définit le SPAM comme un envoi massif, et parfois répété, de courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contacts et dont il a capté l'adresse électronique dans les espaces publics de l'Internet.

Plus vous participez à des forums de discussion publics, plus votre nom figure dans des listes de diffusion et dans des annuaires, plus vous laissez votre adresse de messagerie sur les sites Web, plus vous recevrez des SPAM.

Messages proposant des excitants ou des montres Rolex à des prix incroyables ou encore la suite complète Microsoft Office Professional ou Photoshop à 10% de son prix réel, nos boîtes aux lettres sont encombrées par ces messages indésirables.

Un conseil, ne vous désabonnez jamais d'une liste de messagerie que vous identifiez comme étant du SPAM car c'est ce qu'on attend de vous pour être sûr que votre adresse est active et continuer de plus belle.

Le mass mailing

Le mass mailing est un envoi massif de courriels vers la boîte aux lettres que l'attaquant veut saturer. Il existe des outils qui permettent d'entrer dans une boîte de dialogue « l'origine » :-) et la destination des courriels, l'adresse du serveur de messagerie qui enverra la rafale de courriels, le texte et le sujet et enfin le nombre de courriels à envoyer en une seule fois (1, 100, 10000 ?).

Le mass mailing est une gêne non seulement pour le destinataire mais aussi pour le serveur de messagerie qui achemine les courriels et pour les fournisseurs d'accès Internet.

Le mail bombing

Le mail bombing fait rebondir un courriel piégé qui arrive dans votre messagerie vers les adresses trouvées dans vos listes de distribution. C'est souvent une des attaques utilisée par les virus pour se propager à travers le monde.

Et bien entendu, les courriels ainsi envoyés par vous, à votre insu, le sont à votre nom. Les protestations que vous enverront vos destinataires ne feront qu'augmenter la masse de messages en circulation.

Phishing et pharming

Le mot phishing est une combinaison du mot phreaker qui désignait l'attaquant qui piratait un central téléphonique dans les années 60, pour téléphoner gratuitement, et du mot fishing qui désigne le pêcheur.

Il combine l'utilisation de la messagerie et du Web pour faire tomber la victime dans le panneau et lui soutirer des renseignements qu'elle ne donnerait jamais si elle n'avait pas suffisamment confiance à qui les lui demande. Sa variante plus technique le pharming utilise une combinaison d'attaques sur le serveur de noms de domaine et le Web pour arriver au même résultat.

Le phishing ou l'arnaque en trois étapes :

Première étape on lance l'hameçon sur la toile, et ce ne sont pas les poissons qui manquent. L'attaquant envoie un courriel qui semble, par exemple, provenir de votre banque. Le logo, les fonts, les couleurs, tout vous fait penser que le courriel provient de votre banque, qui a un gros problème : votre compte a été la proie d'un hacker et vous avez sans doute été volé mais la banque assume. Vous devez juste cliquer sur l'URL proposé dans le courriel pour aller sur votre compte en ligne répertorier les dégâts subits.

C'est grave, pas de temps à perdre ! vous cliquez sur l'hyperlien indiqué et votre navigateur ouvre la page Web de votre banque, que vous reconnaissez au logo et à la charte graphique. C'est bien la page familière de la banque qui gère vos comptes. Vous saisissez votre login et votre identifiant pour entrer dans l'espace personnalisé de votre compte.

C'est la deuxième étape de l'arnaque car bien entendu vous n'êtes pas sur le Web de votre banque mais sur celui très éphémère du pirate et qui ressemble comme deux gouttes d'eau à celui de votre banque.

Avez-vous vérifié l'adresse Web où votre courriel vous a conduit ? Avez-vous vérifié que le cadenas au bas de la page de votre navigateur est fermé, traduisant un échange sécurisé par SSL ? Avez-vous téléphoné à votre banque pour vous inquiéter du courriel qu'elle vous a envoyé ? Avez-vous tenu compte des avertissements que toutes les banques sérieuses ont envoyé à leurs clients pour les mettre en garde contre le phishing en leur précisant que jamais elles ne demanderaient par messagerie de rentrer sur un compte ?

La troisième étape est d'utiliser les renseignements que vous avez gentiment entrés et grâce auquel le pirate va entrer cette fois ci sur la page Web de votre vraie banque pour vider, à votre nom, tous vos comptes, ou plutôt de demander à une « mule » de faire ce travail.

Les mules sont des internautes de la même région que la victime qui , moyennant finance, soutirent de l'argent de ces comptes compromis. Parfois les mules naïves n'ont même pas conscience que cette pratique est illégale.

Cantonné au début au marché US, les courriels d'accroches d'une attaque par phishing étaient tous écrits en anglais et concernaient les Américains qui avaient ouvert des comptes dans ces banques. Il était alors facile, pour nous qui recevions de tels courriels, de flairer l'arnaque.

Le problème est qu'aujourd'hui les courriels, de même que les sites Web sur lesquels l'arnaque repose sont pour la plupart écrit dans un français sans reproche et imitent à s'y méprendre les banques les plus connues.

Le pharming ou l'attaque sur les DNS

Et si les internautes devenaient méfiants ? S'ils ne cliquaient plus sur des hyperliens proposés dans des courriels venant soit disant de leur banque ? S'ils saisissaient directement l'adresse Web de leur compte en ligne à partir de leur navigateur ? Alors les attaques par phishing ne pourraient plus aboutir, et c'est là qu'intervient une attaque plus technique : le pharming, ou l'empoisonnement des serveurs de noms.

Sur l'Internet, les êtres humains entrent des adresses comme www.mabanque.fr, les machines comprennent des adresses internet comme 189.23.1.14. Entre ces deux façons d'interpréter les adresses, il y a des machines qui convertissent, ce sont les DNS.

Une attaque ciblant le DNS que votre accès à l'Internet utilise, en passant par une de ses vulnérabilités, pour que l'adresse www.mabanque.fr ne soit pas convertie en 189.23.1.14 mais en 192.17.7.28 qui est l'adresse internet du site Web du hacker et le tour est joué. Vous avez, à partir de votre navigateur, entré la bonne adresse du site Web de votre banque mais vous êtes aiguillé sur le mauvais site, celui du hacker, et ensuite vous commencez directement à subir le phishing à partir de l'étape 2. Tant que votre serveur DNS reste compromis, cette attaque est imparable.

La nouvelle cybercriminalité

Ce qui motive le hacker aujourd'hui n'est plus la notoriété, ni le défi et l'excitation des attaques, ni de faire ses preuves. Ce qui motive aujourd'hui le hacker … c'est de gagner de l'argent facilement, en prenant un minimum de risque. Un virus a montré la voix. Avec les botnets, la cybercriminalité se professionnalise et propose ses services en location. Le chantage se répand laissant présager une utilisation de l'Internet particulièrement inquiétante.

Le virus bugbear

Bugbear est un virus dont l'action première après avoir infecté votre PC est de se faire oublier. Mais il ne dort que d'un œil. Quand vous tapez au clavier le nom de votre banque, Bugbear se met à l'écoute de votre clavier et note tout ce que vous entrez.

Ensuite bien sûr il envoie tous les renseignements recueillis au hacker qui prend alors le relais dans vos transactions bancaires. Comment Bugbear connaît-il le nom de votre banque ? Il n'en a pas besoin, il possède une base de connaissance de plusieurs centaines d'établissements financiers, avec sans doute celui avec qui vous conversez, il suppose alors que c'est celui qui gère vos comptes.

Les botnets

Déjà plusieurs millions de PC dans le monde, connectés à l'Internet, peut-être parmi eux le vôtre, suite à une infection virale, sont passés, à l'insu de leurs propriétaires, à l'état de zombies. Venu avec un virus ou toute autre méthode, caché dans les profondeurs des fichiers du PC, un client IRC reste discrètement actif. Quand le serveur IRC situé sur le poste du hacker lance une requête sur le net, immédiatement tous les clients IRC à l'écoute exécutent le service demandé qui peut être par exemple de déclencher une attaque en déni de service distribué vers une cible qu'on veut faire tomber.

Pourquoi le hacker qui contrôle le serveur IRC à partir de son poste d'attaque ferait-il ça ? Pour des raisons purement mercantiles. Il loue ses services pour attaquer une cible désignée par l'utilisateur qui commande l'attaque. Une attaque par saturation d'un serveur est « facturée » entre quelques dizaines et quelques milliers d'euros suivant la cible.

Certains botnets se composeraient de plusieurs dizaines de milliers de PC zombies prêts à lancer des attaques. De nombreux SPAM qui saturent vos boîtes aux lettres proviennent aujourd'hui de réseaux de botnets, et votre PC est peut-être un relais involontaire de cette nouvelle cybercriminalité.

Le chantage

Aujourd'hui une dérive particulièrement inquiétante de la cybercriminalité se confirme. De plus ou moins passive, la cybercriminalité passe au stade actif et direct et les hackers deviennent des maîtres chanteurs en tirant parti des outils qu'on a évoqués jusque là, dans une chorale qui va vite devenir assourdissante.

Quand un site dont l'existence commerciale repose sur la présence et la disponibilité de son site Web sur l'Internet, site d'enchères en ligne, casino, vente de voyages, reçoit ce type de courriel :

« *Je lance une attaque en déni de service sur votre site, qui va durer quinze minutes, et vous allez en constater immédiatement les effets. Sachez que je peux lancer une attaque vingt fois plus puissante qui pourra durer plusieurs heures. Si vous ne souhaitez pas être exposé à un tel désagrément, vous me versez 7000€ avant ce soir, 19h00 sur ce compte* ».

Suivent les coordonnées d'un compte situé dans un pays où la législation concernant ce genre de transactions est assez floue et le maître chanteur pratiquement intouchable.

Mais vous, comme particulier, vous pensez pouvoir échapper aux maîtres chanteurs ? Détrompez-vous, vous pourriez fort bien constater un jour que vous ne pouvez plus lire vos fichiers Word, PowerPoint et Excel. Seule votre messagerie semble encore fonctionner correctement et vous avez reçu un courriel qui vous annonce que plusieurs de vos fichiers ont été chiffrés et que la clé pour les déchiffrer vous sera envoyée moyennant la somme de 20€.

Retour vers le monde réel

Il y a déjà quelques prémices et ce phénomène va hélas sans doute s'amplifier. L'Internet va être utilisé pour repérer ou attirer les victimes potentielles dans le monde réel. Les clubs de rencontres cachent parfois de bien grands dangers surtout pour celles et ceux sans expérience qui croient que tout le monde est gentil et correct. Surveiller l'utilisation du Web, des forums par vos enfants est loin d'être un conseil à écarter.

On a vu déjà des cybernautes qui ne font plus la différence entre le monde virtuel et le monde réel. On cite un Japonais qui a tué son ami parce qu'il avait vendu sur le net l'identité virtuelle que ce Japonais s'était attribuée. Il y a aussi une dame qui s'est fait violer par un voisin qui avait reçu un courriel semblant provenir de sa future victime et qui lui demandait de le faire.

Le monde est plus que jamais un espace dangereux, mais il existe des contre-mesures juridiques et techniques pour se protéger. Mieux vaut donc les connaître et les utiliser.

Gérard Peliks, EADS Secure Networks

Acronymes

CERT	Computer Emergency Response Teams
DNS	Domain Name System
IRC	Internet Relay Chat
SSL	Socket Secure Layer