YVES-MARIE PEYRY

MENACES CYBER-NÉTIQUES

Le manuel du combattant

éditions du ROCHER
LIGNES DE FEU

Menaces cybernétiques
Le manuel du combattant

Yves-Marie PEYRY

Menaces cybernétiques
Le manuel du combattant

éditions du ROCHER

Ces pages ne sont pas disponibles à la pré-visualisation.

témoigne John Arquilla « *Notre but est de fournir de bonnes conditions à ceux qui accepteront de collaborer. Les États-Unis ne lésinent jamais sur les moyens pour attirer les meilleurs spécialistes mondiaux, c'est pourquoi nous sommes sûrs de pouvoir les convaincre de travailler avec nous* ». Espérons que cette dynamique américaine trouvera écho auprès d'autres pays afin de remporter une victoire décisive sur nos adversaires cybernétiques. Des ennemis qui, je le répète, sont rarement des spécialistes. Mais ils ont tout simplement su courtiser un savoir-faire qui nous a peut-être, depuis trop longtemps, échappé.

CHAPITRE 2

Nous sommes en guerre

La menace cybernétique aurait pu rester limitée aux activités menaçantes de quelques hackers radicaux menant leur combat sur la Toile ou de cybercriminels cherchant un gain facile dans le nouvel espace numérique. Dans ces conditions, difficile de parler de cyber-guerre. Mais le risque cybernétique s'est étendu à l'échelle mondiale. Les États eux-mêmes, à l'image, par exemple, de l'Iran, de la Chine ou des États-Unis, ont levé des armées de hackers (nommées « quatrième armée » après celles de terre, de l'air et de mer) pour des frappes informatiques dignes d'un conflit traditionnel. Ainsi, le « commando cybernétique » de l'armée américaine est estimé à plus de 100 000 hommes et femmes, travaillant, dans l'ombre des réseaux, pour déclencher des attaques contre des serveurs ennemis. La Chine, reconnue pour être à la pointe en matière de guerre cybernétique, dispose, selon certains experts, de plusieurs centaines de milliers de hackers prêts à lancer des attaques sur les structures gouvernementales et économiques d'un pays étranger. D'ailleurs, en février 2011, la société américaine de sécurité informatique Mc Afee avait alerté sur des intrusions massives, en provenance de la Chine, sur les réseaux de multinationales du pétrole. De nombreux documents confidentiels auraient été dérobés à cette occasion.

Pour de nombreux spécialistes, la troisième guerre mondiale a déjà commencé et elle est cybernétique. Une affirmation qui

peut sembler audacieuse. Pourtant, au regard de l'actualité récente, la notion d'une cyber-guerre planétaire semble se dessiner.

L'Estonie face à la première guerre cybernétique de l'Histoire

En avril 2007, les vives tensions entre l'Estonie et la Russie ont entraîné une série d'attaques informatiques qui marquèrent, selon les experts, la première guerre cybernétique entre deux pays. Les premiers assauts informatiques auraient été déclenchés par les services de sécurité russes suite à la décision estonienne, le 27 avril 2007, de déboulonner un monument commémoratif dédié à l'armée soviétique. Les attaques cybernétiques de type DDoS qui ont visé l'Estonie ont mobilisé plusieurs centaines de milliers d'ordinateurs (un million selon certains experts). Elles ont frappé des sites institutionnels, économiques et médiatiques. Des cibles particulièrement pertinentes pour qui veut fragiliser, en quelques instants, l'ensemble d'un pays. À ce niveau, si une action de bombardement d'un site estonien avait eu lieu, elle aurait profondément marqué les esprits mais serait restée locale, si une action de bombardement d'un site militaire estonien avait profondément marqué les esprits, elle serait restée locale, difficilement anonyme et finalement peu paralysante pour le pays. L'uti-lisation d'armes cybernétiques a permis aux Russes de toucher presque tous les Estoniens dans leur quotidien en s'attaquant à des sites gouvernementaux et commerciaux, à des banques, ainsi qu'à la presse nationale. Un impact d'autant plus fort que l'Estonie est l'un des pays les plus à la pointe en matière d'utilisation des nouvelles technologies. En effet, presque toutes les démarches administratives y sont traitées par

Ces pages ne sont pas disponibles à la pré-visualisation.

coordonnées bancaires :

– L’intrusion sur le serveur d’un site de vente en ligne et la récupération des coordonnées bancaires qui y sont stockées. Fort heureusement, tous les sites ne gardent pas les coordonnées financières de leurs clients. Toutefois, l’actualité récente prouve que de nombreuses coordonnées bancaires ont pu être récupérées par ce moyen ;

– L’interception par *sniffage* de vos données au moment où vous vous connectez sur un réseau sans fil de type Wi-Fi. Cette technique, majoritairement utilisée dans le cyber-espionnage, sera abordée dans le chapitre suivant ;

– Des logiciels qui émulent des coordonnées bancaires. Ces programmes pirates utilisent un générateur de numéros de cartes bancaires basé sur les algorithmes des banques. Selon un hacker, les contrôles sur la date de validité de la carte et le cryptogramme visuel (trois derniers chiffres au dos de la carte) ne sont pas effectués en direct mais, à postériori. Le paiement peut ainsi être validé. Le pirate se fera livrer à une adresse postale ou bien il modifiera légèrement son adresse personnelle (en général le nom) pour pouvoir, en cas de souci, justifier qu’il s’agit tout simplement d’une erreur d’envoi. Avec un peu de chance, le facteur livrera tout de même l’objet même si le nom n’apparaît pas sur la boîte ;

– Le *phishing* qui est désormais devenu l’une des techniques les plus utilisées pour récupérer des coordonnées bancaires mais, aussi, des mots de passe de messageries électroniques ou autres informations confidentielles.

Phishing, l’arme principale des pirates pour voler

vos secrets…

Avant d'analyser les rouages de cette technique, je vous propose un « cas concret » basé sur une mésaventure authentique :

Martine reçoit un message électronique de son opérateur de téléphonie mobile. Le message lui indique qu'une panne nationale a eu lieu sur son réseau pendant plusieurs heures et qu'il présente toutes ses excuses à l'abonné. Elle se rappelle, en effet, cet incident qui a fait la une des journaux et qui l'a empêchée de passer le moindre appel pendant presque une journée. Elle avait trouvé ce désagrément particulièrement pénible et espérait que son fournisseur de téléphonie mobile allait faire un geste commercial. Ce message arrive à point nommé puisque l'opérateur assortit ses excuses d'une remise de 10 euros sur son abonnement pour le mois en cours. Il précise : « pour en bénéficier, veuillez cliquer sur le lien suivant ». Avant de cliquer sur le lien, méfiante car son petit-fils l'a avertie que des messages frauduleux circulaient sur les messageries, Martine vérifie le nom de l'expéditeur. Elle reconnaît l'adresse du service clientèle de son fournisseur de téléphonie mobile et clique en toute confiance sur le lien proposé. Le lien affiche un formulaire de saisie en ligne avec l'en-tête de son opérateur. Insouciante, elle remplit le formulaire qui se termine par une demande de vérification de son mode de paiement. Une fois complété, Martine clique, sans se poser de question, sur la case de validation en bas du formulaire. Ensuite, elle voit s'afficher la page d'accueil de son opérateur ce qui la conforte sur la régularité de cette opération. Martine ne mettra pas longtemps pour se rendre compte de la supercherie. En effet, si ses connaissances

informatiques restent limitées, elle garde, depuis la mort de son époux, un regard particulièrement attentif à ses relevés de compte bancaire. Chaque ligne est méticuleusement vérifiée. Ainsi, quelques jours après avoir rempli son formulaire pour bénéficier de la ristourne promise par son opérateur, Martine guette le montant prélevé sur son compte. Étonnée, elle constate que le montant est le même que les mois précédents. Aucune ristourne n'a été effectuée. De plus, deux autres lignes de son relevé de compte l'inquiètent aussi un peu. Les sommes ne sont pas élevées mais elle constate deux prélèvements de 15 et 23 euros qu'elle n'arrive pas à rattacher à une opération connue. En premier lieu, elle appelle son opérateur de téléphonie qui lui apprend qu'aucun message n'a été transmis pour une remise de 10 euros sur son abonnement. Le service client l'informe qu'elle a certainement été victime d'une manœuvre de phishing. Si Martine ne comprend pas le terme, elle réalise ce qui vient de lui arriver lorsque l'opératrice lui conseille d'appeler immédiatement sa banque…

Le *phishing* (contraction de l'expression anglaise *password harvesting fishing*, littéralement « la pêche aux mots de passe ») est l'une des attaques les plus répandues. Nous avons tous reçu ce type de message électronique nous signalant, par exemple, que notre FAI (fournisseur d'accès Internet) ou notre banque doit nous rembourser une somme d'argent ou vérifier les informations de notre compte. Le message se terminera systématiquement par un lien sur lequel il vous sera demandé de cliquer. Ce lien vous enverra vers une belle page avec le logo de l'organisme en question, histoire de vous mettre en confiance. Cette page vous demandera certaines informations personnelles (en général, des identifiants et mots de passe, des coordonnées bancaires). La suite n'a qu'un seul objectif, celui de récupérer

Ces pages ne sont pas disponibles à la pré-visualisation.

planète. Ainsi, de nombreuses sociétés et même des organisations gouvernementales sont vulnérables à ce type d'attaque dont les conséquences peuvent être désastreuses. À titre d'exemple, des sites aussi célèbres que ceux de Microsoft ou de Sony ont été les victimes d'attaques DDoS. On recense même contre le site du Pentagone, plus de 250 000 tentatives d'attaques par heure ! Pour parvenir à empêcher le succès de ces attaques, le département de la défense américain utilise près de 7 millions d'ordinateurs destinés à protéger ses réseaux informatiques !

L'outil principal d'une attaque par DDoS est le nombre d'ordinateurs utilisé. Plus ce nombre sera grand, plus les chances de mettre rapidement hors service le serveur ciblé seront grandes. Évidemment, il est bien difficile, pour ne pas dire impossible, pour un cybercriminel, de réunir plusieurs milliers d'ordinateurs pour réussir son attaque. Des réseaux mafieux proposent désormais de louer, pendant une durée déterminée, une armée d'ordinateurs zombies appelée également *botnet*. Les *botnets* les plus importants dépasseraient le million d'ordinateurs ! Des machines zombies, infectées à l'insu de leur propriétaire qui ne sait pas que son ordinateur participe, sans qu'il le sache, à d'obscurs projets cybercriminels.

Le principe de l'infection qui permettra de transformer votre machine en ordinateur zombie repose sur l'introduction d'un *malware*. Ce programme, pleinement automatisé, répondra aux commandes d'un « centre de contrôle » qui enverra à distance les « missions » à effectuer : par exemple l'envoi d'un message publicitaire (*spams*) ou de messages frauduleux (*phishing*) à l'ensemble des contacts de messagerie de la machine infectée ou la participation à une attaque massive de type DDoS. Au mois

de juillet 2012, le *botnet* baptisé Grumb a été mis hors d'état de nuire par une entreprise de sécurité informatique. Selon les experts, le réseau d'ordinateurs zombies Grumb aurait été responsable de 18 % des *spams* mondiaux !

La menace des *botnets* présente aussi un réel danger de sécurité sur les moyens de chiffrage, même les plus élaborés. Imaginez la puissance conjuguée de plus d'un million d'ordinateurs réunis pour casser un système de cryptage ! Je vous laisse imaginer la suite si ce système protège des installations stratégiques… Un aspect redoutable dont on n'ose imaginer les conséquences en cas d'utilisation terroriste…

Exploits, trojans et menaces virales

Au cœur des deux dernières techniques décrites, le *ransomware* et l'ordinateur zombie, nous avons la mise en place de ce que les hackers appellent un « exploit ». En informatique, l'*exploit* est un programme ou un fichier (image, vidéo, texte) qui contient un processus malveillant destiné à exploiter une faille de sécurité dans un logiciel ou un système d'exploitation. Cette technique permet ensuite au pirate informatique de profiter de cette faille de sécurité pour créer une *backdoor*, une porte dérobée, et d'obtenir ainsi un accès privilégié (mais bien entendu illégitime) à l'ordinateur de sa victime. Cette porte pourra servir à l'implantation d'une application pirate, un *malware*, qui, selon les intentions de l'attaquant, modifiera à votre insu le comportement de votre machine, ou permettra de subtiliser ou de détruire des données.

Cet objet caché au cœur de votre système d'exploitation

pourra être qualifié, par sa présence dissimulée, de *trojan*. La fabrication d'un *trojan* est, hélas ! Facilement accessible, même pour un néophyte. Comme vous pourrez le constater avec votre moteur de recherche favori, on trouve sur Internet une foultitude de sites qui expliquent, pas à pas, comment fabriquer un *trojan* et l'implanter sur l'ordinateur de sa victime. L'un des plus connus s'appelle ProRat. D'une interface très facile d'accès, il vous permet d'élaborer facilement votre cheval de Troie et de l'injecter sur une machine distante. Le *trojan* contient deux modules. Un module serveur, placé sur l'ordinateur de l'attaquant et qui permet de transmettre, à distance, les commandes nécessaires au pilotage du comportement du *trojan* et un module client, placé sur l'ordinateur de la victime, qui va recevoir les ordres transmis par le pirate. Si l'élaboration d'un tel objet s'avère facile, la réussite de l'exploit est beaucoup plus complexe. En effet, la plupart des antivirus (pour ne pas dire tous) vont systématiquement détecter la présence de cet intrus et le rendre non opérationnel. Là vont s'arrêter les compétences du néophyte et commencer celles du hacker. Comme nous avons pu le voir avec des *malware* sophistiqués comme Stuxnet ou Flame, des techniques existent pour rendre votre programme antivirus aveugle à cette menace. Pour cela, certains pirates parviennent à modifier la signature du *trojan*. En effet, la signature, qui est une ligne de code au cœur du programme malveillant, constitue la marque de fabrique de l'objet. C'est cette marque qui est contrôlée par l'antivirus. Ainsi, en modifiant la signature, le pirate pourra parvenir à faire croire à l'antivirus que son *trojan* est un programme légitime et non suspect. D'autres techniques s'attaqueront directement au système de vérification des signatures du programme antivirus pour tenter de désactiver son action.

Ces pages ne sont pas disponibles à la pré-visualisation.

accéder à vos données en clair et y récupérer, par exemple, des coordonnées bancaires, des mots de passe et autres informations confidentielles.

Pour augmenter leur chance d'intercepter vos communications sur Internet, les pirates parviennent également à créer de faux *hotspots* en leur conférant toutes les apparences de *hotspots* officiels. Sous Windows, des logiciels comme Connectify-me permettent de partager, très facilement, votre connexion Internet en émulant un *hotspot* à l'aide de votre carte Wi-Fi. Selon votre convenance, ce *hotspot* pourra être sécurisé (wep ou wpa) ou non. Vous pourrez également lui attribuer le nom de votre choix. Ainsi, on pourra imaginer des noms possédant toutes les apparences de réseaux officiels comme « Région Ile de France-Open Network » ou « Roissy Aéro-port free Network ». Cette émulation rapide d'un *hotspot* constitue, pour le pirate informatique, un moyen efficace de vous faire accéder à Internet par l'intermédiaire de sa carte Wi-Fi et ainsi de *sniffer*, au passage, l'ensemble de vos données échangées sur le Web. Cette technique, utilisée également pour intercepter des communications téléphoniques GSM (voir chapitre sur la sécurité radioélectrique) est appelée Man-In-The-Middle-Attack, l'attaque de l'homme du milieu, puisque que le pirate qui l'utilise se trouve entre vous et Internet (dans le cadre de la création d'un faux *hotspot* Wi-Fi) ou entre vous et votre relais cellulaire (dans le cadre d'une interception GSM).

Le cyber-espion peut même créer, à votre insu, un clone de votre box Internet. Assez facilement réalisable avec la suite Backtrack (qui sera abordée au dernier chapitre), cette opération va consister à vous désauthentifier de votre réseau Wi-Fi domestique pour vous reconnecter sur un réseau équivalent

(portant exactement les mêmes caractéristiques que celles de votre box). Cette attaque ne durera que quelques millisecondes et passera totalement inaperçue. Cependant, votre accès Internet ne sera plus effectué par l'intermédiaire de votre réseau domestique mais par un réseau extérieur émulé par un obscur pirate informatique qui pourra ainsi intercepter vos données. Cette attaque peut également être un moyen de récupérer votre clef de réseau sans fil. Dans ce cas, une fois que le pirate sera parvenu à vous raccorder à son propre réseau, il enverra sur votre machine un faux message vous invitant à taper le mot de passe de votre réseau domestique. Une fois tapée, la clef tombera dans le filet tendu par le pirate et il pourra désormais s'en servir pour se raccorder, en toute impunité, à votre propre réseau Wi-Fi.

Dans ces conditions, l'utilisation d'un réseau sans fil pour se connecter à Internet semble compromise. Toutefois, même sur des réseaux non sécurisés, des solutions de chiffrage existent pour renforcer votre sécurité. À cet effet, plusieurs applications, simples à mettre en œuvre, vous seront présentées dans le dernier chapitre de cet ouvrage.

Aussi, en cas de suspicion d'intrusion sur votre réseau, je vous invite à utiliser le programme *open source* Angry IP Scanner (http://sourceforge.net/projects/ipscan/). Il vous permettra d'effectuer un audit des appareils connectés à votre réseau et de détecter d'éventuelles connexions pirates.

Au-delà du *sniffage* de vos données, certaines informations potentiellement sensibles peuvent être obtenues sans recourir à des techniques d'interception.

Vos mails peuvent vous trahir…

Contrairement à un courrier traditionnel, lorsque vous envoyez un mail, les informations qui y sont contenues ne se limitent pas à votre message et à l'adresse du destinataire. En effet, bien d'autres éléments viennent auto-matiquement se glisser dans votre courrier. Ainsi, sans en avoir conscience, nous transmettons à notre destinataire plus de renseignements que nous pourrions l'imaginer. Des informations cachées qui peuvent être retrouvées en analysant le *code source* d'un mail. Parmi elles, on trouve un élément d'identification particulièrement intéressant, l'*adresse IP* de votre machine. Cette information, transmise à votre insu, permettra de vous géolocaliser à chaque mail envoyé. On imagine l'embarras du mari infidèle qui envoie un mail à son épouse pour lui dire qu'il est bien arrivé à son séminaire à Lyon alors qu'il se trouve à Nice avec sa maîtresse. Ce petit *code source* trahira sa supercherie. Mais, plus grave encore, il permettra aussi de suivre, à chaque mail envoyé, les déplacements professionnels, par exemple, d'un chef d'entreprise. Si ce dernier veut éviter que ses concurrents soient au courant qu'il est en tractation avec une entreprise chinoise, la balise d'un mail le localisant en Chine pourra éveiller l'attention.

L'affichage du code source dépendra de l'application de messagerie utilisée. Avec Outlook, il suffira de faire un clic droit sur le mail reçu et de cliquer ensuite sur *propriétés* puis *détails*. Sous Thunderbird, après ouverture du message, vous cliquerez sur *affichage* puis *code source du message*. La combinaison de touches *ctrl+u* vous permettra d'afficher la source directement. Si vous ne passez pas par une application de messagerie, la plupart des serveurs de messagerie permettent d'afficher la

Ces pages ne sont pas disponibles à la pré-visualisation.

Une nouvelle fois, on assiste à une confusion flagrante entre cryptage et compression numérique. En effet, ce n'est pas parce qu'une transmission est numériquement compressée qu'elle est cryptée ! Les chaînes gratuites de la TNT sont, certes, numériques mais elles ne sont pas cryptées. Il suffit simplement de posséder le codec (le code) de numérisation pour pouvoir fabriquer un démodulateur capable de recevoir les signaux transmis. Par contre, les chaînes payantes possèdent un système de cryptage et nécessitent l'obtention d'une carte possédant la clef de décryptage pour pouvoir y accéder.

Il en va de même pour le DECT. Ce n'est pas parce que les transmissions sont émises numériquement qu'elles garantissent une protection contre une écoute illégale. Et, c'est justement cette sécurité apparente du DECT qui **a été mise à mal**, en décembre 2008, lors du Chaos Computer Club de Berlin qui est un rassemblement annuel de hackers du monde entier. En effet, deux « amateurs éclairés », ingénieurs de formation, ont montré comment il était possible, à partir d'une carte PCMCIA de marque Com on Air modifiée sous Linux, d'écouter les téléphones sans fil DECT. Un système d'écoute amateur digne des services spécialisés officiels ! Le matériel nécessaire est uniquement composé de la carte PCMCIA de marque Com on Air (destinée initialement à permettre à votre ordinateur de se raccorder à votre base DECT pour un usage modem, voix IP, etc.), d'une machine disposant d'un port PCMCIA, et d'un *live CD* disposant d'une suite de logiciels qui effectuent l'ensemble des tâches nécessaires, de l'interception à la démodulation en un fichier audio lisible sur n'importe quel ordinateur. Une ligne de commande *autorec* permet même d'engager un enregistrement dès qu'une station DECT est en communication. D'une portée de 100 à 300 m, ce système amateur d'interception peut s'avérer redou-table en milieu urbain. Si la technique est bien entendue

parfaitement illégale, il est bien difficile d'arriver à empêcher d'éventuels espions amateurs de procéder à ce type d'écoute puisque le matériel utilisé est parfaitement passif (il n'émet aucune onde radioélectrique et ne fait que recevoir) et il est donc indétectable. Ainsi, la seule parade consiste à chiffrer les flux échangés entre votre téléphone et sa base puisque c'est l'échange radioélectrique entre les deux qui peut être intercepté. Cependant, de nombreux téléphones sans fil DECT semblent être vendus sans activation du chiffrage des données. En effet, l'utilisation de certains matériels optionnels comme un répéteur DECT (qui permet d'étendre la portée de votre installation) n'est possible que si les communications ne sont pas cryptées. Aussi, afin d'éviter des soucis de compatibilité, de nombreux fournisseurs ont désactivé par défaut la fonction de cryptage. Normalement, tous les téléphones DECT doivent contenir un module de chiffrage des communications. Toutefois, et au regard de nombreuses notices que j'ai pu parcourir, il est parfois bien difficile de savoir si votre téléphone dispose, par défaut, d'un chiffrage activé. Cependant, de manière sibylline, certains fournisseurs précisent : « au cas où il serait nécessaire d'intégrer un télé-phone d'un fabricant tiers ne supportant pas le chiffrement, cette fonction peut être désactivée… » Une précision qui permet d'en déduire que le cryptage est activé. Cette remarque corrobore aussi le fait que des soucis de compatibilité ont pu inciter certains fabricants à désactiver l'option de chiffrage. Dans tous les cas, sachez, hélas ! Que même certains téléphones bénéficiant d'un système de chiffrage ont réussi à être interceptés par des hackers qui étaient parvenus à casser la clef de cryptage !

Dans ces conditions, l'utilisation d'un téléphone filaire pour toutes ses communications sensibles semble incontournable. D'ailleurs, je vous rappelle que tout particulier doit

normalement disposer, chez lui, d'un téléphone filaire. En effet, le téléphone fixe traditionnel n'est pas tributaire d'une alimentation électrique pour fonctionner. Ainsi, en cas de panne, ce type de téléphone continuera à fonctionner (grâce à l'alimentation propre au réseau téléphonique qui est indépendante de votre réseau électrique) et vous permettra, le cas échéant, d'appeler les services de secours.

Évidemment, même avec un téléphone filaire vous ne pourrez échapper au possible raccordement « sauvage » sur votre ligne. Mais, croyez-moi, ce type de technique est de moins en moins utilisé car elle nécessite une intervention humaine qui peut facilement être repérée. Ainsi, en 1998 à Berne, une équipe du Mossad chargée de poser un système d'écoute sur une ligne téléphonique avait été surprise, en flagrant délit, par une voisine insomniaque !

La sécurité des communications GSM

La France compterait plus de 67 millions de téléphones portables en 2012. Avec plus de cellulaires que d'habitants, ce moyen de communication est devenu incontournable pour nos besoins privés mais également professionnels. Même les services de secours ou de sécurité privilégient désormais son usage, parfois au détriment des moyens radioélectriques habituellement utilisés (comme le réseau Antarès dédié aux missions de sécurité civile). Une prédominance qui peut rapidement devenir synonyme de vulnérabilité. En juillet 2012, une simple panne logicielle chez l'opérateur Orange entrainait un *bug* national de plusieurs heures, empêchant 26 millions d'abonnés de passer des appels, d'envoyer des SMS ou d'accéder à l'Internet mobile. Un incident de grande ampleur qui a aussi valeur

Ces pages ne sont pas disponibles à la pré-visualisation.

systèmes de surveillance.

Les systèmes de brouillage GSM/DECT/GPS

Pour un prix inférieur à 50 euro, le grand public peut se procurer sur Internet des dispositifs permettant d'empêcher toute émission radioélectrique sur certaines plages de fréquences. En général, ces appareils sont essentiellement destinés à brouiller toutes les ondes émises par les téléphones portables (en usage dans certains cinémas) mais, également, par les téléphones domestiques sans fil de type DECT. Leur portée, certes limitée (quelques mètres en général), peut toutefois être considérablement augmentée par l'usage de plusieurs dispositifs placés stratégiquement pour couvrir une large zone. Dans ces conditions, on imagine son pouvoir de nuisance dans un lieu fortement fréquenté.

L'usage de ce type d'appareil est bien connu dans le milieu du grand banditisme puisqu'il permet de brouiller les traceurs GSM ou GPS de la police. Certaines alarmes domestiques basées sur la transmission d'un signal GSM en cas d'intrusion ont également été neutralisées à l'aide de ce dispositif.

CHAPITRE 6

Les réseaux sociaux

Par sa capacité à mettre en relation des millions d'ordinateurs répartis sur l'ensemble de la planète, Internet est devenu un outil privilégié de *réseautage social*. On ne compte plus les sites destinés à vous aider à constituer votre communauté, qu'elle soit professionnelle ou privée, autour d'un thème fédérateur, d'une expérience commune ou, tout simplement, d'une amitié née dans la vie réelle et que l'on souhaite faire vivre sur les réseaux. Pour le néophyte, peut-être à la veille de se lancer dans la grande aventure sociale du Net, une question se pose : Qu'a-t-on à y gagner ? À cette interrogation, certains répondront qu'ils y ont trouvé un moyen de sortir de leur solitude, d'autres une possibilité de nouer de nouveaux contacts professionnels, d'autres encore un moyen d'expression sans entrave de leurs idées avec, toujours en toile de fond, un besoin de les partager avec qui veut bien les lire, y réagir ou simplement les relayer. Mais, il y a une autre question préalable que le néophyte devrait se poser : Qu'ai-je à y perdre ? Et là, chez les utilisateurs, les réponses sont finalement plus complexes, moins évidentes à formuler comme si un tabou nous empêchait de regarder bien en face la réalité des dangers induits par les réseaux sociaux. Un tabou qui tient peut-être au fait que ce que nous avons à perdre n'est rien de moins qu'une partie de nous-mêmes, de notre intimité. Car ce que les réseaux sociaux peuvent construire, ils peuvent aussi le détruire en quelques

clics. Et, derrière cette menace, c'est votre notoriété et, potentiellement, celle de vos proches qui est en danger.

Au mois d'octobre 2012, les médias français rapportaient le suicide d'un jeune Brestois de 18 ans suite à un chantage perpétré par une inconnue rencontrée sur Facebook. Cette dernière avait noué un lien virtuel particulièrement étroit avec le jeune homme. Peu à peu, par Webcams interposées, des échanges visuels intimes avaient eu lieu. Puis, brutalement, l'inconnue si avenante est devenue menaçante « J'ai une vidéo porno de toi. Si tu ne me donnes pas 200 euros, je vais détruire ta vie ». En effet, cette vie sera détruite, foudroyée par cet odieux chantage. Une escroquerie en provenance, selon la justice, de Côte d'Ivoire et qui révèlerait un réseau international.

Hélas ! Ce drame n'est pas isolé. D'autres suicides, suite au même type de chantage, ont été recensés à travers le monde comme celui de l'adolescente canadienne Amanda Todd, âgée de 15 ans et victime d'un harcèlement sur le Web. Des tragédies qui mettent en relief le danger des réseaux sociaux. Pourtant, si un danger existe, il peut être contrôlé en adoptant des consignes simples qui vous permettront d'utiliser les réseaux sociaux et d'en tirer les bénéfices attendus tout en protégeant votre vie privée.

Facebook, le site social qui est virtuellement devenu le troisième pays du monde

Avec plus d'un milliard d'utilisateurs en octobre 2012, Facebook est virtuellement devenu le troisième pays du monde, après la Chine et l'Inde. Toutefois, si Facebook a réussi à

Ces pages ne sont pas disponibles à la pré-visualisation.

au cœur d’un conflit armé

En novembre 2012, le conflit armé entre le Hamas et Israël a révélé la formidable puissance des réseaux sociaux comme arme de propagande, voire même de désinformation. Une arme si puissante qu’elle devance même les médias officiels. D’ailleurs, l’armée israélienne confirmait sur Twitter ses attaques avant même de tenir une conférence de presse. Un ami journaliste qui a vécu ces évènements depuis la bande de Gaza témoigne : « *au point le plus critique, alors que nous étions tous confinés et dans l’inca-pacité d’aller sur le terrain, Twitter était devenu notre moyen privilégié de communication (…) C’était vraiment incroyable de voir l’instantanéité de l’information et ce flot ininterrompu de news qui se déversait sur les flux sociaux. J’entendais une explosion et quelques secondes après, quelqu’un, quelque part à Gaza, l’avait déjà mentionnée sur Twitter (…) Il y avait aussi ce langage, propre à Twitter et ses équivalents, un langage bref et, pourtant, souvent plus redoutable qu’un long discours. Quelques mots biens choisis comme – #Gaza terrible large airstrike right now #help #GazaUnderAttack – et la terreur s’installait sur la toile sociale du Net par un massif* retwittage *planétaire. Une terreur d’autant plus forte qu’elle ne reposait que sur quelques mots, quelques bribes d’information qui obligeaient l’imaginaire collectif à faire le reste. Ainsi, le* tweet *laconique de l’AFP indiquant : Le bâtiment abritant notre bureau à #Gaza a été touché par un raid israélien, laissait les internautes imaginer le pire. D’autres confrères laissaient s’exprimer leurs peurs, leurs envies, leur écœurement, comme si Twitter possédait des vertus désinhibitrices. Même certains organes officiels parlaient sur les réseaux sociaux avec un ton très éloigné du discours policé habituellement utilisé. Là, j’ai compris*

comment quelques mots sur Twitter pouvaient devenir une affaire d'État. On y parlait, certes brièvement, mais, sans retenue ni recul. Je me rendais compte qu'un nouveau langage était né, un langage sans nationalité, sans réelle origine sociale ou culturelle. C'était un langage universel qui reflétait, finalement, les tourments et les angoisses de notre inconscient collectif. C'était tout sauf du journalisme et, pourtant, ce nouveau pouvoir des réseaux sociaux parlait de cyber-journalisme. »

Dès le début des hostilités, l'armée israélienne a affiché sa volonté d'utiliser les réseaux sociaux comme une arme offensive au cœur de la guerre de l'information. On peut citer, par exemple, ce *tweet* de l'armée israélienne présentant la photo du chef du Hamas, Ahmed al-Djaabari, abattu quelques instants auparavant, et portant la mention « éliminé ». De leur côté, les organisations pales-tiniennes ont immédiatement réagi en affichant, en temps réel, témoignages et messages de propagande sur les réseaux sociaux. Ainsi, pendant que la guerre réelle faisait rage, de part et d'autre, sur le terrain, une autre bataille se déroulait, celle d'Internet et des réseaux sociaux où les belligérants s'affrontaient à coups de *tweets*. Alors que les brigades Al-Kassam annonçaient sur Twitter « *les mains bénies atteindront vos dirigeants et vos soldats où qu'ils se trouvent* », l'armée israélienne répliquait en annonçant au Hamas ce message d'avertissement : « *nous recommandons à tous les militants du Hamas, quel que soit leur rang, de garder la face contre terre dans les jours qui viennent* ». Une guerre de la communication qui a d'ailleurs peut-être évité ce *shutdown*, cette censure d'Internet, tant redoutée par les Palestiniens. En effet, selon certaines sources bien informées, les forces armées israéliennes ont préféré laisser un libre accès à Internet afin de

permettre à leur stratégie de communication basée sur le *réseautage social* d'atteindre la bande de Gaza.

Adoptés par plus d'un milliard d'internautes, les réseaux sociaux sur Internet sont devenus l'outil principal de communication du cyberespace. Difficile d'y échapper. Pourtant, son utilisation ne doit pas constituer un « acte d'allégeance ». N'abandonnez pas votre intimité à des serveurs dont vous n'avez pas la propriété. Méfiez-vous aussi de ces amis inconnus, sortis de nulle part, qui risquent de profiter de votre crédulité pour vous nuire. En un mot, gardez le contrôle !

Ces pages ne sont pas disponibles à la pré-visualisation.

vous n’aurez plus ensuite qu’à taper l’adresse URL du site Web que vous souhaitez diagnostiquer. L’application générera un fichier des tests effectués qui décrira l’ensemble des failles trouvées. Pour ceux qui souhaiteraient aller plus avant et tenter une intrusion sur leur propre serveur, le logiciel Havij est l’application majoritairement utilisée par les pirates informatiques pour les attaques par injection SQL. Havij détiendrait un taux de réussite de ses attaques par injection SQL à plus de 95 % (à la condition que le serveur contienne une faille SQL). De nombreux *tutoriels* existent sur Internet. Toutefois, je vous rappelle que l’utilisation de ce logiciel sur un serveur dont vous n’êtes pas le propriétaire est parfaitement illégale.

Concernant l’attaque par DDoS, même les experts les plus pointus dans ce domaine vous confieront qu’il est bien difficile de contrer ce type de menace. D’ailleurs, comme nous l’avons vu précédemment, même les sites des administrations les plus sensibles y sont confrontés. L’attaque puise sa puissance dans son nombre de connexions simultanées. L’appui d’une armada d’ordinateurs zombies est déterminant. Imaginez la connexion de plus d’un million d’ordinateurs en même temps ! Combien de serveurs peuvent résister ? Presque aucun. Le Pentagone utilise 7 millions d’ordinateurs pour protéger son réseau. Aucune entreprise ne peut investir de tels moyens.

De plus en plus, certaines entreprises ont adopté la technique du *Cloud computing* pour parer, parmi d’autres usages, cette menace. Le *Cloud computing* permet de stocker ses informations, d’y accéder et de les traiter par l’intermédiaire de serveurs distants mutualisés non physiquement présents dans l’entreprise et baptisés *Cloud* (« nuage » en français). En cas de

tentative d'attaque par DDoS, le cyber-attaquant ne pourra plus cibler le serveur de l'entreprise puisque, physiquement, il n'y en aura plus. Au mieux, il pourra tenter une attaque sur l'un des serveurs mis à disposition du *Cloud computing*. Toutefois, ce système, basé sur le stockage virtuel d'informations, permet, lorsqu'un serveur n'est plus opérationnel, de basculer sur un autre serveur. Difficile, voire impossible pour l'attaquant, d'arriver à neutraliser l'ensemble des serveurs dédiés au *Cloud computing*. Cette technique séduisante présente toutefois un désavantage. En effet, les données de l'entreprise ne sont plus physiquement présentes dans l'entreprise. Dans ces conditions, la crainte de perdre le contrôle sur la propriété de ses données est grande. De nombreux détracteurs du *Cloud computing* mettent en avant ce risque. Parmi eux, on trouve Steve Wozniak, le cofondateur d'Apple. À propos du *Cloud computing*, il confie : « *avec le nuage, rien ne vous appartient. Moi, j'aime savoir que les choses sont à moi (…) plus on transfère dans le nuage, moins on garde le contrôle*. »

Un risque de perte de contrôle sur ses informations qui pourrait constituer une aubaine pour un éventuel cyber-espionnage.

C'est une menace que l'on retrouve également avec une autre forme d'externalisation de la gestion informatique de l'entreprise, celle du *leasing*.

Avantages et inconvénients du leasing

Face à un marché en perpétuelle mutation, de nombreuses entreprises choisissent le leasing (la location) d'ordinateurs

pour maintenir leur parc informatique à jour. Cette formule est, en effet, particulièrement attractive et peut également proposer la maintenance régulière des machines concernées. Cette nouvelle mode ne touche pas que les entreprises mais aussi, et de plus en plus, des particuliers désireux de rester à la pointe des dernières innovations informatiques.

Le leasing est aussi un moyen d'améliorer la productivité de son entreprise en valorisant le travail de ses employés. En effet, confier un ordinateur puissant et robuste à un employé est un moyen de reconnaître la qualité de son travail. Sans entrer dans une analyse psychologique approfondie, l'écran de cette machine… nous renvoie, quelque part, à l'image d'une partie de nousmême. Ce qui s'affiche à l'écran est directement lié à nos actions sur le clavier ou à la souris. Dans cette société où nos tâches quotidiennes sont de plus en plus souvent dématérialisées, un rapport étroit s'est tissé entre l'homme et la machine. Ainsi, pour un salarié, travailler plusieurs heures par jour sur une machine obsolète ne pourra que lui renvoyer une image médiocre de son travail et, surtout, de lui-même. Sa productivité en sera amoindrie, ce qui augmentera encore son sentiment de médiocrité. Offrir à ses employés un parc informatique moderne et pleinement fonctionnel valorisera grandement leur travail et aura, inéluctablement, un impact significatif sur la productivité de l'entreprise. La location d'ordinateurs régulièrement renouvelés est un moyen efficace d'atteindre cet objectif.

Cependant, certaines sociétés peu scrupuleuses de leasing ont trouvé, dans cette formule en pleine expansion, la possibilité de mettre en œuvre, à l'insu de leur client, des outils de cyber-espionnage au cœur des machines louées. Ainsi, aux États-Unis,

Ces pages ne sont pas disponibles à la pré-visualisation.

logo représentant un verrou apparaîtra sur la barre d'adresse de votre navigateur et l'adresse du site Internet sur lequel vous serez connecté commencera par https (soit http + SSL) et non http. Si ce moyen de protection est assez largement répandu, il n'est pas systématique. Toutefois, le plug-in Https Everywhere (disponible sur Mozilla Firefox et Google Chrome) forcera le passage en mode SSL sur de nombreux sites.

Cependant, il est bon de préciser que même si les données protégées par ce protocole sont inaccessibles, l'analyse du trafic SSL permet, malgré tout, d'accéder à des informations concernant son utilisateur comme sa localisation et les sites consultés.

Dans ces conditions, la solution ultime est l'utilisation d'un protocole qui garantira le cryptage systématique des données échangées tout en assurant à son utilisateur un total anonymat.

L'outil ultime pour sécuriser vos connexions : le VPN

La meilleure façon d'éviter l'interception de vos flux lorsque vous vous connectez en Wi-Fi est de mettre en place un protocole systématique de cryptage afin de rendre incompréhensibles vos données pour un éventuel cyber-espion. Toutefois, comme nous l'avons vu précédemment, le seul cryptage des données n'empêche pas l'analyse de vos connexions (ce DPI, Deep Packet Inspection, utilisé aussi par de nombreux États pour surveiller le contenu des flux échangés sur Internet). Pour réunir ces deux conditions de protection, une stratégie de sécurité existe : le réseau virtuel privé ou VPN

(Virtual Private Network). Cette technique va consister à faire passer vos données dans un tunnel sécurisé entre votre ordinateur et un serveur d'accès distant. Ce dernier, en général situé à l'étranger, sera votre portail d'accès au Web. C'est-à-dire que tout ce qui passera entre vous et lui sera sécurisé et anonyme. Ainsi, lorsque vous vous connecterez, par exemple, à un *hotspot*, toutes vos données seront chiffrées et échapperont aux tentatives de *sniffage*. Ce moyen de chiffrage nécessite qu'entre vous et le serveur d'accès distant une clef de cryptage soit établie.

Pour comprendre le principe d'un accès VPN, il faut s'attarder un instant sur le fonctionnement d'un accès sans VPN. Lorsque vous vous connectez à Internet, votre ordinateur envoie au serveur que vous avez sollicité une adresse IP (même si votre connexion est protégée par cryptage SSL). Cette adresse, composée de quatre groupes de chiffres séparés par des points, constitue votre identité sur Internet. Indispensable pour pouvoir communiquer sur le Web, elle est votre marqueur personnel qui vous distinguera d'un autre ordinateur. En comparaison, votre adresse IP est comme votre adresse postale, c'est elle qui va permettre au facteur de vous adresser votre courrier et de ne pas l'adresser à une autre adresse. Cependant, contrairement à votre adresse postale, cette empreinte réseau peut changer au gré des connexions, toutefois, votre opérateur sera en mesure, en cas d'obligation judiciaire par exemple, de retrouver quel utilisateur a utilisé telle adresse IP à un instant donné. Ainsi, malgré l'anonymat apparent d'Internet, aucune de vos connexions n'est réellement anonyme. Si votre fournisseur d'accès est tenu, par la loi, de garder en mémoire cette adresse pendant un an, tous les sites auxquels vous vous connectez peuvent également le faire. Si vous possédez un blog, faites

l’expérience d’ouvrir un compte gratuit sur Stat-counter (http://statcounter.com/). Ce site vous permet d’analyser les connexions à votre blog. La rubrique *recent visitor activity* est particulièrement intéressante puisqu’elle vous permet d’obtenir l’adresse IP des internautes qui se sont connectés à votre blog avec l’heure et la date précises de connexion. En plus de ces informations, Statcounter vous précisera la localisation, le site visité juste avant la connexion à votre blog, le système d’exploitation de l’utilisateur, son navigateur Internet et même la résolution de son écran ! Avec un peu de pratique et de déduction, vous pourrez assez facilement en déduire l’identité de l’inter-naute s’il s’agit d’une connaissance. Je sais que « Pierre » utilise un Mac et utilise Chrome comme navigateur, je lui ai envoyé un lien vers mon blog à 15 h 30. Il m’a répondu qu’il avait reçu le lien à 16 h 30. Je regarde l’historique des connexions et, effectivement, j’ai une connexion d’un Mac à 16 h 25 utilisant Chrome comme navigateur ! Oui, c’est bien Pierre, mais, surprise, son adresse le localise à Nice alors qu’il m’avait dit qu’il était en déplacement à Paris ! Déduction : Pierre m’a menti mais, Statcounter n’a pas couvert son mensonge. Édifiant ! Vous pourrez en tester la redoutable efficacité. En effet, comme avec le *code source* d’un mail, vos connexions peuvent vous trahir et, surtout, l’exploitation de vos échanges sur Internet n’est pas réservée uniquement à un service judiciaire. N’importe qui peut accéder à votre adresse IP. Une situation assez surprenante au regard de la loi informatique et libertés…

Ainsi, on comprend mieux l’intérêt d’un tunnel VPN. Reprenons le même exemple. Pierre se connecte à votre blog à l’aide d’un VPN dont le serveur d’accès distant est situé en Hollande. La seule information récupérée par Statcounter sera

Ces pages ne sont pas disponibles à la pré-visualisation.

composant électronique sécurisé contenant les données suivantes :

1° Le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance du demandeur ;

2° Le nom dont l'usage est autorisé par la loi, si l'intéressé en a fait la demande ;

3° Son domicile ;

4° Sa taille et la couleur de ses yeux ;

5° Ses empreintes digitales ;

6° Sa photographie.

Le présent article ne s'applique pas au passeport délivré selon une procédure d'urgence.

À propos des intrusions et des attaques informatiques

Article 323-1 du Code pénal

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement

automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 75 000 euro d'amende.

Article 323-2 du Code pénal

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 100 000 euro d'amende.

Article 323-3 du Code pénal

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende.

Sur la détention d'outils ou de programmes permettant de commettre une attaque ou une intrusion informatique

Article 323-3-1 du Code pénal

Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un

instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

À propos de la publicité sur Internet ou par messagerie électronique

Article 20 - Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

Toute publicité, sous quelque forme que ce soit, accessible par un service de communication au public en ligne, doit pouvoir être clairement identifiée comme telle. Elle doit rendre clairement identifiable la personne physique ou morale pour le compte de laquelle elle est réalisée.

À propos de l'utilisation de systèmes de cryptage

Article 11-1 de la Loi n° 91-646 du 10 juillet 1991

Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux agents autorisés dans les conditions prévues à l'article 4, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Les agents autorisés peuvent demander aux fournisseurs de prestations susmentionnés de mettre eux-mêmes en œuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en

Ces pages ne sont pas disponibles à la pré-visualisation.

comparable au NFC mais acceptant des distances plus élevées (jusqu'à 100 m).

Shamoon : Ver informatique qui s'est attaqué, en 2012, à plusieurs compagnies pétrolières saoudiennes.

SIM (Subscriber Identification Module) : Carte à puce utilisée en téléphonie mobile pour y stocker les informations de l'utilisateur et l'identifier sur le réseau GSM.

SMS (Short Message Service) : Service utilisé en téléphonie mobile pour transmettre des textes courts.

Sniffage : Action d'intercepter des données sur un réseau.

SQL : Langage de programmation informatique utilisé pour gérer des bases de données.

SSL (Secure Sockets Layer) *: Protocole de chiffrement utilisé sur Internet pour sécuriser certains échanges comme des transactions bancaires.*

Stéganographie (en informatique) : Art de dissimuler une information dans un fichier informatique.

Stuxnet : Ver informatique, particulièrement complexe, qui aurait été utilisé conjointement par les Américains et les Israéliens pour ralentir le programme nucléaire iranien.

TCP/IP (Transmission Control Protocol/Internet Protocol) : Norme utilisée pour permettre à plusieurs appareils de se connecter entre eux au sein d'un réseau informatique.

Tethering : Technique permettant de relier deux appareils entre eux et d'utiliser les avantages de l'un pour le bénéfice de l'autre. Ainsi, le *tethering modem* permettra d'utiliser son téléphone mobile comme modem d'accès à Internet pour son

ordinateur portable ou sa tablette tactile.

TLS (Transport Layer Security) : Nouvelle appellation du protocole SSL.

Tweet : Format de message utilisé par l'application Twitter.

Tweetonaute : Utilisateur de l'application Twitter.

Trojan : Programme informatique malveillant conçu pour exécuter des actions à l'insu de l'utilisateur.

URL (Uniform Resource Locator) : Chaine de caractères utilisée pour spécifier l'adresse d'un site Internet.

Rançonnage (ransomware en anglais) : Technique qui consiste à crypter les données d'un utilisateur puis à lui demander le versement d'une somme d'argent pour les déchiffrer.

Retweet : Action de relayer un message de l'application Twitter.

Rogue : Fausse application de sécurité qui simule une alerte sur votre ordinateur afin de vous inciter à télé-charger un logiciel payant pour l'éradiquer.

Shutdown : Arrêt d'un serveur informatique.

Spyware : Logiciel malveillant destiné à surveiller l'activité d'un utilisateur à son insu.

SRTP (Secure Real-time Transport Protocol) : Système de chiffrement de la voix utilisé en VoIP.

VoIP (Voice over IP) : Transmission de la voix sur Internet.

VPN (virtual private network) : Réseau virtuel privé permettant d'échanger de manière sécurisée des données sur Internet via une technique dite de tunnel où chaque *paquet*

est transmis de manière chiffrée.

WEP (Wired Equivalent Privacy) : Algorithme de sécurité utilisé pour chiffrer les réseaux Wi-Fi. Ce protocole, très vulnérable aux attaques informatiques, est désormais obsolète.

WPA (Wi-Fi Protected Access) : Algorithme de sécurité utilisé pour chiffrer les réseaux Wi-Fi en remplacement du WEP.

WPA2 (Wi-Fi Protected Access 2) : Seconde génération de WPA utilisant des clefs de chiffrement plus complexes. Le passage du WPA au WPA2 n'exige qu'une mise à jour logicielle contrairement au passage du WEP au WPA qui sollicitait un changement matériel.

ZRTP (Zimmermann Real-time Transport Protocol) : Système de chiffrement utilisé en VoIP et mis au point par l'informaticien américain Philip Zimmermann.

Table des matières