A N D S I

Association Nationale des Directeurs des Systèmes d'Information

www.andsi.fr

Sécurité des réseaux : cybercriminalité
Menaces – Tendances – Nouveaux risques sur Internet
Compte rendu de la présentation du 14 juin 2016, à la Maison des Polytechniciens

Compte rendu rédigé par Laure MUSELLI & ANDSI

En bref…

Xavier AGHINA, expert en cybersécurité chez Orange Labs, aborde la question de la cybercriminalité et explique quelles sont les nouvelles menaces auxquelles les entreprises s'exposent aujourd'hui. Il revient notamment sur les risques liés à un système ouvert sur l'extérieur et présente les enjeux existant autour de la sécurité des objets connectés. Il dresse ensuite un panorama des différents business models qui structurent la cybercriminalité au cœur du web profond, avant de détailler quelques exemples d'attaques et de formuler quelques conseils pour s'en prémunir.

La cybercriminalité : de quoi parle-t-on ?

Aujourd'hui, les petites entreprises comme les grands groupes sont confrontés à la cybercriminalité, qui devient la criminalité du XXIème siècle et de l'ère quaternaire du numérique.

Plusieurs éléments facilitent cette cybercriminalité, parmi lesquels on trouve principalement :

- La convergence vers le tout IP, qui met fin au cloisonnement jadis protecteur entre les protocoles réseau
- De nouveaux usages, comme le nomadisme, qui entraînent une connexion permanente à un réseau à partir d'un terminal mobile ou « device »
- Un nombre croissant d'échanges dématérialisés d'argent et de biens de valeur
- La disponibilité en ligne d'informations techniques permettant de mener des attaques, et l'explosion du nombre de hackers (*black hat*)

La sécurisation reste difficile, pour plusieurs raisons :

- Tout d'abord, la **composante humaine** d'une entreprise et de son système d'information, par définition vulnérable, surtout lorsque les employés ne sont pas sensibilisés aux risques encourus lors de leurs différentes actions. Cet effort de sensibilisation reste primordial.
- Ensuite, les attaquants bénéficient d'un **fort sentiment d'impunité**, avec notamment des législations difficilement applicables et des moyens limités face au nombre d'attaques.
- Enfin, le fait que la **sécurité soit vue par les métiers comme un frein à l'innovation** et à tout nouveau projet. L'enjeu consiste donc à concilier sécurité, ergonomie et développement des usages.

La cybercriminalité se décompose en deux catégories :

- D'une part, les **crimes traditionnels** tels que le blanchiment d'argent, le vol d'identité, la fraude par marketing de masse, qui utilisent la **technologie en tant que nouvel instrument**.

- D'autre part, les **crimes ayant la technologie pour cible**, comme les réseaux de zombies, les logiciels malveillants ou les dénis de service distribué.

La cybercriminalité vise aussi bien les individus, dont on attaque l'identité, l'intimité ou le patrimoine financier, les entreprises, dont on cible la propriété intellectuelle, l'image et l'e-réputation, le patrimoine financier, ou dont on sabote les systèmes de production (SCADA- commande de process industriels), ou enfin l'Etat lui-même et sa souveraineté, pouvant être attaqués par des réseaux d'activistes.

Internet ; entre résilience et fragilité

La dépendance à l'Internet est aujourd'hui de plus en plus grande, avec 3,5 milliards de postes connectés en 2015, soit 43% de la population mondiale, et une croissance de 300% entre 2009 et 2015.

Le réseau repose aujourd'hui sur des câbles sous-marins, avec des réseaux en boucle qui font que les paquets peuvent emprunter un chemin différent en cas de coupure, ce qui confère à Internet une grande capacité de résilience.

De nombreuses affaires ont récemment mis en évidence la fragilité de l'Internet, qui est un objet encore très jeune malgré les transformations sociétales conséquentes qu'il induit, et les enjeux autour de son contrôle. Au-delà de l'émergence des **Bitcoins** et de l'activisme (musulman) d'**Anonghost**, l'affaire **Snowden** a par exemple eu un impact certain sur les activités de normalisation, avec la création, à l'IETF, de groupes de travail autour de la mise en place des protocoles sécurisés.

La **Loi de Programmation Militaire** vise, pour sa part, à permettre la mise sur écoute d'une box sans passer par un juge.

La **Neutralité du Net** est également un enjeu, certains opérateurs étant favorables à la mise en place d'un internet à plusieurs vitesses, alors que Bruxelles s'y opposerait plutôt.

Enfin, des initiatives visant à créer un **code de déontologie pour Internet** voient le jour, à l'instar de celle lancée par Lawrence Lessig.

L'IP et la transformation des risques pour l'entreprise : du château fort à l'aéroport à sécuriser

Grâce à l'IP, l'entreprise s'est transformée, en multipliant les contacts avec l'extérieur. L'architecture qui s'apparentait autrefois à un château fort où une seule porte d'entrée et une seule porte de sortie permettaient un contrôle fort, se transforme en aéroport par lequel transitent une grande quantité d'acteurs, à un rythme élevé. Concrètement, au réseau local s'est ajouté un réseau privé inter-sites, puis une connexion à l'internet et aux réseaux publics, afin d'échanger avec clients et partenaires, mais aussi employés en télétravail et en mobilité, à travers de nouveaux terminaux.

Les applications data centers et les clouds privés, hybrides et publics se sont développés. L'Open Data et l'Internet des Objets font également leur apparition, avec leur lot de problématiques de sécurité. A tout cela s'ajoute une nécessité de simplification des procédures d'accès pour les utilisateurs. L'enjeu pour cette nouvelle architecture consiste alors à garder un niveau de sécurité et de confiance forts, qui deviennent un souci pour les employés et utilisateurs.

Cloud Computing et sécurité

Le Cloud implique toujours plus de produits, de collaborations, de séparation des tâches et de problématiques. Lorsque l'on ne possède pas de cloud privé, c'est le SLA (Service Level Agreement) qui constitue le seul élément de confiance, qui reste toute relative et dépend du fournisseur. Par exemple, il faut savoir que malgré les clauses de suppression des données, celles-ci ne disparaissent généralement pas immédiatement du cloud lorsqu'elles sont supprimées, compte tenu des politiques de réplication et de sauvegardes incrémentales.

Internet des Objets (IoT) et sécurité

GFK, une société d'études, prévoit, pour la France, 2 milliards d'appareils intelligents avant 2020, et d'autres prévisions envisagent le port d'une quinzaine de capteurs par personne.

Concrètement, tous les services, tels que les transports, le commerce de détail, la santé, l'industrie, la domotique, la sécurité & surveillance ou l'infrastructure intelligente sont couverts, avec un déploiement plus ou moins important. La problématique en termes de sécurité concerne le fait que les industriels vendent des boîtes, mais ne se préoccupent que très peu de sécurité. Il s'agit en effet d'équipements de moins de 50 euros en général, qui ne peuvent pas être mis à jour. De ce fait, **si une faille est intégrée dans l'un de ces équipements, elle y sera à vie**.

On commence aujourd'hui à voir les premiers exemples de délits liés à ces objets connectés.

Les jouets connectés sont touchés. VTech, dont le code a été piraté, a vu les photos prises par les enfants et stockées sur le cloud récupérées par des pirates.

Dans le secteur du domicile connecté, Samsung avait mis en place la reconnaissance vocale sur ses télévisions connectées, avec une voix analysée non pas en local, mais sur le cloud de Samsung. Des pirates ont réussi à se servir de ce système pour écouter les conversations, voire espionner les utilisateurs, si leur télé était équipée d'une caméra. Le babyphone a également subi ce type d'attaque, avec des pirates parlant à l'enfant pendant son sommeil. Dans les deux cas, la faille était liée à une option ou un mot de passe activés par défaut. Un réfrigérateur connecté a également servi de relai de spams, car le constructeur l'avait équipé d'une suite Unix et d'une messagerie complète, à laquelle les pirates pouvaient se connecter.

Ces attaques deviennent plus graves lorsqu'elles concernent des équipements de santé comme les pompes à insuline et les pacemakers, ou des armes, car c'est à l'intégrité humaine qu'on peut alors s'attaquer. Jusqu'à une date récente, un pacemaker pouvait être reconfiguré sans l'aide du médecin. Aujourd'hui, un certificat est nécessaire pour réaliser cette action, comme c'est également le cas pour les passeports. De nombreux objets connectés fonctionnent cependant toujours sans certificats, comme les Pass Navigo, sur lesquels on peut lire les derniers déplacements de la personne. Des armes sont également pilotables en wifi à distance, et cela sans sécurité.

Enfin, dans le secteur des transports, la voiture connectée possède de nombreux points de connexion par lesquels in est possible d'atteindre le véhicule. BMW a été victime d'une faille permettant d'ouvrir la voiture et de la démarrer à partir d'un simple téléphone mobile. L'entreprise a toutefois réussi à reconfigurer le logiciel embarqué très rapidement, car les voitures étaient connectées en 3G ou 4G, mais cet exemple montre que l'analyse de risques n'a pas encore été correctement réalisée en ce qui concerne la voiture connectée.

L'Open Web Application Security Project a développé une thématique spécifique concernant l'Internet des Objets, destinée à fournir des recommandations en ligne sur la sécurisation des objets.

Une nécessaire politique de cybersécurité et de cyberdéfense

Au sein des entreprises, la problématique de la sécurité doit donc être prise en compte, ce qui nécessite un budget non-négligeable. Il s'agit donc, pour un DSI ou un RSSI, d'effectuer un chiffrage des conséquences d'une interruption de son système, afin de financiariser le risque et de justifier auprès d'un directeur financier tout achat de matériel destiné à assurer la sécurité du système. Ainsi, on sait qu'Amazon réalise 83 000 $ de ventes par minute, ce qui fournit une indication de la perte occasionnée par une interruption liée à une attaque.

Les aspects juridiques doivent eux aussi être étudiés, dans la mesure où le droit qui s'applique à Internet est celui du pays où Internet est installé. Si les droits sont assez semblables au sein de la communauté européenne, les politiques d'informatique et des données peuvent varier de façon importante en fonction des pays. Ceci n'est pas sans conséquence pour des entreprises qui possèdent des équipements dans des pays étrangers.

Dans ce contexte, la **CyberSécurité** s'avère cruciale, « *afin de permettre au système d'information de résister à des événements issus du cyberspace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou rendent accessibles* » (définition de l'ANSSI). Pour cela, elle repose sur des techniques de sécurité des systèmes d'information, mais aussi sur la mise en place d'une **CyberDéfense**, c'est-à-dire « *la mise en place d'un ensemble de* ***mesures techniques mais aussi non-techniques*** *permettant la défense dans le cyberspace des systèmes d'information jugés essentiels* » (ANSSI). La cyberdéfense ne peut en effet être limitée qu'à l'utilisation d'outils, et une PSSI (Politique de Sécurité des Systèmes d'Information), document d'entreprise présentant les besoins en sécurité de l'entreprise et documentant sa politique de sécurité doit être produite.

Tour d'horizon de la cybercriminalité

Le web profond

Le web profond, représente 90% du World Wide Web. Il représente la partie non-indexée par les moteurs de recherche tels que Google, qui ne recherchent que les liens hypertextes et ne prennent pas en compte les bases de données dynamiques, les serveurs et les forums.

L'accès au web profond peut se faire via des logiciels spécifiques tels que ToR (The Onion Router), clients de navigation à installer sur les navigateurs, qui permettent de faire de la navigation internet anonyme. Leur principe consiste à séparer identification et routage, de façon à dissimuler l'activité du réseau de surveillance. Il faut toutefois

savoir que les principaux moteurs ayant permis de créer le réseau ToR sont Google et le Département de la Défense Américaine, ce qui laisse planer un doute sur le caractère totalement anonyme de la navigation.

Il existe des moteurs de recherche distincts pour naviguer sur le DeepWeb et sur le DarkWeb :

- L'accès au **DeepWeb**, sur lequel s'opère la petite délinquance du Web, se fait par des logiciels tels que la WWW Virtual Library, Yippy, Surfwax, IceRocket, Stumpedia, Freebase ou TechDeepWeb.
- Pour le **DarkWeb**, repaire de la grande délinquance, on utilisera Onion.City, Not Evil ou Memex Web profond Search Engine.

Dans les deux cas, compte tenu des attaques importantes dont les machines font l'objet dans le web profond, il est conseillé d'utiliser une VM pour la navigation.

Les business models de la cybercriminalité

Sur ce web profond, de véritables business models se développent autour d'activités illicites. A la manière des sites marchands classiques, ces sites publient des grilles de tarifs assez sophistiqués, en fonction des multiples produits et services fournis, et utilisent même, pour certains, des systèmes de notation des commerçants. La richesse de cette offre s'explique par l'importante demande qui leur est adressée.

On trouve de nombreuses boutiques en ligne telles que Silk Road ou Blackmarket, qui vendent une large gamme de produits illicites et n'acceptent que des Bitcoins. Elles sont régulièrement fermées par le FBI, mais rouvrent sous d'autres formes. On trouve également des passeports, des cartes d'identité et des cartes de crédit, qui font l'objet de cotations en fonction de leur origine et de leurs caractéristiques, mais aussi des billets de banque contrefaits vendus à un quart de leur valeur ainsi que des armes. De nombreux sites proposent pour leur part du blanchiment d'argent via des jeux en ligne et des virements bancaires effectués par des « mules » recrutées par les sites et prélevant une commission.

Un grand nombre d'activités illicites du web profond sont alimentées par des données obtenues frauduleusement en valorisant les failles de sécurité dans les systèmes. Les canaux d'entrée les plus rencontrés sont les **attaques techniques par canal web** sur une faille existante et l'ingénierie sociale, c'est-à-dire des **mails de phishing** permettant d'obtenir des droits par rebonds successifs.

Des **business models** se développent autour de ces activités. On peut citer entre autres la location de botnet, la vente de faille via un escrow, la vente en gros de bases de données bancaires, ou encore la vente de kits d'hameçonnage (phishing) à installer sur un serveur pour réaliser une campagne qui permettra de récupérer des données à vendre à l'unité.

On assiste finalement à la constitution de **chaînes de valeur virtuelles** aux multiples intermédiaires à destination de l'économie réelle, **permettant la monétisation de ces activités illégales**. L'approvisionnement se fait auprès des hackers, développeurs de malware et personnes pratiquant l'hameçonnage, pour alimenter des plateformes de blackmarket. Ces infrastructures de support permettent :

- La création de monnaie virtuelle que des intermédiaires (moneymules) vont se charger de blanchir à la façon de sociétés écrans.
- L'achat de produits illégaux tels que données bancaires, faux documents ou botnets et malware, que des cybercriminels vont convertir en argent réel ou en monnaie virtuelle.

Il existe donc une offre diversifiée de services à la demande peu chers allant du spam (autour de 5 euros) à l'attaque DDoS sur une ou plusieurs cibles (entre 20 et 200 euros), en passant par l'installation de Bot (50 euros pour 1000 ordinateurs en Europe), les kits clé en main d'hameçonnage (20 euros), le Multi Scanner permettant de vérifier la non-détection d'un logiciel malveillant par les logiciels anti-virus (30 euros) ou encore le FUD (10 euros). Le FUD est un chiffrement à la demande qui consiste à créer un code malveillant en le brouillant grâce à des méthodes d'obfuscation, c'est-à-dire le rajout de code inutile rendant difficile le reverse-engineering.

Quelques exemples d'attaques

Les attaques astucieuses en environnement web

La dernière attaque astucieuse a concerné l'univers très sécurisé de l'AppStore. Son logiciel de création et de développement des applications a été compromis à l'aide d'un malware installé sur un service chinois de partage de fichiers via des serveurs en mirroring, qui permettait aux développeurs de télécharger plus rapidement que sur le site américain ce qu'ils pensaient être les SDK (Software Development Kit). Les applications générées par ces versions ont été légitimement distribuées sur l'AppStore, alors qu'elles contenaient le malware permettant aux pirates de

capturer des informations sur les appareils infectés, à des fins d'hameçonnage. Il leur était ensuite possible de dérober des mots de passe et d'établir une tête de pont pour d'autres programmes malveillants. Cette attaque a été découverte été Apple a pu régler le problème en générant de nouveaux certificats.

Les distributeurs de billets, pourtant bien sécurisés d'un point de vue physique, ont également fait l'objet d'une attaque astucieuse en Russie. Un malware, installé sur les distributeurs via un CD de boot, permettait de prendre le contrôle du distributeur et de faire sortir les billets. Afin que l'attaque passe inaperçue, seulement une petite somme était retirée sur chaque distributeur, ce qui a permis aux pirates de voler plusieurs millions de dollars.

Les 0-days

Les 0-days sont des failles informatiques existantes, mais non-documentées par l'éditeur, que de potentiels pirates peuvent exploiter discrètement avant que l'éditeur ne s'en aperçoive et développe un patch.

Même Google, qui avait investi d'importantes ressources pour développer **Chrome**, un navigateur que l'entreprise voulait sans faille, a été la cible d'un pirate, qui indiquait avoir trouvé une faille dans le système, a refusé d'en fournir les caractéristiques malgré une prime de 60 000 dollars et a revendu l'information.

Un 0-day a également été découvert sous **Open SSL** en 2014. Open SSL est une bibliothèque de sécurité open source largement utilisée dans les produits de sécurité sur étagère. Il s'agit d'une boîte à outils de cryptographie TLS développée par la communauté open source, qui constitue un service d'infrastructure critique. Une nouvelle version de la bibliothèque avait été lancée en 2012, sans que les vérifications n'identifient la faille. Celle-ci impactait à la fois le serveur et le client, et avait été exploitée pendant deux ans, remettant en cause la sécurité des échanges avec les sites webs, serveurs et smartphones. A la suite de cette découverte, Google, Facebook et Apple entre autres, ont décidé d'employer des ingénieurs pour gérer le code Open SSL.

Pour réduire leur surface d'attaque, les entreprises doivent s'assurer qu'elles fonctionnent avec les dernières versions logicielles. Par exemple, Symantec indique une moyenne de 19 jours d'exposition avant qu'une faille soit découverte, auxquels il faut ajouter 4 jours pour sortir le patch. Cependant, en fonction du système patché, il sera difficile d'obtenir les autorisations d'installation directement. La solution consiste à avoir une machine en mirroring sur laquelle le patch est appliqué et de vérifier si les services continuent à fonctionner correctement. Il sera ensuite possible de l'appliquer directement sur les machines. Pendant ce temps, le système reste toutefois vulnérable à l'attaque.

Les zero-days donnent lieu à plusieurs marchés :

- Des sociétés comme Zerodium ou The RealDeal **revendent de la faille** selon une grille tarifaire qui dépend de la complexité de la cible, de sa surface d'attaque, et de l'acheteur lui-même. Ils ont pour cela recours à une forme de crowdsourcing. Par exemple, Zerodium a proposé en 2015 une récompense d'un million de dollar à la première équipe qui rapporterait une faille sur iOS. Le business model de ces entreprises consiste à acheter de la faille et à la revendre.
- Des **services complémentaires** existent également pour permettre aux entreprises de se couvrir en n'adressant pas directement leurs demandes aux fournisseurs de failles. Ainsi, reprenant le principe de la société écran, des systèmes d' **« escrow payment »** consistent à réaliser le paiement par l'intermédiaire d'une tierce personne.
- Enfin, l'activité de **« bug bounty »** consiste à se faire rémunérer pour identifier des bugs. Chez Google, cette rémunération peut aller de 500 à 50 000 dollars en fonction de la surface d'attaque, et quelques personnes en France vivent de cette activité. Elle tend d'ailleurs à se professionnaliser, avec des plateformes de plus en plus reconnues offrant des services à valeur ajoutée comme Hackerone ou Bugcrowd, et dont les clients sont des sociétés telles qu'Adobe, Twitter, Uber, GitHub ou Dropbox.

Les rançongiciels (ransomware)

Un kit de ransomware coûte environ 250 dollars et peut être accompagné d'une hotline d'aide au développement du rançonciel pour 250 dollars supplémentaires. Ils ciblent à la fois les entreprises et les particuliers, en chiffrant le dossier « documents ». Un message apparaît alors, indiquant qu'un versement est nécessaire pour obtenir une clé de déchiffrement permettant de récupérer les données. Si le degré de sophistication du ransomware est faible, **certains sites, tels que Stopransomware.fr permettent de récupérer les données**. En revanche, si les fonctions de chiffrement utilisées sont en AES 256 ou AES 512, la clé de déchiffrement est quasi-impossible à récupérer.

Pour se prémunir d'une telle attaque, il faut **réaliser des sauvegardes non-connectées très régulières**. Et cela vaut évidemment pour les entreprises, mais aussi pour les particuliers.

Les Botnets

Un botnet est un malware tournant sur un PC et pouvant être piloté à distance, qui pourra être utilisé pour effectuer des demandes de rançon.

Pour éradiquer un botnet, il faut désinstaller le malware sur la machine elle-même. Même si on neutralise les commandes de contrôle des systèmes qui donnent leurs instructions, le malware sera inopérant, mais en sommeil, avec le risque de réveiller l'ensemble du parc ultérieurement. Pour savoir si une entreprise a été affectée par un botnet, il faut **observer le flux DNS**, qui peut révéler des flux bizarres allant sur des serveurs pouvant faire partie d'une liste de serveurs hébergeant des réseaux de botnets. Les botnets sont le fruit de véritables entreprises possédant une organisation et un business model similaires à une entreprise traditionnelle. Elles mettent également en place des stratégies visant à attaquer d'autres entreprises pour récupérer leurs botnets.

Les botnets sont en voie de régression en France.

Stuxnet

Il s'agit d'un malware qui cible les systèmes SCADAs (commande de process industriels), dans lesquels il est introduit par des employés, à leur insu, via une clé USB infectée déposée par les pirates.

Il est nécessaire de mettre en place des campagnes de sensibilisation pour l'ensemble des collaborateurs d'une entreprise, visant à leur faire jeter toute clé USB trouvée quelle qu'elle soit, même estampillée du nom de l'entreprise.

L'expérience montre toutefois que malgré ces campagnes, 80% de clés USB estampillées du nom de l'entreprise sont utilisées, alors qu'une insertion suffit pour infecter le système. La principale faille dans le cas d'une infection par Stuxnet est donc humaine.

Les attaques ciblées

De nombreuses entreprises sont victimes d'APT (Advanced Persistent Threat). Parmi elles, les entreprises de sécurité telles que RSA constituent des cibles privilégiées pour les pirates. Le principe consiste à leur dérober des certificats pour les produits de sécurité utilisés par leurs clients. Diginotar, autre entreprise spécialisée dans la sécurité, a mis la clé sous la porte suite à une attaque de son système informatique qui a entamé sa crédibilité vis-à-vis des clients.

Conclusion

Les **profils des pirates sont divers**, des unités militaires spécialisées à l'adolescent désœuvré, en passant par l'employé malveillant et les activistes politiques tels que les Anonymous. Les plus inquiétants sont probablement les cybergangs et cybermercenaires dont le but est de s'enrichir. Les hackers, pour leur part, sont souvent présentés comme malveillants, alors que certains ont justement pour but de découvrir des failles, afin d'élever le niveau de sécurité des systèmes.

Il existe environ **un bug toutes les 1 000 lignes de code**. Quand on sait que Windows XP comporte environ 45 millions de lignes de code, et un Debian environ 320 millions de lignes de code, on peut dire que tous les OS, même embarqués, possèdent des failles.

Aujourd'hui, posséder un antivirus ne suffit pas. Les antivirus ne sont pas capables de reconnaître une menace inconnue. En entreprise, la question ne se pose pas, car on ne pourra jamais reprocher à un DSI d'investir 150 dollars par an dans un antivirus, et ne pas investir peut lui coûter sa place. A la maison, il est préférable d'en posséder un, mais il ne doit pas donner un faux sentiment de sécurité. De plus, les antivirus gratuits n'offrent pas le même support ou le même service, et il faut donc les utiliser avec une petite méfiance. En tant que particulier, on peut se passer d'antivirus, mais tout dépend en réalité du type d'OS et de la politique de sécurité mise en œuvre localement sur le poste, afin d'effectuer des cloisonnements. **En termes de sécurité, le meilleur livre pour commencer est « L'art de la Guerre » de Sun Tzu.**

Débat

Intervenant : Quelles sont vos recommandations concernant la sécurité des objets connectés ?

Xavier AGHINA : Les éditeurs de solutions informatiques essaient d'utiliser le plus souvent possible les certificats. Pour installer ou réaliser des patches, il faut ainsi montrer patte blanche. Il faut également partir du plus petit élément : avoir un composant hardware de sûreté, c'est-à-dire un secure element ou une carte sim par exemple, sur lequel la sécurité va pouvoir être appuyée ; sur lequel on va pouvoir charger un BIOS, charger un bootloader, charger un firmware, qui va pouvoir charger l'OS. Toute une chaîne de confiance pourra alors se mettre en œuvre, et tant que ce

ne sera pas le cas, le système ne démarrera pas, car il ne se considèrera pas intègre. C'est la seule solution à appliquer. Cependant, un Androïd en embarqué sera très difficile à sécuriser, tout comme un iOS. Il faut également cloisonner tout cela et essayer, pour la direction d'une voiture, par exemple, d'avoir son propre réseau en fibre optique, et laisser au smartphone tout ce qui concerne la consommation d'essence, la musique, la température, à la limite la pression des pneus, mais pas plus. Le conducteur n'a pas besoin d'avoir accès à la direction ou au système de freinage.

Int. : Pourquoi ces gens-là peuvent-ils continuer sévir ? Sont-ils protégés par leurs Etats, ou est-ce le mécanisme qui les empêche de se faire prendre ?

X.A. : Ces gens-là sont surtout très nombreux. Ils se servent de sociétés écrans qui empêchent de remonter à la source. Ils sont très représentés en Russie, mais l'Inde et le Viêtnam commencent également à développer ce genre de pratique.

Présentation de l'orateur

Xavier AGHINA est expert en cybersécurité chez Orange Labs.

Dans le département sécurité chez Orange Labs, Xavier AGHINA conduit des projets techniques et un programme de recherche sur le paiement mobile et la protection des objets connectés. Son objectif principal est de concevoir et de mettre en œuvre des solutions de sécurité. Il fournit également un soutien actif et de conseils dans les domaines d'audit de sécurité, l'analyse des risques, l'évaluation de la vulnérabilité et des recommandations. Il anime des formations à Telecom ParisTech ainsi que des séminaires de sensibilisation à la sécurité IT en entreprise.