L'Internet des objets : un nouveau champ d'action pour la cybercriminalité

L'observation de la cybercriminalité et des différentes formes d'abus dans l'utilisation des technologies numériques a montré au cours des dix dernières années que les activités illégales ne se contentaient plus d'un rôle marginal dans l'univers numérique, mues par des mobiles touchant à l'appropriation financière ou à l'appropriation informationnelle. L'émergence d'un Internet des objets en tant que support des activités humaines doit évidemment nous amener à prendre en compte ce type de risque, d'autant plus que les conséquences en sont encore difficiles à évaluer, ne serait-ce que par l'ampleur d'une telle évolution (le nombre des objets, des réseaux qui interagissent, des nouveaux usages étant considérable). C'est donc une multitude d'axes de recherche en matière de sécurité qui doivent être ouverts ou soutenus, y compris ceux qui permettront de tirer profit de ces nouvelles technologies pour améliorer la sécurité.

Par **Éric FREYSSINET***

En matière de cybercriminalité, il faut en permanence observer les nouvelles technologies et les nouveaux usages, parce que les auteurs d'infractions – mais aussi leurs victimes – les maîtrisent toujours très vite et en exploitent les faiblesses ou les forces, pour faire émerger de nouvelles façons de réaliser des infractions qu'elles soient classiques ou de type nouveau. Mais les nouvelles technologies peuvent aussi être l'occasion de développer de nouveaux modes de collecte des preuves des infractions commises. Enfin, il faut toujours garder un œil dans le rétroviseur et ne pas oublier les enseignements tirés du passé.

Nous verrons que c'est particulièrement vrai lorsque l'on considère les évolutions que devraient permettre les technologies que l'on regroupe sous l'intitulé d'*Internet des objets* : il y aura de nouvelles opportunités pour tous, mais, malheureusement, y compris pour les activités criminelles.

* Lieutenant-colonel de gendarmerie, coordinateur du plateau d'investigation Cybercriminalité & Analyses Numériques (CyAN) du pôle judiciaire de la gendarmerie nationale.

Nous nous attarderons tout d'abord sur quelques leçons tirées du passé, puis nous envisagerons des nouvelles formes possibles de délinquance et, enfin, nous détaillerons la façon dont l'Internet des objets pourrait ouvrir la voie au développement de criminalités existantes ou émergentes.
Bien entendu, comme toute analyse de risques et de menaces, ce texte ne remet pas en cause l'intérêt du développement de ces technologies.

DES OBJETS DE PLUS EN PLUS COMMUNICANTS

La notion d'Internet des objets n'est pas le résultat d'une évolution complètement abstraite ou inopinée, elle repose pour beaucoup sur le développement progressif d'un nombre croissant d'objets qui communiquent et/ou interagissent entre eux et qui sont de plus en plus présents dans notre environnement ; cette tendance ne date pas d'hier.
Le plus emblématique de ces objets, pour les Français, est sans doute la carte à puce, un objet que nous avons tous dans notre portefeuille et qui utilise un protocole de communication simple, mais efficace, pour dialoguer localement avec un terminal de paiement ou un distributeur de billets, mais qui, en réalité, dialogue indirectement avec un serveur qui va valider les transactions, en temps réel ou en temps différé. Certaines de ces cartes contiennent même un serveur Web (c'est par exemple le cas des modèles de cartes utilisant la technologie JavaCard). Évidemment, de par les applications qu'elles permettent (paiement électronique, support de données personnelles...), toutes les générations de cartes à puce ont fait l'objet de tentatives réussies ou non d'en abuser (contrefaçon de cartes bancaires, de cartes de téléphone à péage, ou encore conception de dispositifs de décodage des émissions télévisées payantes…). À chaque fois, des contre-mesures ont dû être implémentées.
Au passage, mentionnons qu'un des aspects intéressants des fraudes qui ont pu être constatées est le fait que, de plus en plus, elles exploitent l'ouverture croissante des standards technologiques, comme certaines méthodes de rétroconception utilisées pour comprendre le fonctionnement de certains systèmes (des données techniques confidentielles) et assurer le partage public des résultats obtenus. Ainsi, dans l'exemple récent de la mise en cause de la sécurité des cartes bancaires sans contact (dites NFC, en raison du nom des technologies de communication utilisées, les *near field communications*), notamment sur le plan de la protection des données personnelles, ce sont avant tout les spécifications publiques de ce protocole qui ont permis de découvrir les vulnérabilités potentielles desdits supports de paiement. En tout état de cause, l'information est de plus en plus facilement accessible et notamment pour ceux qui auraient de mauvaises intentions. Il est donc essentiel d'adapter le temps de réaction à la découverte des vulnérabilités découlant de cet état de fait.
Badges de télépéage, puces d'identification par radiofréquences (étiquettes RFID passives pour la gestion de stocks, la prévention des vols...) sont autant d'éléments supplémentaires de vulnérabilité attachés à nos véhicules ou aux objets que l'on achète, dans notre environnement de travail ou familial. Pour chaque situation, il a pu y avoir des tentatives de les contourner, par exemple en les copiant, en les désactivant ou en les rendant inopérants. Parfois, les méthodes employées sont assez basiques, comme le papier aluminium alimentaire ou le four à micro-ondes qui sont couramment utilisés... Mais, plus récemment, on a vu apparaître des sortes de brouilleurs utilisés par des voleurs pour neutraliser les puces RFID des articles en rayon dans les magasins.
Dans le même ordre d'idée, les automobiles ont, dès le début des années 2000, intégré de plus en plus d'électronique pour contrôler l'accès à l'habitacle ou faciliter le diagnostic technique du garagiste. Ces technologies sont très communicantes. Elles utilisent un réseau local (CAN – *Controller Area Network*) dédié au dialogue entre les calculateurs et les capteurs du véhicule, des clés de contact sans contact ! (avec, pour les plus récentes, détection de leur position exacte à l'intérieur ou à l'extérieur du véhicule) et des communications *via* les réseaux de téléphonie mobile et de radio pour obtenir des informations sur le trafic et permettre non seulement aux utilisateurs de communiquer, mais aussi au véhicule lui-même pour certains modèles de voiture grâce au système embarqué (appels de secours, positionnement du véhicule, diagnostic à distance, etc.). Dans ce contexte, les voleurs n'ont pas tardé à recruter des électroniciens et développer toutes sortes de méthodes pour contourner ces sécurités ou les exploiter à leur profit pour prendre le contrôle du véhicule de façon sophistiquée.
Les ordinateurs portables, les téléphones mobiles et autres tablettes numériques sont autant d'objets communicants qui ont envahi notre quotidien. Quelle que soit l'avancée des technologies de communication existantes, elles ont toutes fait l'objet d'attaques : le protocole très local Bluetooth – sensible parfois à des interceptions de communication –, fut un des premiers vecteurs de diffusion de virus sur les téléphones mobiles ; les protocoles de réseaux sans fil Wifi dont la sécurité a été souvent mise à mal – ce qui n'empêche pas que de nombreuses connexions continuent encore aujourd'hui d'être établies en clair, ou bien encore, évidemment, les protocoles de téléphonie mobile qui ont récemment suscité un vif intérêt chez les chercheurs en sécurité.
L'environnement industriel a lui aussi suivi cette tendance générale. Du centre de recherche au site de production, tous les systèmes sont évidemment en réseau. Cela a permis de faire progresser les méthodes de

supervision, comme la gestion des commandes des chaînes de production. Mais cela a aussi introduit un nouveau potentiel pour des attaques. On ne compte plus les publications – scientifiques, ou plus simplement journalistiques – qui dénoncent la faiblesse de la protection des SCADA (1) – les systèmes de commande industriels – et leur trop grande présence sur Internet, à la portée du premier attaquant qui les découvrirait.

LA VULNÉRABILITÉ DE L'INTERNET DES OBJETS : AVANT TOUT, UNE PROBLÉMATIQUE DE SURFACE D'ATTAQUE…

Les progrès techniques s'accompagnent donc (inexorablement ?) d'un développement des attaques ou, en tous les cas, d'une plus forte probabilité de celles-ci : l'augmentation de la surface d'attaque, c'est-à-dire du nombre des systèmes connectés, et la variété des moyens qui leur permettent de communiquer augmentent mécaniquement les possibilités d'attaques, quand, en parallèle, le nombre des personnes susceptibles de réaliser ces attaques augmente certainement proportionnellement à l'accroissement de la population connectée, dans chaque pays et dans le monde.

On a bel et bien constaté l'effet de cette dimension purement quantitative des choses sur le nombre des victimes d'infractions commises en ligne (comme en témoigne la croissance difficilement maîtrisée des fraudes dans les paiements bancaires effectués *via* Internet).

Cet effet est multiplié par une évolution des usages. Ainsi, non seulement ce que l'on appelle l'Internet dans les nuages (*cloud computing*, en anglais), mais aussi l'augmentation de la capacité des outils communicants et le développement d'un nombre exponentiel d'applications incitent tout un chacun à stocker des informations personnelles (ou les secrets de son entreprise) en plus grand nombre, à les partager ou encore à les déposer, à distance, sur des serveurs.

Le constat que font les chercheurs en sécurité sur l'avènement du protocole IPv6, qui va permettre de connecter des milliards d'objets à travers la planète grâce à un nombre beaucoup plus important d'adresses possibles, est que ce protocole présente autant de failles, et souvent les mêmes, que celles que l'on connaissait avec l'IPv4. Il semble que nous soyons incapables de retenir les leçons du passé… Il se pourrait même que l'IPv6 apporte ponctuellement quelques risques supplémentaires, au travers de ces équipements dont la connectivité IPv6 est activée par défaut, alors que les dispositifs de sécurisation des réseaux dans les entreprises ne prennent pas encore en compte ce protocole.

Et c'est bien là un des risques les plus importants, la multiplication d'objets connectés dont on n'aurait pas perçu l'importance – on l'a déjà vu pour les SCADA –, alors qu'en sera-t-il de tous les autres objets, en apparence bien plus anodins ? Ils risquent de multiplier les portes d'accès vers l'information et vers les systèmes d'information des organisations, sans qu'il soit toujours envisagé de les prendre en compte dans les politiques de sécurité. C'est d'ailleurs là le principal problème que soulève à mes yeux la question du BYOD, ce *bring your own device* : l'introduction de systèmes extérieurs que l'on maîtrise mal et qui ont peu ou prou accès au système d'information des organisations. Qu'en sera-t-il des véhicules des sociétés, des stocks en cours de transport ou des milliers d'interrupteurs, de capteurs, de caméras... ? Leurs interactions avec de nombreux autres systèmes, comme celles aujourd'hui de nos ordinophones, pourraient être autant de portes d'entrées.

Enfin, une autre des tendances actuelles est que ces nombreux objets sont de plus en plus souvent jetables. On les déploie, car ils sont peu chers et permettent de rendre immédiatement un service efficace, puis ils sont ensuite oubliés, abandonnés, contenant parfois des informations qui restent sensibles ou laissent ouvertes de multiples portes vers l'intérieur des réseaux.

Ainsi, aura-t-on à l'esprit, par exemple, de désactiver systématiquement l'accès d'une nuée de micro- ou de nano-robots que l'on aura déployés pour nettoyer ou explorer un site ? Pensera-t-on à effacer ou à révoquer leurs certificats de sécurité ? Saura-t-on construire les référentiels complets de ces déploiements, ou se contentera-t-on de les considérer comme inutiles au regard de la courte durée de vie des systèmes mis en œuvre ?

… MAIS AUSSI DE NOUVEAUX TYPES D'ABUS POSSIBLES

Les nouveaux enjeux sécuritaires sont tout aussi intéressants à examiner. Le premier est le corollaire de ce que nous venons d'évoquer dans le paragraphe précédent : l'Internet des objets pourrait entraîner la tentation de déployer des systèmes moins sécurisés pour remplir les mêmes besoins qu'auparavant.

On le voit, par exemple, avec l'arrivée de certains dispositifs de paiement par carte bancaire, qui se contentent d'être un adaptateur ajouté à un terminal mobile (tablette ou téléphone), alors que l'on a fait d'énormes progrès dans la sécurisation des terminaux de paie-

(1) De l'anglais *Supervisory Control And Data Acquisition (CSADA)* : ces dispositifs sont destinés à la surveillance, à la supervision et au contrôle à distance de systèmes industriels. Ce sont des interfaces permettant aussi bien d'accéder à l'état d'un système (données mesurées, images,...) que de lui transmettre des ordres.

ment. Certains réseaux ou nouveaux modes de commercialisation pourraient être tentés d'opter pour ces solutions moins coûteuses et qui, paradoxalement, paraissent plus modernes.

Les *botnets*, ces réseaux reposant sur la prise de contrôle d'un nombre plus ou moins grand de systèmes compromis et utilisés pour commettre une grande variété d'activités illégales, pourraient connaître un nouveau terrain d'application avec l'Internet des objets, ce qui est d'autant plus inquiétant si ces systèmes sont mal sécurisés ou difficilement sécurisables. Les *botnets* sont d'ores et déjà en train de prendre pied de manière patente dans les réseaux de téléphonie mobile, et ils ne manqueront pas d'exploiter ces nouveaux espaces.

Le second risque de l'Internet des objets est plus intrinsèquement lié aux nouveaux objets : ils créent de nouvelles formes de communication qui n'ont pas encore été toutes testées ou dont la sécurisation n'est pas totalement aboutie. Ainsi, la recherche est particulièrement active sur les méthodes de sécurisation des communications dans les réseaux de type MANET (2) (vérification des certificats, révocation des certificats des objets auxquels on ne fait plus confiance, etc.).

Autre inquiétude : lorsqu'il s'agira de construire des réseaux grâce auxquels l'ensemble des véhicules, des feux tricolores et des systèmes de mesure du trafic communiqueront entre eux pour échanger énormément d'informations, aura-t-on auparavant testé toutes les configurations ? Que se passera-t-il lorsqu'un seul de ces objets interconnectés transmettra des informations erronées ? Ou si toute une gamme d'objets de la même série en faisait de même ? Quels sont les risques d'une atteinte non accidentelle portée à ce genre de configuration, alors que l'on sait pertinemment que dans l'univers bien mieux connu des systèmes informatiques classiques, on découvre toutes les semaines de nouvelles vulnérabilités et qu'elles sont exploitées de façon massive dans la plus grande anarchie ? Ce sont là autant de préoccupations qui doivent être prises en compte lors de l'étude des décisions concernant la conduite des véhicules ou la gestion du trafic.

Plus généralement, enfin, ce sont les détournements des fonctions permises par ces nouveaux usages qui doivent être envisagés. Ainsi, par exemple, la surveillance du transport de marchandises *via* un système d'étiquetage électronique pourrait être détourné par des groupes criminels organisés pour faciliter l'accomplissement de leurs méfaits en identifiant rapidement les transports les plus intéressants (notamment au regard du nombre et de la nature des produits transportés).

CONCLUSION

Il ne faut donc pas en douter, la cybercriminalité sera présente dans l'Internet des objets, c'est ce que nous enseignent les exemples du passé, comme l'actualité récente. Comme pour toutes les évolutions technologiques, il ne faut surtout pas que cette perspective en freine le développement, mais il faut prendre en compte, dès la conception des systèmes, ces risques nouveaux qui sont de plus en plus présents.

Et ne nous y trompons pas, autant il était raisonnable de considérer que les activités illégales dans l'univers numérique restaient anecdotiques, ou seulement émergentes dans les années 1990, autant la leçon que nous apportent les dix dernières années est que ces activités illicites sont une partie intégrante du développement technologique d'aujourd'hui.

Partant de ce constat, il ne faut plus se contenter d'utiliser à la marge les technologies de l'Internet des objets pour protéger les activités légitimes contre des activités criminelles ou envisager de sécuriser les activités classiques grâce aux technologies de l'Internet des objets.

Mais nous devons inventer de nouveaux usages. Il est possible, par exemple, d'imaginer des objets de confiance qui effectueraient des sortes de patrouilles numériques sous le contrôle de ceux qui sont chargés de la sécurité des systèmes ou même sous le contrôle des services de police. Ces objets obéiraient évidemment à des règles de transparence et de respect de la vie privée adaptées, mais ils seraient nettement plus efficaces qu'une observation totalement extérieure telle qu'on la réalise aujourd'hui.

(2) Les *Mobile Ad Hoc Networks* sont des réseaux IP construits dynamiquement sur la base d'objets mobiles.