XXXIV UNIVERSITAT D'ESTIU D'ANDORRA
DEL 4 AL 7 DE SETEMBRE DEL 2017

Sessió del 5 de setembre del 2017

Bienvenue dans l'ère du « Janus numérique » : formidable outil de développement et arme offensive surpuissante

Nicolas Arpagian

Director científic del cicle «Seguretat digital»
a l'Institut Nacional d'Alts Estudis de la Seguretat i de la Justícia (INHESJ)
Director de l'estratègia d'Orange Cyberdefense

Director científico del ciclo «Seguridad digital» en el INHESJ.
Director de estrategia de Orange Cyberdefense

Directeur scientifique du cycle « Sécurité numérique » a l'INHESJ.
Directeur de stratégie d'Orange Cyberdefense

Per citar aquest article / Para citar este artículo / Pour citer cet article :

ARPAGIAN, Nicolas. « Bienvenue dans l'ère du "Janus numérique" : formidable outil de développement et arme offensive surpuissante » [en línia], a: Universitat d'Estiu d'Andorra (34a : 4 - 7 set., 2017 : Andorra la Vella). *Tecnologia i humanitat, llums i ombres = Tecnologia y humanidad, luces y sombras = Technologie et humanité, lumières et ombres*. Andorra: Govern d'Andorra. Ministeri d'Educació i Ensenyament Superior. Universitat d'Estiu d'Andorra, 2018, p. 49-56 (978-99920-0-857-7) <http://www.universitatestiu.ad/UEA2017>

La consommation numérique est universelle : elle affecte toutes les générations, ignore largement les frontières géographiques et se joue des anciennes barrières qui voulaient que les sphères privées et professionnelles ou que les mondes civils et militaires soient considérés de manière fort distincte. Les processus de création et de diffusion de la connaissance se trouvent remis en cause. Avec l'avènement d'une logique de plus en plus coopérative et la difficulté à faire valoir les droits historiques de la propriété intellectuelle dès lors que les informations s'échangent et se partagent à l'échelle planétaire sans véritables obstacles techniques. Les créatifs se trouvent en position défensives, misant sur une combinaison de technologies et de droit pour obtenir le pistage de leurs œuvres artistiques ou techniques et le respect de leurs droits d'auteur. Ce qui veulent accéder à l'information à valeur ajoutée (films, romans, chansons, articles de presse ou analyses à usage professionnel) ayant de plus en plus de difficultés à concevoir la nécessité de rémunérer ce travail de l'esprit. Persistant à croire que sa duplication sans frais n'affecte pas le patrimoine de son auteur légitime. Même si les offres d'abonnements comme Netflix, Deezer ou Spotify commencent à inculquer la notion de prix – on ne parle pas encore de valeur – de ces fichiers informatiques qui sont désormais le support de notre consommation numérique.

La transformation numérique est une dynamique de haute intensité : sans réelle formation préalable les consommateurs se sont saisis de leurs smartphones et de leurs connexions haut débit pour ponctuer leurs décisions quotidiennes : chercher un avis sur un artisan, effectuer des transferts bancaires, correspondre avec leurs proches, se renseigner sur une maladie, préparer un voyage, rencontrer l'âme sœur ou postuler à un nouvel emploi. Le réseau des réseaux s'est donc imposé comme la porte d'entrée naturelle pour débuter la plupart des activités humaines. Au point que cette consultation en direct des informations disponibles à tous moments sur la Toile devient un préalable qui se retrouve dans nombre de démarches de la vie professionnelle.

Dans le même temps, les instances économiques, administratives et même militaires ont généralisé la numérisation de leurs processus internes. Les systèmes d'information devenant à la fois la colonne vertébrale qui soutient l'architecture des organisations et les muscles qui les animent et permettent de déployer des activités génératrices de richesses. Dans l'industrie, cette automatisation a été largement envisagée dès son origine pour réduire les coûts

liés à l'activité humaine et accélérer les cadences de production. Chacun appréciait de pouvoir compter sur ces équipements qui ne connaissaient pas la fatigue, ignoraient les limitations d'horaires et assuraient une prestation constante. C'est ainsi que l'informatisation s'est propagée dans l'ensemble des secteurs d'activité jusqu'à atteindre les entités les plus petites. Autant d'atouts pour la compétitivité et une meilleure rentabilité.

Ce phénomène s'est reproduit dans l'ensemble des économies industrialisées et a gagné les pays en développement quand ceux-ci ont fait la bascule vers les technologies numériques après avoir souvent ignoré les phases de transition technique. C'est l'intérêt pour les communautés qui accèdent plus tardivement à l'essor économique que de pouvoir s'appuyer sur les outils les plus récents. Par exemple en Afrique, des zones non pourvues de téléphones filaires se sont ainsi retrouvées couvertes par la téléphonie mobile, permettant l'émergence d'une économie de services autour des smartphones qui se sont multipliés de manière fulgurante dans le grand public.

Il faut avoir à l'esprit cet important déploiement numérique auprès des populations et des acteurs économiques, avec à la clé les nombreuses opportunités de développement qu'il peut susciter, pour prendre conscience de la montée en puissance concomitante du risque numérique.

Dès lors que le nombre d'utilisateurs se démultiplie et que ces derniers confient de plus en plus d'informations à ces équipements, l'exposition au risque croît de manière exponentielle. Car les données peuvent avoir de la valeur dès lors qu'elles concernent un individu ciblé préalablement identifié par un commanditaire. Ou s'il s'agit d'une quantité conséquente d'informations précises, homogènes et récentes. Par exemple, celles qui sont stockées dans les banques concernant les identités, adresses, situations professionnelles, états de santé et patrimoniaux des clients. Dans ce cas, les pirates ne vont généralement pas viser tel ou tel client nommément mais bien chercher à capter la masse cumulée de la clientèle de l'établissement qu'ils ont en ligne de mire. Comme les hôteliers ou les éditeurs de musique qui ont dû revoir leur modèle économique à l'aune des nouveaux usages numériques, la criminalité organisée a adopté la même démarche. Au point que toutes les infractions connues de longue date dans le monde physique : escroquerie, vol, usurpation d'identité, chantage, concurrence déloyale… connaissent des déclinaisons sur le Net. Avec cependant quelques particularités qui donnent toutes les raisons de la voir proliférer encore plus intensément au cours des années à venir.

Le terrain d'affrontement est largement international, pour ne pas dire planétaire. En effet, l'interconnexion des systèmes redessine le principe des frontières géographiques. Puisque la capacité virale des logiciels malveillants qui se reproduisent et circulent sur les réseaux explique certains scores impressionnants attribués à des outils de chiffrement frauduleux comme Wannacry au printemps 2017 : des centaines de milliers d'ordinateurs infectés répartis dans des dizaines de pays. La présence d'équipements similaires dans les entreprises et les collectivités publiques sert aux pirates qui peuvent capitaliser sur l'exploitation de ces infrastructures dès lors qu'ils connaissent les failles qui les fragilisent. On constate ainsi des attaques de dimension industrielle qui tirent parti de cette relative uniformité technique. Ici c'est bien la nature commune des installations informatiques, machines ou logiciels, qui servira de vecteur d'amplification d'une crise numérique.

Cela signifie que l'infection peut circuler via de nombreux territoires et entités – à leurs corps défendants – avant d'atteindre leur but initial. Les investigations a posteriori prendront d'autant plus de temps qu'il faudra reconstituer tel un jeu de pistes le cheminement du maliciel. Mettant à contribution plus ou moins volontaire autant de systèmes juridiques et judiciaires pas toujours très coopératifs.

Des entités subiront des attaques non car elles sont visées spécifiquement mais parce que celui qui est la manœuvre a repéré les caractéristiques du système en place et maîtrise les moyens d'y accéder. Cela modifie la notion d'affrontement : les parties prenantes peuvent ne pas se connaître et n'avoir aucun passé commun ou de contentieux en cours. Ce qui complique d'autant les investigations qui ne pourront reposer que sur des éléments techniques et pas sur un contexte social.

Les organisations ciblées peuvent en outre ignorer les opérations offensives dont elles ont fait l'objet, si elles ne disposent pas d'outils de supervision leur permettant d'entretenir un niveau de surveillance périmétrique pertinent. À l'instar d'une personne qui serait paisible faute de savoir que quelqu'un a visité sa maison en son absence sans rien y déranger. Les pertes causées par l'atteinte aux systèmes d'information peuvent naître d'une interception, d'un blocage et même d'une simple copie des données qui y sont stockées ou échangées.

Cette pluralité de risques oblige les acteurs économiques et institutionnels à disposer d'une connaissance fine et à jour des données dont ils sont détenteurs. Afin de leur attribuer des politiques d'accès qui soient adaptées aux

responsabilités effectives des personnes amenées à consulter, modifier, partager voire supprimer lesdites données. Cette politique de gestion des identités ne doit pas être envisagée dans sa seule perspective sécuritaire mais bien comme une démarche de création de valeur à l'heure de la transformation numérique : connaître les actifs informationnels dont on dispose et identifier celles et ceux qui peuvent en disposer.

La numérisation croissante des modes de production ou de commercialisation doit s'accompagner d'une stratégie de cybersécurité. Afin que les gains générés par l'adoption de ces technologies ne soient pas laminés par un accroissement des risques encourus par l'ensemble de la nouvelle architecture. Il convient donc d'intégrer au fur et à mesure les dispositifs permettant de préserver la durabilité des communications et des données ainsi produites. Cette approche doit être complétée par une politique visant à permettre la résilience de l'ensemble de l'activité : des processus de sauvegarde des informations, des solutions de remplacement et des entraînements des équipes à fonctionner dans un environnement dégradé sont autant d'atouts pour réduire l'impact d'une cyberattaque qui ne pourrait être empêchée. Soit car elle s'appuie sur des négligences ou complicités internes, soit parce qu'elle emploie des codes non encore répertoriés ou des failles techniques non documentées, que l'on désigne sous le nom explicite de « Zero Day ». Un marché occulte de tels moyens d'attaque est accessible sur des plateformes d'échanges ou auprès de prestataires qui commercialisent ces outils malveillants dont le prix vient précisément de leur caractère inconnu. Cela signifie donc que celui qui va concevoir le code offensif peut être – et c'est largement le cas – sans lien avec celui qui va l'utiliser effectivement et sans rapport avec celui qui tirera profit finalement de l'agression numérique. Les concepteurs, les bras armés et les commanditaires peuvent ne s'être jamais rencontrés, vivre dans des contrées éloignées à l'extrême et tout ignorer les uns des autres. Cela complique d'autant la tâche des services d'enquête qui se trouvent en sus très dépendants de la qualité et de la rapidité de la coopération policière et judiciaire internationale. Ici le facteur temps est crucial : il suffit de quelques secondes pour transférer des fichiers d'un pays à un autre, tandis que les policiers compteront au mieux en semaine pour obtenir les réponses à leurs requêtes. Des exceptions existent évidemment mais le décalage des agendas reste extrêmement défavorable aux victimes. Qui en outre peuvent mettre un certain temps à prendre conscience qu'elles ont fait l'objet d'un piratage informatique.

Le numérique trouve désormais sa place dans les outils les plus innocents du quotidien dont la puissance de calcul et la capacité de connexion peuvent être mises à contribution pour déstabiliser par exemple un site Internet. C'est le cas des objets connectés, comme ces caméras domestiques en vente dans les grandes surfaces pour surveiller son domicile ou son jardin. Rarement protégées de manière ad hoc, elles font souvent l'actualité par leur mobilisation massive qui conduit à paralyser un site Internet : le pirate sollicite une très grande quantité de ces appareils connectés mais trop souvent dénués de sécurité et obtient la saturation du site Internet qui doit faire face à ce trop-plein de connexions simultanées.

Mais dans de nombreux cas, les assaillants ne misent pas sur la seule technique mais lui préfèrent l'ingénierie sociale. Grâce aux nombreuses informations variées et à jour, que les internautes publient sur les réseaux sociaux personnels et professionnels, il devient aisé de disposer d'un portrait étayé d'un nombre conséquent de nos contemporains. Et si ces derniers exercent des responsabilités économiques ou administratives ces profils très complets servent à conduire des opérations d'usurpation d'identité, des fraudes et autres escroqueries au président. Il s'agit ici de tromper son interlocuteur en lui faisant croire que l'on est la personne autorisée à lui demander, par exemple, à procéder à un virement financier. Au final, la victime va exécuter de bonne foi le transfert des fonds sur la base d'une histoire suffisamment crédible pour l'amener à se délester elle-même des sommes demandées. Un usage habile de la psychologie humaine à l'heure de la technologie généralisée.

Cette méthode fonctionne également quand les informations recueillies permettent de rédiger des messages qui revêtent tous les aspects de la réalité. Et qu'en cliquant sereinement sur un lien ou une pièce jointe une personne infecte à son insu son ordinateur ou son smartphone. Car ces appareils mobiles sont plus que jamais des cibles privilégiées alors que la consommation numérique s'exerce désormais à plus de 50% sur ces appareils (smartphones, tablettes, ordinateurs portables). Leurs écrans sont plus petits qu'un ordinateur de bureau ce qui rend plus difficile la détection à l'œil de messages frauduleux et leur protection de base par un simple antivirus est rarissime. Ils concentrent en outre l'ensemble des données à haute valeur ajoutée : éléments de géolocalisation, contacts, correspondances des e-mails et des SMS, photos, identifiants de connexion aux applications notamment bancaires, messageries

professionnelles… Une vraie mine d'or pour les pirates qui adaptent désormais leurs logiciels malveillants à l'ergonomie des smartphones.

Il ne s'agit certainement pas de verser dans une paranoïa technologique qui conduirait à un rejet des opportunités et des services offerts par l'innovation numérique. Mais de diffuser une culture de sécurité afin de réduire l'exposition au risque, limiter l'impact d'éventuelles attaques et permettre un retour à une situation normale dans les meilleures conditions.

On ne doit pas faire l'économie de cette maturité d'usage face à la société numérique qui s'annonce. C'est une condition nécessaire à une consommation maîtrisée et éclairée de ces équipements qui se déploient dans l'ensemble des déclinaisons de nos existences. Les citoyens que nous sommes méritons d'être des sujets exigeants et autonomes face à ces canevas techniques qui modèlent notre perception du monde. Afin de ne pas être cantonné au statut peu enviable d'objets, dépendants des règles d'emploi décidées par des esprits pas forcément bienveillants.