LA CYBERSÉCURITÉ EN 2016

Quelles prédictions pour l'Algérie ?

Par Abdelaziz Derdouri, officier supérieur en retraite

Introduction

Chaque année, en cette période, les nombreux rapports bilans sur la cybersécurité apportent de précieux enseignements, permettant de réaliser des études prospectives et une approche pour préparer les stratégies à court, moyen et long termes, en cohérence avec les enjeux majeurs qui associent les technologies de l'information et de communication (TIC). Nous vivons une ère de croissance rapide de l'utilisation de ces dernières qui sont accompagnées de menaces sophistiquées. Aujourd'hui, les progrès technologiques présentent cette dualité : de grandes opportunités accompagnées de grands risques dont les cyberattaques émanant de cybercriminels, de hacktivistes et de plus en plus celles parrainées par des Etats.

Un groupe de hacktivistes a ciblé en ce début janvier 2016 un certain nombre de sites officiels du gouvernement nigérian, dont ceux des ministères de l'Intérieur, des Finances et des Affaires étrangères, et procédé à un vol de données qu'il menace de rendre publiques dans le cas où il n'est pas mis un terme au comportement de certaines personnalités politiques caractérisé par la corruption et le vol de fonds publics qui génèrent dans le pays chômage et pauvreté. Les hacktivistes utilisent le vol de données pour nuire et détruire la crédibilité des institutions ou personnalités ciblées.

Beaucoup a été dit sur la créativité des cybercriminels ; néanmoins, les bilans de l'année 2015 ont montré, en ce qui concerne certains pays, dont l'Algérie, que les cybercriminels n'auront pas à utiliser les techniques les plus avancées ou des méthodes sophistiquées pour réussir leur intrusion dans les réseaux.

Il suffit simplement de comprendre la psychologie derrière la politique de sécurité de ces pays à l'égard des TIC pour ne pas avoir à recourir à des outils sophistiqués. Pourtant, l'absence de sécurité est le plus gros problème dans le secteur des TIC à cause de l'adoption, pour des raisons pratiques et économiques, du cloud, de la mobilité et de l'internet des Objets. Pour compliquer les choses, des études récentes montrent que le niveau de la cybermenace dans les pays arabes a un lien aussi avec la situation politico-socioéconomique de ces derniers. L'année 2015 a été largement dénommée par les experts comme «l'année de la violation de données». Comment définir ce à quoi l'Algérie doit s'attendre en 2016 ?

Le hacktivisme

Le hacktivisme qui se réfère à l'utilisation des techniques des hackers (défiguration de sites web, attaques de déni de service, vol de données, sabotages et vandalisme virtuels, etc.) n'a pas pour objectif le gain financier, mais l'utilisation de la technologie, des outils et techniques des hackers pour exprimer un désaccord ou un mécontentement. C'est la projection de la protestation et de la désobéissance civile sur l'internet.

Lors du mouvement contestataire de janvier 2011 en Algérie, des institutions dont le ministère de l'Intérieur ont été victimes de cyberattaques (#OpAlgeria) émanant de hacktivistes. Un groupe de hacktivistes a ciblé en ce début janvier 2016 un certain nombre de sites officiels du gouvernement nigérian, dont ceux des ministères de l'Intérieur, des Finances et des Affaires étrangères, et procédé à un vol de données qu'il menace de rendre publiques dans le cas où il n'est pas mis un terme au comportement de certaines personnalités politiques caractérisé par la corruption et le vol de fonds publics qui génèrent dans le pays chômage et pauvreté. Les hacktivistes utilisent le vol de données pour nuire et détruire la crédibilité des institutions ou personnalités ciblées.

Au Moyen-Orient et en Afrique du Nord, 45% de toutes les cyberattaques sont effectuées par les hacktivistes.

Les outils utilisés ne sont pas aussi développés que ceux des cybercriminels, pourtant les gouvernements et les organisations craignent plus les hacktivistes à cause du vol et de la divulgation d'informations embarrassantes. Ce type d'incidents, dont le nombre continuera à augmenter en 2016, est à l'origine de préjudices qui sont difficiles sinon impossibles à réparer.

En 2016, les hacktivistes, encouragés par la facilité d'actions, l'impunité et la garantie de succès, passeront du simple sabotage virtuel à des attaques plus méthodiques pour faire entendre leurs revendications et leurs messages politiques ou religieux. Les victimes découvriront à leurs dépens qu'elles ont plus d'ennemis qu'elles ne pensaient et qu'elles peuvent être atteintes dans ce qu'elles ont de plus sensible. Le paysage du hacktivisme politiquement motivé prend de plus en plus d'ampleur dans les pays arabes. Il est instable et ses activités semblent être proportionnelles à l'agitation politique et sociale.

Une augmentation du niveau de l'activité des hacktivistes d'Afrique du Nord est attendue en 2016. Ils peuvent utiliser des outils malveillants développés par eux et qui sont ouvertement disponibles tels que njRAT ou Fallaga RAT (Remote Access Tool). La prolifération de ces nouveaux outils arabes signifie que des individus ou groupes de la région tentent d'obtenir des capacités d'intrusions ciblées. La motivation pour de telles attaques peut varier du mécontentement à la réaction contre l'intervention des services de l'ordre ou un projet de loi impopulaire.

Lien entre la situation politico-socioéconomique et la cybermenace

La vulnérabilité informatique d'un pays ou d'une région n'est pas liée à un seul facteur mais aussi à une variété de facteurs politiques et socioéconomiques. En effet des études d'experts montrent que l'évolution de la cybermenace dans le monde arabe est liée aussi à ces facteurs. Les protestations et troubles politiques dans un pays conduisent à un taux de cyberattaques et d'infections en malwares plus élevé. Le niveau de la cybermenace est beaucoup plus important dans les régions où il y a des conflits internes et externes.

L'instabilité gouvernementale, le niveau de corruption dans un pays, l'absence de l'Etat de droit, de la bonne gouvernance et le niveau de développement économique ont un impact sérieux sur le niveau de la cybermenace.

L'analyse de la diffusion des logiciels malveillants dans le Moyen-Orient met en évidence que les pays de cette région où il y a des conflits ont un taux d'infection par les malwares double de la moyenne mondiale.

La situation en Algérie devrait inquiéter car le taux d'infection est plus élevé comparativement à ces pays.

Le cyberespionnage

Le cyberespionnage, qui est le nouveau visage de l'espionnage classique, utilise comme vecteurs des logiciels malicieux (malwares) ou Trojan Horse (Chevaux de Troie), ainsi que les backdoors (Portes dérobées). Il est «facile, pas cher, de plus en plus sophistiqué et efficace». Il offre l'anonymat et on peut rarement prouver l'identité du responsable. Le renseignement peut maintenant être récupéré très rapidement à la source, dans n'importe quelle partie du monde sans avoir à se déplacer. Il est même devenu le moyen privilégié pour le recueil de renseignement en plus d'être le produit d'une stratégie de domination politique et économique sur l'internet de plusieurs pays. Son impact sur le moyen et le long termes sont dévastateurs. Contrairement aux autres types de crimes, les dommages du cyberespionnage ne peuvent être quantifiés car ils touchent à la sécurité nationale.

En 2014 et 2015, l'Algérie a été ciblée par plusieurs opérations de cyberespionnage émanant principalement de la France. Elle est à l'origine d'opérations consistant à implanter, depuis 2009, plusieurs logiciels espions, dont «Babar», dans les systèmes informatiques d'institutions gouvernementales et économiques de plusieurs pays dont l'Algérie. En 2015, l'«Equation Group», utilisant un virus de cyberespionnage, a été découvert. Les victimes ciblées sont le gouvernement, la défense, les secteurs de l'énergie et de la finance.

Le recueil du renseignement économique sensible et de défense en Algérie par des parties étrangères dont la France continuera en 2016 et sera facilité par l'absence d'une stratégie nationale de cybersécurité, d'une loi sur la cybersécurité et d'une structure pour la protection des infrastructures sensibles comme celle britannique : Centre for the Protection of National Infrastructure (CPNI), qui dépend du MI5, le Service de la sécurité intérieure.

Cyberterrorisme

L'utilisation par les groupes terroristes de cyberarmes contre les réseaux ne peut être exclue. Ils ne semblent pas avoir tous pour le moment la maîtrise et le savoir-faire technique pour organiser des cyberattaques. Mais ceci ne saurait tarder car des indices qui montrent les efforts pour une meilleure maîtrise des technologies de l'information et de communication par les groupes terroristes existent. La tendance en 2015 a été l'utilisation de l'internet à des fins de communication, d'endoctrinement, de recrutement, de formation, de collecte de fonds et aussi pour organiser et coordonner les opérations plus efficacement.

Après les fuites de Snowden, les groupes terroristes Tashfeer Al-Jawwal, Asrar al-Ghuraba et Amn Al-Mujahid (Sécurité du Moudjahid) ont développé leurs propres logiciels de cryptage pour les opérations de chiffrement sur l'internet. En novembre 2015, un groupe de djihadistes a mis en place sur l'internet un bureau d'assistance H/24 et différentes plateformes pour former sur la sécurité informatique et aider les terroristes et leurs sympathisants dans les opérations de cryptage des communications relatives aux activités de recrutement, de propagande et de planification des opérations, échappant ainsi à la surveillances des services de sécurité.

Contrairement à beaucoup de gouvernements, les groupes terroristes s'adaptent à l'évolution des technologies et montrent un intérêt croissant à ces dernières comme celle des mobiles en raison de la grande disponibilité, accessibilité et efficacité dans les lieux de leurs activités. En 2014 et 2015, deux applications de cryptage pour smartphones utilisant le système d'exploitation Android ont été développées par le groupe terroriste Al Fajr.

Des sympathisants d'un groupe terroriste ont lancé en décembre 2015 sur internet un magazine, Kybernetik, pour former les futurs djihadistes sur la façon de prendre part à une «cyberguerre».