Ses éditeurs ont encouragé la traduction des articles en d'autres langues et de les partager sur les réseaux sociaux. «Il est très important pour nous que nos frères et sœurs apprennent la manipulation correcte des logiciels et hardwares» et tirent «avantage de la technologie», selon e-Moudjahid.

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. Selon une compagnie de sécurité russe, les groupes terroristes Cyber Califat, Team System DZ et Fallaga ont attaqué 600 ressources internet russes dont celles des banques, des entreprises de construction, des organisations gouvernementales, des centres de recherche et écoles. Les activités dans le cyberespace des groupes terroristes ont été à ce jour limitées à la guerre psychologique, à la génération de la peur en diffusant sur internet des clips vidéo montrant des décapitations et exécutions de masse ou des défilés pour donner une illusion de la force. L'utilisation d'internet à des fins terroristes est un phénomène qui connaît une croissance rapide. En 2016, internet sera davantage utilisé pour amplifier et généraliser l'impact des opérations terroristes sur les victimes en ayant recours aux cyberarmes, comme ce fut déjà dans le cas sus-évoqué des cyberattaques contre des infrastructures sensibles russes. Elle sera définie comme l'année de la militarisation de l'internet par les terroristes.

La cybercriminalité

Le rapport de l'Europol décrit l'Afrique comme connaissant un rapide développement dans les TIC mais très peu de ses pays peuvent faire face à la cybercriminalité nationale et internationale. Ses infrastructures sont malveillamment exploitées pour héberger des malwares et des sites de Phishing (Hameçonnage) et cette situation «est particulièrement vraie pour des pays nord-africains comme l'Algérie ou le Maroc», selon le même rapport.

Pour un directeur de McAfee qui est une société américaine de sécurité informatique basée à Silicone Valley, «l'Afrique est devenue très connectée», «beaucoup de systèmes d'exploitation en usage sont cependant piratés, ce qui signifie qu'ils ne reçoivent pas de correctifs ou de mises à jour». La conséquence est que «l'Afrique est une immense cible pour les pirates» ; «elle est attaquée et utilisée comme une plaque tournante pour cibler d'autres pays» et «les gouvernements et les utilisateurs africains ne sont ni protégés ni conscients».

En Algérie, qui est concernée par les évaluations de l'Europol et McAfee, la cybercriminalité nationale est aussi impliquée, selon les rapports des autorités, dans la violation de la vie privée des internautes, dans le cybervandalisme d'institutions et structures publiques et privées, dans les menaces, les escroqueries et les comportements contraires à la morale.

Les mobiles

On utilise aujourd'hui dans le monde plus les smartphones et les tablettes que les ordinateurs pour se connecter à l'internet. Avant la fin de 2016, il pourrait y avoir 10 milliards de smartphones dans le monde. En Algérie, plus de 90% des smartphones utilisent le système d'exploitation Android. Le développement et la diffusion de logiciels malveillants pour les smartphones, notamment ceux utilisant Android, qui est le système d'exploitation le plus populaire sur le marché, continuera de croître à un rythme exponentiel tout comme en 2015.

440 000 malwares pour Android ont été recensés rien que durant un trimestre de 2015. Le chiffre de 20 millions de malwares développés en 2016 pourrait être atteint. La proportion de malwares du type Trojan Horse (Cheval de Troie) est de 50%. Les Trojan Horse sont des logiciels espions servant à recueillir des informations. Les chevaux de Troie conçus pour envoyer des programmes malveillants sur des SMS sont les plus répandus en Algérie. «Bien que les attaques contre Android étaient monnaie courante au cours des dernières années, la particularité pour 2016 est la manière dont les smartphones seront infectés. Nous allons voir plus de menaces qui vont s'enraciner dans le dispositif, ce qui rendra leur élimination par un antivirus presque impossible».

L'introduction en Algérie de moyens de paiement non traditionnels en utilisant les smartphones et sans une stratégie de sécurité équivaut à un «tsunami de vols de données». L'année 2016 en Algérie sera l'année où la sécurité d'un dispositif mobile (smartphone ou tablette) doit être prise au sérieux par son utilisateur.

Cyberconflits

Tous les conflits de basse intensité entre nations qui ont eu lieu en 2015 contenaient un élément de cybersécurité : Russie-Ukraine, Corée du Sud-Corée du Nord, Iran-Arabie Saoudite, Israël-Palestine, Inde-Pakistan, Syrie-Turquie-Etats-Unis, etc. Les conflits de basse intensité continueront à migrer vers le cyberespace en 2016 pour interrompre massivement différents services comme la distribution d'électricité, de l'eau, les transports, les opérations financières et administratives, etc. Les cyberarmes étant des Armes d'Interruption Massive (Weapon of Mass Disruption).

Les cybercriminels et les gouvernements qui ont recours aux cyberattaques seront encore victorieux en 2016. Les organisations, les entreprises et les utilisateurs auront intérêt à adopter plus de mesures de protection contre les dangers de l'internet au cours de cette année. Parmi ces mesures celles de sensibilisation, dont le coût est insignifiant, pour éliminer ou amoindrir la menace interne qui représente 40% de la menace globale.

Le 23 décembre 2015, une panne d'électricité massive a eu lieu dans l'ouest de l'Ukraine et laissé environ 700 000 foyers dans l'obscurité. Le gouvernement ukrainien a découvert que c'était des logiciels malveillants installés à son insu à l'intérieur des systèmes de contrôle des générateurs électriques qui ont été à l'origine de la «panne». Le réseau électrique a donc été intentionnellement ciblé, en hiver de surcroît, pour augmenter les impacts de cette opération malveillante sur la population. L'objectif recherché est la démoralisation, l'affaiblissement et la déstabilisation du pays ciblé. Les consommateurs et utilisateurs civils ainsi que les entreprises seront les dommages collatéraux dans les cyberconflits de basse intensité futurs entre nations, comme cela a été le cas de la cyberattaque contre le réseau électrique ukrainien qui a privé d'électricité des foyers, des hôpitaux, des entreprises, etc., ou encore de la cyberattaque, fin décembre 2015, contre un barrage à New-York.

En 2016, l'Algérie sera vulnérable aux cyberattaques contre ses infrastructures sensibles, et l'interruption de services comme la distribution d'électricité, de l'eau ou des transports au profit des citoyens est à prévoir. Les attaques chirurgicales pratiquées dans les autres champs de bataille (terre, air et mer) pour éviter les dommages collatéraux ne sont pas possibles dans le cyberespace.

La menace interne

La menace interne continue à être l'une des principales causes des intrusions dans les réseaux. Elle prendra aussi plus d'ampleur en 2016 à cause de l'absence presque totale de campagnes de sensibilisation au profit des personnels exploitant les outils informatiques. Des pays ont rendu ces campagnes obligatoires grâce à des textes de loi.

Conclusion

Les cybercriminels et les gouvernements qui ont recours aux cyberattaques seront encore victorieux en 2016. Les organisations, les entreprises et les utilisateurs auront intérêt à adopter plus de mesures de protection contre les dangers de l'internet au cours de cette année. Parmi ces mesures celles de sensibilisation, dont le coût est insignifiant, pour éliminer ou amoindrir la menace interne qui représente 40% de la menace globale.

Enfin, je ne saurai terminer sans évoquer l'article 39 de l'avant-projet de révision de la Constitution qui prévoit de garantir la protection des données privées sur le net. Il s'agit d'un pas dans la bonne direction, en ce qui concerne la cybersécurité en Algérie, mais cette garantie ne peut être effective que s'il y a une protection des données en général contre les violations qui ont une origine aussi bien nationale qu'étrangère. Pour arriver à cet objectif il faut une stratégie nationale de cybersécurité que l'Algérie n'a malheureusement pas encore et qui ne doit pas obligatoirement faire l'objet d'un article dans la Constitution. Une loi suffirait et aurait l'avantage de défendre la vie privée sur le Net, les données et les réseaux des infrastructures sensibles nationales contre les cyberattaques émanant de gouvernements étrangers et dont dépend la sécurité nationale.

Ce serait bien si aucune des prédictions de cybersécurité sus-citées ne venait à se réaliser. Mais les tendances et éléments précurseurs prédisent une situation différente de celle à laquelle l'Algérie et les internautes doivent se préparer en 2016. La tâche sera ardue car dans le cybermonde, il est largement considéré qu'il est plus facile d'être l'agresseur que le défenseur : ce dernier doit se protéger contre toutes les vulnérabilités et elles sont très nombreuses, tandis que l'agresseur doit identifier une seule vulnérabilité et l'exploiter.

A. D.