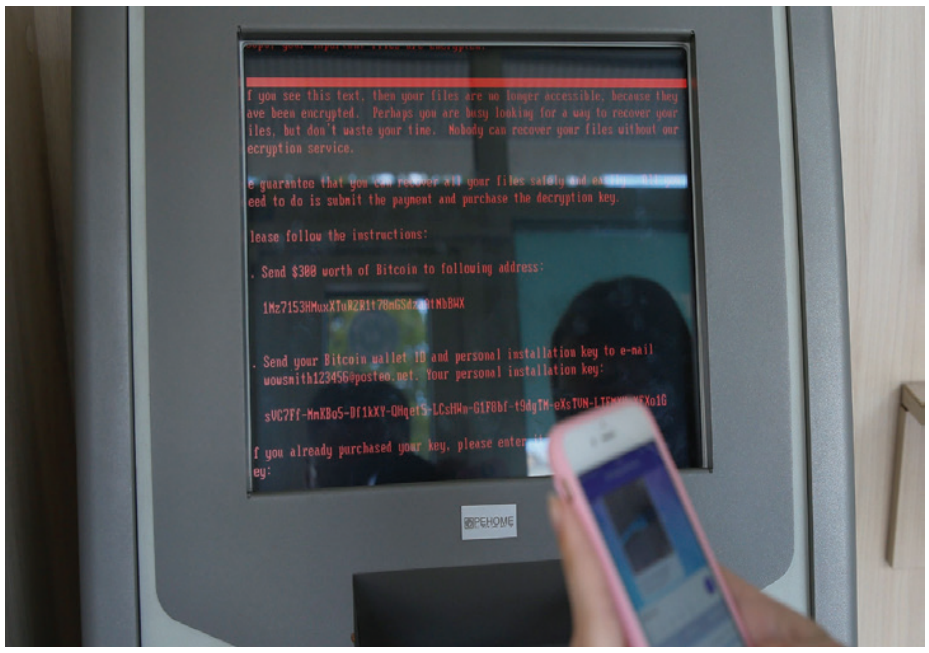
L'Orient LE JOUR
jeudi 30 novembre 2017 | N°15086

CONFÉRENCE

Le Liban de plus en plus ciblé par les cyberattaques

Le pays du Cèdre doit encore adapter sa législation pour intégrer les différents types de cybercrimes.



Les organisateurs du 3e forum sur la cybersécurité considèrent que le renforcement des capacités de lutte du Liban dans ce domaine est une priorité. Photo P.H.B.

Philippe HAGE BOUTROS

Dans un rapport publié hier, la société de sécurité informatique McAfee a affirmé craindre une augmentation de la cybercriminalité dans le monde en 2018, tandis que l'année en cours a déjà été marquée par plusieurs attaques informatiques de grande ampleur.

Cette intensification devrait également se faire ressentir au Liban, selon Jan Kaastrup, directeur de la technologie au sein de la société danoise CSIS Security Group, qui s'attend à une « multiplication de plusieurs types d'offensives » au courant des mois à venir – rançongiciel (ransomware), fraude au fournisseur/président, ou encore hameçonnage (phishing) ciblé, principalement. M. Kaastrup intervenait lors d'un des huit panels programmés lors du 3e forum dédié à la lutte contre la cybercriminalité, hier à l'hôtel Phoenicia, à Beyrouth. L'événement est organisé chaque année par la Banque du Liban (BDL), les Forces de sécurité intérieure (FSI) et le groupe al-Iktissad wal Aamal.

Monnaie virtuelle

Le Liban n'a pas été épargné par les cybercriminels en 2017. En mai, la BDL avait ainsi reconnu avoir déjoué une tentative de piratage dans le cadre de la cyberattaque mondiale Wannacry. Plus récemment, le quotidien français *Le Figaro* a rapporté (lundi) que des hackers iraniens auraient piraté les serveurs des bureaux de la présidence de la République et du Conseil des ministres. Ni le directeur général des FSI, le général Imad Osman, ni le gouverneur de la BDL, Riad Salamé, n'ont commenté l'une ou l'autre attaque lors de leurs interventions respectives en ouverture du forum. Ils ont toutefois désigné le renforcement des capacités du Liban en matière de cybersécurité comme une priorité.

Notant que le nombre de crimes comme les montants détournés au Liban par des cybercriminels avaient augmenté ces trois dernières années, le général Osman a affirmé que les FSI avaient déjà pris plusieurs mesures pour répondre aux situations les plus urgentes. M. Salamé a, quant à lui, considéré que la question prend de plus en plus d'importance « avec le développement des moyens de paiements », d'autant que la BDL se prépare à lancer sa propre monnaie virtuelle. Également présent, le secrétaire général de la Commission d'enquête spéciale (CSI) de la BDL, Abdel-Hafiz Mansour, a noté que les cyberattaques « étaient de plus en plus complexes ».

Le directeur adjoint de la CSI, Antoine Mandour, a pour sa part fourni pendant le forum les données les plus récentes concernant l'évolution de la cybercriminalité financière au Liban. Selon lui, la CSI a été saisie à 127 reprises dans ce cadre sur les neuf premiers mois de 2017 (contre 139 fois pour l'ensemble de l'année 2016). Les infractions relevées ont concerné plus de 4,9 millions de dollars sur la même période (11,5 millions sur l'ensemble de 2016). Toujours selon la CSI, plus de 70 % des cyberattaques ont été menées avec succès fin septembre, même si dans 23 % des cas les enquêteurs ont réussi à récupérer les fonds détournés. Enfin, M. Mandour a indiqué que les cybercriminels s'attaquaient moins aux banques et plus aux autres types de sociétés depuis 2016. Une tendance qui met en évidence la nécessité de sensibiliser les entreprises libanaises à investir dans la cybersécurité, que ce soit pour protéger leurs données ou former leur personnel, rappelle l'expert Hady el-Khoury, qui animait un autre panel, en milieu de journée.

Enjeux concrets

Il reste que la cybercriminalité financière est mieux encadrée par la réglementation locale que d'autres types d'infractions dans ce domaine, la BDL imposant régulièrement aux banques de renforcer leurs moyens de contrôle. Dans sa circulaire n° 144 du 28 novembre 2017, la BDL appelle par exemple les établissements libanais à « avoir recours à l'assistance de leurs banques correspondantes », lorsqu'elles découvrent qu'une « transaction donnée est associée ou dérivée d'un cybercrime ». Le texte enjoint également les banques du pays du Cèdre à se référer au guide publié en octobre 2016 par la CSI pour adapter leurs procédures et détecter les infractions.

La situation est plus compliquée pour les autres formes de cybercriminalité. Selon la juge Hania Helweh, représentant le ministère de la Justice au forum, le cheminement des poursuites pour les cybercrimes « varie en fonction des cas », et les affaires se retrouvent soit devant le juge des référés, soit au civil, soit au pénal. Elle appelle en outre le Parlement à adopter un projet de loi (n° 6341) en la matière qui lui a déjà été transmis.

Pour M. Khoury, « il ne faut pas que les entreprises attendent que le cadre législatif soit opérationnel pour commencer à s'adapter ». Il regrette en outre que le forum, qui a rassemblé près de 400 personnes au plus fort de la journée, « n'ait pas davantage mis l'accent sur le côté pragmatique de la lutte contre la cybercriminalité », et juge que la majorité des intervenants « ont trop insisté sur les dangers des attaques » et pas assez sur les enjeux concrets. Enfin, d'autres intervenants, à l'image de Maria Agha Wevelsiep, directrice du programme Cybersouth, ont estimé que le Liban pourrait plus efficacement renforcer ses capacités de lutte contre la cybercriminalité en coopérant davantage avec ses partenaires étrangers. Lancé cet été et doté d'un budget de 3,3 millions d'euros (3,9 millions de dollars) financés par l'Union européenne et le Conseil de l'Europe, Cybersouth s'étend sur trois ans et vise à aider le Liban ainsi que quatre autres pays méditerranéens (Algérie, Jordanie, Maroc et Tunisie) à renforcer leurs capacités dans ce domaine.