Ukraine : l'amorce d'une cyberguerre

L'attaque militaire menée par la Russie contre l'Ukraine, en plus de provoquer des pertes en vies humaines et des destructions matérielles, s'accompagne d'une montée des périls en matière de cybersécurité.

Dans la nuit du mercredi 23 au jeudi 24 février, lorsque le président russe, Vladimir Poutine, a lancé son « opération militaire » en Ukraine, les autorités américaines et britanniques ont alerté sur la circulation d'un nouveau logiciel malveillant nommé Cyclops Blink.

Le malware, présenté comme le sucesseur de VPNFilter, utilise les appliances de pare-feu du fournisseur de matériel réseau WatchGuard pour former un botnet et diffuser des programmes malveillants destructeurs.

Le groupe de piratage informatique Sandworm, également connu sous d'autres noms comme Fancy Bear ou APT28, dit parrainé par l'État russe, est présenté comme l'initiateur de la menace. Il sévit depuis plusieurs années en Ukraine comme ailleurs.

WatchGuard, de son côté, indique dans un billet de blog avoir mis en place « un plan de remédiation à Cyclops Blink ». L'entreprise américaine ajoute : « selon les estimations actuelles, Cyclops Blink pourrait avoir infecté près de 1% des appliances firewall actives WatchGuard ; aucun autre produit WatchGuard n'est concerné. »

« Renforcement de la vigilance cyber »

Le 23 février 2022 toujours, l'entreprise slovaque de sécurité informatique ESET a annoncé avoir identifié un malware destructeur de type wiper (effaceur), nommé HermeticWiper, conçu pour effacer le contenu de disques durs, sur « des centaines de machines » en Ukraine.

Selon l'éditeur américain de logiciels de sécurité Symantec (Broadcom), cette fois-ci, des sous-traitants en Lettonie et en Lituanie du gouvernement ukrainien, ainsi qu'une banque ukrainienne, font partie des sociétés touchées.

De surcroît, une nouvelle série d'attaques en déni de service distribué (DDoS pour Distributed Denial of Service), attribuées à la Russie, a ciblé et rendu inacessibles des sites institutionnels, notamment ceux des ministères de la défense et de l'intérieur ukrainiens, et d'établissements bancaires ukrainiens – quelques heures avant l'assaut russe contre l'Ukraine.

Aussi, des chercheurs en sécurité informatique ont révélé, via le site Bellingcat, l'existence de sites piégés visant à inciter des cibles en Ukraine à télécharger un logiciel malveillant.

En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a prévenu, jeudi : « si aucune cybermenace visant les organisations françaises en lien avec les récents événements n'a pour l'instant été détectée » le « renforcement de la vigilance cyber » s'impose. L'Agence incite donc les entreprises et les administrations à s'assurer de la mise en place de mesures « d'hygiène informatique », de bonnes pratiques, et à suivre « attentivement les alertes et avis de sécurité émis

par le Centre gouvernemental de veille, d’alerte et de réponse aux attaques informatiques (CERT-FR) ».

(crédit photo © ECPAD)