Challenges
Challenges (site web)
mardi 25 avril 2023 - 16:32 UTC 903 mots

Quand l'armée française joue à la guerre cyber avec des étudiants

Adrien Schwyter

REPORTAGE - Début février, durant plusieurs jours, une centaine d'étudiants de Nancy ont participé à un "wargame" cyber sous l'auspice du Commandement cyberdéfense du ministère des Armées. Le but: susciter des vocations et repérer des talents qui pourraient devenir acteur de la lutte contre la cyberguerre.

"Nous avons pris le contrôle du réseau wifi de l'ambassade, il était peu sécurisé. Une fois dans leur réseau, nous avons hacké l'ordinateur qui gérait le flux vidéo de la caméra de surveillance. Et nous avons pu récupérer pas mal de documents intéressants en faisant sauter le chiffrement au sein de l'ordinateur." Alexandre, le visage masqué par une cagoule, dont on devine les traits tirés, n'est pas là pour rigoler. Pourtant ce mercredi 8 février, l'étudiant en licence pro cyber de l'IUT Nancy-Brabois doit faire gagner son équipe Cryptanga face à Anumérique. Ces deux collectifs s'affrontent déjà depuis plusieurs jours dans ce jeu de rôle en conditions réelles imaginé par le ComCyber (Commandement cyberdéfense du ministère des Armées). Lire aussiComment l'armée prépare la cyberguerre"Nous essayons de coller au maximum à la réalité afin d'être le plus immersif possible, confie Carré d'As*, le capitaine en charge de l'organisation du "wargame". Il faut s'imaginer qu'on est dans l'archipel des Maldives, l'île Rivershell est complètement aux abois financièrement. A cause de la montée du niveau de l'eau, elle ne peut plus profiter du tourisme. Ils ont des ressources minières de lithium importantes, les deux équipes vont devoir remporter la concession minière."Une troisième équipe APT est créé afin de pimenter la situation. Son but étant d'attaquer les deux pays, voire de coopérer contre rémunération avec l'un des acteurs.OIV, darknet et chiffrement au programmePlus de deux cents équipements réels et virtuels ont été mis en place pour l'occasion: une ambassade gardée par un pass sous la surveillance d'une caméra vidéo, un hôpital jouant le rôle d'organisme d'importance vitale (OIV), des automates, des robots, sans oublier un darknet où il est possible d'acheter des logiciels malveillants sur étagère.Tout se déroule en ligne sur des réseaux fermés construits pour l'occasion grâce à deux cyber-ranges de l'Armée, d'imposants serveurs permettant de reproduire un réseau internet totalement hermétique du réseau classique. Signe du degré de réalisme de l'exercice, le ComCyber se sent obligé de préciser qu'aucun "système d'arme n'est mis en jeu, rien de classifié, ni de militaire. Pas besoin d'avoir une arme de pointe pour faire des dégâts en ligne."La centaine d'étudiants qui participent proviennent de six entités: la Faculté des sciences et techniques, l'IUT Nancy-Brabois, les Mines Nancy, Télécom Nancy, et Polytech Nancy. Ils sont répartis dans plusieurs locations physiques dans la ville, afin de compliquer les communications entre les équipes. Chacune dispose de son équipe d'attaque (Red Team), et de la défense (Blue Team), ainsi que son ambassade en terrain hostile.Lire aussiCyberattaques : pourquoi les entreprises françaises sont-elles des cibles ? Au troisième jour de ce wargame, les équipes entrent dans la phase finale. "C'est simple, on envoie tout ce qu'on a en termes d'attaques, résume Julien, capitaine d'Anumériс. Une attaque est en cours sur leur OIV. Le but est également de récupérer des infos, et surtout de le faire savoir. Tout ce qui permet de discréditer l'autre pays va nous servir. Par exemple on a réussi à pirater leur journal, on a créé de fausses publications afin de les diffamer."Fake news et débunkCe qu'oublie de raconter Julien, c'est qu'au cours de la nuit précédente, le compte en banque de son pays s'est fait siphonner par l'équipe adverse. "Pour répondre à leur campagne de fake news en ligne, on a créé un compte dont le but est d'expliquer leur manipulation pour "debunker" tout cela, répond Arthur de l'équipe adverse Cryptanga. On en a profité aussi pour créer plein de faux profils afin de noyer leur opération d'influence."Comme dans un escape game, ou dans tout bon jeu de rôle, les maîtres du jeu sont là pour donner un coup de pouce si les acteurs patinent. "Nous leur donnons des indices lorsqu'ils butent longtemps sur un problème glisse le capitaine Chewbacca. Cette année nous avons mis des documents dans les poubelles, il faut développer leur curiosité. Il faut bien sûr recréer les conditions de fatigues liées à une crise qui dure plusieurs jours, mais le but demeure qu'ils aient la banane à la fin."Lire aussiComment la guerre en Ukraine a remodelé le paysage de la menace cyberOpération de recrutementMême si l'exercice se veut ultra réaliste, en réalité peu importe qui emportera le contrat minier. Le ComCyber de l'Armée française est

surtout là pour susciter des vocations parmi cette centaine d'étudiants, tout en repérant les profils intéressants, afin de venir travailler en son sein. "Cela nous permet de détecter les talents et des compétences rares explique le colonel Eric Koessler, commandant de la base de défense de Nancy. L'idée est de susciter des vocations à servir le pays, voire dans la réserve opérationnelle ou citoyenne."Le ministère espère atteindre 5.200 cybercombattants d'ici 2025 alors qu'ils ne sont aujourd'hui que 3.700. Pour l'anecdote, c'est l'équipe Cryptanga qui a réussi à décrocher le marché minier. Nul doute que les étudiants encagoulés imaginent déjà leur avenir au sein d'opérations qui ressemblent à des jeux d'adultes sous couverture.*Les militaires participant à l'opération n'ont communiqué qu'un pseudo utilisé le temps "wargame".