FUTURA

Cyberguerre : l'offensive russe sur l'Ukraine (TechPod #26)

Podcast écrit et lu par : Emma Hollen

Bonjour à toutes et à tous et bienvenue dans Techpod, la chronique audio de Futura dédiée à l'actualité des technologies et de la mobilité. Je suis Emma Hollen, et aujourd'hui on va parler de cyberguerre en Ukraine.

[*Musique technologique, journalistique*]

C'est une tendance qui continue de se confirmer en ce début d'année 2022 : les canons de la guerre hybride font des dégâts en silence. Actuellement la tension entre les États-Unis, ses alliés et la Russie au sujet d'une potentielle offensive militaire en Ukraine demeure à son comble, et il semblerait qu'en marge du regroupement de plus de 100.000 soldats et de leur armement à la frontière est de l'Ukraine, l'offensive russe aurait peut-être déjà débuté sur les espaces virtuels. Ainsi, il y a un peu plus de 15 jours, dès le lendemain de la fin des pourparlers infructueux entre la Russie et l'Otan sur la crise, 70 sites web gouvernementaux ukrainiens ont été cyberattaqués. Dix-sept d'entre eux ont été défacés, c'est-à-dire que leur page d'accueil avait été remplacée par les revendications des auteurs de l'attaque. Avant qu'il ne disparaisse, un message menaçant rédigé en russe, en ukrainien et étrangement en polonais était affiché. Il indiquait que toutes les données personnelles des Ukrainiens collectées sur ces sites avaient été mises en ligne sur le web, et évoquait également de vieilles querelles datant de la Seconde guerre mondiale entre les Polonais et les Ukrainiens. Si cette étrange note d'intention pourrait laisser supposer que les auteurs de l'attaque seraient polonais et non pas russes, comme tout le monde s'accorde à le penser sans le dire, les autorités ukrainiennes n'hésitent cependant pas à attribuer directement cette attaque, depuis baptisée « Opération Ours sanglant », au Kremlin. En réponse, comme à son habitude, la Russie a nié avec sarcasme être l'auteure de l'attaque. Dans tous les cas, selon Microsoft, ses ramifications seraient bien plus importantes que ce que le constat initial ne laisse présumer et toucheraient de nombreuses agences et organisations gouvernementales ukrainiennes. La charge virale repose sur un ransomware, dont la demande de rançon de 10.000 dollars en Bitcoin n'était qu'un leurre. Son objectif réel était de détruire les données et de paralyser les systèmes. Les auteurs de l'attaque ont sans doute pris soin de laisser sur les serveurs ukrainiens d'autres charges virales dormantes qui pourraient être déclenchées plus tard.

[*Nouvelle musique technologique*]

Alors évidemment, si tous les regards se tournent vers la Russie, c'est parce que l'Ukraine a déjà été ciblée à plusieurs reprises depuis 2014, lorsque Moscou a annexé la Crimée et déclenché une guerre dans la région du Donbass. L'attaque NotPetya en 2017 avait ciblé le secteur économique ukrainien, tandis que des attaques en 2015 et 2016 contre les

infrastructures électriques avaient occasionné des coupures géantes, paralysant le pays. Redoutant qu'une stratégie identique puisse être utilisée à nouveau pour déstabiliser l'Ukraine et faciliter une invasion, plusieurs pays de l'Otan ont envoyé des experts en cyber-défense à Kiev. D'autre part, des opérations de cyber-résistance sont d'ores et déjà enclenchées, comme la cyberattaque menée par les Cyber Partisans en Biélorussie contre les serveurs de la compagnie nationale de chemin de fer russe. L'objectif : perturber l'acheminement des chars et de l'armement au Sud de la Biélorussie, d'où la Russie pourrait potentiellement mener une offensive vers Kiev avec l'armée biélorusse. Donc voilà, la guerre du futur n'est peut-être pas aussi bruyante qu'un véritable champ de bataille, mais son retentissement est clairement au moins tout aussi fracassant.

[*Musique de conclusion douce, évocatrice d'un jeu vidéo*]

Pour ne rien manquer de l'actualité technologique et scientifique, pensez à vous abonner à Fil de Science sur vos apps audio préférées, et pourquoi pas à nos autres podcasts. Je vous propose de découvrir notre dernier épisode de Chasseurs de Science, consacré à Leonid Rogozov, un intrépide médecin russe qui a dû s'opérer lui-même de l'appendicite alors qu'il était coupé du monde extérieur en Antarctique. Pour le reste, on se retrouve lundi prochain avec toujours plus d'actualité technologique. Bonne semaine à toutes et tous.