# En 2020, les hackers n'ont pas chômé : 4 fois plus de cyberattaques

Les spécialistes de la cybersécurité l'ont dit tout le long de l'année : les pirates ont fortement profité de la pandémie et du chaos qu'elle a entraîné dans le monde pour multiplier leurs attaques. Si la majorité étaient des campagnes de phishing ou des arnaques, même lorsqu'il s'agit de cyberattaques plus complexes, l'augmentation a été un record.

200 interventions de l'Ansi en 2020

Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi) en charge de protéger les systèmes informatiques en France, n'y est pas allé par quatre chemins sur BFMTV lundi 11 janvier 2021. Il explique que ses équipes ont fait tout simplement quatre fois plus d'interventions en 2020 par rapport à l'année précédente. « Dans les victimes qui font appel à l'Anssi, avec qui on est en contact, un chiffre à la louche : 50 opérations en 2019, 200 en 2020, donc c'est fois 4 ».

Le nombre d'interventions n'est toutefois pas égal au nombre de cyberattaques : l'Anssi n'est appelée que lorsque le problème ne peut être résolu ou qu'il y a un risque majeur pour la sécurité de la France, comme par exemple en cas d'attaque ciblant des entreprises travaillant dans le secteur de la défense.

Les ransomwares ont toujours la cote auprès des pirates

Si le particulier est généralement la cible de campagnes de phishing visant à lui voler ses données personnelles ou bancaires, les entreprises sont encore et toujours ciblées par les rançongiciels (ou ransomwares) : des logiciels malveillants qui bloquent les systèmes informatiques d'une entreprise. Une fois que les pirates ont le contrôle de ces systèmes, ils demandent une rançon pour les débloquer.

Tous les spécialistes de la sécurité sont concordes pour dire que les entreprises ne doivent pas payer : rien ne leur prouve en effet la bonne fois des pirates concernant la libération des systèmes, ni le fait que les pirates n'ont pas également volé des données ou ont installé d'autres logiciels malveillants. Seuls des spécialistes de la cybersécurité peuvent résoudre le problème et identifier les risques à venir.

Sur le devant de la scène depuis l'attaque mondiale du ransomware WannaCry en 2017, ces logiciels ne cessent d'être développés, ce qui nécessite une adaptation en continu de la part des services de sécurité informatique.