Cybersécurité : la guerre se joue aussi sur Internet
Internet

Posté par : JulieM

Publié le : 28/10/2022 13:00:00

Alors que la 23e édition des Assises de la Sécurité s'est clôturée le 15 octobre dernier, Guillaume Poupard, le directeur général de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) s'est exprimé sur ses craintes face à la multiplication des attaques contre les entreprises et les organismes publics.

Les ransomware, le phishing, ou encore les DDoS (Déni de Service Distribués) sont autant de menaces qui peuvent paralyser les systèmes.

Aussi anciennes que simples, les cybercriminels ne cessent de recourir à ces attaques afin de dérober des données et d'extorquer d'importantes sommes financières, faisant plus que jamais du numérique une arme redoutable.

Richard Hummel, responsable des renseignements sur les menaces de NETSCOUT, estime que la guerre se joue présentement aussi sur internet. Il est même possible d'identifier de nouveaux modes de conflits, uniquement par ordinateurs interposés.

L'intégrité géopolitique dans le cybermonde est indéniable et les guerres, la religion et la politique constituent un véritable champ de bataille pour les attaques DDoS.

« Les experts de la cybersécurité sont les moins directs du recours croissant aux technologies et au monde numérique, comme vecteur d'attaque par des groupes de cybercriminels mais également par des Etats. »

En effet, les cyberattaques sont devenues un problème à grande échelle pour les entreprises du monde entier. Cette année, nous avons pu constater que les conflits entraînent une hausse tendancielle du nombre de cyberattaques DDoS. Ces dernières ont une particularité au sens où elles sont adaptatives.

Par exemple, la zone EMEA a enregistré une hausse de plus de 7 % de ces menaces, dont beaucoup découlent du conflit entre l'Ukraine et la Russie. En France, les attaques et leur fréquence se sont intensifiées au premier semestre 2022. L'Ukraine enregistre, pour sa part, des pics considérables, qui sont également intensifiés les mois suivants sur la Russie, en particulier en juin.

La Finlande en a notamment subi les conséquences en manifestant son soutien à l'Ukraine en février, et en renouvelant son souhait d'intégrer l'OTAN, traduit par un redoublement d'attaques DDoS quotidiennes.

De même, alors que les tensions entre Taïwan, la Chine et Hong Kong s'intensifiaient au cours du premier semestre de cette année, des attaques DDoS contre Taïwan se sont produites en parallèle des événements publics connexes.

Ces exemples montrent que le constat est sans appel ; les attaques DDoS devraient continuer de gagner en puissance et en fréquence. C'est pourquoi les organisations doivent agir maintenant pour se protéger.

Or, les troubles géopolitiques ne constituent qu'un seul des facteurs de l'augmentation de ce type d'attaques. Les entreprises peuvent s'en prémunir et les empêcher de dévaster leur architecture en ligne grâce à des outils d'atténuation et de prévention.

Il est important que les structures auxquelles s'agisse d'entreprises, d'associations, d'Etats ou d'organismes puissent prévenir leurs défenses DDoS dès que possible pour s'assurer que leurs mesures de protection sont effectivement à la hauteur : en somme, elles doivent partir du principe qu'elles seront victimes d'attaques.

La mise en place de mesures d'atténuation à l'échelle de l'entreprise ou de l'organisation, combinée aux meilleures pratiques de sécurité conduites par des spécialistes permettront entre autres la protection des données, des infrastructures, ainsi que la préservation de leur image. »