Se protÃ©ger des attaques dâ□□extorsion DDoS .
Internet
PostÃ© par : JulieM
PubliÃ©e le : 2/4/2021 13:00:00

Les attaques par dÃ©ni de service distribuÃ© (DDoS), conÃ§ues pour submerger et paralyser les systÃ¨mes rÃ©seaux dâ□□une organisation, ont atteint un nombre record en 2020, et ont franchi le seuil des 10 millions, soit une augmentation de 1,6 million par rapport Ã 2019. Les DDoS pourraient bien poursuivre leur progression et marquer 2021 â□□ exposant les entreprises qui nâ□□y sont pas prÃ©parÃ©es Ã un risque accru.

Pour Philippe Alcoy, spÃ©cialiste de la sÃ©curitÃ© chez NETSCOUT, comme ce type de menaces peut paralyser lâ□□ensemble des applications et des services en ligne, anticiper et protÃ©ger les ressources essentielles en adoptant un plan de sÃ©curitÃ© et des mesures adaptÃ©es est indispensable.

Â« La plupart des vecteurs dâ□□attaque par DDoS et des techniques de ciblage sont bien connus. Par consÃ©quent, les organisations sont capables de prÃ©venir une attaque en utilisant des outils et systÃ¨mes de sÃ©curitÃ© Ã©prouvÃ©s contre les DDoS. Dans ce contexte, plusieurs prÃ©cautions sont recommandÃ©es.

Tout dâ□□abord, il est important que les organisations qui disposent de ressources critiques visibles par les utilisateurs prÃ©sents sur le rÃ©seau (employÃ©s et tiers) veillent Ã ce que les meilleures pratiques en matiÃ¨re dâ□□infrastructure, dâ□□architecture et dâ□□exploitation du rÃ©seau soient mises en place. Des politiques dâ□□accÃ¨s propres Ã chaque service, nâ□□autorisant le trafic internet que par lâ□□intermÃ©diaire des protocoles et des ports IP requis, sont donc Ã privilÃ©gier.

En outre, le trafic rÃ©seau pour lâ□□accÃ¨s Ã internet du personnel interne de lâ□□organisation doit Ãªtre dissociÃ© du trafic accessible au public. Dâ□□autre part, les services informatiques - tels que les systÃ¨mes de noms de domaines (DNS) - devraient Ã©galement Ãªtre conÃ§us, dÃ©ployÃ©s et exploitÃ©s de maniÃ¨re compatible avec lâ□□ensemble des meilleures pratiques rÃ©seau actuelles.

DÃ¨s lâ□□instant oÃ¹ elles se retrouvent confrontÃ©es Ã une tentative dâ□□extorsion DDoS, les organisations ciblÃ©es, quel que soit leur secteur, doivent immÃ©diatement contacter leur Ã©cosystÃ¨me, leurs Fournisseurs dâ□□AccÃ¨s Ã Internet (FAI), et les institutions compÃ©tentes, telles que la CNIL et lâ□□ANSSI, au regard de la situation.

Elles doivent veiller Ã ce que leurs plans de dÃ©fense contre les DDoS soient activÃ©s et validÃ©s, et rester vigilantes. Il est Ã©galement important de soumettre les systÃ¨mes de dÃ©fense contre les DDoS Ã des tests pÃ©riodiques, afin de sâ□□assurer que toute modification apportÃ©e aux serveurs/services/applications dâ□□une organisation soit intÃ©grÃ©e dans son plan de dÃ©fense.

Il est Ã©galement nÃ©cessaire que les organisations prennent connaissance des prÃ©cÃ©dentes campagnes dâ□□extorsion DDoS de grande envergure, afin de mieux se prÃ©parer aux menaces futures. Dans un monde connectÃ©, la visibilitÃ© et la connaissance sont ainsi indispensables pour anticiper une quelconque action.

En cybersÃ©curitÃ©, plus que dans tout autre domaine, le savoir permet en effet de garder une longueur dâ□□avance. Partir du principe quâ□□une attaque va arriver et identifier les vecteurs les plus susceptibles de se produire, permet de sâ□□y prÃ©parer et dâ□□y faire face.

Cette approche est dâ□□autant plus essentielle lorsque les entreprises sont dans le viseur des cybercriminels ; Ã lâ□□instar des secteurs de la santÃ©, de la finance, ou encore de lâ□□industrie, qui sont devenus au cours des derniÃ¨res annÃ©es des cibles de premier choix. La force actuelle des attaquants ne rÃ©side plus dans leur niveau de technicitÃ© mais dans leur niveau de persistance. Y opposer une rÃ©sistance Ã la hauteur permettra alors de faire front et de contrer les attaques dâ□□extorsion. Â»

Philippe Alcoy, SpÃ©cialiste de la SÃ©curitÃ© chez NETSCOUT