Les VPN, cibles de choix des attaques DDoS
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 12/1/2022 15:00:00

Les campagnes DDoS menÃ©es contre des entreprises se multiplient, et chacune de ces attaques dure plus longtemps et entraÃ®ne des coÃ»ts plus Ã©levÃ©s que les prÃ©cÃ©dentes. En effet, les acteurs malveillants qui les conÃ§oivent se basent sur de nouvelles technologies et stratÃ©gies pour mettre Ã mal les rÃ©seaux des entreprises mondiales.

Selon Philippe Alcoy, SpÃ©cialiste de la SÃ©curitÃ© chez NETSCOUT, la majoritÃ© de ces attaques DDoS visent des composants qui font depuis longtemps partie du rÃ©seau, tels que les dispositifs de rÃ©seau privÃ© virtuel (VPN), les pare-feux, ou encore les rÃ©partiteurs de tÃ¢ches.

Â« Ces dispositifs recÃ¨lent des informations utilisÃ©es pour acheminer et gÃ©rer le trafic. Câ□□est pourquoi ils sont plus susceptibles de subir des attaques DDoS ; puisquâ□□il sâ□□agit de campagnes conÃ§ues pour remplir les tables dâ□□Ã©tats avec des connexions illÃ©gitimes, empÃªchant ainsi celles lÃ©gitimes dâ□□accÃ©der aux services.

Selon nos recherches, plus de 41 000 attaques DDoS ont Ã©tÃ© lancÃ©es contre des VPN commerciaux au cours du premier semestre de 2021. Face Ã ce niveau de menace, il est indispensable que les entreprises comprennent pourquoi les cybercriminels ciblent les VPN et quelles sont les mesures Ã prendre pour mettre fin Ã ces attaques.

Sectionner un lien essentiel

La pandÃ©mie a contraint les entreprises Ã privilÃ©gier le tÃ©lÃ©travail lorsque cela Ã©tait possible. Elles se sont donc tournÃ©es en masse vers les VPN pour relier les employÃ©s distants aux ressources de lâ□□organisation. Cependant, les cyberattaques DDoS contre les VPN ont accru significativement en parallÃ¨le, et ce pour plusieurs raisons.

En effet, ces campagnes malveillantes isolent les utilisateurs des ressources en ligne de leur organisation et empÃªchent donc les Ã©quipes de sÃ©curitÃ© de rÃ©agir Ã ces incidents, ainsi quâ□□Ã toute autre type de cyberattaques. La pandÃ©mie a Ã©galement contraint les entreprises Ã Ã©tendre les services numÃ©riques proposÃ©s aux clients et aux fournisseurs, ce qui a considÃ©rablement amplifiÃ© les effets potentiels dâ□□une attaque contre le VPN de lâ□□entreprise.

Les cybercriminels ont par consÃ©quent conscience que les entreprises sont plus exposÃ©es lorsque les employÃ©s travaillent Ã distance, ce qui les motive pour lancer des attaques DDoS ciblÃ©es contre les VPN et autres dispositifs Ã table dâ□□Ã©tats. Ainsi, 83 % des organisations interrogÃ©es dans le cadre de notre enquÃªte WISR (Worldwide Infrastructure Security Survey) ont indiquÃ© que les attaques DDoS ciblant les pare-feux et/ou les dispositifs VPN avaient entraÃ®nÃ© une interruption de service, soit une augmentation de 21 % par rapport Ã 2019.

La solution : une attÃ©nuation intelligente et sans Ã©tat

La seule faÃ§on dâ□□arrÃªter les attaques DDoS ciblant les VPN dâ□□entreprise est de mettre en Å□uvre une solution intelligente dâ□□attÃ©nuation des DDoS qui fonctionne sans Ã©tat, ou en semi-Ã©tat, et intÃ¨gre les fonctionnalitÃ©s suivantes :

â□¢ Utilise principalement la technologie de traitement des paquets sans Ã©tat.
â□¢ Lorsquâ□□une inspection avec Ã©tat est nÃ©cessaire, recourt Ã un test Ã©phÃ©mÃ¨re pour dÃ©terminer la lÃ©gitimitÃ© de la connexion.
â□¢ Est dÃ©ployÃ©e dans les locaux de lâ□□entreprise, en amont du pare-feu, de la passerelle VPN et dâ□□autres dispositifs Ã Ã©tat.
â□¢ Sâ□□intÃ¨gre facilement dans la pile de cybersÃ©curitÃ©.

Alors seulement, les organisations pourront mettre fin Ã la vague dâ□□attaques DDoS qui sÃ©vit actuellement et qui tirent profit de vulnÃ©rabilitÃ©s inhÃ©rentes Ã une adoption rapide de technologie VPN. Alors quâ□□une nouvelle annÃ©e est sur le point de dÃ©buter, il est en effet urgent de sâ□□armer face Ã lâ□□Ã©volution des cybermenaces, afin que les entreprises en 2022 ne subissent pas le mÃªme volume dâ□□attaques DDoS. Â»