Supply chain de la connectivitÃ©, nouvelle cible des hackers
Internet
PostÃ© par : JulieM
PubliÃ©e le : 19/1/2022 13:00:00

Il est courant de penser que les cyberattaques sont menÃ©es contre des entitÃ©s spÃ©cifiques, telles que des entreprises ou des fournisseurs de services. Pourtant, les cybercriminels ont dÃ©sormais une autre cible en vue : la supply chain de la connectivitÃ©. La connectivitÃ© fait ici rÃ©fÃ©rence Ã toutes les technologies et services qui permettent aux entreprises et aux particuliers de rester connectÃ©s Ã Internet.

Selon Philippe Alcoy, SpÃ©cialiste de la SÃ©curitÃ© chez NETSCOUT, les services visÃ©s sont ceux qui soutiennent les appareils connectÃ©s, et permettent aux entreprises de se digitaliser ou de dÃ©placer des ressources vers le cloud :

Â« Les hackers se sont longtemps concentrÃ©s sur la perturbation des services qui assurent la connectivitÃ©, ciblant Ã la fois les utilisateurs et lâinfrastructure opÃ©rationnelle des entreprises elles-mÃªmes. Mais lâaugmentation spectaculaire des attaques depuis le dÃ©but de la pandÃ©mie, en particulier celles par dÃ©ni de service distribuÃ© (DDoS), nâest pas une coÃ¯ncidence.

Selon nos recherches, les fournisseurs de services qui assurent la connectivitÃ© reprÃ©sentaient 4 des 10 principaux secteurs ciblÃ©s par les attaques DDoS. Les opÃ©rateurs historiques de tÃ©lÃ©communications occupent ainsi la tÃªte du classement, avec pas moins de 283 516 attaques ; les fournisseurs de services mobiles sont troisiÃ¨mes avec 84 151 attaques ; les autres opÃ©rateurs de tÃ©lÃ©communication sont septiÃ¨mes avec 14 628 attaques ; et les revendeurs tÃ©lÃ©com arrivent neuviÃ¨mes avec 2 175 attaques.

Par ailleurs, lâaugmentation des attaques contre ces fournisseurs de connectivitÃ© a coÃ¯ncidÃ© avec de plus importantes campagnes malveillantes Ã lâencontre des entreprises qui les utilisent. En effet, Ã cause du Covid, les entreprises ont dÃ» soutenir le tÃ©lÃ©travail beaucoup plus rapidement que prÃ©vu.

Plus prÃ©cisÃ©ment, les cybercriminels ont concentrÃ© leur attention sur les technologies qui permettent Ã des services tels que le Cloud de fonctionner sur Internet, en particulier les serveurs DNS (Domain Name System), les rÃ©seaux privÃ©s virtuels (VPN), ou encore les Internet Exchange (IX).

Heureusement, les fournisseurs de services et les entreprises peuvent prendre plusieurs mesures pour protÃ©ger la supply chain de la connectivitÃ© contre les attaques DDoS, notamment en :

Assurant leur conformitÃ© aux meilleures pratiques actuelles de lâindustrie (BCPs) pour les organisations ayant des ressources Internet publiques critiques ;
Mettant en Åuvre des dÃ©fenses DDoS appropriÃ©es pour les Ã©lÃ©ments Internet publiques et lâinfrastructure de support ;
Effectuant des tests frÃ©quents et rÃ©alistes du plan dâattÃ©nuation des attaques DDoS pour les organisations qui exploitent des services et des infrastructures Internet critiques et publiques ;
Personnalisant la sÃ©lection, le rÃ©glage et le dÃ©ploiement des contre-mesures.

Les cybercriminels continuent de viser les points les plus vulnÃ©rables des entreprises pour parvenir Ã leurs fins. La supply chain de la connectivitÃ© est dÃ©sormais une cible clÃ© et les

entreprises doivent prendre conscience de ses risques pour pouvoir se protÃ©ger en consÃ©quence. Â»