Les cyberattaques aggravent la crise mondiale de la cybersÃ©curitÃ©
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 22/9/2021 15:00:00

Le chiffre dâ□□environ 5,4 millions dâ□□attaques DDoS reprÃ©sente une augmentation de 11 % par rapport au premier semestre 2020 et devrait dÃ©passer le record de lâ□□annÃ©e prÃ©cÃ©dente, avec des effets considÃ©rables sur les passerelles Internet critiques

NETSCOUT SYSTEMS, INC., publie les conclusions de son rapport semestriel sur les menaces Threat Intelligence Report, lequel met en Ã©vidence la gravitÃ© des effets que les cyberattaques continuent dâ□□avoir sur les organisations privÃ©es et publiques et sur les gouvernements du monde entier.

Au cours du premier semestre 2021, les cybercriminels ont lancÃ© environ 5,4 millions dâ□□attaques par dÃ©ni de service distribuÃ© (DDoS), soit une augmentation de 11 % par rapport aux chiffres du semestre prÃ©cÃ©dent.

De plus, les projections de donnÃ©es de lâ□□Active Level Threat Analysis System (ATLASâ□¢) Security Engineering and Response Team (ASERT) de NETSCOUT laissent entrevoir que 2021 sera une nouvelle annÃ©e record, en passe de dÃ©passer les 11 millions dâ□□attaques DDoS mondiales. Lâ□□ASERT prÃ©voit la poursuite de cette longue sÃ©rie dâ□□innovations de la part des attaquants, alimentant ainsi une crise accrue de la cybersÃ©curitÃ© qui continuera dâ□□affecter les organisations publiques et privÃ©es.

Dans le sillage de Colonial Pipeline, JBS, Harris Federation, le radiodiffuseur australien Channel Nine, CNA Financial et plusieurs autres attaques trÃ¨s mÃ©diatisÃ©es, lâ□□impact des DDoS et autres attaques de cybersÃ©curitÃ© sâ□□est fait sentir dans le monde entier. En consÃ©quence, les principaux pouvoirs publics mettent en place de nouveaux programmes et de nouvelles politiques pour se dÃ©fendre contre les attaques, tandis que les organisations policiÃ¨res engagent des actions de collaboration sans prÃ©cÃ©dent pour faire face Ã la crise.

Au cours du premier semestre 2021, les cybercriminels ont activÃ© et exploitÃ© sept nouveaux vecteurs dâ□□attaque DDoS de rÃ©flexion/amplification, exposant ainsi les organisations Ã un risque accru. La prolifÃ©ration des vecteurs dâ□□attaque a entraÃ®nÃ© une hausse des attaques DDoS Ã vecteurs multiples, avec un record de 31 vecteurs dÃ©ployÃ©s dans une seule attaque menÃ©e contre une organisation.

Voici dâ□□autres conclusions importantes du Â« Threat Intelligence Report Â» de NETSCOUT pour le premier semestre 2021 :

Les nouvelles techniques dâ□□attaque DDoS adaptatives Ã©chappent aux dÃ©fenses traditionnelles. En personnalisant leurs stratÃ©gies, les cybercriminels ont fait Ã©voluer leurs attaques pour contourner les dÃ©fenses DDoS statiques basÃ©es sur le cloud et sur site et pour cibler les banques commerciales et les processeurs de cartes de crÃ©dit.

Â La supply chaines de composants de connectivitÃ© subit de plus en plus dâ□□attaques. Les acteurs malveillants qui cherchent Ã causer le maximum de dommages collatÃ©raux ont concentrÃ© leurs efforts sur les composants indispensables Ã Internet, notamment les serveurs DNS, les concentrateurs de rÃ©seaux privÃ©s virtuels (VPN), les services et les Internet Exchange, en perturbant les passerelles essentielles.

Â Les cybercriminels ajoutent le DDoS Ã leur arsenal pour lancer des campagnes de triple extorsion. Les ransomwares ont pris de lâ□□ampleur, et les extorqueurs ajoutent les attaques par dÃ©ni de service (DDoS) Ã leur arsenal dâ□□attaques afin dâ□□accroÃ®tre la pression sur les victimes et de mettre les Ã©quipes de sÃ©curitÃ© Ã rude Ã©preuve. La triple extorsion combine le chiffrement de fichiers, le vol de donnÃ©es et les attaques DDoS, augmentant ainsi la possibilitÃ© que les cybercriminels obtiennent un paiement.

Â Lâ□□attaque DDoS la plus rapide a enregistrÃ© une augmentation de 16,17 % par rapport Ã lâ□□annÃ©e prÃ©cÃ©dente. Câ□□est un utilisateur brÃ©silien de lâ□□Internet haut dÃ©bit filaire qui a lancÃ© lâ□□attaque, probablement en ciblant des jeux en ligne. En utilisant les vecteurs rÃ©flexion/amplification DNS, TCP ACK flood, TCP RST flood, et TCP SYN/ACK rÃ©flexion/amplification, lâ□□attaque sophistiquÃ©e a enregistrÃ© un dÃ©bit de 675 Mpps.

Â La plus grande attaque DDoS, 1,5 Tbps, a reprÃ©sentÃ© une augmentation de 169 % par rapport Ã lâ□□annÃ©e prÃ©cÃ©dente. Les donnÃ©es de lâ□□ASERT ont identifiÃ© cette attaque menÃ©e contre un FAI allemand, au moyen dâ□□un vecteur rÃ©flexion/amplification DNS. Cette attaque marque une progression spectaculaire par rapport Ã toutes les attaques enregistrÃ©es au premier semestre 2020.

Â Les botnets jouent un rÃ´le important dans les attaques DDoS - Le suivi des clusters de botnets et des zones Ã haute densitÃ© de sources dâ□□attaques dans le monde entier a mis en Ã©vidence la maniÃ¨re dont les adversaires malveillants ont utilisÃ© ces botnets pour participer Ã plus de 2,8 millions dâ□□attaques DDoS. En outre, les botnets IoT notoires que sont Gafgyt et Mirai continuent de reprÃ©senter une menace grave, puisquâ□□ils ont contribuÃ© Ã plus de la moitiÃ© des attaques DDoS enregistrÃ©es.

Â« Les cybercriminels font la une des journaux parce quâ□□ils dÃ©ploient un nombre sans prÃ©cÃ©dent dâ□□attaques DDoS pour tirer profit des modalitÃ©s de travail Ã distance qui ont dÃ» Ãªtre imposÃ©es en raison de la pandÃ©mie. Pour ce faire, ils sâ□□attaquent Ã des Ã©lÃ©ments vitaux de la chaÃ®ne dâ□□approvisionnement en connectivitÃ©, dÃ©clare Richard Hummel, responsable des renseignements sur les menaces chez NETSCOUT.

Les gangs de ransomware ont intÃ©grÃ© Ã leur arsenal des stratÃ©gies DDoS de triple extorsion. Dans le mÃªme temps, la campagne dâ□□extorsion DDoS de Fancy Lazarus est passÃ©e Ã la vitesse supÃ©rieure, menaÃ§ant des organisations dans de multiples secteurs dâ□□activitÃ©, en se concentrant sur les fournisseurs dâ□□accÃ¨s Internet et plus particuliÃ¨rement sur leurs serveurs DNS faisant autoritÃ©. Â»

Le Â« Threat Intelligence Report Â» de NETSCOUT traite des derniÃ¨res tendances et activitÃ©s dans le paysage des menaces DDoS. Il couvre les donnÃ©es sÃ©curisÃ©es Ã partir de lâ□□Active Level Threat Analysis System (ATLASâ□¢) de NETSCOUT couplÃ© aux connaissances de lâ□□ATLAS Security Engineering & Response Team (ASERT) de NETSCOUT.

La visibilitÃ© et lâ□□analyse prÃ©sentÃ©es dans le Â« Threat Intelligence Report Â» et OmnisÃ□ Threat Horizon alimentent le flux de renseignements ATLAS utilisÃ© dans lâ□□ensemble du portefeuille de produits de sÃ©curitÃ© Omnis de NETSCOUT, afin de dÃ©tecter et de bloquer les activitÃ©s menaÃ§antes auxquelles sont confrontÃ©s les entreprises et les fournisseurs de services du monde entier.

Pour de plus amples informations sur le Â« Threat Intelligence Report Â» semestriel de ***NETSCOUT*** ,Â