Pas d'Internet sans DNS : multiplication des attaques Â« water-torture Â»
Internet
PostÃ© par : JerryG
PubliÃ©e le : 20/12/2023 14:00:00

Les serveurs DNS sont de plus en plus ciblÃ©s par les cybercriminels. Le DNS est le carnet d'adresses d'Internet qui convertit les noms en adresses IP pour permettre aux appareils, aux applications et aux services de savoir oÃ¹ envoyer les paquets.

D'aprÃ¨s NETSCOUT, les attaques de type Â« water-torture Â» contre le DNS sont passÃ©es d'une moyenne de 144 attaques quotidiennes au dÃ©but de l'annÃ©e 2023 Ã 611 Ã la fin du mois de juin, soit une augmentation de prÃ¨s de 353 % en l'espace de six mois seulement. L'attaque la plus impactante a impliquÃ© environ 89,4 millions de requÃªtes par seconde (mqps), soit une augmentation de 51,1 % par rapport Ã la mÃªme pÃ©riode en 2022.

Depuis 1997, les cybercriminels lancent des attaques contre les serveurs DNS pour perturber les applications et les appareils. Si le nom d'un site web, d'un service de jeu en ligne ou d'un fournisseur de vidÃ©o en continu ne peut Ãªtre converti, cela a le mÃªme impact qu'une attaque rÃ©ussie sur le service lui-mÃªme.

Ceci s'applique Ã©galement aux composants critiques d'une organisation tels que les serveurs web, les services de collaboration et les concentrateurs VPN. Si les serveurs DNS faisant autoritÃ© d'une organisation sont perturbÃ©s avec succÃ¨s, l'ensemble de l'entreprise est virtuellement inaccessible. MalgrÃ© cela, les serveurs DNS sont souvent exclus des plans de dÃ©fense DDoS des entreprises.

Philippe Alcoy, spÃ©cialiste de la sÃ©curitÃ© chez NETSCOUT, analyse la prolifÃ©ration des attaques par inondation de requÃªtes visant les serveurs DNS.

Â« La plupart des attaques contre les serveurs DNS consistent en un dÃ©luge de requÃªtes visant Ã surcharger les serveurs afin qu'ils ne puissent plus fournir de services de rÃ©solution de noms aux utilisateurs lÃ©gitimes, et visent n'importe quel type d'Ã©lÃ©ment DNS dans le domaine ciblÃ©.

Les plus efficaces impliquent des taux Ã©levÃ©s de requÃªtes par seconde (qps) pour des entrÃ©es DNS inexistantes. Non seulement elles mettent directement en cause la capacitÃ© des serveurs DNS attaquÃ©s Ã rÃ©pondre Ã des requÃªtes lÃ©gitimes, mais elles les poussent Ã©galement Ã gÃ©nÃ©rer des rÃ©ponses nÃ©gatives (serveurs DNS faisant autoritÃ©) ou Ã les transmettre (serveurs DNS rÃ©cursifs), indiquant que les noms de domaine demandÃ©s n'existent pas.

Cela augmente considÃ©rablement la charge des serveurs DNS exposÃ©s aux attaques DDoS de type Â« DNS query flooding Â» (inondation de requÃªtes DNS).

Depuis 2009, une mÃ©thode particuliÃ¨rement efficace pour gÃ©nÃ©rer des attaques DDoS par inondation de requÃªtes DNS est de plus en plus observÃ©e : les attaques de type Â« water-torture Â».

Des Ã©tiquettes DNS y sont gÃ©nÃ©rÃ©es de maniÃ¨re pseudo-alÃ©atoire et ajoutÃ©es ou remplacÃ©es aux domaines DNS existants. Les attaques par substitution, lesquelles s'appuient sur des dictionnaires d'Ã©tiquettes DNS qui semblent plausibles mais qui n'existent pas, sont moins

courantes mais peuvent reprÃ©senter un dÃ©fi encore plus grand pour les organisations non prÃ©parÃ©es.

Les secteurs de l'accÃ¨s haut dÃ©bit filaire et sans fil, des FAI/cloud/VPS/hÃ©bergement/colocation et de l'assurance ont Ã©tÃ© particuliÃ¨rement touchÃ©s par les attaques par water-torture au cours des six premiers mois de l'annÃ©e 2023. Les fournisseurs de tÃ©lÃ©communications, de traitement des donnÃ©es, dâ□□hÃ©bergement et de services connexes, des sociÃ©tÃ©s d'achat Ã©lectronique et de vente par correspondance ainsi que des agences d'assurance et bureaux de courtage figurent Ã©galement parmi les cibles de ces attaques.

La diversitÃ© des secteurs ciblÃ©s laisse Ã penser que des cyberattaquants motivÃ©s par des considÃ©rations idÃ©ologiques et des extorqueurs DDoS Ã la recherche d'un gain financier s'attaquent aux serveurs DNS afin de perturber les propriÃ©tÃ©s et les activitÃ©s en ligne des entreprises.

La prÃ©valence croissante des services DNS rÃ©cursifs ouverts, connus comme sources de ces attaques indique que les attaquants tentent intentionnellement dâ□□Ã©viter de faire passer leur trafic Ã travers les opÃ©rateurs de rÃ©seau responsables de la sÃ©curitÃ© des ressources DNS.

Les attaques par Â« water-torture Â» qui se reflÃ¨tent dans ces services sont plus difficiles Ã attÃ©nuer pour les dÃ©fenseurs, le trafic d'attaque Ã©tant mÃ©langÃ© Ã des requÃªtes DNS authentiques issues de sources lÃ©gitimes. Face Ã cette recrudescence dâ□□attaques, il est impÃ©ratif que les entreprises veillent Ã ce que leur infrastructure DNS rÃ©cursive et faisant autoritÃ© soit incluse dans les plans de dÃ©fense contre les attaques DDoS et fasse l'objet d'audits rÃ©guliers. Â»