Attaques DDoS : La mÃ©thode du pro-russe Killnet.
Internet
PostÃ© par : JulieM
PubliÃ©e le : 4/5/2023 13:00:00

DÃ¨s son commencement, la guerre russo-ukrainienne a vu naÃ®tre une recrudescence des attaques par DÃ©ni de Service DistribuÃ© (DDoS) dâ□□une envergure inÃ©dite contre des entitÃ©s gouvernementales.

Le groupe pro-russe Killnet a notamment entraÃ®nÃ© une hausse des attaques DDoS Ã hauteur de 16 815 % contre le secteur de la sÃ©curitÃ© nationale des Ã□tats-Unis au second semestre 2022.

Des pics d'attaques ont Ã©galement Ã©tÃ© enregistrÃ©s en juin 2022, le jour oÃ¹ le prÃ©sident amÃ©ricain Joe Biden et le prÃ©sident franÃ§ais Emmanuel Macron ont publiquement rÃ©affirmÃ© leur soutien Ã l'Ukraine lors du sommet du G7.

Philippe Alcoy, spÃ©cialiste de la sÃ©curitÃ© NETSCOUT, explique comment la conjoncture sociopolitique dÃ©finit la multiplication des attaques DDoS :

Â« Les attaques DDoS sont plus faciles Ã lancer, plus complexes dans leur conception et plus difficiles Ã attÃ©nuer, car les cybercriminels contrecarrent les efforts de sÃ©curitÃ©. Des groupes comme Killnet ont Ã©galement commencÃ© Ã tirer parti de ressources telles que les proxys ouverts, pour les aider Ã lancer des campagnes d'attaques DDoS Ã caractÃ¨re politique.

Depuis le dÃ©but de la guerre entre la Russie et lâ□□Ukraine, la France est la cible de nombreuses cybermenaces DDoS, pour la plupart revendiquÃ©es par des groupes pro-russes. Pour preuve, en mars 2023, plusieurs aÃ©roports franÃ§ais ont Ã©tÃ© ciblÃ©s par Anonymous Sudan, un groupe dâ□□hacktivistes sympathisant de Killnet. Ces cybermenaces sâ□□Ã©tendent Ã lâ□□Europe entiÃ¨re et mÃªme au-delÃ .

L'Allemagne a Ã©galement Ã©tÃ© victime d'attaques DDoS menÃ©es par le groupe Killnet contre des sites web aÃ©roportuaires et gouvernementaux, en guise de reprÃ©sailles suite Ã son annonce de livraison de chars Leopard 2 Ã l'Ukraine.

Les attaques DDoS contre des sites web d'aÃ©roports allemands et franÃ§ais, d'hÃ´pitaux amÃ©ricains et d'organisations financiÃ¨res du monde entier montrent que les cybercriminels visent et affectent de plus en plus le quotidien de nombreux citoyens pour semer le chaos.

Si la plupart des campagnes malveillantes menÃ©es par des groupes tels que Killnet ont ciblÃ© des sites web et leur accessibilitÃ© gÃ©nÃ©rale, il est probable quâ□□ils s'en prennent Ã©galement Ã des infrastructures critiques aux ramifications plus importantes.

Dans un contexte gÃ©opolitique complexe, ces menaces sont plus rÃ©elles que jamais et risquent de se rÃ©pÃ©ter Ã lâ□□avenir. Pour faire face, les organisations doivent les anticiper et disposer de systÃ¨mes de protection adaptÃ©s contre les DDoS Ã mÃªme de rÃ©duire au minimum le temps nÃ©cessaire pour se dÃ©fendre contre une attaque.

Elles doivent Ã©galement Ãªtre conscientes des vecteurs utilisÃ©s par les cybercriminels. En effet, leur arsenal Ã©tant de plus en plus sophistiquÃ©, une offensive contre une infrastructure critique pourrait sans aucun doute impacter massivement la population, si elle n'est pas dÃ©tectÃ©e Ã

temps. Â»