Les attaques DDoS contre la Pologne montent en flÃ¨che
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 12/2/2024 14:00:00

Les changements de dirigeants politiques peuvent entraÃ®ner des perturbations dans de nombreux domaines. L'un d'entre eux est le cyberespace, oÃ¹ les attaques DDoS connaissent souvent un pic lors d'un changement de garde.

Ces pics sont souvent le fait d'hacktivistes et d'autres groupes qui s'opposent aux points de vue des nouveaux Ã©lus. Parmi les groupes les plus connus, citons Killnet, Anonymous Sudan et NoName057, qui ciblent souvent des pays perÃ§us comme Â« anti-musulmans Â» ou qui manifestent leur soutien et leur solidaritÃ© avec l'Ukraine.

Le groupe le plus connu qui s'attaque Ã la Pologne est NoName057. Il a ciblÃ© plusieurs types de sites web, notamment l'administration gouvernementale, le transport et la logistique, la finance (banques commerciales), le gouvernement judiciaire, l'industrie manufacturiÃ¨re, le transport aÃ©rien et les mÃ©dias. Cette liste ne reprÃ©sente que ce que NoName057 a revendiquÃ© ; la liste rÃ©elle pourrait Ãªtre beaucoup plus longue.

En suivant les tendances des attaques DDoS contre la Pologne depuis la perspective globale de NETSCOUT, nous constatons que les pics commencent quelques jours seulement aprÃ¨s que le Premier ministre Tusk et son nouveau gouvernement aient prÃªtÃ© serment.

Le volume des attaques commence Ã augmenter aux alentours de NoÃ«l et reste Ã©levÃ© jusqu'Ã aujourd'hui, avec un pic le 14 janvier, avec plus de 5 000 attaques au total. Ce pic d'attaques, alimentÃ© par le soutien du nouveau gouvernement Ã l'Ukraine, a entraÃ®nÃ© une multiplication par 4 du volume des attaques DDoS.

NoName057 utilise gÃ©nÃ©ralement des botnets exÃ©cutant son code DDoSia pour mener Ã bien ses attaques. En examinant le trafic d'attaques DDoS de la Pologne, on a dÃ©couvert que prÃ¨s de la moitiÃ© des attaques contre le pays provenaient de nÅ□uds classÃ©s comme bots DDoS. Cet afflux massif reprÃ©sente 15 Ã 20 % des attaques DDoS menÃ©es par des botnets Ã l'Ã©chelle mondiale et dirigÃ©es comme un tÃ©lescope sur la Pologne.

Des groupes comme NoName057 continueront Ã mener une guerre politique et religieuse contre toute nation qui se mettrait en travers de leurs idÃ©aux et de leurs objectifs. Cela signifie que les gouvernements, les fournisseurs de services et les entreprises, ainsi que la sociÃ©tÃ© dans son ensemble, doivent se prÃ©parer Ã ce que ces attaques se poursuivent et s'intensifient.

Cela est particuliÃ¨rement vrai lorsque les nations et le public soutiennent les idÃ©aux auxquels ces groupes s'opposent. La meilleure dÃ©fense est une solution de protection DDoS solide. DÃ©couvrez comment la gamme de produits Arbor DDoS de NETSCOUT peut vous aider Ã rester opÃ©rationnel en cas d'attaques DDoS.

Richard Hummel, ASERT Threat Intelligence Lead chez NETSCOUT