Elections 2024 : Des attaques DDoS Ã motivation politique
Internet
PostÃ© par : JerryG
PubliÃ©e le : 4/3/2024 13:00:00

L'annÃ©e 2024 s'annonce cruciale sur la scÃ¨ne internationale avec la tenue de plus de 60 Ã©lections, incluant celles des cinq nations les plus peuplÃ©es de la planÃ¨te. Cette annÃ©e, un nombre record d'Ã©lecteurs, reprÃ©sentant prÃ¨s de la moitiÃ© (49 %) de la population mondiale, est attendu aux urnes, soulignant l'importance et l'Ã©tendue de ces scrutins.

Ces Ã©lections, se dÃ©roulant dans des pays tels que les Ã tats-Unis, le Royaume-Uni, la Russie, le BrÃ©sil, et au sein de l'Union EuropÃ©enne, sont susceptibles de redÃ©finir le paysage gÃ©opolitique. ParallÃ¨lement, nous assistons Ã l'Ã©mergence de cybermenaces, avec des attaquants, frustrÃ©s ou dissidents, orchestrant des attaques par dÃ©ni de service distribuÃ© (DDoS) pour des raisons politiques.

Richard Hummel, threat intelligence lead chez NETSCOUT, met en lumiÃ¨re l'impact des attaques DDoS en pÃ©riode Ã©lectorale et explique comment les changements de leadership politique peuvent engendrer des perturbations dans le cyberespace :

Â« Les motivations politiques ont contribuÃ© Ã une augmentation significative des attaques DDoS ces derniÃ¨res annÃ©es. La SuÃ¨de, par exemple, a Ã©tÃ© la cible d'attaques rÃ©pÃ©tÃ©es Ã mesure qu'elle avanÃ§ait dans son processus d'adhÃ©sion Ã l'OTAN, tandis que le Bangladesh a subi des attaques avant ses derniÃ¨res Ã©lections gÃ©nÃ©rales. Nous avons Ã©galement observÃ© que les Ã©lections prÃ©sidentielles particuliÃ¨rement disputÃ©es en Colombie en 2022 ont Ã©tÃ© marquÃ©es par des vagues successives d'attaques DDoS.

Les cybercriminels ont la capacitÃ© de perturber les Ã©lections de diverses maniÃ¨res, notamment en saturant les sites d'information et d'inscription des Ã©lecteurs, en interrompant les plateformes des campagnes et en ciblant la diffusion des rÃ©sultats officiels. Si ces attaques sont lancÃ©es suffisamment proches des Ã©chÃ©ances d'inscription ou de vote, elles peuvent empÃªcher l'accÃ¨s aux services en ligne essentiels, risquant ainsi de priver des Ã©lecteurs de leur droit de vote.

Cependant, l'intÃ©rÃªt des cybercriminels ne se limite pas aux campagnes Ã©lectorales ; les rÃ©sultats des scrutins peuvent Ã©galement entraÃ®ner une recrudescence des cyberattaques. Ã titre d'exemple, Ã la fin de l'annÃ©e 2023, le groupe hacktiviste pro-russe NoName057 a initiÃ© des attaques contre le gouvernement polonais suite Ã l'Ã©lection de Donald Tusk au poste de Premier ministre. Le soutien du nouveau gouvernement envers l'Ukraine, en opposition directe avec les intÃ©rÃªts de ces acteurs malveillants, a semble-t-il alimentÃ© cette vague d'attaques.

Des groupes hacktivistes tels que NoName057 et Anonymous Soudan se distinguent par leur engagement dans une lutte politique et religieuse contre les nations ou les dirigeants qui s'opposent Ã leurs idÃ©aux. Ces groupes visent souvent les pays perÃ§us comme Ã©tant contre l'islam ou ceux soutenant l'Ukraine, attaquant toute entitÃ© divergeant de leur ligne directrice.

Face Ã ce contexte, il est primordial que les gouvernements, les fournisseurs de services, les entreprises et la sociÃ©tÃ© dans son ensemble soient prÃªts Ã faire face Ã une augmentation des attaques DDoS en cette annÃ©e Ã©lectorale dense. Il est essentiel que ces organisations adoptent les meilleures pratiques actuelles du secteur et s'assurent que leurs dispositifs de protection contre les DDoS sont efficaces et prÃ©parÃ©s Ã contrer les menaces posÃ©es par les

groupes hacktivistes. Â»