Le 11 octobre 2012 : le jour oÃ¹ Facebook a plantÃ©
Internet
PostÃ© par : JulieM
PubliÃ©e le : 19/10/2012 14:00:00

Une faille DNS, un bug dâ□□adresse IP, quâ□□est-ce que câ□□est ? **. Rodolphe Moreno**, Regional Manager Southern Europe chez **Infoblox** , nous informe sur cet Ã©vÃ©nement.

Le DNS est lâ□□annuaire de tous les rÃ©seaux qui fournissent un service de traduction des noms lisibles par les humains en des adresses informatiques numÃ©riques (ou adresses IP). Ainsi facebook.com devient 69.171.224.11. Le DNS, la gestion des adresses IP (IPAM) et lâ□□attribution des adresses IP (DHCP), sont des services indispensables : sâ□□ils ne fonctionnent pas, le rÃ©seau, lâ□□accÃ¨s aux applications et la productivitÃ© des utilisateurs sâ□□interrompent Ã©galement.

Le DNS est aujourdâ□□hui la cible privilÃ©giÃ©e des attaques, et elles peuvent Ãªtre de plusieurs types : cache poisoning, fuite de donnÃ©es, base des botnetsâ□¦ Il suffit de regarder le dernier incident survenu sur le cÃ©lÃ¨bre rÃ©seau social Facebook. Suite Ã une modification du DNS dans le cadre d'un test d'optimisation du trafic, des informations erronÃ©es se sont propagÃ©es sur la toile, rendant inaccessible le site pour des milliers dâ□□utilisateurs pendant quelques

heures. Ce genre dâ□□incident est particuliÃ¨rement impactant pour un site oÃ¹ le business model est basÃ© sur la publicitÃ© gÃ©nÃ©rÃ©e par les pages vues.

En plus des erreurs humaines, le scÃ©nario dâ□□attaque est Ã©galement possible comme le Â« dÃ©ni de service Â», le plus commun, oÃ¹ lâ□□attaquant cherche Ã rendre le service inaccessible et Ã rendre publique cette information. Des attaques plus sophistiquÃ©es et plus graves peuvent sâ□□Ã©tendre sur plusieurs jours, voire plusieurs semaines.

Ce qui est arrivÃ© Ã Facebook est plus courant quâ□□on ne le pense, et touche les TPE jusquâ□□aux multinationales. Ainsi, les sites comme AL Jazeera, ZoneEdit et GoDaddy ont subi des arrÃªts de service importants durant le mois de septembre. Plus rÃ©cemment, une attaque au BrÃ©sil a touchÃ© plus de 4 millions dâ□□utilisateurs : en changeant lâ□□adresse du DNS sur les modems-routeurs, les pirates ont redirigÃ©s les requÃªtes des utilisateurs vers une quarantaine de serveurs configurÃ©s comme DNS autoritatifs pour des sites bancaires ou grand public. Les utilisateurs Ã©taient donc renvoyÃ©s vers des sites de phishing.

Il existe nÃ©anmoins des solutions dâ□□automatisation des DNS et de gestion des adresses IP qui permettent de rÃ©duire les risques dâ□□erreur humaine, et rendent les changements dans les rÃ©seaux plus transparents.

La gestion de l'adressage (DNS, DHCP) fait partie du quotidien des administrateurs rÃ©seaux. La gÃ©nÃ©ralisation de la virtualisation a rendu cette tÃ¢che fastidieuse et peut impliquer plusieurs intervenants. Infoblox propose dâ□□automatiser ces diffÃ©rentes opÃ©rations. Infoblox est leader dans lâ□□automatisation des fonctions critiques du rÃ©seau avec une offre couvrant les services IP (DNS/DHCP, gestion de lâ□□adressage IP), la gestion et le changement des configurations des Ã©quipements rÃ©seaux. Ses solutions apportent une meilleure visibilitÃ© et un meilleur contrÃ´le de lâ□□infrastructure.