Attaque Sybil sur un rÃ©seau pair-Ã -pair

Description

Lâ€™intÃ©rÃªt des rÃ©seaux pair-Ã -pair, socle des blockchains publiques, est de se passer dâ€™autoritÃ© centralisÃ©e pour fonctionner. Les attaques dites Â«Â SybilÂ Â» consistent Ã crÃ©er de fausses identitÃ©s pour corrompre le rÃ©seau.

Le propre dâ€™une architecture informatique pair-Ã -pair est dâ€™opÃ©rer des Ã©changes entre plusieurs ordinateurs connectÃ©s au systÃ¨me sans passer par un serveur central.Â Tous les ordinateurs dâ€™un rÃ©seau pair-Ã -pair, appelÃ©sÂ Â«Â nÅ“udsÂ Â», jouent tout Ã la fois le rÃ´le de client et de serveur,Â câ€™est-Ã -direÂ le rÃ´le dâ€™Ã©metteur et de rÃ©cepteur.Â Une appliÂcation largement rÃ©pandue dans le domaine des architectures informatique pair-Ã -pair est celui du partage de fichiers, bÃªte noire des industries culturelles depuis lâ€™avÃ¨nement dâ€™internet et le lancement, en juin 1999, du premier logiciel utilisÃ© Ã grande Ã©chelle, Napster, puis, Ã lâ€™Ã©tÃ© 2002, du protocole de transfert de donnÃ©es BitTorrent. Dans le domaine des rÃ©seaux filaires ou sans fil, la structure du rÃ©seau est diteÂ Â«Â maillÃ©eÂ Â»Â lorsquâ€™elle consiste en la connexion de tous les nÅ“uds (aussi nommÃ©sÂ Â«Â hÃ´tesÂ Â») en pair-Ã -pair, sans hiÃ©rarchie centrale. Tous les hÃ´tes du rÃ©seau sont Ã la fois client et serveur, permettant une bien meilleure rÃ©silience des communications si lâ€™un des points tombe en panne. Aujourdâ€™hui, les rÃ©seaux pair-Ã -pair sont Ã©galement au cÅ“ur du fonctionnement de la plupart des blockchains publiques, comme Bitcoin, Ethereum ou encore Tezos.

Toutes ces applications dont lâ€™architecture technique repose sur un rÃ©seau pair-Ã -pair doivent faire face, notamment, Ã une menace de sÃ©curitÃ© propre Ã cette topologie distribuÃ©e baptisÃ©eÂ Â«Â attaque SybilÂ Â», au cours de laquelleÂ une personne crÃ©e plusieurs comptes ou raccorde plusieurs nÅ“uds ou ordinateurs au sein du rÃ©seau pour tenter dâ€™en prendre le contrÃ´le.Â Le nom de ce type dâ€™attaque informatique est une rÃ©fÃ©Â rence Ã un roman biographique paru en 1973 aux Ã‰tats-Unis, Ã©crit par Flora Rheta Schreiber, qui raconte lâ€™histoire de la psychothÃ©rapie de Shirley Ardell Mason (1923-1998), Ã©galement connue sous lâ€™aliasÂ Â«Â Sybil Isabel DorsettÂ Â», une artiste publicitaire atteinte dâ€™un trouble de la personnalitÃ© multiple, ou trouble dissociatif de lâ€™identitÃ©. Une attaque Sybil dÃ©signe ainsi lâ€™activitÃ© de nÅ“uds malhonnÃªtes au sein dâ€™un rÃ©seau pair-Ã -pair qui se font passer pour des nÅ“uds individuels et indÃ©pendants alors quâ€™ils sont en rÃ©alitÃ© sous le contrÃ´le dâ€™une seule entitÃ© malinÂtentionnÃ©e, et dont lâ€™objectif est dâ€™influencer les dÃ©cisions prises sur le rÃ©seau, deÂ Â«Â dÃ©sanonymiserÂ Â»Â les utilisateurs du rÃ©seau ou encore dâ€™en corrompre le fonctionnement, voire dâ€™en bloquer le protocole.

En 2014, le rÃ©seau Tor, rÃ©seau informatique mondial et dÃ©centralisÃ© qui permet Ã ses utilisateurs

dâ€™anonymiser lâ€™origine de leur connexion, a subi une attaque Sybil pendant plusieurs mois. Lâ€™objectif des attaquants, qui sont parvenus Ã prendre le contrÃ´le Ã lâ€™aide de nÅ“uds malveillants dâ€™environ la moitiÃ© des relais Tor, Ã©tait dâ€™espionner le trafic des donnÃ©es et deÂ Â«Â dÃ©sanonymiserÂ Â»Â un grand nombre dâ€™utilisateurs. Dâ€™aprÃ¨s Sombrecrizt, collaborateur du site linuxadictos.com,Â *Â«Â placer un grand nombre de nÅ“uds contrÃ´lÃ©s par un opÃ©rateur permet aux utilisateurs de dÃ©sanonymiser Ã lâ€™aide dâ€™une attaque de classe Sybil, ce qui peut Ãªtre fait si lesÂ attaquants contrÃ´lent le premier et le dernier nÅ“ud de la chaÃ®ne dâ€™anonymisation. Le premier nÅ“ud de la chaÃ®ne Tor connaÃ®t lâ€™adresse IP de lâ€™utilisateur, et ce dernier connaÃ®t lâ€™adresse IP de la ressource demandÃ©e, qui permetÂ deÂ dÃ©sanonymiser la demande en ajoutantÂ une certaine Ã©tiquette cachÃ©e sur le cÃ´tÃ© du nÅ“ud dâ€™entrÃ©e pour les en-tÃªtesÂ de paquets qui restent inchangÃ©s tout au long de la chaÃ®ne dâ€™anonymisation, puis lâ€™analyse de celui-ciÂ cÃ´tÃ© de nÅ“ud de sortie.Â Â»*Â Ces nÅ“uds malveillants, une fois identifiÃ©s, ont Ã©tÃ© dÃ©connectÃ©s du rÃ©seau Tor.

Le risque dâ€™attaques Sybil existe sur les protocoles blockchain dont le fonctionnement repose Ã©galement sur une architecture pair-Ã -pair.Â Comment les nÅ“uds dâ€™une blockchain se font-ils confiance et acceptent-ilsÂ les nouveaux blocs de transactions diffusÃ©s sur leÂ rÃ©seau ?Â Comment repÃ©rer dâ€™Ã©ventuels nÅ“uds malveillants qui tentent dâ€™inscrire de fausses transactions Ã leur profit dans le registre public ? Pour se prÃ©munir de ce type dâ€™attaque, les blockchains publiques mettent en Å“uvre un mÃ©canisme de consensus, celui notamment de la preuve de travail (*proof of work*). Le mÃ©canisme de consensus de la preuve de travail exige que chaque nÅ“ud impliquÃ© dans la validation des transactions rÃ©solve une Ã©nigme cryptographique, coÃ»teuse en Ã©nergie, afin de participer au processus de minage. Celui qui rÃ©sout cette Ã©nigme cryptographique valide le bloc de transactions et perÃ§oit une rÃ©compense pour ce travail. Or,Â si la crÃ©ation dâ€™idenÂtitÃ©s multiples est toujours possible, il est aujourdâ€™hui quasiment impossible pour un attaquant de fournir une puissance de calcul suffisante pour insÃ©rer Ã lâ€™insu de tous de fausses transactions dans une blockchain publique.Â Le mÃ©canisme de consensus de la preuve de travail, mis en Å“uvre au sein dâ€™un protocole blockchain, permet ainsi de se dÃ©fendre de maniÃ¨re trÃ¨s efficace contre les attaques Sybil. Comme le prÃ©cise le site academy.binance.com,Â *Â«Â il nâ€™empÃªche en rien un attaquant de tenter ce type dâ€™attaque mais a pour objectif de la rendre extrÃªmement difficile, voire impossibleÂ Â»*. Câ€™est par cet ingÃ©nieux moyen que,Â depuis 2009, la blockchain publique Bitcoin se prÃ©munit avec succÃ¨s contre les attaques Sybil et permet de garantir lâ€™inviolabilitÃ© des transactions sur son rÃ©seau.

SourcesÂ :

- Â« Les attaques Sybil Â», Binance Academy, academy.binance.com/fr, 2018, mise Ã jour en 2021.
- Â« Sybil Attacks and Defenses in Internet of Things and Mobile Social Networks Â», Ali Alharbi, Mohamed Zohdy, Debatosh Debnath, Richard Olawoyin, George Corser, *International Journal of Computer Science Issues*, vol. 15, issue 6, zenodo.org, November 30, 2018.
- Â« Lâ€™attaque de Sybil â€“ Free TON est-il vulnÃ©rable ? Â», Vitaly Romanov, freeton.house/fr/,

21 mars 2021.
- Â« Tor 11.0.2 a dÃ©jÃ Ã©tÃ© publiÃ© et est livrÃ© avec quelques correctifs Â», Sombrecrizt, linuxadictos.com/fr, 5 dÃ©cembre 2021.Â

Categorie

1. Techniques

date crÃ©Ã©e
20 juillet 2022
Auteur
jacquesandrefines