VeriSign :ProtÃ¨ge les DNS du .com contre les pirates informatiques
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 11/4/2011 13:00:00

VeriSign, Inc., fournisseur rÃ©putÃ© de services d'infrastructure sur Internet pour le monde en rÃ©seau, annonce que**le domaine .com**, soit le plus grand domaine Internet, comptant plus de 90 millions dâ□□inscriptions de noms de domaine dans le monde entier, prend dÃ©sormais en charge **DNS Security Extensions** (DNSSEC).

Le dÃ©ploiement de DNSSEC dans le domaine .com indique que Verisign a franchi un jalon essentiel dans lâ□□amÃ©lioration de lâ□□intÃ©gritÃ© des communications Internet et la sÃ©curitÃ© des transactions DNS (Domain Name System). Cette rÃ©ussite intervient au terme de plusieurs annÃ©es dâ□□une collaboration Ã©troite et minutieuse entre Verisign, lâ□□ICANN (Internet Corporation for Assigned Names and Numbers) et de nombreux acteurs de lâ□□Internet, depuis les registraires et les fournisseurs de services (ISP), en passant par les constructeurs de matÃ©riels et les Ã©diteurs logiciels.

Â« *En atteignant ce jalon fondamental du dÃ©ploiement de DNSSEC, Verisign et la communautÃ© Internet ont progressÃ© Ã pas de gÃ©ant pour protÃ©ger lâ□□intÃ©gritÃ© des donnÃ©es DNS* Â», explique **Pat Kane**, SVP et directeur gÃ©nÃ©ral des Services de nom de domaine chez Verisign. Â« *Mais les menaces contre lâ□□Ã©cosystÃ¨me Internet, quâ□□elles visent le DNS ou une autre cible, sont incessantes. Câ□□est pourquoi Verisign investit en permanence pour garantir la sÃ©curitÃ© et la disponibilitÃ© de lâ□□infrastructure Internet.* Â»

DNSSEC contribue Ã mettre fin Ã une vulnÃ©rabilitÃ© connue de DNS qui Ã©tait devenue une cible de plus en plus prisÃ©e des pirates informatiques et des usurpateurs dâ□□identitÃ©. Les extensions de sÃ©curitÃ© appliquent des signatures numÃ©riques aux donnÃ©es DNS afin dâ□□authentifier lâ□□origine des donnÃ©es et vÃ©rifier leur intÃ©gritÃ© au fur et Ã mesure de leur transit sur Internet. Les extensions sont pensÃ©es pour protÃ©ger le DNS contre des attaques dâ□□intermÃ©diaires qui corrompent les donnÃ©es DNS stockÃ©es sur des serveurs de noms rÃ©cursifs. Dans DNSSEC, il est beaucoup plus difficile de contaminer le cache dâ□□un serveur de noms rÃ©cursif, parce que les administrateurs DNS signent leurs donnÃ©es. Les signatures numÃ©riques obtenues sur ces donnÃ©es DNS sont validÃ©es par une Â« chaÃ®ne de confiance Â».

Â« *Lâ□□importance de DNSSEC pour rÃ©soudre les problÃ¨mes de confiance sur Internet a atteint un point crucial en signant le domaine .com : câ□□est Ã ce jour lâ□□un des jalons les plus importants dans lâ□□histoire de DNSSEC. Toutefois, il reste du pain sur la planche et le dÃ©ploiement efficace de DNSSEC nÃ©cessite la collaboration de tous les acteurs de*

lâ□□Ã©cosystÃ¨me Internet Â», dÃ©clare **Lawrence Orans**, directeur de Gartner Research.

Le dÃ©ploiement de DNSSEC dans .com fait suite Ã la rÃ©ussite, en 2010, du dÃ©ploiement de DNSSec dans.net en dÃ©cembre, dans .edu en aoÃ»t ainsi quâ□□Ã lâ□□initiative de collaboration entre Verisign, ICANN et le MinistÃ¨re amÃ©ricain du Commerce en vue de signer la zone racine DNS en

juillet. Pour soutenir et encourager lâ□□implÃ©mentation de DNSSEC, Verisign exploite aussi un laboratoire dâ□□interopÃ©rabilitÃ© DNSSEC. Faisant appel Ã du personnel Verisign, le laboratoire aide les fournisseurs de solutions, les ISP et les autres parties prenantes Ã prÃ©parer lâ□□Ã©cosystÃ¨me des communications Internet pour DNSSEC.

Verisign fournit Ã la communautÃ© des registraires toute une gamme dâ□□outils permettant de simplifier lâ□□implÃ©mentation de DNSSEC et de rÃ©duire les coÃ»ts associÃ©s. Pour faciliter lâ□□adoption de DNSSEC, le service de signature DNSSEC est proposÃ© aux registraires pour les aider Ã incorporer la signature et le provisionnement Ã leur infrastructure, tout en allÃ©geant les tÃ¢ches administratives liÃ©es Ã lâ□□assurance dâ□□un support DNSSEC Ã leurs clients. En outre, Verisign DNSSEC Analyzer est une application iPhone qui facilite le diagnostic des problÃ¨mes relatifs aux noms et zones signÃ©s DNSSEC. Le groupe Network Intelligence and Availability (NIA) de Verisign aide en outre les propriÃ©taires de domaine Ã simplifier la gestion complexe nÃ©cessaire Ã lâ□□exploitation dâ□□une zone signÃ©e en intÃ©grant le support DNSSEC Ã son remarquable service gÃ©rÃ© DNS .

Lâ□□initiative DNSSEC de Verisign vient en outre harmonieusement complÃ©ter lâ□□initiative Â« Project Apollo Â» de la sociÃ©tÃ©, qui renforcera et fera progresser considÃ©rablement lâ□□infrastructure de.com en 2020. Pour ce faire, Verisign est en train de faire Ã©voluer, et dans certains cas, de moderniser lâ□□infrastructure dâ□□exploitation de .com. La feuille de route technologique de Verisign pour 2020 stipule une multiplication par 1000 de la capacitÃ©, qui est actuellement de 4 billions de requÃªtes, afin de permettre la gestion de 4 billiards de requÃªtes par jour. Lâ□□augmentation de capacitÃ© pourra supporter des volumes dâ□□attaques normaux et intensifiÃ©s, sur la base des constatations faites par la sociÃ©tÃ©, ainsi que les attaques Internet correspondant aux tendances actuelles.