

Internet, réseau mondial et faillible

Description

Le virus qui a affecté des milliers d'ordinateurs entre 2007 et 2011 était susceptible de faire encore de nombreux dégâts à 04 h 01 GMT le 9 juillet 2012, heure et jour de l'expiration du programme de sécurité du FBI. Avec l'accord de l'autorité judiciaire, les services secrets américains avaient procédé à la mise en œuvre de serveurs intermédiaires assurant le bon fonctionnement des machines dites corrompues par DNS Changer. Les fournisseurs d'accès se sont préparés à l'extinction de ce mécanisme de secours en renforçant leurs systèmes de sécurité. Tant redouté, le bug généralisé a été évité.

Ce virus lancé par des cybercriminels, aujourd'hui sous les verrous, aurait pu affecter 4 millions d'ordinateurs dans le monde. Ce programme malveillant modifiait le Domaine Name Server (DNS) qui sert à faire correspondre l'adresse IP d'un site (une série de chiffres) et l'URL (www.com). Prenant ainsi le contrôle du routage, DNS Changer redirigeait les requêtes des internautes vers de mauvaises adresses internet, générant ainsi un important trafic au profit de campagnes publicitaires. L'arnaque aurait permis à ses auteurs de récolter près de 14 millions de dollars. Reprenant en main la maîtrise du routage affecté par DNS Changer, le FBI a laissé le temps aux entreprises et aux particuliers de reconfigurer leurs machines, la liste des adresses IP concernées ayant été publiée.

Environ 300 000 serveurs sont encore affectés par DNS Changer dans le monde, principalement aux États-Unis (69 000), mais également dans une dizaine d'autres pays (Italie, Allemagne, Royaume-Uni, Canada, Inde, et l'Australie notamment) dont la France, qui en compte 10 000. L'arrêt des machines de substitution, servant à gérer les connexions des machines infectées par le virus, s'est fait sans provoquer de coupure du réseau début juillet 2012. Les ordinateurs touchés devront être reconfigurés, protégés désormais par les mises à jour des anti-virus capables de repérer DNS Changer. Pour savoir si un ordinateur est encore affecté par ce virus, un test peut être effectué en ligne sur le site de l'Autorité canadienne pour les enregistrements internet (www.dns-ok.ca).

Quelques jours avant l'opération du FBI, dans la nuit du 31 juin au 1^{er} juillet 2012, des bugs ont été constatés par plusieurs acteurs opérant sur Internet, au nombre desquels figurent Mozilla et son navigateur Firefox, les réseaux sociaux Reddit et LinkedIn mais nul virus n'a été incriminé. L'ajout d'une seconde au Temps universel (version moderne du temps moyen de Greenwich, GMT) adaptée à la rotation de la terre et gérée par l'Union internationale des télécommunications (UIT) est à l'origine de ces dysfonctionnements informatiques. Aguerri par une expérience similaire en 2008, Google a anticipé le problème en ajoutant progressivement quelques millisecondes à chaque mise à jour de ses serveurs. L'horloge mondiale a évolué de 25 secondes depuis 1972.

À la même période, en juin 2012, une violente tempête, entraînant des coupures d'électricité sur la côte Est des États-Unis, provoquait une panne dans une ferme de serveurs appartenant au spécialiste de la vente en ligne Amazon. L'activité des entreprises, utilisant elles aussi ce site de stockage de données, a été perturbée pendant plusieurs heures. Un dysfonctionnement de même nature avait déjà eu lieu un an auparavant, en avril 2011. À travers sa filiale Amazon Web Services (AWS), le géant d'Internet s'est développé dans le secteur de l'informatique en nuage (*cloud computing*, voir REM n°9, p.43), lui permettant de louer les capacités inexploitées de ses puissantes fermes de serveurs installées dans le monde entier, notamment en Irlande pour l'Europe. Des centaines de milliers d'entreprises, ainsi que des agences gouvernementales américaines comme la Nasa, confient aujourd'hui à Amazon l'hébergement de leurs données. Le nombre de 1 000 milliards de documents stockés a été franchi en juin 2012, contre moins de 3 milliards au lancement de l'activité par Amazon en 2006. À propos des dysfonctionnements récents des machines, Andy Jassy, vice-président senior d'AWS, indique que, le risque zéro n'existant pas, les clients de l'informatique en nuage ont néanmoins la possibilité de s'appuyer sur différentes fermes de serveurs pour obtenir davantage de sécurité.

Le 4 octobre 2012, pour la première fois en Europe, des centaines d'experts en cybersécurité au service des banques, des opérateurs de télécommunications, des grandes entreprises internet et les gouvernements des 27 États membres, ainsi que des institutions européennes, ont participé à un exercice à grand échelle de simulation d'attaque informatique. Selon le World Economic Forum, le risque d'incident majeur en matière de cybersécurité, au cours de la prochaine décennie, est évalué à 10 %, pour un coût estimé à 200 milliards d'euros.

Depuis juillet 2009, la France s'est dotée d'une autorité interministérielle de défense des systèmes d'information, baptisée Agence nationale de la sécurité des systèmes d'information (ANSSI), ainsi que d'une stratégie nationale en matière de cybersécurité depuis février 2011. Pour le sénateur Jean-Marie Bockel, auteur d'un rapport intitulé « La cyberdéfense : un enjeu mondial, une priorité nationale », document adopté à l'unanimité par les membres de la commission des affaires étrangères, de la défense et des forces armées du Sénat en juillet 2012, le dispositif français reste insuffisant, avec un effectif de 230 personnes, face aux 500 et 700 agents employés par les services homologues du Royaume-Uni et de l'Allemagne. Les menaces se multiplient, rappelle le sénateur, citant les attaques informatiques contre l'industriel du nucléaire Areva, contre également le ministre de l'économie et des finances, fin

2010, alors que la France allait prendre la présidence du G8 et du G20, contre enfin le Sénat, fin 2011, au moment du vote sur la loi visant à réprimer la contestation du génocide arménien et contre l'Élysée en mai 2012, avant l'arrivée du nouveau Président de la République. Le manque de sensibilité de l'opinion au niveau national constituerait la première des menaces. Selon l'éditeur de logiciels Symantec, plus de 10 millions d'internautes en France auraient été victimes d'un piratage informatique en 2011, particulièrement sur les réseaux sociaux et le téléphone portable. La facture est estimée à 2,5 milliards d'euros (+38 % par rapport à 2010).

Sources :

- « Vers une coupure d'Internet le 8 mars 2012 ? », Hélène Puel, 01net.com, 20 février 2012.
- « Comment le « cloud » d'Amazon a franchi le cap des 1 000 milliards de documents stockés », Romain Gueugneau, *Les Echos*, 19 juin 2012.
- « L'ajout d'une seconde au Temps universel a créé des bugs informatiques », liberation.fr, 3 juillet 2012.
- « Lundi, des centaines de milliers d'ordinateurs coupés du Web », lesechos.fr, 6 juillet 2012.
- « Internet : le chaos redouté n'a pas eu lieu », AFP, tv5.org, 9 juillet 2012.
- « Cybercriminalité : la France est démunie, souligne un rapport du Sénat », AFP, tv5.org, 19 juillet 2012.
- « Exercice majeur de cybersécurité à l'échelle européenne », AFP, tv5.org, 4 octobre 2012.

Categorie

1. Techniques

date créée

22 septembre 2012

Auteur

françoise