Internet, reÌ•seau mondial et faillible

Description

L e virus qui a affecteÌ• des milliers dâ€™ordinateurs entre 2007 et 2011 eÌ•tait susceptible de faire encore de nombreux deÌ•gaÌ‚ts aÌ€ 04 h 01 GMT le 9 juillet 2012, heure et jour de lâ€™expiration du programme de seÌ•curiteÌ• du FBI. Avec lâ€™accord de lâ€™autoriteÌ• judiciaire, les services secrets ameÌ•ricains avaient proceÌ•deÌ• aÌ€ la mise en Å“uvre de serveurs intermeÌ•diaires assurant le bon fonctionnement des machines dites corrompues par DNS Changer. Les fournisseurs dâ€™acceÌ€s se sont preÌ•pareÌ•s aÌ€ lâ€™extinction de ce meÌ•canisme de secours en renforcÌ§ant leurs systeÌ€mes de seÌ•curiteÌ•. Tant redouteÌ•, le bug geÌ•neÌ•raliseÌ• a eÌ•teÌ• eÌ•viteÌ•.

Ce virus lanceÌ• par des cybercriminels, aujourdâ€™hui sous les verrous, aurait pu affecter 4 millions dâ€™ordinateurs dans le monde. Ce programme malveillant modifiait le Domaine Name Server (DNS) qui sert aÌ€ faire correspondre lâ€™adresse IP dâ€™un site (une seÌ•rie de chiffres) et lâ€™URL (www. … .com). Prenant ainsi le controÌ‚le du routage, DNS Changer redirigeait les requeÌ‚tes des internautes vers de mauvaises adresses internet, geÌ•neÌ•rant ainsi un important trafic au profit de campagnes publicitaires. Lâ€™arnaque aurait permis aÌ€ ses auteurs de reÌ•colter preÌ€s de 14 millions de dollars. Reprenant en main la maiÌ‚trise du routage affecteÌ• par DNS Changer, le FBI a laisseÌ• le temps aux entreprises et aux particuliers de reconfigurer leurs machines, la liste des adresses IP concerneÌ•es ayant eÌ•teÌ• publieÌ•e.

Environ 300 000 serveurs sont encore affecteÌ•s par DNS Changer dans le monde, principalement aux Etats-Unis (69 000), mais eÌ•galement dans une dizaine dâ€™autres pays (Italie, Allemagne, Royaume-Uni, Canada, Inde, et lâ€™Australie notamment) dont la France, qui en compte 10 000. Lâ€™arreÌ‚t des machines de substitution, servant aÌ€ geÌ•rer les connexions des machines infecteÌ•es par le virus, sâ€™est fait sans provoquer de coupure du reÌ•seau deÌ•but juillet 2012. Les ordinateurs toucheÌ•s devront eÌ‚tre reconfigureÌ•s, proteÌ•geÌ•s deÌ•sormais par les mises aÌ€ jour des anti-virus capables de repeÌ•rer DNS Changer. Pour savoir si un ordinateur est encore affecteÌ• par ce virus, un test peut eÌ‚tre effectueÌ• en ligne sur le site de lâ€™AutoriteÌ• canadienne pour les enregistrements internet (www.dns-ok.ca).

Quelques jours avant lâ€™opeÌ•ration du FBI, dans la nuit du 31 juin au 1er juillet 2012, des bugs ont eÌ•teÌ• constateÌ•s par plusieurs acteurs opeÌ•rant sur Internet, au nombre desquels figurent Mozilla et son navigateur Firefox, les reÌ•seaux sociaux Reddit et LinkedIn mais nul virus nâ€™a eÌ•teÌ• incrimineÌ•. Lâ€™ajout dâ€™une seconde au Temps universel (version moderne du temps moyen de Greenwich, GMT) adapteÌ• aÌ€ la rotation de la terre et geÌ•reÌ• par lâ€™Union internationale des teÌ•leÌ•communications (UIT) est aÌ€ lâ€™origine de ces dysfonctionnements informatiques. Aguerri par une expeÌ•rience similaire en 2008, Google a anticipeÌ• le probleÌ€me en ajoutant progressivement quelques millisecondes aÌ€ chaque mise aÌ€ jour de ses serveurs. Lâ€™horloge mondiale a eÌ•volueÌ• de 25 secondes depuis 1972.

A la meÌ‚me peÌ•riode, en juin 2012, une violente tempeÌ‚te, entraiÌ‚nant des coupures dâ€™eÌ•lectriciteÌ• sur la coÌ‚te Est des Etats-Unis, provoquait une panne dans une ferme de serveurs appartenant au speÌ•cialiste de la vente en ligne Amazon. Lâ€™activiteÌ• des entreprises, utilisant elles aussi ce site de stockage de donneÌ•es, a eÌ•teÌ• perturbeÌ•e pendant plusieurs heures. Un dysfonctionnement de meÌ‚me nature avait deÌ•jaÌ€ eu lieu un an auparavant, en avril 2011. A travers sa filiale Amazon Web Services (AWS), le geÌ•ant dâ€™Internet sâ€™est deÌ•veloppeÌ• dans le secteur de lâ€™informatique en nuage (*cloud computing*, voir *REM* nÂ°9, p.43), lui permettant de louer les capaciteÌ•s inexploiteÌ•es de ses puissantes fermes de serveurs installeÌ•es dans le monde entier, notamment en Irlande pour lâ€™Europe. Des centaines de milliers dâ€™entreprises, ainsi que des agences gouvernementales ameÌ•ricaines comme la Nasa, confient aujourdâ€™hui aÌ€ Amazon lâ€™heÌ•bergement de leurs donneÌ•es. Le nombre de 1 000 milliards de documents stockeÌ•s a eÌ•teÌ• franchi en juin 2012, contre moins de 3 milliards au lancement de lâ€™activiteÌ• par Amazon en 2006. A propos des dysfonctionnements reÌ•cents des machines, Andy Jassy, vice-preÌ•sident senior dâ€™AWS, indique que, le risque zeÌ•ro nâ€™existant pas, les clients de lâ€™informatique en nuage ont neÌ•anmoins la possibiliteÌ• de sâ€™appuyer sur diffeÌ•rentes fermes de serveurs pour obtenir davantage de seÌ•curiteÌ•.

Le 4 octobre 2012, pour la premieÌ€re fois en Europe, des centaines dâ€™experts en cyberseÌ•curiteÌ• au service des banques, des opeÌ•rateurs de teÌ•leÌ•communications, des grandes entreprises internet et les gouvernements des 27 Etats membres, ainsi que des institutions europeÌ•ennes, ont participeÌ• aÌ€ un exercice aÌ€ grand eÌ•chelle de simulation dâ€™attaque informatique. Selon le World Economic Forum, le risque dâ€™incident majeur en matieÌ€re de cyberseÌ•curiteÌ•, au cours de la prochaine deÌ•cennie, est eÌ•valueÌ• aÌ€ 10 %, pour un couÌ‚t estimeÌ• aÌ€ 200 milliards dâ€™euros.

Depuis juillet 2009, la France sâ€™est doteÌ•e dâ€™une autoriteÌ• interministeÌ•rielle de deÌ•fense des systeÌ€mes dâ€™information, baptiseÌ•e Agence nationale de la seÌ•curiteÌ• des systeÌ€mes dâ€™information (ANSSI), ainsi que dâ€™une strateÌ•gie nationale en matieÌ€re de cyberseÌ•curiteÌ• depuis feÌ•vrier 2011. Pour le seÌ•nateur Jean-Marie Bockel, auteur dâ€™un rapport intitule Â« La cyberdeÌ•fense : un enjeu mondial, une prioriteÌ• nationale Â», document adopteÌ• aÌ€ lâ€™unanimiteÌ• par les membres de la commission des affaires eÌ•trangeÌ€res, de la deÌ•fense et des forces armeÌ•es du SeÌ•nat en juillet 2012, le dispositif francÌ§ais reste insuffisant, avec un effectif de 230 personnes, face aux 500 et 700 agents employeÌ•s par les services homologues du Royaume-Uni et de lâ€™Allemagne. Les menaces se multiplient, rappelle le seÌ•nateur,

citant les attaques informatiques contre lâ€™industriel du nucleÌ•aire Areva, contre eÌ•galement le ministeÌ€re de lâ€™eÌ•conomie et des finances, fin 2010, alors que la France allait prendre la preÌ•sidence du G8 et du G20, contre enfin le SeÌ•nat, fin 2011, au moment du vote sur la loi visant aÌ€ reÌ•primer la contestation du geÌ•nocide armeÌ•nien et contre lâ€™ElyseÌ•e en mai 2012, avant lâ€™arriveÌ•e du nouveau PreÌ•sident de la ReÌ•publique. Le manque de sensibiliteÌ• de lâ€™opinion au niveau national constituerait la premieÌ€re des menaces. Selon lâ€™eÌ•diteur de logiciels Symantec, plus de 10 millions dâ€™internautes en France auraient eÌ•teÌ• victimes dâ€™un piratage informatique en 2011, particulieÌ€rement sur les reÌ•seaux sociaux et le teÌ•leÌ•phone portable. La facture est estimeÌ•e aÌ€ 2,5 milliards dâ€™euros (+38 % par rapport aÌ€ 2010).

Sources :

- Â« Vers une coupure dâ€™Internet le 8 mars 2012 ? Â», HeÌ•leÌ€ne Puel, 01net.com, 20 feÌ•vrier 2012.
- Â« Comment le Â«Â cloudÂ Â» dâ€™Amazon a franchi le cap des 1 000 milliards de documents stockeÌ•s Â», Romain Gueugneau,*Les Echos*, 19 juin 2012.
- Â« Lâ€™ajout dâ€™une seconde au Temps universel a creÌ•eÌ• des bugs informatiques Â», liberation.fr, 3 juillet 2012.
- Â« Lundi, des centaines de milliers dâ€™ordinateurs coupeÌ•s du Web Â», lesechos.fr, 6 juillet 2012.
- Â« Internet : le chaos redouteÌ• nâ€™a pas eu lieu Â», AFP, tv5.org, 9 juillet 2012.
- Â« CybercriminaliteÌ• : la France est deÌ•munie, souligne un rapport du SeÌ•nat Â», AFP, tv5.org, 19 juillet 2012.
- Â« Exercice majeur de cyberseÌ•curiteÌ• aÌ€ lâ€™eÌ•chelle europeÌ•enne Â», AFP, tv5.org, 4 octobre 2012.

Categorie

1. Techniques

date crÃ©Ã©e
22 septembre 2012
Auteur
francoise