La France menacÃ©e dâ□□une cyber-attaque de grande ampleur
Internet
PostÃ© par : JulieM
PubliÃ©e le : 8/2/2013 15:00:00

Depuis le premier jour de son intervention au Mali, la France, et notamment le site du ministÃ¨re de la dÃ©fense, sont victimes de multiples cyber-attaques. La plupart provoquent des inconvÃ©nients mineurs et impactent temporairement le service, mais des attaques de plus grande ampleur sont redoutÃ©es dans un futur proche

La France nâ□□a pas Ã©tÃ© pionniÃ¨re en matiÃ¨re de cyber protection et dâ□□initiatives pour contrer ces menaces informatiques de plus en plus nombreuses et avancÃ©es. Cependant, depuis lâ□□entrÃ©e en guerre de la France auprÃ¨s de lâ□□armÃ©e Malienne, les cyber-attaques se sont multipliÃ©es.

Elles provoquent des inconvÃ©nients mineurs, mais selon **Eric Bonnemaison**, gÃ©nÃ©ral en charge des affaires stratÃ©giques au sein de ministÃ¨re de la DÃ©fense, des attaques de plus grande ampleur sont redoutÃ©es dans un avenir proche. Lors du Forum International de la Cyber-sÃ©curitÃ© les 28 et 29 janvier, il a Ã©tÃ© rappelÃ© que la cyber-sÃ©curitÃ© constitue une prioritÃ© nationale.

Yogi Chandiramani, Senior Manager of Systems Engineering chez FireEye, commente :

Â« *En France, les cyber-attaques ne sont plus uniquement exÃ©cutÃ©es par des groupes Ã©tatiques ou cyber-criminels, mais Ã©galement par des groupes politiques activistes. A titre dâ□□exemple, les Anonymous ont beaucoup fait parler dâ□□eux depuis 2008, en sâ□□attaquant Ã des structures de grande envergure, mais ils ne sont pas les seuls. On a Ã©galement assistÃ© Ã lâ□□arrestation dâ□□un des hackers Ã lâ□□origine de lâ□□attaque Payback contre le systÃ¨me de*

paiement en ligne Paypal et contre les services amÃ©ricains de carte bancaire Visa et Mastercard.

Les cyber-attaques se dÃ©mocratisent dans des objectifs allant du cyber-espionnage, Ã la cyber-escroquerie (telle sur EDF la semaine derniÃ¨re), ou au simple dÃ©ni de service (DDoS), afin dâ□□enrayer le fonctionnement des sites web et de porter prÃ©judice Ã la rÃ©putation de lâ□□entreprise. Les laboratoires de FireEye ont dâ□□ailleurs rÃ©cemment dÃ©couvert une attaque de grande ampleur sur les secteurs de l'aÃ©rospatiale et l'industrie de dÃ©fense via l'opÃ©ration BeeBus.

Ces attaques ne ciblent pas uniquement les gouvernements mais Ã©galement les entreprises de pointe. Elles sont bien souvent un moyen de revendiquer des opinions politiques et de manifester son opposition. Le blocage informatique permet aux activistes de maximiser la visibilitÃ© de leurs actions et de leurs opinions.

En outre, dans la lutte contre ces cyber-attaques, comprendre les diffÃ©rents types d'acteurs en prÃ©sence et les motifs qui les poussent Ã agir est important.

De plus, nous avons appris hier que les USA ont le pouvoir de lancer des cyber-attaques prÃ©ventives si leur territoire Ã©tait menacÃ©, au nom de la lÃ©gitime dÃ©fense. Face Ã ces constatations, les entreprises, les organisations et la France doivent prendre la menace trÃ¨s au sÃ©rieux, en rÃ©duisant leur dÃ©pendance Ã l'Ã©gard des outils de sÃ©curitÃ© obsolÃ¨tes qui se sont avÃ©rÃ©s maintes fois inefficaces en tant que seuls moyens de dÃ©fense. En bref, nous devons Ã©voluer au moins aussi vite que les cyber-criminels. Â»

FireEye a participÃ© Ã la destruction de Grum, le plus grand botnet au monde, responsable de quelques 18 milliards de spams chaque jour.