Insolite : Palmares des plus grandes attaques de cybercriminels
Insolite
PostÃ© par : JerryG
PubliÃ©e le : 22/6/2011 14:00:00

Depuis 2010 et le dÃ©but de lâannÃ©e 2011, le paysage de la sÃ©curitÃ© sâestÂ profondÃ©ment modifiÃ©, petit retour en arriÃ¨re sur les plus grandes attaques deÂ cybercriminels qui ont fait trembler la terre entiÃ¨re et pose une nouvelle foisÂ la question de la sÃ©curitÃ© informatique.

Quatre diffÃ©rents Ã©vÃ¨nements Wikileaks, Stuxnet, les Advanced Evasion Techniques et le piratage du code source de SecurID ont bouleversÃ© la sÃ©curitÃ©, notamment en termes stratÃ©giques. Ces attaques mettent clairement en lumiÃ¨re la nÃ©cessitÃ© de mettre en place des actions.

Plus les donnÃ©es dâune entreprise sont prÃ©cieuses, plus cette derniÃ¨re est susceptible dâÃªtre la cible dâune attaque.

En 2010-2011, nous avons assistÃ© Ã plusieurs failles de sÃ©curitÃ© critiques :

Nasdaq, 2010

o Tout au long de lâannÃ©e 2010, les hackers ont pÃ©nÃ©trÃ© Ã rÃ©pÃ©tition le rÃ©seau de la sociÃ©tÃ© qui gÃ¨re le Nasdaq. Pour les autoritÃ©s, cela pose deux gros problÃ¨mes : prÃ©server la stabilitÃ© et la fiabilitÃ© des Ã©changes numÃ©riques et maintenir la confiance des investisseurs dans les systÃ¨mes. Les bourses du monde entier sont conscientes quâelles sont frÃ©quemment la cible des pirates.

Faille RSA, mars 2011

o Des pirates sont parvenus Ã accÃ©der au rÃ©seau de RSA et Ã voler des informations relatives Ã ses produits dâauthentification Ã deux facteurs.

Sony piratÃ© Ã plusieurs reprises en 2011

o Cet incident est le tout dernier dans une longue semaine dâattaques et de failles. Les premiers

problÃ¨mes ont commencÃ© le 19 avril. A cette date, la sociÃ©tÃ© Sony commence ses recherches et finit par dÃ©couvrir une faille de sÃ©curitÃ© dans le rÃ©seau PlayStation Network. Plus de 100 millions dâutilisateurs ont Ã©tÃ© touchÃ©s par ce piratage.

Faille Comodo, mars 2011

o Lâorgane de certification Ã©lectronique amÃ©ricain, Comodo, a reconnu que deux de ses nouvelles Registration Authorities (RA) avaient Ã©tÃ© piratÃ©es. Ces piratages nâont semble-t-il rien Ã voir avec lâincident impliquant un pirate iranien isolÃ© au cours duquel au moins cinq comptes ont Ã©tÃ© attaquÃ©s.

Barracuda, avril 2011

o AprÃ¨s avoir sondÃ© le rÃ©seau pendant plusieurs heures, les pirates ont dÃ©couvert et exploitÃ© une faille SQL sur le site de Barracuda afin de mettre la main sur plusieurs bases de donnÃ©es, sâemparer des coordonnÃ©es des partenaires, des clients et des employÃ©s de Barracuda.

Lockheed martin Corp, Mai 2011

o Des pirates inconnus ont accÃ©dÃ© au rÃ©seau dâun des plus gros fabricant dâarmes du monde, Lockheed Martin Corp.

L-3 Communications, tentative de piratage, 2011

o La sociÃ©tÃ© de dÃ©fense L-3 Communications a Ã©tÃ© la cible de tentatives de pÃ©nÃ©tration visant Ã dÃ©rober des informations confidentielles. L-3 nâa dÃ©voilÃ© aucune information quant au succÃ¨s ou non de lâattaque.

Citibank, pirate en mai 2011

o Les informations personnelles et coordonnÃ©es bancaires de plus de 200 000 porteurs de cartes amÃ©ricains, dont des donnÃ©es spÃ©cifiques comme le nom et les adresses emails, ont Ã©tÃ© dÃ©robÃ©es.

FMI piratÃ© en juin 2011

Le Fond MonÃ©taire International, groupe intergouvernemental qui supervise le systÃ¨me financier mondial et regroupe 187 Ã©tats membres est la derniÃ¨re victime dâune cyber-attaque considÃ©rable.

Toutes ces sociÃ©tÃ©s ont un point commun : leurs systÃ¨mes de sÃ©curitÃ© sont

extrÃªmement bien protÃ©gÃ©s. Ces sociÃ©tÃ©s disposent dâ□□Ã©quipes sÃ©curitÃ© en interne, dotÃ©es de commandes et de centres de contrÃ´les pour administrer et protÃ©ger leurs rÃ©seaux contre de multiples attaques. Et pourtant, elles ont Ã©tÃ© piratÃ©es. Les outils de piratage Ã©voluent chaque jour et deviennent de plus en plus disponibles. Il est donc fort probable que des Ã©vÃ¨nements de ce type et des failles de sÃ©curitÃ© se multiplient et touchent Ã©galement des entitÃ©s moins bien protÃ©gÃ©es.

Pour **LÃ©onard Dahan**, Country Manager Stonesoft France et Benelux, Â« *le visage de la sÃ©curitÃ© est dÃ©sormais transformÃ©. Il est maintenant nÃ©cessaire de repenser la protection des entreprises et de leurs donnÃ©es essentielles. Les stratÃ©gies de sÃ©curitÃ© sont chaque jour plus fondamentales, dans la gestion des risques au quotidien. Les dirigeants se doivent de prendre cela en compte et de ne pas laisser uniquement la responsabilitÃ© aux Ã©quipes IT. MÃªme les conseils dâ□□administration devraient participer et superviser le profil de lâ□□entreprise face aux risques.* Â»