BitDefender : Piratage de Bercy, RÃ©action de Marc Blanchard
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 8/3/2011 11:00:00

Nos confrÃ¨res de Paris-Match nous ont rÃ©vÃ©lÃ© une attaque informatique de grande ampleur contre l'une de nos institutions Ã savoir Bercy, pas moins de **150 ordinateurs ont eu la visite de hackers** travaillant Ã la solde de pays Ã©trangers, Le Journal de la Next-Gen a interrogÃ© plusieurs responsables d'Ã©diteurs de solutions de sÃ©curitÃ© Ã l'instar de **Marc Blanchard** de chez **BitDefender**.

Le ministÃ¨re de l'Ã□conomie et des Finances a Ã©tÃ© victime d'une "attaque informatique sans prÃ©cÃ©dent", rÃ©vÃ¨le donc **Paris Match** sur son site internet. **Cibles des pirates :** la direction du TrÃ©sor et les documents du G20. 150 ordinateurs auraient Ã©tÃ© surveillÃ©s depuis le mois de dÃ©cembre dernier. 10.000 postes ont Ã©tÃ© dÃ©branchÃ©s ce week-end pour stopper l'attaque. Qui sont les auteurs ? FranÃ§ois Baroin, ministre du budget, Ã©voque des "pistes" pour l'instant non confirmÃ©es sur Europe 1.

Au temps de la guerre froide et notamment avec l'affaire des missiles de Cuba, le monde a failli sombrer dans l'hiver nuclÃ©aire, suite Ã une 3eme guerre mondiale, La 3eme guerre mondiale ne se fera pas avec un lance-pierre comme l'affirmait Albert Einstein, mais par attaques informatiques, la preuve, cette attaque de hackers qui dure depuis 3 mois et qui met Ã mal nos institutions

Nous avons donc voulu en savoir plus sur cette affaire de piratage en interrogeant diffÃ©rents responsables d'Ã©diteurs de solutions de sÃ©curitÃ©, le 1er a rÃ©pondre Ã nos questions se nomme **Marc Blanchard**, que l'on appelle entre-nous : Docteur Virus.

Le JDNG : PrÃ©sentez-vous Ã nos lecteurs

Marc Blanchard, directeur des Laboratoires Scientifiques et Technologiques pour Editions Profil / BitDefender en France. J'ai passÃ© mes 20 derniÃ¨res annÃ©es dans la lutte contre les virus et autres malwares chez diffÃ©rents Ã©diteurs de sÃ©curitÃ©. J'ai rejoint BitDefender il y a environ 2 ans maintenant.

Le JDNG : Quelle est votre fonction au sein de votre sociÃ©tÃ©

Je suis Ã la base un chercheur, plus prÃ©cisÃ©ment un EpidÃ©miologiste en malwares classifiÃ©s 'Hautes DangÃ©rositÃ©s'. Pour faire simple disons que j'analyse les codes malveillants existants pour prÃ©voir, anticiper, l'Ã©volution Ã venir des menaces. En plus de cela, je dirige les services d'assistance aux utilisateurs.

Le JDNG : Comment une attaque de cette ampleur est-elle possible ?

Les moyens de propagation sont multiples : par un simple mail contenant soit une piÃ¨ce jointe, soit par un lien, soit par une iframe html de redirection dans un mail ou encore par une simple clÃ© USB infectÃ©e.

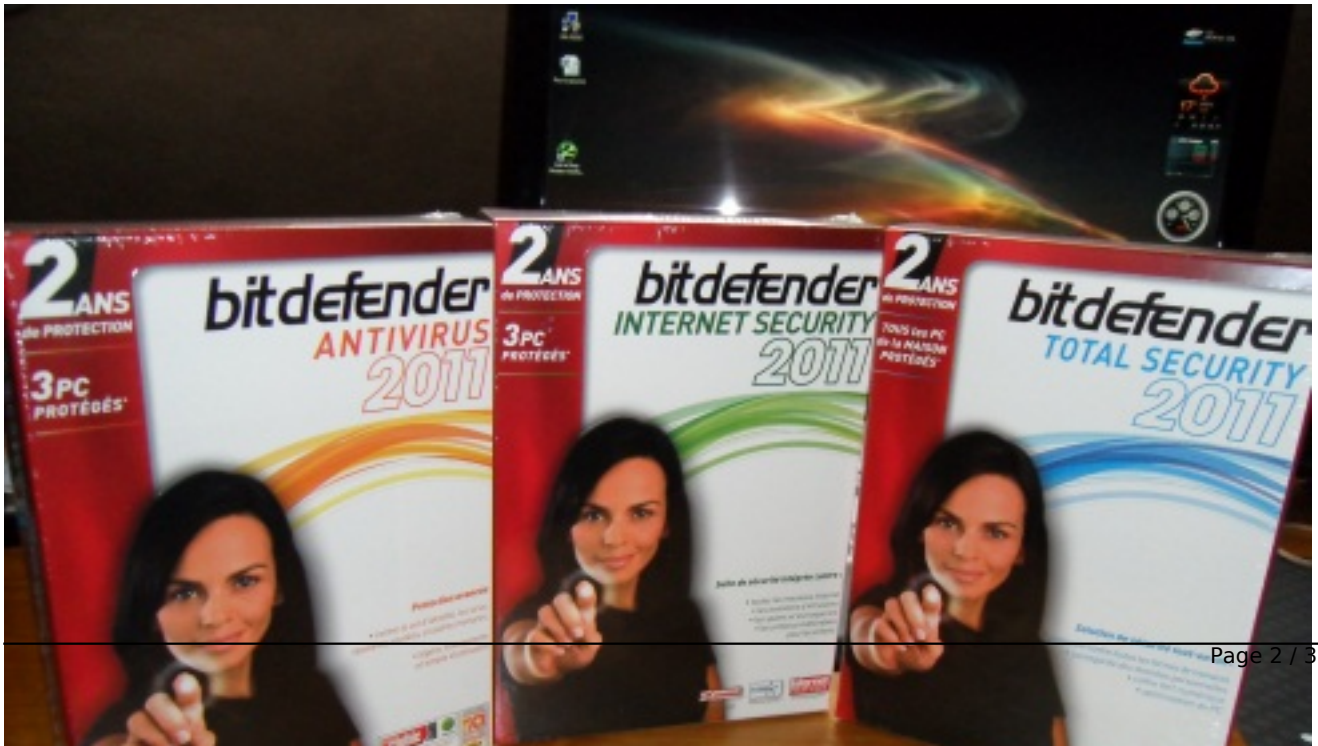
Le JDNG : Quelles prÃ©cautions les grandes organisations mettent-elles en place pour parer aux attaques des hackers ?

Chacun sait qu'il n'y a pas une solution unique et universelle pour assurer la sÃ©curitÃ© d'un rÃ©seau mais la base est bien sÃ»r l'installation d'un antivirus sur les postes de travail, les serveurs de fichiers, les serveurs de mails et les gateway, complÃ©tÃ© par des IDS et pare-feux intelligents.

A cela, il est de plus en plus nÃ©cessaire d'ajouter des solutions de DLP (Data Leak Protection) et de chiffrement de donnÃ©es afin de rÃ©duire encore les risques de fuite, qu'elles soient d'origine interne ou externe comme cela semble Ãªtre le cas dans l'affaire prÃ©sente. En amont, des solutions de filtrage des types de sites consultables peut Ã©galement rÃ©duire les risques de contamination.

Le JDNG : Que propose alors votre sociÃ©tÃ© pour mettre fin Ã ces incidents et sont-ils vraiment efficaces ?

BitDefender est l'un des principaux fournisseurs de technologies antimalware sur le marchÃ© et propose donc des suite de protection complÃ¨tes avec des technologies proactives d'analyses comportementales, d'analyses heuristiques et d'analyse des comportements de process communicants, permettant de dÃ©tecter et bloquer des attaques de type zero-day et pas seulement des menaces dÃ©jÃ rÃ©fÃ©rencÃ©es au niveau mondial. Aucun Ã©diteur ne peut s'engager sur un taux de dÃ©tection Ã 100% Ã tout moment, sachant qu'il y a dÃ©sormais prÃ¨s de 2 millions de nouveaux codes malveillants chaque mois selon AV Test, l'un des organismes de rÃ©fÃ©rences dans le domaine des malwares.



Toutefois, d'aprÃ¨s ce mÃªme organisme, en Janvier 2011 sur Windows 7, BitDefender apporte, en situation rÃ©elle (Real World Test), une protection de 100% contre les malwares se propageant par le web. BitDefender est par ailleurs certifiÃ© par tous les plus grands organismes internationaux comme Virus Bulletin, AV Comparatives, ICSA, Checkmark, Antimalware Test Labs ou encore PCSL et ses technologies exclusives sont utilisÃ©es par de nombreux Ã©diteurs tiers pour assurer la sÃ©curitÃ© de dizaines de millions d'utilisateurs dans plus de 100 pays.

Le JDNG : Vue la loi Hadopi/Loppsi (qui responsabilise lâ□□internaute en cas de hacking de son PC), nâ□□y a-t-il pas un paradoxe voire une ironie ?

Il est difficile de rÃ©pondre Ã cette question dans la mesure oÃ¹ nous ne disposons pas de l'ensemble des Ã©lÃ©ments et des faits qui se sont produits sur ce rÃ©seau. Les lois auxquelles vous faÃ®tes allusion, aussi discutables soient-elles, parlent plus d'obligation de moyens que de rÃ©sultats. Vous comprendrez aisÃ©ment que ce n'est pas notre rÃ´le que de prendre position sur ces aspects lÃ©gislatifs.

Merci Marc.