G-Data : Les cybercriminels surfent sur l'attentat de Boston
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 19/4/2013 14:00:00

Sans retenue pour cette tragÃ©die, les cybercriminels utilisent l'attentat de Boston pour infecter les internautes. **Le G Data SecurityLab** a Ã©tudiÃ© une vague de Spam dÃ©marrÃ©e ce matin dont le but est l'infection massive de systÃ¨mes Ã partir de sites web proposant des vidÃ©os de l'attentat. DÃ©tails de cette attaque.

Une vague de Spam utilise la tragÃ©die de l'attentat de Boston pour infecter les internautes. Cette attaque prend source dans une sÃ©rie de Spams proposant des liens vers des sites renfermant des vidÃ©os soi-disant exclusives des explosions de l'attentat de Boston.

1/ Le lien e-mail conduit Ã un site avec des vidÃ©os YouTube

2/ Cinq vidÃ©os sont rÃ©elles, la sixiÃ¨me ne lâ□□est pas ...

3 /Toutes les vidÃ©os (la sixiÃ¨me inclue) sont intÃ©grÃ©es via iframe.

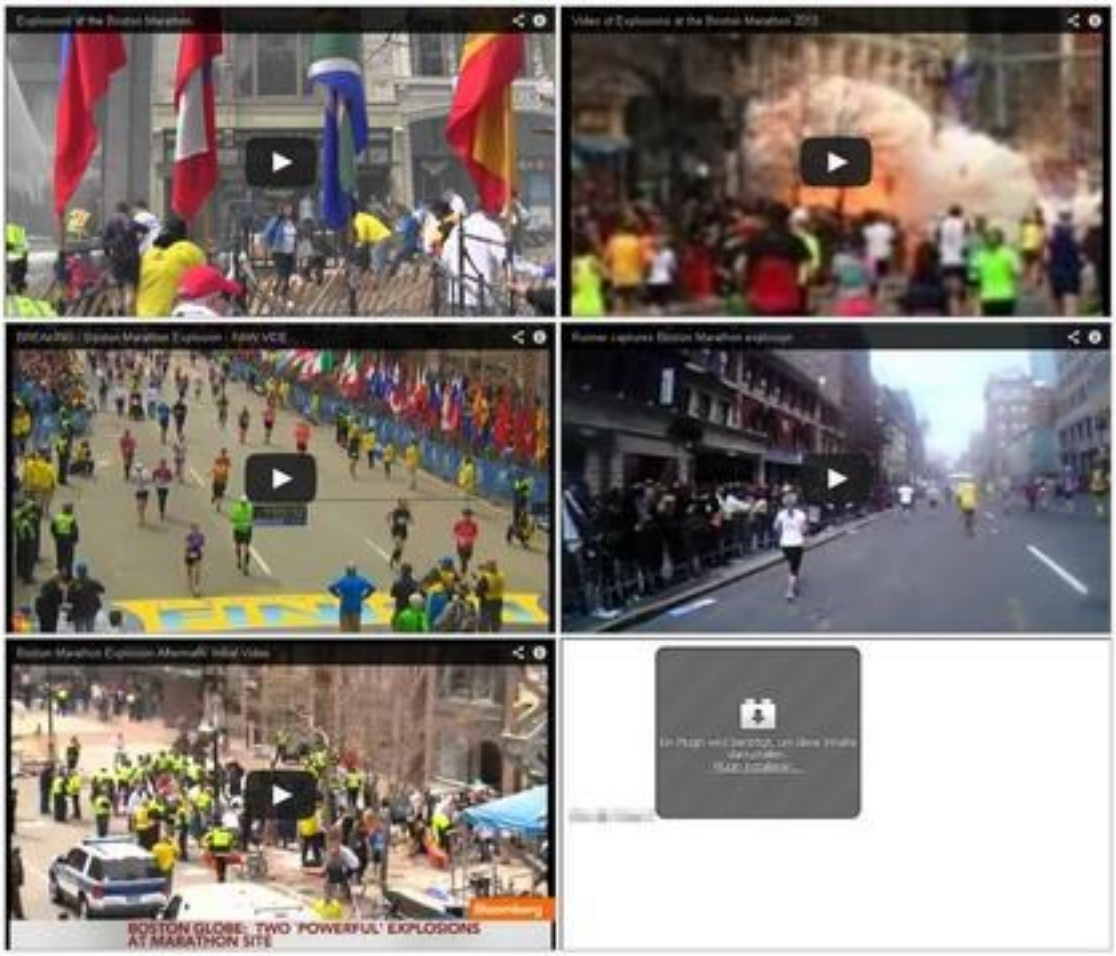
4/ La sixiÃ¨me iframe consiste en un code HTML qui dÃ©clenche une applet Java. Cette applet java est exÃ©cutÃ©e et les systÃ¨mes Ã©quipÃ©s de Java Version 7 mise Ã jour 11, sont vulnÃ©rables !

5/ En restant plus de 60 secondes sur le site Internet, lâ□□internaute est redirigÃ© vers une page spÃ©cifique (http:. / / IP-address.com / boston.avi _____ exe)

6/ Les analyses G Data montrent quâ□□Ã cet instant cette redirection ne dÃ©clenche pas dâ□□action spÃ©cifique, mais rien ne dit quâ□□elle ne le fera pas Ã lâ□□avenir.

6/ Dans le cas oÃ¹ le systÃ¨me est vulnÃ©rable Ã la faille Java : L'applet Java exploite la vulnÃ©rabilitÃ© et envoie la charge infectieuse au systÃ¨me.

7/ Deux URLs diffÃ©rentes ont Ã©tÃ© identifiÃ©es lors de lâ□□analyse, avec deux actions malveillantes distinctes :



Infection 1:

1/ La charge utile nommÃ©e newbos3.exe est exÃ©cutÃ©e sur le systÃ¨me

2/ Ce code nuisible vole les mots de passe sâ□□ils sont stockÃ©s de maniÃ¨re non chiffrÃ©e. Firefox et Filezilla sont clairement ciblÃ©s dans cette attaque, mais cette liste nâ□□est pas exhaustive.

3/ Le code lit aussi tout le trafic rÃ©seau. Signification : Si des donnÃ©es sont envoyÃ©es en clair sur le rÃ©seau, le malware de capte.

4/ L'analyste G Data commente : la partie du malware qui analyse le trafic rÃ©seau est trÃ¨s importante, plus de 800 kilo-octets.

5/ Le malware se connecte Â« Ã la maison Â». Il se connecte Ã un serveur prÃ©dÃ©fini et y envoie des donnÃ©es cryptÃ©es. Si ces donnÃ©es nâ□□ont pour le moment pas Ã©tÃ© dÃ©cryptÃ©es par le G Data Security Lab, il est fort Ã parier que les mots de passe volÃ©s et les informations du rÃ©seau transitent dans cette communication.

6/ Le code malveillant envoie du spam. Le mÃªme Spam Ã lâ□□origine de lâ□□infection est envoyÃ© via lâ□□ordinateur infectÃ©.

7/ Actuellement, le type de destinataires utilisÃ©s dans cet envoi nâ□□a pas Ã©tÃ© identifiÃ©. Vole-t-il le carnet d'adresses de l'utilisateur ou reÃ§oit-il des adresses email du serveur ?

Infection 2:

1/ Quelques minutes aprÃ¨s l'infection, l'ordinateur est verrouillÃ© par ransomware (dans notre exemple GVU Trojan, mais la page est changÃ©e en fonction de la localisation de la victime).

2/ Donc, au premier plan, l'utilisateur est bloquÃ© et ne peut plus rien faire.

3/ En tÃ¢che de fond, le Spam bot commence son travail (envoi du Spam source de lâ□□infection) .

4/ Aucune action de vol de mot de passe nâ□□a Ã©tÃ© dÃ©tectÃ©e dans cette seconde attaque.

Les solutions G-Data sont disponible chez GS2i.

Visitez le site de GS2i