

**G-Data : Les cybercriminels surfent sur l'attentat de Boston**

S curit 

Post  par : JerryG

Publi e le : 19/4/2013 14:00:00

Sans retenue pour cette trag die, les cybercriminels utilisent l'attentat de Boston pour infecter les internautes. **Le G Data SecurityLab** a  tudi  une vague de Spam d marr e ce matin dont le but est l'infection massive de syst mes   partir de sites web proposant des vid os de l'attentat. D tails de cette attaque.

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



1/ Le lien e-mail conduit   un site avec des vid os YouTube

2/ Cinq vid os sont r elles, la sixi me ne l est pas ...

3 /Toutes les vid os (la sixi me incluse) sont int gr es via iframe.

4/ La sixi me iframe consiste en un code HTML qui d clenche une applet Java. Cette applet java est ex cut e et les syst mes  quip s de Java Version 7 mise   jour 11, sont vuln rables !

5/ En restant plus de 60 secondes sur le site Internet, l internaute est redirig  vers une page sp cifique ([http:// IP-address.com / boston.avi](http://IP-address.com/boston.avi) \_\_\_\_\_ exe)

6/ Les analyses G Data montrent qu'à cet instant cette redirection ne déclenche pas d'action spécifique, mais rien ne dit qu'elle ne le fera pas à l'avenir.

6/ Dans le cas où le système est vulnérable à la faille Java : L'applet Java exploite la vulnérabilité et envoie la charge infectieuse au système.

7/ Deux URLs différentes ont été identifiées lors de l'analyse, avec deux actions malveillantes distinctes :



### Infection 1:

1/ La charge utile nommée newbos3.exe est exécutée sur le système

2/ Ce code nuisible vole les mots de passe s'ils sont stockés de manière non chiffrée. Firefox et Filezilla sont clairement ciblés dans cette attaque, mais cette liste n'est pas exhaustive.

3/ Le code lit aussi tout le trafic réseau. Signification : Si des données sont envoyées en clair sur le réseau, le malware de capte.

4/ L'analyste G Data commente : la partie du malware qui analyse le trafic réseau est très importante, plus de 800 kilo-octets.

5/ Le malware se connecte à « la maison ». Il se connecte à un serveur précédent et y envoie des données cryptées. Si ces données n'ont pour le moment pas été décryptées par le G Data Security Lab, il est fort à parier que les mots de passe volés et les informations du réseau transitent dans cette communication.

6/ Le code malveillant envoie du spam. Le même Spam à l'origine de l'infection est envoyé via l'ordinateur infecté.

7/ Actuellement, le type de destinataires utilisés dans cet envoi n'a pas été identifié. Vole-t-il le carnet d'adresses de l'utilisateur ou reçoit-il des adresses email du serveur ?

### Infection 2:

1/ Quelques minutes après l'infection, l'ordinateur est verrouillé par ransomware (dans notre exemple G.V.U Trojan, mais la page est changée en fonction de la localisation de la victime).

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

3/ En tâche de fond, le Spam bot commence son travail (envoi du Spam source de l'infection) .

4/ Aucune action de vol de mot de passe n'a été détectée dans cette seconde attaque.

**Les solutions G-Data sont disponible chez GS2i.**

[Visitez le site de GS2i](#)