

**G-Data : E-mail dangereux : toutes les astuces utilis  es par les cybercriminels**

**S  curit  **

Post   par : JerryG

Publi  e le : 25/11/2011 11:30:00

Afin que chaque internaute puisse facilement diff  rencier entre e-mail    dangereux et l  gitime, les experts du **G Data SecurityLabs** pr  sentent dans leur livre blanc    **Les dangers du courrier   lectronique**   , toutes les astuces les plus couramment utilis  es par les spammeurs et les fraudeurs. Autant d   informations qui permettent aux internautes d   utiliser l   e-mail en toute s  curit  .

**Les cybercriminels ont de nombreuses astuces** pour leurrer leurs victimes et les faire tomber dans le pi  ge du spam : fausses promesses de remboursement ou promotions, suppos  es notifications de mises    jour de compte de r  seaux sociaux ou de services bancaires, offres d'emploi fantaisistes, etc.



   *Les e-mails sont encore tr  s importants dans le syst  me cybercriminel. En moyenne, 83 pour cent du trafic e-mail est du spam*   , explique **Ralf Benzmann**, Directeur du **G Data SecurityLabs**.    *Dans le pass  , le chemin privil  gi   des attaquants   tait l'infection via des codes malicieux contenus dans des fichiers joints. Aujourd'hui leurs e-mails contiennent souvent des liens qui attirent les victimes sur un site dangereux par divers pr  textes. M  me si le nombre d'e-mails est   lev  , la plupart utilisent les m  mes astuces. Ainsi, quiconque est familiaris   avec ces escroqueries les reconna  tra tout de suite, m  me si le filtre antispam a   chou   dans le filtrage.*   

**Trois exemples d'attaques v  hicul  es par l   e-mail et pr  sent  es dans le livre blanc**

**L   irr  gularit  **

**Principe :** Le compte de l   utilisateur pr  sente des irr  gularit  s.

Fonctionnement : Le courrier   lectronique demande    son destinataire d'entrer ses coordonn  es de connexion sur un site Internet dont l   adresse lui est communiqu  e. Si l'utilisateur ne se conforme pas    cette demande, le courrier l   informe du risque de voir son compte bloqu   ou supprim  . Le lien communiqu   m  ne vers une r  plique du site officiel. Toutes informations saisies sur la page Internet sont transmises au cybercriminels.

Secteurs privil  gi  s : R  seaux sociaux, vente aux ench  res, compte bancaire, site e-commerce

## La remise

**Principe :** L  utilisateur b  n  ficie d  un tarif remis   exceptionnel.

Fonctionnement : Le courrier   lectronique annonce    son destinataire des remises exceptionnelles sur des produits de luxe. Montres, v  tements et bijoux de grandes marques sont propos  s    des tarifs d  fiant toute concurrence. Dans un tout autre registre, des logiciels connus peuvent aussi   tre propos  s pour seulement quelques euros. En se rendant sur la boutique propos  e, l  internaute risque d  acheter des produits contrefaits. Il risque aussi de voir ses informations de cartes bancaires vol  es et/ou son ordinateur infect  .



**Secteurs privil  gi  s :** commerce du luxe, du logiciel, de la pharmacie ou de la minceur.

  « Regarde par ici !  »

**Principe :** L  internaute est invit      regarder quelque chose d    tonnant

Fonctionnement : Le courrier   lectronique invite son destinataire    visionner des photos ou des vid  os scandaleuses de c  l  brit  s ou de fausses informations d  actualit  . Le courrier   lectronique contient un lien vers un site Internet infect  . Le code malveillant avec lequel l'ordinateur est infect   peut int  grer le PC dans un botnet ou espionner les mots de passe et les donn  es sensibles qu  il contient.

**Secteurs privil  gi  s :** actualit  , r  seaux sociaux.

**Les conseils de G Data Software pour limiter les risques :**

    Il ne faut jamais r  pondre    un spam, m  me si un lien de d  sinscription est propos  . R  pondre    un spam confirme au spammeur la validit   de l  adresse e-mail.



   En cas de doute sur leur contenu, les e-mails provenant d'exp  diteurs inconnus doivent   tre supprim  s. Aucune pi  ce jointe ne doit   tre ouverte, car elle peut contenir du code malveillant. Si l  e-mail contient un lien, l  utilisateur ne doit jamais cliquer dessus.

   L  utilisation d  une solution de s  curit   avec une fonction antispam int  gr  e est n  cessaire. Elle r  duit le nombre de spams re  us et prot  ge des e-mails infect  s.

   L  ouverture de pi  ces jointes provenant de destinataires inconnus doit   tre pr  c  d  e d  une analyse antivirus syst  matique.

### **Les grands principes    avoir en t  te avant l  ouverture d  un e-mail :**

1/ Jamais une enseigne de e-commerce, de vente aux ench  res, un r  seau social, un fournisseur d  acc  s Internet ou une banque ne demande    ses clients de confirmer leurs donn  es d  acc  s par e-mail ou sur une page Internet.

2/ Pour proc  der    une r  gularisation de   trop per  su   , jamais une institution (s  curit   sociale, minist  re des Finances, etc.) ne demande par e-mail la saisie sur un site Internet des coordonn  es bancaires, voire de carte bancaire, du destinataire du courrier. Si elle connaît le destinataire (allocataire, d  clarant, etc.), elle dispose d  j   de tous les   l  ments n  cessaires pour proc  der    un remboursement.

3/ Comment gagner    une loterie sans y avoir particip   ? Les promesses de gains   tonnants cachent    coup s  r une arnaque sous-jacente.

4/ D  une mani  re g  n  rale, sur Internet quand câ  est trop beau pour   tre vrai, câ  est souvent le cas  ! Les solutions G-Data sont [\*\*Disponibles chez : GS2i.\*\*](#)