

### **Bitdefender : Exploit Zero-day pour Yahoo! Messenger**

S curit 

Post  par : JerryG

Publi e le : 5/12/2011 14:00:00

Bitdefender annonce un nouvel exploit de type Â« zero-day Â» s visant surÂ Yahoo! Messenger en modifiant les statuts des utilisateurs   et diffuse bien s r  des malwares !

**La diffusion de malwares via Yahoo! Instant Messenger** existe depuis plusieurs ann es. L infection  tait toutefois limit e par le fait qu elle requ rait une certaine interaction avec les utilisateurs.

Ce n est d sormais plus le cas.



Un exploit d couvert r cemment dans la version 11.x du client de messagerie (y compris la r cente version 11.5.0.152-us) permet   un attaquant de modifier de fa on arbitraire,   distance, le message du statut de pratiquement tout utilisateur de Yahoo! Messenger disposant de la version vuln rable.

Les messages de statut sont particuli rement efficaces en termes de Â« taux de clics Â» puisqu ils sont adress s   un petit groupe d amis. Il y a donc de fortes chances pour que la plupart des contacts qui les voient cliquent dessus.

La victime ignore alors que son message de statut a  t  pirat .

Attention donc, si vous recevez des messages de contacts ne faisant pas partie de votre liste, vous  tes vuln rable   cet exploit.

#### **Vous n  tes pas vuln rable si :**

1. Vous utilisez une solution de s curit  Bitdefender (Bitdefender Antivirus Plus, Bitdefender Internet Security ou Bitdefender Total Security). Nous d tectons cette menace via le scanner HTTP et la bloquons avant qu elle n atteigne l application de messagerie.

2. Vous avez paramétré Yahoo! Messenger afin qu'il ignore toute personne ne faisant pas partie de vos contacts Yahoo! (option d'activer par défaut).

Bitdefender a identifié ce type d'attaque en circulation. Pour éviter ce type d'attaque, Bitdefender recommande d'installer une solution antivirus ou de régler vos paramètres de sécurité selon les instructions ci-dessus.

Bitdefender a fourni à Yahoo! la documentation et le code « proof of concept » pour leur permettre de corriger ce problème.

**[Pour en savoir plus sur cette menace.](#)**

**[Pour retrouver Bitdefender en ligne](#)**