

Offensive de Trojans sur les billets d'avion

Depuis deux semaines, de nombreuses boîtes mails reçoivent des spams prétendant délivrer des **billets électroniques et des factures** provenant de compagnies aériennes. Ces pourriels contiennent en fait une **archive zip détenant un Trojan**.

Après jetBlue Airways, d'autres compagnies ont été ciblées. Selon BitDefender, il s'agirait de « *Delta Air Lines, Virgin America, United Airlines, Continental Airlines, mais également des compagnies américaines intérieures. De même des **compagnies plus exotiques** sont prises pour cible comme Sun Country Airlines, Spirit Airlines, Allegiant Air, Frontier Airlines, AirTran Airlines, Hawaiian Airlines et Alaska Airlines...* » Que du rêve.

Les Chevaux de Troie diffusés ne sont, pour leur part, pas très nouveaux. Les **Trojan.Spy.Zbot.KJ** et **Trojan.Spy.Wsnpoem.HA**, plus connu sous les noms de [faux mails UPS et FedEx](#) sont les instigateurs des menaces.

Ces malwares s'installent dans le **répertoire Windows ou dans le dossier Program Files**. Une fois bien au chaud, ces chevaux de Troie instaurent des règles d'exception au **pare-feu Microsoft Windows**. Il est alors possible pour un pirate d'entrer par une porte dérobée (*backdoor*). Ces Trojans peuvent même se connecter à des serveurs enregistrés en **Russie**.

Il faut dire que le billet d'avion traditionnel délivré par les compagnies aériennes a fait son temps. L'**IATA** (International Airport Transportation Association), a permis aux compagnies de délivrer des [billets électroniques](#). Bien que plus écologiques et plus pratiques, ces billets ainsi que leur mode de diffusion sont plus **sujets au piratage**.

94% des compagnies auraient déjà adopté le dispositif, logiquement la hausse des menaces devrait suivre la tendance.