

# Le virus informatique Duqu est en France

Par *mogirard*

Créé le 07/11/2011 - 07:22

## Le virus informatique Duqu est en France

Lundi, 07/11/2011 - 06:22 [0 commentaire](#)

- [Diminuer la police](#)
- [Augmenter la police](#)
- [Imprimer](#)
- [Version PDF](#)

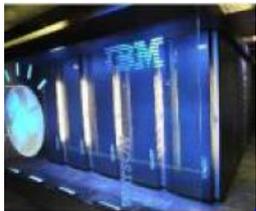
•

- [Tweeter](#)

•

•

0 avis :



[zoom](#)

Repéré il y a quelques semaines, Duqu, un [cheval de Troie](#) qui se glisse dans un fichier Word, est comparé à Stuxnet et pourrait préfigurer une attaque très ciblée contre des sites industriels. Microsoft estime le risque faible et vient seulement de publier un patch.

Le 9 octobre dernier, l'éditeur Symantec publiait sa découverte d'un [virus](#) nommé [Duqu](#) (car il génère deux fichiers dont le nom commence par DQ), « qui semble le précurseur d'une attaque de type [Stuxnet](#) ». Il partage en effet une partie de son code avec ce [virus](#) qui, en 2010, avait ciblé des équipements industriels, du type de ceux utilisés en Iran dans des installations industrielles.

Duqu exploite une faille de Windows jusque-là inconnue et se glisse dans les routines du système d'exploitation chargées de l'affichage des polices de caractères TrueType. Cet intrus peut alors « exécuter du code en mode [kernel](#) », vient d'expliquer [Microsoft](#) dans un communiqué. Autrement dit, obtenir les droits les plus élevés et pouvoir tout faire dans l'[ordinateur](#) et par exemple installer de nouveaux programmes ou ouvrir les comptes utilisateurs.

Ce serait là le travail de Duqu : explorer le poste de travail, collecter des données, les envoyer sur des [serveurs](#) distants et télécharger des [logiciels](#). Deux de ces serveurs ont été repérés et débranchés, en

Inde puis en Belgique. De son côté, Microsoft, qui juge le risque faible, dit travailler à un correctif et, en attendant qu'il soit publié, propose une méthode pour éviter l'intrusion : désactiver la [reconnaissance des polices TrueType](#).

- **Un [robot](#) espion spécialisé dans le renseignement**

Ce cheval de Troie, cependant, ne se réplique pas. Il a été volontairement envoyé par courrier électronique dans des documents Word « **à six organisations** » et ce dans huit pays selon le dernier [communiqué de Symantec](#) : France, Hollande, Inde, Iran, Soudan, Suisse, Ukraine et Vietnam. D'autres distributeurs l'ont signalé également en Autriche, en Hongrie, en Indonésie, au Royaume-Uni ainsi que dans d'autres entités en Iran.

[Futura Sciences](#)

**Noter cet article :**

**Recommander cet article :**

- 
- [Tweeter](#)
- 
- **Nombre de consultations :** 125
- **Publié dans :** [Informatique](#)
- **Partager :**
  - [Facebook](#)
  - [Viadeo](#)
  - [Twitter](#)
  - [Wikio](#)

[Informatique cheval de Troie Duqu ordinateur Stuxnet Symantec virus](#)

---

URL source: <https://www.rtflash.fr/virus-informatique-duqu-est-en-france/article>