

# 250 millions de PC infectés par un nouveau malware

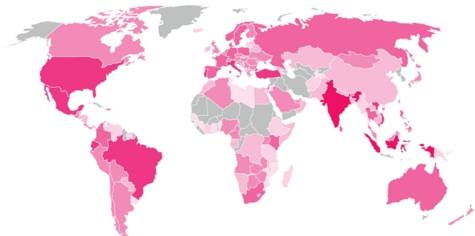


250  
millions  
de PC  
infectés  
par un  
nouveau  
malware

Après Wannacry, c'est au tour de Fireball de menacer les ordinateurs. Ce malware chinois ne bloque pas les machines pour exiger de l'argent, mais il détourne les recherches effectuées sur le navigateur et récupère discrètement les données.

Les internautes n'ont pas fini de s'arracher les cheveux à cause des virus informatiques. Après Wannacry qui bloquait les ordinateurs pour demander des rançons, voici le malware Fireball. Ce logiciel asiatique qui infecte les ordinateurs a été détecté par les experts de **Check Point**. Il prend discrètement le contrôle d'un PC pour détourner les recherches et récupérer les données. Il aurait déjà infecté plus de 250 millions de machines dans le monde. Les zones géographiques les plus touchées sont l'Inde, le Brésil et l'Amérique, mais l'Europe et la France ne sont pas épargnées.

Ce logiciel n'est pourtant pas le fruit d'un gang de hackers. C'est officiellement un adware -nom donné aux logiciels publicitaires- qui a été développé en toute légalité par **Rafotech**, une agence de marketing digitale chinoise qui a pignon sur rue. Et pour le répandre, l'entreprise l'a inséré discrètement dans des suites logicielles téléchargeables gratuitement, tels que « FVP Imageviewer », « Deal Wifi » ou « SoSo Desktop ». Mais il ne se contente pas de diffuser de la pub.



Check Point – Diffusion mondiale de Fireball

Une fois installé, Fireball change la page d'accueil du navigateur pour afficher un faux moteur de recherche (« Trotux ») qui redirige les recherches vers des moteurs que l'utilisateur n'aura pas forcément choisis. Il va également installer un système de traçage pour collecter des données de navigation, mais aussi, selon Check Point, les mots de passe ou les numéros de cartes bancaires.

Fireball pourrait également prendre le contrôle d'une machine pour installer et d'exécuter à distance des logiciels espions. Il crée aussi une porte dérobée pour espionner ses victimes. Les experts en sécurité conseillent aux victimes de le supprimer au plus vite. Si la page d'accueil de votre PC a été modifiée sans votre intervention, il y a de grande chance qu'il ait été contaminé.

[Source : BFM Business]

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en **RGPD** (Protection des Données à Caractère Personnel).



- Audits **RGPD**
- Accompagnement à la mise en conformité **RGPD**
- Formation de Délégués à la Protection des Données
- Analyse de risques **ISO 27001**
- Expertises techniques et judiciaires ;
- Recherche de preuves : téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

**Le Net Expert**  
**INFORMATIQUE**  
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

ou suivez nous sur

Réagissez à cet article

Source : *Après Wannacry, c'est au tour de Fireball de menacer les ordinateurs. Ce malware chinois ne bloque pas les machines pour exiger de l'argent, mais il détourne les recherches effectuées sur le navigateur et récupère discrètement les données.*