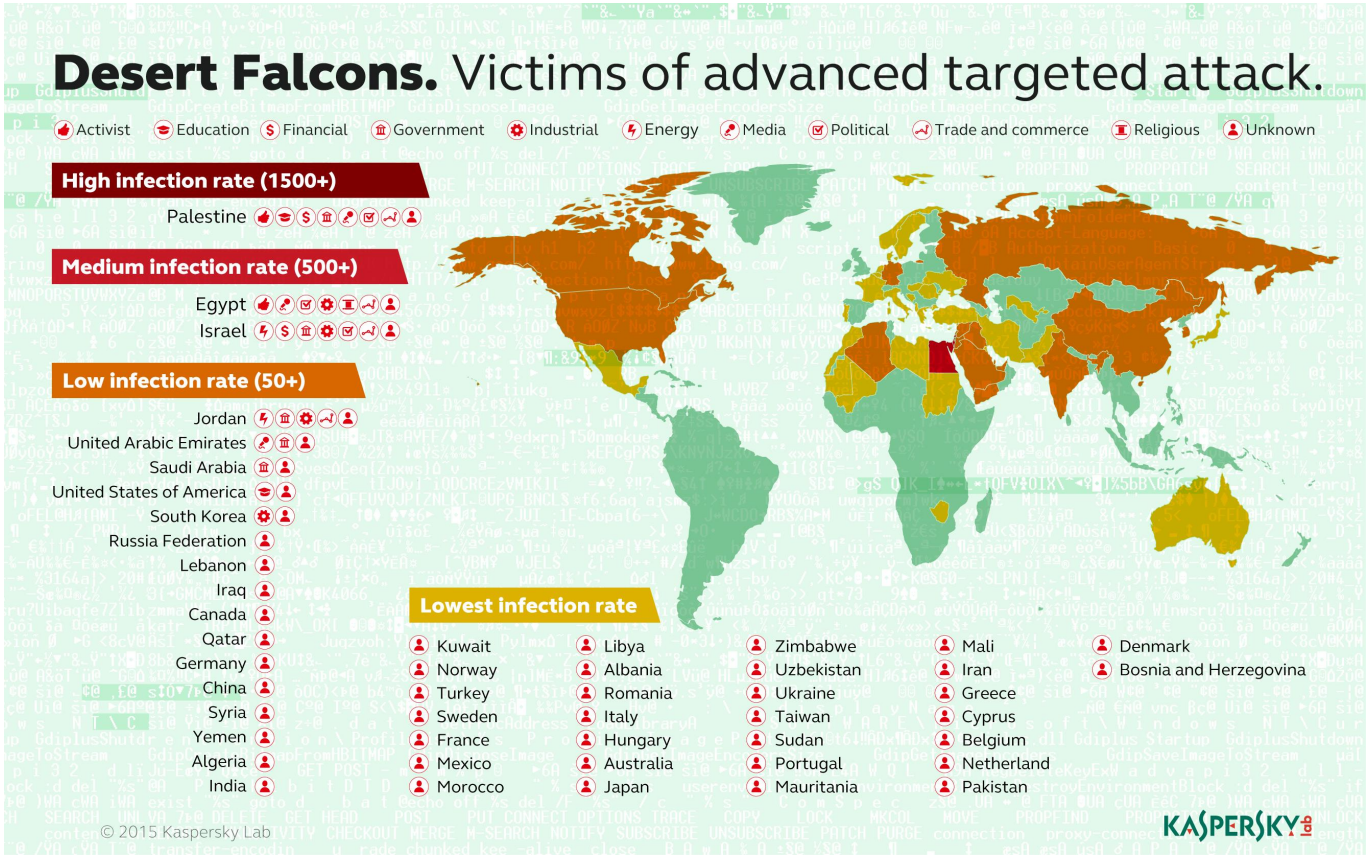
Desert Falcons : Kaspersky identifie un groupe de cybermercenaires arabes

Quelques jours après avoir révélé la portée d'une attaque contre de nombreux établissements bancaires dans le monde, les laboratoires de l'éditeur Kaspersky mettent au jour l'activité de Desert Falcons, groupe de cyberespions s'attaquant surtout à des individus et entreprises au Moyen-Orient (Egypte, Palestine, Israël et Jordanie principalement). Pour l'éditeur, il s'agit là du « *premier groupe arabe connu de cybermercenaires* », maniant des APT (attaques persistantes avancées) pour soutirer de l'information. La campagne d'attaques est **en cours depuis au moins deux ans** (même si Kaspersky affirme que le groupe de pirates est actif depuis 2011). Et le pic d'activité a été enregistré en ce début d'année.



Au total, Kaspersky estime que les Desert Falcons ont fait **3 000 victimes dans une cinquantaine de pays** – leur activité ne se limitant pas au seul Moyen-Orient, même si cette région reste leur théâtre d'opérations privilégié. Kaspersky mentionne la France parmi les pays ciblés (avec toutefois un faible taux d'infection : moins de 50 organisations concernées). Et donne une liste assez longue des organisations ciblées : agences de défense, administrations (notamment des responsables de la lutte anti-blanchiment), santé, médias, recherche, enseignement, banques, entreprises assurant la sécurité physique (une cible qualifiée de « *mystérieuse* » par Kaspersky), réseaux d'énergie mais aussi des responsables politiques ou des militants.

Pirater le journal des appels d'Android

La méthode d'infection est assez classique. Via **du phishing**, les hackers incitent les utilisateurs visés à ouvrir des documents corrompus ou à cliquer sur des liens débouchant sur le téléchargement d'un fichier infecté. Kaspersky signale que Desert Falcons emploie la **technique de l'inversion de suffixe** pour endormir la vigilance des utilisateurs même avertis. Ainsi un fichier se terminant normalement par fdp.scr se conclut par rcs.pdf…

Ensuite, les hackers. **Une trentaine de personnes réparties en trois équipes** situées en Palestine, Egypte et Turquie selon Kaspersky, utilisent **leurs propres malwares** (un Troyen nommé Desert Falcons et la backdoor DHS) pour soutirer de l'information, via des copies d'écran, l'enregistrement des frappes clavier, l'exfiltration de fichiers, la collecte d'informations dans les fichiers Word et Excel présents sur le disque dur et les périphériques USB, le vol de mots de passe dans la base de registre Windows (IE et Live Messenger) ou des enregistrements audio. Kaspersky Lab a également détecté l'activité d'un malware « *qui semble être un backdoor Android capable de pirater le journal des appels et des SMS sur un mobile* ».

Au total, les Desert Falcons, dont Kasperky affirme connaître l'identité de certains membres, ont **dérobé plus d'un million de fichiers** à leurs victimes, estime l'éditeur. Dont des communications diplomatiques, des plans et documents militaires, des documents financiers ou des carnets d'adresses de média.

A lire aussi :

Plus d'un milliard de données volées en 2014
FIC 2015 : les hackers ont gagné une bataille, pas la guerre

crédit photo © Pavel Ignatov – shutterstock

crédit photo @ GlebStock – Shutterstock