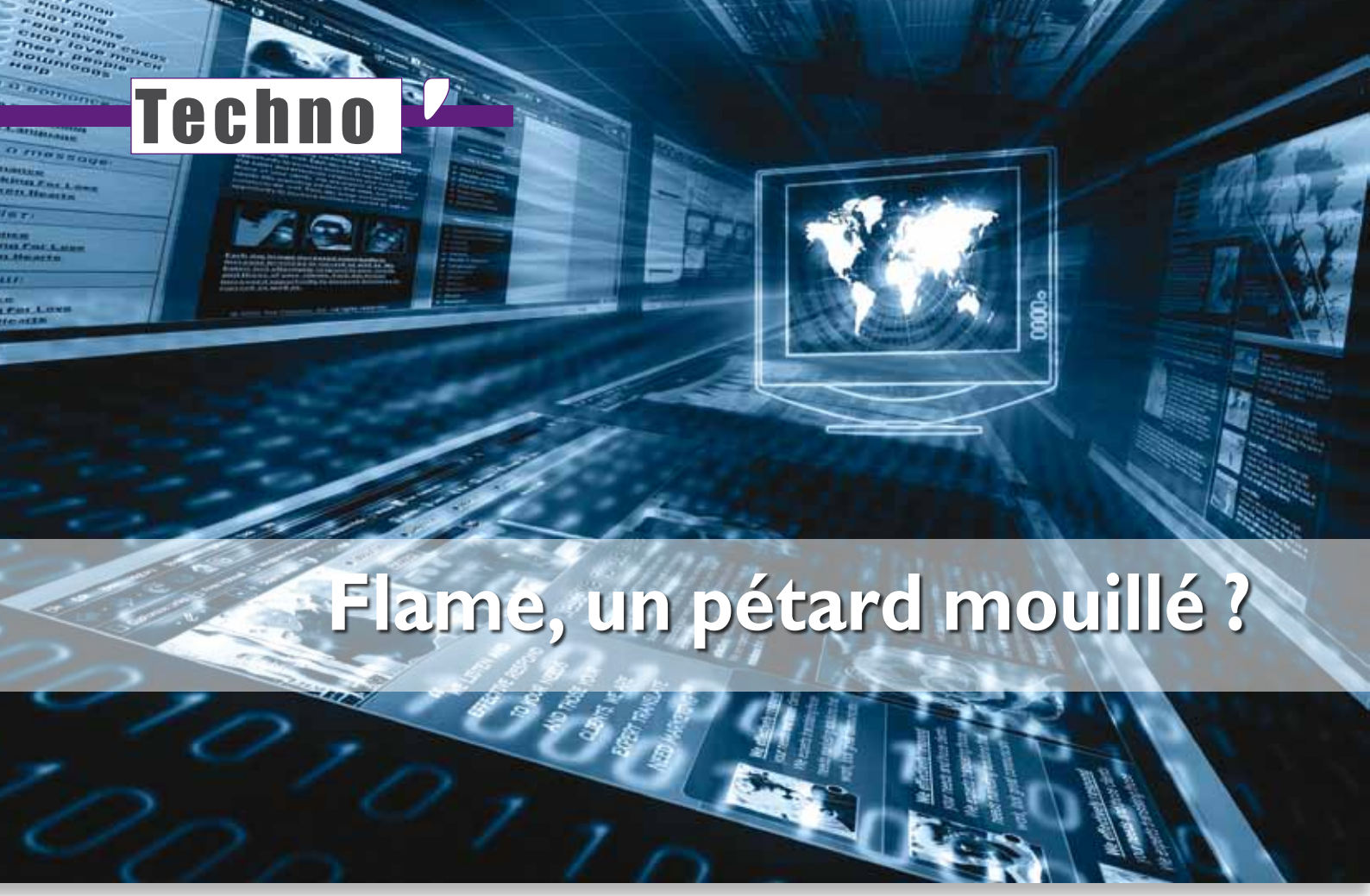


Flame, un pétard mouillé ?

Après Stuxnet et Duqu, un nouveau virus surpuissant susceptible de fragiliser des sites industriels a été mis à jour par Kapersky Lab. Mais quelques semaines plus tard, alors que des révélations sur son origine sont dévoilées, la menace s'autodétruit.

Un petit tour et puis s'en va ! Le virus Flame (flamme, en français), digne héritier de Stuxnet et Duqu, 50 fois plus puissant que ses prédécesseurs à en croire les spécialistes, a défrayé la chronique dans le monde industriel au mois de mai… et a disparu en juin sans laisser de trace. *« Certains centres de commande de Flame ont envoyé un nouvel ordre à plusieurs ordinateurs contaminés. Cet ordre est destiné à faire complètement disparaître Flame des ordinateurs compromis »*, annonçait ainsi récemment la société de sécurité informatique Symantec sur son blog. Les acteurs du domaine, à commencer par les éditeurs de solutions de supervision, dont certains avaient été bousculés à l'époque de Stuxnet, peuvent donc respirer. Les industriels français aussi, puisqu'il semble que cette vérole n'a pas passé nos frontières – elle est cependant présente ailleurs en Europe et aux Etats-Unis. Mais désormais, on sait que la faille existe, que des virus informatiques peuvent s'immiscer dans pratiquement n'importe quelle machine, n'importe où, en ponctionner le contenu et modifier les réglages de parties opératives, sans que personne ne s'en aperçoive. D'ailleurs, certains spécialistes estiment que des virus semblables à Stuxnet seraient actuellement actifs quelque part…

Toujours un coup d'avance

Selon Kapersky, qui a débusqué le virus presque par hasard, Flame s'est attaqué à des PC Windows en Iran et dans la région israélo-palestinienne et dans quelques machines en Amérique du Nord. Il contiendrait 20 fois plus de lignes de code que Stuxnet et *« 100 fois plus que n'importe quel*

Trois frères, toujours plus puissants

Stuxnet : premier virus de la trilogie, identifié en 2010, il a été créé pour analyser et détruire une cible industrielle déterminée.

Duqu : découvert l'an dernier, ce deuxième virus est un descendant direct de Stuxnet, dont il reprend une partie du code. Il est quant à lui destiné à l'espionnage industriel et le vol de données critiques.

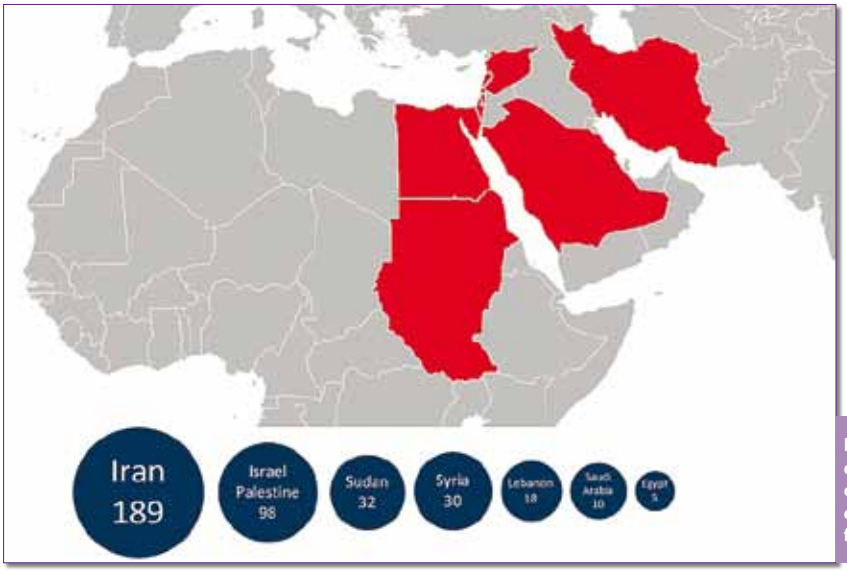
Flame : c'est le plus puissant de tous, dont le but est de collecter des informations sur les ordinateurs qu'il envahit. Identifié cette année, il a surtout sévi en Iran et dans les pays limitrophes : Egypte, Syrie et Arabie saoudite.

logiciel pirate classique conçu pour subtiliser des données financières ». Il est en mesure d'aller piocher des données à distance, d'intervenir sur les réglages d'un ordinateur, d'activer son micro et d'enregistrer une conversation… Mieux, comme Duqu, il réalise des captures d'écran de l'ordinateur infecté à intervalles réguliers, se connecte à des messageries instantanées, active le Bluetooth et interroge les périphériques ambiants, comme des smartphones… Sa porte d'entrée ? Une faille de Windows.

Le grand talent de ces virus d'un nouveau genre, c'est d'avoir sévi plusieurs années avant d'être détectés – plus d'un an et demi pour Stuxnet, et jusqu'à cinq ans pour Duqu et Flame – alors qu'ils sont relativement imposants. Flame atteint une vingtaine de Mégaoctets (600 Ko pour Stuxnet). Une taille importante, mais qui passe inaperçue lorsque le mode de propagation passe par des mises à jour de Windows…

Sommes nous menacés ?

Pour l'heure, Flame est déjà entré en Europe, par la Russie, la Hongrie et l'Autriche et, jusqu'à présent, il n'y aurait atteint qu'un peu plus de 600 machines. En outre, ce type de programme malveillant n'a été créé que pour ponctionner des données sur les machines et, selon Kaspersky, c'est avant tout une *« cyber-arme utilisée à des fins d'espionnage d'État à État »*. Pour l'instant, les spécialistes des antivirus n'y ont décelé que des morceaux de code déjà connus, et si un ordinateur peut être contaminé par Flame à cause d'une simple clé USB ou d'un accès à un réseau local, le malware ne saurait pas, contrairement à Stuxnet, se démultiplier seul afin d'infecter un grand nombre de machines. Une volonté manifeste de ses concepteurs, pour ne pas renouveler la diffusion incontrôlée du virus... Enfin, le centre Maher, dépendant du ministère iranien des Télécommunications iranien, aurait *« réussi à identifier le virus Flame puis à préparer un anti-virus capable de l'identifier et de l'éliminer »*, selon un communiqué. Cet anti-virus *« est à la disposition des organes et des administrations qui en font la demande »*, poursuit ce communiqué. Et de toute façon, la disparition *« programmée »* de Flame pourrait non seulement marquer la fin du fléau, mais aussi forcer l'arrêt de toute investigation… ▮



La contamination a été majoritairement constatée en Iran et dans les pays frontaliers.

Stuxnet and Co : un coup des Américains

On le sait maintenant, le fameux virus Stuxnet, qui visait avant toute chose des centrifugeuses iraniennes, a été mis au point dès 2006 et déployé par les Américain et leurs alliés au Proche-Orient. Un ouvrage qui vient de sortir aux USA – *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, par David E. Sanger – livre ainsi tous les détails de cette affaire de « cyberguerre » des Etats-Unis contre l'Iran et son programme nucléaire, qui aurait débuté avec George W. Bush et se serait poursuivie en 2009 sous Barack Obama.

On y apprend que le virus développé conjointement par National Security Agency (NSA)et Israël, d'abord baptisé « Olympic Games » (jeux olympiques), a bénéficié du plein feu vert de la Maison blanche. Et l'auteur de ce livre n'est pas équivoque quant à la responsabilité de l'actuel président américain dans cette entreprise. *« Jamais [...] un président n'avait été impliqué d'aussi près dans l'escalade pas à pas d'une attaque contre les infrastructures d'une nation étrangère »*, écrit-il. Au point qu'il aurait même suivi l'évolution des opérations semaine après semaine…

La mission était simple : le virus, une fois implanté – tout simplement par l'intermédiaire d'une clé USB confiée à l'un des employés –, devait modifier, sans que cela soit décelable par les exploitants, la vitesse de rotation des centrifugeuses, au point de provoquer des dégâts irréversibles. Par le fruit du hasard, le virus est devenu Stuxnet et s'est propagé hors de l'Iran. Les Américains auraient donc décidé de l'enterrer, mais seraient revenus à la charge avec une nouvelle version, encore plus perfectionnée : Flame. Un virus terriblement efficace puisqu'il aurait abouti à la destruction de mille centrifugeuses iraniennes et, par voie de conséquence, à un retard de plus de deux ans et demie du programme nucléaire iranien. Ne reste plus qu'à espérer que l'arme ne se retourne pas contre son créateur et que des terroristes geeks ne se mettent pas à lancer des offensives du même type contre les Etats-Unis, d'autres nations ou des entreprises mondialement connues. Car, manifestement, aucune n'est vraiment prête à faire face à ce genre d'attaque.