L'ESPION ÉTAIT DANS LE .DOC

LE 14 SEPTEMBRE 2012 ***JEAN MARC MANACH***

Les marchands d'armes de surveillance n'ont vraiment pas de chance : à chaque fois qu'on entend parler d'eux, c'est parce qu'ils fournissent des dictateurs, espionnent des défenseurs des droits humains ou bien des journalistes.

Fin juillet, on **découvrait** que le logiciel espion du marchand d'armes de surveillance numérique britannique FinFisher avait été utilisé à l'encontre de défenseurs des droits humains bahreïnis. En août, on découvre que des journalistes marocains ont, eux, été ciblés par Hacking Team, un concurrent italien de FinFisher.

COLÈRES D'ARABIE : LE LOGICIEL ESPION

Cruel paradoxe de ce printemps arabe : les défenseurs des droits de l'homme bahreïnis utilisent les réseaux sociaux ...

Mamfakinch ("*nous n'abandonnerons pas*", en arabe marocain), est un site d'informations créé par un collectif de blogueurs et militants marocains dans la foulée du printemps arabe, et plus particulièrement du mouvement dit **du 20 Février**, qui appelait notamment à l'ouverture d'une enquête sur "*les arrestations arbitraires et les procès expéditifs* », et à la « *rupture avec la logique de répression face au droit des manifestations pacifiques*". Devenu, en moins d'un an, l'un des médias citoyens les plus populaires au Maroc, il a plusieurs fois fait l'objet d'attaques ou de tentatives de déstabilisation visant à le faire taire.

Ce 2 juillet 2012, Google et ***GlobalVoices*** remettait à *Mamfakinch* un **Breaking Border Awards**, prix créé pour honorer les sites qui s'illustrent par leur défense de la liberté d'expression sur Internet. Le 20 juillet, la rédaction de Mamfakinch recevait un email intitulé *Dénonciation*, accompagné d'une pièce jointe, *scandale (2).doc*, et d'une phrase sibylline en français :

> ***Svp ne mentionnez pas mon nom ni rien du tout je ne veux pas dembrouilles…***

Appâtés, les journalistes tentent d'ouvrir le fichier joint… sans succès. Intrigués, et doutant de la véracité du mail, ils le font suivre à **Abderahman Zohry**, co-fondateur de *Mamfakinch* et du Parti pirate marocain, mais également directeur technique de **DefensiveLab**, une société de sécurité informatique marocaine. **Anas El Filali**, blogueur et principal actionnaire de Defensive Lab, a **raconté** à *Yabiladi*, un site d'information marocain, qu'en analysant le document, les hackers de son entreprise ont découvert un virus qui n'avait encore jamais été identifié :

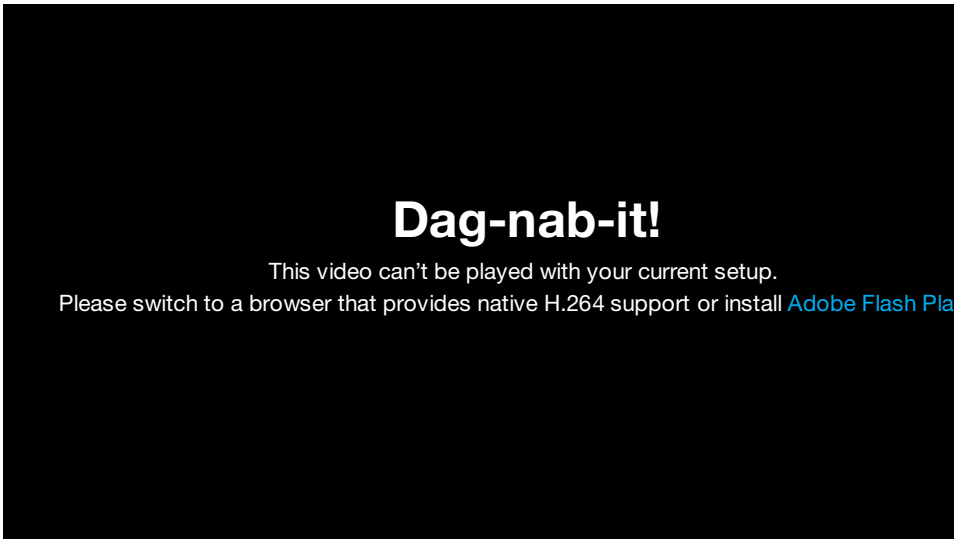
> ***Ce dernier prend pour cible les machines qui tournent sous MAC OS et Windows, et il était encore indétectable par les antivirus. Un document Word contenait un code exploitant une faille existante dans le composant Flash afin d'installer le cheval de Troie.***
>
> ***Techniquement, une attaque de ce genre peut donner à l'attaquant un accès à toutes les données de l'ordinateur infecté, ainsi que d'enregistrer tout le trafic entrant et sortant (discussions et contacts MSN, Skype, mots de passe, touches tapées et URLs visitées sur le navigateur…).***

Le 24, Lysa Meyers, une des chercheuses d'Intego, une société de sécurité informatique spécialisée dans l'univers Mac, **découvre** le cheval de Troie, que DefensiveLab a envoyé à **Virus Total**, un site qui permet à tout internaute de passer n'importe quel fichier au travers des scanners de 41 éditeurs d'anti-virus, et que Google vient de **racheter**.

DES CHEVAUX DE TROIE DANS NOS DÉMOCRATIES

OWNI lève le voile sur les chevaux de Troie. Ces logiciels d'intrusion vendus aux États, en particulier en France et en ...

Le 25, Lysa Myers publie un **nouveau billet** expliquant comment le logiciel malveilant fonctionne, révélant qu'on y trouve des bouts de code évoquant le nom d'un concurrent italien de FinFisher, **Hacking Team**. Son cheval de Troie, **Remote Control System Da Vinci** (RCS, pour "*système de contrôle à distance* "), présenté comme une "*suite de hacking pour l'interception gouvernementale*", se targue de pouvoir pirater n'importe quel système informatique, afin de pouvoir surveiller, espionner et récupérer tout type de données sur les ordinateurs infectés.



Des dizaines d'articles ont relayé cet été, dans la foulée, la découverte de ce nouveau cheval de Troie, surnommé Crisis par Intego, **Morcut** par Sophos, ou encore

BackDoor.DaVinci.1 par Dr.Web -qui qualifie Hacking Team de *"criminels"*. Depuis, les éditeurs d'anti-virus rivalisent de communiqués pour annoncer qu'ils avaient rajouté le cheval de Troie dans la liste des logiciels malveillants, de sorte qu'ils ne puissent plus contaminer les ordinateurs de leurs clients.

A ce jour, 26 éditeurs d'antivirus **détecteraient** le cheval de Troie de Hacking Team, et 36 **celui** de FinFisher, ce qui n'est pas sans poser quelques problèmes à ces marchands d'armes de surveillance numérique. D'une part parce que l'on en sait un peu plus sur leurs technologies, et donc comment s'en protéger, d'autre part parce qu'ils se targuaient, auprès de leurs clients, d'avoir créé des chevaux de Troie que les antivirus ne détectaient pas.

UN GROS REQUIN DE L'INTRUSION

En partenariat avec WikiLeaks, OWNI révèle le fonctionnement de FinFisher, l'une de ces redoutables armes d'espionnage ...

FinFisher, Hacking Team et leurs quelques concurrents défendent leurs logiciels espions en expliquant qu'ils ne le vendent qu'à des services de renseignement, forces de police et gouvernements, et qu'ils ne seraient donc utilisés que dans le cadre de la lutte contre le terrorisme ou la criminalité. On a désormais la preuve qu'ils servent aussi à espionner des défenseurs des droits humains et journalistes.

Les autorités britanniques, de leur côté, **viennent d'annoncer** que FinSpy avait été placé dans la liste des "*technologies duales*" dont l'exportation, hors union européenne, doit être dûment autorisée.

Le blocage des chevaux de Troie par les antivirus, ainsi que la décision britannique de contrôler leur prolifération, constitue un tournant. Et la facture pourrait s'avérer salée : David Vincenzetti, le fondateur de Hacking Team, avait **expliqué** en novembre 2011 qu'il commercialisait la licence de RCS Da Vinci pour 200 000 euros, par an. **D'après Ryan Gallagher**, un journaliste de *Slate* qui l'avait rencontré en octobre 2011, RCS a été vendu depuis 2004 "*à approximativement 50 clients dans 30 pays sur les cinq continents* ". FinSpy, à en croire cette **proposition de contrat** trouvée en mars 2011 dans l'un des bâtiments de la sécurité égyptienne après la chute du régime Moubharak, serait vendu, de son côté, près de 300 000 euros.

Image CC **quantumlars** du **Trojan Horse** de Burning Man 2011.

J
le 14 septembre 2012 - 21:03 • SIGNALER UN ABUS - PERMALINK

J'ai trouvé hier trois virus dans des documents .doc que l'on m'avait donné il y a trois ans (heureusement jamais ouverts), et qui n'avaient jamais été détecté durant toute cette période. C'était des livres en espagnol de Adorno, Gramsci, et un autre sur les Tupamaros. Plutôt bizarre.

VOUS AIMEZ 1 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

M. CAMOMILLE
le 18 septembre 2012 - 17:15 • SIGNALER UN ABUS - PERMALINK

Comme quoi… Ce sont les mêmes méthodes qu'utilise la Chine à l'encontre de ses opposants en tout genre. Les démocraties doivent choisir leur camp !

VOUS AIMEZ 1 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

NOPE
le 18 septembre 2012 - 18:32 • SIGNALER UN ABUS - PERMALINK

Les démocraties ont déjà choisi leur camp : celui de l'argent.

Sinon, pourquoi délocaliser des activités en Chine, grand pays honorablement connu comme défenseur actif des droits de l'homme ?

Sinon, pourquoi soutenir l'activité de ces petites officines, plus ou moins officielles, dont l'espionnage tous azimuths est le fond de commerce ?

VOUS AIMEZ 4 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

LE POURFANEUR

le 26 septembre 2012 - 10:39 • SIGNALER UN ABUS - PERMALINK

J'ai vous lire, j'aime vous voir pensez que les gouvernements ont encore leurs mots à dire, qu'ils ont encore une once de pouvoir ! C'est beau d'être niai comme ça !

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE