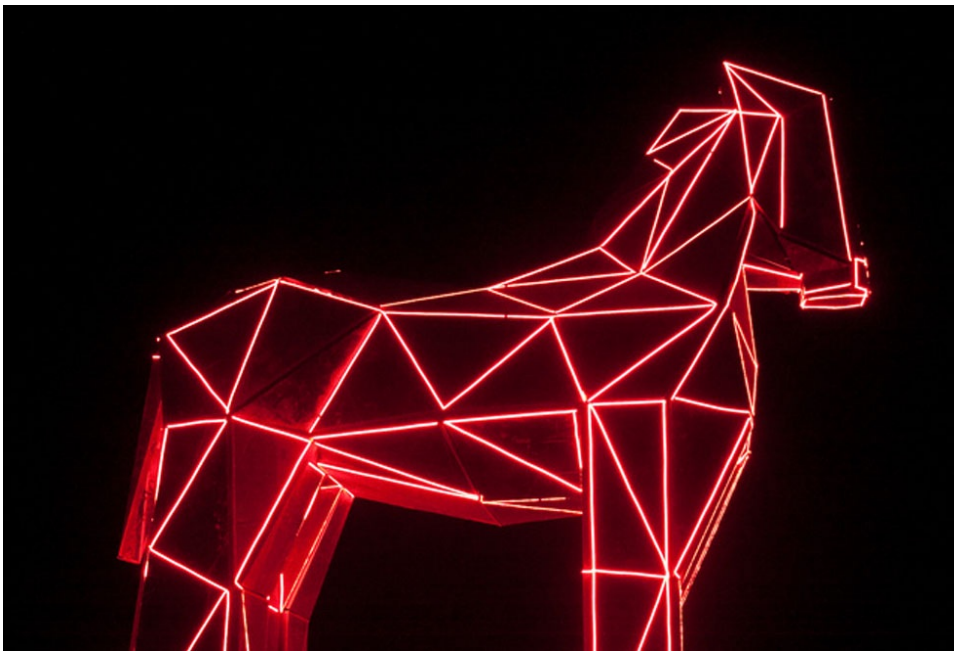
DES CHEVAUX DE TROIE DANS NOS DÉMOCRATIES

LE 13 DÉCEMBRE 2011 ***JEAN MARC MANACH***

OWNI lève le voile sur les chevaux de Troie. Ces logiciels d'intrusion vendus aux États, en particulier en France et en Europe, pénètrent tous les systèmes, depuis les smartphones jusqu'aux connexions WiFi. Enquête réalisée en partenariat avec WikiLeaks.



Ces dernières années, un quarteron d'entreprises privées a développé des logiciels espions visant à déjouer tous les mécanismes de sécurité ou de chiffrement des communications utilisés par ceux qui cherchent à protéger leurs données, et leur vie privée. Ces logiciels, ce sont des **chevaux de Troie**. OWNI, en partenariat avec WikiLeaks dans le cadre de la publication des **SpyFiles**, s'est penché sur les documents se rapportant à ces technologies très particulières.

Comme dans la mythologie, un cheval de Troie se fait passer pour ce qu'il n'est pas, permet de prendre le contrôle total de l'ordinateur qu'il infecte, à distance, de sorte de pouvoir y lire les données avant même qu'elles ne soient chiffrées et donc sécurisées, ou encore de pouvoir y activer le micro, ou bien la caméra, et cætera.

Les hackers allemands du Chaos Computer Club ont ainsi récemment **révélé** comment la police allemande utilisait, en toute illégalité selon eux, un tel virus informatique pour espionner les ordinateurs de criminels supposés.

Mouchards

La police suisse a **reconnu** utiliser elle aussi le même cheval de Troie. Début novembre, la France publiait de son côté, au Journal Officiel, la **liste** des services, unités et organismes habilités à installer de tels logiciels espions permettant, à distance, la "*captation des données informatiques*", terme officiel pour qualifier l'utilisation de mouchards informatiques.

Les documents internes de la société FinFisher **démontrent** ainsi toute l'étendue du savoir-faire de ces pirates informatiques au service, officiellement, des seuls forces de l'ordre et des services de renseignements. Dans le cadre de l'opération SpyFiles menée avec WikiLeaks, nous avons pu recueillir plusieurs vidéos d'entreprise de cette société, réalisées à des fins commerciales, pour convaincre leurs clients – essentiellement des États – de la simplicité de leurs outils d'espionnage. En voici un montage (la musique et les explications sont d'origine), révélateur du fonctionnement de ces chevaux de Troie :

Chiffrés

Un reportage **diffusé** dans le magazine Zapp de la chaîne de télévision allemande ARD [en] montre qu'ils ont aussi servi à espionner des défenseurs des droits de l'homme en Egypte. Pire : on y découvre que si le discours officiel des autorités allemandes est de soutenir les défenseurs des libertés de ce "*printemps arabe*", dans les faits, elles soutiennent également, et activement, l'exportation de ces armes de surveillance, même et y compris à des dictateurs ou des régimes totalitaires où elles sont utilisées pour réprimer la population, au motif qu'il s'agirait d'un "*marché du futur* ".

Ces comportements, favorisant le développement de telles technologies intrusives, s'expliquent par l'évolution de nos relations aux télécommunications. Car, signe des temps, si la majeure partie des conversations téléphoniques et des données échangées sur le Net circulent en clair, une partie de plus en plus importante de ces flux d'information sont désormais chiffrés.

En 1991, **Philip Zimmermann**, un développeur américain, met en ligne Pretty Good Privacy (PGP), le premier logiciel de **cryptographie** grand public permettant à ses utilisateurs de pouvoir échanger des emails ou documents chiffrés, et donc sécurisés au sens où, même interceptés, ils ne peuvent pas être déchiffrés.

Jusqu'alors, ce genre de systèmes n'était utilisé que par les services de renseignements, les militaires, ambassades, gouvernements et, bien entendu, les espions. Mais dans la mesure où les données circulant sur le Net sont à peu près aussi protégées que le sont les cartes postales, Zimmermann estima que les internautes devaient pouvoir fermer l'enveloppe, et donc communiquer en toute confidentialité.

Dans les faits, la robustesse de PGP s'apparenterait plutôt à celle d'un coffre-fort. Pour communiquer, leurs utilisateurs doivent installer le logiciel, et créer une "*clef publique* ", sorte de coffre-fort ouvert et mis à disposition des autres utilisateurs, et une "*clef privée* ", qui permet d'ouvrir le coffre-fort une fois celui-ci fermé. Si quelqu'un veut communiquer avec moi, il place le message dans mon coffre-fort public, claque la porte, que je serai le seul à pouvoir ouvrir en utilisant ma clef privée.

La mise en ligne de PGP visait à améliorer la protection des droits de l'homme et la défense de la vie privée, comme il l'**expliqua** brillamment dans un texte placé sous l'égide du Mahatma Gandhi. Dans les faits, elle lui valut aussi d'être poursuivi, pendant trois ans, par les autorités américaines, qui voyaient d'un très mauvais œil ce qu'elles qualifièrent alors d '*"exportation illégale de matériel de guerre"* .

Dans un grand nombre de pays, la cryptographie relève en effet de cette catégorie de matériels sensibles que l'on ne peut pas exporter sans l'aval des autorités. A l'époque, Zimmermann bénéficia du soutien d'internautes du monde entier, et les autorités américaines abandonnèrent leurs poursuites. Son logiciel était accessible, et utilisé, dans le monde entier.

Dans le même temps, l'essor du commerce électronique rendait obligatoire la libéralisation

de la cryptographie : le seul moyen de sécuriser les transactions est en effet de faire de sorte que l'on puisse envoyer son n° de carte bancaire sur le Net sans risque de le voir intercepté. Et c'est précisément pour cette raison que la France, qui la classait jusqu'alors comme relevant du matériel de guerre, libéralisa finalement la cryptographie à la fin des années 90.

Vie privée

Depuis, un nombre croissant de sites, non seulement de commerce électronique, mais également de réseaux sociaux, fournisseurs de mails, etc., sont accessibles en **`https`** ("*s*" pour "*sécurisé*"), rendant inopérante les écoutes classiques. L'EFF, pionnière des organisations de défense des droits de l'homme et de la vie privée sur le Net, a ainsi développé un plugin pour Firefox, **HTTPS everywhere**, afin de généraliser, autant que faire se peut, l'utilisation du **`https`**.

Skype et BlackBerry, utilisés par des centaines millions de personnes pour se téléphoner, ou échanger des données, dans le monde entier, sont eux aussi un cauchemar pour les espions aux "*grandes oreilles*", dans la mesure où, même interceptées, les communications, chiffrées, sont a priori indéchiffrables.

GnuPG, le logiciel de protection de la vie privée qui permet de chiffrer, sécuriser et authentifier données et e-mails, et qui a supplanté PGP, est de son côté utilisé par la quasi-totalité des développeurs de logiciels libres. Et, au vu de la montée en puissance des technologies de surveillance, nombreux sont désormais les internautes à utiliser des coffre-forts électroniques, tel **TrueCrypt**, pour sécuriser leurs données et éviter qu'elles ne puissent tomber dans de mauvaises mains.

Afin de répondre aux risques d'espionnage informatique, ou de pertes de données confidentielles, les autorités elle-mêmes encouragent les entreprises à apprendre à leurs salariés comment s'initier à la sécurité informatique, et sécuriser leurs communications (voir, à ce titre, mon **Petit manuel de contre-espionnage informatique**).

C'est cette évolution des pratiques numériques qui a favorisé l'émergence de systèmes de surveillance et d'intrusion de plus en plus sophistiqués, qui répondent de nos jours à la demande de tous les États. La question reste de savoir qui encadrera l'exportation de ces armes de surveillance de sorte que nos démocraties cessent de porter aide et assistance aux dictateurs…

Photos des chevaux de troie au festival Burning man par **Abraxas3d [cc-bync]** et **Terra Incognita [cc-bync]** via Flickr
Retrouvez notre dossier sur le sujet :
Un gros requin de l'instruction et **Une journée sous surveillance**

Tous les articles OWNI/WikiLeaks **sont là**

Défense. Peut-être que ça peut aider celles et ceux qui souhaite approfondir le sujet http://archives.livreblancdefenseetsecurite.gouv.fr/information/les_dossiers_actualites_19/livre_blanc_sur_defense_8

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

PLORF
le 13 décembre 2011 - 9:50 • SIGNALER UN ABUS - PERMALINK

"Skype et BlackBerry, utilisés par des centaines millions de personnes pour se téléphoner, ou échanger des données, dans le monde entier, sont eux aussi un cauchemar pour les espions aux "grandes oreilles", dans la mesure où, même interceptées, les communications, chiffrées, sont a priori indéchiffrables."

Oui mais, sous couvert du Patriot Act, les serveurs sont grand ouvert aux besoins des gouvernements donc pas de "problème" d'accès pour ces services. Même si le fait d'avoir des coms en P2P rend le travail plus complexe.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

TTH
le 13 décembre 2011 - 9:53 • SIGNALER UN ABUS - PERMALINK

Diane, OpenDNS semble ne pas être si clair que ça dans ses actions : http://www.bortzmeyer.org/opendns-non-merci.html

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

DIANE
le 13 décembre 2011 - 10:07 • SIGNALER UN ABUS - PERMALINK

@TTH: merci beaucoup pour cette remarque, je m'incline, je ne connaissais pas cet article. En plus tout ce qu'écrit Stéphane Bortzmeyer quand il appelle de ses voeux au déploiement d'IPsec pourrait venir compléter le tableau favorablement.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

DIANE
le 13 décembre 2011 - 10:12 • SIGNALER UN ABUS - PERMALINK

@TTH Merci beaucoup pour cette remarque, je m'incline, je ne connaissais pas cet article. En plus, les prises de position répétées de Stéphane Bortzmeyer en faveur du déploiement d'IPsec pourraient favorablement venir contribuer au débat et à la sécurité des échanges.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

L3B0WSKI
le 13 décembre 2011 - 18:54 • SIGNALER UN ABUS - PERMALINK

"The target accepts the fake update message sent"

Mouhahaha ! elle est superbe celle-là ! Ton update tu peux te la rouler et te la…

Plus sérieusement, la plupart des mouchards dont on parle et notament celui découvert par le CCC ciblent Windows. Premiere phrase de leur analyse :

"Die Malware bestand aus einer Windows-DLL ohne exportierte Routinen. Das ist für eine DLL ungewöhnlich; erfahrungsgemäß kommt dies so gut wie aus-schließlich bei Schadsoftware vor."

Alors bon, hein, pas de quoi trop flipper, c'est surtout des gros titres et derrière, finalement, y'a rien. D'ailleurs si vous lisez bien les articles suisses, rien de précis… En effet, développer puis maintenir ce genre d'outil pour toutes les plateformes est quasi

impossible.

De plus un bon live-CD linux, un utilisateur averti et hop ! Tu peux toujours venir avec ton “logiciel espion indétectable de la mort qui tue”.

Restons sérieux siouplait :-)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

DADA

le 13 décembre 2011 - 23:58 • SIGNALER UN ABUS - PERMALINK

Contrairement à ce qu’en dit l3b0wski, il n’y a pas que Windows qui est ciblé, les Apple aussi. Ça fait quelques années que je sais être espionnée depuis mon iMac, mais le dire peut nous faire passer pour parano parce que, aller prouver ça…

Il n’y a aucune possibilité encore pour détecter qui nous espionne et/ou pour neutraliser le cheval ??

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

ZEDE

le 14 décembre 2011 - 10:09 • SIGNALER UN ABUS - PERMALINK

“Skype et BlackBerry, utilisés par des centaines millions de personnes pour se téléphoner, ou échanger des données, dans le monde entier, sont eux aussi un cauchemar pour les espions aux “grandes oreilles“, dans la mesure où, même interceptées, les communications, chiffrées, sont a priori indéchiffrables”

Je veux pas dire mais ça fait un moment que les ministères français ont interdit l’installation et l’utilisation de skype dans leurs services, parce que jugé pas assez sûr.

Sinon bon article

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

MOIALORS

le 14 décembre 2011 - 15:27 • SIGNALER UN ABUS - PERMALINK

Le simple fait de laisser un commentaire ici fait probablement sonner une alarme à quelque part c’est sûr mais bon il ne faut pas laisser les fascistes/nazistes nous terroriser et nous empêcher d’exprimer librement nos opinions. Je ferrai très attention à l’avenir à toutes les mises à jour que je reçois, comme par exemple Java, Flash, produits Apple, et autres addons. Nous sommes certainement nous aussi tous visés par ces chevaux de Troie, que l’on soit en démocratie ou non. J’ai depuis longtemps abandonné le combat pour protéger ma vie privée et mes communications, et ça fait longtemps que je sais que ce genre de pratiques existent, je limite donc au maximum mes échanges sur le net ou par tout autre moyen de communication moderne. Je n’ai pas de portable et j’envoie le moins de email possible. Même si je n’ai rien à cacher, je tiens à la confidentialité de mes communications et c’est pour ça que je ne dis jamais rien d’important ou de personnel dans mes emails. Je les considères comme des cartes postales. Ce n’est malheureusement pas le cas de tout le monde.

Je comprend que c’est possible de crypter toutes nos communications mais ça demande quand même une bonne connaissance technique et du temps à consacrer à notre protection. De plus je crois que si on utilise le chiffrement on fait sonner une alarme dans les bureaux des fascistes/nazistes et on attire inutilement l’attention sur nos communications, même si c’est anodin. C’est mon opinion et je ne critique pas ceux qui le font mais pour moi je trouve que c’est vraiment triste qu’on en soit rendu là. La liberté et la confidentialité de nos communications ne devrait pas être si compliquée à obtenir.

*Pour terminer j’aimerais dire aux fascistes/nazistes que je sais depuis longtemps que vous espionnez nos communications et que vous pouvez aller vous faire f***tre royalement. Un jour vos armes se retourneront contre vous et les gens que vous aimez. Vous n’êtes pas libre et vous n’êtes que des esclaves de vos propres armes. Vous me faites pitié.*

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

LASORCIEREROUGE
le 11 janvier 2012 - 18:39 • SIGNALER UN ABUS - PERMALINK

La démocratie n'existe pas et n'a jamais exicté, il faut dire OLIGARCHIE !

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

6 pings

Articles à relire by romanooo - Pearltrees le 13 décembre 2011 - 9:30

[...] Tous les articles OWNI/Wikileaks sont là Un gros requin de l'instruction et Une journée sous surveillance Retrouvez notre dossier sur le sujet : Photos des chevaux de troie au festival Burning man par Abraxas3d [cc-bync] et Terra Incognita [cc-bync] via Flickr Des chevaux de Troie dans nos démocraties » OWNI, News, Augmented [...]

Vie privée by webqualite - Pearltrees le 13 décembre 2011 - 15:55

[...] Des chevaux de Troie dans nos démocraties » OWNI, News, Augmented Ces dernières années, un quarteron d'entreprises privées a développé des logiciels espions visant à déjouer tous les mécanismes de sécurité ou de chiffrement des communications utilisés par ceux qui cherchent à protéger leurs données, et leur vie privée. Ces logiciels, ce sont des chevaux de Troie. OWNI, en partenariat avec WikiLeaks dans le cadre de la publication des SpyFiles, s'est penché sur les documents se rapportant à ces technologies très particulières. Comme dans la mythologie, un cheval de Troie se fait passer pour ce qu'il n'est pas, permet de prendre le contrôle total de l'ordinateur qu'il infecte, à distance, de sorte de pouvoir y lire les données avant même qu'elles ne soient chiffrées et donc sécurisées, ou encore de pouvoir y activer le micro, ou bien la caméra, et cætera. [...]

Documents by oliviersc - Pearltrees le 13 décembre 2011 - 19:08

[...] Des chevaux de Troie dans nos démocraties » OWNI, News, Augmented [...]

Libertés by olivier93fr - Pearltrees le 16 décembre 2011 - 18:09

[...] Un reportage diffusé dans le magazine Zapp de la chaîne de télévision allemande ARD [en] montre qu'ils ont aussi servi à espionner des défenseurs des droits de l'homme en Egypte. Pire : on y découvre que si le discours officiel des autorités allemandes est de soutenir les défenseurs des libertés de ce "printemps arabe", dans les faits, elles soutiennent également, et activement, l'exportation de ces armes de surveillance, même et y compris à des dictateurs ou des régimes totalitaires où elles sont utilisées pour réprimer la population, au motif qu'il s'agirait d'un "marché du futur". Ces comportements, favorisant le développement de telles technologies intrusives, s'expliquent par l'évolution de nos relations aux télécommunications. Car, signe des temps, si la majeure partie des conversations téléphoniques et des données échangées sur le Net circulent en clair, une partie de plus en plus importante de ces flux d'information sont désormais chiffrés. Des chevaux de Troie dans nos démocraties » OWNI, News, Augmented [...]

Le Petit Monde Cozillon » Des chevaux de Troie dans nos démocraties le 11 janvier 2012 - 22:08

[...] OWNI [...]

Soudain, un espion vous offre une fleur | BUG BROTHER le 7 juin 2012 - 8:49

[...] un logiciel espion. Las : un ami de sa fille, féru de sécurité informatique, trouva le cheval de Troie, et remonta jusqu'à l'ordinateur de l'espion [...]