# LE CYBERESPION RUSSE ESPIONNÉ

*LE 2 NOVEMBRE 2012* ***PIERRE ALONSO***

**Tel est espionné qui croyait cyberespionner. Un pirate, travaillant visiblement pour le gouvernement russe, a été identifié par les autorités géorgiennes, cible de ses attaques depuis mars 2011. Histoire de le faire savoir, la Géorgie a publié les photos du cyberespion.**

C'est une histoire tirée d'un roman d'espionnage, plutôt à la mode OSS 117. Un État fabrique un logiciel espion, le lance sur sa cible, un autre État. Celui-ci s'en rend compte, dissèque ledit logiciel dans le plus grand secret. Il décide ensuite de piéger l'attaquant, y parvient. À la fin, il publie un rapport avec les photos du pirate ennemi, obtenues en entrant dans son ordinateur.

Fin de la fiction. L'histoire est réelle. Le rapport **a été publié** en anglais la semaine dernière par l'agence d'échange de données géorgienne. Il pointe la main de la Russie dans une cyberattaque importante contre la Géorgie découverte en mars 2011. *"Un acte de cyberespionnage"* écrit l'agence dans son rapport qui détaille le *modus operandi* sophistiqué de l'attaque.

## Informations confidentielles

Première étape : des sites d'informations géorgiens sont piratés. Le script malveillant placé sur ces pages infecte les ordinateurs des visiteurs. La pêche aux "informations confidentielles et sensibles" peut commencer. Étape deux : les ordinateurs piratés sont criblés pour dénicher les précieuses informations qui sont renvoyées (c'est l'étape trois) vers un serveur distant. Malins, les artisans de l'attaque changent régulièrement l'adresse du serveur.

Non content d'obtenir ces documents – principalement word, powerpoint et pdf à propos des questions des relations avec les États-Unis ou l'Otan – les pirates peuvent avoir accès aux micros et caméra de l'ordinateur infecté. Des fonctionnalités sophistiquées, mais **pas hors du commun** à en croire **le catalogue** de certains marchands d'armes de surveillance…

390 ordinateurs ont été infectés détaille le rapport de l'agence géorgienne. Une immense majorité en Géorgie, et quelques 5% en Europe et en Amérique du Nord. Les autorités géorgiennes affirment avoir reçu l'aide de services étrangers (américains et allemands) ainsi que

UN JOUR SOUS SURVEILLANCE

**Les documents révélés par WikiLeaks laissent entrevoir le paysage de la**

l'assistance de grandes entreprises comme la division cybersécurité de Microsoft. Une fois disséqué, le logiciel malveillant a permis de remonter à la source. Les autorités géorgiennes sont parvenues à identifier le pirate, et le prendre en photo avec sa webcam.

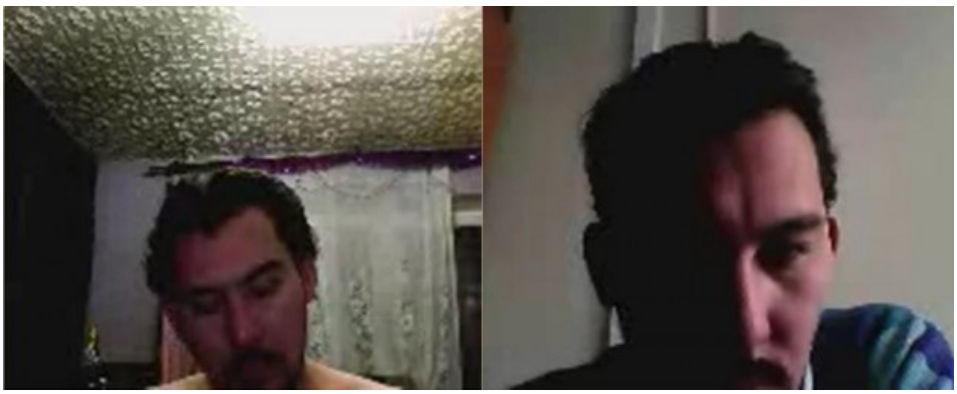
**surveillance. Un téléphone portable devient un ...**

## La moustache de Moscou

Pas peu fière, l'organisation chargée de la cybersécurité géorgienne raconte :

> ***Nous avons trouvé un PC infecté dans notre lab, avons envoyé une fausse archive ZIP, intitulée "Georgian-Nato agreement', qui contenait le virus. L'attaquant a dérobé cette archive et a exécuté le fichier malveillant. Nous avons maintenu le contrôle sur son PC, puis capturé une vidéo de lui, personnellement.***

La prise est évidemment jointe au dossier : deux photos d'un homme moustachu, sans uniforme, dans ce qui ressemble à un appartement.



Pour la Géorgie, l'origine de l'attaque ne fait aucun doute : Moscou est derrière. Ce ne serait pas une première. Lors de la guerre entre les deux pays à l'été 2008, le Russie **avait mené** des cyberattaques concomitamment aux attaques sur le terrain. Le rapport ne manque pas de le rappeler, citant *"deux organisations indépendantes américaines"*. Les cyberattaquants avaient alors pu compter sur *"certaines ressources"* appartenant à l'Institut de recherche du ministère de la défense russe.

---

Illustration par **Alvaro Tapia Hidalgo** [CC-byncnd]
Photos tirées du rapport [PDF] **Cyber Espionnage against Georgian government** (DR)

**CORRECTOR**
*le 2 novembre 2012 - 22:36* • SIGNALER UN ABUS - PERMALINK

*Ne pas penser à occulter sa Webcam, quand on fait soi-même de l'espionnage, comment dire?…*

VOUS AIMEZ 1 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

**PIERRE ALONSO**
*le 3 novembre 2012 - 15:59* • SIGNALER UN ABUS - PERMALINK

*Re-bonjour Corrector,*

*J'ai également été surpris par ce qui ressemble à une erreur grossière. Peut-être que info@dea.gov.ge pourrait apporter des précisions ?*

*Cordialement,*

*PA*

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

**CORRECTOR**

*le 3 novembre 2012 - 16:22* • SIGNALER UN ABUS - PERMALINK

*Attention, je ne veux surtout pas dire que cette histoire est bidon pour autant :*
*- les bourdes arrivent, c'est comme ça que les criminels "prudents" se font prendre, en faisant une seule petite erreur*
*- et même dans les services secrets (il y a des exemples!)*
*- n'importe quel ahuri peut avoir été commandité pour lancer cette opération depuis son appartement soviétique, même s'il était interrogé il ne connait pas forcément l'identité du commanditaire*

*Je suis assez peu adepte des théories de complot : ce n'est pas parce que c'est gros que c'est faux.*

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE