Quelques précisions au sujet du keylogger installé sur mon ordinateur

Quelques précisions au sujet du keylogger installé sur mon ordinateur

Texte d'origine en italien

Alcune precisazioni riguardo al Key-logger installato sul mio computer

2018

anarhija.info/library/radioazione-italia-alcune-precisazioni-riguardo-al-key-logger-installato-sul-mio-computer-it

Traduction française

attaque.noblogs.org/post/2018/10/11/operation-scripta-manent-quelques-precisions-au-sujet-du-keylogger-installe-sur-mon-ordinateur

Mise en page

No Trace Project

notrace.how/resources/fr/#quelques-precisions

Ces derniers jours, en lisant le compte-rendu des audiences[1] du procès qui nous voit inculpés pour l'enquête « Scripta Manent »[2], orchestrée par le procureur de Turin Roberto Sparagna, j'ai[4] remarqué une explication concernant le keylogger, un logiciel enregistreur de frappe (ou Agent Elena[5], comme l'appelaient les misérables Carabinieri du ROS[6] de Naples).

Dans ce texte, paru sur des sites Internet, on dit que le keylogger aurait servi pour capter les commentaires « hors antenne » lors des directs radio de RadioAzione.

Ça aurait été bien si c'était le cas, mais malheureusement la réalité est différente.

Ce keylogger était un vrai mouchard, envoyé via Internet à mon ordinateur, sous forme d'un virus, et capable de capter tout ce qui se passait autour de l'ordi.

Il suffisait que l'ordinateur soit connecté à Internet et les misérables flics pouvaient écouter tout l'environnement sonore dans le lieu (mais pas d'images, car la webcam a toujours été occultée).

L'ordi étant dans la chambre, ils n'ont pas seulement écouté les commentaires hors antenne, mais aussi d'autres choses… tout !

En plus, le logiciel a été utilisé pour prendre des captures d'écran de mon ordi pendant que j'écrivais des textes ou que je traduisais ceux d'autres compagnons, des textes publiés par la suite sur le site de RadioAzione.

---

[1] https://anarhija.info/library/italia-resoconto-udienze-processo-scripta-manent-aprile-luglio-it

[2] *Note du No Trace Project (NdNTP) :* Vous pouvez trouver plus d'informations sur l'opération répressive italienne « Scripta Manent » ici[3].

[3] https://notrace.how/threat-library/repressive-operations/scripta-manent.html

[4] *NdNTP :* L'auteurice de ce texte était membre de la radio anarchiste italienne *RadioAzione*. Dans le cadre d'une enquête contre cette radio, un logiciel malveillant (appelé « keylogger » dans ce texte) a été installé sur l'ordinateur de l'auteurice.

[5] *NdNTP :* Le logiciel malveillant était un logiciel appelé « Enhanced Law Enforcement Neotronic Agent » (ELANA, « Agent Neotronic amélioré pour le maintien de l'ordre »), commercialisé par l'entreprise italienne Neotronic.

[6] *NdNTP :* Le *Raggruppamento Operativo Speciale* (ROS) est une agence de maintien de l'ordre italienne.

Tout cela pendant six ans, même si j'ai formaté l'ordinateur plusieurs fois entre-temps[7].

J'ai pensé qu'il était important de faire cette précision parce que comme cela avait été écrit dans le texte sur les audiences, il pouvait y avoir de incompréhensions. On peut tous avoir un keylogger dans l'ordi (même si ça leur coûte 120 euros par jour… s'ils n'ont pas triché avec les factures versées au dossier) et c'est donc mieux d'expliquer comment ça marche.

Mon conseil pour ceux qui pensent en avoir un d'installé sur leur ordi est donc de l'éteindre si on n'est pas en train de l'utiliser et d'éviter de parler dans la pièce où il est allumé.

J'avais connecté un micro externe qui allait dans une console de mixage et j'ai erronément pensé qu'en le mettant en position « muet » il n'aurait pas capté le son, mais cela n'a servi a rien. Avec le keylogger, les flics pouvaient activer le micro interne à l'ordi.

[7] *NdNTP :* Un autre texte[8] donne plus de détails sur le logiciel malveillant :

> « Le système d'exploitation de l'ordinateur infecté par le logiciel de surveillance était Windows. Le logiciel a été installé à distance par Internet. Il est resté sur l'ordinateur pendant quatre ans. Lorsque l'ordinateur était ré-installé/formatté, le logiciel de surveillance était de nouveau installé à distance par Internet. Apparemment, le logiciel avait besoin d'une connexion à Internet constante pour espionner et pour envoyer les informations collectées. Il n'était pas capable de sauvegarder des données localement pour les envoyer plus tard. Le logiciel était capable d'enregistrer le texte tapé sur le clavier, de prendre régulièrement des captures d'écran, et, selon les mesures de protection présentes sur l'ordinateur, d'enregistrer les communications entrantes et sortantes (pages web visitées, etc). L'existence du logiciel a été découverte grâce à des fichiers d'enquête. »

[8] https://earsandeyes.noblogs.org/fr/post/2019/01/27/encore-des-precisions-keylogger-italie

Il faut se rappeler de débrancher l'ordinateur d'Internet avant d'écrire ou de traduire un texte[9].

[9] *NdNTP :* Ceci n'est pas un bon conseil, car certains logiciels malveillents peuvent enregistrer localement des données quand Internet est désactivé, puis transmettre les données enregistrées quand Internet est activé de nouveau. Pour se protéger face au risque de logiciels malveillants, nous recommandons d'adopter de bonnes pratiques numériques[10].

[10] https://notrace.how/threat-library/mitigations/digital-best-practices.html

Ce keylogger était un vrai mouchard, envoyé via Internet à mon ordinateur, sous forme d'un virus, et capable de capter tout ce qui se passait autour de l'ordi. Il suffisait que l'ordinateur soit connecté à Internet et les misérables flics pouvaient écouter tout l'environnement sonore dans le lieu (mais pas d'images, car la webcam a toujours été bouchée). L'ordi étant dans la chambre, ils n'ont pas seulement écouté les commentaires hors antenne, mais aussi d'autres choses… tout !

No Trace Project / Pas de trace, pas de procès. Un ensemble d'outils pour aider les anarchistes et autres rebelles à **comprendre** les capacités de leurs ennemis, **saper** les efforts de surveillance, et au final **agir** sans se faire attraper.

Selon votre contexte, la possession de certains documents peut être criminalisée ou attirer une attention indésirable—faites attention aux brochures que vous imprimez et à l'endroit où vous les conservez.