DFIR ORC : l'Anssi bascule en open source son outil forensique

« *N'oublions pas non plus les félicitations aux développeurs d'origine d'ORC* ».

Stéphane Lenco a posté ce commentaire sur la page LinkedIn de l'Anssi.

Le CISO du groupe Thales fait écho à l'ouverture, sous licence GPL, dudit ORC.

> *#DFIRORC : un logiciel de collecte de données forensiques, créé et utilisé par l'ANSSI pour l'investigation et la réponse à incident à grande échelle :*
> *https://t.co/X3w12eSPCg*
>
> *Découvrez ce nouvel outil #opensource et contribuez à son développement ! #DFIR #Digital #Forensics pic.twitter.com/YnO2XnFpE9*
>
> *— ANSSI (@ANSSI_FR) September 23, 2019*

Conçu en 2011, le logiciel est destiné à la collecte de données forensiques sur les systèmes Windows. L'Anssi dit l'avoir utilisé sur « plus de 150 000 postes » dans le cadre de ses missions d'investigation et de réponse à incident.

ORC comprend, en standard, une dizaine d'outils pour la recherche, l'extraction et la mise à disposition de données*. Son architecture *framework* permet d'en élargir les capacités tout en conservant un seul exécutable.

La prise en charge des OS Microsoft démarre à partir de Windows XP SP2 et Windows Server 2003 SP3.

** FastFind pour détecter la présence d'indicateurs de compromission, GetThis pour collecte des informations sur le système de fichiers, NTFSUtil pour inspecter la table d'allocation…*

Photo d'illustration © École polytechnique / Paris / France via *Visualhunt / CC BY-SA*