COMMUNIQUÉ DE PRESSE
Paris, le 23 septembre 2019

L'ANSSI présente DFIR ORC : un outil de collecte libre pour l'analyse forensique

Conçu en 2011 pour répondre aux missions opérationnelles de l'ANSSI en matière d'investigation et de réponse à incident, le logiciel DFIR ORC (pour Outil de recherche de compromission) n'a cessé d'évoluer pour regrouper un ensemble d'outils qui permettent la recherche, l'extraction et la mise à disposition de données forensiques dans un environnement Microsoft Windows… à l'échelle d'un parc entier ! L'outil, intégralement libre, est aujourd'hui publié par l'agence à l'usage des acteurs et des professionnels de la communauté.

DFIR ORC : UN LOGICIEL DE COLLECTE DE DONNEES FORENSIQUES EPROUVE

Pour faire face à des incidents d'un genre nouveau, les « Advanced Persistent Threats » (APTs), apparus il y a près de 10 ans, l'ANSSI a dû adapter sa méthodologie de traitement ainsi que son outillage. DFIR ORC est directement issu de cette démarche et n'a cessé de se développer depuis pour s'adapter aux besoins en matière d'investigation et de réponse à incident.

Créé et utilisé de longue date par les équipes de l'ANSSI, le logiciel de collecte DFIR ORC regroupe un ensemble d'outils qui permettent la recherche, l'extraction et la mise à disposition des données forensiques. Il a été entièrement conçu afin de fonctionner dans l'écosystème Microsoft Windows de façon décentralisée et à grande échelle.

« Après 8 ans d'usage, DFIR ORC a été utilisé sur plus de 150 000 postes dans le cadre de nos activités opérationnelles en matière de réponse à incident. » indique François Deruty, sous-directeur Opérations de l'ANSSI.

En s'engageant dans une démarche d'ouverture avec la communauté de la sécurité numérique, l'ANSSI souhaite aujourd'hui partager cet outil mature qu'elle utilise au quotidien depuis plusieurs années*. [https://dfir-orc.github.io]

DFIR ORC – POUR QUI ? POUR QUOI ?

DFIR ORC s'adresse aux professionnels de la sécurité informatique soucieux d'acquérir les données nécessaires à la réponse aux incidents de sécurité de façon fiable, ainsi qu'à tous les développeurs qui souhaiteront s'en inspirer ou contribuer à son développement.

DFIR ORC peut être déployé sur l'intégralité d'un parc Microsoft Windows, tout en minimisant l'impact sur son fonctionnement normal. Il assure ainsi la collecte des informations souhaitées avec une exigence de fiabilité, de

qualité et de traçabilité, sans modifier la configuration des machines analysées, tout en minimisant les risques d'altérations des données collectées.

Par son usage, DFIR ORC permet donc de disposer d'une vision de l'état du parc au moment de la collecte. Il ne vise cependant pas à pratiquer une analyse sur les données collectées : c'est le rôle de spécialistes disposant d'une méthodologie et d'outils adaptés.

CONTRIBUEZ AU DEVELOPPEMENT DE DFIR ORC

DFIR ORC est un outil modulaire, configurable, qui peut embarquer d'autres outils, notamment ceux qui sont déjà proposés par l'agence.

Avec la publication de DFIR ORC, l'ANSSI partage le code source, la procédure de compilation ainsi que des exemples de configuration de l'outil. Tous ces éléments permettent la génération d'un outil fonctionnel adapté à l'usage souhaité.

« À travers DFIR ORC, nous avons l'ambition de contribuer activement à la vie de la communauté de la réponse à incident, en lui permettant de s'approprier et de développer l'outil à sa manière », ajoute François Deruty.

L'ANSSI souhaite encourager l'émergence d'une communauté publique de développeurs et d'utilisateurs de l'outil, pour favoriser sa montée en maturité et l'apparition de nouvelles fonctionnalités. L'agence continuera de même à développer DFIR ORC, et publiera régulièrement des mises à jour de l'outil.

L'agence invite tous les acteurs de la communauté à enrichir dès à présent ce projet avec nos équipes.

*Publication sous licence LGPL 2.1+

À PROPOS DE L'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n°2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale.

L'agence assure la mission d'autorité nationale en matière de défense et sécurité des systèmes d'information. Elle est rattachée au secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP

www.ssi.gouv.fr - communication@ssi.gouv.fr

CONTACTS PRESSE

Margaux Vincent
margaux.vincent@ssi.gouv.fr
01 71 75 84 04

Bureau relations presse
communication@ssi.gouv.fr