PRESS RELEASE
Paris, 23 September 2019

The French National Cybersecurity Agency presents DFIR ORC : an open-source forensics tool dedicated to artefact collection

Created in 2011 to address operational needs of incident responders at ANSSI, DFIR ORC is a modular framework to collect forensic artefacts on machines running a Microsoft Windows operating system.

DFIR ORC, A RELIABLE AND SCALABLE ASSET FOR INCIDENT RESPONDERS

In the last decade, the DFIR community has had to deal with ever-growing installed bases and address Advanced Persistent Threats. In an effort to face these challenges, ANSSI has reviewed its investigation methodology and developed suitable tooling. DFIR ORC is a direct result of this change in paradigm.

DFIR ORC, where ORC stands for "Outil de Recherche de Compromission" in French, is a set of specialized tools dedicated to the reliable parsing and collection of critical forensic artefacts. Designed to scale up, it gathers data in a decentralized manner. It is meant to be used easily in the Microsoft Windows ecosystem, and to have low impact on production environments.

« Incident responders have used DFIR ORC successfully on more than 150K machines to fulfill their operational missions.» François Deruty, ANSSI's Deputy Director of Operations said.

ANSSI wants to contribute to the digital security community. This is why the DFIR ORC framework [https://dfir-orc.github.io], resulting from 8 years of active development, is now open-sourced*.

WHO CAN USE DFIR ORC ? WHAT DOES IT DO ?

DFIR ORC is meant to be used by computer security professionals to collect forensically relevant data without altering them. It can also inspire security developers and analysts, who can contribute to the project.

Meant to scale up for use on large installed bases, DFIR ORC also supports fine-tuning to suit specific forensics use-cases as well as information system particularities. DFIR ORC collects data, but does not analyze it: it is not meant to triage machines. It rather provides a forensically relevant snapshot of machines running Microsoft Windows, which expert analysts then have to examine.

CONTRIBUTE TO DFIR ORC

DFIR ORC is a modular framework which requires configuration. It can embed tools amongst those proposed, as well as external tools.

ANSSI releases the source code of the framework and documents its compilation process, which only requires free software. Moreover, examples of relevant configurations are provided, allowing users to build their own customized version of the tool.

"Through the DFIR ORC, we aspire to contribute actively to the DFIR community, by providing it the chance to appropriate and develop the tool. », François Deruty added.

The DFIR ORC framework developers at ANSSI hope that a community of users and developers will emerge following this release. This can only result in a better and more suitable tool. Software updates will be released in the future, as developers keep working on the tool internally.

ANSSI invites the DFIR community to take part in the evolution of this framework.

*licence LGPL 2.1+

ABOUT ANSSI

ANSSI is the national authority in the area of cyberdefence and network and information security.

To fulfil its missions, ANSSI deploys a broad range of regulatory and operational activities, from issuing regulations and verifying their application, to monitoring, alert and rapid response – particularly on government networks.

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

PRESS CONTACT

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

Press service
communication@ssi.gouv.fr