



# SCReeD Dataset Declaration Form

Dataset name:\* Ransomware Data

Dataset version:\* 1.0

Dataset URL:\* <https://github.com/CSCRC-SCREED/CSU-Ransomware-Data>

Creation date:\* 25/9/2024

Last update:\* 13/11/2024

Author(s):\* Jamil Ispahany, Islam MD Rafiquel, Oscar Blessed Deho

Author(s) affiliation(s): Charles Sturt University (CSU), Cyber Security Cooperative Research Centre (CSCRC)

Author contact(s):\* JIspahany@csu.edu.au, mislam@csu.edu.au, odeho@csu.edu.au

Keywords:\* Sysmon, Ransomware, Ransomware detection, Ransomware attacks, Malware

Description/background:\* This dataset contains Sysmon events which have been generated from running ransomware and goodware on a Windows 11 virtual machine. The intention for the dataset is to be used for training machine learning algorithms for classification.

Dataset funding: CSCRC

Attribute details:\* File\_created, File\_Delete\_archived, File\_creation\_time\_changed, Registry\_value\_set, Process\_Create, Pipe\_Created, process-related, network-related, file-related, suspicious\_path, system\_executable, path\_length, directory\_depth, process\_vs\_parent\_freq\_ratio, process\_name\_length, executable\_depth\_diff, parent\_is\_system\_executable, extension\_similarity, file\_name\_entropy, Ware Type

Intended target (if specified): [Click or tap here to enter text.](#)

Format:\* CSV

License:\* Open

Standard compliance: [Click or tap here to enter text.](#)

Type:\* Numerical and Categorical

Size:\* 25MB

Availability: Click or tap here to enter text.

Data status: Click or tap here to enter text.

Data provenance:\* Ransomware activity was captured by detonating ransomware samples on an isolated virtual machine, while goodware activity was recorded by performing typical, non-malicious day-to-day tasks. Sysmon was employed to monitor suspicious behavior and forward the generated events to a central logging server for analysis.Click or tap here to enter text.

Source computing infrastructure :\* Simulated environment

Accompanying program(s)/script(s): Click or tap here to enter text.

Software installer or VM for replication: Virtual machine

Generated or captured via :\* Experiment

Category/categories :\* Event log

Published in: Click or tap here to enter text.

Open research question(s) (if any): Click or tap here to enter text.

Potential use case(s) or application area(s): Machine learning training / testing

Data access control :\* Global access

Data retention period:\* Permanent

Data validation/checksum:\* CSU Team

GDPR compliance:\* Yes

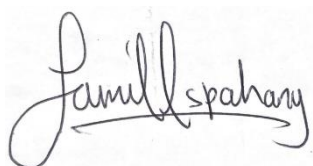
Consent: Click or tap here to enter text.

Ethics approval: N/A

Ethics considerations: N/A

*\* denotes mandatory field*

- ☒ I confirm that I have read, understood, and agreed to the submission guidelines, policies, and submission declaration.
- ☒ I confirm that the contributors of the dataset have no conflict of interest to declare.
- ☒ I agree to take public responsibility for my dataset's contents.

A handwritten signature in black ink, reading "Jamil Spahary". The signature is fluid and cursive, with a horizontal line underlining the name.

Signature of Corresponding Author (sign here)

Date: 13/11/2024

(signed on behalf of all contributors)