Data in Brief, vol.61, pp.111723-1-111723-9, August, 2025.

COMISET: Dataset for the analysis of malicious events in Windows systems

A. Pérez Sánchez; G. López López; R. Palacios Hielscher

Abstract-

The evaluation of threat detection and prevention systems requires the use of datasets that are up-to-date and correctly designed according to the most common threats. Currently, the availability of event datasets containing sufficient information to perform these analyses on Microsoft Windows systems is practically non-existent. In the background section we summarize the existing datasets, highlighting their main limitations to conduct studies of threat detection. Following we present COMISET, the dataset we have generated through the collection of events in real time and updated according to the current threats and malware obfuscation techniques. The main advantage of using this dataset with respect to those already available is that it was developed specifically for the evaluation of threat detection and prevention systems, and the events were labelled according to techniques and tactics of the MITRE ATT&amp;CK matrix. COMISET is freely available for research purposes and contains about 250 million events of both malicious and non-malicious types. To create the dataset the experiments have been performed in two different scenarios: a laboratory emulating the infrastructure of a small company, and a computer network commonly used by students at Comillas University. In the laboratory environment, real attacks were executed involving a variety of techniques and tactics commonly used by the adversaries. The monitoring system was able to capture the events and label them according to the MITRE ATT&amp;CK matrix. Some of these events are shown in this paper as an example of the worthy information contained in the dataset.&nbsp;

Index Terms- Event-based threat detection; MITRE ATT&CK; Cyber kill chain; Advanced persistent threats

Citation:

López, G.; Palacios, R.; Pérez-Sánchez, A. "COMISET: Dataset for the analysis of malicious events in Windows systems", Data in Brief, vol.61, pp.111723-1-111723-9, August, 2025.