I. Background

1. Purpose

The purpose of this standard is to set a consistent manner in which malware bits or Indicators of Compromise (IOC) are reported to the general public.

2. Why

Between Anti-Virus vendor virus descriptions, malware analysis done by researchers, InfoSec professionals reporting what they found and Advanced Persistent Threats (APT) reports, data from these sources is inconsistently reported making it difficult to consume for IT and Information Security professionals.

3. Goal

The goal of this proposal is to provide guidance to malware researchers, anti-virus companies, consultancies and software developers to encourage reporting of malware bits that we can all use, regardless of the tool(s) we might use.

4. Want to Help

Anyone wishing to contribute to this proposed standard can contact us and provide feedback and input.

https://malwarearchaeology.com/contact

II. Overview:

This standard is to provide the needed data and order in which to record information about malware for reporting to the public for use by information technology and information security professionals.

III. Format:

The format of the output should be provided in one or more of the following formats:

1. Comma Separated Values (CSV)
2. Extended Markup Language (XML)
3. Standard Text Report

Tools that utilize data feeds or input (e.g. CIF, MIR) may consume the data format(s) provided by this standard.

IV. STANDARD:

The following is information that is to be provided in the output of malware research and/or analysis for consumption by tool(s), script(s) or reported to the public.

PARAMETER NAME	DESCRIPTION
Description	Short description of malware (e.g. WinNTI or virus name)
Filename	The full name of the file
Extension of file	The extension of the file
Location/Directory	Location file is placed by the malware if known
MD5	MD5 Hash(es) of the file(s)
SHA1	SHA1 Hash(es) of the file(s)
SHA256	SHA256 Hash(es) of the file(s)
SHA3	SHA3 Hash(es) of the file(s)
Digital Signature	Digital signature of any certificates used in, or by the malware
Registry	Hive and Key(s) used by the malware (Windows only)
IP Address(es)	List of IP's used by the malware
URL(s)	List of URL's used by the malware
Domain(s)	List of domain(s) used by the malware for C&C or other use
Port(s)	List of port(s) used by the malware

PARAMETER NAME	DESCRIPTION
Assessment	Per CIF – CIF Assessment description
Confidence	Per CIF – CIF confidence rating
Severity	Per CIF – CIF severity rating

Additional research/analysis information may be before or after the standardized data as the order of where the standardized data exists does not matter, just that it exists.

More Information:

- The Collective-Intelligence-Framework (CIF)
  - **https://code.google.com/p/collective-intelligence-framework/**
- OpenIOC
  - **http://www.openioc.org/**

Revisions

This Standard will be periodically modified in accordance with industry feedback and changes in the Malware Management Framework details.

Revision	Date	Description
DRAFT	07/01/2013	Initial Draft