Cybersecurity
Progress. Protected.

SAMPLE SUBMISSION REPORT

ESET Threat Intelligence Investigation Lab

(eset):research

SAMPLE REPORT

CLIENT	**Demo**
REPORT DATE	2023-10-11 13:40:47 UTC
REPORT ID	F9E3BBB2-686E-47F5-98BF-4CBAA7D6FB33/2023

File details

NAME	Sample_report___.zip
TYPE	Zip archive data, at least v1.0 to extract
SIZE	184 B
MD5	6CE6F415D8475545BE5BA114F208B0FF
SHA1	D27265074C9EAC2E2122ED69294DBC4D7CCE9141
SHA256	2546DCFFC5AD854D4DDC64FBF056871CD5A00F2471CB7A5BFD4AC23B6E9EEDAD
SSDEEP	3:vh9NeYh/CTpA/cAJraNvsgzsVqSwHqXzj9//9eYh/F/aHEpIh/+lIl//:59sYMTpDAJuOgzskozj9sY//zpW+lIt/
SIGNATURE	Unsigned

Detection

VENDOR	LAST UPDATE	DETECTION
ESET	Wed Oct 11 10:54:59 2023 UTC	Eicar test file

ESET LiveGrid®

COUNT	10 000 to 100 000
FIRST SEEN	2000-07-11
LAST SEEN	2023-10-11

Countries

Romania	1 000 to 10 000
Czech Republic	100 to 1 000
Slovakia	100 to 1 000
United Kingdom	100 to 1 000
Japan	100 to 1 000

Sample seen in URLs

IP ADDRESS	URL
13.230.77.110	https://strage[dot]ec-masters[dot]net/file>[dot]php?h=1e4729a0795a597b7942721dfb44a00>7[dot]zip&force=true
91.212.136.200	https://www[dot]ikarussecurity[dot]com/wp->content/downloads/eicar_com[dot]zip
89.238.73.97	https://secure[dot]eicar[dot]org/eicar_com>[dot]zip
89.238.73.97	https://www[dot]eicar[dot]org/download/eic>ar_com[dot]zip
91.189.91.81	http://archive[dot]ubuntu[dot]com/ubuntu/p>ool/universe/r/rspamd/rspamd_2[dot]7[dot]o>rig[dot]tar[dot]xz
5.28.62.61	https://scan[dot]cyberessentials[dot]site/>usersc/testfiles/eicar/eicar_com[dot]zip
13.230.77.110	https://strage[dot]ec-masters[dot]net/file>[dot]php?h=701b1500778b64cc438d51bc5dc30da>d[dot]zip
31.172.183.10	https://test[dot]vfml[dot]pl/$J@5YgwQEgGxO>gAZCYCxhc48EDxoLHcot9hPEEoJHfd82aTLUa6s4L->p2g
174.127.110.249	http://kingofgng[dot]com/media/eicar_com[d>ot]zip

Known filenames

eicar_com.zip

sample.zip

Similar file extracts

MALICIOUS EXTRACTS	FIRST SEEN	COUNT	SIMILARITY	SHA1
Eicar test file eicar.com	2011-08-24	10 to 100	100%	CF8BD9DFDDFF007F75ADF4C2BE48005CEA317C62

Explanations

If some of the following sections are not in the report then it means that those sections are empty.

YARA

Contains a list of all matched YARA strings.

If the sample is analyzed by Botnet Tracker, this part will also contain a list of all its C&C servers.

File details

Contains static information about the file. If the file is portable executable file, then also contains **PE Information**.

Detection

Scan results are added only if they are known at the time of generating the report.

Only for ESET scan result:

YELLOW	Potentially Unwanted/Unsafe Application (PUA) detected
RED	malware threat detected (non-PUA)

On top of that, if the link anywhere in the report is RED, **it is always blocked** by ESET.

Sandbox detections	Contains detections of samples executed in sandbox environment. YELLOW = Potentially Unwanted/Unsafe Application (PUA) detected RED = malware threat detected (non-PUA) In sandbox, the file is executed and the product of this execution are samples from: memory = binary sequence found in memory file = new or changed file found in filesystem
Network detections	List of all detections found in network traffic. Samples are executed in isolated network. The stats show the number of detected packets.
Machine Learning Prediction	Contains prediction based on ESET machine learning model. Predictions are available for unpacked executable binaries. If the sample is archived or packed, the sample is automatically unpacked and subsequently samples are analyzed by the machine learning model. All the files machine learning model is able to analyze are shown. YELLOW = the highest likelihood is that the file is Potentially Unwanted/Unsafe application (PUA) RED = the highest likelihood is that the file is Malware threat NOTE: If the detection is shown, it does not automatically mean that the file is malware/PUA. Further investigation is advised.

ESET LiveGrid®

Contains aggregated information from all our clients who are connected to ESET LiveGrid. Information changes over time, so the result can differ between reports with different reporting dates.

COUNT	How many times this file was seen (each client is counted only once): YELLOW = medium number (100 - 1,000) RED = high number (more than 1,000)
FIRST SEEN	When the file was first seen.

LAST SEEN	When the file was last seen.
COUNTRIES	How often the file was seen in each country over the last year.
SEEN IN URLS	List of URLs where the file was seen/downloaded. Very similar URLs are omitted and a maximum of 50 URLs are listed.
THREAT ALSO FOUND IN THESE URLS	URLs where we have seen files with the same detection (can be for a different file)
SAME DOMAIN MALICIOUS URLS	URLs where we have seen malware, if this was from the same domain listed in "Seen in URL". Includes the detection name for that malware
PARENT EXECUTABLES	List of all known parent processes under which the file was executed. For example, if the file was downloaded and executed during browsing, then the parent process is usually a web browser
KNOWN FILENAMES	Other known filenames of the sample.

Similar files

Contains lists of files or extracts of files detected by ESET, which are according to DNA signature**similar to the original file**.

Only files that are more than 70% similar are displayed, and only the 10 most similar files from each list are displayed.

The lists of infected files also contain the detection names. The lists of clean files also contain the source of the software (if available).

MALICIOUS FILES	Shows malicious files or extracts of malicious files.
CLEAN FILES	Shows clean files or extracts of clean files.

YELLOW	more than 80% similarity
RED	more than 90% similarity

[*] indicates that the matched file is an extract from the file detected by ESET. For example, it can be memory dump which is not shared. That means that the similarity is not calculated to the shown file, but to part/extract of this file. This information may be useful in case the analysed file is 100% similar to a memory dump of another file. However, it can be also misleading, if extracts of uploaded file are similar to extracts of many other files.

NOTE: If the detection is shown, it does not mean automatically that the file is malware/PUA. Further investigation is advised.

Similar file extracts

Contains lists of files or extracts of files detected by ESET, which are according to DNA signature**similar to the extracts of original file**.

Only files that are more than 70% similar are displayed, and only the 10 most similar files from each list are displayed.

The lists of infected files also contain the detection names. The lists of clean files also contain the source of the software (if available).

MALICIOUS FILES	Shows malicious files or extracts of malicious files.
CLEAN FILES	Shows clean files or extracts of clean files.

YELLOW	more than 80% similarity
RED	more than 90% similarity

[*] indicates that the matched file is an extract from the file detected by ESET. For example, it can be memory dump which is not shared. That means that the similarity is not calculated to the shown file, but to part/extract of this file. This information may be useful in case the analysed file is 100% similar to a memory dump of another file. However, it can be also misleading, if extracts of uploaded file are similar to extracts of many other files.

NOTE: If the detection is shown, it does not mean automatically that the file is malware/PUA. Further investigation is advised.

Similar behavior

Shows the most similar malicious file and the most similar clean file. Similarity is calculated based on behavior of file in ESET sandbox. This model works differently from the one in "Machine Learning Prediction" section.

Malicious file is marked as RED if the sample would be detected by propietary ESET machine learning prediction model for automated behavioral evaluation.

NOTE: If the detection is shown, it does not mean automatically that the file is malware/PUA. Further investigation is advised.

Sandbox

The file is executed in an ESET sandbox, which records all relevant actions and changes.

MBR & VBR	Master Boot Record & Volume Boot Record: Information whether either has been changed. RED = boot record changed
FILE SYSTEM CHANGES	List of files which were added, changed or removed. YELLOW = PUA changed RED = non-PUA threat changed
REGISTRY CHANGES	List of registry keys which were added, changed or removed.
NETWORK	List of all HTTP and DNS requests and emails sent. (These are not real-world communications, since the sample is executed in an isolated network.)
PROCESSES	List of all creations and terminations of the main process and its sub-processes.

Related files

You can download all relevant files related to this report directly from web portal. Files are packed into one zip archive with password "infected". There can be:

file	Reported file
activity.xml	Detailed informations from sandbox.
screen*	Screenshots from sandbox.
tcpdump.pcap	Raw dump of whole TCP communication from sandbox. (can be viewed by Wireshark for example)
bin_config	Malicious configuration downloaded and decrypted by Botnet Tracker.
config	Malicious configuration downloaded, decrypted and parsed by Botnet Tracker.
c2	List of C & C servers from Botnet Tracker.
targets	List of targets from Botnet Tracker.