ESET Threat Intelligence

User guide

[Click here to display the online version of this document]

Digital Security
Progress. Protected.

ESET Threat Intelligence was developed by ESET, spol. s r.o.

For more information visit https://www.eset.com.

Technical Support: https://support.eset.com

REV. 4/12/2024

About help

This guide was written to help you get familiar with ESET Threat Intelligence and provides instructions to use it.

For consistency and to help prevent confusion, the terminology used throughout this guide is based on the ESET Threat Intelligence parameter names. We also use a set of symbols to highlight topics of specific interest or significance.

> ℹ Notes can provide valuable information, such as specific features or a link to a related topic.

> ! This requires your attention and it should not be skipped. Usually, it provides non-critical but significant information.

> ⚠ Critical information you should treat with increased caution. Warnings are placed specifically to deter you from committing potentially harmful mistakes. Please read and understand text placed in warning brackets, as it references highly sensitive system settings or something risky.

> ✓ Example scenario that describes a user case relevant for the topic where it is included. Examples are used to explain more complicated topics.

Convention	Meaning
Bold type	Names of interface items such as boxes and option buttons.
Italic type	Placeholders for information you provide. For example, filename or path means you type the actual path or a name of file.
`Courier New`	Code samples or commands.
Hyperlink	Provides quick and easy access to cross-referenced topics or external web location. Hyperlinks are highlighted in blue and may be underlined.
%ProgramFiles%	The Windows system directory which stores installed programs of Windows and others.

- Online Help is the primary source of help content. The latest version of Online Help will automatically be displayed when you have a working internet connection.
- Topics in this guide are divided into several chapters and sub-chapters. You can find relevant information by using the search field at the top.
- The ESET Knowledgebase contains answers to the most frequently asked questions, as well as recommended solutions for various issues. Regularly updated by ESET technical specialists, the Knowledgebase is the most powerful tool for resolving various types of problems.
- The ESET Forum provides ESET users with an easy way to get help and to help others. You can post any problem or question related to your ESET products

Introduction

ESET Threat Intelligence (ETI) provides evidence-based information and actionable advice about an existing or emerging threat. ETI services warn you about malicious software or activity that might threaten your organization or its customers. This information is analyzed and presented in a structured manner to help inform decisions about your security policy. ETI does not require ESET endpoint or server solutions to be deployed on your network to provide information, it can be used by non-ESET customers as an additional layer of security to inform you of threats your existing security vendor may not be aware.

ESET Threat Intelligence Portal

The ESET Threat Intelligence Portal provides the following functionality based on the service level of your subscription:

- **Automatic Sample Analysis** (see Sample reports) - Receive automatically generated reports from a manually uploaded file or SHA1 hash
- **Early Warning** (see Reports) - Get reports and updates based on your custom rules any time that a targeted botnet attack or phishing attack occurs. Receive global weekly reports on tracked malware/botnets.
- **APT Reports** (see APT Reports) - Regular reports on Advanced Persistent Threats.
- **Data Feeds** (see TAXII feeds) - Data Feeds designed to integrate with your existing Security Information and Event Management (SIEM) systems.
- **MSSP functionality** (YARA, API)

The portal works best in the following web browsers: Google Chrome, Mozilla Firefox

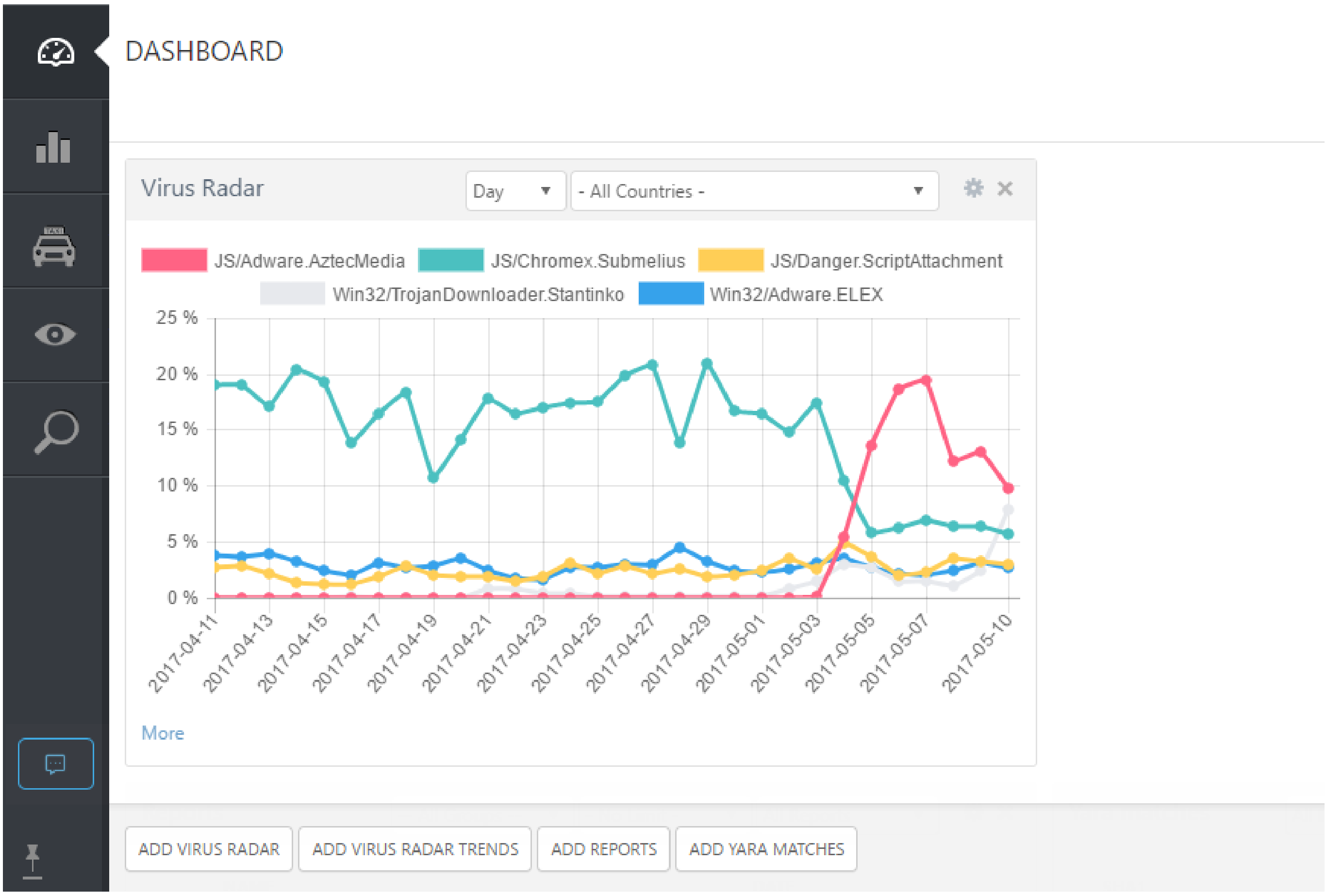
Changelog: To view the Portal changelog, expand the left menu and then click the version number at the bottom ("Version: #.#").

To make the menu not to expand upon mouse over, click the pin 📌.

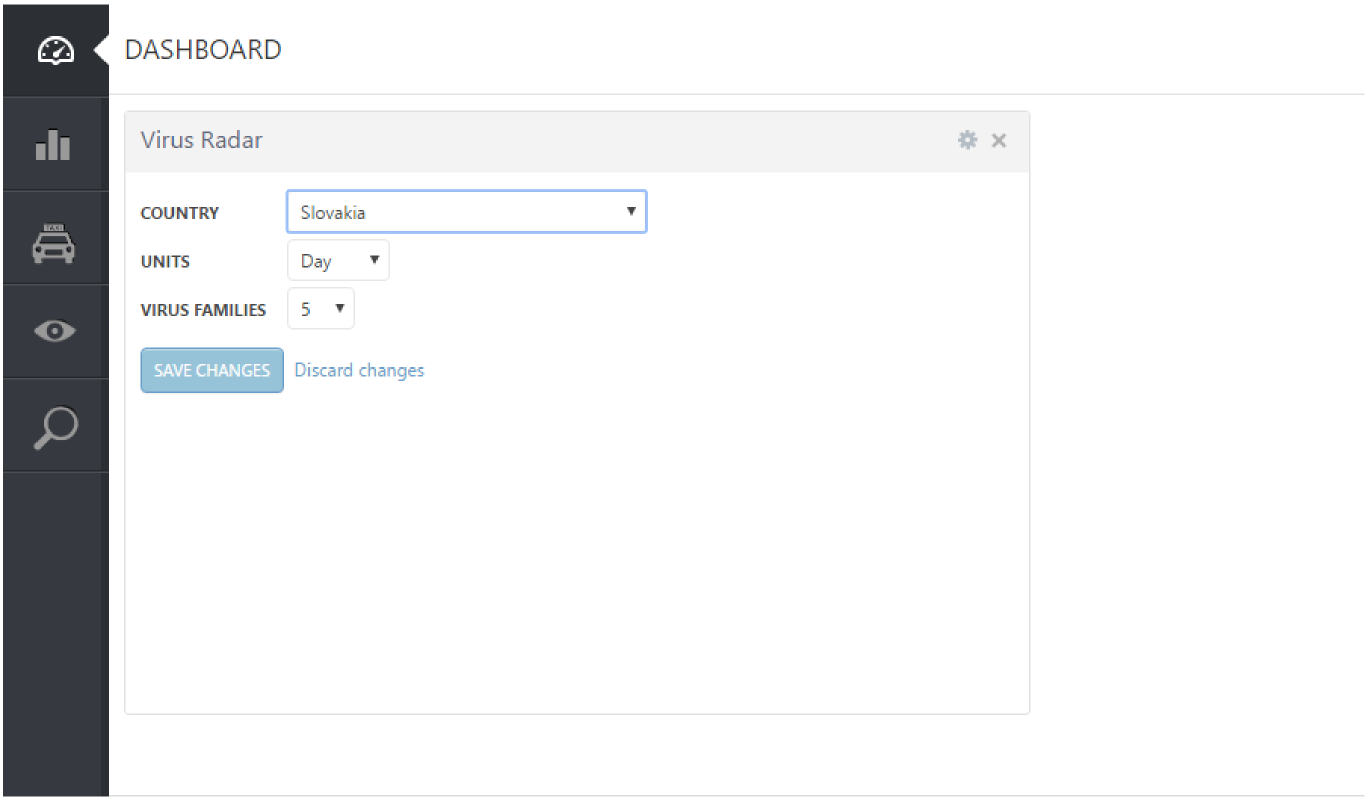
Dashboard

The dashboard features different widgets that you can display for an instant overview of relevant data. By default it is empty.

Click **Add Virus Radar** to display the **Virus Radar** widget. This widget displays the top threats from all over the world. Use the drop-down menus to filter the data by time period or country.



Click the gear icon to change the default values - time period, country, virus families.

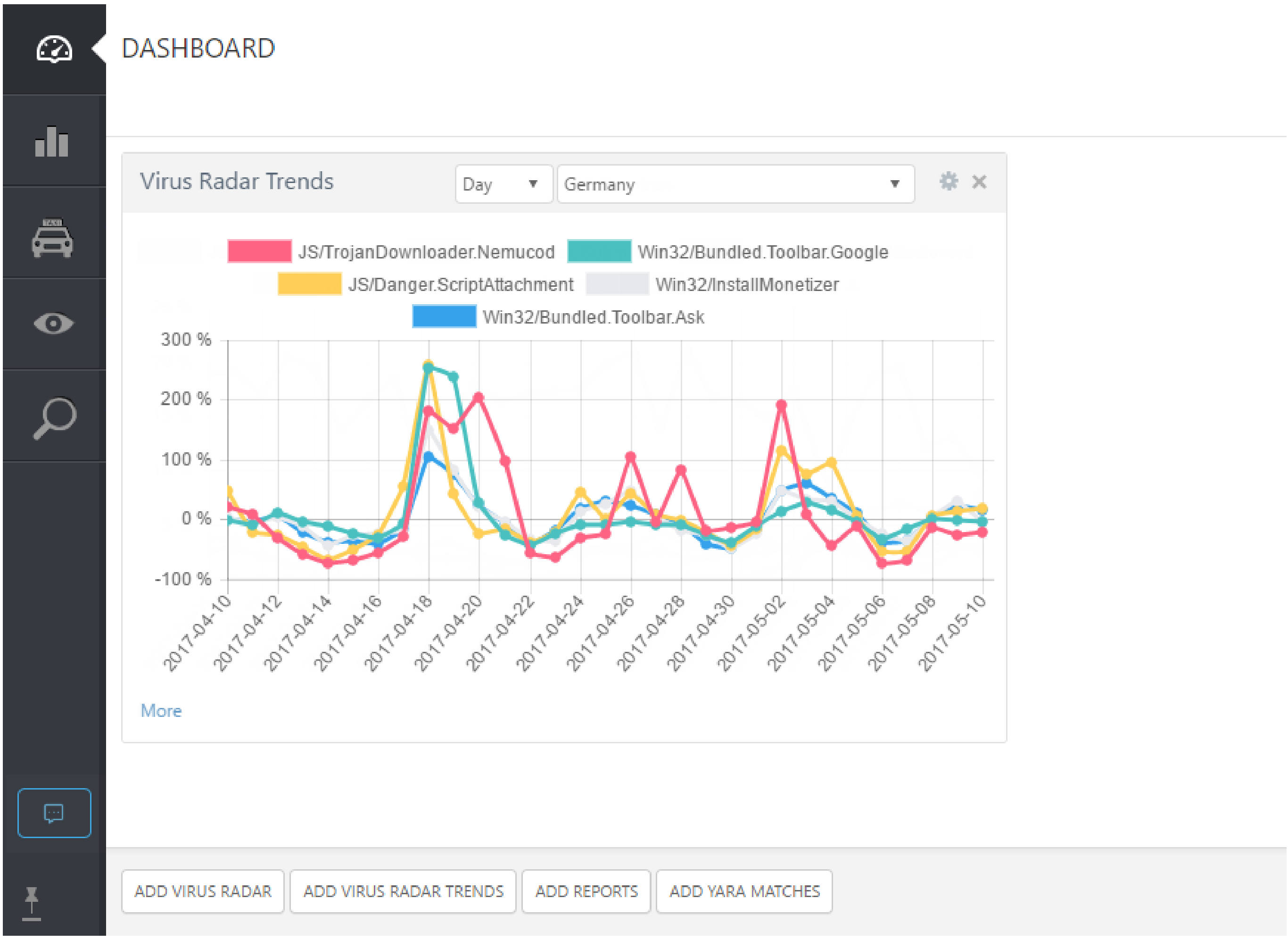


COUNTRY Slovakia

UNITS Day

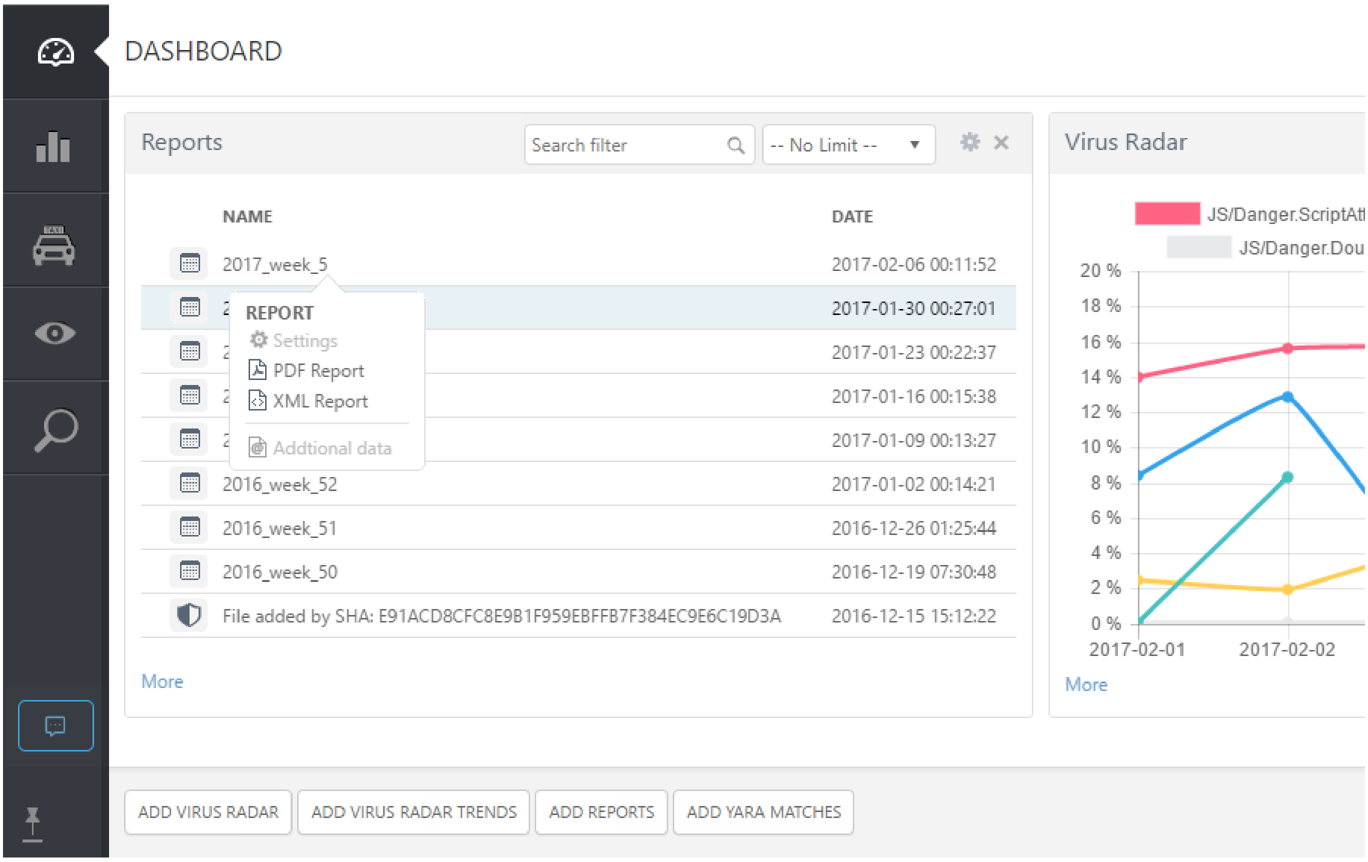
VIRUS FAMILIES 5

Virus Radar Trends widget shows you the change in the value relative to the moving average of top growing threats.



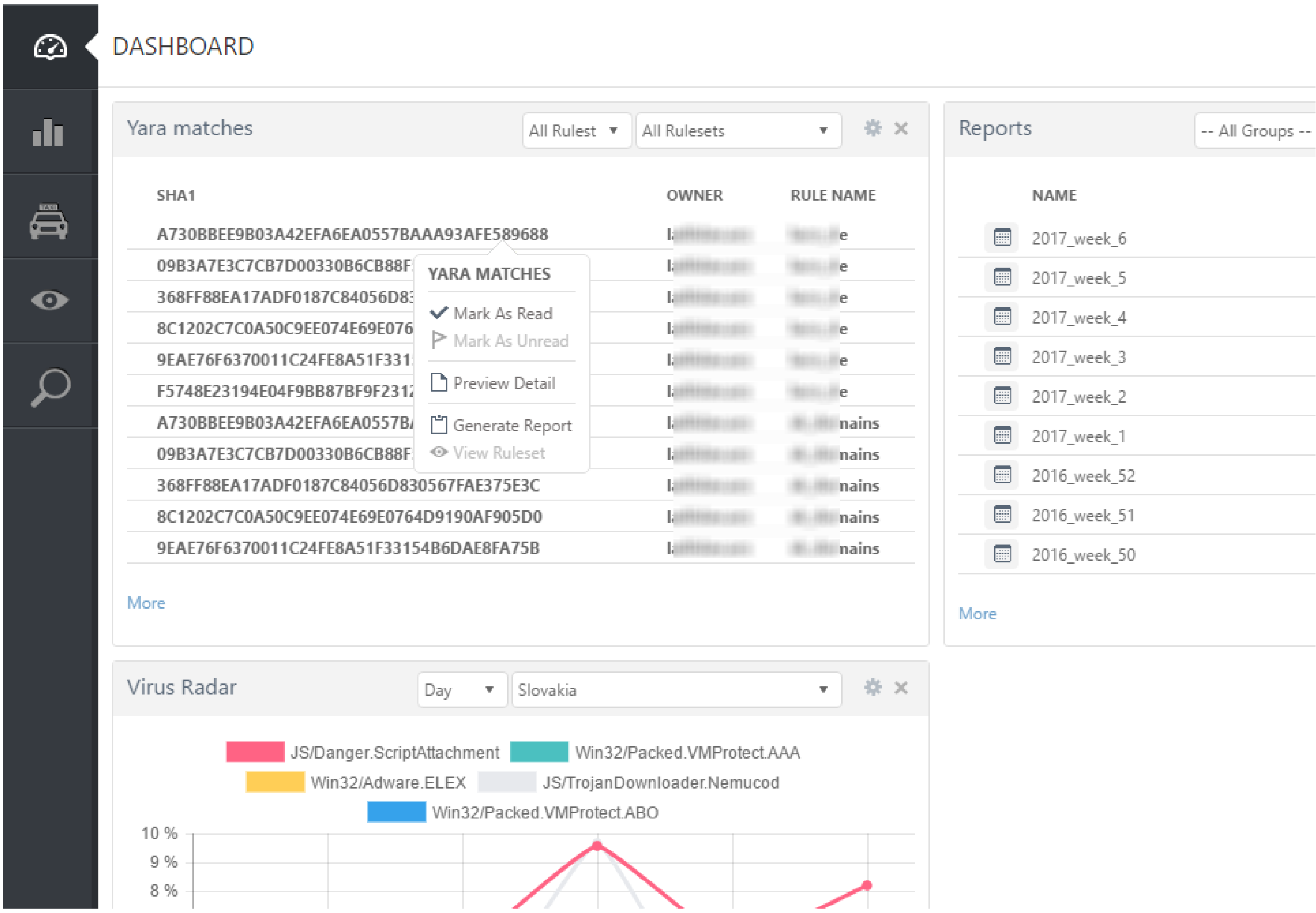
Click the gear icon to change the default values - time period, country, virus families, moving average interval.

Using the **Reports** widget, you can view the most recent reports and check the details of a selected report. Use the list boxes to filter the reports by group, period or type.



NAME	DATE
2017_week_5	2017-02-06 00:11:52
2	2017-01-30 00:27:01
2	2017-01-23 00:22:37
2	2017-01-16 00:15:38
2	2017-01-09 00:13:27
2016_week_52	2017-01-02 00:14:21
2016_week_51	2016-12-26 01:25:44
2016_week_50	2016-12-19 07:30:48
File added by SHA: E91ACD8CFC8E9B1F959EBFFB7F384EC9E6C19D3A	2016-12-15 15:12:22

The **Yara matches** widget lists the results of recently matched Yara rules and allows you to mark each match as read or unread, generate reports for it, or preview its details. If you select **Preview details**, you are redirected to the Yara matches screen where the details show up. Filter the results using the available list boxes.

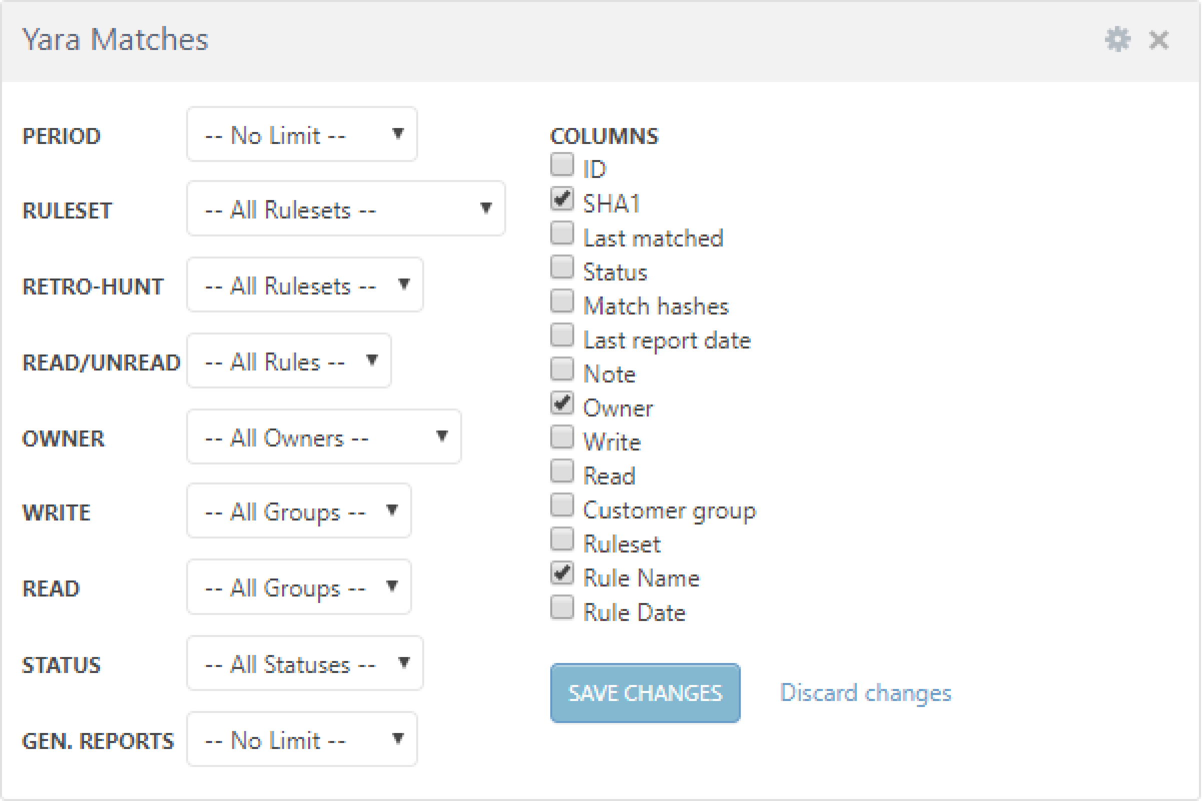


SHA1	OWNER	RULE NAME
A730BBEE9B03A42EFA6EA0557BAAA93AFE589688	[redacted]	[redacted]
09B3A7E3C7CB7D00330B6CB88F	[redacted]	[redacted]
368FF88EA17ADF0187C84056D83	[redacted]	[redacted]
8C1202C7C0A50C9EE074E69E076	[redacted]	[redacted]
9EAE76F6370011C24FE8A51F331	[redacted]	[redacted]
F5748E23194E04F9BB87BF9F231	[redacted]	[redacted]
A730BBEE9B03A42EFA6EA0557B	[redacted]	[redacted]
09B3A7E3C7CB7D00330B6CB88F	[redacted]	[redacted]
368FF88EA17ADF0187C84056D830567FAE375E3C	[redacted]	[redacted]
8C1202C7C0A50C9EE074E69E0764D9190AF905D0	[redacted]	[redacted]
9EAE76F6370011C24FE8A51F33154B6DAE8FA75B	[redacted]	[redacted]

NAME
2017_week_6
2017_week_5
2017_week_4
2017_week_3
2017_week_2
2017_week_1
2016_week_52
2016_week_51
2016_week_50

More
Virus Radar
Day ▾
Slovakia ▾
JS/Danger.ScriptAttachment
Win32/Packed.VMProtect.AAA
Win32/Adware.ELEX
JS/TrojanDownloader.Nemucod
Win32/Packed.VMProtect.ABO
10 %
9 %
8 %

Click the gear icon to change the default view of the **Yara matches** widget. You can select different columns to show, choose the type of matches to display by default.


Yara Matches

PERIOD	-- No Limit --
RULESET	-- All Rulesets --
RETRO-HUNT	-- All Rulesets --
READ/UNREAD	-- All Rules --
OWNER	-- All Owners --
WRITE	-- All Groups --
READ	-- All Groups --
STATUS	-- All Statuses --
GEN. REPORTS	-- No Limit --

COLUMNS

- □ ID
- ☑ SHA1
- □ Last matched
- □ Status
- □ Match hashes
- □ Last report date
- □ Note
- ☑ Owner
- □ Write
- □ Read
- □ Customer group
- □ Ruleset
- ☑ Rule Name
- □ Rule Date

Advanced Persistent Threat reports

An Advanced Persistent Threat (APT) is an adversary with sophisticated expertise and significant resources to create opportunities to achieve its objectives by using multiple attack vectors.

Threat intelligence reports provide contextual information about various adversaries, the latest APTs, technical analysis of such threats, and activity summaries of the threat landscape.

ESET Threat Intelligence APT reports PREMIUM service provides access to comprehensive information produced by the ESET research team in human- and machine-readable formats.

Technical analyses (monthly)

These regular in-depth threat analysis reports describe recent campaigns, new toolsets, and related subjects. They also contain recommendations to protect your network and remediation advice where applicable. These reports are helpful for defenders looking to protect their networks against the latest threats. They are also beneficial for researchers and incident responders who must analyze and report threats that might target their organizations.

Activity summary (bimonthly)

Summary activity reports issued every two weeks describe the latest APT campaigns ESET researchers have been tracking from various threat actors and their targets and the associated Indicators of Compromise (IoCs). Network defenders can use this data to protect their network by blocking these IoCs. These reports also allow researchers and incident response handlers to improve their understanding of APT groups targeting their organizations by knowing their most up-to-date Tactics, Techniques, and Procedures (TTPs).

Pre-access to research (1+ per month)

This service enables an organization to get pre-access to all ESET research publications on We Live Security. This service helps defenders prepare their response, in advance, to breakthrough developments discovered by ESET researchers, for instance, by pre-briefing senior management on urgent issues.

Access to MISP server

The ESET Malware Information Sharing Platform (MISP) server contains IoCs described in the reports. Every time a new report is available, the administrator receives an email notification. Historical reports are also available.

Access APT reports

1. Log in to the ETI portal.

2. Click **Reports**.

3. From **Report Type**, select **APT Reports**.

TAXII feeds

> ℹ Function availability based on the service level of subscription
> Access to this functionality is dependent on the service level of your subscription. Not all functionality described in this topic is available to all users.

Data feeds are available as STIX feeds and JSON feeds via TAXII. The feeds can be accessed in the **TAXII FEED** section or you can incorporate it into your internal system by standard TAXII interface. See our sample python script for accessing TAXII feeds . Once downloaded and extracted, open the script in a simple text editor to see further instructions for use.

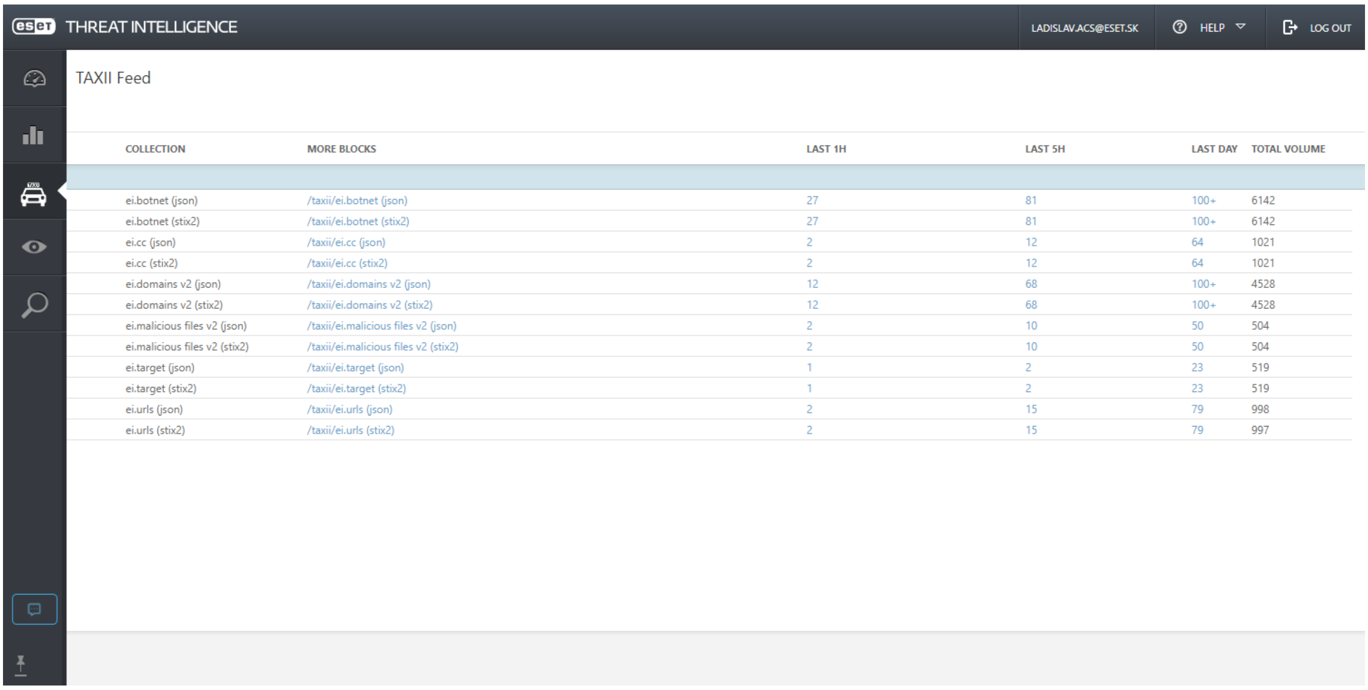
JSON and STIX feed formats

In the TAXII feed section each feed is available in 2 formats. For example:

- **ei.botnet** (json) — JSON feed format

- **ei.botnet** (stix2) — STIX version 2.0 feed

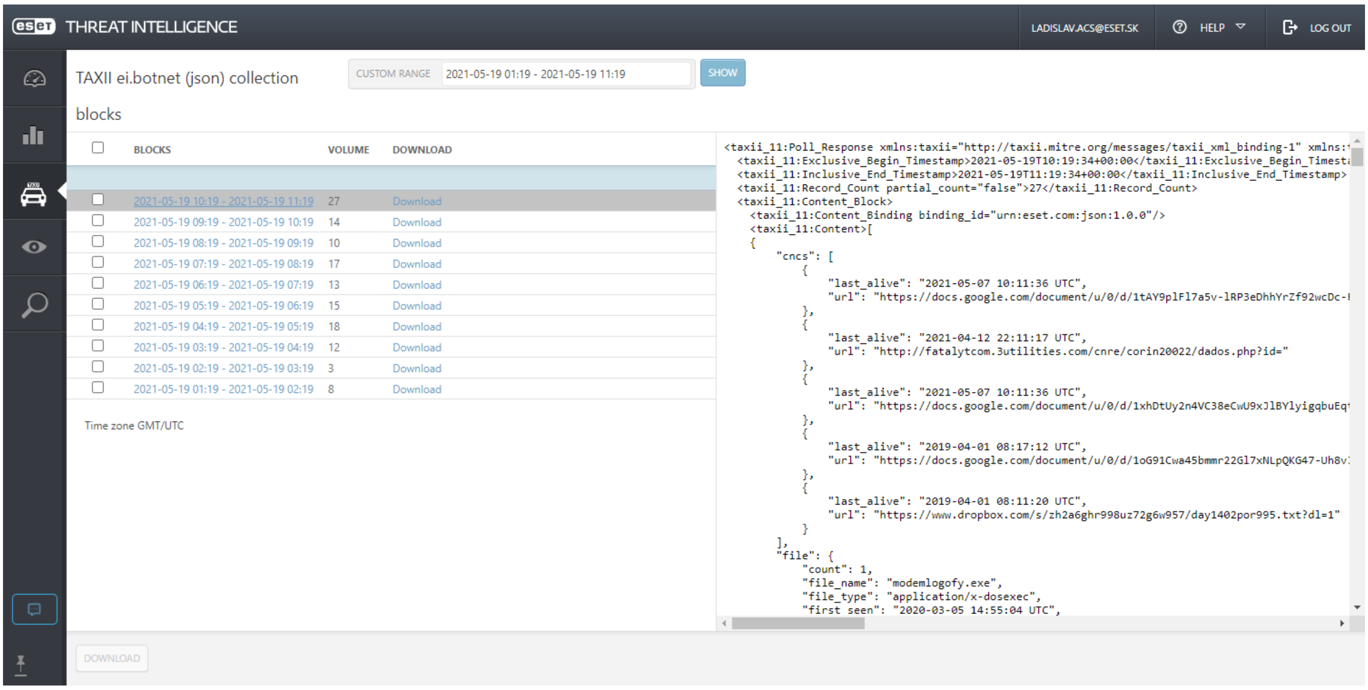
To preview feeds in the portal, select a report collection and then select one of the available options, or click the corresponding number under **Last 1h**, **Last 5h** or **Last day** column.



TAXII Feed

COLLECTION	MORE BLOCKS	LAST 1H	LAST 5H	LAST DAY	TOTAL VOLUME
ei.botnet (json)	/taxii/ei.botnet (json)	27	81	100+	6142
ei.botnet (stix2)	/taxii/ei.botnet (stix2)	27	81	100+	6142
ei.cc (json)	/taxii/ei.cc (json)	2	12	64	1021
ei.cc (stix2)	/taxii/ei.cc (stix2)	2	12	64	1021
ei.domains v2 (json)	/taxii/ei.domains v2 (json)	12	68	100+	4528
ei.domains v2 (stix2)	/taxii/ei.domains v2 (stix2)	12	68	100+	4528
ei.malicious files v2 (json)	/taxii/ei.malicious files v2 (json)	2	10	50	504
ei.malicious files v2 (stix2)	/taxii/ei.malicious files v2 (stix2)	2	10	50	504
ei.target (json)	/taxii/ei.target (json)	1	2	23	519
ei.target (stix2)	/taxii/ei.target (stix2)	1	2	23	519
ei.urls (json)	/taxii/ei.urls (json)	2	15	79	998
ei.urls (stix2)	/taxii/ei.urls (stix2)	2	15	79	997

Alternatively, click a report link under **More blocks**, then click a data range of non-zero **Volume** under **Blocks**.



TAXII ei.botnet (json) collection

CUSTOM RANGE 2021-05-19 01:19 - 2021-05-19 11:19

blocks

□	BLOCKS	VOLUME	DOWNLOAD
□	2021-05-19 10:19 - 2021-05-19 11:19	27	Download
□	2021-05-19 09:19 - 2021-05-19 10:19	14	Download
□	2021-05-19 08:19 - 2021-05-19 09:19	10	Download
□	2021-05-19 07:19 - 2021-05-19 08:19	17	Download
□	2021-05-19 06:19 - 2021-05-19 07:19	13	Download
□	2021-05-19 05:19 - 2021-05-19 06:19	15	Download
□	2021-05-19 04:19 - 2021-05-19 05:19	18	Download
□	2021-05-19 03:19 - 2021-05-19 04:19	12	Download
□	2021-05-19 02:19 - 2021-05-19 03:19	3	Download
□	2021-05-19 01:19 - 2021-05-19 02:19	8	Download

Time zone GMT/UTC

```
<taxii_11:Poll_Response xmlns:taxii="http://taxii.mitre.org/messages/taxii_xml_binding-1" xmlns:
  <taxii_11:Exclusive_Begin_Timestamp>2021-05-19T10:19:34+00:00</taxii_11:Exclusive_Begin_Timesta
  <taxii_11:Inclusive_End_Timestamp>2021-05-19T11:19:34+00:00</taxii_11:Inclusive_End_Timestamp>
  <taxii_11:Record_Count partial_count="false">27</taxii_11:Record_Count>
  <taxii_11:Content_Block>
    <taxii_11:Content_Binding binding_id="urn:eset.com:json:1.0.0"/>
    <taxii_11:Content>[
    {
        "cncs": [
            {
                "last_alive": "2021-05-07 10:11:36 UTC",
                "url": "https://docs.google.com/document/u/0/d/1tAY9plFl7a5v-lRP3eDhhYrZf92wcDc-
            },
            {
                "last_alive": "2021-04-12 22:11:17 UTC",
                "url": "http://fatalytcom.3utilities.com/cnre/corin20022/dados.php?id="
            },
            {
                "last_alive": "2021-05-07 10:11:36 UTC",
                "url": "https://docs.google.com/document/u/0/d/1xhDtUy2n4VC38eCwU9xJlBYlyigqbuEq
            },
            {
                "last_alive": "2019-04-01 08:17:12 UTC",
                "url": "https://docs.google.com/document/u/0/d/1oG91Cwa45bmmr22Gl7xNLpQKG47-Uh8v
            },
            {
                "last_alive": "2019-04-01 08:11:20 UTC",
                "url": "https://www.dropbox.com/s/zh2a6ghr998uz72g6w957/day1402por995.txt?dl=1"
            }
        ],
        "file": {
            "count": 1,
            "file_name": "modemlogofy.exe",
            "file_type": "application/x-dosexec",
            "first seen": "2020-03-05 14:55:04 UTC",
```

If you click **Download**, the feed opens in a new tab. Right-click the new feed and select **Save**.

You can choose from several types of feeds:

- Botnet feed
- Domain feed
- Malicious files feed

- URL feed
- IP feed
- APT feed

Botnet feed

The botnet feed shares all the data ESET has about the Botnet network. The feed consists of three types of feeds (botnet, cc, and target). Each feed contains different information.

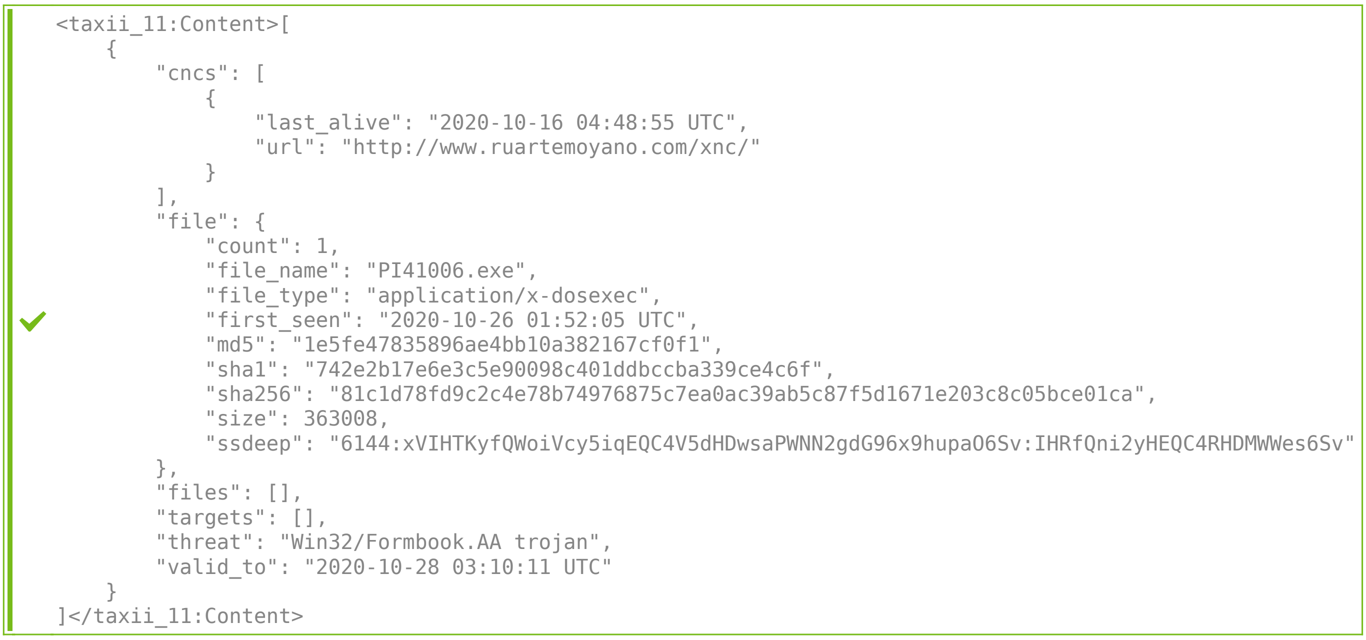
ei.botnet

Below is a description of some attributes of the ei.botnet feed.

- Detection—The name of the detection defined by ESET (`Win32/TrojanDownloader.Wauchos.CX trojan`).
- Hashes—The hash of the detected file (`SHA1`, `MD5`, `SHA256`).
- File_extension—The type of malicious file (`.exe`, `.sys`, `.dll`, `script`, or `unk`).
- Used by—The family name of the attacking botnet. This field has the same value as the target field in `ei.target` (`Win32/Dorkbot.H worm`).
- Last alive—The timestamp of when ESET was last able to communicate with the server (`2015-12-03 13:17:31`).
- URIobj type=C2—The link of the Command and Control (CnC) server. This value might be a TOR link also (`http://t7yz3cihrrzalznq.onion/assets`).
- Config—The `SHA-1` hash of the configuration file when downloaded (`.ini`, `.bin`).
- URIobj type=target—The targeted link string botnet is attacking (`*paypal.*/webscr?cmd=_login-submit*`).
- Files downloaded by the main file—These files may be downloaded by the main file. If so, the feed contains the following:
  - Detection—The name of the detection defined by ESET.
  - Hashes (`SHA1`, `MD5`, or `SHA256`)
  - Type of file (`.exe`, `.sys`, `.dll`, `script`, or `unk`)

JSON

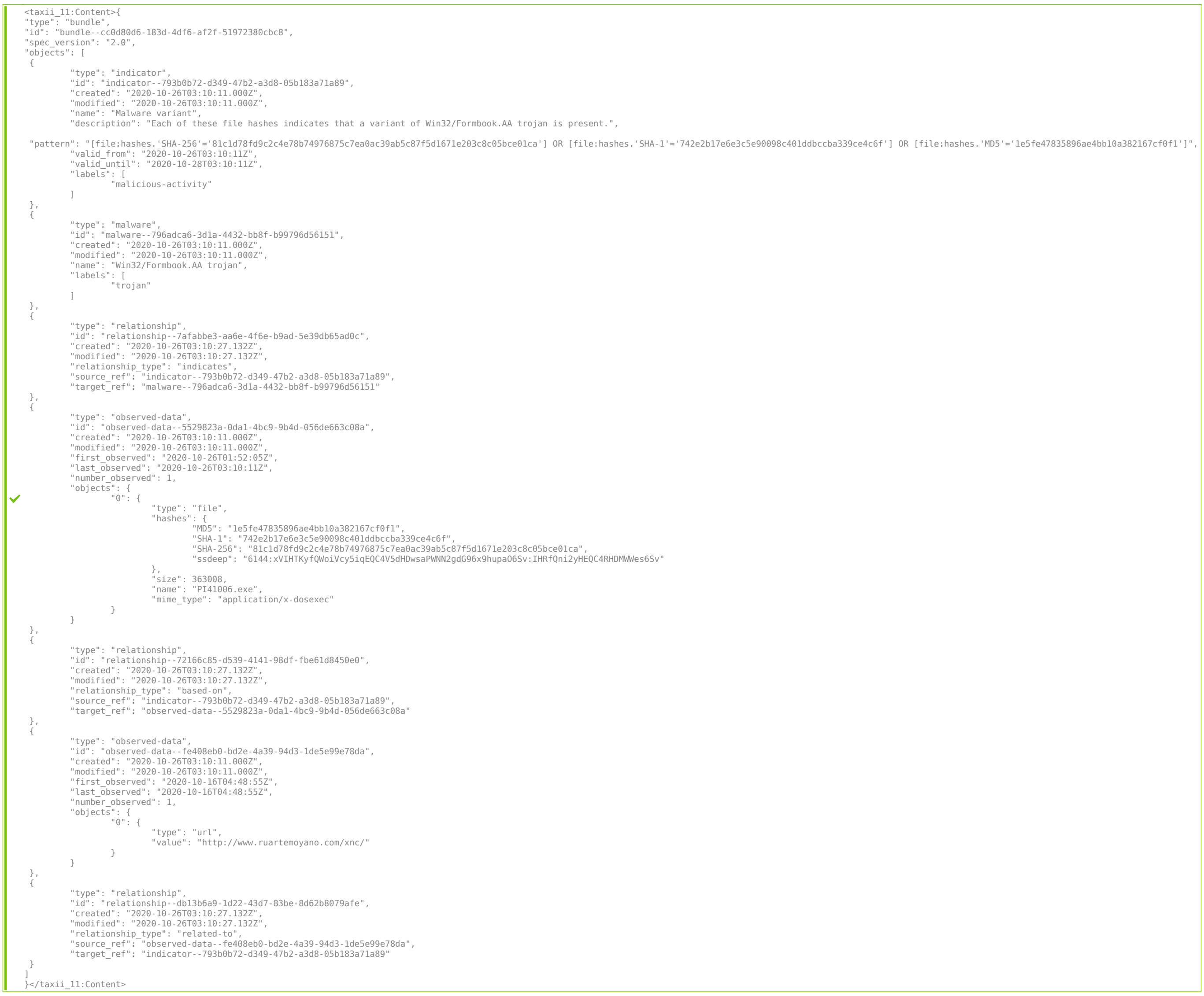
Below is a snippet of an ei.botnet feed in JSON format.



```
<taxii_11:Content>[
    {
        "cncs": [
            {
                "last_alive": "2020-10-16 04:48:55 UTC",
                "url": "http://www.ruartemoyano.com/xnc/"
            }
        ],
        "file": {
            "count": 1,
            "file_name": "PI41006.exe",
            "file_type": "application/x-dosexec",
            "first_seen": "2020-10-26 01:52:05 UTC",
            "md5": "1e5fe47835896ae4bb10a382167cf0f1",
            "sha1": "742e2b17e6e3c5e90098c401ddbccba339ce4c6f",
            "sha256": "81c1d78fd9c2c4e78b74976875c7ea0ac39ab5c87f5d1671e203c8c05bce01ca",
            "size": 363008,
            "ssdeep": "6144:xVIHTKyfQWoiVcy5iqEQC4V5dHDwsaPWNN2gdG96x9hupaO6Sv:IHRfQni2yHEQC4RHDMWWes6Sv"
        },
        "files": [],
        "targets": [],
        "threat": "Win32/Formbook.AA trojan",
        "valid_to": "2020-10-28 03:10:11 UTC"
    }
]</taxii_11:Content>
```

STIX 2.0

Below is a snippet of an ei.botnet feed in STIX 2.0 format.

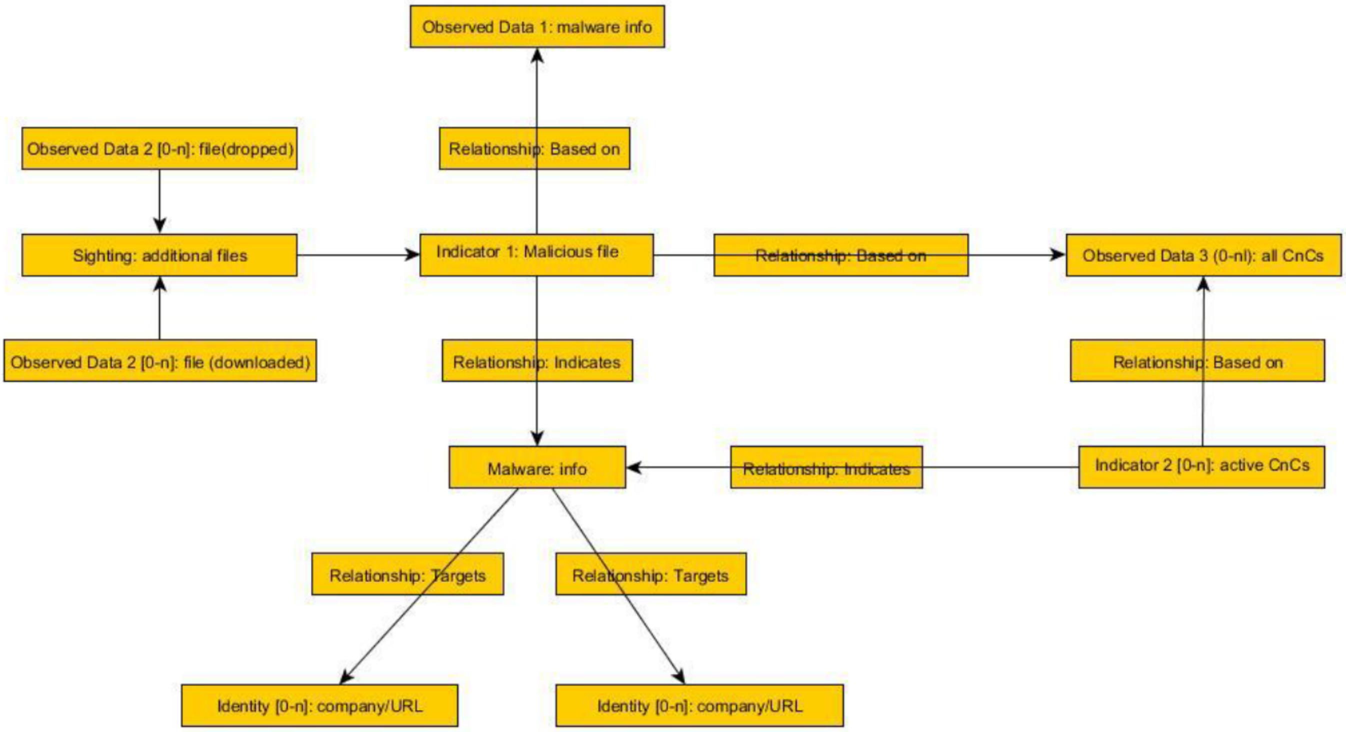


```
<taxii_11:Content>{
"type": "bundle",
"id": "bundle--cc0d80d6-183d-4df6-af2f-51972380cbc8",
"spec_version": "2.0",
"objects": [
 {
        "type": "indicator",
        "id": "indicator--793b0b72-d349-47b2-a3d8-05b183a71a89",
        "created": "2020-10-26T03:10:11.000Z",
        "modified": "2020-10-26T03:10:11.000Z",
        "name": "Malware variant",
        "description": "Each of these file hashes indicates that a variant of Win32/Formbook.AA trojan is present.",

 "pattern": "[file:hashes.'SHA-256'='81c1d78fd9c2c4e78b74976875c7ea0ac39ab5c87f5d1671e203c8c05bce01ca'] OR [file:hashes.'SHA-1'='742e2b17e6e3c5e90098c401ddbccba339ce4c6f'] OR [file:hashes.'MD5'='1e5fe47835896ae4bb10a382167cf0f1']",
        "valid_from": "2020-10-26T03:10:11Z",
        "valid_until": "2020-10-28T03:10:11Z",
        "labels": [
                "malicious-activity"
        ]
 },
 {
        "type": "malware",
        "id": "malware--796adca6-3d1a-4432-bb8f-b99796d56151",
        "created": "2020-10-26T03:10:11.000Z",
        "modified": "2020-10-26T03:10:11.000Z",
        "name": "Win32/Formbook.AA trojan",
        "labels": [
                "trojan"
        ]
 },
 {
        "type": "relationship",
        "id": "relationship--7afabbe3-aa6e-4f6e-b9ad-5e39db65ad0c",
        "created": "2020-10-26T03:10:27.132Z",
        "modified": "2020-10-26T03:10:27.132Z",
        "relationship_type": "indicates",
        "source_ref": "indicator--793b0b72-d349-47b2-a3d8-05b183a71a89",
        "target_ref": "malware--796adca6-3d1a-4432-bb8f-b99796d56151"
 },
 {
        "type": "observed-data",
        "id": "observed-data--5529823a-0da1-4bc9-9b4d-056de663c08a",
        "created": "2020-10-26T03:10:11.000Z",
        "modified": "2020-10-26T03:10:11.000Z",
        "first_observed": "2020-10-26T01:52:05Z",
        "last_observed": "2020-10-26T03:10:11Z",
        "number_observed": 1,
        "objects": {
                "0": {
                        "type": "file",
                        "hashes": {
                                "MD5": "1e5fe47835896ae4bb10a382167cf0f1",
                                "SHA-1": "742e2b17e6e3c5e90098c401ddbccba339ce4c6f",
                                "SHA-256": "81c1d78fd9c2c4e78b74976875c7ea0ac39ab5c87f5d1671e203c8c05bce01ca",
                                "ssdeep": "6144:xVIHTKyfQWoiVcy5iqEQC4V5dHDwsaPWNN2gdG96x9hupaO6Sv:IHRfQni2yHEQC4RHDMWWes6Sv"
                        },
                        "size": 363008,
                        "name": "PI41006.exe",
                        "mime_type": "application/x-dosexec"
                }
        }
 },
 {
        "type": "relationship",
        "id": "relationship--72166c85-d539-4141-98df-fbe61d8450e0",
        "created": "2020-10-26T03:10:27.132Z",
        "modified": "2020-10-26T03:10:27.132Z",
        "relationship_type": "based-on",
        "source_ref": "indicator--793b0b72-d349-47b2-a3d8-05b183a71a89",
        "target_ref": "observed-data--5529823a-0da1-4bc9-9b4d-056de663c08a"
 },
 {
        "type": "observed-data",
        "id": "observed-data--fe408eb0-bd2e-4a39-94d3-1de5e99e78da",
        "created": "2020-10-26T03:10:11.000Z",
        "modified": "2020-10-26T03:10:11.000Z",
        "first_observed": "2020-10-16T04:48:55Z",
        "last_observed": "2020-10-16T04:48:55Z",
        "number_observed": 1,
        "objects": {
                "0": {
                        "type": "url",
                        "value": "http://www.ruartemoyano.com/xnc/"
                }
        }
 },
 {
        "type": "relationship",
        "id": "relationship--db13b6a9-1d22-43d7-83be-8d62b8079afe",
        "created": "2020-10-26T03:10:27.132Z",
        "modified": "2020-10-26T03:10:27.132Z",
        "relationship_type": "related-to",
        "source_ref": "observed-data--fe408eb0-bd2e-4a39-94d3-1de5e99e78da",
        "target_ref": "indicator--793b0b72-d349-47b2-a3d8-05b183a71a89"
 }
]
}</taxii_11:Content>
```

The following types of STIX domain objects are available for the botnet feed:

- **Indicator** 1—The main Indicator of Comprise (IoC), which is a malicious file that communicates with a CnC server. This object is always present in the feed
- **Observed data** 1—Additional information about the malicious file.
- **Malware**—A detection of a malicious botnet file.
- **Identity**—The targets of the malware obtained from the configuration of the CnC. This object is optional.
- **Observed data** 2—If a malicious file (IoC 1) creates or downloads additional files, the files will be connected to that file (IoC 1) via **Sighting**.
- **Indicator** 2—The secondary IoC tied to IoC 1. This object refers to the link of the CnC server and the associated data. If the last communication with the CnC server through the given link was more than 48 hours ago, **Indicator** 2 turns to **Observed data** 3.
- **Observed data** 3—This object shows all links that were pointing to the CnC server hosting the malware. If the links were active in the last 48 hours, they have a relationship also with **Indicator** 2.
- **Relationship:**


Observed Data 1: malware info
Observed Data 2 [0-n]: file(dropped)
Relationship: Based on
Sighting: additional files
Indicator 1: Malicious file
Relationship: Based on
Observed Data 3 (0-nl): all CnCs
Observed Data 2 [0-n]: file (downloaded)
Relationship: Indicates
Relationship: Based on
Malware: info
Relationship: Indicates
Indicator 2 [0-n]: active CnCs
Relationship: Targets
Relationship: Targets
Identity [0-n]: company/URL
Identity [0-n]: company/URL

CC feed

This feed is a subset of a botnet feed and provides information about links of Command and Control (CnC) servers and associated data. Thus the name **CC feed**.

ei.cc

Below is a description of some attributes of the ei.cc feed.

- Used by—The family name of the attacking Botnet. This field has the same value as the "target" field in `ei.target` (`Win32/Dorkbot.H worm`).
- Last alive—The timestamp of when ESET was last able to communicate with the server (`2015-12-03 13:17:31`).
- URIobj—The link to the CnC server. This value might be a TOR link also (`http://t7yz3cihrrzalznq.onion/assets`).
- Protocols:
  - Protocols used by URIobj
  - Layer4_Protocol (`TCP`)
  - Layer7_Protocol (`http`)
- IP_Address—The IP address of the CnC server (`204.95.99.243`).
- Hostname—The hostname of the CnC server. This name is not always the same as the link (`n.lbxfqfcxj.ru`).
- Port_value—The port-communicated number (`443`).

JSON

Below is a snippet of an ei.cc feed in JSON format.

```
{
 "cnc": "http://62.30.7.67:443",
 "domain_count": 16584,
 "domain_first_seen": "2019-09-28 23:00:00 UTC",
 "domain_last_seen": "2020-10-26 11:51:04 UTC",
 "host": "62.30.7.67",
 "ip": "62.30.7.67",
 "last_alive": "2020-10-26 10:37:15 UTC",
 "port": 443,
 "prot_l4": "TCP",
 "prot_l7": "http",
 "state": null,
 "threat": "Win32/Emotet.CI trojan",
 "valid_to": "2020-10-28 12:00:14 UTC"
}
```

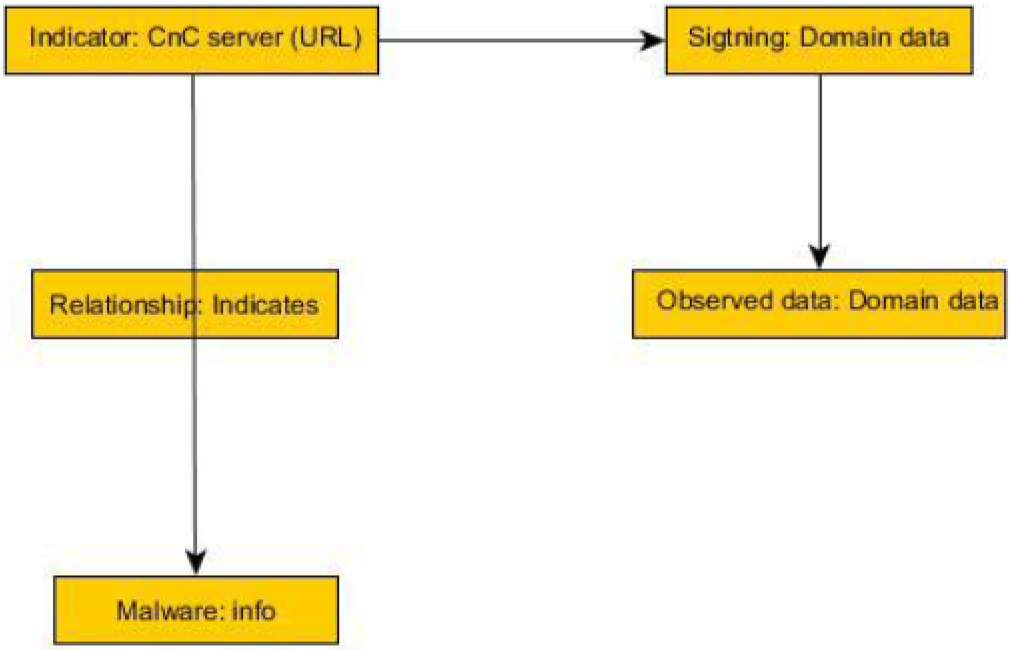
STIX 2.0

Below is a snippet of an ei.cc feed in STIX 2.0 format.

```
{
 "type": "indicator",
 "id": "indicator--8425fc2b-adc6-4e71-a2b5-7a469dd1b2e0",
 "created": "2020-10-26T12:00:14.000Z",
 "modified": "2020-10-26T12:00:14.000Z",
 "name": "Not blocked",
 "description": "C&amp;C of Win32/Emotet.CI trojan",
 "pattern": "[url:value='http://62.30.7.67:443']",
 "valid_from": "2020-10-26T12:00:14Z",
 "valid_until": "2020-10-28T12:00:14Z",
 "labels": [
         "malicious-activity"
 ]
}
```

The following types of STIX domain objects are available for the cc feed:

- **Indicator**—The link to the CnC server that should be blocked
- **Malware**—Information about the malware that communicates with the CnC server through the given link
- **Observed data**—Additional information about the domain on which the CnC link is hosted
- **Relationship**:



Target feed

This feed is a subset of a botnet feed and provides information about the targets.

ei.target

Below is a description of some attributes of the ei.target feed.

- Target—The targeted link string that the botnet is attacking (`*paypal.*/webscr?cmd=_login-submit*`).
- Targeted by—The family name of attacking botnet. This field has the same value as `ei.botnet` and `ei.cc` (`Win32/Dorkbot.B worm`).

JSON

Below is a snippet of an ei.target feed in JSON format.

```
{
 "cnc": "http://81.215.230.173:443",
 "domain_count": 5524,
 "domain_first_seen": "2020-10-16 12:10:42 UTC",
 "domain_last_seen": "2020-10-26 12:55:19 UTC",
 "host": "81.215.230.173",
 "ip": "81.215.230.173",
 "last_alive": "2020-10-26 03:52:54 UTC",
 "port": 443,
 "prot_l4": "TCP",
 "prot_l7": "http",
 "state": null,
 "threat": "Win32/Emotet.CI trojan",
 "valid_to": "2020-10-28 13:11:06 UTC"
}
```

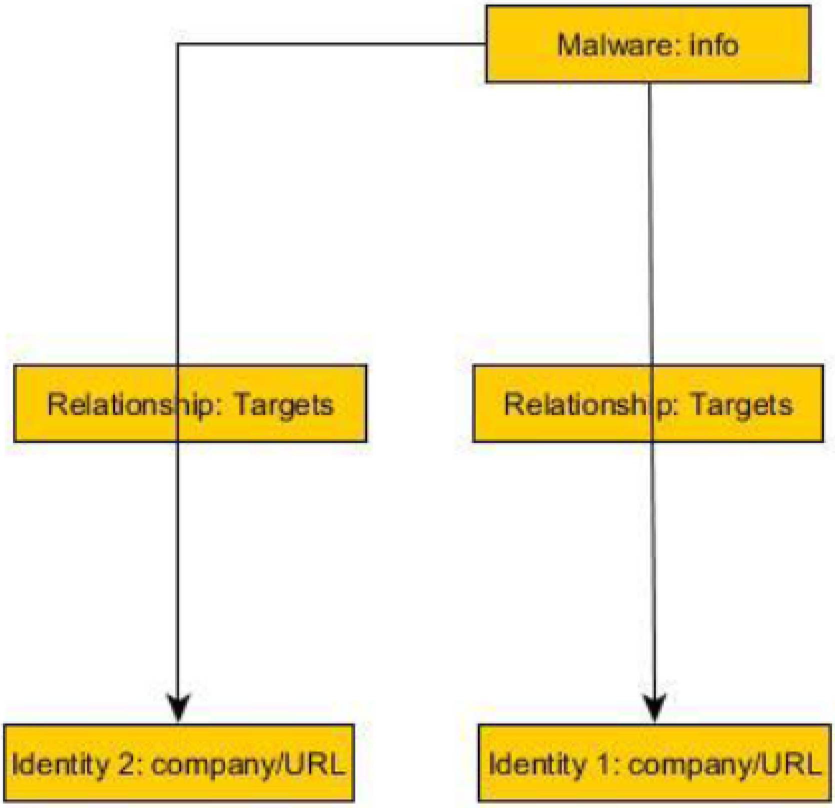
STIX 2.0

Below is a snippet of an ei.target feed in STIX 2.0 format.

```
{
 "type": "identity",
 "id": "identity--1982c472-79dc-41a3-a43e-1a756f9c7b64",
 "created": "2020-10-26T12:56:07.577Z",
 "modified": "2020-10-26T12:56:07.577Z",
 "name": "https://www24.bmo.com/onlinebanking/*",
 "identity_class": "unknown"
},
{
 "type": "malware",
 "id": "malware--0fe7e8a7-5302-468a-975d-7872599d629e",
 "created": "2020-10-26T12:56:07.000Z",
 "modified": "2020-10-26T12:56:07.000Z",
 "name": "Win32/Qbot.CO trojan",
 "labels": [
         "bot"
 ]
},
{
 "type": "relationship",
 "id": "relationship--0dd64678-3d06-4415-9a1c-82535320398e",
 "created": "2020-10-26T12:56:07.577Z",
 "modified": "2020-10-26T12:56:07.577Z",
 "relationship_type": "targets",
 "source_ref": "malware--0fe7e8a7-5302-468a-975d-7872599d629e",
 "target_ref": "identity--1982c472-79dc-41a3-a43e-1a756f9c7b64"
}
```

The following types of STIX domain objects are available for the target feed:

- **Malware** - The detection name of the malware targeting the identity
- **Identity** - The name of the target, usually in the form of a link string, human-readable company name, or process name
- **Relationship:**



Domain feed

The domain feed consists of domains that are considered malicious. This feed recognizes and shares the following specifications about the domains:

- DomainName
  - The name of the domain (`un-stop.org`)
  - The type of maliciousness of the domain. Following are the possible types:
    - Block—A malicious link is blocked in the domain
    - Phishing—A phishing link is blocked in the domain
    - Unwanted—A potentially unwanted application link is blocked in the domain
    - Blocked Object—The domain hosts downloadable malware but should not be blocked as a whole
  - The number of times the domain is identified as malicious in a given type
- AddressObj—The IP address of the malicious domain (`192.3.136.10)`
- Downloaded_detection—The detection of a file downloaded from a given blocked link (`Application.JS/Adware.Imali.A`)
- Parent_detection—The detection of a file that was trying to access the given blocked link

(`Application.Win32/Adware.ICLoader.ME`)

JSON

Below is a snippet of a domain feed in JSON format.

```
<taxii_11:Content_Block>
    <taxii_11:Content_Binding binding_id="urn:eset.com:json:1.0.0"/>
    <taxii_11:Content>[
    {
        "confidence": "Low",
        "count": 16054,
        "count_24h": 12,
        "countries": [
            {
                "code": "UNKNOWN",
                "count_24h": 12,
                "unique_users_count_24h": 1
            }
        ],
        "domain": "tgory.pl",
        "downloaded_detection": null,
        "first_seen": "2018-07-31 23:00:00 UTC",
        "ip": null,
        "last_seen": "2020-10-22 11:17:59 UTC",
        "location": null,
        "opener_detection": null,
        "reason": "Host actively distributes high-severity threat in the form of executable code.",
        "state": "BlockedObject",
        "valid_to": "2020-10-24 11:41:26 UTC"
    }
 ]</taxii_11:Content>
    <taxii_11:Timestamp_Label>2020-10-22T11:41:30+00:00</taxii_11:Timestamp_Label>
</taxii_11:Content_Block>
```

STIX 2.0

Below is a snippet of a domain feed in STIX 2.0 format.

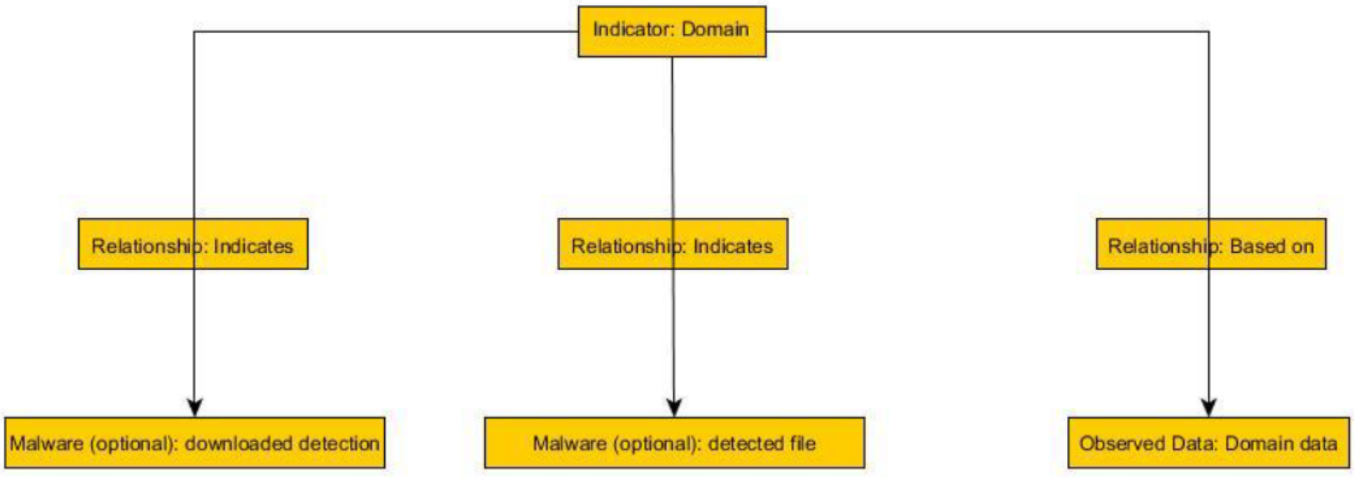
```
{
 "type": "observed-data",
 "id": "observed-data--491ae041-7454-42e9-a7ee-8f3b25d7d035",
 "created": "2020-10-22T11:41:26.000Z",
 "modified": "2020-10-22T11:41:26.000Z",
 "first_observed": "2018-07-31T23:00:00Z",
 "last_observed": "2020-10-22T11:17:59Z",
 "number_observed": 16054,
 "objects": {
         "0": {
                 "type": "domain-name",
                 "value": "tgory.pl"
         }
 }
}
```

The following STIX domain objects are available for the Domain feed:

- **Indicator**—An Indicator of Comprise (IoC) to use for further blocking or investigation
- **Observed data**—Extra information about the given domain that is intended for manual investigation

- **Malware**—An optional object shared with every domain IoC only if a malicious file downloaded from the given domain is detected and blocked

- **Relationship**:


Indicator: Domain
Relationship: Indicates
Relationship: Indicates
Relationship: Based on
Malware (optional): downloaded detection
Malware (optional): detected file
Observed Data: Domain data

Malicious files feed

The Malicious files feed contains executable files that are considered malicious. This feed recognizes and shares the following specifications about files:

- Hash (`SHA1`, `MD5`, and `SHA256`).

- Detection—The name of the detection defined by ESET (`VBA/TrojanDownloader.Agent.GKT`).

- Size_In_Bytes—The size of the file in bytes (`1433600`).

- File_Format—The format of the file based on a common UNIX utility file (`PE32 executable (GUI) Intel 80386, for MS Windows`). For more information, refer to this link.

JSON
Below is a snippet of a Malicious files feed in JSON format.

```
{
 "count": 3,
 "countries": [
        {
               "count": 2,
               "country": "United States",
               "region": "NORAM"
        },
        {
               "count": 1,
               "country": "Ecuador",
               "region": "LATAM"
        }
 ],
 "file_name": "31113.html",
 "file_type": "text/plain",
 "first_seen": "2019-03-13 12:46:46 UTC",
 "md5": "29e476f594ed5e226b2c0c60c243fc9a",
 "sha1": "47b49ae4de0bf559a3be264df6b747584b0188d5",
 "sha256": "ce61716a17f8950e1d46a6230d0bc80e02d9a87796a683aa6c8532fbcb235ce5",
 "size": 1731,
 "ssdeep": "24:hAYkvfTol1MXPsRzqAXJ3UNSdV9O0W+bDxgb3ORWUjcHjvc6tjDxnILMFIiC1IdP:GYkvfToZkgRO07Ke5jcHooITIdk2",
 "threat": "JS/Exploit.Shellcode.A.gen trojan",
 "valid_to": "2020-10-23 06:38:34 UTC"
}
```

STIX 2.0

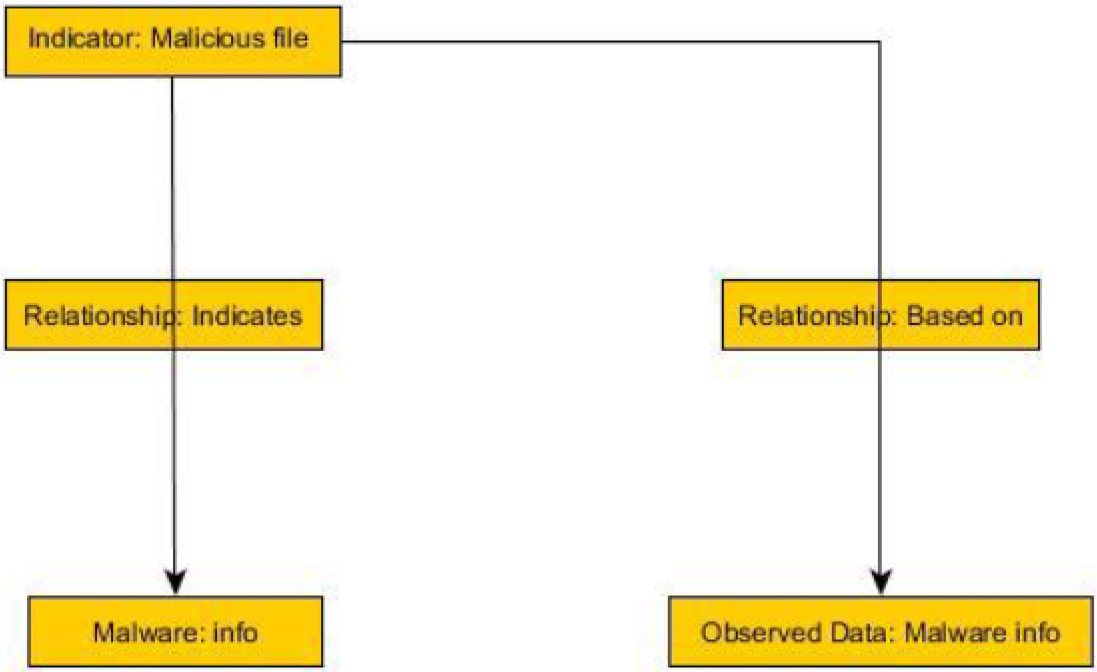
Below is a snippet of a Malicious files feed in STIX 2.0 format.

```
{
 "type": "observed-data",
 "id": "observed-data--25cd0fbd-98ed-4199-8469-9c8f08704028",
 "created": "2020-10-21T06:38:34.000Z",
 "modified": "2020-10-21T06:38:34.000Z",
 "first_observed": "2019-03-13T12:46:46Z",
 "last_observed": "2020-10-21T06:38:34Z",
 "number_observed": 3,
 "objects": {
        "0": {
               "type": "file",
               "hashes": {
                      "MD5": "29e476f594ed5e226b2c0c60c243fc9a",
                      "SHA-1": "47b49ae4de0bf559a3be264df6b747584b0188d5",
                      "SHA-256": "ce61716a17f8950e1d46a6230d0bc80e02d9a87796a683aa6c8532fbcb235ce5",

 "ssdeep": "24:hAYkvfTol1MXPsRzqAXJ3UNSdV9O0W+bDxgb3ORWUjcHjvc6tjDxnILMFIiC1IdP:GYkvfToZkgRO07Ke5jcHooITIdk2"
               },
               "size": 1731,
               "name": "31113.html",
               "mime_type": "text/plain"
        }
 }
}
```

The following types of STIX domain objects are available for the Malicious files feed:

- **Indicator**—An Indicator of Comprise (IoC) to use for further blocking or investigation.
- **Malware**—Additional information about given hashes, which includes the name of the detection. This information is intended for manual investigation.
- **Observed data**—Additional information about the file.
- **Relationship**:



URL feed

The URL feed contains domains that are considered malicious. Compared to the Domain feed, the URL feed can show different results due to different filter options. For example, there are objects blocked on the URL level only and not at the domain level. The feed recognizes and shares the same specifications as the Domain feed. However, there is a URL address instead of a domain name due to identifying the exact location of malicious content.

JSON

Below is a snippet of an URL feed in JSON format.

```
<taxii_11:Content>[
{
 "confidence": "High",
 "count_24h": 1,
 "countries": [
        {
                "code": "UNKNOWN",
                "count_24h": 1,
                "unique_users_count_24h": 1
        }
 ],
 "domain": "bejnz.com",
 "domain_count": 1065,
 "domain_first_seen": "2018-07-31 23:00:00 UTC",
 "domain_last_seen": "2020-10-22 11:04:55 UTC",
 "downloaded_detection": null,
 "ip": null,
 "location": null,
 "opener_detection": "Trojan.MSIL/Kryptik.MSS",
 "reason": "Host is used as command and control server of MSIL/Kryptik.MSS trojan malware family.",
 "state": "Blocked",
 "url": "http://bejnz.com/IP.php",
 "valid_to": "2020-10-24 11:56:16 UTC"
}
]</taxii_11:Content>
```

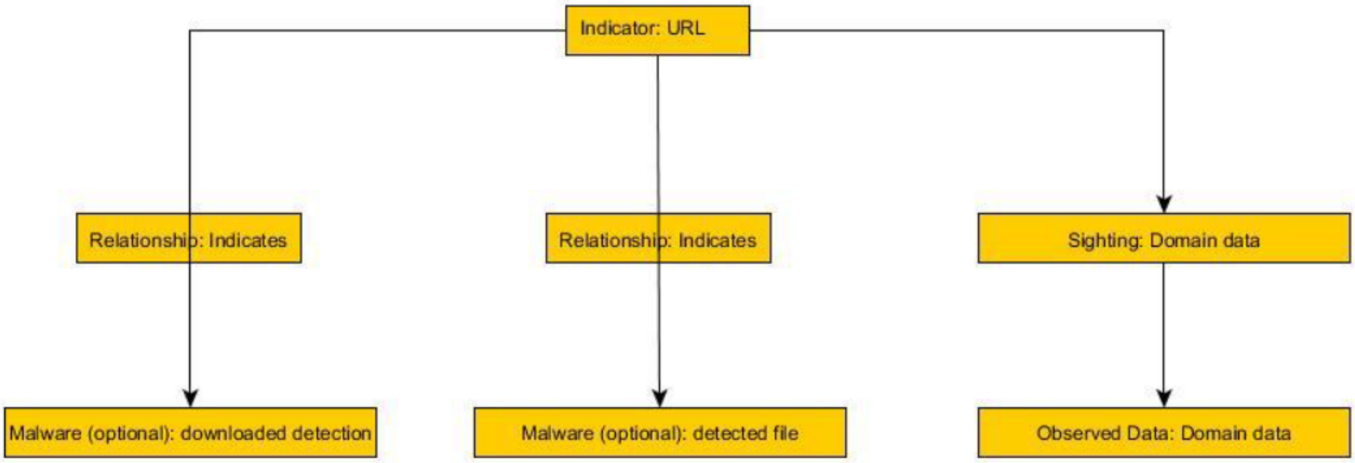
STIX 2.0

Below is a snippet of an URL feed in JSON format.

```
{
 "type": "indicator",
 "id": "indicator--d0a27e9b-7f72-4587-95a0-173634a27a25",
 "created": "2020-10-22T11:56:16.000Z",
 "modified": "2020-10-22T11:56:16.000Z",
 "name": "Blocked",
 "description": "Host is used as command and control server of MSIL/Kryptik.MSS trojan malware family.",
 "pattern": "[url:value='http://bejnz.com/IP.php']",
 "valid_from": "2020-10-22T11:56:16Z",
 "valid_until": "2020-10-24T11:56:16Z",
 "labels": [
         "malicious-activity"
 ]
}
```

The following types of STIX domain objects available for the URL feed:

- **Indicator**—An Indicator of Comprise (IoC) to use for further blocking or investigation.
- **Observed data**—Extra information about the given domain.
- **Malware**—An optional object shared with every domain IoC if a malicious file downloaded from the given domain is detected and blocked.
- **Sighting**—Additional data about the domain hosting the URL. This object is always associated with Observed data, which provides more information about the domain.
- **Relationship**:


Indicator: URL
Relationship: Indicates
Relationship: Indicates
Sighting: Domain data
Malware (optional): downloaded detection
Malware (optional): detected file
Observed Data: Domain data

IP feed

The IP feed contains malicious IP addresses and data associated with them. The structure of the data displayed here is similar to the display of domains in URL feed. One of the main uses is to understand what malicious IP addresses are currently prevalent in the wild. To block those IP addresses with high severity and monitor those IP addresses with milder severity, and to further investigate based on additional information in case they have already caused any harm.

JSON

Below is a snippet of an IP feed in JSON format.

```
{
"confidence": "Low",
"direction": "outgoing",
"downloaded.detection": [
"URL/Urlik.AAF object",
"VBS/Agent.OMW trojan"
],
"ip": "87.244.43.42"
"location": "Russian Federation",
"opener_detection": [
"URL/Urlik.AAF object"
]
"port": 11985
"protocol": "tcp"
"reason": "Host actively distributes high-severity threat in the form of executable code.",
"state": "BlockedObject",
"urls": [
"https://87.244.43.42:11985/08388E25.Png"
],
"valid_to": "2021-12-15 09:35:10 UTC"
}
```

- **Confidence**- How confident we are that the given IP address should be automatically blocked
  - **High** - consists of IP address that have shown malicious and phishing activities
  - **Medium** - consists of IP address that have shown potentially unwanted (PUA) or SCAM activities
  - **Low** - consists of IP address from which users are advised not to download files, but which are considered safe to browse
- **Direction -** Considered from client perspective. In case IP address is communicating with customer/application it is incoming. In case customer/application is asking IP address, it is outgoing.
  - **Outgoing** or **Incoming**
- **Downloaded detection**: detection of file that would be downloaded from the given malicious IP address
- **IP**: main IoC itself.
- **Location**: country where the IP address is hosted (IP address to location)
- **Opener detection**: in cases where a malicious file tries to communicate with an IP address, this is the detection of the file which was trying to access the given IP address.
- **Port**: port communicated number
- **Protocol**: network communication protocol
- **Reason**: human-readable information about why the given domain has been identified as malicious
  - The host is actively distributing high-severity malicious content in the form of executable code.

  - The host is actively distributing a high-severity threat in the form of executable code.
  - The host is actively distributing a high-severity threat in the form of script code.
  - The host is actively distributing a high-severity threat in the form of malicious code.
  - The host is actively distributing a potentially unwanted or unsafe threat.
  - The host is known to be a source of active fraudulent content.
  - The host is known to be a source of phishing or other fraudulent content.
  - The host is known to abuse search engine optimization features to distribute unwanted content and spam.
  - The host is known to be actively distributing high-severity mobile threats or low-risk software.
  - The host is known to be actively distributing threats or is of uncertain reputation.
  - The host is known to be actively distributing adware or other medium-risk software.
  - The host is known to be distributing low-risk and potentially unwanted content.
  - The host is used as a command and control server by the {} malware family.
  - The host is used as a command and control server.
  - VNS bruteforce IP
  - RDP bruteforce IP
  - SQL bruteforce IP
  - SMB bruteforce IP
  - FTP bruteforce IP
  - Web services scanning and attacks
- **State**: what kind of category the given malicious IP address is in:
  - **Blocked** – IP address that shows malicious activity (high confidence)
  - **Unwanted** – IP address that is considered a PUA or SCAM (medium confidence)
  - **Blocked Object** – IP address that hosts downloadable malware but should not be blocked as a whole (low confidence)
- **URLs**: bad URLs we have seen on given IP
- **Valid to**: date of share +48h

STIX 2.0

4 types of STIX domain objects are available for **IP feed**:

- **Indicator**
- **Malware**
- **Observed data**
- **Relationship**

- **Indicator** - IoC that should be used for further blocking and/or investigation
    - **Name**: what category the given malicious IP address belongs to
        - **Blocked** – IP address that shows malicious activity (high confidence)
        - **Unwanted** – IP address that is considered a PUA or SCAM (medium confidence)
        - **Blocked Object** – IP address that hosts downloadable malware but should not be blocked as a whole (low confidence)
    - **Description**: Human-readable information about why the given IP address has been identified as malicious
    - **Pattern**: IoC
    - **Valid from**: time of share of IoC
    - **Valid until**: time of share +48h
    - **Label**: category of detection in a format different than name
        - **Malicious activity** (name - Blocked)
        - **Benign** (name – Blocked Object)
- **Malware** - this object is optional and does not necessarily need to be shared with every IP address IoC. In the event that we

have been able to detect and block a file related to malware that was downloaded from a given IP address, this data will be

shared. In the event that malware was trying to communicate with a given IP address, data about the malware that tried to

communicate will be shared.

- **Name**: name of the malware detection
- **Description**: what type of malware-based additional information this is
    - Detected malware was downloaded from the IP address

        - Detected malware tried to contact the IP address

    - **Labels**: what category of malware this is

        - Trojan
        - Worm
        - Virus
        - Dropper
        - Adware
        - Rogue security software
        - Ransomware
        - Keylogger
        - Rootkit
        - DDoS
        - Bot
        - Spyware

- **Observed data** - additional information for the given domain

    - **First observed**: when was this IP address first seen in the wild
    - **Last observed**: when the IP address was last seen
    - **Number observed**: the total number of times the IP address has been seen
    - **Type**: ipv4 or URL
    - **Value**: the IP address on which the blocked URL is hosted

- **Relationship**

APT feed

APT feed consists of information about **Advanced Persistent Threats** that are outcome from **ESET research**. This feed is an export from **ESET internal MISP server**. All the data that are shared are also in more detailed explained in **APT reports**. **APT feed** is also part of APT reports offering, however, the feed can also be purchased separately.

JSON

Below is a snippet of an APT feed in JSON format.

```
"Attribute": [
{
"Galaxy": [],
"ShadowAttribute": [],
"category": "Network activity", "comment": "",
"deleted": false,
"disable_correlation": false,
"distribution": "5",
"event_id": "282",
"first_seen": "2022-01-28T08:42:57.000000+00:00",
"id": "143094",
"last_seen": null, "object_id": "59977",
"object_relation": "domain", "sharing_group_id": "0",
"timestamp": "1643710782",
"to ids": false,
"type": "domain",
"uuid":
"21b993a3-fd4a-4ab1-8a3f-1f5d45db7577",
"value": "corolain.ru"
}
],
"ObjectReference": [],
"comment": "",
"deleted": false,
"description": "A domain/hostname and IP address seen as a tuple in a specific time frame.", "distribution": "5",
"event_id": "282",
"first_seen": "2022-01-25T14:11:03.000000+00:00",
"id": "59977",
"last_seen": null,
"meta-category": "network",
"name": "domain-ip",
"sharing_group_id": "0",
"template_uuid": "43b3b146-77eb-4931-b4cc-b66c60f28734",
"template_version":"10",
"timestamp": "1643730789",
"uuid":"a9e5bc0d-eb8f-455d-8e62-c3930fa2447d"
```

STIX 2.0

Standard STIX2 export from MISP.

- File is the main IoC and all the other objects are connected to this main IoC. Currently used attributes for this indicator are:
  - Filename
  - MD5, SHA1 and SHA256 file hash (IDS flag) as main IoCs
  - Comment
- **Detected as** gives information about what is the object detected as by ESET. In some cases here can be multiple detections. Available attributes are:

    - Software (always ESET)
    - Signature (IDS flag) as main IoC

- **Includes** gives additional information, which however do not have to be always present. Available attributes are:
    - PE file or macho file or elf file
    - Type of file indication
    - Compilation date
    - Imphash
    - And potentially additional metadata

- **Connected to** objects bring additional information about network and it’s IoCs. Each of the objects (URL, domain, IP) can be available separately, or also all at the same time.
    - **URL**
        - URL (IDS flag) as main IoC
        - Scheme
        - Query string
        - Resource path
        - Port
        - Comment
    - **Domain**
        - Domain as main IoC
        - Comment
    - **IP**
        - IP address as main IoC
        - Comment

- **Dropped by file** object is available only sometimes. This is available in case the given main file also either drops or downloads an additional file. Available attributes are:
    - Filename
    - MD5, SHA1 and SHA256 file hash (IDS flag) as main IoCs
    - Comment

- **Downloaded from URL** object with it’s acompying objects are available only sometimes. This is available in case there is a trace from which URL given file has been downloaded. Available attributes are:

  oURL

  ▪URL (IDS flag) as main IoC

  ▪Scheme

  ▪Query string

  ▪Resource path

  ▪Port

  ▪Comment

  oDomain

  ▪Domain as main IoC

  ▪Comment

  oIP

  ▪IP address as main IoC

  ▪Comment

API

The API offers another way to access the ESET Threat Intelligence (ETI) portal. To help you begin using the API, we have written a sample API script in python. Download and extract the script, and then open it in a simple text editor for further instructions.

Usage of our API does not necessarily require implementation in a programming language. The API can be used directly in the address bar of a browser as a REST API. In the syntax description below `ETI_URL` stands for the URL address leading to the ETI portal.

Authentication is ensured via a token generated in the profile section. Each token is valid for only one hour for security reasons. A token can also be generated using a CURL request:

```
✓ curl -F name="YOUR-USERNAME" -F pass="YOUR-PASSWORD" ETI_URL/auth/
```

Authentication limits

If the authentication fails 10 times within 5 minutes due to a wrong password provided, the user trying to authenticate will be blocked for 15 minutes.
If the authentication fails 20 times within 5 minutes from a certain IP address due to wrong username and/or password, any authentication attempt from the particular IP address within 15 minutes will be blocked.

To view reports via the REST API, use the following syntax:

```
ETI_URL/reports/[all|sample|targeted|botnet|phish]/api
```

Values in brackets ("[" and "]") represent the desired report type. Only use a single report type in your request.

Mandatory POST parameter:

- `auth` - represents the token you generated.

Optional GET parameters:

- `pid` - represents a time period. Its values can be: 24h, 48h, 1w, 2w
- `oid` - represents the owner ID.
- `gid` - represents the group ID.
- `datetimefrom` - represents the beginning of date range the report was updated/generated in (2017-07-18%2009:34:51 or 2017-07-18 09:34:51 or 2017-07-18).
- datetimeto - represents the end of date range the report was updated/generated in (2017-07-18%2009:34:51 or 2017-07-18 09:34:51 or 2017-07-18).
- `idfrom` - represents the report ID.
- `idto` - represents the report ID.

Retrieve XML content, or short details of a certain report:

```
ETI_URL/reports/REPORT-ID/[xml|detail]/api
```

Mandatory POST parameter:

- `auth` - represents the token you generated.

Retrieve reports by type:

```
ETI_URL/reports/[all|sample|targeted|botnet|phish]/api
```

Retrieve XML or PDF content, additional data or short details of a certain report:

```
ETI_URL/reports/REPORT-ID/[xml|pdf|adds|detail]/api
```

`REPORT-ID` represents the report ID.

The `pdf` version works only for reports with `finished` status.

To read YARA matches via the REST API, use the following syntax:

```
ETI_URL/ymatches/all/api
```

Optional GET parameters:

- `tid` - represents a time period. Values can be: 24h, 48h, 1w, 2w
- `rid` - represents a ruleset ID. It can be retrieved from the xml output of a Rest API call from the `<filter name="rid"> ...</filter>` block, where the ID and name of each rule is listed as `<info name="123">Test rule</info>`, where '123' is the rule ID.
- `rst` - can be used to list matches marked read or unread. Available values are "0" (lists all matches), "1" (lists only matches marked as unread), and "2" (lists only matches marked as read). The values are used without quotation marks.
- `detail` - used to retrieve a certain match by its ID. Match ID can be found in the `<info name="yara_match_id">` field of the xml output of a REST API call.
- `rsst` - can be used to list matches based on their status. Available values are "0" (list all matches), "1" (list only new matches) and "2" (list only updated matches).
- `owner` - can be used to list matches by owner.
- `gread` - used to retrieve matches for groups that have only read access to corresponding ruleset.
- `gwrite` - used to retrieve matches for groups that have write access to corresponding ruleset.
- `datetimefrom` - represents the beginning of date range of **Last match**(2017-07-18%2009:34:51 or 2017-07-18 09:34:51 or 2017-07-18).
- datetimeto - represents the end of date range of **Last match** (2017-07-18%2009:34:51 or 2017-07-18 09:34:51 or 2017-07-18).
- `idfrom` - represents the match ID.
- `idto` - represents the match ID.

Generate a report from a YARA match:

```
ETI_URL/ymatches/report/MATCH-ID/auth/YOUR-TOKEN
```

Preview details of a YARA match:

```
ETI_URL/ymatches/[detail|read|unread]/MATCH-ID/api
```

Edit note of a YARA match:

```
ETI_URL/ymatches/detail/MATCH-ID/auth/YOUR-TOKEN?setnote=NOTE
```

or send the new note as the value of `setnote` POST parameter.

To upload a suspicious sample file, use the following CURL request:

```
curl -X POST -H "Content-Type: multipart/form-data" -F "sample_file"=@file.txt ETI_URL/reports/add-file/auth/YOUR-TOKEN
```

where `file.txt` is the name of the file to be uploaded.

To upload a suspicious sample by hash, either use the following REST API syntax:

```
ETI_URL/reports/add-hash/auth/YOUR-TOKEN?&hash=HASH
```

or the following CURL request:

```
curl -X POST -F "hash"="HASH" ETI_URL/reports/add-hash/auth/YOUR-TOKEN
```

where `HASH` is the hash (MD5, SHA1 or SHA256) of the sample to be uploaded.

Profile

In the **Profile** section you can change your password, select the frequency of email notifications, or generate a token for API use. If email notifications are turned on, you will receive a notification about each generated report, except for botnet reports.

To access the profile section, click your name in the top-right corner of the portal.

Limited features

The following features are limited to specific countries:

- Reports
- Yara rules
- Yara matches

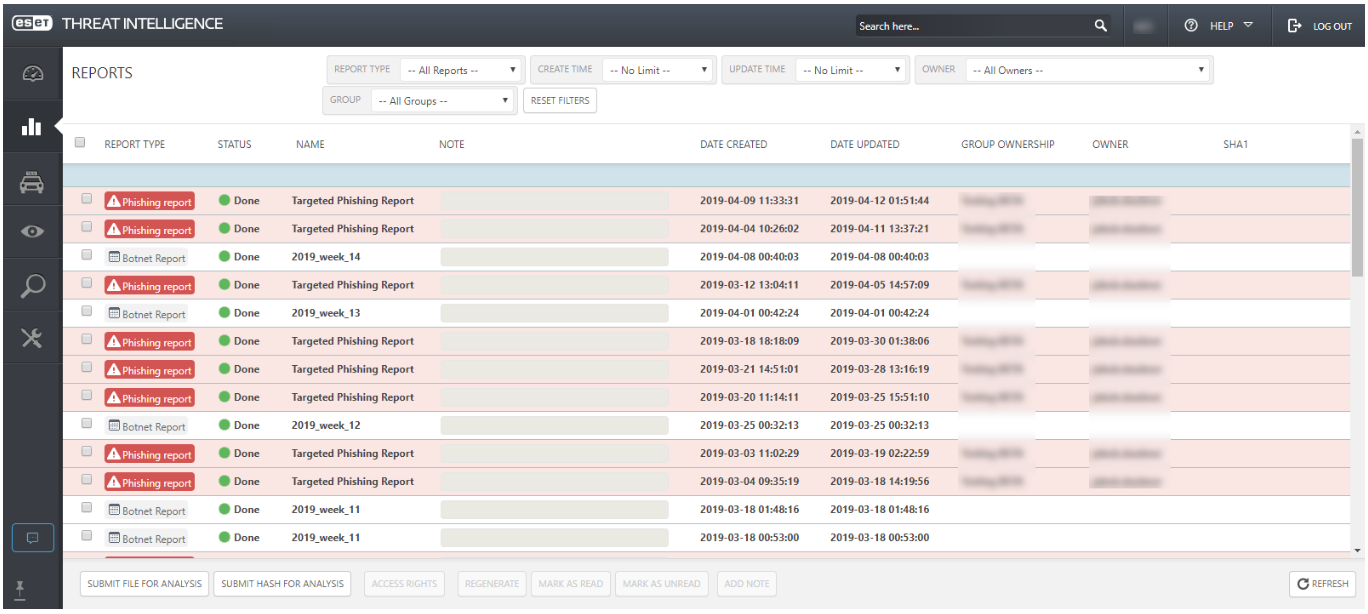
For more information, fill in the contact form.

Reports

The **Reports** screen displays **Botnet reports** by default. Use the **All Reports** drop-down menu to select a report type.

Users from the same company, who have access to ESET Threat Intelligence portal, can filter reports per colleague using the **Owner** list box. If you manage **Early Warning** for several companies, use the **Group** list box to see reports per company. Use the search bar for a full-text search.

> ### Search
> If you type into the search bar "www.eset.com" (without quotation marks), the exact sought string can be found in the *.xml* file of the search result. In the *.pdf* file of the search result, the first occurrence of the dot in an URL address is replaced with "[dot]" (without quotation marks).



REPORTS

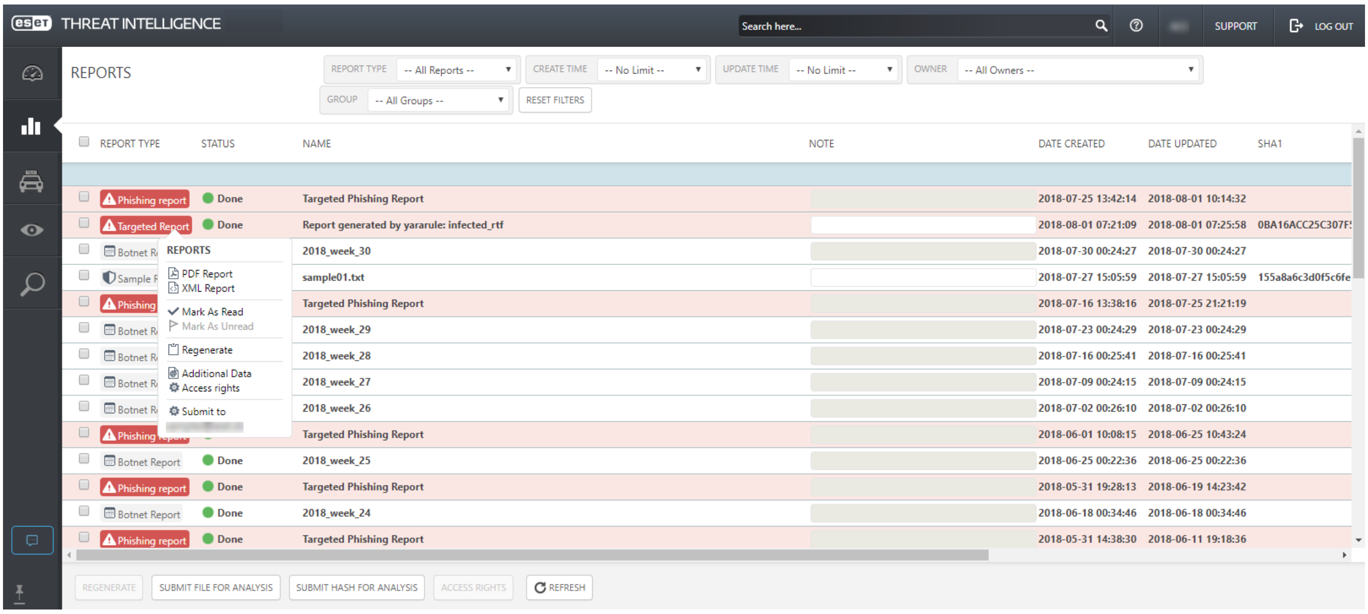
REPORT TYPE: -- All Reports -- | CREATE TIME: -- No Limit -- | UPDATE TIME: -- No Limit -- | OWNER: -- All Owners --

GROUP: -- All Groups -- | RESET FILTERS

□	REPORT TYPE	STATUS	NAME	NOTE	DATE CREATED	DATE UPDATED	GROUP OWNERSHIP	OWNER	SHA1
□	Phishing report	● Done	Targeted Phishing Report		2019-04-09 11:33:31	2019-04-12 01:51:44	[redacted]	[redacted]	
□	Phishing report	● Done	Targeted Phishing Report		2019-04-04 10:26:02	2019-04-11 13:37:21	[redacted]	[redacted]	
□	Botnet Report	● Done	2019_week_14		2019-04-08 00:40:03	2019-04-08 00:40:03			
□	Phishing report	● Done	Targeted Phishing Report		2019-03-12 13:04:11	2019-04-05 14:57:09	[redacted]	[redacted]	
□	Botnet Report	● Done	2019_week_13		2019-04-01 00:42:24	2019-04-01 00:42:24			
□	Phishing report	● Done	Targeted Phishing Report		2019-03-18 18:18:09	2019-03-30 01:38:06	[redacted]	[redacted]	
□	Phishing report	● Done	Targeted Phishing Report		2019-03-21 14:51:01	2019-03-28 13:16:19	[redacted]	[redacted]	
□	Phishing report	● Done	Targeted Phishing Report		2019-03-20 11:14:11	2019-03-25 15:51:10	[redacted]	[redacted]	
□	Botnet Report	● Done	2019_week_12		2019-03-25 00:32:13	2019-03-25 00:32:13			
□	Phishing report	● Done	Targeted Phishing Report		2019-03-03 11:02:29	2019-03-19 02:22:59	[redacted]	[redacted]	
□	Phishing report	● Done	Targeted Phishing Report		2019-03-04 09:35:19	2019-03-18 14:19:56	[redacted]	[redacted]	
□	Botnet Report	● Done	2019_week_11		2019-03-18 01:48:16	2019-03-18 01:48:16			
□	Botnet Report	● Done	2019_week_11		2019-03-18 00:53:00	2019-03-18 00:53:00			

When a new **Targeted report** or **Certificate report** is generated, an email notification is sent to you. For both reports, you can add notes using the **Note** field.

Select a report and click **PDF Report** or **XML Report** to view the details of the report. Instructions to download and open the attachment (**Additional data**) are included at the end of all PDF reports.



REPORTS

REPORT TYPE: -- All Reports -- | CREATE TIME: -- No Limit -- | UPDATE TIME: -- No Limit -- | OWNER: -- All Owners --

GROUP: -- All Groups -- | RESET FILTERS

□	REPORT TYPE	STATUS	NAME	NOTE	DATE CREATED	DATE UPDATED	SHA1
□	Phishing report	● Done	Targeted Phishing Report		2018-07-25 13:42:14	2018-08-01 10:14:32	
□	Targeted Report	● Done	Report generated by yararule: infected_rtf		2018-08-01 07:21:09	2018-08-01 07:25:58	0BA16ACC25C307F!
□	Botnet R		2018_week_30		2018-07-30 00:24:27	2018-07-30 00:24:27	
□	Sample F		sample01.txt		2018-07-27 15:05:59	2018-07-27 15:05:59	155a8a6c3d0f5c6fe
□	Phishing		Targeted Phishing Report		2018-07-16 13:38:16	2018-07-25 21:21:19	
□	Botnet R		2018_week_29		2018-07-23 00:24:29	2018-07-23 00:24:29	
□	Botnet R		2018_week_28		2018-07-16 00:25:41	2018-07-16 00:25:41	
□	Botnet R		2018_week_27		2018-07-09 00:24:15	2018-07-09 00:24:15	
□	Botnet R		2018_week_26		2018-07-02 00:26:10	2018-07-02 00:26:10	
□	Phishing report		Targeted Phishing Report		2018-06-01 10:08:15	2018-06-25 10:43:24	
□	Botnet Report	● Done	2018_week_25		2018-06-25 00:22:36	2018-06-25 00:22:36	
□	Phishing report	● Done	Targeted Phishing Report		2018-05-31 19:28:13	2018-06-19 14:23:42	
□	Botnet Report	● Done	2018_week_24		2018-06-18 00:34:46	2018-06-18 00:34:46	
□	Phishing report	● Done	Targeted Phishing Report		2018-05-31 14:38:30	2018-06-11 19:18:36	

Sample reports allow you to report any suspicious samples (files, hashes) to ESET for further analysis.

> ### Report status
> Sample report statuses:
> - **In progress**—analysis of the reported sample is incomplete
> - **Done**—analysis of the reported sample is complete
> - **File not found**—ESET could not identify any file based on the hash submitted for analysis. In this case, submit the file the hash belongs to for analysis.

> ### Report access rights
> If you manage **Early Warning** for several companies, share your generated reports (for example, Targeted reports, Certificate reports, Sample reports) with any of the companies.
> 1. In the **Reports** screen, click the appropriate report.
> 2. Select **Access Rights**.
> 3. In the **Select Group** drop-down menu, select the applicable company.
> 4. Click **Update Report**.
>
> If you select a different owner from **Select User** drop-down menu, you will not be able to see the report anymore.

Botnet reports

Botnet activity report brings regular reporting and quantitative data about the identified malware families and variants of botnet malware, which are being monitored as part of ESET Threat Intelligence. Classified according to malware type, the report provides a list of known Command and Control servers involved in botnet management, as well as a list of targets of this malware.

These reports are regularly generated on weekly basis and all past reports are displayed. There is no email notification when a new report is generated. Select a report and click **PDF Report** to view the details of the report.

Targeted reports

To see **Targeted Reports**, configure the corresponding Yara rules. Each time new information flows into the system, the rule set will be applied to it. If information matches, it is analyzed by ESET lab. If it is not a false positive, a new **Targeted report** is generated, and an email notification is sent to you. You can add notes using the **Note** field.

Certificate reports

Whenever ESET detects that a new SSL certificate matching your Yara rule has been released, a report is generated in the Yara matches section. Detecting a new SSL certificate may indicate the start of a potential phishing campaign that links to a phishing website.

The report is analyzed by ESET lab, and if it is not a false positive, a new **Certificate report** is generated in the **Reports** screen. You can add notes using the **Note** field.

Source of new SSL certificates: Certificate Transparency

Phishing reports

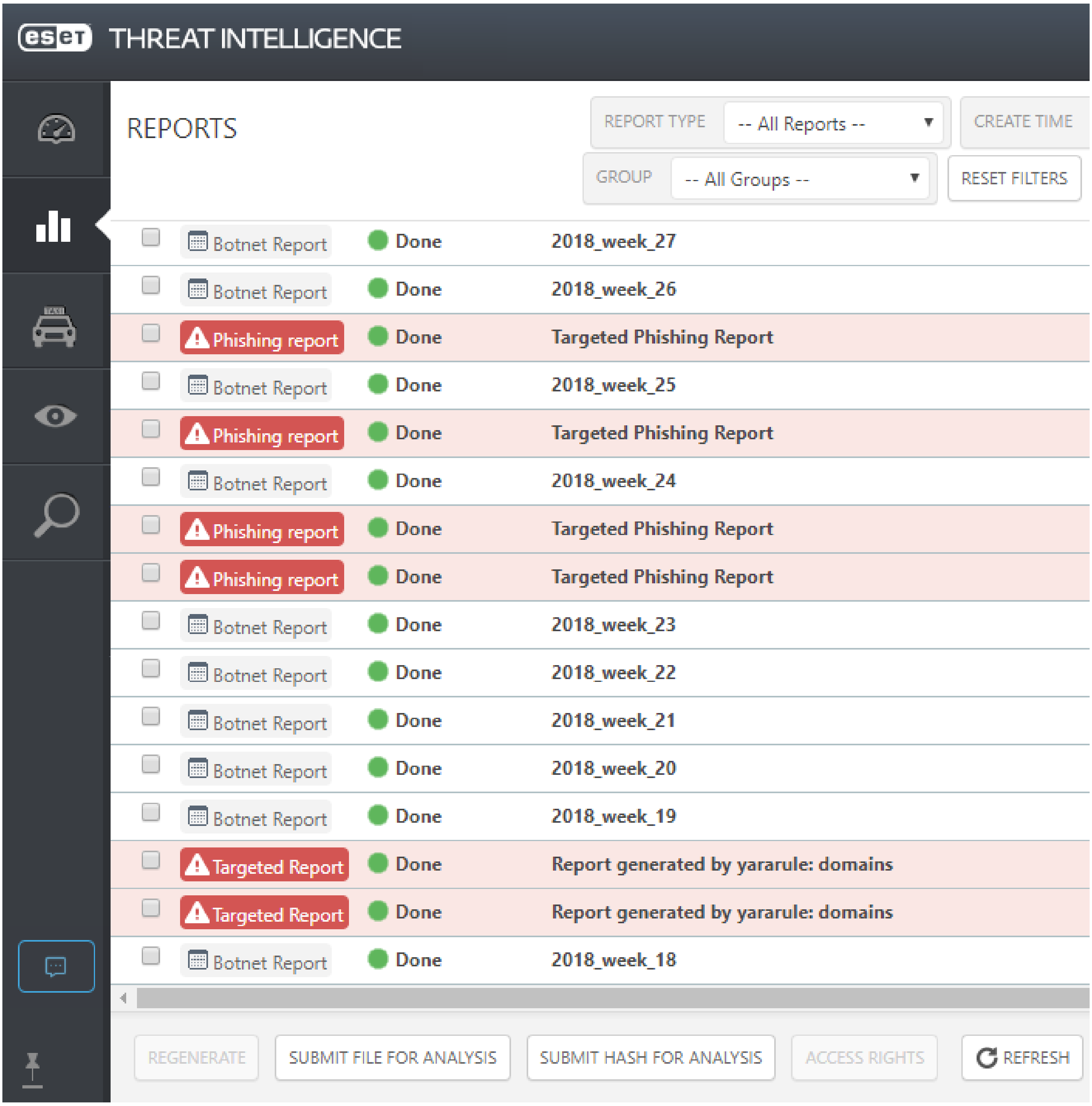
Phishing reports can be activated upon personal request. An email notification is sent to you whenever a new phishing report is generated. You can select the type of phishing reports for which you want to receive email notifications: Full report, New URLs only, or both.

You can also filter these reports by the time of update.

Sample reports

Follow the steps below to report a suspicious sample:

1. In the **Reports** screen, click **Submit File For Analysis**.

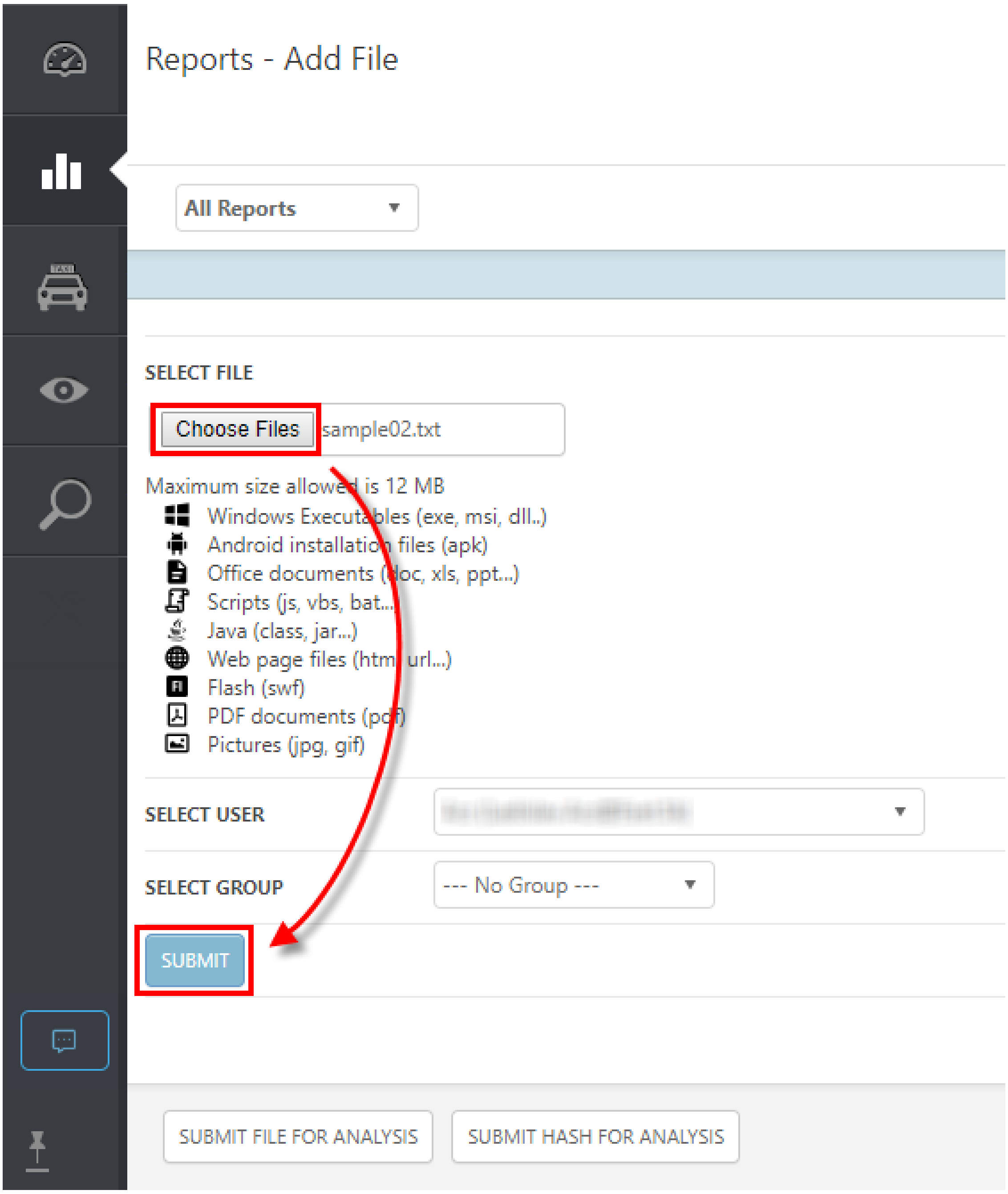


REPORT TYPE: -- All Reports --

GROUP: -- All Groups --

□	Botnet Report	● Done	2018_week_27
□	Botnet Report	● Done	2018_week_26
□	Phishing report	● Done	Targeted Phishing Report
□	Botnet Report	● Done	2018_week_25
□	Phishing report	● Done	Targeted Phishing Report
□	Botnet Report	● Done	2018_week_24
□	Phishing report	● Done	Targeted Phishing Report
□	Phishing report	● Done	Targeted Phishing Report
□	Botnet Report	● Done	2018_week_23
□	Botnet Report	● Done	2018_week_22
□	Botnet Report	● Done	2018_week_21
□	Botnet Report	● Done	2018_week_20
□	Botnet Report	● Done	2018_week_19
□	Targeted Report	● Done	Report generated by yararule: domains
□	Targeted Report	● Done	Report generated by yararule: domains
□	Botnet Report	● Done	2018_week_18

2. Click **Choose Files**, browse to the sample file, double click it and then click **Submit**.



Reports - Add File

All Reports ▾

SELECT FILE

Choose Files sample02.txt

Maximum size allowed is 12 MB

- Windows Executables (exe, msi, dll..)
- Android installation files (apk)
- Office documents (doc, xls, ppt...)
- Scripts (js, vbs, bat...)
- Java (class, jar...)
- Web page files (html, url...)
- Flash (swf)
- PDF documents (pdf)
- Pictures (jpg, gif)

SELECT USER [redacted] ▾

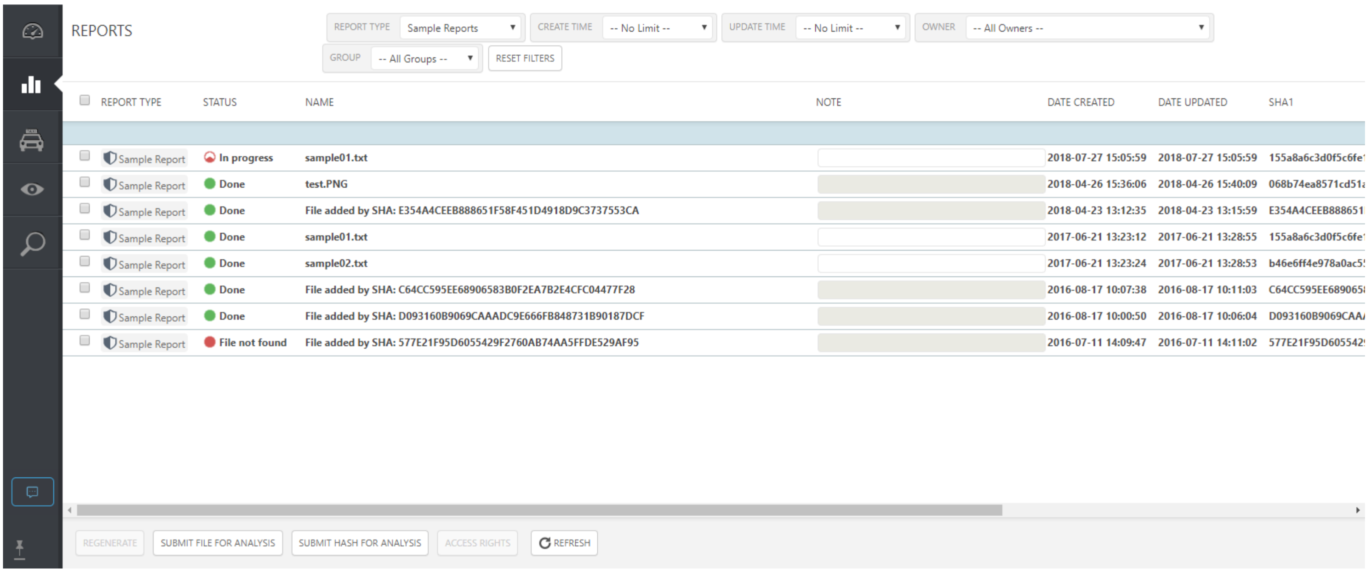
SELECT GROUP --- No Group --- ▾

SUBMIT

SUBMIT FILE FOR ANALYSIS

SUBMIT HASH FOR ANALYSIS

3. The uploaded sample file will be shown in the **Reports** screen when **Sample Reports** is selected.



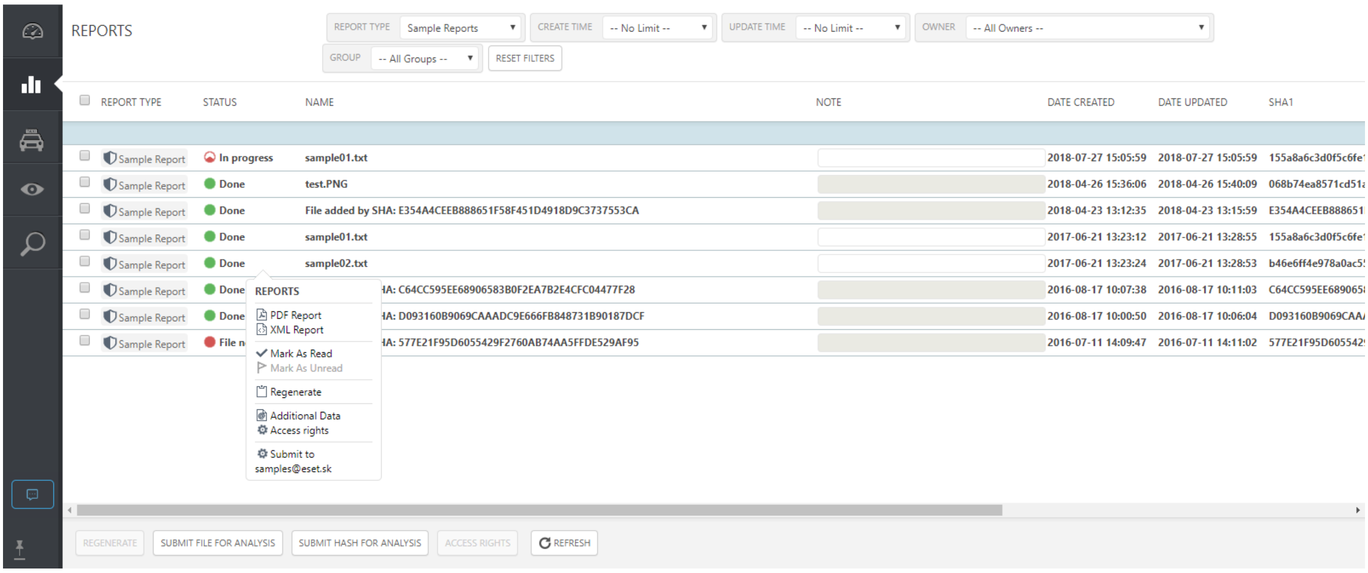
REPORTS

REPORT TYPE: Sample Reports | CREATE TIME: -- No Limit -- | UPDATE TIME: -- No Limit -- | OWNER: -- All Owners --

GROUP: -- All Groups --

□	REPORT TYPE	STATUS	NAME	NOTE	DATE CREATED	DATE UPDATED	SHA1
□	Sample Report	In progress	sample01.txt		2018-07-27 15:05:59	2018-07-27 15:05:59	155a8a6c3d0f5c6fe
□	Sample Report	● Done	test.PNG		2018-04-26 15:36:06	2018-04-26 15:40:09	068b74ea8571cd51
□	Sample Report	● Done	File added by SHA: E354A4CEEB888651F58F451D4918D9C3737553CA		2018-04-23 13:12:35	2018-04-23 13:15:59	E354A4CEEB888651
□	Sample Report	● Done	sample01.txt		2017-06-21 13:23:12	2017-06-21 13:28:55	155a8a6c3d0f5c6fe
□	Sample Report	● Done	sample02.txt		2017-06-21 13:23:24	2017-06-21 13:28:53	b46e6ff4e978a0ac5
□	Sample Report	● Done	File added by SHA: C64CC595EE68906583B0F2EA7B2E4CFC04477F28		2016-08-17 10:07:38	2016-08-17 10:11:03	C64CC595EE689065
□	Sample Report	● Done	File added by SHA: D093160B9069CAAADC9E666FB848731B90187DCF		2016-08-17 10:00:50	2016-08-17 10:06:04	D093160B9069CAA
□	Sample Report	● File not found	File added by SHA: 577E21F95D6055429F2760AB74AA5FFDE529AF95		2016-07-11 14:09:47	2016-07-11 14:11:02	577E21F95D605542

4.Once the submitted sample file is analyzed, you can download the results of the analysis as a *pdf* or *xml* document. Instructions to download and open the attachment (**Additional data**) are included at the end of all PDF reports.



REPORTS

REPORT TYPE: Sample Reports | CREATE TIME: -- No Limit -- | UPDATE TIME: -- No Limit -- | OWNER: -- All Owners --

GROUP: -- All Groups --

□	REPORT TYPE	STATUS	NAME	NOTE	DATE CREATED	DATE UPDATED	SHA1
□	Sample Report	In progress	sample01.txt		2018-07-27 15:05:59	2018-07-27 15:05:59	155a8a6c3d0f5c6fe
□	Sample Report	● Done	test.PNG		2018-04-26 15:36:06	2018-04-26 15:40:09	068b74ea8571cd51
□	Sample Report	● Done	File added by SHA: E354A4CEEB888651F58F451D4918D9C3737553CA		2018-04-23 13:12:35	2018-04-23 13:15:59	E354A4CEEB888651
□	Sample Report	● Done	sample01.txt		2017-06-21 13:23:12	2017-06-21 13:28:55	155a8a6c3d0f5c6fe
□	Sample Report	● Done	sample02.txt		2017-06-21 13:23:24	2017-06-21 13:28:53	b46e6ff4e978a0ac5
□	Sample Report	● Done	HA: C64CC595EE68906583B0F2EA7B2E4CFC04477F28		2016-08-17 10:07:38	2016-08-17 10:11:03	C64CC595EE689065
□	Sample Report	● Done	HA: D093160B9069CAAADC9E666FB848731B90187DCF		2016-08-17 10:00:50	2016-08-17 10:06:04	D093160B9069CAA
□	Sample Report	● File n	HA: 577E21F95D6055429F2760AB74AA5FFDE529AF95		2016-07-11 14:09:47	2016-07-11 14:11:02	577E21F95D605542

To report a suspicious hash, click **Submit Hash For Analysis** and follow the on-screen instructions.

The following types of files can be analyzed:

- Windows Executables (exe, dll…)
- Android application installation files (apk)
- Office documents (doc, xls, ppt…)
- Scripts (js, vbs, bat…)
- Java (class, jar…)
- Web page files (htm, URL…)

- Flash (swf)
- PDF documents (pdf)
- Pictures (jpg, gif)

A Sample Report provides the following information:

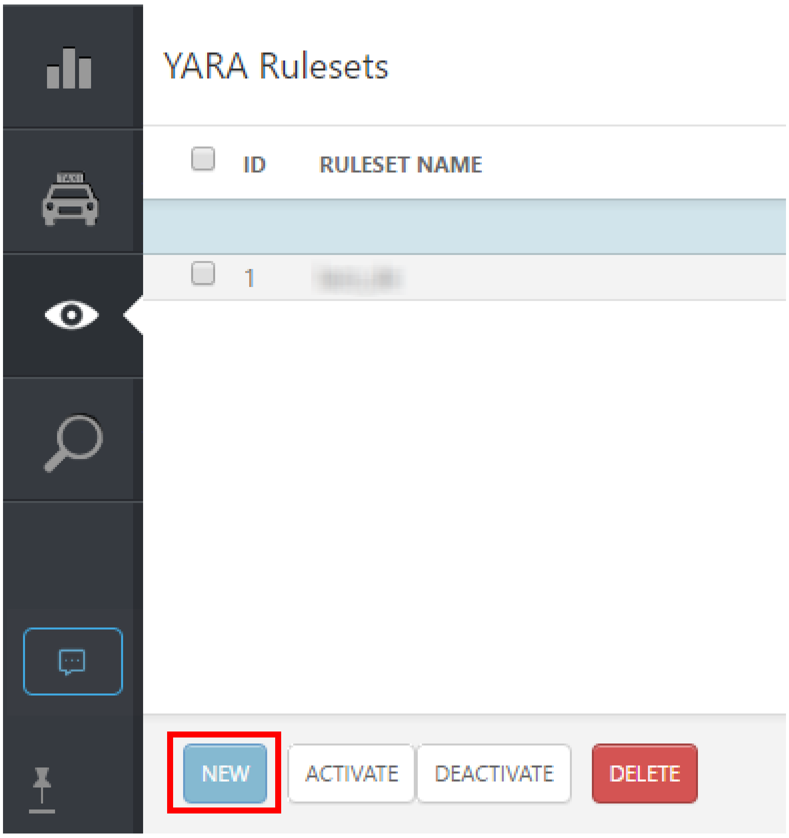
- Detailed detection information—Name of given malicious file in competing security solutions that also detected the file.
- Reputation information from ESET LiveGrid®
  - How frequently the file was seen in the world and in the country the report was requested from
  - When it was first seen and last seen in the world
- Similar binaries—Existence of similar files based on DNA Detection.
- File details
  - Name, type, size, MD5, SHA1, SHA256 and Signature
  - PE Information—Machine, Timestamp, Mafic Optional Header, Entry Point, Subsystem, OS Version, Subsystem Version, Linker Version, Image Version, Number of Sections and Sections.
- Sandbox output
  - File system changes with Size and SHA1 information
  - Registry changes with Type of change and Value of change
  - Network communication with Type of communication, IP Address and Location it communicated with and PDNS value
  - Processes with Time the process started, PID value, Parent value and Name

Yara rules

> Function availability based on the service level of subscription
>
> Access to this functionality is dependent on the service level of your subscription. Not all functionality described in this topic is available to all users.

To see **Targeted Reports**, configure the corresponding Yara rules.
Typically, we configure Yara rules and generate targeted reports based on subscriber requirements and the service levels. See our step-by-step instructions below to create a new Yara Ruleset.

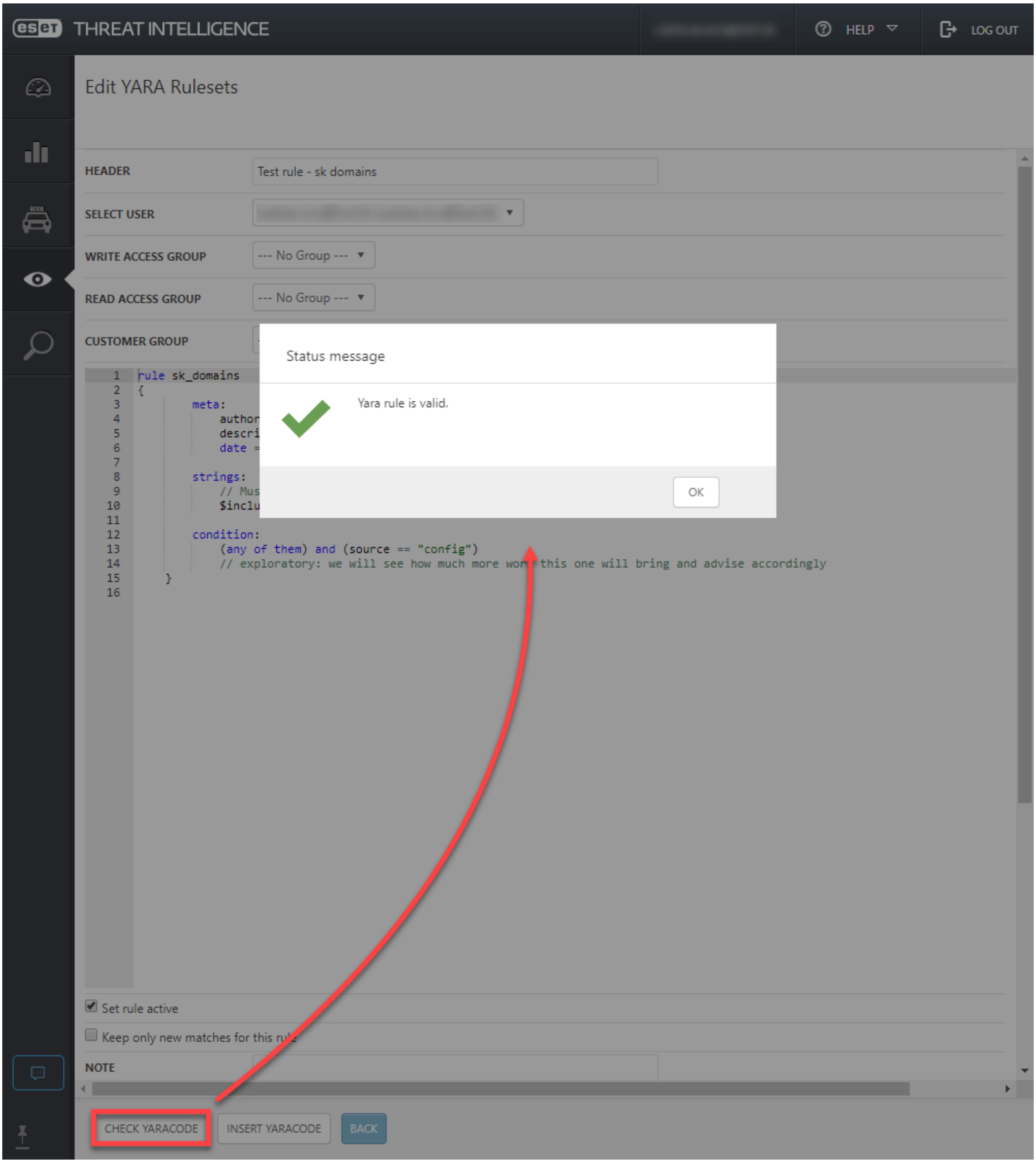
1. Click **New** in the **Yara Rulesets** screen.



YARA Rulesets

□	ID	RULESET NAME
□	1	[redacted]

2. Name the rule, define the rule in the **Rules** field and then click **Check Yara Code** to make sure the code is valid according to official Yara rules documentation.
The content of the **NOTE** field will show up in each Targeted report generated for a particular rule.



Edit YARA Rulesets

HEADER Test rule - sk domains

SELECT USER [redacted]

WRITE ACCESS GROUP --- No Group ---

READ ACCESS GROUP --- No Group ---

CUSTOMER GROUP

```
rule sk_domains
{
        meta:
            author
            descri
            date =

        strings:
            // Mus
            $inclu

        condition:
            (any of them) and (source == "config")
            // exploratory: we will see how much more wor  this one will bring and advise accordingly
    }

```

Status message

Yara rule is valid.

☑ Set rule active

☐ Keep only new matches for this rule

NOTE

3. If the code is valid, click **Insert Yara Code**.

Each time new information flows into the system, the rule set will be applied to it. If information matches a rule, the last matched date/time will be updated in the Yara matches section.

You can deactivate or delete unnecessary rule sets.

Pre-configured Yara rules

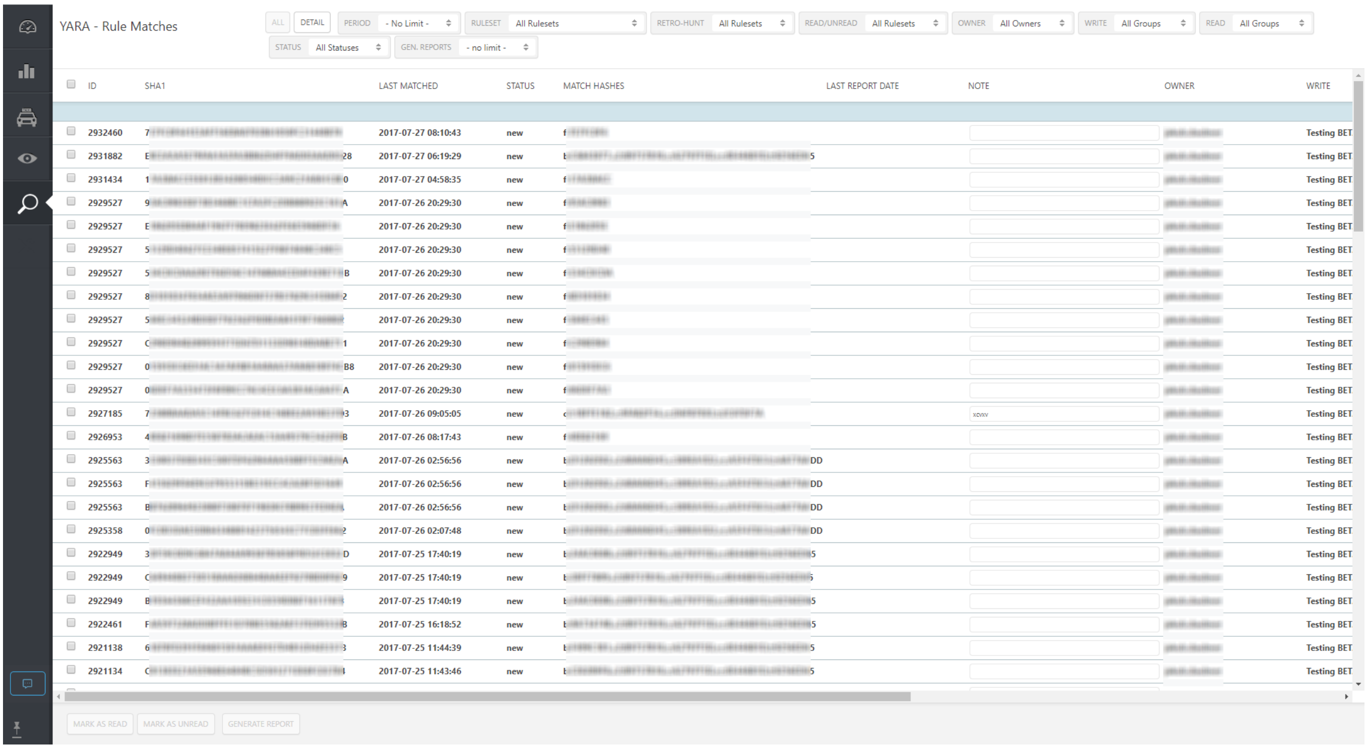
Yara rules configured by the ESET Threat Intelligence team based on the submitted "registration form / subscriber requirements" are not visible to users by default. Customers can request the "Yara rules visibility" feature through the support form. The rules then will be displayed in read-only mode. To edit pre-configured Yara rules, submit your request through the support form.

Yara matches

Each time a Yara rule matches files, the **Last matched** date/time will be updated. To filter matches, use the drop-down menus above the list of matches, or use the full-text search bar at the top of the screen.

Search

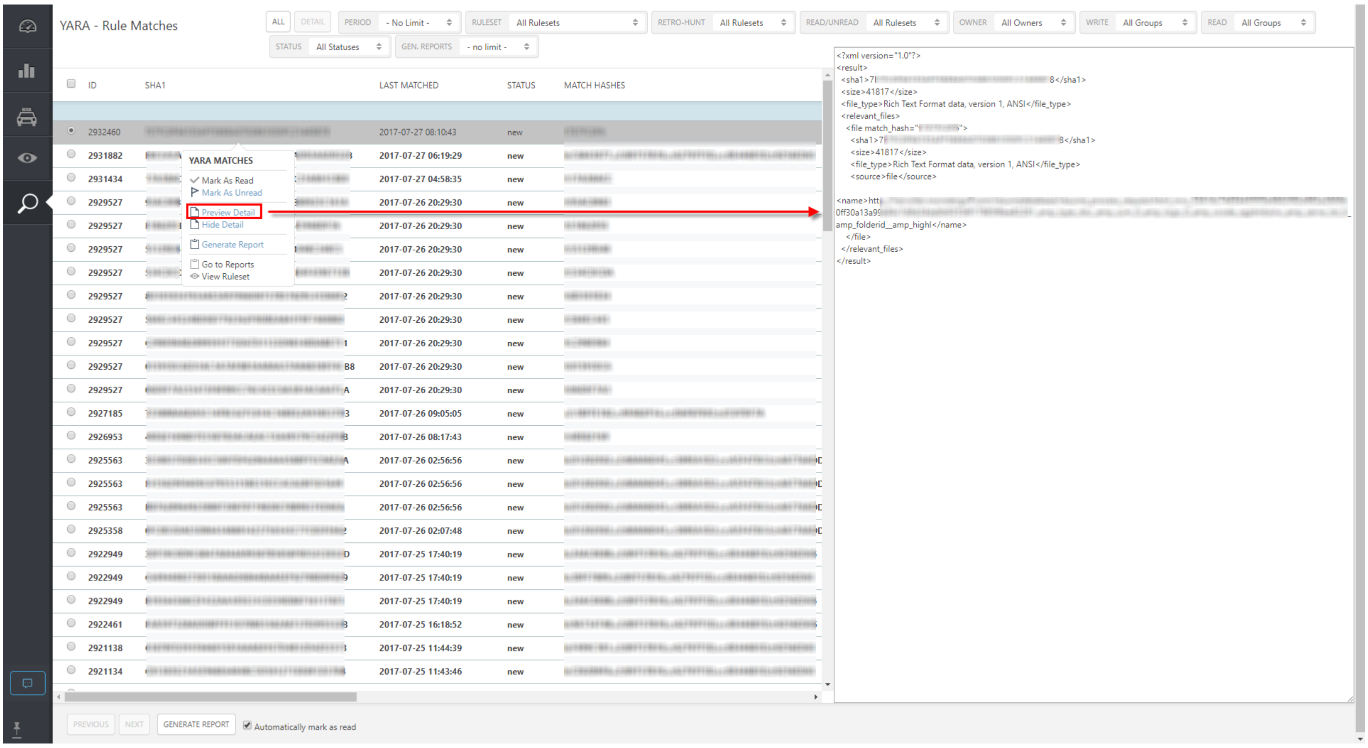
If you type into the search bar "www.eset.com" (without quotation marks), the exact sought string can be found in the *.xml* file of the search result. In the *.pdf* file of the search result, the first occurrence of the dot in an URL address is replaced with "[dot]" (without quotation marks).



PERIOD: - No Limit -
RULESET: All Rulesets
RETRO-HUNT: All Rulesets
READ/UNREAD: All Rulesets
OWNER: All Owners
WRITE: All Groups
READ: All Groups
STATUS: All Statuses
GEN. REPORTS: - no limit -

☐	ID	SHA1	LAST MATCHED	STATUS	MATCH HASHES	LAST REPORT DATE	NOTE	OWNER	WRITE
☐	2932460	7[redacted]	2017-07-27 08:10:43	new	f[redacted]			[redacted]	Testing BET
☐	2931882	E[redacted]28	2017-07-27 06:19:29	new	b[redacted]5			[redacted]	Testing BET
☐	2931434	1[redacted]0	2017-07-27 04:58:35	new	f[redacted]			[redacted]	Testing BET
☐	2929527	9[redacted]A	2017-07-26 20:29:30	new	f[redacted]			[redacted]	Testing BET
☐	2929527	E[redacted]	2017-07-26 20:29:30	new	f[redacted]			[redacted]	Testing BET
☐	2929527	5[redacted]	2017-07-26 20:29:30	new	f[redacted]			[redacted]	Testing BET
☐	2929527	5[redacted]B	2017-07-26 20:29:30	new	f[redacted]			[redacted]	Testing BET
☐	2929527	8[redacted]2	2017-07-26 20:29:30	new	f[redacted]			[redacted]	Testing BET
☐	2929527	5[redacted]	2017-07-26 20:29:30	new	f[redacted]			[redacted]	Testing BET
☐	2929527	C[redacted]1	2017-07-26 20:29:30	new	f[redacted]			[redacted]	Testing BET
☐	2929527	0[redacted]B8	2017-07-26 20:29:30	new	f[redacted]			[redacted]	Testing BET
☐	2929527	0[redacted]A	2017-07-26 20:29:30	new	f[redacted]			[redacted]	Testing BET
☐	2927185	7[redacted]3	2017-07-26 09:05:05	new	c[redacted]		xcvxv	[redacted]	Testing BET
☐	2926953	4[redacted]B	2017-07-26 08:17:43	new	f[redacted]			[redacted]	Testing BET
☐	2925563	3[redacted]A	2017-07-26 02:56:56	new	b[redacted]DD			[redacted]	Testing BET
☐	2925563	F[redacted]	2017-07-26 02:56:56	new	b[redacted]DD			[redacted]	Testing BET
☐	2925563	B[redacted]	2017-07-26 02:56:56	new	b[redacted]DD			[redacted]	Testing BET
☐	2925358	0[redacted]2	2017-07-26 02:07:48	new	b[redacted]DD			[redacted]	Testing BET
☐	2922949	3[redacted]D	2017-07-25 17:40:19	new	b[redacted]5			[redacted]	Testing BET
☐	2922949	C[redacted]9	2017-07-25 17:40:19	new	b[redacted]5			[redacted]	Testing BET
☐	2922949	B[redacted]	2017-07-25 17:40:19	new	b[redacted]5			[redacted]	Testing BET
☐	2922461	F[redacted]B	2017-07-25 16:18:52	new	b[redacted]5			[redacted]	Testing BET
☐	2921138	6[redacted]3	2017-07-25 11:44:39	new	b[redacted]5			[redacted]	Testing BET
☐	2921134	C[redacted]4	2017-07-25 11:43:46	new	b[redacted]5			[redacted]	Testing BET

To view the content of a matched file, click the file and select **Preview Detail**. In the preview window, the **Mark as read** and **Mark as unread** buttons change to **Previous** and **Next**. Use them to navigate through each report in preview mode. Use the **Note** field to add a custom note to any of the matches.



PERIOD - No Limit -
RULESET All Rulesets
RETRO-HUNT All Rulesets
READ/UNREAD All Rulesets
OWNER All Owners
WRITE All Groups
READ All Groups
STATUS All Statuses
GEN. REPORTS - no limit -

ID	SHA1	LAST MATCHED	STATUS	MATCH HASHES
● 2932460	[redacted]	2017-07-27 08:10:43	new	[redacted]
○ 2931882	[redacted]	2017-07-27 06:19:29	new	[redacted]
○ 2931434	[redacted]	2017-07-27 04:58:35	new	[redacted]
○ 2929527	[redacted]	2017-07-26 20:29:30	new	[redacted]
○ 2929527	[redacted]	2017-07-26 20:29:30	new	[redacted]
○ 2929527	[redacted]	2017-07-26 20:29:30	new	[redacted]
○ 2929527	[redacted]	2017-07-26 20:29:30	new	[redacted]
○ 2929527	[redacted]	2017-07-26 20:29:30	new	[redacted]
○ 2929527	[redacted]	2017-07-26 20:29:30	new	[redacted]
○ 2929527	[redacted]	2017-07-26 20:29:30	new	[redacted]
○ 2929527	[redacted]	2017-07-26 20:29:30	new	[redacted]
○ 2929527	[redacted]	2017-07-26 20:29:30	new	[redacted]
○ 2927185	[redacted]	2017-07-26 09:05:05	new	[redacted]
○ 2926953	[redacted]	2017-07-26 08:17:43	new	[redacted]
○ 2925563	[redacted]	2017-07-26 02:56:56	new	[redacted]
○ 2925563	[redacted]	2017-07-26 02:56:56	new	[redacted]
○ 2925563	[redacted]	2017-07-26 02:56:56	new	[redacted]
○ 2925358	[redacted]	2017-07-26 02:07:48	new	[redacted]
○ 2922949	[redacted]	2017-07-25 17:40:19	new	[redacted]
○ 2922949	[redacted]	2017-07-25 17:40:19	new	[redacted]
○ 2922949	[redacted]	2017-07-25 17:40:19	new	[redacted]
○ 2922461	[redacted]	2017-07-25 16:18:52	new	[redacted]
○ 2921138	[redacted]	2017-07-25 11:44:39	new	[redacted]
○ 2921134	[redacted]	2017-07-25 11:43:46	new	[redacted]

☑ Automatically mark as read

```
<?xml version="1.0"?>
<result>
 <sha1>[redacted]</sha1>
 <size>41817</size>
 <file_type>Rich Text Format data, version 1, ANSI</file_type>
 <relevant_files>
  <file match_hash="[redacted]">
   <sha1>[redacted]</sha1>
   <size>41817</size>
   <file_type>Rich Text Format data, version 1, ANSI</file_type>
   <source>file</source>

<name>htt[redacted]
0ff30a13a9[redacted]
amp_folderid__amp_highl</name>
  </file>
 </relevant_files>
</result>
```

To view a more detailed report, click **Generate report** to generate a **Targeted Report** or **Certificate Report** of the matched and analyzed file.

Terms of use

ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 (hereinafter referred to as "ESET ") as the controller of ESET Threat Intelligence website (hereinafter referred to as "ETI") provides the access to Early Warning Service (hereinafter referred to as "Service") to Customers in compliance with terms stipulated in special agreement concluded between ESET and Customer and these Terms of Use (hereinafter referred to as "Terms"). The Service provides information on malware and associated configurations which are prepared to or used to attack specific organization or its customers. The Service provides the access to intelligence on malware in form of Targeted Malware Report and Botnet Activity Report to registered users.

Customer shall receive an access to Botnet Activity Report on periodic weekly basis after the activation of the Service. In case of targeted attack via malware, Customer shall receive email notification on Targeted Malware Report creation, which shall be available on ETI. All outputs of Service shall be available to Customer on limited access area of ETI.

Customer may submit a request for Malware Analysis in compliance with special agreement concluded between ESET and Customer in case of targeted attack via malware which is not captured in the Service. Customer's possession of particular malware is required.

ETI Account

The ETI Account provides access to services provided by ESET. You are responsible for maintaining the security of the ETI Account and password. ESET shall not be liable for any loss or damage resulting from your failure to comply with this obligation to maintain security. The user is also responsible for any activity related to the use of the ETI Account, authorized or not. If the ETI Account is compromised, you should notify the provider immediately. Details about privacy and personal data protection can be found on https://www.eset.com/privacy.

Copyright

ESET or its respective suppliers own or may exercise copyright to all content available on the ETI Account sites (hereinafter referred to as "Content"). The Content can be used only in accordance with the end-user license/framework agreement (hereinafter referred to as "License Agreement"). Content is supplied together with the Licence Agreement. Content supplied with the License Agreement cannot be used without the user's consent to the License Agreement. Other information regarding licensing, copyright, documentation and trademarks are stipulated in the Legal Information document (https://www.eset.com/int/legal-information).

Disclaimers

AS THE USER, YOU HEREBY ACKNOWLEDGE THAT THE ACCOUNT IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NEITHER THE PROVIDER, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT ACCOUNT WILL NOT INFRINGE ANY THIRD PARTY'S PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THE PROVIDER OR ANY OTHER PARTY MAKE NO GUARANTEE THAT THE FUNCTIONS CONTAINED IN ACCOUNT WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF ACCOUNT WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION AND USE OF ACCOUNT TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE RESULTS OBTAINED FROM IT.

No other obligations. These Terms create no obligations on the part of the Provider and its licensors other than as specifically set forth herein.

Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR LICENSORS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR OTHER THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THE ACCOUNT, EVEN IF THE PROVIDER OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME COUNTRIES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY, BUT MAY ALLOW LIABILITY TO BE LIMITED, IN SUCH CASES THE LIABILITY OF THE PROVIDER, ITS EMPLOYEES OR LICENSORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID TO PROVIDER.

Trade control compliance

(a) You will not, directly or indirectly, export, re-export, transfer or otherwise make available the Software to any person, or use it in any manner, or be involved in any act, that could result in ESET or its holding companies, its subsidiaries, and the subsidiaries of any of its holding companies, as well as entities controlled by its holding companies (hereinafter referred to as "Affiliates") being in violation of, or being subject to negative consequences under, Trade Control Laws which includes

i. any laws that control, restrict, or impose licensing requirements on export, re-export or transfer of goods, software, technology, or services, issued or adopted by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under these Terms are to be performed, or in which ESET or any of its Affiliates are incorporated or operate (hereinafter referred to as "Export Control Laws") and

ii. any economic, financial, trade or other, sanction, restriction, embargo, import or export ban, prohibition on transfer of funds or assets or on performing services, or equivalent measure imposed by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under these Terms are to be performed, or in which ESET or any of its Affiliates are incorporated or operate (hereinafter referred to as "Sanction Laws").

(b) ESET shall have the right to suspend its obligations under, or terminate, these Terms with immediate effect in the event that:

i. ESET determines that, in its reasonable opinion, the User has breached or is likely to breach provision of section (a) of this Trade control compliance clause of these Terms; or

ii. the End User and/or the Software become subject to Trade Control Laws and, as a result, ESET determines that, in its reasonable opinion, the continued performance of its obligations under these Terms could result in ESET or its Affiliates being in violation of, or being subject to negative consequences under, Trade Control Laws.

(c) Nothing in these Terms is intended, and nothing should be interpreted or construed, to induce or require either party to act or refrain from acting (or to agree to act or refrain from acting) in any manner which is inconsistent with, penalized, or prohibited under any applicable Trade Control Laws.

Governing Law and Language

These Terms shall be governed by and construed in accordance with Slovak law. The End User and the Provider agree that conflict provisions of the governing law and United Nations Convention on Contracts for the International Sale of Goods shall not apply. You expressly agree that exclusive jurisdiction for any claim or dispute with the Provider or relating in any way to Your use of the Software resides in District Court Bratislava I, Slovakia and you further agree and expressly consent to the exercise of the personal jurisdiction in the District Court Bratislava I in connection with any such dispute or claim.

In the case of discrepancies between the language versions the English version shall always prevail as the English version is deemed original.

General provisions

ESET reserves the right to revise these Terms or any portion thereof at any time without prior notice by updating this document to reflect changes to the law or changes to Account. You will be notified about any revision of these Terms by way of Account. If you disagree with the changes to these Terms, you may cancel your Account. Unless you cancel your Account, you are bound by any amendments or revisions of these Terms. You are encouraged to periodically visit this page to review the current Terms that apply to your use of Account.

Notices

All notices must be delivered to: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.