ANY.RUN

INTERACTIVE MALWARE ANALYSIS

TAXII Documentation

for TI Feeds by ANY.RUN

Thank you for choosing ANY.RUN as your security software provider. This document aims to assist you in utilizing our product

New Approach to Network IOCs Delivery

ANY.RUN offers regularly updated Threat Intelligence Feeds (TI Feeds) to help businesses enhance threat detection and coverage of emerging and persistent threats, enabling SOC teams to more effectively mitigate attacks.

TAXII is a protocol used for exchanging cyber threat intelligence. ANY.RUN maintains compliance with the TAXII Version 2.1 OASIS Standard published on 10 June 2021. This allows for simple and transparent integration with third-party systems.

You'll gain access to fresh and unique data retrieved from threat investigations in 15,000 companies with near-zero false positive rate. As a result, TI Feeds will help you with early detection of attacks in your company's infrastructure.

By implementing TAXII, we engage in the best practices and standards for describing and delivering IOCs in cybersecurity.

ANY.RUN's TI Feeds include network-based Indicators of Compromise (IOCs) in STIX format delivered via the TAXII 2.1 application-layer protocol. The set is comprised of multiple collections, each containing specific indicator types, including IP addresses, domain names, URLs.

TAXII 2.1 Specification

Authorization

For authorization, use basic access authentication:

Header	Type	Description
authorization	string	Required. Basic <EncryptedBase64(Username:Password)>

Request

Discovery Endpoint

Use this URL to access the Discovery Endpoint, which provides general information about the TAXII server, including its title, description, contact information, and advertised API Roots. The Discovery Endpoint also indicates the default API Root and serves as the primary entry point for TAXII clients:

```
https://api.any.run/v1/feeds/taxii2
```

API Root

With this URL request, you can explore the API Root resource that provides general information about a specific API Root:

```
https://api.any.run/v1/feeds/taxii2/api1/
```

Collections

Via this link, you can explore information about all collections hosted under the ANY.RUN API Root, including each collection's ID, which is required to request objects or manifest entries from it:

```
https://api.any.run/v1/feeds/taxii2/api1/collections/
```

Discovery Endpoint

Name	Description	ID
All indicators	Contains IOCs of all formats (IPs, Domains, URLs)	3dce855a-c044-5d49-9334-533c24678c5a
IPs collection	Contains only IPs	55cda200-e261-5908-b910-f0e18909ef3d
Domains collection	Contains only Domains	2e0aa90a-5526-5a43-84ad-3db6f4549a09
URLs collection	Contains only URLs	05bfa343-e79f-57ec-8677-3122ca33d352

Object Manifests

You can also get Object Manifests, metadata about objects in a collection using the endpoint below. It provides information, such as the object ID, addition time, version, and media type. It supports filtering similar to the "Get Objects" endpoint and helps determine whether it's necessary to retrieve full objects.

```
https://api.any.run/v1/feeds/taxii2/api1/collections/{collection_id}/manifest/
```

Get Objects / Get an Object

Requests "Get Objects" and "Get an Object" provide you with information on all objects in a collection or on a specific object (via specify object_id line in the URL).

```
https://api.any.run/v1/feeds/taxii2/api1/collections/{collection_id}/objects/
```

```
https://api.any.run/v1/feeds/taxii2/api1/collections/{collection_id}/objects/{object_id}
```

See all query parameters below. They are optional and can be combined with each other.

Parameter	Type	Description
added_after	ISO 8601 Date and time in UTC format	Timestamp that filters objects to only include those objects added after a specific timestamp
modified_after	ISO 8601 (UTC)	Timestamp that filters objects to only include those that were modified after a specific timestamp
limit	integer	A value that indicates the maximum number of objects that a client would like to receive in a single response
next	string	This is a pagination token returned by our TAXII 2.1 server when more results are available. Use this value in your next request, along with original filter parameters, to retrieve the next set of records. The token is encrypted and is generated by the server
match[<field>]	list of fields	
	id	The identifier of the object(s) that are being requested. When searching for a STIX Object, this is a STIX ID
	spec_version	Request specification version(s) of the STIX object
	type	The type of requested object(s)
	version	The version(s) of requested object(s) from either the "Get an Object" or "Object Manifests" endpoint. You can filter the results: match[version]=<value> all - will return all versions of objects last - will return last versions of objects first - will return first versions of objects <date and time value> - requests a specific version of an object. The date and time value will be provided in UTC format (ISO 8601).
	revoked	The field shows if the indicator is out of date and is considered revoked. Can only take a boolean value: true or false.

Request examples:

```
curl --location --globoff --request GET
'https://api.any.run/v1/feeds/taxii2/api1/collections/{collection_id}/objects?
limit=1&match[type]=indicator'\
--header 'Authorization: Basic <Your token here>'
```

```
curl --location --globoff --request GET
'https://api.any.run/v1/feeds/taxii2/api1/collections/{collection_id}/objects?
match[type]=indicator&match[version]=2021-09-29T07:23:40.000Z' \
--header 'Authorization: Basic <Your token here>'
```

Response

As a result of "Get Objects” and "Get an Object URL” requests via the TAXII 2.1 application-layer protocol, you get STIX indicators with the following types of IOCs: URL, IP, or domain name, along with relationships and 'identity' object that describes ANY.RUN as the organization that created this object.

The response also includes the following headers regarding indicators from each data delivery:

- **X-TAXII-Date-Added-First** and **X-TAXII-Date-Added-Last**: to show dates when the first and the last IOC was created;
- **X-TAXII-Date-Modified-First** and **X-TAXII-Date-Modified-Last**: to show dates when the first and the last IOC was modified.

STIX 2.1. Specification

Fields description for main types of IOCs

Parameter	Field	Description	Example
Indicator	type	Specifies the category of a STIX object	indicator
	id	A unique identifier assigned to the IOC in a standardized format [type]--[uuid]	indicator--88d2a5bd-aa44-590b-b852-7206e24afbe9
	created	The date and time when the IOC was first identified or created in the system	2022-11-29T06:52:43.000Z
	modified	The date and time when the IOC was last modified	2023-12-20T17:33:06.000Z

Parameter	Field	Description	Example
	lables[]	An array of labels or tags associated with the IOC that provide context, such as the type of threat (e.g., 'malware') or the name of the malware (e.g., 'dcrat')	malware, dcrat
	external_ references []	Additional metadata and context-specific information on the IOC, such as the entry's author and data sources	"source_name": "ANY.RUN task <id>", "url": "https://app.any.run/tasks/{task id}"
	created_by_ref	A reference to the entity (e.g., organization, person, or system) that created the IOC	identity--96a9cd9c-2f73-5ad3-a2ab-c14b3eba65c7
	spec_version	Specifies the version of a STIX specification that the object conforms to. For objects created according to STIX 2.1, this value will always be "2.1"	2.1
	revoked	A boolean field indicating whether the IOC has been officially invalidated or is no longer active. If it equals “true”, it signifies that the IOC is no longer considered a valid threa	true
	confidence	The confidence value is a number in the range of 0-100. It measures how confident the creator is in the correctness of their data	100
	pattern	The field contains a STIX Pattern written in the STIX Patterning Language, a standardized, machine-readable language designed for threat detection. It defines the detection logic—the conditions under which an observed event matches the indicator	http://malicious.example.com
	pattern_type	The pattern_type field specifies the **syntax** used in the pattern field of an indicator. **This means the pattern is written using the STIX Patterning Language.**	stix
	valid_from	The field indicates the timestamp from which the indicator becomes active and should be considered valid for detecting the threat behavior it describes. It defines the start of a time period during which this indicator is relevant and actionable	2022-11-29T06:52:43.000Z

Fields describing the 'type': 'identity' object, which contains information on the organization that created the STIX JSON, as referenced by the 'created_by_ref' property.

Object	Field	Description	Example
Identity	type	Specifies the category of a STIX object	identity
	id	A unique identifier assigned to the entity (e.g., organization, person, or system) that created the IOC	identity--96a9cd9c-2f73-5ad3-a2ab-c14b3eba65c7
	contact_ information	Contact details of the entity (e.g., an email address, a phone number, or a link)	https://any.run/
	created	The date and time when an object was added in the STIX JSON	2016-05-01T00:00:01.000Z
	modified	The date and time when the object was last modified	2016-05-01T00:00:01.000Z
	spec_version	Specifies the version of the STIX specification that the object conforms to. For objects created according to STIX 2.1, this value will always be "2.1".	2.1
	name	The name of entity (e.g., organization, person, or system) that created the IOC	ANY.RUN
	description	The description of entity (e.g., organization, person, or system) that created the IOC	ANY.RUN Threat Intelligence Feed
	identity_class	The type of entity which this object describes	organization

The recommendations for each type of an indicator are the following:

- **For domain-name:** we recommend blocking all requests to this domain.
- **For IP:** we recommend blocking all requests to this IP address, including requests to URLs whose domain resolves to this IP address.
- **For URL:** we recommend blocking all URLs, including those with parameters following "?" which match our IOC record. It's important to note that our URLs have their parameters truncated after the "?" and they should be blocked regardless of their parameters.

However, these recommendations are advisory in nature. It is best to consider each case individually. You can learn more about the standards for describing IOCs via this link:

https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_Toc31107564

Note: Currently our feed offers only one version of each STIX object.

Please note that this document is the property of ANY.RUN and is protected by international treaties. Unauthorized reproduction or distribution, in whole or in part, may result in civil, administrative, or criminal liability under applicable law. Any reproduction or distribution, including translations, requires written permission from ANY.RUN.

ANY.RUN may revise this document without providing additional notification.

ANY.RUN does not accept responsibility for any potential harm resulting from the use of this document.

Document revision date: July 24, 2025

https://any.run