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

Description of Threat Intelligence Feed: Network IOCs

ANY.RUN offers regularly updated Threat Intelligence Feeds to inform your business or clients about risks and implications associated with security breaches. Constant updates also help to mitigate cyber threats more effectively and defend against attacks before they are even launched:

- Network IOCs is a set of indicators of compromise (IOCs) in STIX format that include different types of IP addresses, domain names and URL addresses with related files.

Authorization

You can use your API authentification:

Header	Type	Description
authorization	string	Required. API-Key <APIKEY>

Or use basic access authentication:

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

Request

Request URL:

```
https://api.any.run/v1/feeds/stix.json
```

Query parameters, all parameters are optional:

Parameter	Type	Description
IP	bool	Enable or disable the IP type from the feed. Default: "true"
URL	bool	Enable or disable the URL type from the feed. Default: "true"
Domain	bool	Enable or disable the Domain type from the feed. Default: "true"
period	string	Time period for the feed. Possible values: "day", "week", "month".
limit	string	The number of tasks on a page should be greater than 100. Default: all IOCs are included.
page	string	Page number

Example:

```
curl --location --request GET
'https://api.any.run/v1/feeds/stix.json?
IP=false&Host=true&URL=false&period=week&page=3=limit=500' \
 --header 'Authorization: Basic <Your token here>'
```

Response

Get STIX records with the following types of IOCs: url, ip, or domain-name, along with optional related objects of types file and port.

Fields description for main types of IOCs

Parameter	Field	Description	Example
URL, Domain, IP	type	Specifies the category of the indicator of compromise (IoC)	url, domain-name, ipv4-addr
	id	A unique identifier assigned to the IoC in a standardized format [type]--[uuid]	url--88d2a5bd-aa44-590b-b852-7206e24afbe9
	value	The actual value of the IoC, which can be a URL, an IP address, etc.	http://www.car-insurance-27673.bond/gd12/, mail.agaliofu.top, 63.12.201.52, 198.51.100.1/32
	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
	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').	"labels": ["malware", "dcrat"]

	related_objects[]	An array of related objects or other IoCs that have a defined relationship with the primary IoC, such as a URL containing a particular file.	"related_objects": [
			{
			"relationship_type": "contains",
			"source_ref": "url--88d2a5bd-aa44-590b-b852-7206e24afbe9",
			"target_ref": "file--01b63091-35e1-5e36-90c8-4517bda44667"
			}
			]

Fields description for optional types of IOCs

Parameter	Field	Description	Example
File	type	Specifies the category of the indicator of compromise (IoC)	file
	id	A unique identifier assigned to the IoC in a standardized format [type]--[uuid]	file--88d2a5bd-aa44-590b-b852-7206e24afbe9

	hashes	This field holds the cryptographic hash values associated with a file	"hashes": {
			"SHA-256": "1e6790df2471be2bc8210901b6d54045082caf912f703e5f05676cf6ebd31fed",
			"SHA-1": "852f41b9503c9b06687ebb3e52872940f473d07a",
			"MD5": "637e1ac866d727b5924f294441db651d"
			}

Port	type	Specifies the category of the indicator of compromise (IoC)	port
	id	A unique identifier assigned to the IoC in a standardized format [type]--[uuid]	port--88d2a5bd-aa44-590b-b852-7206e24afbe9
	port_value	This field specifies the port number associated with the network activity	16458
	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
	labels[]	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').	"labels": ["malware", "dcrat"]

	related_objects[]	An array of related objects or other IoCs that have a defined relationship with the primary IoC, such as a URL containing a particular file.	"related_objects": [
			{
			"relationship_type": "contains",
			"source_ref": "url--88d2a5bd-aa44-590b-b852-7206e24afbe9",
			"target_ref": "file--01b63091-35e1-5e36-90c8-4517bda44667"
			}
			]

The matching rules for each record type are as follows:

- **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:** recommend blocking all URLs, including those with parameters following the "?," 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 any parameters they may have.

Related objects with the "port" type refer to TCP/UDP ports found in malware configurations. In many cases, we have information that malware uses these ports. This field is optional.

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: 10.03.2024

https://any.run