ThreatQuotient

MISP Galaxy Data CDF User Guide

Version 1.0.1

December 11, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.1
Compatible with ThreatQ Versions	>= 4.40.0
Support Tier	ThreatQ Supported

Introduction

The MISP Galaxy Data Integration is a collection of multiple feeds that provide data that seeds a new MISP instance.

The integration provides the following feeds:

- **MISP Cluster - Threat Actors** - ingests data on known or estimated adversary groups targeting organizations and employees.
- **MISP Cluster - Branded Vulnerabilities** - ingests a list of known vulnerabilities and attacks with a branding.
- **MISP Cluster - RansomWare** - ingests data on reported ransomware.
- **MISP Cluster - Android Malware** - ingest data on android-based malware.
- **MISP Cluster - RAT** - ingests data on remote administration tools.
- **MISP Cluster - Banker** - ingests malware data specifically targeted towards banking.
- **MISP Cluster - Countries** - ingests target information.
- **MISP Cluster - Tool** - ingests a list of malware and common software regularly used by the adversaries.

The integration ingests the following system objects:

- Adversaries
  - Adversary Attributes
- Identities
  - Identity Attributes
- Indicators
  - Indicator Attributes
- Malware
  - Malware Attributes
- Vulnerabilities
  - Vulnerability Attributes

All the data is available in the public domain under the license noted below.

```
Original data is dual licensed, as per https://raw.githubusercontent.com/MISP/
misp-galaxy/master/LICENSE.md
---
 The MISP galaxy (JSON files) are dual-licensed under:
 - [CC0 1.0 Universal](https://creativecommons.org/publicdomain/zero/1.0/
legalcode) (CC0 1.0) - Public Domain Dedication.
 or
 ~~~~
  Copyright (c) 2015-2018 Alexandre Dulaunoy - a@foo.be
  Copyright (c) 2015-2018 CIRCL - Computer Incident Response Center Luxembourg
  Copyright (c) 2015-2018 Andras Iklody
  Copyright (c) 2015-2018 Raphael Vinot
  Copyright (c) 2015-2018 Deborah Servili
  Copyright (c) 2016-2018 Various contributors to MISP Project
  Redistribution and use in source and binary forms, with or without
modification,
  are permitted provided that the following conditions are met:
     1. Redistributions of source code must retain the above copyright notice,
        this list of conditions and the following disclaimer.
     2. Redistributions in binary form must reproduce the above copyright
notice,
        this list of conditions and the following disclaimer in the
documentation
        and/or other materials provided with the distribution.
  THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND
  ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
  WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED.
  IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY
DIRECT,
 INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
  BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
  DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY
OF
  LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE
  OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED
  OF THE POSSIBILITY OF SUCH DAMAGE.
~~~~~
```

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration file on your local machine

   > ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Save CVE Data As *(MISP Cluster - Threat Actors and Branded Vulnerabilities feeds Only)*	Select how to ingest CVE data. Options include: ◦ Indicators ◦ Vulnerabilities ◦ Both
Verify SSL	Enable/Disable this option to verify the server's SSL certificate.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

MISP Cluster - Threat Actors

Known or estimated adversary groups targeting organizations and employees. Adversary groups are regularly confused with their initial operation or campaign. threat-actor-classification meta can be used to clarify the understanding of the threat-actor if also considered as operation, campaign or activity group.

`GET https://raw.githubusercontent.com/MISP/misp-galaxy/main/clusters/threat-actor.json`

Sample Response:


```
{
  "authors": [
    "Alexandre Dulaunoy",
    "Florian Roth",
    "Thomas Schreck",
    "Timo Steffens",
    "Various"
  ],
  "category": "actor",
  "description": "Known or estimated adversary groups targeting organizations
and employees. Adversary groups are regularly confused with their initial
operation or campaign. threat-actor-classification meta can be used to clarify
the understanding of the threat-actor if also considered as operation, campaign
or activity group.",
  "name": "Threat Actor",
  "source": "MISP Project",
  "type": "threat-actor",
  "uuid": "7cdff317-a673-4474-84ec-4f1754947823",
  "values": [
    {
      "description": "PLA Unit 61398 (Chinese: 61398部队, Pinyin: 61398 bùduì)
is the Military Unit Cover Designator (MUCD)[1] of a People's Liberation Army
advanced persistent threat unit that has been alleged to be a source of Chinese
computer hacking attacks",
      "meta": {
        "attribution-confidence": "50",
        "cfr-suspected-state-sponsor": "China",
        "cfr-suspected-victims": [
          "United States",
          "Taiwan",
          "Israel",
          "Norway",
          "United Arab Emirates",
          "United Kingdom",
```

```
          "Singapore",
          "India",
          "Belgium",
          "South Africa",
          "Switzerland",
          "Canada",
          "France",
          "Luxembourg",
          "Japan"
        ],
        "cfr-target-category": [
          "Private sector",
          "Government"
        ],
        "cfr-type-of-incident": "Espionage",
        "country": "CN",
        "refs": [
          "https://en.wikipedia.org/wiki/PLA_Unit_61398",
          "http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf",
          "https://www.cfr.org/interactive/cyber-operations/pla-unit-61398",
          "https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/
mandiant-apt1-report.pdf",
          "https://blog.trendmicro.com/trendlabs-security-intelligence/the-
siesta-campaign-a-new-targeted-attack-awakens/",
          "https://www.fireeye.com/blog/threat-research/2014/03/a-detailed-
examination-of-the-siesta-campaign.html",
          "https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/
operation-oceansalt-delivers-wave-after-wave/",
          "https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-
oceansalt.pdf",
          "https://www.symantec.com/connect/blogs/apt1-qa-attacks-comment-
crew",
          "https://attack.mitre.org/groups/G0006/",
          "https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-
with-cyberspying.html"
        ],
        "synonyms": [
          "Comment Panda",
          "PLA Unit 61398",
          "APT 1",
          "APT1",
          "Advanced Persistent Threat 1",
          "Byzantine Candor",
          "Group 3",
          "TG-8223",
          "Comment Group",
          "Brown Fox",
          "GIF89a",
          "ShadyRAT",
          "Shanghai Group"
```

```
        ]
      },
      "related": [
        {
          "dest-uuid": "6a2e693f-24e5-451a-9f88-b36a108e5662",
          "tags": [
            "estimative-language:likelihood-probability=\"likely\""
          ],
          "type": "similar"
        }
      ],
      "uuid": "1cb7e1cc-d695-42b1-92f4-fd0112a3c9be",
      "value": "Comment Crew"
    },
  ],
  "version": 157
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.values[].value	Adversary.Name	N/A	N/A	Comment Crew	
.values[].value	Adversary.Attribute	Common Name	N/A	Comment Crew	Only applies to adversaries created from `.values[].synonyms`
.values[].meta.synonyms	Adversary.Name	N/A	N/A	APT1	
.values[].meta.synonyms	Adversary.Attribute	Synonym	N/A	APT1	Only applies to adversaries created from `.values[].value`
.values[].description	Vulnerability.Value	N/A	N/A	CVE-2020-0001	
.values[].description	Indicator.Value	CVE	N/A	CVE-2020-0001	
.values[].description	Adversary.Description / Indicator.Description / Vulnerability.Description	N/A	N/A	Known or estimated adversary groups targeting organizations and employees. Adversary groups are regularly confused with their initial operation or campaign. threat-actor-classification meta can be used to clarify the understanding of the threat-actor if also considered as operation, campaign or activity group.	
.values[].meta.country	Adversary.Attribute	Country Code	N/A	CN	
.values[].meta.cfr-suspected-state-sponsor	Adversary.Attribute / Indicator.Attribute / Vulnerability.Attribute	Suspected State Sponsor	N/A	China	
.values[].meta.attribution-confidence	Adversary.Attribute / Indicator.Attribute / Vulnerability.Attribute	Attribution Confidence	N/A	50	
.values[].meta.cfr-suspected-victims	Adversary.Attribute / Indicator.Attribute / Vulnerability.Attribute	Suspected Victim Country	N/A	United States	
.values[].meta.cfr-target-category	Adversary.Attribute / Indicator.Attribute / Vulnerability.Attribute	Target Industry	N/A	Government	
.values[].meta.cfr-type-of-incident	Adversary.Attribute / Indicator.Attribute / Vulnerability.Attribute	Type of Incident	N/A	Espionage	
.values[].meta.refs	Adversary.Attribute / Indicator.Attribute / Vulnerability.Attribute	Reference URL	N/A	https://en.wikipedia.org/wiki/PLA_Unit_61398	
.values[].meta.motive	Adversary.Attribute / Indicator.Attribute / Vulnerability.Attribute	Motive	N/A	Hacktivism-Nationalist	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.values[].related.type	Adversary.Attribute / Indicator.Attribute / Vulnerability.Attribute	Type	N/A	similar	
.values[].related.tags	Adversary.Attribute / Indicator.Attribute / Vulnerability.Attribute	Tag	N/A	estimative-language:likelihood-probability="likely"	

MISP Cluster - Branded Vulnerabilities

List of known vulnerabilities and attacks with a branding. This helps answer the question of "what do we know about X", where X is a non standard name.

`GET https://raw.githubusercontent.com/MISP/misp-galaxy/main/clusters/branded_vulnerability.json`

Sample Response:


```
{
  "authors": [
    "Unknown"
  ],
  "category": "vulnerability",
  "description": "List of known vulnerabilities and attacks with a branding",
  "name": "Branded Vulnerability",
  "source": "Open Sources",
  "type": "branded-vulnerability",
  "uuid": "93715a12-f45b-11e7-bcf9-3767161e9ebd",
  "values": [
    {
      "description": "Meltdown exploits the out-of-order execution feature of
modern processors, allowing user-level programs to access kernel memory using
processor caches as covert side channels. This is specific to the way out-of-
order execution is implemented in the processors. This vulnerability has been
assigned CVE-2017-5754.",
      "meta": {
        "aliases": [
          "CVE-2017-5754"
        ],
        "logo": [
          "https://upload.wikimedia.org/wikipedia/commons/thumb/5/56/
Meltdown_with_text.svg/300px-Meltdown_with_text.svg.png"
        ]
      },
      "uuid": "70bee5b7-0fa3-4a4d-98ee-d8ab787c6db1",
      "value": "Meltdown"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.values[].value	Vulnerability.Name	N/A	N/A	Meltdown	
.values[].value	Indicator.Attribute / Vulnerability.Attribute	Branded as	N/A	Meltdown	
.values[].meta.aliases	Vulnerability.Value	N/A	N/A	CVE-2020-0001	
.values[].meta.aliases	Indicator.Value	CVE	N/A	CVE-2020-0001	
.values[].description	Vulnerability.Description / Indicator.Description	N/A	N/A	Badlock is a security bug disclosed on April 12, 2016 affecting the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) remote protocols[1] supported by Windows and Samba servers.	
.values[].meta.refs	Indicator.Attribute / Vulnerability.Attribute	Reference URL	N/A	https://www.welivesecurity.com/2019/05/22/patch-now-bluekeep-vulnerability/	

MISP Cluster - Ransomware

`GET https://raw.githubusercontent.com/MISP/misp-galaxy/main/clusters/ransomware.json`

Sample Response:


```
{
  "authors": [
    "https://docs.google.com/spreadsheets/d/1TWS238xacAto-
fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml",
    "http://pastebin.com/raw/GHgpWjar",
    "MISP Project"
  ],
  "category": "tool",
  "description": "Ransomware galaxy based on https://docs.google.com/
spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml and http://
pastebin.com/raw/GHgpWjar",
  "name": "Ransomware",
  "source": "Various",
  "type": "ransomware",
  "uuid": "10cf658b-5d32-4c4b-bb32-61760a640372",
  "values": [
    {
      "description": "This is most likely to affect English speaking users,
since the note is written in English. English is understood worldwide, thus
anyone can be harmed. The hacker spread the virus using email spam, fake
updates, and harmful attachments. All your files are compromised including
music, MS Office, Open Office, pictures, videos, shared online files etc..",
      "meta": {
        "date": "March 2017",
        "encryption": "AES",
        "extensions": [
          "RANDOM 3 LETTERS ARE ADDED"
        ],
        "payment-method": "Bitcoin",
        "price": "1(300$)",
        "ransomnotes-refs": [
          "https://4.bp.blogspot.com/-OkiR6pVmYUw/WMFiLGPuJhI/AAAAAAAAEME/
wccYzFDIzJYWKXVxaTQeB4vM-4X6h3atgCLcB/s1600/note-nhtnwcuf.gif"
        ],
        "refs": [
          "https://id-ransomware.blogspot.co.il/2017/03/nhtnwcuf-
ransomware.html"
        ]
      },
      "uuid": "81b4e3ac-aa83-4616-9899-8e19ee3bb78b",
      "value": "Nhtnwcuf Ransomware (Fake)"
    }
```

```
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.values[].value	Malware.Value	N/A	N/A	Wannacry	
.values[].value	Malware.Attribute	Common Name	N/A	Wannacry	Only applies to malware created from `.values[].meta.synonyms`
.values[].meta.synonyms	Malware.Value	N/A	N/A	Fake CTB-Locker	
.values[].meta.synonyms	Malware.Attribute	Synonym	N/A	Fake CTB-Locker	Only applies to malware created from `.values[].value`
.values[].meta.ransomnotes-filenames	Indicator.Value	N/A	N/A	note.txt	Frequently filenames describe a file, vs. provide a list of real filenames. Therefore these are added in a review state.
.values[].meta.description	malware	Malware.Description / Indicator.Description	N/A	N/A	This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Payments in Monero
.values[].meta.ransomnotes-refs	Malware.Attribure / Indicator.Attribute	Ransom Note	N/A	https://twitter.com/JakubKroustek/status/842034887397908480	
.values[].meta.date	Malware.Attribure / Indicator.Attribute	Discovered Date	N/A	March 2017	
.values[].meta.encryption	Malware.Attribure / Indicator.Attribute	Encryption	N/A	AES	
.values[].meta.extensions	Malware.Attribure / Indicator.Attribute	Extensions	N/A	.ZINO	
.values[].meta.price	Malware.Attribure / Indicator.Attribute	Price	N/A	13 (4980$)	
.values[].meta.payment-method	Malware.Attribure / Indicator.Attribute	Payment Method	N/A	Bitcoin	
.values[].meta.ransomnotes	Malware.Attribure / Indicator.Attribute	Ransom Note	N/A	HELP_YOUR_FILES.html (CryptXXX)	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.values[].related.type	Malware.Attribure / Indicator.Attribute	Type	N/A	similar	
.values[].related.tags	Malware.Attribure / Indicator.Attribute	Tag	N/A	estimative-language:likelihood-probability="likely"	

MISP Cluster - Android Malware

`GET https://raw.githubusercontent.com/MISP/misp-galaxy/main/clusters/android.json`

Sample Response:


```
{
  "authors": [
    "Unknown"
  ],
  "category": "tool",
  "description": "Android malware galaxy based on multiple open sources.",
  "name": "Android",
  "source": "Open Sources",
  "type": "android",
  "uuid": "84310ba3-fa6a-44aa-b378-b9e3271c58fa",
  "values": [
    {
      "description": "CopyCat is a fully developed malware with vast
capabilities, including rooting devices, establishing persistency, and
injecting code into Zygote – a daemon responsible for launching apps in the
Android operating system – that allows the malware to control any activity on
the device.",
      "meta": {
        "refs": [
          "https://blog.checkpoint.com/2017/07/06/how-the-copycat-malware-
infected-android-devices-around-the-world/"
        ]
      },
      "uuid": "40aa797a-ee87-43a1-8755-04d040dbea28",
      "value": "CopyCat"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.values[].value	Malware.Value	N/A	N/A	Andr/Dropr-FH	
.values[].value	Malware.Attribute	Common Name	N/A	Andr/Dropr-FH	Only applies to malware created from `.values[].meta.synonyms`
.values[].meta.synonyms	malware.value	N/A	N/A	GhostCtrl	
.values[].meta.synonyms	Malware.Attribute	Synonym	N/A	GhostCtrl	Only applies to malware created from `.values[].value`
N/A	Malware.Attribute	Target Platform	N/A	Android	
.values[].meta.refs	Malware.Attribute	Reference URL	N/A	https://blog.checkpoint.com/2017/07/06/how-the-copycat-malware-infected-android-devices-around-the-world/	
.values[].meta.description	Malware.Description	N/A	N/A	Andr/Dropr-FH can silently record audio and video, monitor texts and calls, modify files, and ultimately spawn ransomware.	
.values[].related.type	Malware.Attribure	Type	N/A	similar	
.values[].related.tags	Malware.Attribure	Tag	N/A	estimative-language:likelihood-probability="likely"	

MISP Cluster - RAT

Remote administration tool or remote access tool (RAT), also called sometimes remote access trojan, is a piece of software or programming that allows a remote "operator" to control a system as if they have physical access to that system.

`GET https://raw.githubusercontent.com/MISP/misp-galaxy/main/clusters/rat.json`

Sample Response:


```
{
  "authors": [
    "Various",
    "raw-data"
  ],
  "category": "tool",
  "description": "remote administration tool or remote access tool (RAT), also
called sometimes remote access trojan, is a piece of software or programming
that allows a remote \"operator\" to control a system as if they have physical
access to that system.",
  "name": "RAT",
  "source": "MISP Project",
  "type": "rat",
  "uuid": "312f8714-45cb-11e7-b898-135207cdceb9",
  "values": [
    {
      "description": "TeamViewer is a proprietary computer software package for
remote control, desktop sharing, online meetings, web conferencing and file
transfer between computers.",
      "meta": {
        "refs": [
          "https://www.teamviewer.com"
        ]
      },
      "uuid": "8ee3c015-3088-4a5f-8c94-602c27d767c0",
      "value": "TeamViewer"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
values[].value	Malware.Value	N/A	N/A	JadeRAT	
.values[].value	Malware.Attribute	Common Name	N/A	JadeRAT	Only applies to malware created from `.values[].meta.synonyms`
.values[].meta.synonyms	Malware.Value	N/A	N/A	SomethingElse	
.values[].meta.synonyms	Malware.Attribute	Synonym	N/A	SDB bot	Only applies to malware created from `.values[].value`
.values[].meta.description	Malware.Description	N/A	N/A	In the wild since February 2015. The malware comes equipped with a variety of features and can be purchased for $50 directly from the author. It has been deployed in attacks against organizations across many industries and is predominantly delivered via phishing emails.	
.values[].meta.date	Malware.Attribute	Year	N/A	2014	
N/A	Malware.Attribute	Type	N/A	Remote Aceess Tool	
.values[].meta.refs	Malware.Attribute	Reference URL	N/A	https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments	
.values[].meta.cfr-suspected-state-sponsor	Malware.Attribute	Suspected State Sponsor	N/A	China	
.values[].meta.cfr-suspected-victims	Malware.Attribute	Suspected Victim Country	N/A	Ethnic minorities in China	
.values[].meta.cfr-target-category	Malware.Attribute	Target Industry	N/A	Civil society	
.values[].meta.cfr-type-of-incident	Malware.Attribute	Type of Incident	N/A	Espionage	
.values[].related.type	Malware.Attribure	Type	N/A	similar	
.values[].related.tags	Malware.Attribure	Tag	N/A	estimative-language:likelihood-probability="likely"	

MISP Cluster - Banker

A collection of malware specifically designed for 'banking'.

`GET https://raw.githubusercontent.com/MISP/misp-galaxy/main/clusters/banker.json`

Sample Response:


```
{
  "authors": [
    "Unknown",
    "raw-data"
  ],
  "category": "tool",
  "description": "A list of banker malware.",
  "name": "Banker",
  "source": "Open Sources",
  "type": "banker",
  "uuid": "59f20cce-5420-4084-afd5-0884c0a83832",
  "values": [
    {
      "description": "Zeus is a trojan horse that is primarily delivered via drive-by-downloads, malvertising, exploit kits and malspam campaigns. It uses man-in-the-browser keystroke logging and form grabbing to steal information from victims.  Source was leaked in 2011.",
      "meta": {
        "date": "Initally discovered between 2006 and 2007. New bankers with Zeus roots still active today.",
        "refs": [
          "https://usa.kaspersky.com/resource-center/threats/zeus-virus"
        ],
        "synonyms": [
          "Zbot"
        ]
      },
      "related": [
        {
          "dest-uuid": "0ce448de-c2bb-4c6e-9ad7-c4030f02b4d7",
          "tags": [
            "estimative-language:likelihood-probability=\"likely\""
          ],
          "type": "similar"
        },
        {
          "dest-uuid": "e878d24d-f122-48c4-930c-f6b6d5f0ee28",
          "tags": [
            "estimative-language:likelihood-probability=\"likely\""
          ],
          "type": "similar"
```

```
        },
        {
          "dest-uuid": "4e8c1ab7-2841-4823-a5d1-39284fb0969a",
          "tags": [
            "estimative-language:likelihood-probability=\"likely\""
          ],
          "type": "similar"
        }
      ],
      "uuid": "f0ec2df5-2e38-4df3-970d-525352006f2e",
      "value": "Zeus"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.values[].value	Malware.Value	N/A	N/A	Zeus	
.values[].value	Malware.Attribute	Common Name	N/A	Zeus	Only applies to malware created from `.values[].synonyms`
.values[].meta.synonyms	Malware.Value	N/A	N/A	Zbot	
.values[].meta.synonyms	Malware.Attribute	Synonym	N/A	Zbot	Only applies to malware created from `.values[].value`
.values[].meta.description	Malware.Description	N/A	N/A	Dridex leverages redirection attacks designed to send victims to malicious replicas of the banking sites they think they're visiting.	
N/A	Malware.Attribute	Type	N/A	Banker	
.values[].meta.date	Malware.Attribute	Date	N/A	first seen 2017	
.values[].meta.refs	Malware.Attribute	Reference URL	N/A	https://feodotracker.abuse.ch/	
.values[].related.type	Malware.Attribure	Type	N/A	similar	
.values[].related.tags	Malware.Attribure	Tag	N/A	estimative-language:likelihood-probability="likely"	

MISP Cluster - Countries

Data from the MISP Cluster that describes "target-information" - specially countries. This is useful for information and metadata about the source/destination geography of an event.

`GET https://raw.githubusercontent.com/MISP/misp-galaxy/main/clusters/target-information.json`

Sample Response:


```
{
 "authors": [
   "Unknown"
 ],
 "category": "target",
 "description": "Description of targets of threat actors.",
 "name": "Target Information",
 "source": "Various",
 "type": "target-information",
 "uuid": "cc6feae0-968a-11e9-a29a-bf581ae8eee3",
 "values": [
   {
     "meta": {
       "calling-code": [
         "+352"
       ],
       "capital": [
         "Luxembourg"
       ],
       "currency": [
         "€",
         "EUR",
         "EURO"
       ],
       "iso-code": [
         "LU",
         "LUX"
       ],
       "member-of": [
         "NATO"
       ],
       "official-languages": [
         "French",
         "Luxembourgish",
         "German"
       ],
       "synomyms": [
         "Grand Duchy of Luxembourg",
         "Grand-Duché de Luxembourg",
         "Lëtzebuerg",
```

```
          "Groussherzogtum Lëtzebuerg",
          "Luxemburg",
          "Großherzogtum Luxemburg"
        ],
        "territory-type": [
          "Country"
        ],
        "top-level-domain": "lu"
      },
      "uuid": "f9a1d7f4-980a-11e9-a8b6-23162ddc4255",
      "value": "Luxembourg"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
.values[].value	Identity.Value	N/A	N/A	United Kingdom
.values[].meta.member-of	Identity.Value	N/A	N/A	NATO
.values[].meta.synonyms	Identity.Attribute	Synonym	N/A	UK
N/A	Identity.Attribute	Type	N/A	Country
.values[].meta.calling-code	Identity.Attribute	Calling Code	N/A	+44
.values[].meta.capital	Identity.Attribute	Capital	N/A	Luxembourg
.values[].meta.iso-code	Identity.Attribute	Country Code	N/A	LUX
.values[].meta.top-level-domain	Identity.Attribute	Top Level Domain	N/A	.uk
.values[].meta.currency	Identity.Attribute	Currency	N/A	Lek
.values[].meta.territory-type	Identity.Attribute	Territory Type	N/A	Country
.values[].meta.official-languages	Identity.Attribute	Official language	N/A	Albanian
.values[].uuid	Identity.Attribute	MISP UUID	N/A	2d0b4ddc-4b46-4e75-8c8b-02f4f7446507

MISP Cluster - Tool

Threat-actor-tools is an enumeration of tools used by adversaries. The list includes malware but also common software regularly used by the adversaries.

```
GET https://raw.githubusercontent.com/MISP/misp-galaxy/main/clusters/tool.json
```

Sample Response:


```
{
  "authors": [
    "Alexandre Dulaunoy",
    "Florian Roth",
    "Timo Steffens",
    "Christophe Vandeplas",
    "Dennis Rand",
    "raw-data"
  ],
  "category": "tool",
  "description": "threat-actor-tools is an enumeration of tools used by
adversaries. The list includes malware but also common software regularly used
by the adversaries.",
  "name": "Tool",
  "source": "MISP Project",
  "type": "tool",
  "uuid": "0d821b68-9d82-4c6d-86a6-1071a9e0f79f",
  "values": [
    {
      "description": "Banking Malware",
      "meta": {
        "refs": [
          "https://thehackernews.com/search/label/Zusy%20Malware",
          "http://blog.trendmicro.com/trendlabs-security-intelligence/the-
tinbatinybanker-malware/"
        ],
        "synonyms": [
          "Hunter",
          "Zusy",
          "TinyBanker"
        ],
        "type": [
          "Banking"
        ]
      },
      "related": [
        {
          "dest-uuid": "96b2b31e-b191-43c4-9929-48ba1cbee62c",
          "tags": [
            "estimative-language:likelihood-probability=\"likely\""
          ],
```

```
          "type": "similar"
        },
        {
          "dest-uuid": "5594b171-32ec-4145-b712-e7701effffdd",
          "tags": [
            "estimative-language:likelihood-probability=\"likely\""
          ],
          "type": "similar"
        },
        {
          "dest-uuid": "5eee35b6-bd21-4b67-b198-e9320fcf2c88",
          "tags": [
            "estimative-language:likelihood-probability=\"likely\""
          ],
          "type": "similar"
        }
      ],
      "uuid": "75f53ead-1aee-4f91-8cb9-b4170d747cfc",
      "value": "Tinba"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.values[].value	Tool.Value	N/A	N/A	Zeus	
.values[].value	Tool.Attribute	Common Name	N/A	Zeus	Only applies to tools created from `.values[].synonyms`
.values[].meta.synonyms	Tool.Value	N/A	N/A	Zbot	
.values[].meta.synonyms	Tool.Attribute	Synonym	N/A	Zbot	Only applies to tools created from `.values[].value`
.values[].meta.description	Tool.Description	N/A	N/A	Trojan (RAT) linked to current targeted attacks and others dating back to at least early 2009	
.values[].meta.refs	Tool.Attribute	Reference URL	N/A	https://www.zscaler.com/pdf/whitepapers/msupdater_trojan_whitepaper.pdfx	
.values[].meta.country	Tool.Attribute	Country	N/A	IT	
.values[].related.type	Tool.Attribure	Type	N/A	similar	
.values[].related.tags	Tool.Attribure	Tag	N/A	estimative-language:likelihood-probability="likely"	

Average Feed Run

> Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

MISP Cluster - Threat Actors - Indicators

Scheduled run ingesting CVE data as CVE Indicators (default configuration).

METRIC	RESULT
Run Time	1 minute
Adversaries	885
Adversary Attributes	3,703
Indicators	6

MISP Cluster - Threat Actors - Indicators and Vulnerabilities

Scheduled run ingesting CVE data as CVE Indicators and Vulnerabilities.

METRIC	RESULT
Run Time	1 minute
Adversaries	885
Adversary Attributes	3,703
Vulnerabilities	6

METRIC	RESULT
Indicators	6

MISP Cluster - Branded Vulnerabilities - Indicators

Scheduled run ingesting CVE data as CVE Indicators (default configuration).

METRIC	RESULT
Run Time	1 minute
Vulnerabilities	14
Indicators	17
Indicator Attributes	34

MISP Cluster - Branded Vulnerabilities - Indicators and Vulnerabilities

Scheduled run ingesting CVE data as CVE Indicators and Vulnerabilities.

METRIC	RESULT
Run Time	1 minute
Vulnerabilities	31
Vulnerability Attributes	34
Indicators	17
Indicator Attributes	34

MISP Cluster - Ransomware

METRIC	RESULT
Run Time	2 minutes
Indicators	432
Indicator Attributes	432
Malware	808
Malware Attributes	4,433

MISP Cluster - Android Malware

METRIC	RESULT
Run Time	1 minute
Malware	442
Malware Attributes	912

MISP Cluster - RAT

METRIC	RESULT
Run Time	1 minute
Malware	303
Malware Attributes	1,113

MISP Cluster - Banker

METRIC	RESULT
Run Time	1 minute
Malware	94
Malware Attributes	334

MISP Cluster - Countries

METRIC	RESULT
Run Time	1 minute
Identities	241
Identity Attributes	1,668

MISP Cluster - Tool

METRIC	RESULT
Run Time	1 minute
Malware	743
Malware Attributes	1,113

Change Log

- **Version 1.0.1**
  - Removed an extra Status setting to ensure that indicators respect the configuration selections of the user.
- **Version 1.0.0**
  - Initial release