ThreatQuotient

Mandiant Intelligence Reports CDF

Version 2.0.2

January 21, 2025

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.

Copyright © 2025 ThreatQuotient, Inc.
All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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	2.0.2
Compatible with ThreatQ Versions	>= 5.6.0
Support Tier	ThreatQ Supported

Introduction

The Mandiant Intelligence Reports integration allows a user to ingest threat intelligence reports from Mandiant's API.

The integration provides the following feeds:

- **Mandiant Intelligence Reports** - returns a list of finished intelligence reports created by Mandiant.
- **Mandiant Report Download (Supplemental)** - returns details of a Mandiant report.
- **Mandiant Report Related Indicators (Supplemental)** - returns indicators from a Mandiant report.

The integration ingests the following system object types:

- Adversaries
- Indicators
- Malware
- Reports
- Vulnerabilities
- TTP
- Signatures

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:

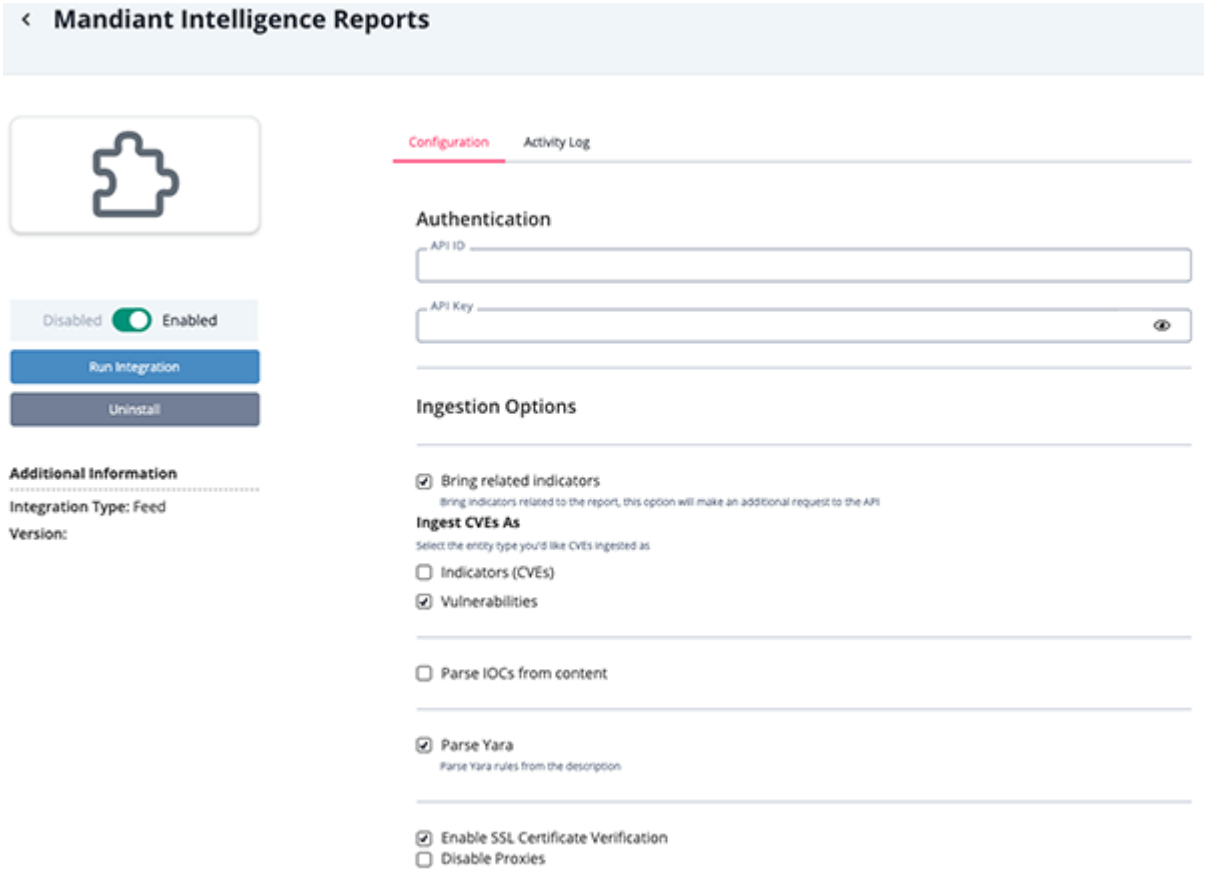
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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
API ID	Your Mandiant API ID used for authentication.
API Key	Your Mandiant API key used for authentication.
Ingest CVEs As	Select the entity type you'd like CVEs ingested as. Options include: ◦ Indicators ◦ Vulnerabilities (default)
Parse IoCs from content	If enabled, select the IOC types you would like to automatically parse from the content. Options include: ◦ CVE ◦ IP Address ◦ IPv6 Address ◦ CIDR Block ◦ MD5 ◦ SHA-1 ◦ SHA-256 ◦ SHA-512 ◦ Email Address ◦ Registry Key
Bring Related Indicators	Enable this parameter to bring in indicators related to the report. > Enabling this option will result in an additional API request.

PARAMETER	DESCRIPTION
Parse YARA	Enable if this parameter to ingest the YARA rules present in the description.
Enable SSL Certificate Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.



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

Mandiant Intelligence Reports

Retrieves a list of reports from Mandiant. Additionally, the `objects[].report_id` is used as a parameter in the Mandiant Report Download supplemental feed call.

`GET https://api.intelligence.mandiant.com/v4/reports`

Sample Response:


```
{
  "next":
"DnF1ZXJ5VGhlbkZldGNoAwAAAAfysFdFkxkSkRHeU1DUXJDRVlyYXN4UW5wSmcAAAAAGnyQvBZSZ2
loUlRuRVRueXJ2bXptWHh3eXFRAAAAAB0MHPUWUU9NTTVqYWpTeENGWnF0VTd0Q0Vhdw==",
  "objects": [
    {
      "id": "report--19234216-0b31-50b1-88bc-e862b1a6ec80",
      "report_id": "23-00007019",
      "title": "A LNK Between Browsers",
      "audience": [
          "Media Highlights"
      ],
      "publish_date": "2023-11-10T20:14:41.018Z",
      "version": "1",
      "version_one_publish_date": "2023-11-10T20:14:41.018Z",
      "intelligence_type": "tmh",
      "report_type": "TTP Deep Dive",
      "report_link": "https://advantage.mandiant.com/reports/23-00007019"
    }
  ],
  "total_count": 3054
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.objects[].report_link	report.attribute	Report Link	.publish_date	https://advantage.mandiant.com/reports/22-00015388	N/A

Mandiant Report Download (Supplemental)

The supplemental feed uses the `objects[].report_id` retrieved from the Mandiant Intelligence Reports as the `reportId` parameter in order to fetch the detailed report.

`GET https://api.intelligence.mandiant.com/v4/report/{reportId}`

Sample Response:


```
{
    "id": "report--fe809b11-9789-51a6-96f7-14ff8088656e",
    "report_id": "23-00007019",
    "report_type": "TTP Deep Dive",
    "version": 1,
    "publish_date": "2023-04-28T19:28:47.15Z",
    "title": "A LNK Between Browsers",
    "audience": [
        "cyber crime",
        "cyber espionage"
    ],
    "threat_scape": [
        "Cyber Crime",
        "Cyber Espionage"
    ],
    "requester_org_id": "ThreatQ - Development Org v4",
    "previous_versions": [
        {
            "report_id": "23-00007019",
            "title": "Mandiant Blog: A LNK Between Browsers",
            "publish_date": "2023-04-28T19:28:47.15Z",
            "version_number": 1
        }
    ],
    "version_one_publish_date": "2023-04-28T19:28:47.15Z",
    "threat_detail": "<p style=\"margin: 0in; font-size: 10pt; font-family:
'Open Sans';\"><span style=\"font-size: 12.0pt;\">Two pillars in sleight of
hand magic are <em>User Initiated Action</em>, where the target needs to
believe their actions are their own, and <em>Hidden Action</em>, where the
trick needs to be concealed behind something ordinary and nonthreatening.
Mandiant became aware of a chain of adversary methodologies that leverage these
two pillars to achieve <a style=\"font-family: 'Open Sans'; color: navy; text-
decoration: underline;\" href=\"https://attack.mitre.org/tactics/
TA0003/\">persistence</a>.</span></p>\n<p style=\"margin: 0in; font-size: 10pt;
font-family: 'Open Sans';\"><span style=\"font-size: 12.0pt;\"> </span></
p>\n<ol style=\"margin-bottom: 0in; font-family: 'open sans', sans-serif; font-
size: 12pt;\">\n<li><span style=\"font-size: 12.0pt;\">The user executes an LNK
shortcut file that, unbeknownst to them, has been tampered with.</span></
li>\n<li><span style=\"font-size: 12.0pt;\">The modified LNK shortcut file
executes a legitimate browser, hiding the malicious extension.</span></li>\n</
ol>\n<p style=\"margin: 0in; font-size: 10pt; font-family: 'Open Sans';\"><span
style=\"font-size: 12.0pt;\"> </span></p>\n<p style=\"margin: 0in; font-
```

size: 10pt; font-family: 'Open Sans';\"><span style=\"font-size: 12.0pt;\">If the technical sleight of hand is successful, the adversary will achieve persistence by means of malicious Chromium-based browser extensions.</p>\n<p style=\"margin: 0in; font-size: 10pt; font-family: 'Open Sans';\"><span style=\"font-size: 12.0pt;\"> </p>\n<p style=\"margin: 0in; font-size: 10pt; font-family: 'Open Sans';\"><span style=\"font-size: 12.0pt;\">While hunting this methodology, Mandiant identified BRAINSTORM, a rust-based dropper that ultimately led to RILIDE, a Chromium-based extension first publicly reported by SpiderLabs. Careful investigation identified that the email and cryptocurrency theft ecosystem of RILIDE is larger than reported. This research dissects the relevant adversary methodologies, discusses the identified malware families abusing this methodology, and includes numerous detection opportunities to expand the defender's hunting and detection repertoire.</p>\n<p style=\"margin: 0in; font-size: 10pt; font-family: 'Open Sans';\"><span style=\"font-size: 12.0pt;\"> </p>\n<p style=\"margin: 0in; font-size: 10pt; font-family: 'Open Sans';\"><span style=\"font-size: 12.0pt;\">The Connection from LNK to Extension</p>\n<p style=\"margin: 0in; font-size: 10pt; font-family: 'Open Sans';\"><span style=\"font-size: 12.0pt;\"> </p>\n<p style=\"margin: 0in; font-size: 10pt; font-family: 'Open Sans';\"><span style=\"font-size: 12.0pt;\">The LNK File</p>\n<p style=\"margin: 0in; font-size: 10pt; font-family: 'Open Sans';\"><span style=\"font-size: 12.0pt;\"> </p>\n<p style=\"margin: 0in; font-size: 10pt; font-family: 'Open Sans';\"><span style=\"font-size: 12.0pt;\">Files with the extension .lnk are colloquially known as LNK files, but are officially known as Shell Link Binary Files, and they follow a standardized format. LNK files contain information that points a user's interaction to another data object on the system. In many instances, this is transparent to an end user. A Windows user may click on the Google Chrome icon in the Start Menu and Chrome opens. What is not shown to the user is that they are executing an LNK file with properties that point to the actual Chrome executable.</p>\n<p style=\"margin: 0in; font-size: 10pt; font-family: 'Open Sans';\"><span style=\"font-size: 12.0pt;\"> </p>\n<p style=\"margin: 0in; font-size: 10pt; font-family: 'Open Sans';\"><span style=\"font-size: 12.0pt;\">RILIDE C&C URL</p>\n</td>\n</tr>\n<tr style=\"height: 15.0pt;\">\n<td style=\"width: 238.0pt; border: solid windowtext 1.0pt; border-top: none; padding: 0in 5.4pt 0in 5.4pt; height: 15.0pt;\">\n<p style=\"margin: 0in; font-size: 10pt; font-family: 'Open Sans';\"><span style=\"font-size: 12.0pt;\">https://vceilinichego.ru/api/machine/get-urls</p>\n</td>\n<td style=\"width: 202.75pt; border-top:

```
none; border-left: none; border-bottom: solid windowtext 1.0pt; border-right:
solid windowtext 1.0pt; padding: 0in 5.4pt 0in 5.4pt; height: 15.0pt;\">\n<p
style=\"margin: 0in; font-size: 10pt; font-family: 'Open Sans';\"><span
style=\"font-size: 12.0pt;\">RILIDE C&amp;C URL</span></p>\n</td>\n</tr>\n<tr
style=\"height: 15.0pt;\">\n<td style=\"width: 238.0pt; border: solid
windowtext 1.0pt; border-top: none; padding: 0in 5.4pt 0in 5.4pt; height:
15.0pt;\">\n<p style=\"margin: 0in; font-size: 10pt; font-family: 'Open Sans';
\"><span style=\"font-size: 12.0pt;\">https://vceilinichego.ru/api/machine/
init</span></p></p>",
    "executive_summary": "<ul style=\"margin-bottom: 0in; font-family: 'open
sans', sans-serif; font-size: 12pt;\">\n<li><strong><span style=\"font-size:
12pt;\">A version of this report will appear on the Mandiant blog the week of
</span></strong><strong><span style=\"font-size: 12pt;\">May 1, 2023.</span></
strong></li>\n</ul>",
    "tags": {
        "malware_families": [
            {
                "id": "malware--276eca6c-68bd-541d-8f3e-6ef07f544145",
                "name": "BRAINSTORM",
                "aliases": [
                    "BRAINSTORM"
                ]
            }
        ]
    },
    "relations": {},
    "files": [
        {
            "identifier": "Attacker",
            "size": "17825792",
            "name": "undefined.exe",
            "md5": "5133177ac4950cf772d2f729bb0622ec",
            "sha1": "042839871fa456d7d82b34a1eb85de5afe54ccd1",
            "sha256":
"1cc7939b1a7d7462f1cf54ba88d2ab2b62a70e225d31b4883e9c42ecbd230ff3",
            "type": "application/x-dosexec"
        }
    ],
    "networks": [
        {
            "identifier": "Attacker",
            "network_type": "url",
            "port": "443",
            "protocol": "https",
            "url": "https://panger-top.click/1/install-win64-11.5.8_en-US.exe"
        }
    ],
    "cvss_base_score": "0",
    "cvss_temporal_score": "0",
    "zero_day": false,
    "in_the_wild": false,
```

```
    "report_confidence": "ND"
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.title	report.value	N/A	.publish_date	Mandiant Blog: A LNK Between Browsers	N/A
.report_type + .publish_date + .executive_summary + .threat_detail	report.description	N/A	N/A	`Report Type: TTP Deep Dive Published At: 2023-04-28T19:28:47.15Z Executive Summary [Truncated - see full report]` will be appended to the description.	N/A
.executive_summary	attack_pattern.value	N/A	N/A	N/A	N/A
.audience	report.attribute	Audience	.publish_date	cyber crime	N/A
.report_type	report.attribute	Report Type	.publish_date	TTP Deep Dive	N/A
.outlet	report.attribute	Media Outlet	.publish_date	N/A	N/A
.tmh_accuracy_ranking	report.attribute	Accuracy Ranking	.publish_date	N/A	N/A
.document_type	report.attribute	Document Type	.publish_date	N/A	N/A
.customer_sensitive	report.attribute	Customer Sensitive	.publish_date	N/A	N/A
.mitigations	report.attribute	Mitigation	.publish_date	N/A	N/A
.risk_rating	report.attribute	Risk Rating	.publish_date	N/A	N/A
.report_id	report.attribute	Report ID	.publish_date	23-00007019	N/A
.previous_versions[].version_number	report.attribute	Previous Version Number	.publish_date	1	If multiple `previous_version` objects exist, only the most recent `previous_version` object is reported.
.previous_versions[].publish_date	report.attribute	Previous Version Date	.publish_date	2023-04-28 19:28:47-00:00	If multiple `previous_version` objects exist, only the most recent `previous_version` object is reported.
.tags.affected_industries[]	report.attribute / adversary.attribute / malware.attribute	Affected Industry	.publish_date	Civil N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.tags.affected_systems[]	report.attribute / adversary.attribute / malware.attribute	Affected System	.publish_date	N/A	N/A
.tags.motivations[]	report.attribute / adversary.attribute / malware.attribute	Motivation	.publish_date	N/A	N/A
.tags.source_geographies[]	report.attribute / adversary.attribute / malware.attribute	Source Geography	.publish_date	N/A	N/A
.tags.target_geographies[]	report.attribute / adversary.attribute / malware.attribute	Target Geography	.publish_date	N/A	N/A
.tags.targeted_informations[]	report.attribute / adversary.attribute / malware.attribute	Targeted Information	.publish_date	N/A	N/A
.tags.intended_effects[]	report.attribute / adversary.attribute / malware.attribute	Intended Effect	.publish_date	N/A	N/A
.tags.ttps[]	report.attribute / adversary.attribute / malware.attribute	TTP	.publish_date	N/A	N/A
.tags.actors[].name	adversary.name	N/A	.publish_date	n/A	Adversary objects are related to the primary Report object.
.tags.actors[].id	adversary.attribute	ID	.publish_date	N/A	N/A
.tags.malware_families[].name	malware.value	N/A	.publish_date	BRAINSTORM	Malware objects are related to the primary Report object and all other Adversary, Malware, and Indicator objects parsed from the Report object.
.tags.malware_families[].id	malware.attribute	ID	.publish_date	malware--276eca6c-68bd-541d-8f3e-6ef07f544145	N/A
.tags.malware_families[].aliases[]	malware.attribute	Alias	.publish_date	BRAINSTORM	N/A
.networks[].ip	related indicator.value	IP Address	.publish_date	n/A	N/A
.networks[].url	related indicator.value	URL	.publish_date	https://panger-top.click/1/install-win64-11.5.8_en-US.exe	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.networks[].port	indicator.attribute	Port	.publish_date	443	N/A
.networks[].protocol	indicator.attribute	Protocol	.publish_date	http	N/A
.networks[].identifier	indicator.attribute	Identifier	.publish_date	N/A	N/A
.networks[].domain	related indicator.value	FQDN	.publish_date	N/A	N/A
.files[].name	related indicator.value	Filename	.publish_date	undefined.exe	N/A
.files[].sha1	related indicator.value	SHA-1	.publish_date	042839871fa456d7d82b34a1eb85de5afe54ccd1	N/A
.files[].sha256	related indicator.value	SHA-256	.publish_date	1cc7939b1a7d7462f1cf54ba88d2ab2b62a70e225d31b4883e9c42ecbd230ff3	N/A
.files[].md5	related indicator.value	MD5	.publish_date	5133177ac4950cf772d2f729bb0622ec	N/A
.files[].size	indicator.attribute	File Size	.publish_date	17825792	N/A
.files[].identifier	indicator.attribute	Identifier	.publish_date	Attacker	N/A
.files[].type	indicator.attribute	File Type	.publish_date	application/x-dosexec	N/A
.files[].malwareFamily	indicator.attribute	Malware Family	.publish_date	N/A	N/A
.files[].actor	indicator.attribute	Actor	.publish_date	N/A	N/A
.threat_scape	report.attribute / indicator.attribute	Threat Scape	.publish_date	Cyber Crime	N/A
.cvss_base_score	report.attribute / adversary.attribute / cve.attribute	CVSS Base Score	.publish_date	0	N/A
.cvss_temporal_score	report.attribute / adversary.attribute / cve.attribute	CVSS Temporal Score	.publish_date	0	N/A
.report_confidence	report.attribute / adversary.attribute / cve.attribute	Report Confidence	.publish_date	ND	N/A
.in_the_wild	report.attribute / adversary.attribute / cve.attribute	Observed in the Wild	.publish_date	false	N/A
.zero_day	report.attribute / adversary.attribute / cve.attribute	Has Zero Day	.publish_date	false	N/A
.affected_vendors	report.attribute / adversary.attribute / cve.attribute	Affected Vendor	.publish_date	N/A	N/A
.threat_detail	related indicator.value	IP Address, CVE, MD5, SHA-1,	.publish_date	https://vceilinichego.ru/api/machine/init	Indicators are parsed out of

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
		SHA-256, or SHA-512			the description

Mandiant Report Related Indicators (Supplemental)

The Mandiant Report Related Indicators Supplemental feed uses `objects[].report_id` retrieved from the Mandiant Intelligence Reports as the `reportId` parameter to fetch the related indicators from the report.

`GET https://api.intelligence.mandiant.com/v4/report/{reportId}/indicators`

Sample Response:

```
{
    "id": "report--40407bd5-07d9-5073-90b0-68ef23ea35f8",
    "report_id": "25-10001400",
    "report_type": "News Analysis",
    "version": "1.0",
    "title": "RedDelta Deploys PlugX Malware to Target Mongolia and Taiwan in
Espionage Campaigns",
    "audience": [
        "Media Highlights",
        "cyber espionage"
    ],
    "publish_date": "2025-01-10T20:40:55.000Z",
    "threat_scape": [
        "Cyber Espionage"
    ],
    "indicators": [
        {
            "id": "md5--617f53c1-d40a-5697-bd6d-1c5ec6e1512e",
            "mscore": 100,
            "type": "md5",
            "value": "7f091aac694a1cdc6060f474999c5c96",
            "is_publishable": true,
            "sources": [
                {
                    "first_seen": "2024-11-13T15:20:44.000+0000",
                    "last_seen": "2024-11-13T15:20:44.000+0000",
                    "osint": false,
                    "category": [],
                    "source_name": "Mandiant"
                }
            ],
            "associated_hashes": [
                {
                    "id": "md5--ce4fb3fe-79f2-5ba0-a18b-a4b514d80cfd",
                    "type": "md5",
```

```
                    "value": "2ee40f0dba22041a049604df232a8661"
                },
                {
                    "id": "sha1--6bffdaed-7978-5da8-8715-c97e7b84430f",
                    "type": "sha1",
                    "value": "eef3d508447d4bfa20c9d88ddcc0974dcc3e0ec3"
                },
                {
                    "id": "sha256--132c7ae6-1b0d-56d2-9396-1e479331e7ee",
                    "type": "sha256",
                    "value":
"f84f24225866ccd14dfda0ffcebb071960af02aca6d588e3dd7dff412c2d8c33"
                }
            ],
            "misp": {
                "akamai": false,
                "alexa": false,
                "amazon-aws": false,
                "apple": false,
                "automated-malware-analysis": false,
                "tranco10k": false,
                "umbrella-blockpage-hostname": false,
                "umbrella-blockpage-v4": false,
                "umbrella-blockpage-v6": false,
                "university_domains": false,
                "url-shortener": false,
                "vpn-ipv4": false,
                "vpn-ipv6": false,
                "whats-my-ip": false,
                "wikimedia": false,
                "zscaler": false
            },
            "last_updated": "2025-01-10T20:40:56.727Z",
            "first_seen": "2024-10-26T16:41:45.000Z",
            "last_seen": "2025-01-10T14:53:18.000Z"
        }
    ],
    "indicator_count": {
        "total": 65,
        "file": 65,
        "hash": 195,
        "url": 0,
        "fqdn": 0,
        "ipv4": 0,
        "email": 0
    },
    "next":
"FGluY2x1ZGVfY29udGV4dF91dWlkDnF1ZXJ5VGhlbkZldGNoKhY4NUFEWGJSNlNoS3JyZFNDSUczaz
h3AAAAAKPHyDwWZmNRSTJMb3dTZGV0T2dQeWFRWVRzURZwaUJyR251elE0bVdDSmpMWEpDQ3lRAAAAA
JM5owsWWVBZNlNRUVNSei1wLUgwdjZHT0RmQRZ2allWRnlLYlF3LXc2SklUcE1EcDFRAAAAAIJB8tcW
```

```
OHZrbVJLVnZULU9HUzc1Z181Ql9GZxZpd1UteGl4MVNxV0VOeW8zMGdSdXZnAAAAAIgjCFMWRmpzOVV
6NlhTcnFqVHlMRDFmT0JKdxZkV21TMXI3SVNfQ05wSy1oNkxTbk9BAAAAAJ0zJBAWQkJnVDJUX0NTLU
tGYmxqYnJOMkFGQRZ3cVdTUlU3QlFkZXEyNUZhWW4zSXJRAAAAAH05h6kWTEhuQjNOOGpUQjJJS2pSQ
TZCdmNWZxZ4T0YwVHdXZVNndWNvOE9mek1MOGFRAAAAAISy3I8WRnQzblgySkRRLS05dmVmY2RRY0p6
URZ0S1JfWVU4LVJLbXpqSWJfQUZETURBAAAAAJCunc8WY3ZIaG40LWJUUmE4NDNOS0dQc3JlURZ0S1J
fWVU4LVJLbXpqSWJfQUZETURBAAAAAJCundAWY3ZIaG40LWJUUmE4NDNOS0dQc3JlURZKanBaTllwSV
E4eV94M1ZFODRaU0JBAAAAAJFHqzQWanNqcjBuc1pRZlNkYVJaQ0traXh5QRZ3cVdTUlU3QlFkZXEyN
UZhWW4zSXJRAAAAAH05h6oWTEhuQjNOOGpUQjJJS2pSQTZCdmNWZxZTY2l2NWtOMVJqQzhoSElsSmZJ
cnF3AAAAAHj9_KcWQXpndHZHV0dROHk0WVA0OGVaVWx4QRZkV21TMXI3SVNfQ05wSy1oNkxTbk9BAAA
AAJ0zJBEWQkJnVDJUX0NTLUtGYmxqYnJOMkFGQRZ4T0YwVHdXZVNndWNvOE9mek1MOGFRAAAAAISy3J
EWRnQzblgySkRRLS05dmVmY2RRY0p6URZ4T0YwVHdXZVNndWNvOE9mek1MOGFRAAAAAISy3JAWRnQzb
lgySkRRLS05dmVmY2RRY0p6URZTY2l2NWtOMVJqQzhoSElsSmZJcnF3AAAAAHj9_KgWQXpndHZHV0dR
OHk0WVA0OGVaVWx4QRZTY2l2NWtOMVJqQzhoSElsSmZJcnF3AAAAAHj9_KkWQXpndHZHV0dROHk0WVA
0OGVaVWx4QRZmRUJxcGtCX1FqQ2xvQkN3d1dVcGZBAAAAAIYhk3cWT2RwcTBCOFFRaW1WdmZqLVV2bj
dGQRZwaUJyR251elE0bVdDSmpMWEpDQ3lRAAAAAJM5owwWWVBZNlNRUVNSei1wLUgwdjZHT0RmQRZwa
UJyR251elE0bVdDSmpMWEpDQ3lRAAAAAJM5ow0WWVBZNlNRUVNSei1wLUgwdjZHT0RmQRY4NUFEWGJS
NlNoS3JyZFNDSUczazh3AAAAAKPHyD0WZmNRSTJMb3dTZGV0T2dQeWFRWVRzURZpd1UteGl4MVNxV0V
OeW8zMGdSdXZnAAAAAIgjCFQWRmpzOVV6NlhTcnFqVHlMRDFmT0JKdxZ2allWRnlLYlF3LXc2SklUcE
1EcDFRAAAAAIJB8tgWOHZrbVJLVnZULU9HUzc1Z181Ql9GZxZ2allWRnlLYlF3LXc2SklUcE1EcDFRA
AAAAIJB8tkWOHZrbVJLVnZULU9HUzc1Z181Ql9GZxZkV21TMXI3SVNfQ05wSy1oNkxTbk9BAAAAAJ0z
JBIWQkJnVDJUX0NTLUtGYmxqYnJOMkFGQRZmRUJxcGtCX1FqQ2xvQkN3d1dVcGZBAAAAAIYhk3gWT2R
wcTBCOFFRaW1WdmZqLVV2bjdGQRZkV21TMXI3SVNfQ05wSy1oNkxTbk9BAAAAAJ0zJBMWQkJnVDJUX0
NTLUtGYmxqYnJOMkFGQRZ3cVdTUlU3QlFkZXEyNUZhWW4zSXJRAAAAAH05h6sWTEhuQjNOOGpUQjJJS
2pSQTZCdmNWZxZpd1UteGl4MVNxV0VOeW8zMGdSdXZnAAAAAIgjCFUWRmpzOVV6NlhTcnFqVHlMRDFm
T0JKdxZiSjgtN1RPOFJTcXBBQ1V3OEg5Ml9RAAAAAJVjCNgWUmVDVURvLURRYkt5NnRTYlQyOWc5dxZ
mRUJxcGtCX1FqQ2xvQkN3d1dVcGZBAAAAAIYhk3kWT2RwcTBCOFFRaW1WdmZqLVV2bjdGQRZ0S1JfWV
U4LVJLbXpqSWJfQUZETURBAAAAAJCundEWY3ZIaG40LWJUUmE4NDNOS0dQc3JlURZiSjgtN1RPOFJTc
XBBQ1V3OEg5Ml9RAAAAAJVjCNkWUmVDVURvLURRYkt5NnRTYlQyOWc5dxZ0S1JfWVU4LVJLbXpqSWJf
QUZETURBAAAAAJCundIWY3ZIaG40LWJUUmE4NDNOS0dQc3JlURZTY2l2NWtOMVJqQzhoSElsSmZJcnF
3AAAAAHj9_KoWQXpndHZHV0dROHk0WVA0OGVaVWx4QRZ4T0YwVHdXZVNndWNvOE9mek1MOGFRAAAAAI
Sy3JIWRnQzblgySkRRLS05dmVmY2RRY0p6URY4NUFEWGJSNlNoS3JyZFNDSUczazh3AAAAAKPHyD4WZ
mNRSTJMb3dTZGV0T2dQeWFRWVRzURZmRUJxcGtCX1FqQ2xvQkN3d1dVcGZBAAAAAIYhk3oWT2RwcTBC
OFFRaW1WdmZqLVV2bjdGQRZKanBaTllwSVE4eV94M1ZFODRaU0JBAAAAAJFHqzUWanNqcjBuc1pRZlN
kYVJaQ0traXh5QRZKanBaTllwSVE4eV94M1ZFODRaU0JBAAAAAJFHqzYWanNqcjBuc1pRZlNkYVJaQ0
traXh5QRY4NUFEWGJSNlNoS3JyZFNDSUczazh3AAAAAKPHyD8WZmNRSTJMb3dTZGV0T2dQeWFRWVRzU
RZwaUJyR251elE0bVdDSmpMWEpDQ3lRAAAAAJM5ow4WWVBZNlNRUVNSei1wLUgwdjZHT0RmQQ==.eyJ
pbmNsdWRlX2F0dHJpYnV0ZWRfYXNzb2NpYXRpb25zIjp0cnVlLCJsaW1pdCI6MjUsImVuYWJsZV9uZX
h0X3BhZ2luYXRpb24iOnRydWUsIm5leHRfcGFnZV9pbmRleCI6MSwic3lzdGVtIjoiZ2Nwb3MiLCJuZ
Xh0X3RpbWVzdGFtcCI6MTczNjc1ODg3N30="
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.indicators[].type	Indicator.Type	N/A	.indicators[].last_updated	MD5	N/A
.indicators[].Value	Indicator.Value	MD5	.indicators[].last_updated	7f091aac694a1cdc6060f474999c5c96	N/A
.indicators[].associated_hashes[].Value	Related Indicator.Value	SHA-256	.indicators[].last_updated	f84f24225866ccd14dfda0ffcebb071960af02aca6d588e3dd7dff412c2d8c33	N/A
.indicators[].associated_hashes[].Value	Related Indicator.Value	SHA-1	.indicators[].last_updated	eef3d508447d4bfa20c9d88ddcc0974dcc3e0ec3	N/A
.indicators[].associated_hashes[].Value	Related Indicator.Value	MD5	.indicators[].last_updated	2ee40f0dba22041a049604df232a8661	N/A

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.

Mandiant Intelligence Reports

METRIC	RESULT
Run Time	5 minutes
Reports	480
Report Attributes	6,950
Adversaries	53
Adversary Attributes	1,860
Indicators	1,355
Indicator Attributes	6,348
Malware	149
Malware Attributes	5,945
TTP	13
Vulnerabilities	21
Vulnerability Attributes	151

METRIC	RESULT
Signatures	41

Known Issues / Limitations

- MITRE ATT&CK attack patterns must have already been ingested by a previous run of the MITRE ATT&CK feeds in order for MITRE ATT&CK attack patterns extracted from a report's Executive Summary to be related to the report. MITRE ATT&CK attack patterns are ingested from the following feeds:
  - MITRE Enterprise ATT&CK
  - MITRE Mobile ATT&CK
  - MITRE PRE-ATT&CK

Change Log

- **Version 2.0.2**
  - Renamed the **Parse for IOCs** parameter to **Parse IOCs from Content**.
  - Added a new supplemental feed, **Mandiant Report Related Indicators**, which gives users the option to ingest indicators from reports.
  - Added the following new configuration parameters:
    - **Bring Related Indicators** - enable the feed to bring in indicators related to the report.
    - **Enable SSL Certificate Verification** - enable or disable verification of the server's SSL certificate.
    - **Disable Proxies** - determine if the feed should honor proxy settings set in the ThreatQ UI.
  - Resolved a YARA format issue that would occur after ingestion into ThreatQ.
- **Version 2.0.1**
  - Added the ability to parse YARA rules from reports with the new **Parse YARA** configuration parameter.
  - Resolved a `Type Error` that would occur with MITRE ATT&CK Patterns.
- **Version 2.0.0**
  - Added the ability to fetch data older than 90 days.
  - Added a new attribute: `Intended Effect`.
  - Updated the way relationships and attributes are made.
  - Added support for News Analysis Reports.
  - Added two new configuration options:
    - Ingest CVEs As
    - Parse for IoCs
  - The IOC Parser now utilizes the built-in ThreatQ indicator parser.
  - Vulnerability Reports will now be ingested as Vulnerability objects.
  - Resolved an issue where users would encounter a `filter-mapping` error when loading MITRE Attack Patterns from the ThreatQ API.
- **Version 1.1.4**
  - Removed the restriction on description length.
  - Resolved an issue where IOCs from report descriptions were not ingested.
  - Updated minimum ThreatQ version to 5.6.0.
- **Version 1.1.3**
  - IP addresses, FQDNs and URLs are now ingested as indicators when parsed from a report
- **Version 1.1.2**
  - Updated the `response_content_type` for all Mandiant API requests.
  - Updated the method for retrieving Attack Patterns from the ThreatQ API.
- **Version 1.1.0**
  - Decreased the number of API Attack Patterns retrieved, per request, to prevent timeout errors.
- **Version 1.0.1**

  - Fixed an issue with the `Category` field that prevented users from installing the integration on ThreatQ version 4 instances.
- **Version 1.0.0**
  - Initial release