ThreatQuotient

A Securonix Company

Google Threat Intelligence CDF

Version 2.2.0

June 23, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.com
Phone: 703.574.9893

Contents

Warning and Disclaimer **3**
Support **4**
Integration Details **5**
Introduction **6**
Prerequisites **8**
Installation **9**
Configuration **10**
Google Threat Intelligence Parameters 10
Google Threat Intelligence Campaigns 18
Google Threat Intelligence Indicators Parameters 25
Google Threat Intelligence Malware Parameters 30
Google Threat Intelligence Threat Lists Parameters 36
Google Vulnerability Intelligence Parameters 41
Google Digital Threat Monitoring Alerts Parameters 46
ThreatQ Mapping **49**
Google Threat Intelligence 49
Google Threat Intelligence Related Malware (Supplemental) 80
Google Threat Intelligence Related Attack Pattern (Supplemental) 90
Google Threat Intelligence Related Campaigns (Supplemental) 93
Google Threat Intelligence Related IOC (Supplemental) 110
IP Addresses 110
Hashes 114
FQDNs 116
URLs 121
Indicator Type Mapping 128
Google Threat Intelligence Related Vulnerabilities (Supplemental) 129
Google Threat Intelligence Related Adversaries (Supplemental) 137
Google Threat Intelligence Campaigns 139
Google Threat Intelligence Indicators 142
Google Threat Intelligence Malware 144
Google Vulnerability Intelligence 146
Google Threat Intelligence Threat Lists 157
Threat List Threat Type Mapping 160
Google Digital Threat Monitoring Alerts 161
Alert Indicators Type Mapping 167
Average Feed Run **168**
Google Threat Intelligence 168
Google Threat Intelligence Campaigns 168
Google Threat Intelligence Indicators 169
Google Threat Intelligence Malware 170
Google Vulnerability Intelligence 170
Google Threat Intelligence Threat Lists 171
Google Digital Threat Monitoring Alerts 171
Known Issues / Limitations **172**
Change Log **173**

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 © 2026 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: tq-support@securonix.com
Support Web: https://ts.securonix.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	2.2.0
Compatible with ThreatQ Versions	>= 6.6.0
Support Tier	ThreatQ Supported

Introduction

Google is on a mission to make every organization secure from cyber threats and confident in its readiness. They deliver dynamic cyber defense solutions powered by industry-leading expertise, intelligence, and innovative technology.

The Google Threat Intelligence CDF integration provides the following feeds:

- **Google Threat Intelligence** - ingests compromised Adversaries objects and any related Indicators, Malware, Vulnerabilities, Attack Patterns, and Tags.
  - **Google Threat Intelligence Related Malware (Supplemental)** - returns associated collections of malware family objects.
  - **Google Threat Intelligence Related Attack Pattern (Supplemental)** - fetches related attack patterns.
  - **Google Threat Intelligence Related Vulnerabilities (Supplemental)** - fetches related CVEs.
  - **Google Threat Intelligence Related Campaigns (Supplemental)** - returns associated collections of campaign objects.
  - **Google Threat Intelligence Related IOC (Supplemental)** - fetches related indicators to threat actors.
  - **Google Threat Intelligence Related Adversaries (Supplemental)** - fetches related adversaries.
- **Google Threat Intelligence Campaigns** - ingests a list of campaigns tracked by Google Threat Intelligence.
- **Google Threat Intelligence Indicators** - ingests a list of indicators tracked by Google Threat Intelligence.
- **Google Threat Intelligence Malware** - ingests a list of malware tracked by Google Threat Intelligence.
- **Google Vulnerability Intelligence** - ingests a list of vulnerabilities tracked by Google Threat Intelligence.
- **Google Threat Intelligence Threat Lists** - ingests indicators from the selected threat lists.
- **Google Digital Threat Monitoring Alerts** - ingests alerts for the current organization.

The integration ingests the following system objects:

- Adversaries

- Attack Patterns
- Campaigns
- Events
- Indicators
- Malware
- Signatures
- Vulnerabilities

Prerequisites

The integration requires the following:

- A Google Threat Intelligence API Key.
- MITRE ATT&CK attack patterns must have already been ingested by a previous run of the MITRE ATT&CK CDF feeds in order for MITRE TIDs extracted from Actor Profiles to be mapped to the corresponding MITRE ATT&CK attack patterns. Feeds included in the MITRE ATT&CK CDF are:
  - MITRE Enterprise ATT&CK
  - MITRE Mobile ATT&CK
  - MITRE PRE-ATT&CK

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.
>
> If you are upgrading to version 2.0.0 or later from a version > 2.0.0 and are utilizing the **Google Vulnerability Intelligence** (formerly **Mandiant Vulnerability Intelligence**) feed, you should ensure that your credentials and other configurations are backed up as you will need to re-enter your configuration and re-enable the feed after upgrading.

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

   > 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.

7. The feeds will be added to the integrations page. You will still need to configure and then enable the feeds.

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:

Google Threat Intelligence Parameters

PARAMETER	DESCRIPTION
Base URL	The base URL for the Google Threat Intelligence API. > You will not have to modify this unless Google changes its API URL.
API Key	Enter your Google Threat Intelligence API Key to authenticate.
Origin Filter	Filter the results based on the origin of the intelligence. Options include: ◦ Google Threat Intelligence (Curated) (default) ◦ Partner (i.e. AlienVaultOTX) ◦ Crowdsourced (i.e. Individual Users)

	⚠ ThreatQuotient highly recommends only selecting the curated origin to ensure data quality and reduce noise/volume.
Target Industry	Specify the industry objects you want to ingest.
Custom API Filter	An optional custom filter can be applied to all API requests when retrieving collections. This filter applies only to the top-level collection request and does not affect API calls used to fetch associated data. It is appended to the default query using logical AND and is evaluated alongside the existing `collection_type`, `origin`, `last_modification_date`, and `target_industry` filters. Additional details on filter construction are available at: https://gtidocs.virustotal.com/reference/list-threats.
Supplemental Context Confidence Filter	Specify the confidence levels of the context you want to ingest. Only context with the selected confidence levels will be included in the ingestion process. Context such as Target Industry, Target Region, Motivation, etc. are reported with a confidence level. Using this filter helps ensure that only high-confidence context is ingested into ThreatQ. Options include: ◦ Confirmed ◦ Suspected ◦ Unconfirmed
Adversaries Context Selection	Select the context to bring back with each ingested Adversary. Options include: ◦ Target Industry ◦ Target Region ◦ Target Sub Region ◦ Target Country ◦ Source Sub Region ◦ Source Country ◦ Source Country Code ◦ Motivation

	◦ Target Country Code ◦ Source Region ◦ Aliases (as Tags)
Fetch Related Attack Patterns	Enable this parameter to utilize additional API calls to fetch related Attack Patterns. ⚠ This feature can quickly consume the daily rate limit.
Fetch Related Malware	Enable this parameter to utilize additional API calls to fetch related Malware. ⚠ This feature can quickly consume the daily rate limit.
Malware Context Selection	Select the context to bring back with each ingested Malware. Options include: ◦ Industry *(default)* ◦ Target Operating System *(default)* ◦ Detection This parameter is only accessible if the **Fetch Related Malware** parameter is enabled.
Fetch Related Campaigns	Enable this parameter to utilize additional API calls to fetch related Campaigns. ⚠ This feature can quickly consume the daily rate limit.
Campaign Context Selection	Select the context to bring back with each ingested Campaign. Options include: ◦ Motivations *(default)*

- Source Regions Context
- Target regions Context

> This parameter is only accessible if the **Fetch Related Campaigns** parameter is enabled.

Fetch Related CVEs	Enable this parameter to utilize additional API calls to fetch related CVEs. ⚠ This feature can quickly consume the daily rate limit.
CVE Context Selection	Select the context to bring back with each ingested CVE. Options include: ◦ CVSS v2 Vector ◦ CVSS v2 Scores ◦ CVSS v3 Vector *(default)* ◦ CVSS v3 Scores *(default)* ◦ Exploitation Vectors ◦ EPSS Score *(default)* This parameter is only accessible if the **Fetch Related CVEs** parameter is enabled.
Ingest CVEs As	Select which entity type to ingest CVEs as into ThreatQ. Options include: ◦ Vulnerabilities ◦ Indicators (CVE) This parameter is only accessible if the **Fetch Related CVEs** parameter is enabled.
Fetch Related Indicators	Enable this parameter to utilize additional API calls to fetch related Indicators.

> ⚠ This feature can quickly consume the daily rate limit.

Ingested Indicator Types	Select the types of indicators to ingest into ThreatQ. Options include: ◦ IP Addresses *(default)* ◦ URLs *(default)* ◦ Domains *(default)* ◦ Hashes (*default*) This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Ingested Related Hash Types	Optional - Select the types of the related hashes to ingest for SHA-256. Options include: ◦ MD5 ◦ SHA-1 ◦ SHA-256 This parameter is only accessible if you have selected the Hashes (SHA-256) option for the **Ingested Indicator Types** parameter.
Minimum Threat Score Threshold	Enter the minimum score required to ingest a related indicator. The default value is 40. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Set Indicator Status to Active if Verdict is Malicious	Enable this parameter to dynamically set the status of indicators with a verdict of malicious to Active.

> This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.

Set Indicator Status to Whitelisted if Threat Score is 0	Enable this parameter to dynamically set the status of indicators with threat scores of 0 to whitelisted. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Normalize Threat Scores	Enable this parameter to normalize the Threat Score from the default 0-100 range to a human-readable value. The normalization will be based on the mapping field set in **Threat Score Normalization Mapping** parameter. This is useful for developing a ThreatQ Scoring Policy that is based on these normalized values. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Threat Score Normalization Mapping	Enter your mapping to normalize the numeric threat score values to the scorable attribute, `Normalized Threat Score`. The raw Threat Score value will always be ingested. This mapping should contain a line-separated CSV-formatted string with the following columns: Minimum, Maximum, Normalized Value. *default: (0,39,Low 40,79,Medium 80,94,High 95,100,Critical)* This parameter is only accessible if the **Fetch Related Indicators** and **Normalize Threat Scores** parameters are enabled.
Indicator Context Selection	Select the context to bring back with each ingested indicator. Verdict is not enabled by default as it's a binary value of malicious or benign. Instead, it is recommended to use the **Normalize Threat Score** parameter to create a more granular range to use in your ThreatQ Scoring Policy. Options include:

- Threat Score
- Confidence Score
- Severity
- Verdict
- Safe Browsing Verdict
- Category
- Tags
- Type Tags
- Is Pervasive
- Malicious Count
- Suspicious Count
- AS Organization
- RIR
- Country Code
- Continent Code
- ASN
- Meaningful Name
- Site Title
- Last Submission Date
- Mandiant Score (Deprecated)
- Crowdsourced IDS Signatures (Snort)

This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.

Indicator Description Context Selection

Select the context used to populate each indicator's description based on available fields. Options include:

- GTI Assessment
- WHOIS
- Crowdsourced AI Summary
- Crowdsourced Context
- Associated Names
- Outgoing Links
- Crowdsourced YARA Results
- Sigma Analysis Results

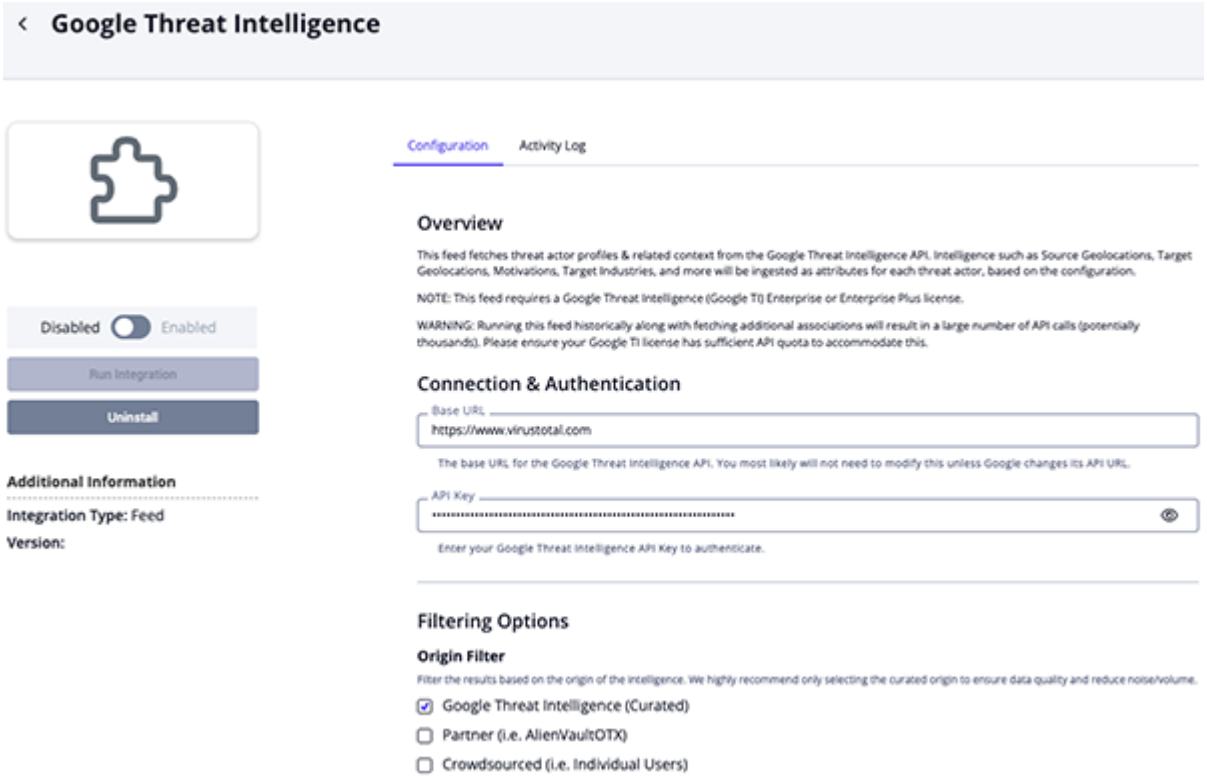
Ingests ASNs As

Select which entity type to ingest ASNs as in ThreatQ. Options include:

- Attributes (*default*)

- Indicators (Type: ASN)

Enable SSL Certificate Verification	Enable this parameter 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.



Google Threat Intelligence Campaigns

PARAMETER	DESCRIPTION
Base URL	The base URL for the Google Threat Intelligence API. You will not have to modify this unless Google changes its API URL.
API Key	Enter your Google Threat Intelligence API Key to authenticate.
Origin Filter	Filter the results based on the origin of the intelligence. Options include: ◦ Google Threat Intelligence (Curated) (default) ◦ Partner (i.e. AlienVaultOTX) ◦ Crowdsourced (i.e. Individual Users) ThreatQuotient highly recommends only selecting the curated origin to ensure data quality and reduce noise/volume.
Target Industry	Specify the industry objects you want to ingest.
Custom API Filter	An optional custom filter can be applied to all API requests when retrieving collections. This filter applies only to the top-level collection request and does not affect API calls used to fetch associated data. It is appended to the default query using logical AND and is evaluated alongside the existing `collection_type`, `origin`, `last_modification_date`, and `target_industry` filters. Additional details on filter construction are available at: https://gtidocs.virustotal.com/reference/list-threats.

Supplemental Context Confidence Filter	Specify the confidence levels of the context you want to ingest. Only context with the selected confidence levels will be included in the ingestion process. Context such as Target Industry, Target Region, Motivation, etc. are reported with a confidence level. Using this filter helps ensure that only high-confidence context is ingested into ThreatQ. Options include: ◦ Confirmed ◦ Suspected ◦ Unconfirmed
Context Options	Select the context for the campaign's attributes to ingest into ThreatQ. Options include: ◦ Target Sector ◦ Target Country ◦ Target Country Code ◦ Target Region ◦ Target Sub Region ◦ Country ◦ Country Code ◦ Region ◦ Sub Region ◦ Motivation ◦ Last Seen
Fetch Related Attack Patterns	Enable this parameter to utilize additional API calls to fetch related Attack Patterns. ⚠ This feature can quickly consume the daily rate limit.
Fetch Related Adversaries	Enable this parameter to utilize additional API calls to fetch related Adversaries. ⚠ This feature can quickly consume the daily rate limit.

Adversaries Context Selection	Select the context to bring back with each ingested Adversary. Options include: ◦ Target Industry ◦ Target Region ◦ Target Sub Region ◦ Target Country ◦ Target Country Code ◦ Source Region ◦ Source Sub Region ◦ Source Country ◦ Source Country Code ◦ Motivation ◦ Aliases (as Tags) This parameter is only accessible if the **Fetch Related Adversaries** parameter is enabled.
Fetch Related Malware	Enable this parameter to utilize additional API calls to fetch related Malware. This feature can quickly consume the daily rate limit.
Malware Context Selection	Select the context to bring back with each ingested Malware. Options include: ◦ Industry *(default)* ◦ Target Operating System *(default)* ◦ Detection This parameter is only accessible if the **Fetch Related Malware** parameter is enabled.
Fetch Related CVEs	Enable this parameter to utilize additional API calls to fetch related CVEs.

	⚠ This feature can quickly consume the daily rate limit.
CVE Context Selection	Select the context to bring back with each ingested CVE. Options include: ◦ CVSS v2 Vector ◦ CVSS v2 Scores ◦ CVSS v3 Vector *(default)* ◦ CVSS v3 Scores *(default)* ◦ Exploitation Vectors ◦ EPSS Score *(default)* ✎ This parameter is only accessible if the **Fetch Related CVEs** parameter is enabled.
Ingest CVEs As	Select which entity type to ingest CVEs as into ThreatQ. Options include: ◦ Vulnerabilities ◦ Indicators (CVE) ✎ This parameter is only accessible if the **Fetch Related CVEs** parameter is enabled.
Fetch Related Indicators	Enable this parameter to utilize additional API calls to fetch related Indicators. ⚠ This feature can quickly consume the daily rate limit.
Ingested Indicator Types	Select the types of indicators to ingest into ThreatQ. Options include: ◦ IP Addresses *(default)* ◦ URLs *(default)*

	◦ Domains *(default)* ◦ Hashes (*default*) This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Ingested Related Hash Types	Optional - Select the types of the related hashes to ingest for SHA-256. Options include: ◦ MD5 ◦ SHA-1 ◦ SHA-256 This parameter is only accessible if you have selected the Hashes option for the **Ingested Indicator Types** parameter.
Inherit Context from Indicators to Related Hashes	Enable this parameter to inherit the context from the top-level indicators to the associated hashes. This parameter is only accessible if you have selected the Hashes (SHA-256) option for the **Ingested Indicator Types** parameter.
Minimum Threat Score Threshold	Enter the minimum score required to ingest a related indicator. The default value is 40. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Set Indicator Status to Active if Verdict is Malicious	Enable this parameter to dynamically set the status of indicators with a verdict of malicious to Active. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.

Set Indicator Status to Whitelisted if Threat Score is 0	Enable this parameter to dynamically set the status of indicators with threat scores of 0 to whitelisted. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Normalize Threat Scores	Enable this parameter to normalize the Threat Score from the default 0-100 range to a human-readable value. The normalization will be based on the mapping field set in **Threat Score Normalization Mapping** parameter. This is useful for developing a ThreatQ Scoring Policy that is based on these normalized values. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Threat Score Normalization Mapping	Enter your mapping to normalize the numeric threat score values to the scorable attribute, `Normalized Threat Score`. The raw Threat Score value will always be ingested. This mapping should contain a line-separated CSV-formatted string with the following columns: Minimum, Maximum, Normalized Value. *default: (0,39,Low 40,79,Medium 80,94,High 95,100,Critical)* This parameter is only accessible if the **Fetch Related Indicators** and **Normalize Threat Scores** parameters are enabled.
Indicator Context Selection	Select the context to bring back with each ingested indicator. Verdict is not enabled by default as it's a binary value of malicious or benign. Instead, it is recommended to use the **Normalize Threat Score** parameter to create a more granular range to use in your ThreatQ Scoring Policy. Options include: ◦ Threat Score ◦ Confidence Score ◦ AS Organization ◦ RIR

- Severity
- Verdict
- Safe Browsing Verdict
- Category
- Tags
- Type Tags
- Is Pervasive
- Malicious Count
- Suspicious Count
- Country Code
- Continent Code
- ASN
- Meaningful Name
- Site Title
- Last Submission Date
- Mandiant Score (Deprecated)
- Crowdsourced IDS Signatures (Snort)

This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.

Indicator Description Context Selection

Select the context used to populate each indicator's description based on available fields. Options include:

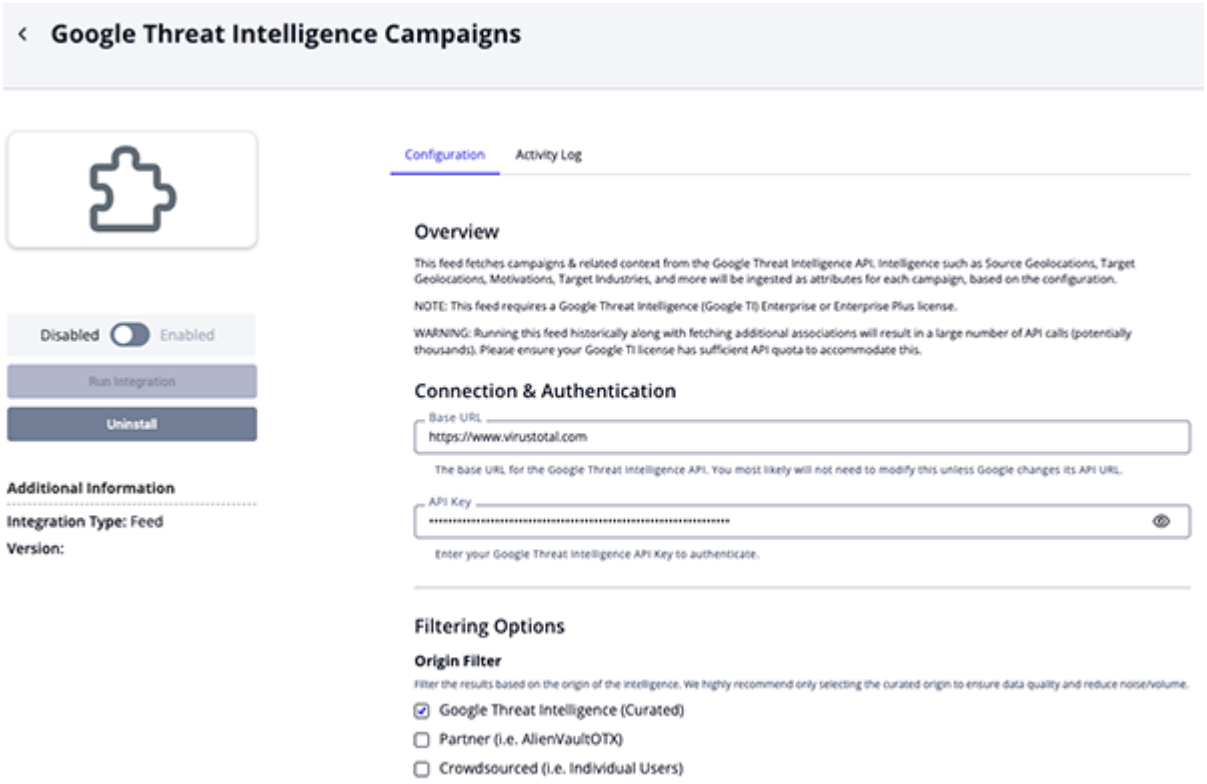
- GTI Assessment
- WHOIS
- Crowdsourced AI Summary
- Crowdsourced Context
- Associated Names
- Outgoing Links
- Crowdsourced YARA Results
- Sigma Analysis Results

Ingests ASNs As

Select which entity type to ingest ASNs as in ThreatQ. Options include:

- Attributes (*default*)
- Indicators (Type: ASN)

Enable SSL Certificate Verification	Enable this parameter 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.



Google Threat Intelligence Indicators Parameters

PARAMETER	DESCRIPTION
Base URL	The base URL for the Google Threat Intelligence API. You will not have to modify this unless Google changes its API URL.
API Key	Enter your Google Threat Intelligence API Key to authenticate.

Origin Filter	Filter the results based on the origin of the intelligence. Options include: ◦ Google Threat Intelligence (Curated) (default) ◦ Partner (i.e. AlienVaultOTX) ◦ Crowdsourced (i.e. Individual Users) ⚠ ThreatQuotient highly recommends only selecting the curated origin to ensure data quality and reduce noise/volume.
Target Industry	Specify the industry objects you want to ingest.
Custom API Filter	An optional custom filter can be applied to all API requests when retrieving collections. This filter applies only to the top-level collection request and does not affect API calls used to fetch associated data. It is appended to the default query using logical AND and is evaluated alongside the existing `collection_type`, `origin`, `last_modification_date`, and `target_industry` filters. Additional details on filter construction are available at: https://gtidocs.virustotal.com/reference/list-threats.
Ingested Indicator Types	Select the types of indicators to ingest into ThreatQ. Options include: ◦ IP Addresses *(default)* ◦ URLs *(default)* ◦ Domains *(default)* ◦ Hashes (*default*)
Ingested Related Hash Types	Optional - Select the types of the related hashes to ingest for SHA-256. Options include: ◦ MD5 ◦ SHA-1 ◦ SHA-256

	This parameter is only accessible if you have selected the `Hashes (SHA-256)` option for the **Ingested Indicator Types** parameter.
Minimum Threat Score Threshold	Enter the minimum score required to ingest a related indicator. The default value is 40. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Set Indicator Status to Active if Verdict is Malicious	Enable this parameter to dynamically set the status of indicators with a verdict of malicious to Active. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Set Indicator Status to Whitelisted if Threat Score is 0	Enable this parameter to dynamically set the status of indicators with threat scores of 0 to whitelisted. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Normalize Threat Scores	Enable this parameter to normalize the Threat Score from the default 0-100 range to a human-readable value. The normalization will be based on the mapping field set in **Threat Score Normalization Mapping** parameter. This is useful for developing a ThreatQ Scoring Policy that is based on these normalized values. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Threat Score Normalization Mapping	Enter your mapping to normalize the numeric threat score values to the scorable attribute, `Normalized Threat Score`. The raw Threat Score value will always be ingested. This mapping should contain a line-separated CSV-formatted string with the following columns:

Minimum, Maximum, Normalized Value. *default: (0,39,Low 40,79,Medium 80,94,High 95,100,Critical)*

> This parameter is only accessible if the **Fetch Related Indicators** and **Normalize Threat Scores** parameters are enabled.

Indicator Context Selection

Select the context to bring back with each ingested indicator. Verdict is not enabled by default as it's a binary value of malicious or benign. Instead, it is recommended to use the **Normalize Threat Score** parameter to create a more granular range to use in your ThreatQ Scoring Policy. Options include:

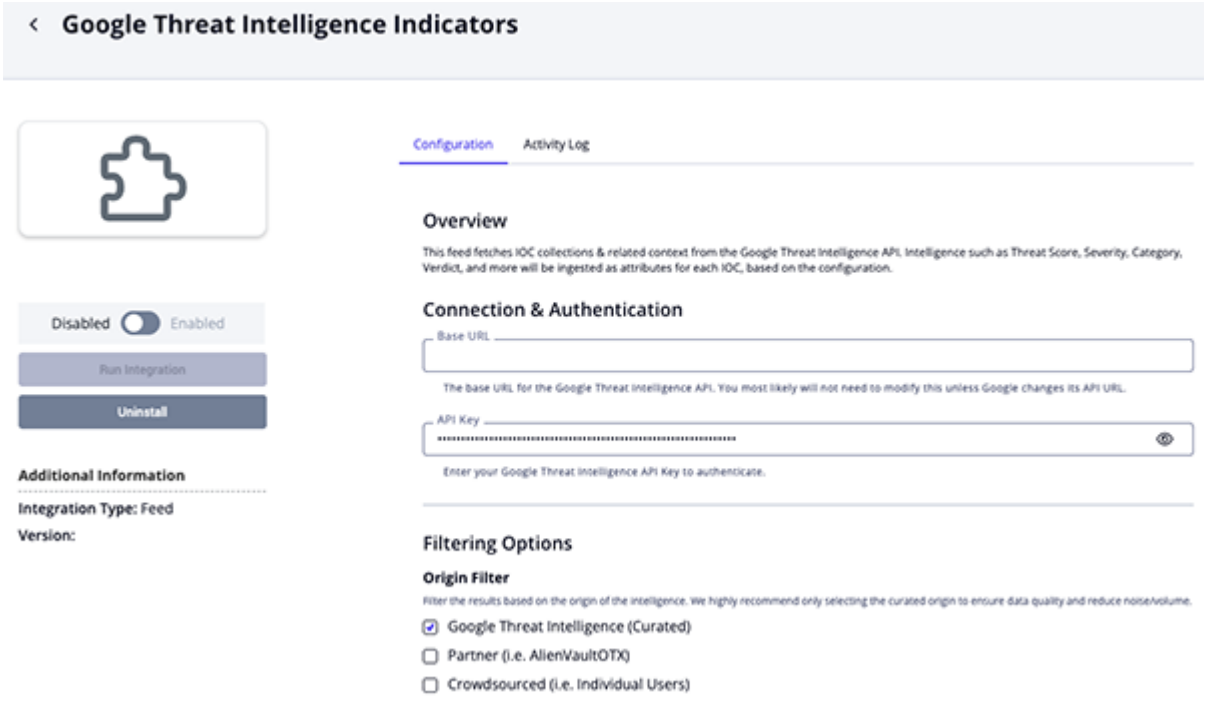
- Threat Score
- Confidence Score
- Severity
- Verdict
- Safe Browsing Verdict
- Category
- Tags
- Type Tags
- Is Pervasive
- Malicious Count
- Suspicious Count
- AS Organization
- RIR
- Country Code
- Continent Code
- ASN
- Meaningful Name
- Site Title
- Last Submission Date
- Mandiant Score (Deprecated)
- Crowdsourced IDS Signatures (Snort)

> This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.

Indicator Description

Select the context used to populate each indicator's description based on available fields. Options include:

Context Selection	◦ GTI Assessment ◦ WHOIS ◦ Crowdsourced AI Summary ◦ Crowdsourced Context ◦ Associated Names ◦ Outgoing Links ◦ Crowdsourced YARA Results ◦ Sigma Analysis Results
Ingests ASNs As	Select which entity type to ingest ASNs as in ThreatQ. Options include: ◦ Attributes (*default*) ◦ Indicators (Type: ASN)
Enable SSL Certificate Verification	Enable this parameter 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.



Google Threat Intelligence Malware Parameters

PARAMETER	DESCRIPTION
Base URL	The base URL for the Google Threat Intelligence API. You will not have to modify this unless Google changes its API URL.
API Key	Enter your Google Threat Intelligence API Key to authenticate.
Origin Filter	Filter the results based on the origin of the intelligence. Options include: ◦ Google Threat Intelligence (Curated) (default) ◦ Partner (i.e. AlienVaultOTX) ◦ Crowdsourced (i.e. Individual Users) ThreatQuotient highly recommends only selecting the curated origin to ensure data quality and reduce noise/volume.
Target Industry	Specify the industry objects you want to ingest.
Custom API Filter	An optional custom filter can be applied to all API requests when retrieving collections. This filter applies only to the top-level collection request and does not affect API calls used to fetch associated data. It is appended to the default query using logical AND and is evaluated alongside the existing `collection_type`, `origin`, `last_modification_date`, and `target_industry` filters. Additional details on filter construction are available at: https://gtidocs.virustotal.com/reference/list-threats.
Supplemental Context	Specify the confidence levels of the context you want to ingest. Only context with the selected confidence levels

Confidence Filter	will be included in the ingestion process. Context such as Target Industry, Target Region, Motivation, etc. are reported with a confidence level. Using this filter helps ensure that only high-confidence context is ingested into ThreatQ. Options include: ◦ Confirmed ◦ Suspected ◦ Unconfirmed
Context Options	Select the context for the campaign's attributes to ingest into ThreatQ. Options include: ◦ Target Sector ◦ Capability ◦ Target Operating Systems ◦ Role ◦ Aliases ◦ Last Active
Fetch Related Attack Patterns	Enable this parameter to utilize additional API calls to fetch related Attack Patterns. ⚠ This feature can quickly consume the daily rate limit.
Fetch Related Adversaries	Enable this parameter to utilize additional API calls to fetch related Adversaries. ⚠ This feature can quickly consume the daily rate limit.
Adversaries Context Selection	Select the context to bring back with each ingested Adversary. Options include: ◦ Target Industry ◦ Source Sub Region

- Target Region
- Target Sub Region
- Target Country
- Target Country Code
- Source Region
- Source Country
- Source Country Code
- Motivation
- Aliases (as Tags)

This parameter is only accessible if the **Fetch Related Adversaries** parameter is enabled.

Fetch Related CVEs

Enable this parameter to utilize additional API calls to fetch related CVEs.

This feature can quickly consume the daily rate limit.

CVE Context Selection

Select the context to bring back with each ingested CVE. Options include:

- CVSS v2 Vector
- CVSS v2 Scores
- CVSS v3 Vector *(default)*
- CVSS v3 Scores *(default)*
- Exploitation Vectors
- EPSS Score *(default)*

This parameter is only accessible if the **Fetch Related CVEs** parameter is enabled.

Ingest CVEs As

Select which entity type to ingest CVEs as into ThreatQ. Options include:

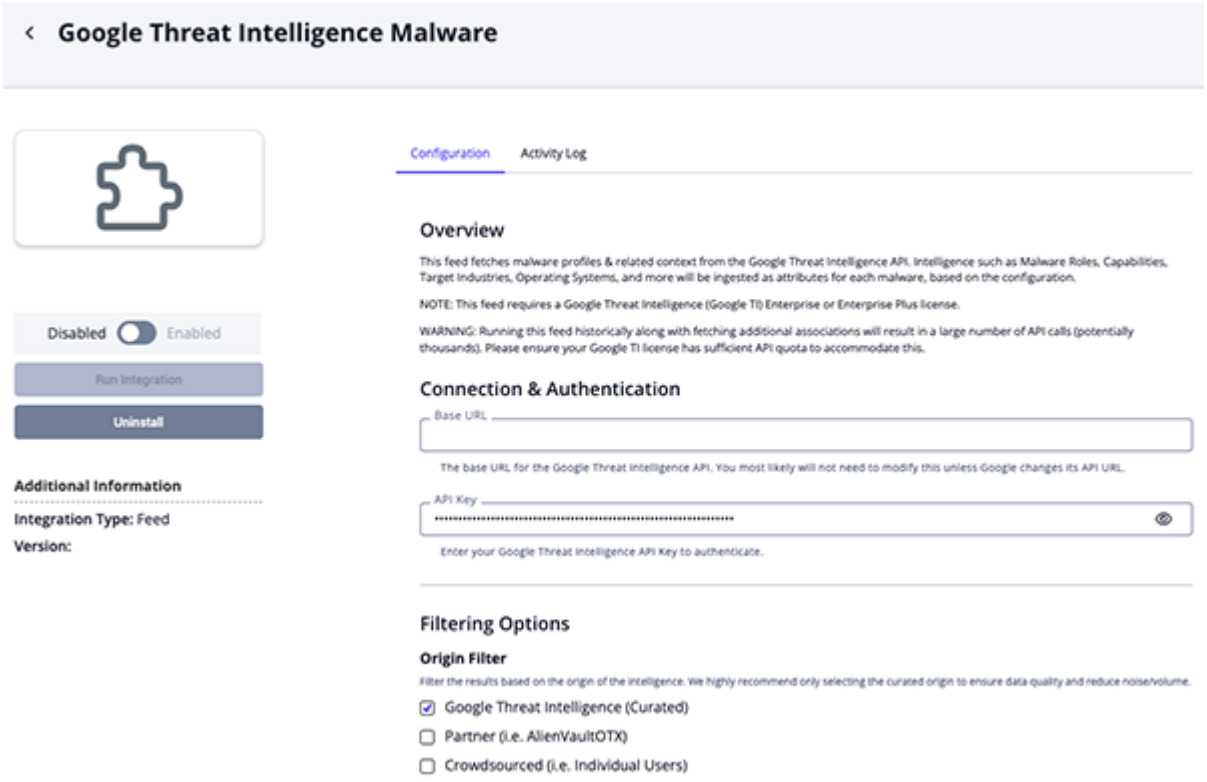
- Vulnerabilities
- Indicators (CVE)

	This parameter is only accessible if the **Fetch Related CVEs** parameter is enabled.
Fetch Related Indicators	Enable this parameter to utilize additional API calls to fetch related Indicators. This feature can quickly consume the daily rate limit.
Ingested Indicator Types	Select the types of indicators to ingest into ThreatQ. Options include: ◦ IP Addresses *(default)* ◦ URLs *(default)* ◦ Domains *(default)* ◦ Hashes (*default*) This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Ingested Related Hash Types	Optional - Select the types of the related hashes to ingest for SHA-256. Options include: ◦ MD5 ◦ SHA-1 ◦ SHA-256 This parameter is only accessible if you have selected the Hashes for the **Ingested Indicator Types** parameter.
Minimum Threat Score Threshold	Enter the minimum score required to ingest a related indicator. The default value is 40.

	This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Set Indicator Status to Active if Verdict is Malicious	Enable this parameter to dynamically set the status of indicators with a verdict of malicious to Active. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Set Indicator Status to Whitelisted if Threat Score is 0	Enable this parameter to dynamically set the status of indicators with threat scores of 0 to whitelisted. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Normalize Threat Scores	Enable this parameter to normalize the Threat Score from the default 0-100 range to a human-readable value. The normalization will be based on the mapping field set in **Threat Score Normalization Mapping** parameter. This is useful for developing a ThreatQ Scoring Policy that is based on these normalized values. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Threat Score Normalization Mapping	Enter your mapping to normalize the numeric threat score values to the scorable attribute, `Normalized Threat Score`. The raw Threat Score value will always be ingested. This mapping should contain a line-separated CSV-formatted string with the following columns: Minimum, Maximum, Normalized Value. *default: (0,39,Low 40,79,Medium 80,94,High 95,100,Critical)* This parameter is only accessible if the **Fetch Related Indicators** and **Normalize Threat Scores** parameters are enabled.

Indicator Context Selection	Select the context to bring back with each ingested indicator. Verdict is not enabled by default as it's a binary value of malicious or benign. Instead, it is recommended to use the **Normalize Threat Score** parameter to create a more granular range to use in your ThreatQ Scoring Policy. Options include: ◦ Threat Score ◦ Confidence Score ◦ Severity ◦ Verdict ◦ Safe Browsing Verdict ◦ Category ◦ Tags ◦ Type Tags ◦ Is Pervasive ◦ Malicious Count ◦ Suspicious Count ◦ AS Organization ◦ RIR ◦ Country Code ◦ Continent Code ◦ ASN ◦ Meaningful Name ◦ Site Title ◦ Last Submission Date ◦ Mandiant Score (Deprecated) ◦ Crowdsourced IDS Signatures (Snort) This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Indicator Description Context Selection	Select the context used to populate each indicator's description based on available fields. Options include: ◦ GTI Assessment ◦ WHOIS ◦ Crowdsourced AI Summary ◦ Associated Names ◦ Outgoing Links ◦ Crowdsourced YARA Results

	◦ Crowdsourced Context ◦ Sigma Analysis Results
Ingests ASNs As	Select which entity type to ingest ASNs as in ThreatQ. Options include: ◦ Attributes (*default*) ◦ Indicators (Type: ASN)
Enable SSL Certificate Verification	Enable this parameter 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.



Google Threat Intelligence Threat Lists Parameters

PARAMETER	DESCRIPTION

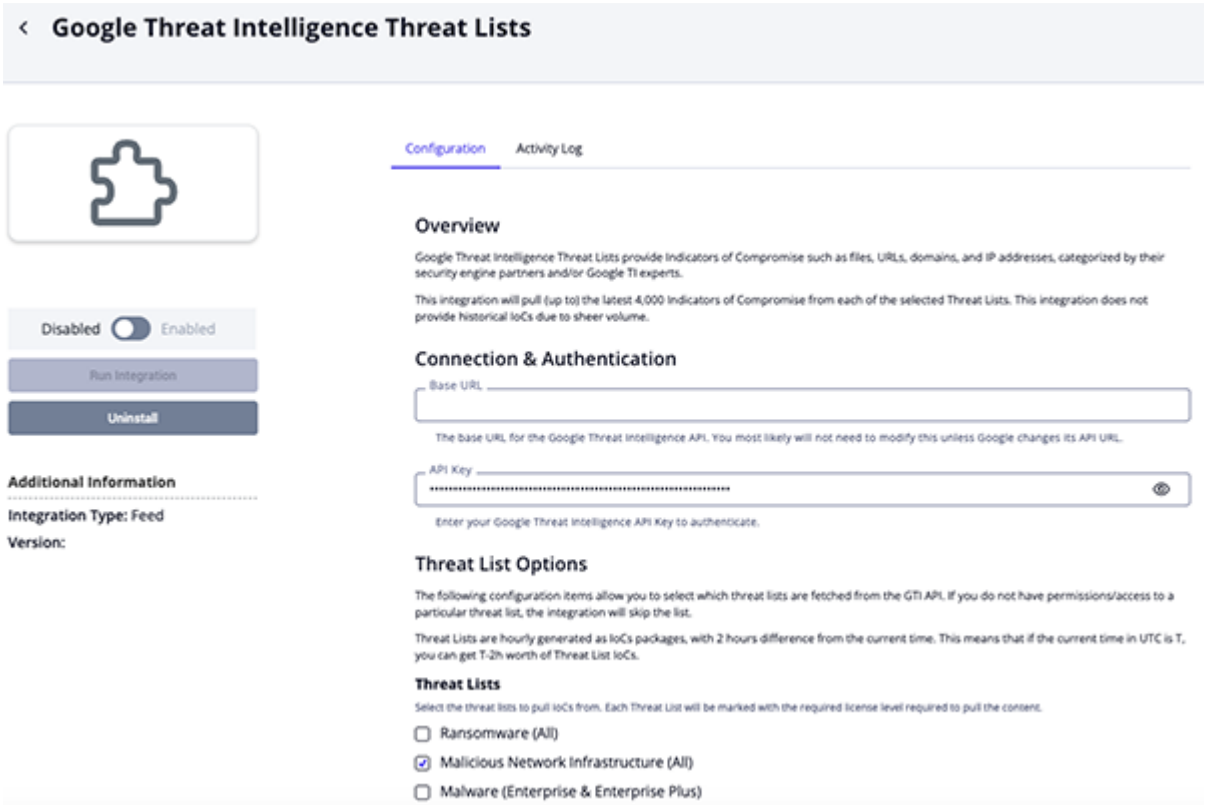
Base URL	The base URL for the Google Threat Intelligence API. You will not have to modify this unless Google changes its API URL.
API Key	Enter your Google Threat Intelligence API Key to authenticate.
Threat Lists	Select the threat lists to pull IoCs from. Each Threat List will be marked with the required license level required to pull the content. Options include: ◦ Ransomware (All) ◦ Malicious Network Infrastructure (All) ◦ Malware (Enterprise & Enterprise Plus) ◦ Threat Actor (Enterprise & Enterprise Plus) ◦ Daily Top Trending (Enterprise & Enterprise Plus) ◦ Mobile (Enterprise Plus) ◦ OS X (Enterprise Plus) ◦ Linux (Enterprise Plus) ◦ Internet of Things (Enterprise Plus) ◦ Cryptominers (Enterprise Plus) ◦ Phishing (Enterprise Plus) ◦ First Stage Delivery Vectors (Enterprise Plus) ◦ Vulnerability Weaponization (Enterprise Plus) ◦ Infostealers (Enterprise Plus)
Ingested Indicator Types	Select the types of indicators to ingest into ThreatQ. Options include: ◦ IP Addresses (*default*) ◦ URLs (*default*) ◦ Domains (*default*) ◦ Hashes (*default*)

Minimum Threat Score Threshold	Enter the minimum score (0-100) required to an indicator from the API and ingest into ThreatQ. ThreatQuotient highly recommend that you set this value to at least `40`, the default value, to avoid ingesting low-confidence indicators.
Minimum Positive Detections Threshold	Enter the minimum positive detections required to return an indicator from the API and ingest into ThreatQ. This must be a numeric value with a minimum of 0.
Require Malware Family Association	Enable this parameter to configure the feed to only return indicators from the API that have a malware family associated with them.
Require Campaign Association	Enable this parameter to configure the feed to only return indicators from the API that have a campaign associated with them.
Require Report Association	Enable this parameter to configure the feed to only return indicators from the API that have a report associated with them.
Require Threat Actor Association	Enable this parameter to configure the feed to only return indicators from the API that have a threat actor associated with them.

Ingested Severities	Select the severities of the indicators to ingest. This allows you to filter out indicators that do not meet a certain severity level criteria. This option will be used in addition to the "Minimum Threat Score Threshold" and "Minimum Positive Detections Threshold" options above. Options include ◦ None ◦ Unknown ◦ Low (*default*) ◦ Medium (*default*) ◦ High (*default*)
Ingested Hash Types	Optional - Select the types of the related hashes to ingest for indicators. Options include: ◦ MD5 ◦ SHA-1 ◦ SHA-256
Set Indicator Status to Active if Verdict is Malicious	Enable this parameter to dynamically set the status of indicators with a verdict of malicious to Active.
Set Indicator Status to Whitelisted if Threat Score is 0	Enable this parameter to dynamically set the status of indicators with threat scores of 0 to whitelisted.
Indicator Context Selection	Select the context to bring back with each ingested indicator. Verdict is not enabled by default as it's a binary value of malicious or benign. Instead, it is recommended to use the **Normalize Threat Score** parameter to create a more granular range to use in your ThreatQ Scoring Policy. Options include:

	◦ Threat List ◦ Threat Type ◦ Threat Score ◦ Severity ◦ Verdict ◦ Category ◦ Malicious Count ◦ Suspicious Count ◦ Last Submission Date ◦ Meaningful Name ◦ Continent Code ◦ Country Code ◦ ASN ◦ AS Organization ◦ Regional Internet Registry ◦ Last HTTP Response Code ◦ Site Title ◦ Tags ◦ Type Tags
Indicator Association Selection	Select the context used to populate each indicator's description based on available fields. Options include: ◦ Malware Families ◦ Threat Actors
Normalize Threat Scores	Enable this parameter to normalize the Threat Score from the default 0-100 range to a human-readable value. The normalization will be based on the mapping field set in **Threat Score Normalization Mapping** parameter. This is useful for developing a ThreatQ Scoring Policy that is based on these normalized values.
Threat Score Normalization Mapping	Enter your mapping to normalize the numeric threat score values to the scorable attribute, `Normalized Threat Score`. The raw Threat Score value will always be ingested. This mapping should contain a line-separated CSV-formatted string with the following columns: Minimum, Maximum, Normalized Value. *default: (0,39,Low 40,79,Medium 80,94,High 95,100,Critical)*
Ingests ASNs As	Select which entity type to ingest ASNs as in ThreatQ. Options include:

	◦ Attributes (*default*) ◦ Indicators (Type: ASN)
Enable SSL Certificate Verification	Enable this parameter 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.



Google Vulnerability Intelligence Parameters

PARAMETER	DESCRIPTION
Base URL	The base URL for the Google Threat Intelligence API. You will not have to modify this unless Google changes its API URL.

API Key	Enter your Google Threat Intelligence API Key to authenticate.
Origin Filter	Filter the results based on the origin of the intelligence. Options include: ◦ Google Threat Intelligence (Curated) (default) ◦ Partner (i.e. AlienVaultOTX) ◦ Crowdsourced (i.e. Individual Users) ⚠ ThreatQuotient highly recommends only selecting the curated origin to ensure data quality and reduce noise/volume.
Target Industry	Specify the industry objects you want to ingest.
Custom API Filter	An optional custom filter can be applied to all API requests when retrieving collections. This filter applies only to the top-level collection request and does not affect API calls used to fetch associated data. It is appended to the default query using logical AND and is evaluated alongside the existing `collection_type`, `origin`, `last_modification_date`, and `target_industry` filters. Additional details on filter construction are available at: https://gtidocs.virustotal.com/reference/list-threats.
Risk Rating Filter	Select the risk ratings for vulnerabilities to ingest into ThreatQ. Options include: ◦ Low ◦ Medium *(default)* ◦ High *(default)* ◦ Critical *(default)*
Exploitation State Filter	Select the exploitation states for vulnerabilities to ingest into ThreatQ. Options include: ◦ No Known *(default)*

- Confirmed *(default)*
- Reported *(default)*
- Suspected *(default)*

Exploitation Vector Filter

Select the exploitation vectors for vulnerabilities to ingest into ThreatQ. Options include:

- Administrative Interface *(default)*
- Bluetooth Access *(default)*
- Browser *(default)*
- Email *(default)*
- Exposed Web Application *(default)*
- File Share *(default)*
- General Network Connectivity *(default)*
- Local Access *(default)*
- Local Network Access *(default)*
- Malicious Application *(default)*
- Malicious File *(default)*
- Malicious Server *(default)*
- Open Port *(default)*
- Physical Access *(default)*
- Short Range Radio *(default)*
- Unspecified Local Vector *(default)*
- Unspecified Remote Vector *(default)*
- VPN Access *(default)*
- Web *(default)*
- WiFi Access *(default)*

Specific Vulnerability Filter

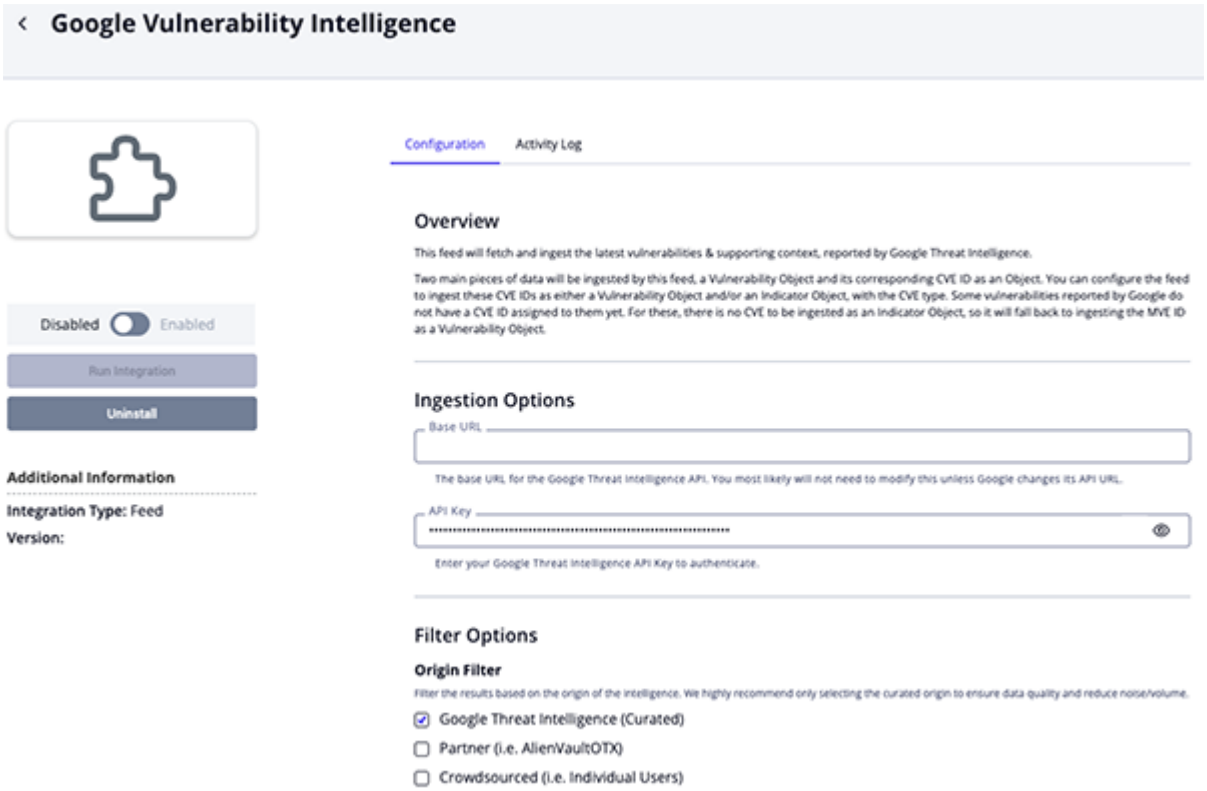
Select particularities to use to filter vulnerabilities. Options include:

- Must Affect Cloud
- Must Affect Operational Technology
- Must be observed In The Wild
- Must require User Interaction

	◦ Must be CISA Exploited ◦ Must Have Exploits ◦ Must have Zero Day
Ingest CVEs As	Select which entity type to ingest CVEs as in ThreatQ. Options include: ◦ Indicators ◦ Vulnerabilities *(default)*
Vulnerability Attribute Context	Select the context for vulnerabilities to ingest into ThreatQ. Options include: ◦ Available Mitigation *(default)* ◦ CWE *(default)* ◦ Affected Platforms (Based on CPEs) ◦ Affected Products (Based on CPEs) ◦ Affected Vendors (Based on CPEs) *(default)* ◦ Exploitation Consequence *(default)* ◦ Exploitation State *(default)* ◦ Exploitation Vector *(default)* ◦ MVE ID ◦ Observed in the Wild *(default)* ◦ Risk Rating *(default)* ◦ Has Zero Day *(default)* ◦ Is Predicted ◦ Targeted Industry *(default)*
Description Context	Select the pieces of context to include in the vulnerability's description. Options include: ◦ Analysis *(default)* ◦ Description *(default)* ◦ Vendor Fix References *(default)* ◦ Vulnerable CPEs

- Executive Summary *(default)*
- Sources *(default)*
- Workarounds *(default)*
- CVSS Ratings *(default)*

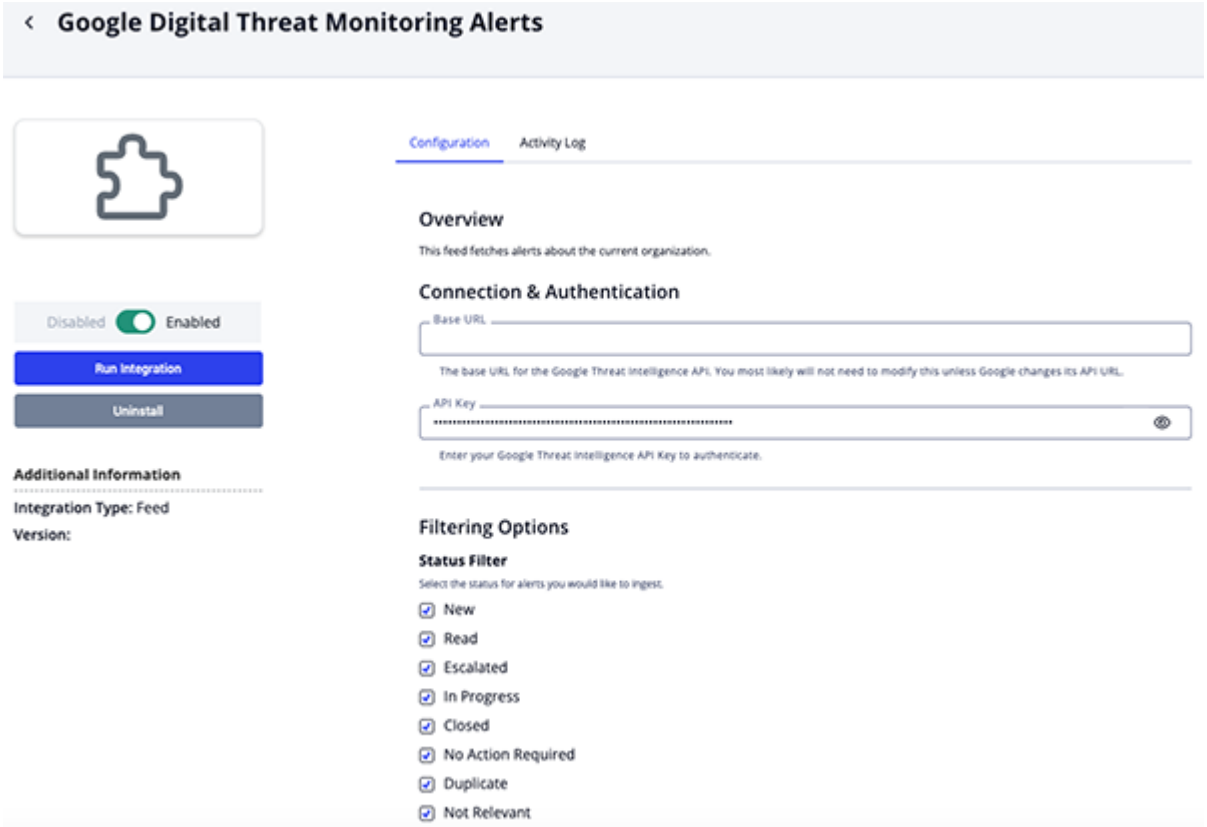
CVSS Attribute Context	Select the CVSS context for vulnerabilities to ingest into ThreatQ. Options include: ◦ Base Score *(default)* ◦ Exploit Code Maturity *(default)* ◦ Temporal Score *(default)* ◦ Vector String *(default)*
Enable SSL Certificate Verification	Enable this parameter for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.



Google Digital Threat Monitoring Alerts Parameters

PARAMETER	DESCRIPTION
Base URL	The base URL for the Google Threat Intelligence API. You will not have to modify this unless Google changes its API URL.
API Key	Enter your Google Threat Intelligence API Key to authenticate.
Status Filter	Select the status for alerts to ingest into ThreatQ. Options include: ◦ New ◦ Read ◦ Escalated ◦ In Progress ◦ Closed ◦ No Action Required ◦ Duplicate ◦ Not Relevant ◦ Tracked External
Type Filter	Select the type for alerts to ingest into ThreatQ. Options include: ◦ Compromised Credentials ◦ Domain Discovery ◦ Forum Post ◦ Message ◦ Paste ◦ Shop Listing ◦ Tweet ◦ Web Content
Severity Filter	Select the severity for alerts to ingest into ThreatQ. Options include: ◦ High

	◦ Medium ◦ Low
Context Selection	Select the context to bring back with each ingested alert. Options include: ◦ Alert Type ◦ Confidence Score ◦ Malicious Count ◦ Severity ◦ Similarity Score ◦ Status ◦ Monitor ◦ Labels (As Tags) ◦ Organization ◦ Identity ◦ Product ◦ Brand ◦ City ◦ Country
Indicator Relationship Filter	Select the specific entities from the alert to ingest as related indicators. Options include: ◦ MD5 ◦ SHA-1 ◦ SHA-256 ◦ Filename ◦ File Path ◦ FQDN ◦ IP Address ◦ IPv6 Address ◦ URL ◦ Email Address ◦ Telegram Username
Enable SSL Certificate Verification	Enable this parameter 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

Google Threat Intelligence

The Google Threat Intelligence feed ingests ingests compromised Adversary objects and any related Indicators, Malware, Vulnerabilities, and Attack Patterns.

```
GET {base_url}/api/v3/collections?filter=collection_type:threat-actor
```

Sample Response:

```
{
    "data": [
        {
            "id": "threat-actor--8211bc17-9216-5e83-b54d-
d1b04add12f3",
            "type": "collection",
            "links": {
                "self": "https://www.virustotal.com/api/v3/
collections/threat-actor--8211bc17-9216-5e83-b54d-d1b04add12f3"
            },
            "attributes": {
                "merged_actors": [
                    {
                        "value": "UNC3856",
                        "first_seen": 1655826491,
                        "description": "threat-actor--6bddb7c2-
bb5c-5f1f-9f95-1ef370189c1a",
                        "confidence": "confirmed",
                        "last_seen": 1655826491
                    }
                ],
                "detection_names": [],
                "available_mitigation": [],
                "recent_activity_summary": [
                    273,
                    641
                ],
                "targeted_industries": [],
                "top_icon_md5": [
                    "a9bed4661fae1103c9f7e6cc3b718932",
                    "a681bad11b862d06eeec1352e97630ef",
```

```
            "e757fba9022b94d32b1ba2189e4051da"
        ],
        "targeted_regions_hierarchy": [
            {
                "region": "Europe",
                "sub_region": "Western Europe",
                "country": "Austria",
                "country_iso2": "AT",
                "confidence": "confirmed",
                "first_seen": 1520867153,
                "last_seen": 1710319777,
                "description": null,
                "source": null
            }
        ],
        "targeted_informations": [],
        "capabilities": [],
        "references_count": 350,
        "first_seen_details": [
            {
                "value": "2007-01-16T00:00:00Z",
                "first_seen": null,
                "description": null,
                "confidence": "confirmed",
                "last_seen": null
            }
        ],
        "operating_systems": [],
        "technologies": [],
        "malware_roles": [],
        "ip_addresses_count": 459,
        "alt_names": [
            "Group74 (Cisco Systems)",
            "Fancy Bear (DuskRise Inc.)",
            "Frozenlake (Google)",
            "APT28 (Google)"
        ],
        "threat_scape": [],
        "workarounds": [],
        "motivations": [
            {
                "value": "Attack / Destruction",
```

```
                "first_seen": null,
                "description": null,
                "confidence": "confirmed",
                "last_seen": null
            },
            {
                "value": "Espionage",
                "first_seen": null,
                "description": null,
                "confidence": "confirmed",
                "last_seen": null
            }
        ],
        "summary_stats": {
            "first_submission_date": {
                "min": 0.0,
                "max": 1750336636.0,
                "avg": 1398991817.8962307
            },
        },
        "collection_links": [],
        "urls_count": 834,
        "risk_factors": [],
        "targeted_regions": [
            "TR",
            "CZ",
            "PT"
        ],
        "status": "COMPUTED",
        "name": "APT28",
        "alt_names_details": [
            {
                "value": "APT28 (Google)",
                "first_seen": null,
                "description": null,
                "confidence": "confirmed",
                "last_seen": null
            }
        ],
        "vulnerable_products": "",
        "vendor_fix_references": [],
        "files_count": 1988,
```

```
                "last_seen_details": [
                    {
                        "value": "2025-06-19T19:51:19Z",
                        "first_seen": null,
                        "description": null,
                        "confidence": "confirmed",
                        "last_seen": null
                    }
                ],
                "field_sources": [],
                "is_content_translated": false,
                "intended_effects": [],
                "targeted_industries_tree": [
                    {
                        "industry_group": "Aerospace & Defense",
                        "industry": null,
                        "confidence": "confirmed",
                        "first_seen": 1441948486,
                        "last_seen": 1749112145,
                        "description": null,
                        "source": null
                    }
                ],
                "subscribers_count": 45,
                "first_seen": 1168905600,
                "collection_type": "threat-actor",
                "last_modification_date": 1751251305,
                "domains_count": 995,
                "counters": {
                    "files": 1988,
                    "domains": 995,
                    "ip_addresses": 459,
                    "urls": 834,
                    "iocs": 4276,
                    "subscribers": 45,
                    "attack_techniques": 177
                },
                "tags": [],
                "affected_systems": [],
                "description": "APT28 is a highly active cyber
espionage group that has employed a variety of malware and TTPs,
including spearphishing, watering holes, credential collection, and
```

```
the exploitation of mobile platforms, toward intelligence collection
intended to provide political and military advantage. APT28
operations have primarily impacted entities across the public and
private sectors in North America and Europe, and the group, which
multiple governments have attributed to Unit 26165 within the Main
Directorate of the General Staff of the Armed Forces of the Russian
Federation (GRU), has heavily targeted Ukraine in particular
following Russia's February 2022 full-scale invasion. However, we
have also observed APT28's targeting of government and military
entities in other regions such as the Middle East and Asia, and open-
source reporting further corroborates our observations of the group's
activity in these regions.",
                "recent_activity_relative_change":
-0.0510632142340518,
                "private": true,
                "source_region": "RU",
                "version_history": [],
                "creation_date": 1168905600,
                "mitigations": [],
                "source_regions_hierarchy": [
                    {
                        "region": "Europe",
                        "sub_region": "Eastern Europe",
                        "country": "Russian Federation",
                        "country_iso2": "RU",
                        "confidence": "confirmed",
                        "first_seen": null,
                        "last_seen": null,
                        "description": null,
                        "source": null
                    }
                ],
                "exploitation_vectors": [],
                "autogenerated_tags": [
                    "armadillo",
                    "attachment",
                    "cve-2021-40444"
                ],
                "origin": "Google Threat Intelligence",
                "last_seen": 1750362679,
                "tags_details": [],
                "aggregations": {
                    "files": {
```

```
                        "itw_urls": [
                            {
                                "value": "http://
45.77.156.179/1.html",
                                "count": 2,
                                "total_related": 2,
                                "prevalence": 1.0
                            }
                        ],
                        "email_subjects": [
                            {
                                "value": "Test Meeting",
                                "count": 12,
                                "total_related": 22,
                                "prevalence": 0.5454545454545454
                            }
                        ],
                        "email_senders": [
                            {
                                "value": "commercial@vanadrink.com",
                                "count": 5,
                                "total_related": 5,
                                "prevalence": 1.0
                            }
                        ],
                        "contacted_urls": [
                            {
                                "value": "http://23.227.196.215/
close/?ags=OBy5Qj-
s0zvkV&ags=K4g4_hHH7vf&oprnd=ui&aq=8zrsUz&utm=Kth&from=unSCXQ&text=d8
2Ggk3&itwm=NjLTWK3ardX5QxCNwzzSe5hOAQUhl",
                                "count": 1,
                                "total_related": 1,
                                "prevalence": 1.0
                            }
                        ],
                        "contacted_domains": [
                            {
                                "value": "api.btloader.com",
                                "count": 10,
                                "total_related": 11436,
                                "prevalence": 0.0008744316194473592
```

```
                            }
                        ],
                        "contacted_ips": [
                            {
                                "value": "91.208.207.223",
                                "count": 5,
                                "total_related": 159,
                                "prevalence": 0.031446540880503145
                            }"prevalence": 2e-05
                            }
                        ],
                        "execution_parents": [
                            {
                                "value":
"54a27464c7ad7f2e32cd123b27c0f9082590cd5ba48526bf00728e8107048f48",
                                "count": 3,
                                "total_related": 4,
                                "prevalence": 0.75
                            }
                        ],
                        "compressed_parents": [
                            {
                                "value":
"069a20cb5daaef9ff756cfd19f3ddfa4d7ecddd73d6e9f744e7156ea07d0801c",
                                "count": 4,
                                "total_related": 8,
                                "prevalence": 0.5
                            }
                        ],
                        "pcap_parents": [
                            {
                                "value":
"06b691b5d6b12c72afaa9caed3c5fc158bbab18188262f49608ff68ab5479fb2",
                                "count": 1,
                                "total_related": 1,
                                "prevalence": 1.0
                            }
                        ],
                        "dropped_files_sha256": [
                            {
                                "value":
"caa37f136c564145d0447d1d573e880fa4f1d31c430de7fc585ae6439a8a7329",
```

```
                                "count": 7,
                                "total_related": 72435,
                                "prevalence": 9.663836543107614e-05
                            }
                        ],
                        "email_parents": [
                            {
                                "value":
"a301260b4887b1f2126821825cacce19dc5b8a8006ab04f0a26f098a9555750a",
                                "count": 2,
                                "total_related": 2,
                                "prevalence": 1.0
                            }
                        ],
                        "tags": [
                            {
                                "value": "pedll",
                                "count": 59
                            }
                        ],
                        "main_icon_dhash": [
                            {
                                "value": "0000100033320000",
                                "count": 5,
                                "total_related": 7,
                                "prevalence": 0.7142857142857143
                            }
                        ],
                        "main_icon_raw_md5": [
                            {
                                "value":
"a9bed4661fae1103c9f7e6cc3b718932",
                                "count": 5,
                                "total_related": 7,
                                "prevalence": 0.7142857142857143
                            }
                        ],
                        "vhash": [
                            {
                                "value":
"96a88ebaa2fe6fe510c5af279ce832ce1",
                                "count": 29,
```

```
                                "total_related": 23058,
                                "prevalence": 0.0012576979790094543
                            }
                        ],
                        "imphash": [
                            {
                                "value":
"1e79c6496a07d4391cba25a551392410",
                                "count": 15,
                                "total_related": 61,
                                "prevalence": 0.2459016393442623
                            }
                        ],
                        "behash": [
                            {
                                "value":
"76a8f43d77060240bf707251c1cd5008",
                                "count": 6,
                                "total_related": 49242,
                                "prevalence": 0.00012184720360667723
                            }
                        ],
                        "telfhash": [
                            {
                                "value":
"t139f05945fa380b9649d2ac24dc1e05674593e379e524eb04bf95ced00c7e001f7a
8daa",
                                "count": 1,
                                "total_related": 1,
                                "prevalence": 1.0
                            }
                        ],
                        "tlshhash": [
                            {
                                "value":
"T149D308B7131017BE69468B489FA86D4D3224D4B770B685C4FBAE9B28CF439EF813
5D14",
                                "count": 2,
                                "total_related": 2,
                                "prevalence": 1.0
                            }
                        ],
```

```
                        "elfhash": [
                            {
                                "value":
"4bf18b2cee846e961b86562f856b69d0",
                                "count": 1,
                                "total_related": 1,
                                "prevalence": 1.0
                            }
                        ],
                        "attributions": [
                            {
                                "value": "gamefish",
                                "count": 124,
                                "total_related": 337,
                                "prevalence": 0.36795252225519287
                            }
                        ],
                        "crowdsourced_ids_results": [
                            {
                                "value": {
                                    "id": "1:2047948",
                                    "message": "ET INFO Custom
Endpoint Service Domain in DNS Lookup (run .mocky .io)",
                                    "category": "bad-unknown",
                                    "source": "Proofpoint Emerging
Threats Open",
                                    "url": "https://
rules.emergingthreats.net/",
                                    "rule": "alert dns $HOME_NET any
-> any any (msg:\"ET INFO Custom Endpoint Service Domain in DNS
Lookup (run .mocky .io)\"; dns.query; bsize:12; content:
\"run.mocky.io\"; nocase; classtype:bad-unknown; sid:2047948; rev:1;
metadata:attack_target Client_Endpoint, created_at 2023_09_07,
deployment Perimeter, performance_impact Low, confidence High,
signature_severity Informational, updated_at 2023_09_07, reviewed_at
2024_04_09; target:src_ip;)"
                                },
                                "count": 40,
                                "total_related": 87,
                                "prevalence": 0.45977011494252873
                            }
                        ],
```

```
                        "embedded_domains": [
                            {
                                "value": "run.mocky.io",
                                "count": 38,
                                "total_related": 9048,
                                "prevalence": 0.004199823165340406
                            }
                        ],
                        "embedded_ips": [
                            {
                                "value": "24.17.89.89",
                                "count": 26,
                                "total_related": 26,
                                "prevalence": 1.0
                            }
                        ],
                        "embedded_urls": [
                            {
                                "value": "https://accounts.ukr.net/
login/favicon.ico",
                                "count": 23,
                                "total_related": 97,
                                "prevalence": 0.5021367521367521
                            }
                        ],
                        "mutexes_created": [
                            {
                                "value": "\\Sessions\\1\
\BaseNamedObjects\\vgekW8b1st6yjzPA9fewB70o7KC",
                                "count": 4,
                                "total_related": 32,
                                "prevalence": 0.125
                            }
                        ],
                        "mutexes_opened": [
                            {
                                "value": "Local\
\4F75746C6F6F6B5E16934AF0EE4642B5A2BDBA4CC7666902_S-1-5-21-870151485-
863566166-2146164720-1000",
                                "count": 5,
                                "total_related": 23584,
                                "prevalence": 0.0002120081411126187 4
```

```
                            }
                        ],
                        "registry_keys_deleted": [
                            {
                                "value": "HKLM\\SOFTWARE\\MICROSOFT\
\OFFICE\\14.0\\WORD\\FILE MRU",
                                "count": 2,
                                "total_related": 651,
                                "prevalence": 0.0030721966205837174
                            }
                        ],
                        "registry_keys_opened": [
                            {
                                "value": "52-54-00-63-20-e5\
\WpadDecisionReason",
                                "count": 1,
                                "total_related": 165,
                                "prevalence": 0.006060606060606061
                            }
                        ],
                        "registry_keys_set": [
                            {
                                "value": "HKEY_CLASSES_ROOT\
\Wow6432Node\\CLSID\\{3543619C-D563-43f7-95EA-4DA7E1CC396A}\
\InProcServer32\\(Default)",
                                "count": 1,
                                "total_related": 2,
                                "prevalence": 0.5
                            }
                        ],
                        "file_types": [
                            {
                                "value": "html",
                                "count": 187
                            }
                        ],
                        "crowdsourced_sigma_results": [
                            {
                                "value": {
                                    "id":
"8b884f70bb47a8e06faf8f548fcfef77fe3802d22c310c4cdfa01f35cb030bac",
                                "level": "medium",
```

```
                                    "title": "WSF/JSE/JS/VBA/VBE File
Execution Via Cscript/Wscript",
                                    "author": "Michael Haag",
                                    "source_url": "https://
github.com/Neo23x0/sigma",
                                    "source": "Sigma Integrated Rule
Set (GitHub)",
                                    "description": "Detects script
file execution (.js, .jse, .vba, .vbe, .vbs, .wsf) by Wscript/
Cscript"
                                },
                                "count": 18,
                                "total_related": 92144,
                                "prevalence": 0.00019534641430803959
                            }
                        ],
                        "debug_codeview_guids": [
                            {
                                "value": "d7633b5d-7f73-4804-
b5e7-78663bfec15e",
                                "count": 2,
                                "total_related": 2,
                                "prevalence": 1.0
                            }
                        ],
                        "debug_codeview_names": [
                            {
                                "value": "Z:\\PROJECTS\\Dll1\\x64\
\Release\\Dll1.pdb",
                                "count": 6,
                                "total_related": 6,
                                "prevalence": 1.0
                            }
                        ],
                        "debug_timestamps": [
                            {
                                "value": "Wed Aug 10 07:38:01 2016",
                                "count": 5,
                                "total_related": 5,
                                "prevalence": 1.0
                            }
                        ],
```

```
                        "dropped_files_path": [
                            {
                                "value": "C:\\ProgramData\\Microsoft\
\Windows\\WER\\Temp\\WER1122.tmp.WERInternalMetadata.xml",
                                "count": 2,
                                "total_related": 21825,
                                "prevalence": 9.163802978235968e-05
                            }
                        ],
                        "elfinfo_exports": [
                            {
                                "value":
"_ZStplIwSt11char_traitsIwESaIwEESbIT_T0_T1_ERKS6_S8_",
                                "count": 3,
                                "total_related": 1218,
                                "prevalence": 0.0024630541871921183
                            }
                        ],
                        "elfinfo_imports": [
                            {
                                "value":
"_ZNSbIwSt11char_traitsIwESaIwEE5beginEv",
                                "count": 3,
                                "total_related": 808,
                                "prevalence": 0.0037128712871287127
                            }
                        ],
                        "exiftool_authors": [
                            {
                                "value": "Rafael Moon",
                                "count": 3,
                                "total_related": 8,
                                "prevalence": 0.375
                            }
                        ],
                        "exiftool_create_dates": [
                            {
                                "value": "2022:09:08 03:07:43+00:00",
                                "count": 14,
                                "total_related": 51,
                                "prevalence": 0.27450980392156865
                            }
```

```
                        ],
                        "exiftool_creators": [
                            {
                                "value": "Apache Software
Foundation",
                                "count": 2,
                                "total_related": 16254,
                                "prevalence": 0.00012304663467454166
                            }
                        ],
                        "exiftool_last_printed": [
                            {
                                "value": "2008:01:08 14:56:00Z",
                                "count": 1,
                                "total_related": 1,
                                "prevalence": 1.0
                            }
                        ],
                        "exiftool_producers": [
                            {
                                "value": "Qt 4.8.7",
                                "count": 2,
                                "total_related": 100000,
                                "prevalence": 2e-05
                            }
                        ],
                        "exiftool_subjects": [
                            {
                                "value": "TVqQAAMAAAAEAAAA//
8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA4AAAAA4
fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUu
DQ0KJAAAAAAAAACseA3F6BljlugZY5boGWOWh2/IlsEZY5aHb...",
                                "count": 3,
                                "total_related": 3,
                                "prevalence": 1.0
                            }
                        ],
                        "exiftool_titles": [
                            {
                                "value": " Good thing we disabled
macros ",
                                "count": 3,
```

```
                            "total_related": 71,
                            "prevalence": 0.04225352112676056
                        }
                    ],
                    "filecondis_dhash": [
                        {
                            "value": "bebabcbe86c6c350",
                            "count": 15,
                            "total_related": 15,
                            "prevalence": 1.0
                        }
                    ],
                    "netassembly_mvid": [
                        {
                            "value": "50367b8c-fa12-4c3e-
aa3d-57620d1fa124",
                            "count": 2,
                            "total_related": 3,
                            "prevalence": 0.6666666666666666
                        }
                    ],
                    "office_application_names": [
                        {
                            "value": "Microsoft Office Word",
                            "count": 12,
                            "total_related": 100000,
                            "prevalence": 0.00012
                        }
                    ],
                    "office_authors": [
                        {
                            "value": "Nick Daemoji",
                            "count": 3,
                            "total_related": 4,
                            "prevalence": 0.75
                        }
                    ],
                    "office_creation_datetimes": [
                        {
                            "value": "2017-10-03 01:36:00",
                            "count": 3,
                            "total_related": 9,
```

```
                            "prevalence": 0.3333333333333333
                        }
                    ],
                    "office_last_saved": [
                        {
                            "value": "2012-10-31 10:10:27",
                            "count": 5,
                            "total_related": 11,
                            "prevalence": 0.45454545454545453
                        }
                    ],
                    "office_macro_names": [
                        {
                            "value": "NewMacros.bas",
                            "count": 3,
                            "total_related": 76472,
                            "prevalence": 3.9230044983784915e-05
                        }
                    ],
                    "pe_info_imports": [
                        {
                            "value": "POWRPROF.DLL",
                            "count": 1,
                            "total_related": 2911,
                            "prevalence": 0.00034352456200618345
                        }
                    ],
                    "pe_info_exports": [
                        {
                            "value": "Init1",
                            "count": 34,
                            "total_related": 396,
                            "prevalence": 0.08585858585858586
                        }
                    ],
                    "pe_info_section_md5": [
                        {
                            "value":
"4031479fbcd57a5f6c8dbf647bfcd376",
                            "count": 12,
                            "total_related": 196,
                            "prevalence": 0.061224489795918366
```

```
                        }
                    ],
                    "pe_info_section_names": [
                        {
                            "value": ".rc_it",
                            "count": 2,
                            "total_related": 828,
                            "prevalence": 0.0024154589371980675
                        }
                    ],
                    "sandbox_verdicts": [
                        {
                            "value": "Clean",
                            "count": 173,
                            "sandbox_name": "Zenbox"
                        }
                    ],
                    "signature_info_comments": [
                        {
                            "value": "Check Network
Identification",
                            "count": 3,
                            "total_related": 5,
                            "prevalence": 0.6
                        }
                    ],
                    "signature_info_copyrights": [
                        {
                            "value": "Â® Microsoft Corporation.
All rights reserved.",
                            "count": 83,
                            "total_related": 1117,
                            "prevalence": 0.07430617726051925
                        }
                    ],
                    "signature_info_descriptions": [
                        {
                            "value": "Network Identification
Service DLL",
                            "count": 33,
                            "total_related": 53,
                            "prevalence": 0.6226415094339622
```

```
                            }
                        ],
                        "signature_info_internal_names": [
                            {
                                "value": "NetIds.dll",
                                "count": 33,
                                "total_related": 53,
                                "prevalence": 0.6226415094339622
                            }
                        ],
                        "signature_info_original_names": [
                            {
                                "value": "NetIds.dll",
                                "count": 33,
                                "total_related": 53,
                                "prevalence": 0.6226415094339622
                            }
                        ],
                        "signature_info_products": [
                            {
                                "value": "DocumentSaver",
                                "count": 5,
                                "total_related": 8,
                                "prevalence": 0.625
                            }
                        ],
                        "symhash": [
                            {
                                "value":
"704b879d425b7bbe366a345454774ff2",
                                "count": 3,
                                "total_related": 5,
                                "prevalence": 0.6
                            }
                        ],
                        "trusted_verdict_filenames": [
                            {
                                "value": "amd64_windowsdeviceportal-
wcos-
www_31bf3856ad364e35_10.0.17751.1_none_deb753ded4321364_favicon.ico",
                                "count": 1,
                                "total_related": 1,
```

```
                                "prevalence": 1.0
                            }
                        ],
                        "rich_pe_header_hash": [
                            {
                                "value":
"cafcda8746b34ccb88ddb50252db58d0",
                                "count": 7,
                                "total_related": 25,
                                "prevalence": 0.28
                            }
                        ],
                        "popular_threat_category": [
                            {
                                "value": "trojan",
                                "count": 717
                            }
                        ],
                        "popular_threat_name": [
                            {
                                "value": "sednit",
                                "count": 247
                            }
                        ],
                        "suggested_threat_label": "trojan.sednit/
sofacy",
                        "attack_techniques": [
                            {
                                "value": "T1497.003",
                                "count": 3,
                                "total_related": 94867,
                                "prevalence": 3.16232198762478e-05
                            }
                        ],
                        "malware_config_family_name": [
                            {
                                "value": "gamefish",
                                "count": 49,
                                "total_related": 77,
                                "prevalence": 0.6363636363636364
                            }
                        ],
```

```
                        "malware_config_crypto_key": [
                            {
                                "value": "0x32407b67472c3f42226b",
                                "count": 4,
                                "total_related": 10,
                                "prevalence": 0.4
                            }
                        ],
                        "malware_config_c2_url": [
                            {
                                "value": "http://
swsupporttools.com/",
                                "count": 4,
                                "total_related": 6,
                                "prevalence": 0.6666666666666666
                            }
                        ],
                        "malware_config_c2_user_agent": [
                            {
                                "value": "Mozilla/5.0 (Windows NT
6.1; WOW64; Trident/7.0; rv:11.0) like Gecko",
                                "count": 1,
                                "total_related": 100000,
                                "prevalence": 1e-05
                            }
                        ],
                        "malware_config_host_port": [
                            {
                                "value": "netcorpscanprotect.com",
                                "count": 1,
                                "total_related": 3,
                                "prevalence": 0.3333333333333333
                            }
                        ],
                        "malware_config_dropped_file": [
                            {
                                "value":
"a0d05eece2585035f553de7533258d7b63c96509aba4176c7844155435f89211",
                                "count": 3,
                                "total_related": 3,
                                "prevalence": 1.0
                            }
```

```
                        ],
                        "malware_config_dropped_file_path": [
                            {
                                "value":
"258887afb9501cfd860dfc2f333adb35",
                                "count": 3,
                                "total_related": 3,
                                "prevalence": 1.0
                            }
                        ],
                        "memory_pattern_urls": [
                            {
                                "value": "https://www.msn.com/",
                                "count": 8,
                                "total_related": 27652,
                                "prevalence": 0.0002893099956603501
                            }
                        ],
                        "attack_tactics": [
                            {
                                "value": "TA0011",
                                "count": 794
                            }
                        ],
                        "parent_contacted_domains": [
                            {
                                "value": "btloader.com",
                                "count": 20,
                                "total_related": 111436,
                                "prevalence": 0.0001794752144728813
                            }
                        ]
                    },
                    "urls": {
                        "attributions": [
                            {
                                "value": "roughedge",
                                "count": 41,
                                "total_related": 47,
                                "prevalence": 0.8723404255319149
                            }
                        ],
```

```
                        "http_response_contents": [
                            {
                                "value":
"05a5f6513b2ffc4b059ce0099a0df624dc12dac43f7b98ebfe0f924af6465964",
                                "count": 37,
                                "total_related": 320,
                                "prevalence": 0.115625
                            }
                        ],
                        "contacted_domains": [
                            {
                                "value": "netmediaresources.com",
                                "count": 2,
                                "total_related": 3,
                                "prevalence": 0.6666666666666666
                            }
                        ],
                        "communicating_files": [
                            {
                                "value":
"604dbb615d6ff549f9ff3c3484a32d5e3f50853761f029f9d30c6f8eb982bf84",
                                "count": 2,
                                "total_related": 2,
                                "prevalence": 1.0
                            }
                        ],
                        "cookie_names": [
                            {
                                "value": "MBizSessionID",
                                "count": 27,
                                "total_related": 297,
                                "prevalence": 0.09090909090909091
                            }
                        ],
                        "cookie_values": [
                            {
                                "value": "00a6fcfa-
b774-401e-82ad-85af73a02f79",
                                "count": 1,
                                "total_related": 1,
                                "prevalence": 1.0
                            }
```

```
                        ],
                        "downloaded_files": [
                            {
                                "value":
"05a5f6513b2ffc4b059ce0099a0df624dc12dac43f7b98ebfe0f924af6465964",
                                "count": 73,
                                "total_related": 223,
                                "prevalence": 0.3273542600896861
                            }
                        ],
                        "domains": [
                            {
                                "value": "webhook.site",
                                "count": 115,
                                "total_related": 2863,
                                "prevalence": 0.04016765630457562
                            }
                        ],
                        "embedded_js": [
                            {
                                "value":
"6af9edac35f5a75d57f9da9e46955c4f66f35daf638cdd305acc1f0a35b292a3",
                                "count": 33,
                                "total_related": 72,
                                "prevalence": 0.4583333333333333
                            }
                        ],
                        "favicon_dhash": [
                            {
                                "value": "708c8e0a2baad0e1",
                                "count": 131,
                                "total_related": 5129,
                                "prevalence": 0.025541041138623512
                            }
                        ],
                        "favicon_raw_md5": [
                            {
                                "value":
"06bde06ab3839695045d6a0a8920d0e7",
                                "count": 131,
                                "total_related": 5129,
                                "prevalence": 0.025541041138623512
```

```
                            }
                        ],
                        "html_titles": [
                            {
                                "value": "ÐŸÐ¾Ñˆ,Ð° @ ukr.net -
ÑƒÐ°Ñ€Ð°Ñ–Ð½ÑŒÐ°Ð° ÐµÐ»ÐµÐ,Ñ€Ð¾Ð½Ð½Ð° Ð¿Ð¾Ñˆ,Ð°",
                                "count": 129,
                                "total_related": 155,
                                "prevalence": 0.832258064516129
                            }
                        ],
                        "ip_addresses": [
                            {
                                "value": "46.4.105.116",
                                "count": 69,
                                "total_related": 2067,
                                "prevalence": 0.033381712626995644
                            }
                        ],
                        "memory_patterns": [
                            {
                                "value":
"b8324a0250ac770ccdc92dcc8e809c8804638bf6e78e69f44dce3883dfc6e89c",
                                "count": 38,
                                "total_related": 295,
                                "prevalence": 0.1288135593220339
                            }
                        ],
                        "outgoing_links": [
                            {
                                "value": "https://mail.ukr.net/
terms_uk.html",
                                "count": 39,
                                "total_related": 462,
                                "prevalence": 0.08441558441558442
                            }
                        ],
                        "path": [
                            {
                                "value": "/filedwn.php",
                                "count": 73,
                                "total_related": 139,
```

```
                        "prevalence": 0.5251798561151079
                    }
                ],
                "prefix_paths": [
                    {
                        "value": "/filedwn.php",
                        "count": 92,
                        "total_related": 78,
                        "prevalence": 1.1794871794871795
                    }
                ],
                "suffix_paths": [
                    {
                        "value": "/filedwn.php",
                        "count": 79,
                        "total_related": 71,
                        "prevalence": 1.1126760563380282
                    }
                ],
                "ports": [
                    {
                        "value": "5000",
                        "count": 11,
                        "total_related": 40673,
                        "prevalence": 0.00027044968406559635
                    }
                ],
                "query_strings": [
                    {
                        "value": "i=1",
                        "count": 15,
                        "total_related": 87578,
                        "prevalence": 0.0001712758912055539
                    }
                ],
                "query_param_keys": [
                    {
                        "value": "fuid",
                        "count": 2,
                        "total_related": 1659,
                        "prevalence": 0.0012055455093429777
                    }
```

```
                        ],
                        "query_param_values": [
                            {
                                "value": "6a98168f-
f14f-4014-8b28-8329b0118936",
                                "count": 5,
                                "total_related": 7,
                                "prevalence": 0.7142857142857143
                            }
                        ],
                        "query_param_key_values": [
                            {
                                "value": "id=6a98168f-
f14f-4014-8b28-8329b0118936",
                                "count": 5,
                                "total_related": 7,
                                "prevalence": 0.7142857142857143
                            }
                        ],
                        "referring_files": [
                            {
                                "value":
"4b2b188ff864453b75071c0ba80b00f87475d880c35ecdfc1cf262eb1d587580",
                                "count": 33,
                                "total_related": 66,
                                "prevalence": 0.5
                            }
                        ],
                        "tags": [
                            {
                                "value": "external-resources",
                                "count": 278
                            }
                        ],
                        "tracker_ids": [
                            {
                                "value": "UA-71917162-10",
                                "count": 14,
                                "total_related": 8366,
                                "prevalence": 0.0016734401147501792
                            }
                        ]
```

```
                    },
                    "domains": {
                        "attributions": [
                            {
                                "value": "chopstick_v2",
                                "count": 46,
                                "total_related": 57,
                                "prevalence": 0.8070175438596491
                            }
                        ],
                        "communicating_files": [
                            {
                                "value":
"85c100e140389bbbc467cc348d7c17a59c27a106b6c26b2499719aee57f2cf52",
                                "count": 5,
                                "total_related": 6,
                                "prevalence": 0.8333333333333334
                            }
                        ],
                        "downloaded_files": [
                            {
                                "value":
"b00a6010b9640e448ed277a2a62fd8905284d0d60ee2b2f51c4f20d7d115c1a1",
                                "count": 19,
                                "total_related": 9435,
                                "prevalence": 0.00201377848436672
                            }
                        ],
                        "favicon_dhash": [
                            {
                                "value": "dcc69eb0b2f2f060",
                                "count": 17,
                                "total_related": 49,
                                "prevalence": 0.3469387755102041
                            }
                        ],
                        "favicon_raw_md5": [
                            {
                                "value":
"c44bbec78ebc720a8c3783f5f2f37898",
                                "count": 17,
                                "total_related": 49,
```

```
                                "prevalence": 0.3469387755102041
                            }
                        ],
                        "urls": [
                            {
                                "value": "http://
00e66943.proxy.webhookapp.com/",
                                "count": 1,
                                "total_related": 1,
                                "prevalence": 1.0
                            }
                        ],
                        "registrant_names": [
                            {
                                "value": "b94871993eab339b",
                                "count": 16,
                                "total_related": 11567,
                                "prevalence": 0.0013832454396126913
                            }
                        ]
                    },
                    "ip_addresses": {
                        "attributions": [
                            {
                                "value": "empire",
                                "count": 14,
                                "total_related": 545,
                                "prevalence": 0.025688073394495414
                            }
                        ],
                        "communicating_files": [
                            {
                                "value":
"efc1a4706a737437b387795566ef7e9d9a3d8066d661484337c333feaa1ad204",
                                "count": 2,
                                "total_related": 56,
                                "prevalence": 0.03571428571428571
                            }
                        ],
                        "downloaded_files": [
                            {
                                "value":
```

```
"a214568945ac98c7836485c5a493334fcc3d74ab32e55c3aef371599e9431e80",
                                "count": 5,
                                "total_related": 20,
                                "prevalence": 0.25
                            }
                        ],
                        "urls": [
                            {
                                "value": "file://124.168.91.178/
webdav/wody.pdf",
                                "count": 1,
                                "total_related": 1,
                                "prevalence": 1.0
                            }
                        ]
                    }
                }
            },
            "context_attributes": {
                "shared_with_me": false,
                "role": "viewer"
            }
        }
]
}
```


Each `.data[].id` Is used to retrieve the related objects in the following Supplemental feeds.

ThreatQ provides the following default mapping for this feed based on each item within the `.data[]` list.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.attributes.name`	`Adversary.Value`	`Adversary`	`.attributes.last_modification_date`	`APT28`	N/A
`.attributes.alt_names_details[].value`	`Adversary.Tag`	`N/A`	`N/A`	`APT28 (Google)`	User-configurable.
`.attributes.description`	`Adversary.Description`	`N/A`	`N/A`	`APT28 is a highly active cyber espionage group that ...`	N/A
`.attributes.motivations[].value`	`Adversary.Attribute`	`Motivation`	`.attributes.last_modification_date`	`Attack / Destruction`	User-configurable. When the Motivation option is checked in the context.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.attributes.targeted_industries_tree[].industry_group	Adversary.Attribute	Target Industry	.attributes.last_modification_date	Aerospace & Defense	User-configurable. When the Industry option is checked in the context.
.attributes.source_regions_hierarchy[].region	Adversary.Attribute	Region	.attributes.last_modification_date	Europe	User-configurable. When the Source Context option is checked in the context.
.attributes.source_regions_hierarchy[].sub_region	Adversary.Attribute	Sub Region	.attributes.last_modification_date	Eastern Europe	User-configurable. When the Source Context option is checked in the context.
.attributes.source_regions_hierarchy[].country	Adversary.Attribute	Country	.attributes.last_modification_date	Russian Federation	User-configurable. When the Source Context option is checked in the context.
.attributes.source_regions_hierarchy[].country_iso2	Adversary.Attribute	Country Code	.attributes.last_modification_date	RU	User-configurable. When the Source Context option is checked in the context.
.attributes.targeted_regions_hierarchy[].region	Adversary.Attribute	Target Region	.attributes.last_modification_date	Europe	User-configurable. When the Target Region option is checked in the context.
.attributes.targeted_regions_hierarchy[].country	Adversary.Attribute	Target Country	.attributes.last_modification_date	Austria	User-configurable. When the Target Region option is checked in the context.
.attributes.targeted_regions_hierarchy[].country_iso2	Adversary.Attribute	Target Country Code	.attributes.last_modification_date	AT	User-configurable. When the Target Region option is checked in the context.
.attributes.targeted_regions_hierarchy[].sub_region	Adversary.Attribute	Target Sub Region	.attributes.last_modification_date	Western Europe	User-configurable. When the Target Region option is checked in the context.
.id	Related Malware	Malware	.attributes.last_modification_date	threat-actor--8211bc17-9216-5e83-b54d-d1b04add12f3	User-configurable. ID is used in supplemental requests if configured. See Google Threat Intelligence Related Malware (Supplemental)
.id	Related.Attack Pattern	Attack Pattern	.attributes.last_modification_date	threat-actor--8211bc17-9216-5e83-b54d-d1b04add12f3	User-configurable. ID is used in supplemental requests if configured. See Google Threat Intelligence Related Attack Pattern (Supplemental)
.id	Related.Campaign	Campaign	.attributes.last_modification_date	threat-actor--8211bc17-9216-5e83-b54d-d1b04add12f3	User-configurable. ID is used in supplemental requests if configured. See Google Threat Intelligence Related Campaigns (Supplemental)
.id	Related.Indicator/	CVE/ Vulnerability	.attributes.last_modification_date	threat-actor--8211bc17-92	User-configurable. ID is used in supplemental requests if configured. See Google Threat Intelligence

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
	`Vulnerability`			`16-5e83-b54d-d1b04add12f3`	`Related Vulnerabilities (Supplemental)`
`.id`	`Related.Indicator`	`IP Address/ URL/ FQDN/MD5/ SHA-1/SHA-256`	`.attributes.last_modification_date`	`threat-actor--8211bc17-9216-5e83-b54d-d1b04add12f3`	User-configurable. ID is used in supplemental requests if configured. See `Google Threat Intelligence Related IOC (Supplemental)`. A request is made for each indicator type.

Google Threat Intelligence Related Malware (Supplemental)

The Google Threat Intelligence Related Malware Supplemental feed is called once for each object `.id` returned by the main feed.

```
GET {base_url}/api/v3/collections/{entity_id}/malware_families
```

Sample Response:


```
{
    "data": [
        {
            "id": "malware--05b4251d-f5cf-5f90-b1b8-8d75da6d9387",
            "type": "collection",
            "links": {
                "self": "https://www.virustotal.com/api/v3/
collections/malware--05b4251d-f5cf-5f90-b1b8-8d75da6d9387"
            },
            "attributes": {
                "available_mitigation": [],
                "collection_links": [],
                "detection_names": [],
                "merged_actors": [],
                "recent_activity_summary": [
                    0,
                    2,
                    0
                ],
                "status": "COMPUTED",
                "last_seen": 1695609000,
                "ip_addresses_count": 0,
                "source_regions_hierarchy": [],
                "mitigations": [],
                "affected_systems": [],
                "recent_activity_relative_change": -0.6875,
```

```
                "counters": {
                    "files": 13,
                    "domains": 0,
                    "ip_addresses": 0,
                    "urls": 0,
                    "iocs": 13,
                    "subscribers": 0,
                    "attack_techniques": 13
                },
                "targeted_industries_tree": [],
                "capabilities": [
                    {
                        "confidence": "unconfirmed",
                        "last_seen": null,
                        "description": "Capable of allocating
memory.",
                        "first_seen": null,
                        "value": "Allocates memory"
                    }
                ],
                "description": "MILDMAP is an APT28 dropper for the
SOURFACE backdoor.",
                "last_modification_date": 1682107632,
                "alt_names_details": [],
                "alt_names": [],
                "private": true,
                "vendor_fix_references": [],
                "is_content_translated": false,
                "exploitation_vectors": [],
                "risk_factors": [],
                "malware_roles": [
                    {
                        "confidence": "unconfirmed",
                        "last_seen": null,
                        "description": null,
                        "first_seen": null,
                        "value": "Dropper"
                    }
                ],
                "top_icon_md5": [],
                "workarounds": [],
                "last_seen_details": [
```

```
            {
                "confidence": "unconfirmed",
                "last_seen": null,
                "description": null,
                "first_seen": null,
                "value": "2023-09-25T02:30:00Z"
            }
        ],
        "summary_stats": {
            "first_submission_date": {
                "min": 1347557862.0,
                "max": 1596301806.0,
                "avg": 1418747098.6153846
            },
            "last_submission_date": {
                "min": 1373322911.0,
                "max": 1725889743.0,
                "avg": 1554571734.2307692
            },
            "files_detections": {
                "min": 28.0,
                "max": 60.0,
                "avg": 46.61538461538461
            }
        },
        "intended_effects": [],
        "name": "MILDMAP",
        "vulnerable_products": "",
        "files_count": 13,
        "field_sources": [],
        "operating_systems": [
            {
                "confidence": "unconfirmed",
                "last_seen": null,
                "description": null,
                "first_seen": null,
                "value": "Windows"
            }
        ],
        "targeted_regions_hierarchy": [],
        "creation_date": 1714525336,
        "tags": [],
```

```
                "first_seen_details": [],
                "subscribers_count": 0,
                "motivations": [],
                "domains_count": 0,
                "tags_details": [],
                "targeted_informations": [],
                "targeted_regions": [],
                "threat_scape": [],
                "autogenerated_tags": [
                    "armadillo"
                ],
                "version_history": [],
                "origin": "Google Threat Intelligence",
                "collection_type": "malware-family",
                "references_count": 2,
                "urls_count": 0,
                "targeted_industries": [],
                "technologies": [],
                "aggregations": {
                    "files": {
                        "contacted_domains": [
                            {
                                "value": "www.bing.com",
                                "count": 1,
                                "total_related": 100000,
                                "prevalence": 1e-05
                            }
                        ],
                        "contacted_ips": [
                            {
                                "value": "200.106.145.122",
                                "count": 2,
                                "total_related": 5,
                                "prevalence": 0.4
                            }
                        ],
                        "execution_parents": [
                            {
                                "value":
"1acb16dc9c194718758c017c91c439423efcdce6c06ccbb3d1696304eb555b84",
                                "count": 1,
                                "total_related": 1,
```

```
                                "prevalence": 1.0
                            }
                        ],
                        "compressed_parents": [
                            {
                                "value":
"1d986e304d2a4acc507e548b70e18f4ea51b8c8ab042ab21c68feb89d002de01",
                                "count": 1,
                                "total_related": 1,
                                "prevalence": 1.0
                            }
                        ],
                        "tags": [
                            {
                                "value": "armadillo",
                                "count": 9
                            },
                            {
                                "value": "pedll",
                                "count": 8
                            }
                        ],
                        "vhash": [
                            {
                                "value": "154056655d15751078z3f?z1",
                                "count": 5,
                                "total_related": 7,
                                "prevalence": 0.7142857142857143
                            }
                        ],
                        "imphash": [
                            {
                                "value":
"9c58b46236c2f82467517fb1a07efe2d",
                                "count": 5,
                                "total_related": 10,
                                "prevalence": 0.5
                            }
                        ],
                        "behash": [
                            {
                                "value":
```

```
"2f603f6672ac4e8122820c10927707b2",
                                "count": 3,
                                "total_related": 17,
                                "prevalence": 0.17647058823529413
                            }
                        ],
                        "tlshhash": [
                            {
                                "value":
"T12192AE8AF77418B3F3E71AB84C211068BB69AD71CF51EC8ED67302C518E6E5ADC2
0661",
                                "count": 1,
                                "total_related": 1,
                                "prevalence": 1.0
                            }
                        ],
                        "attributions": [
                            {
                                "value": "mildmap",
                                "count": 12,
                                "total_related": 12,
                                "prevalence": 1.0
                            }
                        ],
                        "crowdsourced_yara_results": [
                            {
                                "value": {
                                    "id": "000f4bfd25|IMPLANT_6_v3",
                                    "ruleset_id": "000f4bfd25",
                                    "ruleset_name":
"apt_grizzlybear_uscert",
                                    "rule_name": "IMPLANT_6_v3",
                                    "source": "https://github.com/
Neo23x0/signature-base"
                                },
                                "count": 3,
                                "total_related": 23,
                                "prevalence": 0.13043478260869565
                            }
                        ],
                        "embedded_urls": [
                            {
                                "value": "http://200.106.145.122/
```

```
~bars/cgi-bin/brvc.cgi?14",
                                "count": 1,
                                "total_related": 1,
                                "prevalence": 1.0
                            }
                        ],
                        "mutexes_created": [
                            {
                                "value": "\\Sessions\\1\
\BaseNamedObjects\\Local\\ZonesCacheCounterMutex",
                                "count": 1,
                                "total_related": 100000,
                                "prevalence": 1e-05
                            }
                        ],
                        "registry_keys_opened": [
                            {
                                "value": "HKEY_CURRENT_USER_Classes\
\APPID\\{de5d803e-5d2a-4b5f-9c63-af25a465cc44}",
                                "count": 3,
                                "total_related": 87396,
                                "prevalence": 3.432651379925855e-05
                            }
                        ],
                        "registry_keys_set": [
                            {
                                "value": "HKEY_LOCAL_MACHINE\
\software\\microsoft\\windows nt\\currentversion\\svchost\\ntsvcs",
                                "count": 2,
                                "total_related": 2,
                                "prevalence": 1.0
                            }
                        ],
                        "file_types": [
                            {
                                "value": "pedll",
                                "count": 5
                            }
                        ],
                        "crowdsourced_sigma_results": [
                            {
                                "value": {
                                    "id":
```

```
"63bcc6f98c4a5594772428a329b433392d70f18a841926328607f303f3d782a5",
                                    "level": "medium",
                                    "title": "Rundll32 Spawned Via
Explorer.EXE",
                                    "author": "CD_ROM_",
                                    "source_url": "https://
github.com/Neo23x0/sigma",
                                    "source": "Sigma Integrated Rule
Set (GitHub)",
                                    "description": "Detects execution
of \"rundll32.exe\" with a parent process of Explorer.exe. This has
been observed by variants of Raspberry Robin, as first reported by
Red Canary."
                                },
                                "count": 2,
                                "total_related": 100000,
                                "prevalence": 2e-05
                            }
                        ],
                        "dropped_files_path": [
                            {
                                "value": "C:\\Users\\user\\AppData\
\Local\\mscsv.tmp (copy)",
                                "count": 2,
                                "total_related": 3,
                                "prevalence": 0.6666666666666666
                            }
                        ],
                        "filecondis_dhash": [
                            {
                                "value": "787a783c58902000",
                                "count": 2,
                                "total_related": 2,
                                "prevalence": 1.0
                            }
                        ],
                        "pe_info_imports": [
                            {
                                "value": "KERNEL32.dll",
                                "count": 13,
                                "total_related": 100000,
                                "prevalence": 0.00013
                            }
```

```
                        ],
                        "pe_info_exports": [
                            {
                                "value": "Start",
                                "count": 8,
                                "total_related": 100000,
                                "prevalence": 8e-05
                            }
                        ],
                        "pe_info_section_md5": [
                            {
                                "value":
"3fdf81929ae3bb2619c7f1bddf0a18c1",
                                "count": 2,
                                "total_related": 2,
                                "prevalence": 1.0
                            }
                        ],
                        "pe_info_section_names": [
                            {
                                "value": ".data",
                                "count": 13,
                                "total_related": 100000,
                                "prevalence": 0.00013
                            }
                        ],
                        "sandbox_verdicts": [
                            {
                                "value": "Malware",
                                "count": 3,
                                "sandbox_name": "Lastline"
                            }
                        ],
                        "rich_pe_header_hash": [
                            {
                                "value":
"cb419b26f269240aced3c33db2613de2",
                                "count": 3,
                                "total_related": 6,
                                "prevalence": 0.5
                            }
                        ],
```

```
                        "popular_threat_category": [
                            {
                                "value": "trojan",
                                "count": 13
                            }
                        ],
                        "popular_threat_name": [
                            {
                                "value": "sednit",
                                "count": 10
                            }
                        ],
                        "suggested_threat_label": "trojan.sednit/
foosace",
                        "attack_techniques": [
                            {
                                "value": "T1129",
                                "count": 5,
                                "total_related": 100000,
                                "prevalence": 5e-05
                            }
                        ],
                        "memory_pattern_urls": [
                            {
                                "value": "http://200.106.145.122/
~bars/cgi-bin/brvc.cgi?14",
                                "count": 1,
                                "total_related": 1,
                                "prevalence": 1.0
                            }
                        ],
                        "attack_tactics": [
                            {
                                "value": "TA0005",
                                "count": 14
                            }
                        ],
                        "parent_contacted_domains": [
                            {
                                "value": "bing.com",
                                "count": 1,
                                "total_related": 100000,
```

```
                                "prevalence": 1e-05
                            }
                        ]
                    }
                }
            },
            "context_attributes": {
                "shared_with_me": false,
                "role": "viewer"
            }
        }
    ]
}
```

ThreatQ provides the following default mapping for these two feeds based on each item within the `.data[]` list.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.attributes.name`	Related Malware.Value	N/A	`.attributes.last_modification_date`	'MILDMAP'	N/A
`.attributes.description`	Related Malware.Description	N/A	`N/A`	'MILDMAP is an APT28 dropper for the SOURFACE backdoor.'	N/A
`.attributes.operating_systems[].value`	Related Malware.Attribute	Target Operating System	`.attributes.last_modification_date`	'Windows'	User-configurable
`.attributes.targeted_industries_tree[].industry_group`	Related Malware.Attribute	Industry	`.attributes.last_modification_date`	N/A	User-configurable
`.attributes.detection_names[].value`	Related Malware.Attribute	Detection	`.attributes.last_modification_date`	N/A	User-configurable

Google Threat Intelligence Related Attack Pattern (Supplemental)

The Google Threat Intelligence Related Attack Pattern Supplemental feed fetches related attack patterns.

`GET {base_url}/api/v3/collections/{entity_id}/attack_techniques`

Sample Response:

```
{
  "data": [
    {
      "id": "T1003",
```

```
      "type": "attack_technique",
      "links": {
        "self": "https://www.virustotal.com/api/v3/attack_techniques/
T1003"
      },
      "attributes": {
        "last_modification_date": 1744757617,
        "creation_date": 1496266219,
        "description": "Adversaries may attempt to dump credentials
to obtain account login and credential material, normally in the form
of a hash or a clear text password. Credentials can be obtained from
OS caches, memory, or structures. Credentials can then be used to
perform Lateral Movement and access restricted information.\nSeveral
of the tools mentioned in associated sub-techniques may be used by
both adversaries and professional security testers. Additional custom
tools likely exist as well.",
        "name": "OS Credential Dumping",
        "info": {
          "x_mitre_attack_spec_version": "3.2.0",
          "x_mitre_contributors": [
            "Vincent Le Toux",
            "Ed Williams, Trustwave, SpiderLabs",
            "Tim (Wadhwa-)Brown",
            "Yves Yonan"
          ],
          "x_mitre_deprecated": false,
          "x_mitre_domains": [
            "enterprise-attack"
          ],
          "x_mitre_is_subtechnique": false,
          "x_mitre_modified_by_ref": "identity--
c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
          "x_mitre_platforms": [
            "Windows",
            "Linux",
            "macOS"
          ],
          "x_mitre_version": "2.2",
          "x_mitre_data_sources": [
            "Network Traffic: Network Traffic Content",
            "Process: Process Creation",
            "Network Traffic: Network Traffic Flow",
```

```
            "File: File Creation",
            "Windows Registry: Windows Registry Key Access",
            "Process: OS API Execution",
            "File: File Access",
            "Process: Process Access",
            "Command: Command Execution",
            "Active Directory: Active Directory Object Access"
          ],
          "x_mitre_detection": "Windows\nMonitor for unexpected
processes interacting with lsass.exe. Common credential dumpers such
as Mimikatz access the LSA Subsystem Service (LSASS) process by
opening the process, locating the LSA secrets key, and decrypting the
sections in memory where credential details are stored. Credential
dumpers may also use methods for reflective Process Injection to
reduce potential indicators of malicious activity.\nHash dumpers open
the Security Accounts Manager (SAM) on the local file system
(%SystemRoot%/system32/config/SAM) or create a dump of the Registry
SAM key to access stored account password hashes. Some hash dumpers
will open the local file system as a device and parse to the SAM
table to avoid file access defenses. Others will make an in-memory
copy of the SAM table before reading hashes. Detection of compromised
Valid Accounts in-use by adversaries may help as well. \nOn Windows
8.1 and Windows Server 2012 R2, monitor Windows Logs for LSASS.exe
creation to verify that LSASS started as a protected process.
\nMonitor processes and command-line arguments for program execution
that may be indicative of credential dumping. Remote access tools may
contain built-in features or incorporate existing tools like
Mimikatz. PowerShell scripts also exist that contain credential
dumping functionality, such as PowerSploit's Invoke-Mimikatz module,
which may require additional logging features to be configured in the
operating system to collect necessary information for analysis.
\nMonitor domain controller logs for replication requests and other
unscheduled activity possibly associated with DCSync.    Note: Domain
controllers may not log replication requests originating from the
default domain controller account. . Also monitor for network
protocols    and other replication requests  from IPs not associated
with known domain controllers. \nLinux\nTo obtain the passwords and
hashes stored in memory, processes must open a maps file in the /proc
filesystem for the process being analyzed. This file is stored under
the path /proc/<pid>/maps, where the <pid> directory is the unique
pid of the program being interrogated for such authentication data.
The AuditD monitoring tool, which ships stock in many Linux
```

```
distributions, can be used to watch for hostile processes opening
this file in the proc file system, alerting on the pid, process name,
and arguments of such programs."
        },
        "stix_id": "attack-pattern--0a3ead4e-6d47-4ccb-854c-
a6a4f9d96b22",
        "link": "https://attack.mitre.org/techniques/T1003/",
        "revoked": false
      }
    }
  ]
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data[].id - .data[].attributes.name`	`Related AttackPattern .Value`	`N/A`	`.data[] attributes.creation_date`	`T1003 - OS Credential Dumping`	If there is a MITRE Attack Pattern in ThreatQ Library, it will be related; if not, it will be ingested in the `ID - Name` format.
`.data[].attributes.description`	`Related AttackPattern .Description`	`N/A`	`N/A`	`Adversaries may attempt to dump credentials ...`	`N/A`

Google Threat Intelligence Related Campaigns (Supplemental)

The Google Threat Intelligence Related Campaigns supplemental feed returns associated collections of the campaign objects.

```
GET {base_url}/api/v3/collections/{entity_id}/campaigns
```

Sample Response:

```
{
  "data": [
    {
      "id": "campaign--27396631-640a-5079-954a-73a54f1c4d70",
      "type": "collection",
      "links": {
        "self": "https://www.virustotal.com/api/v3/collections/
campaign--27396631-640a-5079-954a-73a54f1c4d70"
      },
      "attributes": {
        "alt_names_details": [
          {
```

```
            "first_seen": null,
            "confidence": "confirmed",
            "last_seen": null,
            "description": null,
            "value": "CAMP.24.044"
          }
        ],
        "first_seen_details": [
          {
            "first_seen": null,
            "confidence": "unconfirmed",
            "last_seen": null,
            "description": "Mandiant Observed First Activity of
Campaign",
            "value": "2024-02-08T00:00:00Z"
          }
        ],
        "tags_details": [],
        "vulnerable_products": "",
        "exploitation_vectors": [],
        "version_history": [],
        "detection_names": [],
        "campaign_type": "INDIVIDUAL",
        "first_seen": 1707350400,
        "recent_activity_summary": [
          0,
          3
        ],
        "subscribers_count": 0,
        "vendor_fix_references": [],
        "last_modification_date": 1751319613,
        "operating_systems": [],
        "risk_factors": [],
        "private": true,
        "origin": "Google Threat Intelligence",
        "targeted_industries_tree": [
          {
            "industry_group": "Government",
            "industry": null,
            "confidence": "confirmed",
            "first_seen": null,
            "last_seen": null,
```

```
            "description": null,
            "source": null
          }
        ],
        "name": "APT28 Conducts Credential Harvesting Campaign
Targeting Multiple European Entities",
        "affected_systems": [],
        "source_region": "RU",
        "available_mitigation": [],
        "capabilities": [],
        "summary_stats": {
          "first_submission_date": {
            "min": 0.0,
            "max": 1728998106.0,
            "avg": 1587694613.9230769
          },
          "last_submission_date": {
            "min": 0.0,
            "max": 1748843074.0,
            "avg": 1591272176.5384614
          },
          "files_detections": {
            "min": 0.0,
            "max": 2.0,
            "avg": 1.0
          },
          "urls_detections": {
            "min": 0.0,
            "max": 12.0,
            "avg": 4.125
          }
        },
        "last_seen": 1727913600,
        "mitigations": [],
        "references_count": 0,
        "domains_count": 1,
        "autogenerated_tags": [
          "contains-embedded-js",
          "base64-embedded"
        ],
        "description": "Starting in early February 2024, Mandiant
observed UNC4697, a subcluster of APT28 focused on credential
```

```
harvesting activity. The threat group distributed phishing emails to
organizations containing links to websites hosting fake Outlook login
and password change templates. Targets of this broad campaign
included primarily Government entities in Europe and the Middle
East.",
        "last_seen_details": [
          {
            "first_seen": null,
            "confidence": "unconfirmed",
            "last_seen": null,
            "description": null,
            "value": "2024-10-03T00:00:00Z"
          }
        ],
        "files_count": 8,
        "motivations": [
          {
            "first_seen": null,
            "confidence": "confirmed",
            "last_seen": null,
            "description": null,
            "value": "Espionage"
          }
        ],
        "top_icon_md5": [
          "fc1881a5a70d2f3994eab9ea36b40305",
          "06bde06ab3839695045d6a0a8920d0e7"
        ],
        "creation_date": 1725545954,
        "collection_links": [],
        "technologies": [],
        "urls_count": 8,
        "counters": {
          "files": 8,
          "domains": 1,
          "ip_addresses": 0,
          "urls": 8,
          "iocs": 17,
          "subscribers": 0,
          "attack_techniques": 3
        },
        "malware_roles": [],
        "tags": [],
```

```
      "collection_type": "campaign",
      "is_content_translated": false,
      "targeted_informations": [],
      "targeted_regions_hierarchy": [
        {
          "region": "Europe",
          "sub_region": "Western Europe",
          "country": "France",
          "country_iso2": "FR",
          "confidence": "confirmed",
          "first_seen": null,
          "last_seen": null,
          "description": null,
          "source": null
        }
      ],
      "intended_effects": [],
      "threat_scape": [],
      "recent_activity_relative_change": 2.0,
      "ip_addresses_count": 0,
      "source_regions_hierarchy": [
        {
          "region": "Europe",
          "sub_region": "Eastern Europe",
          "country": "Russian Federation",
          "country_iso2": "RU",
          "confidence": "confirmed",
          "first_seen": null,
          "last_seen": null,
          "description": null,
          "source": null
        }
      ],
      "status": "COMPUTED",
      "field_sources": [],
      "targeted_regions": [
        "RO",
        "TR"
      ],
      "merged_actors": [],
      "targeted_industries": [],
      "workarounds": [],
```

```
        "alt_names": [
          "CAMP.24.044"
        ],
        "aggregations": {
          "files": {
            "itw_urls": [
              {
                "value": "http://run.mocky.io/v3/1070436c-7a99-47eb-
a30c-c34609165fe7",
                "count": 1,
                "total_related": 1,
                "prevalence": 1.0
              }
            ],
            "contacted_domains": [
              {
                "value":
"73ce1aae8a9ba738b91040232524f51a.serveo.net",
                "count": 1,
                "total_related": 2,
                "prevalence": 0.5
              }
            ],
            "contacted_ips": [
              {
                "value": "138.68.79.95",
                "count": 1,
                "total_related": 883,
                "prevalence": 0.0011325028312570782
              }
            ],
            "dropped_files_sha256": [
              {
                "value":
"502365d41f45ede605f0c59e78bf58039f6262bd97d6b89f801ace3e9d9e04c8",
                "count": 1,
                "total_related": 1,
                "prevalence": 1.0
              }
            ],
            "tags": [
              {
```

```
              "value": "base64-embedded",
              "count": 3
            }
          ],
          "vhash": [
            {
              "value": "htm:223a8178b49e7ca1fbe433b41ed8c536",
              "count": 1,
              "total_related": 1,
              "prevalence": 1.0
            }
          ],
          "behash": [
            {
              "value": "76a8f43d77060240bf707251c1cd5008",
              "count": 2,
              "total_related": 49242,
              "prevalence": 4.0615734535559076e-05
            }
          ],
          "tlshhash": [
            {
              "value":
"T10E03BF3F57A23D0EA45B40E8F6A19D4A3F1E48138CCF96347C3C2B4CDF82AE8425
1A58",
              "count": 1,
              "total_related": 1,
              "prevalence": 1.0
            }
          ],
          "crowdsourced_ids_results": [
            {
              "value": {
                "id": "1:2027942",
                "message": "ET POLICY DNS Query to a Reverse Proxy
Service Observed",
                "category": "policy-violation",
                "source": "Proofpoint Emerging Threats Open",
                "url": "https://rules.emergingthreats.net/",
                "rule": "alert dns $HOME_NET any -> any any (msg:
\"ET POLICY DNS Query to a Reverse Proxy Service Observed\";
dns.query; content:\".serveo.net\"; nocase; endswith;
```

```
classtype:policy-violation; sid:2027942; rev:3;
metadata:affected_product Any, attack_target Client_Endpoint,
created_at 2019_09_03, deployment Perimeter, confidence High,
signature_severity Major, updated_at 2020_09_17;)"
                },
                "count": 1,
                "total_related": 207,
                "prevalence": 0.004830917874396135
              }
            ],
            "crowdsourced_yara_results": [
              {
                "value": {
                  "id": "0122bae1e9|Base64_Encoded_URL",
                  "ruleset_id": "0122bae1e9",
                  "ruleset_name": "Base64_Encoded_URL",
                  "rule_name": "Base64_Encoded_URL",
                  "source": "https://github.com/InQuest/yara-rules-
vt"
                },
                "count": 4,
                "total_related": 100000,
                "prevalence": 4e-05
              }
            ],
            "embedded_domains": [
              {
                "value": "enry48yoi2olq.x.pipedream.net",
                "count": 1,
                "total_related": 1,
                "prevalence": 1.0
              }
            ],
            "embedded_ips": [
              {
                "value": "178.158.223.1",
                "count": 1,
                "total_related": 1,
                "prevalence": 1.0
              }
            ],
            "embedded_urls": [
              {
```

```
                "value": "https://enry48yoi2olq.x.pipedream.net/",
                "count": 1,
                "total_related": 1,
                "prevalence": 1.0
              }
            ],
            "mutexes_created": [
              {
                "value": "\\Sessions\\1\\BaseNamedObjects\\Local\
\x64_10MU_ACB10_S-1-5-5-0-394236",
                "count": 1,
                "total_related": 726,
                "prevalence": 0.0013774104683195593
              }
            ],
            "mutexes_opened": [
              {
                "value": "Local\\10MU_ACB10_S-1-5-5-0-189300",
                "count": 1,
                "total_related": 8883,
                "prevalence": 0.00011257458065968704
              }
            ],
            "registry_keys_deleted": [
              {
                "value": "HKEY_CURRENT_USER\\Software\\Google\
\Chrome\\PreferenceMACs\\Default\\extensions.settings",
                "count": 2,
                "total_related": 100000,
                "prevalence": 2e-05
              }
            ],
            "registry_keys_opened": [
              {
                "value": "HKEY_CURRENT_USER\\SOFTWARE\\Policies\
\Google\\Chrome",
                "count": 2,
                "total_related": 100000,
                "prevalence": 2e-05
              }
            ],
            "registry_keys_set": [
```

```
              {
                "value": "HKEY_CURRENT_USER\\Software\\Microsoft\
\Office\\16.0\\Outlook\\Perf\\RoamingStreamsCache\
\6154541E1BB6474FBCF1DBF1502AFDA8",
                "count": 1,
                "total_related": 1,
                "prevalence": 1.0
              }
            ],
            "file_types": [
              {
                "value": "html",
                "count": 3
              },
              {
                "value": "email",
                "count": 1
              }
            ],
            "crowdsourced_sigma_results": [
              {
                "value": {
                  "id":
"cfd44c3835317e846b18021a9060f4b9b011294ec53eb3ac1fad568abeb37922",
                  "level": "medium",
                  "title": "Office Application Initiated Network
Connection To Non-Local IP",
                  "author": "Christopher Peacock '@securepeacock',
SCYTHE '@scythe_io', Florian Roth (Nextron Systems), Tim Shelton,
Nasreddine Bencherchali (Nextron Systems)",
                  "source_url": "https://github.com/Neo23x0/sigma",
                  "source": "Sigma Integrated Rule Set (GitHub)",
                  "description": "Detects an office application
(Word, Excel, PowerPoint)  that initiate a network connection to a
non-private IP addresses.\nThis rule aims to detect traffic similar
to one seen exploited in CVE-2021-42292.\nThis rule will require an
initial baseline and tuning that is specific to your organization.\n"
                },
                "count": 1,
                "total_related": 100000,
                "prevalence": 1e-05
              }
```

```
            ],
            "dropped_files_path": [
              {
                "value": "40861A75-839A-43E8-A7CF-A151C68F93E5",
                "count": 1,
                "total_related": 1,
                "prevalence": 1.0
              }
            ],
            "sandbox_verdicts": [
              {
                "value": "Malware",
                "count": 2,
                "sandbox_name": "Zenbox"
              }
            ],
            "popular_threat_category": [
              {
                "value": "phishing",
                "count": 1
              }
            ],
            "popular_threat_name": [
              {
                "value": "phishingx",
                "count": 1
              }
            ],
            "suggested_threat_label": "phishing.phishingx",
            "attack_techniques": [
              {
                "value": "T1056.002",
                "count": 1,
                "total_related": 7666,
                "prevalence": 0.00013044612575006522
              }
            ],
            "memory_pattern_urls": [
              {
                "value": "https://
73ce1aae8a9ba738b91040232524f51a.serveo.net/img?fuid=rada-sng",
                "count": 1,
```

```
              "total_related": 1,
              "prevalence": 1.0
            }
          ],
          "attack_tactics": [
            {
              "value": "TA0005",
              "count": 10
            }
          ],
          "parent_contacted_domains": [
            {
              "value": "serveo.net",
              "count": 1,
              "total_related": 2,
              "prevalence": 0.5
            }
          ]
        },
        "urls": {
          "http_response_contents": [
            {
              "value":
"21319c912fc4a6f63a92e53c3f9026e64ab6bb764de4166e402896210f0b0c3f",
              "count": 1,
              "total_related": 1,
              "prevalence": 1.0
            }
          ],
          "downloaded_files": [
            {
              "value":
"c955e57777ec0d73639dca6748560d00aa5eb8e12f13ebb2ed9656add3908f97",
              "count": 3,
              "total_related": 95789,
              "prevalence": 3.1318836192047103e-05
            }
          ],
          "domains": [
            {
              "value": "run.mocky.io",
              "count": 3,
```

```
                "total_related": 773,
                "prevalence": 0.0038809831824062097
              }
            ],
            "embedded_js": [
              {
                "value":
"23ff9bedb5083664a04982c42a1fe8a31879fe9f8e09c3e4c4d30818f53f7916",
                "count": 1,
                "total_related": 1,
                "prevalence": 1.0
              }
            ],
            "favicon_dhash": [
              {
                "value": "a6d8de2b2a84a49a",
                "count": 3,
                "total_related": 1772,
                "prevalence": 0.001693002257336343
              }
            ],
            "favicon_raw_md5": [
              {
                "value": "fc1881a5a70d2f3994eab9ea36b40305",
                "count": 3,
                "total_related": 1772,
                "prevalence": 0.001693002257336343
              }
            ],
            "html_titles": [
              {
                "value": "Outlook Web App",
                "count": 3,
                "total_related": 100000,
                "prevalence": 3e-05
              }
            ],
            "ip_addresses": [
              {
                "value": "91.208.207.221",
                "count": 2,
                "total_related": 987,
```

```
                "prevalence": 0.0020263424518743667
              }
            ],
            "memory_patterns": [
              {
                "value":
"1797e4cfe9e0162014c2628d9289c14ab140d002f32f8e54312f2be9a1fb6d89",
                "count": 1,
                "total_related": 1,
                "prevalence": 1.0
              }
            ],
            "outgoing_links": [
              {
                "value": "https://enjr7ohxba0fn.x.pipedream.net",
                "count": 1,
                "total_related": 5,
                "prevalence": 0.2
              }
            ],
            "path": [
              {
                "value": "/3a417ebd-87b4-4b50-af7c-863d65fee25f",
                "count": 1,
                "total_related": 2,
                "prevalence": 0.5
              }
            ],
            "prefix_paths": [
              {
                "value": "/3a417ebd-87b4-4b50-af7c-863d65fee25f",
                "count": 1,
                "total_related": 2,
                "prevalence": 0.5
              }
            ],
            "suffix_paths": [
              {
                "value": "/3a417ebd-87b4-4b50-af7c-863d65fee25f",
                "count": 1,
                "total_related": 2,
                "prevalence": 0.5
```

```
            }
          ],
          "query_strings": [
            {
              "value": "fuid=rada-sng@ukr.net",
              "count": 1,
              "total_related": 2,
              "prevalence": 0.5
            }
          ],
          "query_param_keys": [
            {
              "value": "fuid",
              "count": 1,
              "total_related": 1659,
              "prevalence": 0.0006027727546714888
            }
          ],
          "query_param_values": [
            {
              "value": "rada-sng@ukr.net",
              "count": 1,
              "total_related": 2,
              "prevalence": 0.5
            }
          ],
          "query_param_key_values": [
            {
              "value": "fuid=rada-sng@ukr.net",
              "count": 1,
              "total_related": 2,
              "prevalence": 0.5
            }
          ],
          "referring_files": [
            {
              "value":
"1797e4cfe9e0162014c2628d9289c14ab140d002f32f8e54312f2be9a1fb6d89",
              "count": 1,
              "total_related": 1,
              "prevalence": 1.0
            }
```

```
            ],
            "tags": [
              {
                "value": "base64-embedded",
                "count": 3
              }
            ]
          },
          "domains": {
            "downloaded_files": [
              {
                "value":
"c955e57777ec0d73639dca6748560d00aa5eb8e12f13ebb2ed9656add3908f97",
                "count": 1,
                "total_related": 4245,
                "prevalence": 0.00023557126030624264
              }
            ],
            "urls": [
              {
                "value": "https://enjr7ohxba0fn.x.pipedream.net/",
                "count": 1,
                "total_related": 1,
                "prevalence": 1.0
              }
            ]
          }
        },
        "context_attributes": {
          "shared_with_me": false,
          "role": "viewer"
        }
      }
    ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.name	Related Campaign.Value	N/A	.data[].attributes.last_modification_date	APT28 Conducts Credential Harvesting Campaign Targeting Multiple European Entities	N/A
.data[].attributes.description	Related Campaign.Description	N/A	N/A	Starting in early February 2024, Mandiant observed UNC4697 ...	N/A
.data[].attributes.motivations[].value	Related Campaign.Attribute	Motivation	.data[].attributes.last_modification_date	Espionage	User-configurable. If Motivations is checked in Campaign Context.
.data[].attributes.source_regions_hierarchy[].region	Related Campaign.Attribute	Source Region	.data[].attributes.last_modification_date	Europe	User-configurable. If Source Regions Context is checked in Campaign Context.
.data[].attributes.source_regions_hierarchy[].sub_region	Related Campaign.Attribute	Source Sub Region	.data[].attributes.last_modification_date	Eastern Europe	User-configurable. If Source Regions Context is checked in Campaign Context.
.data[].attributes.source_regions_hierarchy[].country	Related Campaign.Attribute	Source Country	.data[].attributes.last_modification_date	Russian Federation	User-configurable. If Source Regions Context is checked in Campaign Context.
.data[].attributes.source_regions_hierarchy[].country_iso2	Related Campaign.Attribute	Source Country Code	.data[].attributes.last_modification_date	RU	User-configurable. If Source Regions Context is checked in Campaign Context.
.data[].attributes.targeted_regions_hierarchy.region	Related Campaign.Attribute	Target Region	.data[].attributes.last_modification_date	Europe	User-configurable. If Targeted Regions Context is checked in Campaign Context.
.data[].attributes.targeted_regions_hierarchy.country	Related Campaign.Attribute	Target Country	.data[].attributes.last_modification_date	France	User-configurable. If Targeted Regions Context is checked in Campaign Context.
.data[].attributes.targeted_regions_hierarchy.sub_region	Related Campaign.Attribute	Target Sub Region	.data[].attributes.last_modification_date	Western Europe	User-configurable. If Targeted Regions Context is checked in Campaign Context.
.data[].attributes.targeted_regions_hierarchy.country_iso2	Related Campaign.Attribute	Target Country Code	.data[].attributes.last_modification_date	FR	User-configurable. If Targeted Regions Context is checked in Campaign Context.
.data[].attributes.last_seen	Related Campaign.Attribute	Last Seen	.data[].attributes.last_modification_date	1727913600	Updatable. Timestamp value.
.data[].attributes.targeted_industries_tree[].industry_group	Related Campaign.Attribute	Target Sector	.data[].attributes.last_modification_date	Government	User-configurable.

Google Threat Intelligence Related IOC (Supplemental)

The Google Threat Intelligence Related IOC supplemental feed fetches indicators related to threat actors.

```
GET {base_url}/api/v3/collections/{entity_id}/search
```

IP Addresses

```
GET {base_url}/api/v3/collections/{entity_id}/search?query=entity:ip
```

Sample Response:


```
{
  "data": [
    {
      "id": "45.154.13.229",
      "type": "ip_address",
      "links": {
        "self": "https://www.virustotal.com/api/v3/ip_addresses/
45.154.13.229"
      },
      "attributes": {
        "threat_severity": {
          "version": "I3",
          "threat_severity_level": "SEVERITY_NONE",
          "threat_severity_data": {
            "belongs_to_bad_collection": true
          },
          "last_analysis_date": "1713287964",
          "level_description": "Severity NONE because it has no
detections."
        },
        "reputation": 0,
        "mandiant_ic_score": 35,
        "last_https_certificate_date": 1713287964,
        "tags": [],
        "whois": "inetnum: 45.0.0.0 - 45.255.255.255\nnetname: IANA-
NETBLOCK-45\ndescr: This network range is not fully allocated to
APNIC.\ndescr:\ndescr: If your whois search has returned this
message, then you have\ndescr: searched the APNIC whois database for
an address that is\ndescr: allocated by another Regional Internet
Registry (RIR).\ndescr:\ndescr: Please search the other RIRs at
whois.arin.net or whois.ripe.net\ndescr: for more information about
```

```
that range.\ncountry: AU\nadmin-c: IANA1-AP\ntech-c: IANA1-AP\nabuse-
c: AA1452-AP\nstatus: ALLOCATED PORTABLE\nremarks: For general info
on spam complaints email spam@apnic.net.\nremarks: For general info
on hacking & abuse complaints email abuse@apnic .net.\nmnt-by: APNIC-
HM\nmnt-lower: APNIC-HM\nmnt-irt: IRT-APNIC-AP\nlast-modified:
2021-02-15T05:31:12Z\nsource: APNIC\nirt: IRT-APNIC-AP\naddress:
Brisbane, Australia\ne-mail: helpdesk@apnic.net\nabuse-mailbox:
helpdesk@apnic.net\nadmin-c: HM20-AP\ntech-c: NO4-AP\nauth: #
Filtered\nremarks: APNIC is a Regional Internet Registry.\nremarks:
We do not operate the referring network and\nremarks: are unable to
investigate complaints of network abuse.\nremarks: For information
about IRT, see www.apnic.net/irt\nremarks: helpdesk@apnic.net was
validated on 2020-02-03\nmnt-by: APNIC-HM\nlast-modified:
2023-08-18T00:42:38Z\nsource: APNIC\nrole: ABUSE APNICAP\naddress:
Brisbane, Australia\ncountry: ZZ\nphone: +000000000\ne-mail:
helpdesk@apnic.net\nadmin-c: HM20-AP\ntech-c: NO4-AP\nnic-hdl:
AA1452-AP\nremarks: Generated from irt object IRT-APNIC-AP\nremarks:
helpdesk@apnic.net was validated on 2020-02-03\nabuse-mailbox:
helpdesk@apnic.net\nmnt-by: APNIC-ABUSE\nlast-modified:
2023-08-18T19:08:30Z\nsource: APNIC\nrole: Internet Assigned Numbers
Authority\naddress: see http://www.iana.org.\nadmin-c: IANA1-
AP\ntech-c: IANA1-AP\nnic-hdl: IANA1-AP\nremarks: For more
information on IANA services\nremarks: go to IANA web site at http://
www.iana.org.\nmnt-by: MAINT-APNIC-AP\nlast-modified:
2018-06-22T22:34:30Z\nsource: APNIC\n",
        "first_seen_itw_date": 1616047642,
        "last_analysis_results": {
          "Acronis": {
            "method": "blacklist",
            "engine_name": "Acronis",
            "category": "harmless",
            "result": "clean"
          }
        },
        "network": "45.154.12.0/22",
        "continent": "AS",
        "as_owner": "MOACK.Co.LTD",
        "country": "KR",
        "asn": 138195,
        "last_analysis_stats": {
          "malicious": 0,
          "suspicious": 0,
          "undetected": 32,
```

```
          "harmless": 62,
          "timeout": 0
        },
        "last_seen_itw_date": 1655397785,
        "last_modification_date": 1746637167,
        "total_votes": {
          "harmless": 0,
          "malicious": 0
        },
        "whois_date": 1713222068,
        "jarm":
"3fd3fd20d3fd3fd21c42d42d000000937221baefa0b90420c8e8e41903f1d5",
        "regional_internet_registry": "APNIC",
        "last_analysis_date": 1713287954,
        "last_https_certificate": {
          "cert_signature": {
            "signature_algorithm": "sha256RSA",
            "signature":
"df3a652aa0a5b21920b0554d2ccafcd68471e0f8bf445c57877c540c8f29e2a9c1e2
e13a455b7e07dca63330801c9ece9d9d58b44e471a35815241c425489c94bde07c597
c5cc21e0aca452d75905685e52ca591fb27e0fe45227ec5a60ccf0c2819d6eaf52d51
f5e04928bc369d3c3c847cbafe3cfe7ab36f87ea71549f85e9526fbfdb838fb54e221
cac594b1c3c3d6a32573e602b210ca77989bb3fc56f1d51868b5938d27c3d97adb245
9613b7b536383161969cdd24448617cbc6b8dc82df246bd6b8b992d144ca0dc2a55e2
c08c3017d576684df46f81dcb628fa3c5363424d94b914f65efaa4c83d4054e8774ae
63a9296546c4cbd2814f87d712bb03"
          },
          "extensions": {
            "authority_key_identifier": {
              "keyid": "78df91905feedeacf6c575ebd54c5553ef244ab6"
            },
            "subject_key_identifier":
"ba370b6e8713bcc5e05fcd61f1406674764039fc",
            "subject_alternative_name": [
              "juoffer.com",
              "www.juoffer.com"
            ],
            "key_usage": [
              "digitalSignature",
              "keyEncipherment"
            ],
            "extended_key_usage": [
```

```
              "serverAuth",
              "clientAuth"
            ],
            "certificate_policies": [
              "2.23.140.1.2.1"
            ],
            "ca_information_access": {
              "OCSP": "http://ocsp.digicert.com",
              "CA Issuers": "http://cacerts.digicert.com/
EncryptionEverywhereDVTLSCA-G2.crt"
            },
            "CA": false,
            "1.3.6.1.4.1.11129.2.4.2":
"0482016c016a007700eecdd064d5db1acec55cb79db4cd13a23287467cbcecde"
          },
          "validity": {
            "not_after": "2024-08-20 23:59:59",
            "not_before": "2023-08-20 00:00:00"
          },
          "size": 1538,
          "version": "V3",
          "public_key": {
            "algorithm": "RSA",
            "rsa": {
              "modulus":
"b2f83f6781fa5ed3f32a2385110b2d89c3aff8e67fe06af33132163354ce68a7785f
5c6e35f2d68797434acd232c716967e891c876c545d3ef6c23d9e6d478ac35471a159
101b5b5735de360a8bfc42bcc51fc0aa3bab6f695fc946dd0e62af61e14f9f5a686a3
bfa8cda8f0c5162ee2d77bc4e4039f4fc1924a0c1e9ad9141306854c13691e607a9b5
2cc3477f01a9de7316bd0cf1b21dfb4c6cda14bcd788ff72c0ee99cfc860af365c03a
5dd4a0234bb94320354e38370717958d28fef87b9ffb62677de78ca394a98af204334
5b47b5bf0fc04cbc0e13a1d15af44430315cb391e565c7ecedc59842425cc908375bd
9f3d7f83ca62a8f9f7d88f292e37b1",
              "exponent": "10001",
              "key_size": 2048
            }
          },
          "thumbprint_sha256":
"595ac1d22ba540a8a92a66436094e54dbb6265f6f9a8227470c56dade415e60a",
          "thumbprint": "db988be0f18edc5db901b82854f1cfd026895623",
          "serial_number": "76b33e3cb51cc417fe6a884dbee617a",
          "issuer": {
```

```
            "C": "US",
            "O": "DigiCert Inc",
            "OU": "www.digicert.com",
            "CN": "Encryption Everywhere DV TLS CA - G2"
          },
          "subject": {
            "CN": "juoffer.com"
          }
        },
        "gti_assessment": {
          "threat_score": {
            "value": 1
          },
          "severity": {
            "value": "SEVERITY_NONE"
          },
          "contributing_factors": {
            "mandiant_association_actor": true,
            "mandiant_confidence_score": 35,
            "gti_confidence_score": 59,
            "malicious_sandbox_verdict": false,
            "mandiant_association_report": true,
            "mandiant_association_malware": true,
            "safebrowsing_verdict": "harmless"
          },
          "verdict": {
            "value": "VERDICT_UNDETECTED"
          },
          "description": "This indicator did not match our detection
criteria and there is currently no evidence of malicious activity."
        }
      }
    }
  ]
}
```


Hashes

```
GET {base_url}/api/v3/collections/{entity_id}/search?query=entity:url
```

Sample Response:

```
{
    "data": [
        {
            "id":
"c8fd3259549a33b42da38c3f53301f73a66df1a007dbbd2d18ad94b95b4ca37a",
            "type": "file",
            "links": {
                "self": "https://www.virustotal.com/api/v3/files/
c8fd3259549a33b42da38c3f53301f73a66df1a007dbbd2d18ad94b95b4ca37a"
            },
            "attributes": {
                "names": [],
                "last_submission_date": 1446069053,
                "unique_sources": 0,
                "last_analysis_stats": {
                    "malicious": 0,
                    "suspicious": 0,
                    "undetected": 0,
                    "harmless": 0,
                    "timeout": 0,
                    "confirmed-timeout": 0,
                    "failure": 0,
                    "type-unsupported": 0
                },
                "md5": "2c397d151a6137a2a9be6455d143d165",
                "first_seen_itw_date": 1445641333,
                "mandiant_ic_score": 50,
                "available_tools": [],
                "sha1": "2cc2ad776a7a4149ddded992c05b6c458accb0c6",
                "type_description": "unknown",
                "last_seen_itw_date": 1446069053,
                "tags": [],
                "type_tags": [],
                "total_votes": {
                    "harmless": null,
                    "malicious": null
                },
                "last_modification_date": 1741350537,
                "last_analysis_results": {},
                "downloadable": false,
                "sha256":
"c8fd3259549a33b42da38c3f53301f73a66df1a007dbbd2d18ad94b95b4ca37a",
                "first_submission_date": 1445641333,
```

```
                "gti_assessment": {
                    "contributing_factors": {
                        "mandiant_confidence_score": 50,
                        "mandiant_association_actor": true
                    },
                    "threat_score": {
                        "value": 1
                    },
                    "severity": {
                        "value": "SEVERITY_NONE"
                    },
                    "verdict": {
                        "value": "VERDICT_UNKNOWN"
                    },
                    "description": "This indicator did not match our
detection criteria and there is currently no evidence of malicious
activity."
                }
            }
        }
    ]
}
```


FQDNs

`GET {base_url}/api/v3/collections/{entity_id}/search?query=entity:domain`

Sample Response:


```
{
  "data": [
    {
      "id": "update.centosupdates.com",
      "type": "domain",
      "links": {
        "self": "https://www.virustotal.com/api/v3/domains/
update.centosupdates.com"
      },
      "attributes": {
        "last_analysis_date": 1768880897,
        "last_modification_date": 1768881776,
        "tld": "com",
```

```
        "last_dns_records": [
          {
            "type": "A",
            "ttl": 10800,
            "value": "210.71.232.9"
          }
        ],
        "last_update_date": 1765584000,
        "tags": [],
        "whois": "Administrative city: REDACTED FOR
PRIVACY\nAdministrative country: Taiwan, Province Of
China\nAdministrative email: 50a11fe4587b136es@gmail.com,
\nAdministrative state: Taiwan\nBilling city: REDACTED FOR
PRIVACY\nBilling country: Taiwan, Province Of China\nBilling email:
d52ad5e18ac11e26s@net-chinese.com.tw\nCreate date: 2024-12-05
00:00:00\nDomain name: centosupdates.com\nDomain registrar id:
1336.0\nDomain registrar url: whois.net-chinese.com.tw\nExpiry date:
2026-12-05 00:00:00\nQuery time: 2025-12-14 04:50:33\nRegistrant
address: 1f8f4166599d23ee\nRegistrant city:
1f8f4166599d23ee\nRegistrant company: 1f8f4166599d23ee\nRegistrant
country: Taiwan, Province Of China\nRegistrant email:
50a11fe4587b136es@gmail.com,\nRegistrant name:
1f8f4166599d23ee\nRegistrant state: 12a25dd97c2aa81d\nRegistrant zip:
1f8f4166599d23ee\nTechnical city: REDACTED FOR PRIVACY\nTechnical
country: Taiwan, Province Of China\nTechnical email:
d52ad5e18ac11e26s@net-chinese.com.tw\nUpdate date: 2025-12-13
00:00:00",
        "first_seen_itw_date": 1640789950,
        "favicon": {
          "raw_md5": "3fa1bd1b382e00cabf7d0048f411af2a",
          "dhash": "41a6597969699641"
        },
        "jarm":
"29d29d00029d29d21c29d29d29d29d4d38a7b5ffb0e5536d09513d9de81205",
        "last_https_certificate_date": 1727165567,
        "creation_date": 1733356800,
        "reputation": 0,
        "last_analysis_results": {
          "Acronis": {
            "method": "blacklist",
            "engine_name": "Acronis",
            "category": "harmless",
```

```
            "result": "clean"
          },
          "ZeroFox": {
            "method": "blacklist",
            "engine_name": "ZeroFox",
            "category": "undetected",
            "result": "unrated"
          }
        },
        "last_seen_itw_date": 1694684844,
        "categories": {},
        "popularity_ranks": {},
        "total_votes": {
          "harmless": 0,
          "malicious": 0
        },
        "threat_severity": {
          "version": "D3",
          "threat_severity_level": "SEVERITY_NONE",
          "threat_severity_data": {
            "num_detections": 13,
            "has_bad_communicating_files_high": true,
            "has_bad_communicating_files_medium": true,
            "belongs_to_bad_collection": true,
            "belongs_to_threat_actor": true
          },
          "last_analysis_date": "1765204575",
          "level_description": "Severity NONE because it has less
than 2 detections."
        },
        "last_dns_records_date": 1768880935,
        "last_analysis_stats": {
          "malicious": 13,
          "suspicious": 1,
          "undetected": 27,
          "harmless": 52,
          "timeout": 0
        },
        "last_https_certificate": {
          "cert_signature": {
            "signature_algorithm": "sha256RSA",
            "signature":
```

```
"59462d40461e843083f948198463089877da104178d8b8324d2518ef23775c703b04
abc6edada89d917f94ab1c734d8658d40408de3eabae73ec89df3a4f8364954ff69c1
34606b40250ccc8e4aed4cad94f29d6c6423d1689989d36c750e5a07e344dcf2fb4b1
47ebee0df9bf9a70594f4db9e26961a0fd5cf07135e391abfe7a344526bc61510054e
0317deee97bd18acb7ecd558c169ed6dc23e032bb9b0b8d53a819f2fb28747e8ebb21
af1959aae41cc1f5ff00c034a1c21f8c71024e0979631961854a6ff5a0664f46223b7
ebf065cd6f86c737a9ce3388f1444b49761a0cca666ea017d2b00b348456fecf924d4
1b9d64fd77c673d3c7d33cc178aee8"
          },
          "extensions": {
            "key_usage": [
              "digitalSignature",
              "keyEncipherment"
            ],
            "CA": false,
            "ca_information_access": {
              "CA Issuers": "http://secure.globalsign.com/cacert/
gsgccr3dvtlsca2020.crt",
              "OCSP": "http://ocsp.globalsign.com/gsgccr3dvtlsca2020"
            },
            "certificate_policies": [
              "1.3.6.1.4.1.4146.1.10",
              "2.23.140.1.2.1"
            ],
            "crl_distribution_points": [
              "http://crl.globalsign.com/gsgccr3dvtlsca2020.crl"
            ],
            "subject_alternative_name": [
              "*.value-domain.com",
              "value-domain.com"
            ],
            "extended_key_usage": [
              "serverAuth",
              "clientAuth"
            ],
            "authority_key_identifier": {
              "keyid": "0d98c0737fabbdbdd9474b49ad0a4a0cac3ec77c"
            },
            "subject_key_identifier":
"f64a642d24e28968a6bb468a547fbc09908450d8",
            "1.3.6.1.4.1.11129.2.4.2":
"0482016b0169007600e6d2316340778cc1104106d771b9cec1d240f6968486fb"
          },
```

```
          "validity": {
            "not_after": "2025-06-22 09:36:51",
            "not_before": "2024-05-21 09:36:52"
          },
          "size": 1634,
          "version": "V3",
          "public_key": {
            "algorithm": "RSA",
            "rsa": {
              "modulus":
"d3cd29371c6c3cf811692053afe0a5a6d0915f3fdc245de58db79fc596d8e66f4a95
a6db55df369da915b7e575d2782f391b485de574f5456849ce808097e5b1516ea84db
34f7db003269d55ac4a0a25d5a3abed85c7f8b92cbce863e93d741112b7a51895039d
6efc9e6c18cb149bcbbcd8fe4948251d6830e266bb5929494f4b38a0c183c966f7dd8
0587d04340fd664745e714ac776af74a8808aed425cf0548a36ede19fe4f2b1433298
14970fa37f52dffcf2bbb534043ffe68d0ef56126489efa880457afb1305b1d249592
50478686e7b7ce9754b7dbd5efc19f1a0392a656ef617d24081fc20dcbc8c38f024c6
3b54c4a9b61281c68b91a300703a39",
              "exponent": "10001",
              "key_size": 2048
            }
          },
          "thumbprint_sha256":
"0ef793be2789c1f720db3d14af3409a275b2a07bc9f71940d483c35fd1c64dc8",
          "thumbprint": "ef063301053de37e2cab57b8da7d8f51073ceebe",
          "serial_number": "43dd1a276886f0260ac72bfc",
          "issuer": {
            "C": "BE",
            "O": "GlobalSign nv-sa",
            "CN": "GlobalSign GCC R3 DV TLS CA 2020"
          },
          "subject": {
            "CN": "*.value-domain.com"
          }
        },
        "gti_assessment": {
          "threat_score": {
            "value": 60
          },
          "severity": {
            "value": "SEVERITY_MEDIUM"
          },
```

```
          "verdict": {
            "value": "VERDICT_MALICIOUS"
          },
          "contributing_factors": {
            "malicious_sandbox_verdict": false,
            "mandiant_association_malware": true,
            "mandiant_confidence_score": 50,
            "gti_confidence_score": 90,
            "normalised_categories": [
              "phishing"
            ],
            "mandiant_association_actor": true,
            "safebrowsing_verdict": "harmless",
            "associated_actor": true
          },
          "description": "This indicator is malicious (medium
severity). GTI's ML scoring model identified this indicator as
malicious, it is associated with a tracked Mandiant threat actor, it
is associated with a tracked Mandiant malware family, it is contained
within a collection provided by the Google Threat Intelligence team,
or a trusted partner or security researcher and it was detected as a
Mandiant malware family that downloads and potentially executes a
payload."
        }
      }
    }
  ]
}
```


URLs

```
GET {base_url}/api/v3/collections/{entity_id}/search?query=entity:url
```

Sample Response:


```
{
  "data": [
    {
      "id":
"2d2c5810e379ac61b4b40453e40d78f0e93b1748d868520ad016888ce102b96c",
      "type": "url",
      "links": {
        "self": "https://www.virustotal.com/api/v3/urls/
```

```
2d2c5810e379ac61b4b40453e40d78f0e93b1748d868520ad016888ce102b96c"
      },
      "attributes": {
        "last_submission_date": 1749988084,
        "last_http_response_code": 200,
        "last_analysis_date": 1749988084,
        "total_votes": {
          "harmless": 0,
          "malicious": 0
        },
        "favicon": {
          "raw_md5": "c44bbec78ebc720a8c3783f5f2f37898",
          "dhash": "dcc69eb0b2f2f060"
        },
        "reputation": 0,
        "threat_severity": {
          "version": "U3",
          "threat_severity_level": "SEVERITY_NONE",
          "threat_severity_data": {
            "num_detections": 5,
            "has_bad_downloaded_files_high": true,
            "has_bad_downloaded_files_medium": true,
            "belongs_to_bad_collection": true,
            "belongs_to_threat_actor": true
          },
          "last_analysis_date": "1749991873",
          "level_description": "Severity NONE because it has less
than 2 detections."
        },
        "tld": "com",
        "last_http_response_cookies": {},
        "title": "DriveHQ Error Page",
        "first_seen_itw_date": 1710134463,
        "times_submitted": 18,
        "last_analysis_stats": {
          "malicious": 5,
          "suspicious": 1,
          "undetected": 27,
          "harmless": 64,
          "timeout": 0
        },
        "last_final_url": "https://www.drivehq.com/errorpage.aspx?
fromURL=https://info-mod.firstcloudit.com/
```

```
&errcode=8&errmsg=Permission+Denied!
+The+file+owner+is+not+allowed+to+publish+files+of+this+type.&gotoURL
=/",
        "tags": [
          "password-input",
          "external-resources"
        ],
        "has_content": false,
        "categories": {
          "alphaMountain.ai": "Information Technology, Malicious
(alphaMountain.ai)",
          "BitDefender": "computersandsoftware",
          "Sophos": "information technology",
          "Forcepoint ThreatSeeker": "malicious web sites"
        },
        "last_http_response_content_length": 85993,
        "first_submission_date": 1702405015,
        "mandiant_ic_score": 100,
        "redirection_chain": [
          "https://info-mod.firstcloudit.com/"
        ],
        "url": "https://info-mod.firstcloudit.com/",
        "last_seen_itw_date": 1712670553,
        "outgoing_links": [
          "https://www.linkedin.com/company/drivehq",
          "https://x.com/TheDriveHQ",
          "https://www.cameraftp.com/CameraFTP/pricing.aspx"
        ],
        "threat_names": [
          "Mal/HTMLGen-A"
        ],
        "last_modification_date": 1750006722,
        "last_http_response_content_sha256":
"463ec407ab626fd608299649f5e3aa868b02968eb7bfd63cb5734d4e5736d44c",
        "last_analysis_results": {
          "Artists Against 419": {
            "method": "blacklist",
            "engine_name": "Artists Against 419",
            "category": "harmless",
            "result": "clean"
          }
        },
        "html_meta": {
```

```
          "viewport": [
            "width=device-width, initial-scale=1.0"
          ],
          "author": [
            "DriveHQ"
          ]
        },
        "last_http_response_headers": {
          "Cache-Control": "private",
          "Content-Type": "text/html; charset=utf-8",
          "Vary": "User-Agent,User-Agent",
          "Server": "Microsoft-IIS/10.0",
          "X-Frame-Options": "DENY",
          "X-AspNet-Version": "4.0.30319",
          "Set-Cookie": "refID=0; expires=Wed, 15-Oct-2025 12:46:04
GMT; path=/; secure; HttpOnly, srcID=0; expires=Wed, 15-Oct-2025
12:46:04 GMT; path=/; secure; HttpOnly, randID=10126508554473907 45;
expires=Wed, 15-Oct-2025 12:46:04 GMT; path=/; secure; HttpOnly,
ServerUTCDateOffset=-25200000; expires=Mon, 16-Jun-2025 08:46:04 GMT;
path=/; secure",
          "X-Powered-By": "ASP.NET",
          "Date": "Sun, 15 Jun 2025 12:46:03 GMT",
          "Content-Length": "85993"
        },
        "gti_assessment": {
          "verdict": {
            "value": "VERDICT_MALICIOUS"
          },
          "threat_score": {
            "value": 100
          },
          "severity": {
            "value": "SEVERITY_HIGH"
          },
          "contributing_factors": {
            "safebrowsing_verdict": "harmless",
            "associated_actor": true,
            "mandiant_confidence_score": 100,
            "gti_confidence_score": 99,
            "mandiant_association_actor": true,
            "mandiant_analyst_malicious": true
          },
```

```
          "description": "This indicator is malicious (high severity)
with high impact. It was determined as malicious by a Mandiant
analyst, Mandiant's scoring pipeline identified this indicator as
malicious, GTI's ML scoring model identified this indicator as
malicious, it is associated with a tracked Mandiant threat actor and
it is contained within a collection provided by the Google Threat
Intelligence team, or a trusted partner or security researcher.
Analysts should prioritize investigation."
        }
      },
      "context_attributes": {
        "url": "https://info-mod.firstcloudit.com/"
      }
    }
  ]
}
```

ThreatQ provides the following default mapping for this feed:

> The following fields are added to the description if they are enabled: `.data[].attributes.gti_assessment.description`, `.attributes.whois`, `.attributes.outgoing_links`, `.attributes.crowdsourced_ai_results[]`, `.crowdsourced_context`, `attributes.names`, `.attributes.crowdsourced_yara_results`, `.attributes.sigma_analysis_results`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data[].id/ data[].attributes.sha256 / data[].attributes.url`	`Indicator .Value`	`Mapped: .type`	`.data[].attributes. first_submission_date/.data[].attributes.first_seen_itw_date`	`45.154.13.229/ https://info-mod.firstcloudit.com/`	See Indicator Type Mapping Table. For `url` type, the value is mapped to `url` key. For type `file`, the value is mapped to `.sha256` and for the rest of them, it is mapped to the `.id` key.
`.data[].attributes.tags, data[].attributes.type_tags`	`Indicator .Tags`	`N/A`	`N/A`	`N/A`	User-configurable. Updatable
`.data[].context_attributes[].sources[type=threat_profile].label`	`Indicator .Attribute`	`Threat Profile`	`.data[].attributes. first_submission_date/.data[].attributes.first_seen_itw_date`	`N/A`	User-configurable. Updatable
`.data[].attributes.gti_assessment.contributing_factors.mandi`	`Indicator .Attribute`	`Mandiant Score`	`.data[].attributes. first_submission_date/.data[].attribut`	`100`	User-configurable. Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
ant_confidence_score			es.first_seen_itw_date		
.data[].attributes.gti_assessment.contributing_factors.normalised_categories[]	Indicator.Attribute	Category	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	N/A	User-configurable
.data[].attributes.gti_assessment.contributing_factors.gti_confidence_score	Indicator.Attribute	Confidence Score	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	99	User-configurable. Updatable
.data[].attributes.gti_assessment.severity.value	Indicator.Attribute	Severity	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	High	User-configurable. Updatable. Title-cased . Severity_ was removed
.data[].attributes.gti_assessment.threat_score.value	Indicator.Attribute	Threat Score	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	100	User-configurable. Updatable
.data[].attributes.gti_assessment.threat_score.value	Indicator.Attribute	Normalised Threat Score	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	High	Normalized based on user-field mapping. User-Configurable. Updatable
.data[].attributes.gti_assessment.verdict.value	Indicator.Attribute	Verdict	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	VERDICT_MALICIOUS	User-configurable, Updatable
.data[].attributes.gti_assessment.contributing_factors.safebrowsing_verdict	Indicator.Attribute	Safe Browsing Verdict	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	Harmless	User-configurable, Updatable
.data[].attributes.gti_assessment.contributing_factors.pervasive_indicator	Indicator.Attribute	Is Pervasive	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	True	User-configurable, Updatable. Converted to String
.data[].attributes.last_analysis_stats.malicious	Indicator.Attribute	Malicious Count	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	N/A	User-configurable, Updatable.
.data[].attributes.last_analysis_stats.suspicious	Indicator.Attribute	Suspicious Count	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	N/A	User-configurable, Updatable.
.data[].attributes.as_owner	Indicator.Attribute	As Organization	.data[].attributes.first_submission_date/.data[].attribut	MOACK.Co.LTD	User-configurable.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
			es.first_seen_itw_date		
.data[].attributes.asn	Indicator.Attribute	ASN	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	MOACK.Co.LTD	User-configurable, Ingested according to Ingest ASNs As.
.data[].attributes.asn	Related Indicator.Value	ASN	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	MOACK.Co.LTD	User-configurable, Ingested according to Ingest ASNs As.
.data[].attributes.regional_internet_registry	Indicator.Attribute	RIR	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	APNIC	User-configurable.
.data[].attributes.last_http_response_code	Indicator.Attribute	Last HTTP Response Code	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	200	User-configurable.
.data[].attributes.title	Indicator.Attribute	Site Title	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	N/A	User-configurable.
.data[].attributes.last_submission_date	Indicator.Attribute	Last Submission Date	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	2015-10-29T03:20:53	User-configurable.
.data[].attributes.md5	Related Indicator.Value	MD5	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	2c397d151a6137a2a9be6455d143d165	User-configurable.
.data[].attributes.sha1	Related Indicator.Value	SHA-1	.data[].attributes.first_submission_date/.data[].attributes.first_seen_itw_date	2cc2ad776a7a4149ddded992c05b6c458accb0c6	User-configurable.
.data[].attributes.crowdsourced_ids_results[].rule_msg	Signature.Name	Snort	N/A	N/A	User-configurable.
.data[].attributes.crowdsourced_ids_results[].rule_raw	Signature.Value	Snort	N/A	N/A	User-configurable.
.data[].attributes.crowdsourced_ids_results[].alert_severity	Signature.Attribute	Severity	N/A	N/A	User-configurable.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data[].attributes.crowdsourced_ids_results[].rule_category`	`Signature.Attribute`	`Category`	`N/A`	`N/A`	User-configurable.
`.data[].attributes.crowdsourced_ids_results[].rule_source`	`Signature.Attribute`	`Source`	`N/A`	`N/A`	User-configurable.
`.data[].attributes.meaningful_name`	`Indicator.Attribute`	`Meaningful Name`	`.data[].attributes.last_modification_date`	`Malicious`	User-configurable.
`.data[].attributes.continent`	`Indicator.Attribute`	`Continent Code`	`N/A`	`AS`	User-configurable.
`.data[].attributes.country`	`Indicator.Attribute`	`Country Code`	`N/A`	`RU`	User-configurable.

For `.data[].attributes.first_submission_date` is not received for IP Addresses and Domains. In this case, the "Published Date" falls on `.data[].attributes.first_seen_itw_date`.

Indicator Type Mapping

The following table displays indicator type mapping from Google to ThreatQ.

GOOGLE TYPE	THREATQ INDICATOR TYPE
ip_address	IP Address
url	URL
domain	FQDN
sha1	SHA-1
md5	MD5
file	SHA-256

Google Threat Intelligence Related Vulnerabilities (Supplemental)

The Google Threat Intelligence Related Vulnerabilities supplemental feed fetches related CVEs.

`GET {base_url}api/v3/collections/{{run_params.entity_id}}/vulnerabilities`

Sample Response:


```
{
    "data": [
        {
            "id": "vulnerability--cve-2004-0210",
            "type": "collection",
            "links": {
                "self": "https://www.virustotal.com/api/v3/
collections/vulnerability--cve-2004-0210"
            },
            "attributes": {
                "risk_factors": [
                    "Local Access Required"
                ],
                "cve_id": "CVE-2004-0210",
                "files_count": 1,
                "creation_date": 1646663312,
                "alt_names": [],
                "targeted_regions": [],
                "alt_names_details": [],
                "priority": "P1",
                "source_regions_hierarchy": [],
                "field_sources": [
                    {
                        "source": {
                            "sources": [],
                            "field_type": "Ranked",
                            "source_name": "Cybersecurity and
Infrastructure Security Agency (CISA)",
                            "source_url": ""
                        },
                        "field": "cvss.cvssv3_x"
                    }
                ],
                "cisa_known_exploited": {
```

```
                    "ransomware_use": "Unknown",
                    "due_date": 1648080000,
                    "added_date": 1646265600
                },
                "status": "COMPUTED",
                "collection_type": "vulnerability",
                "workarounds": [],
                "technologies": [],
                "recent_activity_summary": [
                    0,
                    0
                ],
                "first_seen_details": [],
                "date_of_disclosure": 1089676800,
                "capabilities": [],
                "origin": "Google Threat Intelligence",
                "cvss": {
                    "cvssv3_x": {
                        "vector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/
C:H/I:H/A:H",
                        "base_score": 7.8,
                        "temporal_score": 7.8
                    },
                    "cvssv2_0": {
                        "vector": "AV:L/AC:L/Au:N/C:C/I:C/A:C/E:F/
RL:OF/RC:C",
                        "base_score": 7.2,
                        "temporal_score": 6.0
                    }
                },
                "available_mitigation": [
                    "Patch"
                ],
                "affected_systems": [],
                "top_icon_md5": [],
                "tags": [
                    "has_exploits",
                    "observed_in_the_wild"
                ],
                "sources": [
                    {
                        "url": "https://exchange.xforce.ibmcloud.com/
```

```
vulnerabilities/16590",
                        "title": "Microsoft Windows POSIX buffer
overflow allows local attacker to gain privileges",
                        "cvss": {
                            "cvssv3_x": null,
                            "cvssv2_0": null,
                            "cvssv3_x_translated": null,
                            "cvssv4_x": null
                        },
                        "md5": null,
                        "unique_id": null,
                        "published_date": 1089748800,
                        "name": "IBM Corp.",
                        "source_description": null
                    }
                ],
                "targeted_industries_tree": [],
                "urls_count": 0,
                "last_seen_details": [],
                "references_count": 0,
                "malware_roles": [],
                "subscribers_count": 0,
                "tags_details": [
                    {
                        "first_seen": null,
                        "description": null,
                        "last_seen": null,
                        "value": "observed_in_the_wild",
                        "confidence": "possible"
                    }
                ],
                "private": true,
                "epss": {
                    "percentile": 0.9259,
                    "score": 0.10564
                },
                "executive_summary": "\n\n* A Buffer Overflow
vulnerability exists that, when exploited, allows a local, privileged
attacker to bypass certain security mechanisms.\n* This vulnerability
has been confirmed to be exploited in the wild. Unverified exploit
code is available.\n* Google Threat Intelligence Group (GTIG)
considers this a Medium-risk vulnerability due to the potential for
bypassing certain security mechanisms, offset by local access
```

```
requirements.\n* Mitigation options include a patch.\n",
                "motivations": [],
                "version_history": [
                    {
                        "date": 1743734117,
                        "version_notes": [
                            "exploitation_vectors: Added
['Unspecified Local Vector'] to existing exploitation_vectors. "
                        ]
                    }
                ],
                "vulnerable_products": "",
                "last_modification_date": 1743734117,
                "cpes": [
                    {
                        "end_rel": null,
                        "end_cpe": null,
                        "start_rel": "=",
                        "start_cpe": {
                            "version": "",
                            "product": "Windows 2000",
                            "uri":
"cpe:2.3:o:microsoft:windows_2000:-:sp3:*:*:advanced_server:*:*:*",
                            "vendor": "Microsoft"
                        }
                    }
                ],
                "summary_stats": {
                    "first_submission_date": {
                        "min": 1639345444.0,
                        "max": 1639345444.0,
                        "avg": 1639345444.0
                    },
                    "last_submission_date": {
                        "min": 1639390624.0,
                        "max": 1639390624.0,
                        "avg": 1639390624.0
                    },
                    "files_detections": {
                        "min": 0.0,
                        "max": 0.0,
                        "avg": 0.0
                    }
```

```
                },
                "exploitation_vectors": [
                    "Local Access",
                    "Unspecified Local Vector"
                ],
                "analysis": "\n\nAn attacker could exploit this
vulnerability to gain elevated privileges. An attacker would need to
specially craft a malicious application and run it on the vulnerable
system. A failed attempt at exploitation could potentially cause a
crash of the application, resulting in a denial-of-service condition.
\n\nThis vulnerability has been exploited by the Tsar Team since at
least 2007 in a variety of campaigns. For more information, please
refer to the report, \"[Overview of Tsar Team Espionage Activity]
(https://advantage.mandiant.com/reports/16-00014614).\"\n\nIn January
2014, a campaign ofÂ targeted spam messages began with the intent of
installing Gameover Zeus on victim systems. For more information,
please refer to the report, \"[Gameover Zeus Resumes Operations with
Altered Malware and Increased Use of Fluxxy and KOL Fast-Flux
Infrastructure Hosting](https://advantage.mandiant.com/reports/
Intel-1167778).\"\n\nCISA added this vulnerability to its Known
Exploited Vulnerabilities Catalog on March 3, 2022, with a required
remediation date of March 24, 2022.\n\n  \nMandiant Threat
Intelligence considers this a Medium-risk vulnerability due to the
potential for escalation of privileges, offset by the local access
required.\n\n",
                "ip_addresses_count": 0,
                "risk_rating": "MEDIUM",
                "days_to_report": 6446,
                "exploitation_consequence": "Security Bypass",
                "intended_effects": [],
                "mati_genids_dict": {
                    "cve_id": "vulnerability--e35ba016-5a4d-55e1-
a812-ee56477a6df6",
                    "report_id": "report--
c81eb59b-89fe-5c73-8659-5cd10d51e2b3",
                    "mve_id": "vulnerability--23e4110d-
ee84-5250-8ce3-ef5e84cad030"
                },
                "name": "CVE-2004-0210",
                "exploitation_state": "Confirmed",
                "predicted_risk_rating": "",
                "targeted_industries": [],
```

```
                "exploitation": {
                    "first_exploitation": 1474761600,
                    "tech_details_release_date": null,
                    "exploit_release_date": 1089936000
                },
                "domains_count": 0,
                "counters": {
                    "files": 1,
                    "domains": 0,
                    "ip_addresses": 0,
                    "urls": 0,
                    "iocs": 1,
                    "subscribers": 0,
                    "attack_techniques": 0
                },
                "autogenerated_tags": [],
                "targeted_informations": [],
                "merged_actors": [],
                "detection_names": [],
                "operating_systems": [],
                "mitigations": [],
                "threat_scape": [],
                "exploit_availability": "Unverified",
                "cwe": {
                    "title": "Buffer Overflow",
                    "id": "CWE-120"
                },
                "mve_id": "MVE-2004-88",
                "vendor_fix_references": [
                    {
                        "url": "http://www.kb.cert.org/vuls/id/
647436",
                        "title": "Microsoft Windows contains a buffer
overflow in the POSIX subsystem",
                        "cvss": null,
                        "md5": null,
                        "unique_id": "VU#647436",
                        "published_date": 1089835200,
                        "name": "CERT/CC",
                        "source_description": null
                    }
                ],
```

```
                "collection_links": [],
                "targeted_regions_hierarchy": [],
                "description": "\n\nThe National Vulnerability
Database (NVD) has provided the following description:\n\n*The POSIX
component of Microsoft Windows NT and Windows 2000 allows local users
to execute arbitrary code via certain parameters, possibly by
modifying message length values and causing a buffer overflow.*\n\n",
                "is_content_translated": false,
                "aggregations": {
                    "files": {
                        "tags": [
                            {
                                "value": "javascript",
                                "count": 1
                            }
                        ],
                        "vhash": [
                            {
                                "value":
"3101773ac42964b4fd3c05b2c4d8e433",
                                "count": 1,
                                "total_related": 36356,
                                "prevalence": 2.750577621300473e-05
                            }
                        ],
                        "tlshhash": [
                            {
                                "value":
"T12632B6D94839693321BB861947072A5DFA5D401B53A8E719FC8C874C9FB21A0C6E
8F98",
                                "count": 1,
                                "total_related": 1,
                                "prevalence": 1.0
                            }
                        ],
                        "embedded_domains": [
                            {
                                "value": "www.securityfocus.com",
                                "count": 1,
                                "total_related": 44620,
                                "prevalence": 2.2411474675033616e-05
                            }
```

```
                        ],
                        "embedded_urls": [
                            {
                                "value": "https://
www.securityfocus.com/bid/10710/info",
                                "count": 1,
                                "total_related": 1,
                                "prevalence": 1.0
                            }
                        ]
                    }
                }
            },
            "context_attributes": {
                "shared_with_me": false,
                "role": "viewer"
            }
        }
        ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.name	Related Vulnerability/ Indicator.Value	CVE	.data[].attributes.creation_date	CVE-2004-0210	User-configurable. Based on Ingest CVE as selected option
.data[].attributes.description	Related Vulnerability/ Indicator.Description	N/A	N/A	The National Vulnerability Database (NVD) has provided.....	N/A
.data[].attributes.cvss.cvssv2_0.vector	Related Vulnerability/ Indicator.Attribute	CVSS v2 Vector	.data[].attributes.creation_date	AV:L/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C	User-configurable
.data[].attributes.cvss.cvssv2_0.base_score	Related Vulnerability/ Indicator.Attribute	CVSS v2 Base Score	.data[].attributes.creation_date	7.2	User-configurable
.data[].attributes.cvss.cvssv2_0.temporal_score	Related Vulnerability/ Indicator.Attribute	CVSS v2 Temporal Score	.data[].attributes.creation_date	6.0	User-configurable
.data[].attributes.cvss.cvssv3_x.vector	Related Vulnerability/ Indicator.Attribute	CVSS v3 Vector	.data[].attributes.creation_date	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	User-configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.cvss.cvssv3_x.base_score	Related Vulnerability/ Indicator.Attribute	CVSS v3 Base Score	.data[].attributes.creation_date	7.8	User-configurable
.data[].attributes.cvss.cvssv3_x.temporal_score	Related Vulnerability/ Indicator.Attribute	CVSS v3 Temporal Score	.data[].attributes.creation_date	7.8	User-configurable
.data[].attributes.cvss.exploitation_vectors[]	Related Vulnerability/ Indicator.Attribute	Exploitation Vector	.data[].attributes.creation_date	Local Access	User-configurable
.data[].attributes.epss.score	Related Vulnerability/ Indicator.Attribute	EPSS Score	.data[].attributes.creation_date	0.10564	User-configurable

Google Threat Intelligence Related Adversaries (Supplemental)

The Google Threat Intelligence Related Adversaries supplemental feed fetches related adversaries.

```
GET {base_url}/api/v3/collections/{entity_id}/threat_actors
```

> Sample Response is the same as the sample response for: `Google Threat Intelligence`

ThreatQ provides the following default mapping for this feed based on each item within the *`.data[]`* list.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.attributes.name	Related Adversary.Value	Adversary	.attributes.last_modification_date	APT28	N/A
.attributes.alt_names_details[].value	Related Adversary.Tag	N/A	N/A	APT28 (Google)	User-Configurable
.attributes.description	Related Adversary.Description	N/A	N/A	APT28 is a highly active cyber espionage group that ...	N/A
.attributes.motivations[].value	Related Adversary.Attribute	Motivation	.attributes.last_modification_date	Attack / Destruction	User-Configurable. When the Motivation option is checked in the context
.attributes.targeted_industrie	Related Adversary.Attribute	Target Industry	.attributes.last_modification_date	Aerospace & Defense	User-Configurable. When the Industry option is checked in the context

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
s_tree[].industry_group					
.attributes.source_regions_hierarchy[].region	Related Adversary.Attribute	Region	.attributes.last_modification_date	Europe	User-Configurable. When the Source Context option is checked in the context
.attributes.source_regions_hierarchy[].sub_region	Related Adversary.Attribute	Sub Region	.attributes.last_modification_date	Eastern Europe	User-Configurable. When the Source Context option is checked in the context
.attributes.source_regions_hierarchy[].country	Related Adversary.Attribute	Country	.attributes.last_modification_date	Russian Federation	User-Configurable. When the Source Context option is checked in the context
.attributes.source_regions_hierarchy[].country_iso2	Related Adversary.Attribute	Country Code	.attributes.last_modification_date	RU	User-Configurable. When the Source Context option is checked in the context
.attributes.targeted_regions_hierarchy[].region	Related Adversary.Attribute	Target Region	.attributes.last_modification_date	RO	User-Configurable. When the Target Region option is checked in the context
.attributes.targeted_regions_hierarchy[].sub_region	Related Adversary.Attribute	Target Sub Region	.attributes.last_modification_date	Eastern Europe	User-Configurable. When the Target Region option is checked in the context
.attributes.targeted_regions_hierarchy[].country	Related Adversary.Attribute	Target Country	.attributes.last_modification_date	Russian Federation	User-Configurable. When the Target Region option is checked in the context
.attributes.targeted_regions_hierarchy[].country_iso2	Related Adversary.Attribute	Target Country Code	.attributes.last_modification_date	RU	User-Configurable. When the Target Region option is checked in the context

Google Threat Intelligence Campaigns

The Google Threat Intelligence Campaigns feed ingests campaigns tracked by Google. This feed also ingests any related indicators, malware, threat actors, vulnerabilities, and attack patterns relevant to the campaign.

```
GET {base_url}/api/v3/collections?filter=collection_type:campaign
```

Sample Response is the same as the one for `Google Threat Intelligence Related Campaigns Supplemental feed`.

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data[].attributes.name`	Campaign.Value	N/A	`.data[].attributes.last_modification_date`	APT28 Conducts Credential Harvesting Campaign Targeting Multiple European Entities	N/A
`.data[].attributes.description`	Campaign.Description	N/A	`.data[].attributes.last_modification_date`	Starting in early February 2024, Mandiant observed UNC4697 ...	N/A
`.data[].attributes.motivations[].value`	Campaign.Attribute	Motivation	`.data[].attributes.last_modification_date`	Espionage	User-configurable
`.data[].attributes.targeted_industries_tree[].industry_group`	Campaign.Attribute	Target Sector	`.data[].attributes.last_modification_date`	Government	User-configurable
`.data[].attributes.source_regions_hierarchy[].region`	Campaign.Attribute	Region	`.data[].attributes.last_modification_date`	Europe	User-configurable
`.data[].attributes.source_regions_hierarchy[].sub_region`	Campaign.Attribute	Sub Region	`.data[].attributes.last_modification_date`	Eastern Europe	User-configurable
`.data[].attributes.source_regions_hierarchy[].country`	Campaign.Attribute	Country	`.data[].attributes.last_modification_date`	Russian Federation	User-configurable
`.data[].attributes.source_regions_hierarchy[].country_iso2`	Campaign.Attribute	Country Code	`.data[].attributes.last_modification_date`	RU	User-configurable
`.data[].attributes.targeted_regions_hierarchy[].sub_region`	Campaign.Attribute	Target Sub Region	`.data[].attributes.last_modification_date`	Eastern Europe	User-configurable
`.data[].attributes.targeted_re`	Campaign.Attribute	Target Country	`.data[].attributes.last_modification_date`	Russian Federation	User-configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
gions_hierarchy[].country					
.data[].attributes.targeted_regions_hierarchy[].country_iso2	Campaign.Attribute	Target Country Code	.data[].attributes.last_modification_date	RU	User-configurable
.data[].attributes.targeted_regions_hierarchy[].region	Campaign.Attribute	Target Region	.data[].attributes.last_modification_date	RO	User-configurable
.data[].attributes.campaign_type	Campaign.Attribute	Campaign Type	.data[].attributes.last_modification_date	INDIVIDUAL	User-configurable
.data[].attributes.last_seen	Campaign.Attribute	Last Seen	.data[].attributes.last_modification_date	1727913600	Updatable. Timestamp value.
.data[].id	Related Adversary	Adversary	N/A	N/A	User-configurable. See Google Threat Intelligence Related Adversaries (Supplemental)
.data[].id	Related Malware	Malware	N/A	N/A	User-configurable. See Google Threat Intelligence Related Malware (Supplemental)
.data[].id	Related Vulnerability/ Related Indicator	Vulnerability/CVE	N/A	N/A	User-configurable. See Google Threat Intelligence Related Vulnerabilities (Supplemental)
.data[].id	Related Attack Pattern	Attack Pattern	N/A	N/A	User-configurable. See Google Threat Intelligence Related Attack Pattern (Supplemental)
.data[].id	Related Indicator	Indicator	N/A	N/A	User-configurable. See Google Threat Intelligence Related IOC (Supplemental)

For each campaign ID in the collection, the supplemental feeds collect all related objects. Sample data & mapping for them can be found in each

Supplemental feed mapping section, as specified in the above mapping table notes.

Google Threat Intelligence Indicators

The Google Threat Intelligence Indicators feed ingests a list of Indicators tracked by Google TI filtered by time.

```
GET {base_url}/api/v3/collections?filter=collection_type:collection
```

Sample Response [truncated]:


```
{
    "data": [
        {
            "id":
"fee4323cebb88f025586fd9f3e7d0de183fd536fad2312d4ccccdb21f2f7185f",
            "type": "collection",
            "links": {
                "self": "https://www.virustotal.com/api/v3/
collections/
fee4323cebb88f025586fd9f3e7d0de183fd536fad2312d4ccccdb21f2f7185f"
            },
            "attributes": {

            },
            "context_attributes": {
                "shared_with_me": false,
                "role": "viewer"
            }
        }
  ],
    "meta": {
        "count": 6898,
        "cursor": "eJwVjN1uwiAYQF-JlpHMyxnAn-
Wjih_QclerUws43FxszR5-3eXJOTm_vo7vh5jv7ppbJ2XGMs87En-213iBIj9cOLijibd
9GXc6rM3ORdo6GKs6hi0JpaVZHsXAd7jeWJLvmAqrDLsZtH5vDcGUv1vDlro-
qGPqHs4VGmQYbX3eaMI-0RVVK7NAnFcQwohGfykzW2KdlRWSTj-
pxEzodN7YYvL_PZl8yus9F-xjOZRAh1fArgA80QobBteJk6GeA1HP8KL4lvkkhmrRUN-
fBoWrBzyhVM6GClcUeMeg11Fx2aseRsXDs-ltArcq_cJfmh4Y4Bv1pz84PGUl"
    },
    "links": {
        "self": "https://www.virustotal.com/api/v3/collections?
filter=collection_type:collection%20last_modification_date:2025-01-01
%2B",
        "next": "https://www.virustotal.com/api/v3/collections?
```

```
filter=collection_type%3Acollection+last_modification_date%3A2025-01-
01%2B&cursor=eJwVjN1uwiAYQF-JlpHMyxnAn-
Wjih_QclerUws43FxszR5-3eXJOTm_vo7vh5jv7ppbJ2XGMs87En-213iBIj9cOLijibd
9GXc6rM3ORdo6GKs6hi0JpaVZHsXAd7jeWJLvmAqrDLsZtH5vDcGUv1vDlro-
qGPqHs4VGmQYbX3eaMI-0RVVK7NAnFcQwohGfykzW2KdlRWSTj-
pxEzodN7YYvL_PZl8yus9F-xjOZRAh1fArgA80QobBteJk6GeA1HP8KL4lvkkhmrRUN-
fBoWrBzyhVM6GClcUeMeg11Fx2aseRsXDs-ltArcq_cJfmh4Y4Bv1pz84PGUl"
    }
  }
```

For each `data[].id` of the IOC Collection, related indicators are retrieved. See the Google Threat Intelligence Related IOC (Supplemental) mapping is the same.

Google Threat Intelligence Malware

The Google Threat Intelligence Malware feed ingests malware tracked by Google TI. This feed also ingests any related indicators, threat actors, vulnerabilities, and attack patterns relevant to the malware.

`GET {base_url}/api/v3/collections?filter=collection_type:malware-family`

> Sample Response is the same as the sample response for: `Google Threat Intelligence Related Malware Supplemental feed.`

ThreatQ provides the following default mapping for this data:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data[].attributes.name`	Malware Value	Malware	`.data[].attributes.last_modification_date`	`LOCKBIT`	N/A
`.data[].attributes.description`	Malware Description	N/A	`.data[].attributes.last_modification_date`	`LOCKBIT is a ransomware written in C...`	N/A
`.data[].attributes.alt_names[]`	Attribute	`Alias`	`.last_upddata[].attributes.last_modification_dateated`	N/A	User-configurable.
`.data[].attributes.capabilities[].value`	Attribute	`Capability`	`.data[].attributes.last_modification_date`	N/A	User-configurable.
`.data[].attributes.targeted_industries_tree[].industry_group`	Attribute	`Target Sector`	`.last_updata[].attributes.last_modification_datedated`	N/A	User-configurable.
`.data[].attributes.last_seen`	Attribute	`Last Active`	`.data[].attributes.last_modification_date`	N/A	User-configurable.Updatable
`.data[].attributes.operating_systems[].value`	Attribute	`Target Operating System`	`.data[].attributes.last_modification_date`	N/A	User-configurable.
`.data[].attributes.malware_roles[].value`	Attribute	`Role`	`.data[].attributes.last_modification_date`	N/A	User-configurable.
`.data[].id`	Related Adversary	Adversary	N/A	N/A	User-configurable. See `Google Threat Intelligence Related Adversaries (Supplemental)` above
`.data[].id`	Related Campaign	Campaign	N/A	N/A	User-configurable. See `Google Threat Intelligence Related`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					`Campaigns (Supplemental)` above
`.data[].id`	Related Vulnerability/ Related Indicator	Vulnerability/CVE	N/A	N/A	User-configurable. See `Google Threat Intelligence Related Vulnerabilities (Supplemental)` above
`.data[].id`	Related Attack Pattern	Attack Pattern	N/A	N/A	User-configurable. See `Google Threat Intelligence Related Attack Pattern (Supplemental)` above
`.data[].id`	Related Indicator	Indicator	N/A	N/A	User-configurable. See `Google Threat Intelligence Related IOC (Supplemental)` above

Google Vulnerability Intelligence

The Google Vulnerability Intelligence feed will fetch and ingest the latest vulnerabilities & supporting context, reported by Google TI.

Two main pieces of data will be ingested by this feed: a Vulnerability Object and its corresponding CVE ID as an Object. You can configure the feed to ingest these CVE IDs as either a Vulnerability Object and/or an Indicator Object, with the CVE type.

```
GET {base_url}/api/v3/collections?
filter=collection_type:vulnerability
```

Sample Response:


```
{
  "data": [
    {
      "id": "vulnerability--cve-2025-31324",
      "type": "collection",
      "links": {
        "self": "https://www.virustotal.com/api/v3/collections/
vulnerability--cve-2025-31324"
      },
      "attributes": {
        "description": "SAP NetWeaver Visual Composer Metadata
Uploader is not protected with a proper authorization, allowing
unauthenticated agent to upload potentially malicious executable
binaries that could severely harm the host system. This could
significantly affect the confidentiality, integrity, and availability
of the targeted system.",
        "collection_type": "vulnerability",
        "recent_activity_summary": [
          0,
          0
        ],
        "targeted_informations": [],
        "epss": {
          "score": 0.66207,
          "percentile": 0.98406
        },
        "top_icon_md5": [],
        "targeted_regions_hierarchy": [],
        "creation_date": 1745520314,
```

```
        "references_count": 0,
        "sources": [
          {
            "md5": "71ff8f7bd1271b29afb6ff0f61b36a0b",
            "published_date": 1745513427,
            "name": "Cybersecurity and Infrastructure Security Agency
(CISA)",
            "source_description": null,
            "url": "https://github.com/cisagov/vulnrichment/blob/
develop/2025/31xxx/CVE-2025-31324.json",
            "cvss": {
              "cvssv4_x": null,
              "cvssv2_0": null,
              "cvssv3_x_translated": null,
              "cvssv3_x": {
                "base_score": 10.0,
                "temporal_score": null,
                "vector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/
A:H"
              }
            },
            "title": null,
            "unique_id": null
          }
        ],
        "subscribers_count": 7,
        "tags": [
          "affects_ot",
          "observed_in_the_wild",
          "was_zero_day",
          "has_exploits",
          "media_attention"
        ],
        "threat_scape": [],
        "summary_stats": {},
        "tags_details": [
          {
            "description": null,
            "first_seen": null,
            "confidence": "possible",
            "last_seen": null,
            "value": "affects_ot"
```

```
          },
          {
            "description": null,
            "first_seen": null,
            "confidence": "possible",
            "last_seen": null,
            "value": "has_exploits"
          }
        ],
        "analysis": "An attacker would need to send an HTTP(S)
request to the '/developmentserver/metadatauploader' endpoint with
the 'CLIENT' parameter set to any value and the 'CONTENTTYPE'
parameter set to 'MODEL'. The JSP file contents must be sent in the
request body with the 'name' and 'filename' form-data fields set
appropriately. The JSP file is executed with a GET request to the '/
irj/filename' endpoint, where 'filename' is the name of the file
uploaded in the previous step. This JSP file will be executed with
Operating System user privileges.\n\nOn April 22, 2025, ReliaQuest
published a blog post detailing exploitation of this vulnerability in
the wild. Exploitation of this vulnerability was conducted to deploy
web-shells on several vulnerable systems. For more information,
please refer to their blog \"[ReliaQuest Uncovers New Critical
Vulnerability in SAP NetWeaver.](https://reliaquest.com/blog/threat-
spotlight-reliaquest-uncovers-vulnerability-behind-sap-netweaver-
compromise/)\"\n\nOn April 25, 2025, Onapsis released a blog post
detailing observed exploitation of this vulnerability in the wild.
For more information and IOCs, please refer to their blog post
\"[Active Exploitation of SAP Zero-Day Vulnerability (CVE-2025-31324,
SAP Security Note 3594142).](https://onapsis.com/blog/active-
exploitation-of-sap-vulnerability-cve-2025-31324/)\"\n\nOn April 28,
2025, Rapid7 reported they observed exploitation of this
vulnerability as early as March 27, 2025, against multiple customer
environments, primarily affecting manufacturing companies. For more
information, please refer to their blog post \"[Active exploitation
of SAP NetWeaver Visual Composer CVE-2025-31324.](https://
www.rapid7.com/blog/post/2025/04/28/etr-active-exploitation-of-sap-
netweaver-visual-composer-cve-2025-31324/)\"\n\nOn April 30, 2025,
WithSecure published a report detailing exploitation of this
vulnerability to deploy the XMRig coin miner. The earliest
exploitation activity they are aware of occurred on March 18, 2025.
For more information, please refer to their report \"[SAP NetWeaver
CVE-2025-31324 Exploitation.](https://labs.withsecure.com/
```

```
publications/netweaver-cve-2025-31324)\"\n\nOn May 13, 2025,
EclecticIQ published a [report](https://blog.eclecticiq.com/china-
nexus-nation-state-actors-exploit-sap-netweaver-cve-2025-31324-to-
target-critical-infrastructures) detailing China-nexus nation-state
APTs launching campaigns against critical infrastructure networks via
this vulnerability.\n\nOn May 14, 2025, ReliaQuest published an
[update](https://reliaquest.com/blog/threat-spotlight-reliaquest-
uncovers-vulnerability-behind-sap-netweaver-compromise/) stating that
multiple threat groups have attempted exploitation of this
vulnerability.\n\nGoogle Threat Intelligence Group (GTIG) has
observed exploitation of this vulnerability in the wild as early as
mid-March 2025.",
        "cisa_known_exploited": {
          "ransomware_use": "Unknown",
          "added_date": 1745884800,
          "due_date": 1747699200
        },
        "source_regions_hierarchy": [],
        "mati_genids_dict": {
          "report_id": null,
          "cve_id": "vulnerability--1d7f26d7-c182-55ae-9ab4-
c81951c63480",
          "mve_id": "vulnerability--e2ccf457-8ba4-5c45-
a63c-63bedaf70f21"
        },
        "targeted_industries": [],
        "field_sources": [
          {
            "field": "cvss.cvssv4_x.vector",
            "source": {
              "source_name": "Google Threat Intelligence Group
(GTIG)",
              "field_type": "Ranked",
              "sources": [],
              "source_url": ""
            }
          },
          {
            "field": "cvss.cvssv3_x_translated",
            "source": {
              "source_name": "Google Threat Intelligence Group
(GTIG)",
              "field_type": "Ranked",
```

```
            "sources": [],
            "source_url": ""
          }
        }
      ],
      "risk_factors": [],
      "detection_names": [],
      "predicted_risk_rating": "",
      "technologies": [],
      "exploitation": {
        "exploit_release_date": 1745280000,
        "tech_details_release_date": 1745539200,
        "first_exploitation": 1737331200
      },
      "cve_id": "CVE-2025-31324",
      "priority": "P0",
      "collection_links": [],
      "alt_names_details": [],
      "capabilities": [],
      "risk_rating": "CRITICAL",
      "cvss": {
        "cvssv3_x": {
          "base_score": 10.0,
          "temporal_score": 9.3,
          "vector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/
E:F/RL:O/RC:C"
        }
      },
      "vendor_fix_references": [
        {
          "md5": null,
          "published_date": 1745452800,
          "name": "SAP SE",
          "source_description": null,
          "url": "https://support.sap.com/en/my-support/knowledge-
base/security-notes-news/april-2025.html",
          "cvss": null,
          "title": "SAP Security Patch Day - April 2025",
          "unique_id": null
        }
      ],
      "targeted_regions": [],
```

```
        "affected_systems": [],
        "merged_actors": [],
        "mitigations": [],
        "private": true,
        "ip_addresses_count": 0,
        "domains_count": 0,
        "intended_effects": [],
        "days_to_patch": -14,
        "last_modification_date": 1750839775,
        "workarounds": [
          "<p>Restrict access to /uddi/ URLs to internal network
traffic, especially if upgrading isnâ€™t feasible.</p>"
        ],
        "exploit_availability": "Publicly Available",
        "origin": "Google Threat Intelligence",
        "last_seen_details": [],
        "exploitation_state": "Confirmed",
        "date_of_disclosure": 1745280000,
        "malware_roles": [],
        "executive_summary": "* An Improper Authorization
vulnerability exists that, when exploited, allows a remote attacker
to execute arbitrary code.\n* This vulnerability has been confirmed
to be exploited in the wild. Proof-of-concept and weaponized code is
publicly available.\n* Google Threat Intelligence Group (GTIG)
considers this a Critical-risk vulnerability due to the potential for
arbitrary code execution.\n* Mitigation options include a patch and a
workaround.",
        "motivations": [],
        "status": "COMPUTED",
        "files_count": 12,
        "operating_systems": [],
        "targeted_industries_tree": [
          {
            "industry_group": "Manufacturing",
            "industry": null,
            "confidence": "possible",
            "first_seen": null,
            "last_seen": null,
            "description": null,
            "source": null
          }
        ],
```

```
    "autogenerated_tags": [],
    "cwe": {
      "id": "CWE-285",
      "title": "Improper Authorization"
    },
    "exploitation_consequence": "Code Execution",
    "alt_names": [],
    "days_to_report": 2,
    "is_content_translated": false,
    "exploitation_vectors": [
      "Exposed Web Application"
    ],
    "mve_id": "MVE-2025-10681",
    "counters": {
      "files": 12,
      "domains": 0,
      "ip_addresses": 0,
      "urls": 0,
      "iocs": 12,
      "subscribers": 7,
      "attack_techniques": 0
    },
    "version_history": [
      {
        "date": 1750445522,
        "version_notes": [
          "epss.score: 0.80997 -> 0.66207"
        ]
      }
    ],
    "urls_count": 0,
    "first_seen_details": [],
    "cpes": [
      {
        "start_rel": "=",
        "end_cpe": null,
        "start_cpe": {
          "version": "7.50",
          "product": "Netweaver",
          "vendor": "SAP",
          "uri": "cpe:2.3:a:sap:netweaver:7.50:*:*:*:*:*:*:*"
        },
```

```
            "end_rel": null
          },
          {
            "start_rel": null,
            "end_cpe": {
              "version": "7.50 for Visual Composer Development
Server",
              "product": "Netweaver",
              "vendor": "SAP",
              "uri":
"cpe:2.3:a:sap:netweaver:7.50:*:*:*:*:visual_composer_development_ser
ver:*:*"
            },
            "start_cpe": null,
            "end_rel": "<="
          }
        ],
        "name": "CVE-2025-31324",
        "available_mitigation": [
          "Intrusion Prevention Signatures",
          "Patch"
        ],
        "aggregations": {}
      },
      "context_attributes": {
        "shared_with_me": false,
        "role": "viewer"
      }
    }
  ],
  "meta": {
    "count": 97,
    "cursor": "eJwVjMFugzAQRH8J262UHhOBoVRrBKwx5pYAReBV5KipTK1-
fOlhDqM3b36Hnj4m8k9z91cjpUfuL2NC3_WdVmA-GDeZWdPjxqltXKlbQ-
Jq4KfqydWJ453w8n9vNrk2sfuynOXHUT8XF9fmzwTlVAF5hIJUk7mAspGzfss0qvKWZq-
fxc5B7CfAkQEuL7AtAYr9NKQLq_AcqjQLKh0F4DuDCOJIorBcFY7Cbu7olh08DpvjA-
poeedsJFLouIru8Osw5FkCRge7_AFwNVDi"
  },
  "links": {
    "self": "https://www.virustotal.com/api/v3/collections?
filter=collection_type:vulnerability%20creation_date:2025-01-01%2B%20
(exploitation_state:Confirmed%20or%20exploitation_state:Suspected%20o
```

```
r%20exploitation_state:Reported)
%20(risk_rating:Critical%20or%20risk_rating:High%20or%20risk_rating:L
ow)",
    "next": "https://www.virustotal.com/api/v3/collections?
filter=collection_type%3Avulnerability+creation_date%3A2025-01-01%2B+
%28exploitation_state%3AConfirmed+or+exploitation_state%3ASuspected+o
r+exploitation_state%3AReported%29+
%28risk_rating%3ACritical+or+risk_rating%3AHigh+or+risk_rating%3ALow%
29&cursor=eJwVjMFugzAQRH8J262UHhOBoVRrBKwx5pYAReBV5KipTK1-
fOlhDqM3b36Hnj4m8k9z91cjpUfuL2NC3_WdVmA-GDeZWdPjxqltXKlbQ-
Jq4KfqydWJ453w8n9vNrk2sfuynOXHUT8XF9fmzwTlVAF5hIJUk7mAspGzfss0qvKWZq-
fxc5B7CfAkQEuL7AtAYr9NKQLq_AcqjQLKh0F4DuDCOJIorBcFY7Cbu7olh08DpvjA-
poeedsJFLouIru8Osw5FkCRge7_AFwNVDi"
  }
}
```


ThreatQ provides the following default mapping for this feed based on each item within the *.data[]* list.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.name	Vulnerability.Value	Vulnerability	.data[].attributes.last_modification_date	CVE-2025-31324	N/A
.data[].attributes.executive_summary, .data[].attributes.analysis, .data[].attributes.description, .data[].attributes.workarounds[], .data[].attributes.sources[], .data[].attributes.vendor_fix_references[], .data[].attributes.cpes[], .data[].attributes.cvss	Vulnerability.Description	N/A	.data[].attributes.last_modification_date	N/A	User-Configurable. All fields are optional. Fields are concatenated into HTML when enabled.
.data[].attributes.cve_id	Related Vulnerability/ Related Indicator	Vulnerability/ CVE	.data[].attributes.last_modification_date	CVE-2025-31324	N/A
.data[].attributes.risk_rating	Vulnerability.Attribute	Risk Rating	.data[].attributes.last_modification_date	CRITICAL	User-configurable.
.data[].attributes.available_mitigation	Vulnerability.Attribute	Available Mitigation	.data[].attributes.last_modification_date	Intrusion Prevention Signatures	User-configurable.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data[].attributes.cwe.title`	Vulnerability.Attribute	CWE	`.data[].attributes.last_modification_date`	`Improper Authorization`	User-configurable.
`.data[].attributes.exploitation_consequence`	Vulnerability.Attribute	Exploitation Consequence	`.data[].attributes.last_modification_date`	`Code Execution`	User-configurable.
`.data[].attributes.exploitation_state`	Vulnerability.Attribute	Exploitation State	`.data[].attributes.last_modification_date`	`Confirmed`	User-configurable. Updatable.
`.data[].attributes.exploitation_vectors`	Vulnerability.Attribute	Exploitation Vector	`.data[].attributes.last_modification_date`	`Exposed Web Application`	User-configurable.
`.data[].attributes.targeted_industries_tree[].industry_group`	Vulnerability.Attribute	Targeted Industry	`.data[].attributes.last_modification_date`	`Manufacturing`	User-configurable.
`.data[].attributes.mve_id`	Vulnerability.Attribute	MVE ID	`.data[].attributes.last_modification_date`	`MVE-2025-10681`	User-configurable.
`.data[].attributes.tags_details`	Vulnerability.Attribute	Observed in the Wild	`.data[].attributes.last_modification_date`	`false`	User-configurable. Updatable. True if `observed_in_the_wild` exists in `data[].attributes.tags_details[].value`
`.data[].attributes.tags_details`	Vulnerability.Attribute	Has Zero Day	`.data[].attributes.last_modification_date`	`false`	User-configurable. Updatable. True if `was_zero_day` exists in `data[].attributes.tags_details[].value`
`.data[].attributes.tags_details`	Vulnerability.Attribute	Is Predicted	`.data[].attributes.last_modification_date`	`false`	User-configurable. Updatable. True if `is_predicted` exists in `data[].attributes.tags_details[].value`
`.data[].attributes.cpes[].start_cpe.vendor` / `.data[].attributes.cpes[].end_cpe.vendor`	Vulnerability.Attribute	Affected Vendor	`.data[].attributes.last_modification_date`	`SAP`	User-configurable.
`.data[].attributes.cpes[].start_cpe.product` / `.data[].attributes.cpes[].end_cpe.product`	Vulnerability.Attribute	Affected Product	`.data[].attributes.last_modification_date`	`Netweaver`	User-configurable.
`.data[].attributes.cpes[].start_cpe.uri` / `.data[].attributes.cpes[].end_cpe.uri`	Vulnerability.Attribute	Affected Platform	`.data[].attributes.last_modification_date`	`visual_composer_development_server`	User-configurable. The 11th value extracted from the `.data[].attribute`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					`s.cpes[].start_cpe.uri` or `data[].attributes.cpes[].end_cpe.uri` after splitting by `:`
`.data[].attributes.cvss[{cve_version}].base_score/ .data[].attributes.cvss[cvssv4_x].score`	Vulnerability.Attribute	CVSS Base Score	`.data[].attributes.last_modification_date`	`10`	User-configurable. Updatable. Only for CVE vulnerability/ indicator. For `cvssv4_x` the path is: `.data[].attributes.cvss[cvssv4_x].score`
`.data[].attributes.cvss[{cve_version}].temporal_score`	Vulnerability.Attribute	CVSS Temporal Score	`.data[].attributes.last_modification_date`	`9.3`	User-configurable. Updatable. Only for CVE vulnerability/ indicator.
`.data[].attributes.cvss[{cve_version}].vector`	Vulnerability.Attribute	CVSS Vector String	`.data[].attributes.last_modification_date`	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:C`	User-configurable. Only for CVE vulnerability/ indicator.
`.data[].attributes.cvss[cvssv4_x].threat.exploit_maturity`	Vulnerability.Attribute	CVSS Exploit Code Maturity	`.data[].attributes.last_modification_date`	N/A	User-configurable. Updatable. Only for `cvssv4_x` CVSS version. Only for CVE vulnerability/ indicator.

For CVSS attributes, if `data[].attributes.cvss` has more versions, the biggest one will be selected.

Google Threat Intelligence Threat Lists

The Google Threat Intelligence Threat Lists feed will fetch up to 4,000 indicators or compromise for each of the selected Threat Lists.

```
GET {base_url}/api/v3/collections?filter=collection_type:threat_lists
```

Sample Response:


```
{
  "iocs": [
    {
      "data": {
        "type": "ip_address",
        "id": "1.221.254.82",
        "attributes": {
          "gti_assessment": {
            "verdict": {
              "value": "VERDICT_MALICIOUS"
            },
            "threat_score": {
              "value": 80
            },
            "severity": {
              "value": "SEVERITY_HIGH"
            }
          },
          "asn": 3786,
          "as_owner": "lg dacom corporation",
          "continent": "as",
          "country": "kr",
          "last_analysis_stats": {
            "malicious": 13,
            "undetected": 30,
            "harmless": 49
          },
          "last_modification_date": 1769068959,
          "network": "1.220.0.0/15",
          "positives": 13,
          "regional_internet_registry": "apnic"
        },
        "relationships": {
          "malware_families": {
            "data": [
              {
                "id": "malware--f1151a22-9d9c-589d-90ad-1157ea90033e",
                "type": "collection",
                "attributes": {
                  "name": "emotet",
                  "collection_type": "malware-family"
                }
```

```
              },
              {
                "id": "threatfox_win_emotet",
                "type": "collection",
                "attributes": {
                  "name": "emotet",
                  "collection_type": "malware-family"
                }
              }
            ]
          },
          "reports": {
            "data": [
              {
                "id": "report--20-00018831",
                "type": "collection",
                "attributes": {
                  "name": "silentnight observed distributing emotet as a secondary
payload",
                  "collection_type": "report"
                }
              }
            ]
          }
        },
        "context_attributes": {
          "threat_list_id": "ransomware"
        }
      }
    }
  ]
}
```


ThreatQ provides the following default mapping for this feed based on each item within the *.data[]* list.

The following fields are added to the indicator description: `.relationships.campaigns.data[]`, `.relationships.reports.data[]`, `attributes.names` and `.attributes.outgoing_links`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.relationships.threat_actors.data[].attributes.name`	Related Adversary	Adversary	`.data[].attributes.last_modification_date`	N/A	User-configurable.
`.relationships.malware_familie`	Related Malware	Adversary	`.data[].attributes.last_modification_date`	emotet	User-configurable.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
s.data[].attributes.name					
.context_attributes.threat_list_id	Indicator.Attribute	Threat List	.data[].attributes.last_modification_date	Ransomware	User-configurable.
.context_attributes.threat_list_id	Indicator.Attribute	Threat Type	.data[].attributes.last_modification_date	Ransomware	User-configurable. See table Threat Type Mapping
.attributes.last_submission_date	Indicator.Attribute	Last Submission Date	.data[].attributes.last_modification_date	N/A	User-configurable.
.attributes.title	Indicator.Attribute	Site Title	.data[].attributes.last_modification_date	Login Page	User-configurable.
.attributes.last_http_response_code	Indicator.Attribute	Last HTTP Response Code	.data[].attributes.last_modification_date	200	User-configurable.Updatable
.attributes.regional_internet_registry	Indicator.Attribute	RIR	.data[].attributes.last_modification_date	APNIC	User-configurable.
.attributes.as_owner	Indicator.Attribute	AS Organization	.data[].attributes.last_modification_date	MOACK.Co.LTD	User-configurable.
.attributes.asn	Indicator.Attribute	ASN	.data[].attributes.last_modification_date	MOACK.Co.LTD	User-configurable.
.attributes.continent	Indicator.Attribute	Continent Code	N/A	AS	User-configurable.
.attributes.country	Indicator.Attribute	Country Code	N/A	RU	User-configurable.
.attributes.categories[]	Indicator.Attribute	Category	.data[].attributes.last_modification_date	N/A	User-configurable.
.attributes.meaningful_name	Indicator.Attribute	Meaningful Name	.data[].attributes.last_modification_date	Malicious	User-configurable.
.attributes.last_analysis_stats.suspicious	Indicator.Attribute	Suspicious Count	.data[].attributes.last_modification_date	N/A	User-configurable.
.attributes.last_analysis_stats.malicious	Indicator.Attribute	Malicious Count	.data[].attributes.last_modification_date	N/A	User-configurable.
.gti_assessment.threat_score.value	Indicator.Attribute	Threat Score	.data[].attributes.last_modification_date	100	User-configurable.
.gti_assessment.verdict.value	Indicator.Attribute	Verdict	.data[].attributes.last_modification_date	VERDICT_MALICIOUS	User-configurable.
.gti_assessment.severity.value	Indicator.Attribute	Severity	.data[].attributes.last_modification_date	Severity_None	User-configurable.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.gti_assessment.threat_score.value`	Indicator.Attribute	Threat Score	`.data[].attributes.last_modification_date`	100	User-configurable.
`.attributes.tags[] + .attributes.type_tags[]`	Indicator.Attribute	Tag	`.data[].attributes.last_modification_date`	100	User-configurable. Updatable. True if `is_predicted` exists in `data[].attributes.tags_details[].value`
`.id/.attributes.{sha256,sha1,md5} / .attributes.url`	Indicator.Value	Mapped: `.type`	`.data[].attributes.last_modification_date`	1.221.254.82	User-configurable.

Threat List Threat Type Mapping

The following table illustrates how Google Threat Intelligence Threat Types are mapped as ThreatQ Attributes.

GOOGLE THREAT LIST	THREATQ ATTRIBUTE
infostealer	Infostealer
ransomware	Ransomware
cryptominer	Cryptominer
phishing	Phishing
vulnerability-weaponization	Exploit
malicious-network-infrastructure	Malware Infrastructure
mobile	Mobile
iot	IoT

Google Digital Threat Monitoring Alerts

The Google Digital Threat Monitoring Alerts feed ingests alerts for the current organization detected by Google Digital Threat Monitoring.

`GET {base_url}/api/v3/dtm/alerts`

Request Parameters:

```
{
  "since": "2026-01-30T09:00:00Z",
  "until": "2026-01-30T10:00:00Z",
  "sort": "updated_at",
  "order": "asc",
  "monitor_name": "true",
  "sanitize": "true",
  "size": 25,
  "status": "new",
  "alert_type": "Compromised Credentials",
  "severity": "high"
}
```

Sample Response:

```
{
  "alerts": [
    {
      "id": "d5ndloibntts73fgbm00",
      "monitor_id": "d4bkpr65pjos73c72tdg",
      "doc": {
        "__id": "f80291dc-8909-4314-8180-42e9628fca90",
        "__type": "account_discovery",
        "ingested": "2026-01-20T01:30:09Z",
        "service_account": {
          "login": "jlai",
          "password": {
            "plain_text": "*********"
          },
          "profile": {
            "identity": {
              "name": "jlai"
            }
          },
```

```
          "service": {
            "inet_location": {
              "domain": "securonix.com",
              "path": "/resources/downloads",
              "protocol": "https",
              "url": "https://securonix.com/resources/downloads"
            },
            "name": "securonix.com"
          }
        },
        "source": "ccmp",
        "source_file": {
          "filename": "Free_line_181.105.103 kk.rar",
          "hashes": {
            "md5": "ec19f9f79e162891251c59efb69703ce",
            "sha1": "08bca8a925033e7b72a6b186d951d4417fc6a1df",
            "sha256":
"ecd7c2ccf0f4412e9b36b3f66dba5e5c481d810a7ea3ef3c3996ce915e96d2f2"
          },
          "size": 2507772569
        },
        "source_url": "https://t.me/SKYCLOUDULP/204",
        "timestamp": "2025-12-05T03:15:48Z"
      },
      "labels": [
        {
          "id": "7ea8d7fc-2105-4bda-9cfa-cf631afd93a8",
          "classifier": "soup-threat-label",
          "version": "0.1",
          "label": "information-security/information-leak/
credentials",
          "confidence": 100,
          "type": "threat"
        }
      ],
      "topics": [
        {
          "id": "29bc44a7-034c-4f9c-a0e2-e9d6a9f139dc",
          "type": "sha1_hash",
          "value": "08bca8a925033e7b72a6b186d951d4417fc6a1df",
          "extractor": "dtm-ma",
          "extractor_version": "1.0.740",
```

```
          "entity_locations": [
            {
              "element_path": "source_file.hashes.sha1",
              "offsets": [
                0,
                40
              ]
            }
          ]
        },
        {
          "id": "57735fd8-cb1c-4d5b-90a2-0e8a8e72b207",
          "type": "telegram_user_name",
          "value": "FTMixture001",
          "extractor": "dtm-ma",
          "extractor_version": "1.0.761",
          "entity_locations": [
            {
              "element_path": "sender.telegram.name",
              "offsets": [
                0,
                12
              ]
            }
          ]
        },
        {
          "id": "942046d5-cfb6-43f5-b61b-b53a3d2008a5",
          "type": "product",
          "value": "Talkatone",
          "extractor": "analysis-pipeline.nerprocessor-nerenglish-
gpu",
          "extractor_version": "4-0-2",
          "confidence": 88,
          "entity_locations": [
            {
              "element_path": "body",
              "offsets": [
                431,
                440
              ]
            }
```

```
          ]
        },
        {
          "id": "bb7cfc3f-c714-4a99-8d7d-1147cdfd2bc4",
          "type": "identity_name",
          "value": "Verons",
          "extractor": "dtm-ma",
          "extractor_version": "1.0.761",
          "entity_locations": [
            {
              "element_path": "sender.identity.last_name",
              "offsets": [
                0,
                6
              ]
            }
          ]
        }
      ],
      "topic_matches": [
        {
          "topic_id": "doc_type:account_discovery",
          "value": "account_discovery"
        }
      ],
      "label_matches": [],
      "doc_matches": [
        {
          "match_path":
"service_account.service.inet_location.domain",
          "locations": [
            {
              "offsets": [
                0,
                13
              ],
              "value": "securonix.com"
            }
          ]
        }
      ],
      "tags": [],
```

```
      "created_at": "2026-01-20T01:31:14.529Z",
      "updated_at": "2026-01-20T01:31:16.567Z",
      "labels_url": "https://api.intelligence.mandiant.com/v4/dtm/
docs/account_discovery/f80291dc-8909-4314-8180-42e9628fca90/labels",
      "topics_url": "https://api.intelligence.mandiant.com/v4/dtm/
docs/account_discovery/f80291dc-8909-4314-8180-42e9628fca90/topics",
      "doc_url": "https://api.intelligence.mandiant.com/v4/dtm/docs/
account_discovery/f80291dc-8909-4314-8180-42e9628fca90",
      "status": "new",
      "alert_type": "Compromised Credentials",
      "alert_summary": "ccmp",
      "title": "Leaked Web Service Credentials from
\"securonix.com\"",
      "email_sent_at": "",
      "indicator_mscore": 0,
      "severity": "low",
      "confidence": 0.27283120687581575,
      "aggregated_under_id": "d4bm49eghh8s739pl860",
      "monitor_name": "Compromised Credentials",
      "has_analysis": false,
      "meets_password_policy": "policy_unset",
      "severity_reasoning": {
        "rule": ""
      },
      "confidence_reasoning": {
        "version": "",
        "response_count": 0,
        "malicious_count": 0,
        "benign_count": 0,
        "confidence_count": null,
        "explanation": null
      },
      "ignore": false,
      "monitor_version": 1
    }
  ]
}
```


ThreatQ provides the following default mapping for this data based on each item within the `.alerts[]` list.

The following fields are added to the event description: `.alert_summary`, `.ai_doc_summary`, and `.doc_url`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title, .alert_type, .id`	`Event.Value`	`Alert`	`.created_at`	`Leaked Web ... (Compromised Credentials) (Alert ID: d4bm42jp39cc73afrr30)`	Values are concatenated
`.labels[].label`	`Event.Tag`	`N/A`	`N/A`	`information-security/information-leak/credentials`	User-Configurable
`.alert_type`	`Event.Attribute`	`Alert Type`	`.created_at`	`Compromised Credentials`	User-Configurable
`.confidence`	`Event.Attribute`	`Confidence Score`	`.created_at`	`0.27`	User-Configurable. Updatable
`.confidence_reasoning.malicious_count`	`Event.Attribute`	`Malicious Count`	`.created_at`	`0`	User-Configurable. Updatable
`.severity`	`Event.Attribute`	`Severity`	`.created_at`	`Low`	User-Configurable. Updatable. Title-cased.
`.similarity_score`	`Event.Attribute`	`Similarity Score`	`.created_at`	`N/A`	User-Configurable. Updatable
`.status`	`Event.Attribute`	`Status`	`.created_at`	`New`	User-Configurable. Updatable. Title-cased.
`.monitor_name`	`Event.Attribute`	`Monitor`	`.created_at`	`Compromised Credentials`	User-Configurable
`.topics[].{type=organization}.value`	`Event.Attribute`	`Organization`	`.created_at`	`N/A`	User-Configurable
`.topics[].{type=identity_name}.value`	`Event.Attribute`	`Identity`	`.created_at`	`Verons`	User-Configurable
`.topics[].{type=product}.value`	`Event.Attribute`	`Product`	`.created_at`	`Talkatone`	User-Configurable
`.topics[].{type=brand}.value`	`Event.Attribute`	`Brand`	`.created_at`	`N/A`	User-Configurable
`.topics[].{type=city}.value`	`Event.Attribute`	`City`	`.created_at`	`N/A`	User-Configurable
`.topics[].{type=country}.value`	`Event.Attribute`	`Country`	`.created_at`	`N/A`	User-Configurable
`.topics[].{type=}.value`	`Related Indicator.Value`	`See Alert Indicators Type Mapping`	`.created_at`	`08bca8a925033e7b72a6b186d951d4417fc6a1df`	User-Configurable
N/A	`Related Indicator.Attribute`	`Platform`	`N/A`	`Telegram`	Hardcoded attribute for telegram_user_name

Alert Indicators Type Mapping

The following table details how Google Alert Indicator types are mapped into ThreatQ Indicators.

ALERT INDICATOR TYPE	THREAT INDICATOR TYPE
md5_hash	MD5
sha1_hash	SHA-1
sha256_hash	SHA-256
filename	Filename
path	File Path
domain	FQDN
ipv4_address	IP Address
ipv6_address	IPv6 Address
url	URL
email_address	Email Address
telegram_user_name	Username

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.

Google Threat Intelligence

METRIC	RESULT
Run Time	27 minutes
Adversaries	532
Adversary Attributes	7,056
Attack Patterns	263
Malware	4
Malware Attributes	201
Vulnerabilities	298
Vulnerability Attributes	1,132

Google Threat Intelligence Campaigns

METRIC	RESULT
Run Time	2 minutes
Adversaries	98

METRIC	RESULT
Adversary Attributes	104
Attack Patterns	289
Campaigns	121
Campaign Attributes	1,551
Indicators	481
Indicator Attributes	481
Malware	342
Vulnerabilities	41

Google Threat Intelligence Indicators

METRIC	RESULT
Run Time	48 minutes
Adversaries	41
Indicators	159,178
Indicator Attributes	142,805

Google Threat Intelligence Malware

METRIC	RESULT
Run Time	4 minutes
Adversaries	60
Attack Patterns	105
Indicators	3,985
Indicator Attributes	10,619
Malware	41
Malware Attributes	1,336
Vulnerabilities	2

Google Vulnerability Intelligence

METRIC	RESULT
Run Time	1 minute
Indicators	207
Indicator Attributes	4,731
Vulnerabilities	363
Vulnerability Attributes	6,194

Google Threat Intelligence Threat Lists

METRIC	RESULT
Run Time	6 minutes
Indicators	20
Indicator Attributes	92

Google Digital Threat Monitoring Alerts

METRIC	RESULT
Run Time	2 minutes
Event	7
Event Attributes	70
Indicators	120
Indicator Attributes	2

Known Issues / Limitations

- Each feed has optional parameters for retrieving related objects. These parameters were made optional to avoid encountering the daily rate limit. It highly recommended that you use these optional parameters with caution to avoid hitting the daily rate limit.
- The MITRE ATT&CK filter introduced in version 2.2.0 of this integration utilizes an in-memory cache to store all MITRE ATT&CK data. The cache is automatically refreshed every 24 hours to ensure the integration remains synchronized with the latest MITRE ATT&CK content.

Change Log

- **Version 2.2.0**
  - Added a new MITRE ATT&CK filter that streamlines the retrieval and processing of MITRE ATT&CK data by leveraging in-memory caching. The filter automatically refreshes its cache every 24 hours to ensure access to the latest MITRE ATT&CK content while improving performance and reducing data load times.
  - Updated the minimum ThreatQ version to 6.6.0.
- **Version 2.1.1**
  - Added a new feed: **Google Digital Threat Monitoring Alerts.**
- **Version 2.1.0**
  - Added a new feed: **Google Threat Intelligence Threat Lists**.
  - Added support for parsing out IDS (Snort) rules linked to indicators.
  - Performed improvements to pagination to better select a delta from the API for each feed run.
  - Updated integration processes to reduce the number of API calls made during each feed run.
  - Made improvements to description formatting.
  - Resolved a bug that would cause IOC date filtering to not function as expected.
  - Resolved a bug that caused all related IOCs to be re-ingested into ThreatQ on each feed run. Only new/updated indicators related to a given collection will be ingested on each feed run based on the feed run timeframe and minimum threat score threshold.
  - `Industry` attribute for Adversaries & Malware has been renamed to `Target Industry` to better align with the standard data model.
  - `Targeted Industry` attribute has been renamed to Target Industry to better align with the standard data model.
  - Added an Overview section to each feed's configuration to describe what the feed does and what sort of information will be ingested.
  - Added the following new configuration parameters to all feeds:
    - **Origin Filter** - filter the results based on the origin of the intelligence.
    - **Custom API Filter** - an optional custom filter to append to all API requests when fetching collections from the API.

- Added the following new configuration parameters for all feeds excluding Vulnerability Intelligence:
  - **Indicator Description Context Selection** - select the context used to populate each indicator's description.
  - **Ingest ASNs As** - select which entity type to ingest ASNs as in ThreatQ.
- Added the following new configuration parameter for the Threat Intelligence, Campaigns, and Malware feeds:
  - **Supplemental Context Confidence Filter** -
- Added the new options for the **Ingest Related Hash Types**, **Adversaries Context Selection**, and **Indicator Context Selection** parameters for all feeds excluding Vulnerability Intelligence.
- Removed legacy configuration parameter: **Inherit Context from Indicators to Related Hashes**.

- **Version 2.0.0**
  - Rebranded the integration from Mandiant Threat Intelligence CDF to **Google Threat Intelligence CDF**.
  - Migrated the integration feeds from Mandiant to Google Threat Intelligence.
  - Added new parameters to retrieve related objects with a customizable context.
  - Added configuration parameter to filter by industries.
  - Resolved an issue where CVE IDs would not be ingested into ThreatQ when the `Indicators (Type: CVE)` option was selected in the `Ingest CVEs As` field for the **Google Vulnerability Intelligence** (formerly Mandiant Vulnerability Intelligence) feed.

    A note has also been added to this feed to clarify how CVE IDs will be ingested into the platform. You will need to re-enter your configuration and re-enable the feed after upgrading to this version. **Ensure your credentials and other configurations are backed up before upgrading.**
  - Added the ability to ingest the Last Activity Date for Campaigns as an attribute.
  - Performed the following updates and fixes for Google Score & Threat Score mapping:
    - Google Score is no longer used for threshold filtering, in favor of the new "Threat Score" field.

        - Google's new Confidence and Severity fields are now ingested as attributes alongside the threat score.
        - Google's new Verdict field is now ingested as an attribute for indicators.
        - Google's new Category field is now ingested as an attribute for indicators.
    - Added the ability to dynamically set the status of indicators based on the threat score or verdict.
        - Automatically set status to Active if the verdict is malicious.
        - Automatically set status to Whitelisted if the threat score is 0.
    - Added the ability to normalize the Threat Score for indicators into a value range of your choosing.
    - Added the ability to select which pieces of context get brought into ThreatQ with each indicator.
- **Version 1.5.0**
    - Added the following new feeds:
        - Mandiant Threat Intelligence Campaigns
        - Mandiant Threat Intelligence Malware
    - The **Mandiant Threat Intelligence** (actors) feed no longer will fetch attack patterns related to *related malware* as this fetch will be handled by the dedicated **Mandiant Threat Intelligence Malware** feed.
    - Added a new configuration parameter, **Ingest CVEs As**, to the Mandiant Vulnerability Intelligence feed.
    - Performed the following updates regarding Mandiant Score Mapping:
        - Mandiant Score now normalizes to an attribute called `Disposition`. It was previously called `Mandiant Confidence.` Users should adjust their scoring policy to account for this change.
        - Score thresholds are now inclusive (previously exclusive).
        - Added the ability to map to a Disposition of `Suspicious.`
        - Modified the default score thresholds based on Mandiant's recommendations:
            - 0-39: Unknown
            - 40-59: Indeterminate
            - 60-79: Suspicious
            - 80-100: Malicious

        - Indicators are no longer marked as `Benign` if their score does not reach the Indeterminate threshold. Instead, they will be marked as `Unknown`, per Mandiant's recommendations
    - Added TLP mapping Support.
    - Added the ability to have associated hashes (to indicators) inherit attributes from the top-level indicator
    - Added `Category` attribute for indicators based on the reporting sources.
    - Added the ability to ingest MISP flags into the description of each indicator (Indicators feed only).
    - Removed the redundant `Audience Name` attribute from the `Mandiant Threat Intelligence` feed and renamed the `Audience License` attribute to `Audience.`
    - Resolved a pagination issue where the supplemental feed may error out when relationships exceed 10k.
    - Renamed the `Operating System` attribute for Malware to `Target Operation System`
    - The default selection for how CVEs will be ingested is now set to `Vulnerabilities.`
    - The default MScore threshold is now 40 to prevent ingestion of unrated indicators.
    - Added the ability to enable/disable SSL Verification.
    - Added the ability to enable/disable Proxies.
    - Added two new known issues / limitation entries:
        - Users upgrading from an integration version <1.5.0 will have to reconfigure and reenable their feeds upon upgrade to 1.5.0 or later.
        - Disabling the **Only Ingest Recently Updated Entities** configuration parameter for the Mandiant Threat Intelligence Malware feed will result in extremely long run times and may trigger a 500 internal server error from Mandiant.
    - Updated the minimum ThreatQ version to 5.12.1.
- **Version 1.4.0**
    - Updated the minimum ThreatQ version to 5.6.0.
    - The **Mandiant Threat Intelligence Vulnerabilities** feed has been renamed to the **Mandiant Vulnerability Intelligence** feed.
        - The feed can now parse and return more context and details regarding vulnerabilities.

        - Added the following parameters:
            - **Range Type Filter** - select the rating types for vulnerabilities to ingest.
            - **Risk Rating Filter** - select the risk ratings for vulnerabilities to ingest.
            - **Exploitation State Filter** - select the exploitation states for vulnerabilities to ingest.
            - **Exploitation Vector Filter** - select the exploitation vectors for vulnerabilities to ingest.
            - **Vulnerability Must Have a Zero Day** - filter out vulnerabilities that do not have zero days exploits.
            - **Vulnerability Must be Observed in the Wild** - filter out vulnerabilities that have not been observed in the wild.
            - **Vulnerability Must be CISA Known Exploited** - filter out vulnerabilities that are not CISA known exploited.
            - **Vulnerability Must Have Exploits** - filter out vulnerabilities that have no associated exploits.
            - **Vulnerability Attribute Context** - select the context for vulnerabilities to ingest.
            - **Description Context** - select the pieces of context to include in the vulnerability's description.
            - **CVSS Attribute Context** - select the CVSS context for vulnerabilities to ingest.
        - Removed the **Save CVE Data As** parameter from the feed.
    - Added the following parameters to the Intelligence and Indicator Intelligence feeds:
        - **Inherit Attributes from Indicators to Associated Hashes** - adds the ability to inherit attribution from top-level indicators to the associated hashes.
        - **Add MISP Flags to Indicator Descriptions** - adds the ability to ingest the MISP flags into the description of each indicator.
    - Added the **Parsing Entities** parameter field to the Mandiant Threat Intelligence feed.
    - Resolved an issue where the Confidence mapping was not an inclusive threshold.
- **Version 1.3.4**

  - Added a new configuration parameter, **Parsed Entries**, that allows you to select the IOC types to automatically parse from the content.
  - Added ingestion rules for certain attributes.
  - Updated the **Save CVE Data** default setting. The Vulnerabilities option will now be selected by default.
- **Version 1.3.3**
  - Added new configuration option: **Base URL**, that allows you set the Mandiant Base URL for the feeds.
  - New Known Issue / Limitation chapter entry added to the user guide regarding data ranges.
- **Version 1.3.2**
  - Resolved an issue where feed requests would fail with a 400 Bad Request message when the epoch value was empty.
- **Version 1.3.1**
  - Added the following new configuration options for the **Mandiant Threat Intelligence** and **Mandiant Threat Intelligence Indicators** feeds:
    - Mandiant Score Confidence Indeterminate Threshold
    - Mandiant Score Confidence Malicious Threshold
  - Added additional attribute, **Mandiant Classification**, that is derived from the Mandiant Score.
- **Version 1.3.0**
  - Added two new feeds: **Mandiant Threat Intelligence Indicators** and **Mandiant Threat Intelligence Vulnerabilities**.
- **Version 1.2.1**
  - Updated integration authentication method to use **API ID** and **Secret Key** opposed to Username and Password.
- **Version 1.2.0**
  - Added the ability to:
    - Include uncategorized groups as tags.
    - Filter data by recently updated entities.
    - Fetch related attack patterns to the threat actors.
    - Fetch related indicators to the threat actors.
    - Fetch related attack patterns to the related malware.

  - Fixed an issue where the feed attempted to ingest related malware as Indicators

- **Version 1.1.1**
  - Fixed an issue where the integration would attempt to ingest related malware as indicators.
  - Added the following configuration parameters:
    - **Only Ingest Recently Updated Threat Actors -** Adds ability to filter data by recently updated entities.
    - **Add Uncategorized Groups as Tags -** Adds ability to include uncategorized groups as tags.
    - **Fetch Attack Patterns Related to Threat Actors -** Adds ability to fetch related attack patterns to the threat actors.
    - **Fetch Indicators Related to Threat Actors -** Adds ability to fetch related indicators to the threat actors.
    - **Fetch Indicators Related to Malware -** Adds ability to fetch related attack patterns to the related malware.
- **Version 1.1.0**
  - Added X-App-Name as a header.
  - Performed internal refactoring.
- **Version 1.0.0**
  - Initial release