ThreatQuotient

A Securonix Company

Google Threat Intelligence Action

Version 1.0.0

March 03, 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 **7**
Installation **8**
Configuration **9**
Actions **13**
Google Threat Intelligence - Enrich Indicators 14
Endpoint Type Mapping 26
Related Adversaries 27
Related Campaigns 31
Related Malware Families 40
Related Reports 43
Related Vulnerabilities 46
Historical WHOIS 47
Known Issues / Limitations **48**
Change Log **49**

Warning and Disclaimer

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

Support

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

Support Email: 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	1.0.0
Compatible with ThreatQ Versions	>= 5.25.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Google Threat Intelligence Action enables organizations to enrich supported indicators within ThreatQ by retrieving contextual intelligence from Google Threat Intelligence.

The integration provides the following action:

- **Google Threat Intelligence - Enrich Indicators -** enriches submitted indicators and fetches related Google Threat Intelligence context.

The integration is compatible with the following indicator types:

- FQDNs
- IP Address
- IPv6 Address
- MD5
- SHA-1
- SHA-256
- URL

The integration returns the following enriched object types:

- Adversaries
- Campaigns
- Indicators (IP, FQDN - WHOIS context attributes)
- Malware
- Reports

> This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- Google Threat Intelligence base URL.
- Your Google Threat Intelligence API Key.
- A data collection containing at least one of the following indicator objects:
    - FQDNs
    - IP Address
    - IPv6 Address
    - MD5
    - SHA-1
    - SHA-256
    - URL

Installation

Perform the following steps to install the integration:

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

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

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

You will still need to configure the action.

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:

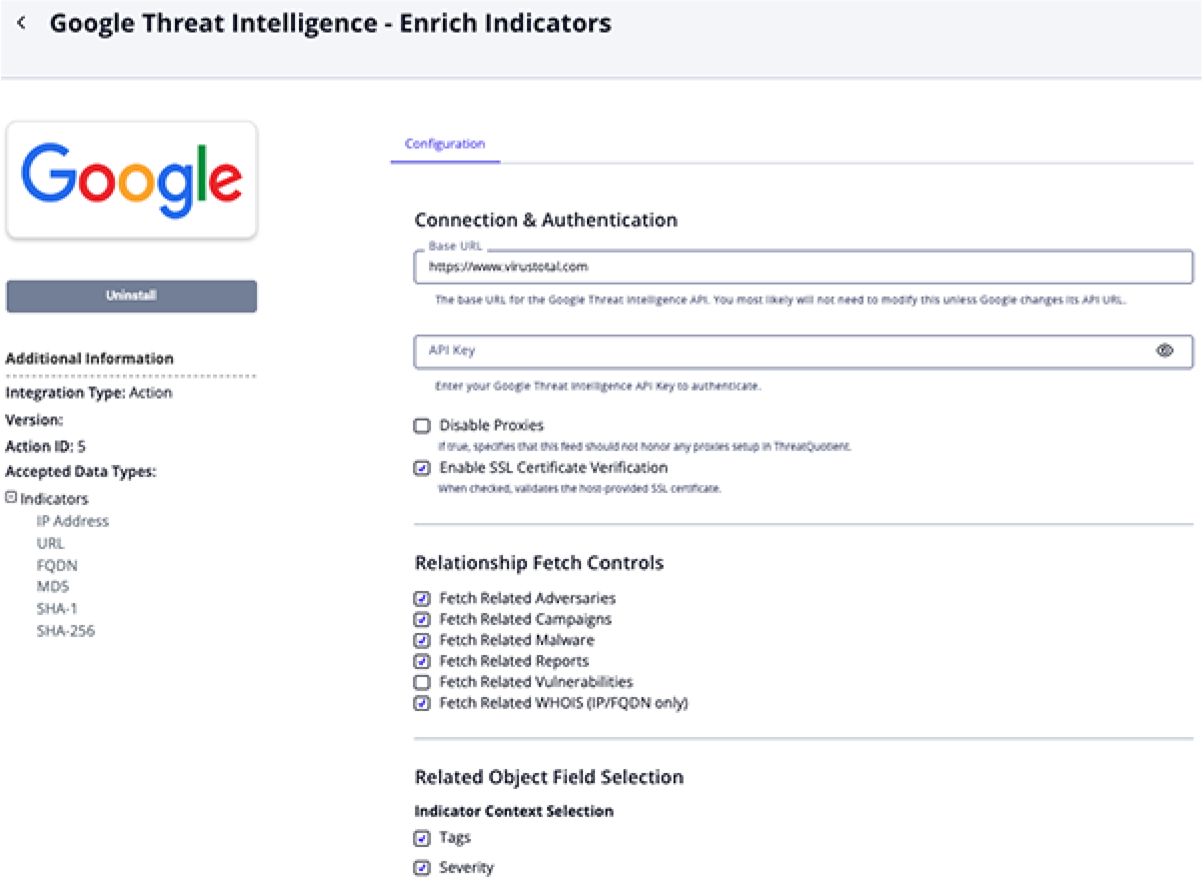
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
Base URL	Enter your Google Threat Intelligence base URL. The default is: `https://www.virustotal.com`
API Key	Enter your API Key used to authenticate with the Google Threat Intelligence API
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Fetch Related Adversaries	Enable this parameter to perform a related adversaries lookup. This is enabled by default.
Fetch Related Campaigns	Enable this parameter to perform a related campaigns lookup. This is enabled by default.

PARAMETER	DESCRIPTION
Fetch Related Malware	Enable this parameter to perform a related malware families lookup. This is enabled by default.
Fetch Related Reports	Enable this parameter to perform a related reports lookup. This is enabled by default.
Fetch Related Vulnerabilities	Enable this parameter to perform a related vulnerabilities lookup. This is disabled by default.
Fetch Related WHOIS (IP/FQDN only)	Enable this parameter to perform a related WHOIS lookup. This is enabled by default.
Ingest CVEs As	Select how to invest CVEs as in ThreatQ. Options include Vulnerabilities or Indicators. The default selection is Vulnerabilities.
Indicator Context Selection	Select the indicator attributes to ingest into ThreatQ. Options include: ◦ Tags *(default)* ◦ Severity *(default)* ◦ Malicious Count *(default)* ◦ Suspicious Count *(default)* ◦ Reputation *(default*) ◦ ASN ◦ AS Organization ◦ Network ◦ Site Title ◦ Last HTTP Response Code ◦ Registrar ◦ Meaningful Name ◦ Last Submission Date ◦ Mandiant Score ◦ Confidence Score ◦ Threat Score ◦ Normalised Threat Score ◦ Verdict ◦ Safe Browsing Verdict ◦ Is Pervasive ◦ Category ◦ RIR ◦ Continent Code ◦ Country Code
Malware Context Selection	Select the malware context into ThreatQ. Options include: ◦ Target Industry *(default)*

PARAMETER	DESCRIPTION
	◦ Target Operating System *(default)* ◦ Detection ◦ Last Seen
Report Context Selection	Select the report context to ingest into ThreatQ. Options include: ◦ Report ID *(default)* ◦ Report Type *(default)* ◦ Report Confidence *(default)* ◦ Author *(default)* ◦ Analyst Comment ◦ Executive Summary ◦ Content ◦ Target Industry
WHOIS Context Selection	Select the WHOIS context to ingest into ThreatQ. Options include: ◦ WHOIS Record ID *(default)* ◦ Registrant Country *(default)* ◦ Registrar Name ◦ First Seen Date ◦ Last Updated
Objects Per Run	Enter the maximum number of objects to process per run.



Google Threat Intelligence - Enrich Indicators

Additional Information

Integration Type: Action

Version:

Action ID: 5

Accepted Data Types:

Indicators

- IP Address
- URL
- FQDN
- MD5
- SHA-1
- SHA-256

Configuration

Connection & Authentication

Base URL: https://www.virustotal.com

The base URL for the Google Threat Intelligence API. You most likely will not need to modify this unless Google changes its API URL.

API Key

Enter your Google Threat Intelligence API Key to authenticate.

☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

☑ Enable SSL Certificate Verification

When checked, validates the host-provided SSL certificate.

Relationship Fetch Controls

☑ Fetch Related Adversaries
☑ Fetch Related Campaigns
☑ Fetch Related Malware
☑ Fetch Related Reports
☐ Fetch Related Vulnerabilities
☑ Fetch Related WHOIS (IP/FQDN only)

Related Object Field Selection

Indicator Context Selection

☑ Tags

☑ Severity

5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Google Threat Intelligence - Enrich Indicators	Enriches indicators and fetches related Google Threat Intelligence context.	Indicator	IP Address, IPv6 Address, URL, FQDN, MD5, SHA-1, SHA-256

Google Threat Intelligence - Enrich Indicators

The Google Threat Intelligence - Enrich Indicators action action enriches ThreatQ indicators using Google Threat Intelligence.

`GET https://www.virustotal.com/api/v3/{indicator_type}/{indicator_value}`

Sample Response:

```
{
    "data": {
        "id": "1.1.1.1",
        "type": "ip_address",
        "links": {
            "self": "https://www.virustotal.com/api/v3/ip_addresses/1.1.1.1"
        },
        "attributes": {
            "as_owner": "Cloudflare, Inc.",
            "tags": [
                "suspicious-udp"
            ],
            "reputation": 80,
            "threat_severity": {
                "version": "I3",
                "threat_severity_level": "SEVERITY_NONE",
                "threat_severity_data": {
                    "has_bad_communicating_files_high": true,
                    "has_bad_communicating_files_medium": true,
                    "belongs_to_bad_collection": true
                },
                "last_analysis_date": "1771375483",
                "level_description": "Severity NONE because it has no detections."
            },
            "last_analysis_results": {},
            "jarm": "27d27d27d00027d00042d43d00041df04c41293ba84f6efe3a613b22f983e6",
            "first_seen_itw_date": 1312949507,
            "last_https_certificate_date": 1771415338,
            "last_seen_itw_date": 1769543593,
            "last_analysis_date": 1771415034,
            "network": "1.1.1.0/24",
            "last_modification_date": 1771416212,
            "last_analysis_stats": {
                "malicious": 0,
                "suspicious": 0,
                "undetected": 31,
                "harmless": 62,
                "timeout": 0
            },
            "rdap": {
                "object_class_name": "ip network",
                "handle": "1.1.1.0 - 1.1.1.255",
                "start_address": "1.1.1.0",
                "end_address": "1.1.1.255",
                "ip_version": "v4",
                "name": "APNIC-LABS",
                "type": "ASSIGNED PORTABLE",
                "country": "AU",
                "status": [
                    "active"
                ],
                "links": [
                    {
                        "href": "https://rdap.apnic.net/ip/1.1.1.0/24",
                        "rel": "self",
                        "type": "application/rdap+json",
                        "value": "https://rdap.apnic.net/ip/1.1.1.1",
                        "title": "",
                        "media": "",
                        "href_lang": []
                    }
                ],
                "notices": [
                    {
                        "title": "Source",
                        "description": [
                            "Objects returned came from source",
                            "APNIC"
                        ],
                        "links": [],
                        "type": ""
                    },
                    {
                        "title": "Terms and Conditions",
                        "description": [
                            "This is the APNIC WHOIS Database query service. The objects are in RDAP format."
                        ],
                        "links": [
                            {
                                "href": "http://www.apnic.net/db/dbcopyright.html",
                                "rel": "terms-of-service",
                                "type": "text/html",
                                "value": "https://rdap.apnic.net/ip/1.1.1.1",
                                "title": "",
                                "media": "",
                                "href_lang": []
                            }
                        ],
                        "type": ""
                    },
                    {
                        "title": "Whois Inaccuracy Reporting",
                        "description": [
                            "If you see inaccuracies in the results, please visit: "
                        ],
                        "links": [
                            {
                                "href": "https://www.apnic.net/manage-ip/using-whois/abuse-and-spamming/invalid-
contact-form",
                                "rel": "inaccuracy-report",
                                "type": "text/html",
                                "value": "https://rdap.apnic.net/ip/1.1.1.1",
                                "title": "",
                                "media": "",
                                "href_lang": []
                            }
                        ],
                        "type": ""
                    }
                ],
                "events": [
                    {
                        "event_action": "registration",
                        "event_date": "2011-08-10T23:12:35Z",
                        "event_actor": "",
                        "links": []
                    },
            {
                "event_action": "last changed",
                "event_date": "2023-04-26T22:57:58Z",
                "event_actor": "",
                "links": []
            }
        ],
        "rdap_conformance": [
            "history_version_0",
            "nro_rdap_profile_0",
            "cidr0",
            "rdap_level_0"
        ],
        "entities": [
            {
                "object_class_name": "entity",
                "handle": "IRT-APNICRANDNET-AU",
                "vcard_array": [
                    {
                        "name": "version",
                        "type": "text",
                        "values": [
                            "4.0"
                        ],
                        "parameters": {}
                    },
                    {
                        "name": "fn",
                        "type": "text",
                        "values": [
                            "IRT-APNICRANDNET-AU"
                        ],
                        "parameters": {}
                    },
                    {
                        "name": "kind",
                        "type": "text",
                        "values": [
                            "group"
                        ],
                        "parameters": {}
                    },
                    {
                        "name": "adr",
                        "parameters": {
                            "label": [
                                "PO Box 3646\nSouth Brisbane, QLD 4101\nAustralia"
                            ]
                        },
                        "type": "text",
                        "values": [
                            "",
                            "",
                            "",
                            "",
                            "",
                            "",
                            ""
                        ]
                    },
                    {
                        "name": "email",
                        "type": "text",
                        "values": [
                                    "helpdesk@apnic.net"
                                ],
                                "parameters": {}
                            },
                            {
                                "name": "email",
                                "parameters": {
                                    "pref": [
                                        "1"
                                    ]
                                },
                                "type": "text",
                                "values": [
                                    "helpdesk@apnic.net"
                                ]
                            }
                        ],
                        "roles": [
                            "abuse"
                        ],
                        "remarks": [
                            {
                                "title": "remarks",
                                "description": [
                                    "helpdesk@apnic.net was validated on 2021-02-09"
                                ],
                                "links": [],
                                "type": ""
                            }
                        ],
                        "links": [
                            {
                                "href": "https://rdap.apnic.net/entity/IRT-APNICRANDNET-AU",
                                "rel": "self",
                                "type": "application/rdap+json",
                                "value": "https://rdap.apnic.net/ip/1.1.1.1",
                                "title": "",
                                "media": "",
                                "href_lang": []
                            }
                        ],
                        "events": [
                            {
                                "event_action": "registration",
                                "event_date": "2011-04-12T17:56:54Z",
                                "event_actor": "",
                                "links": []
                            },
                            {
                                "event_action": "last changed",
                                "event_date": "2025-11-18T00:26:57Z",
                                "event_actor": "",
                                "links": []
                            }
                        ],
                        "public_ids": [],
                        "entities": [],
                        "as_event_actor": [],
                        "status": [],
                        "port43": "",
                        "networks": [],
                        "autnums": [],
                        "url": "",
                        "lang": "",
                        "rdap_conformance": []
                    },
                    {
                        "object_class_name": "entity",
                        "handle": "ORG-ARAD1-AP",
                        "vcard_array": [
                            {
                                "name": "version",
                                "type": "text",
                                "values": [
                                    "4.0"
                                ],
                                "parameters": {}
                            },
                            {
                                "name": "fn",
                                "type": "text",
                                "values": [
                                    "APNIC Research and Development"
                                ],
                                "parameters": {}
                            },
                            {
                                "name": "kind",
                                "type": "text",
                                "values": [
                                    "org"
                                ],
                                "parameters": {}
                            },
                            {
                                "name": "adr",
                                "parameters": {
                                    "label": [
                                        "6 Cordelia St"
                                    ]
                                },
                                "type": "text",
                                "values": [
                                    "",
                                    "",
                                    "",
                                    "",
                                    "",
                                    "",
                                    ""
                                ]
                            },
                            {
                                "name": "tel",
                                "parameters": {
                                    "type": [
                                        "voice"
                                    ]
                                },
                                "type": "text",
                                "values": [
                                    "+61-7-38583100"
                                ]
                            },
                            {
                                "name": "tel",
                                "parameters": {
                                    "type": [
                                        "fax"
                                    ]
                                },
                                "type": "text",
                                "values": [
                                    "+61-7-38583199"
                                ]
                            },
                            {
                                "name": "email",
                                "type": "text",
                                "values": [
                                    "helpdesk@apnic.net"
                                ],
                                "parameters": {}
                            }
                        ],
                        "roles": [
                            "registrant"
                        ],
                        "links": [
                            {
                                "href": "https://rdap.apnic.net/entity/ORG-ARAD1-AP",
                                "rel": "self",
                                "type": "application/rdap+json",
                                "value": "https://rdap.apnic.net/ip/1.1.1.1",
                                "title": "",
                                "media": "",
                                "href_lang": []
                            }
                        ],
                        "events": [
                            {
                                "event_action": "registration",
                                "event_date": "2017-08-08T23:21:55Z",
                                "event_actor": "",
                                "links": []
                            },
                            {
                                "event_action": "last changed",
                                "event_date": "2023-09-05T02:15:19Z",
                                "event_actor": "",
                                "links": []
                            }
                        ],
                        "public_ids": [],
                        "entities": [],
                        "remarks": [],
                        "as_event_actor": [],
                        "status": [],
                        "port43": "",
                        "networks": [],
                        "autnums": [],
                        "url": "",
                        "lang": "",
                        "rdap_conformance": []
                    },
                    {
                        "object_class_name": "entity",
                        "handle": "AIC3-AP",
                        "vcard_array": [
                            {
                                "name": "version",
                                "type": "text",
                                "values": [
                                    "4.0"
                                ],
                                "parameters": {}
                            },
                            {
                                "name": "fn",
                                "type": "text",
                                "values": [
                                    "APNICRANDNET Infrastructure Contact"
                                ],
                                "parameters": {}
                            },
                            {
                                "name": "kind",
                                "type": "text",
                                "values": [
                                    "group"
                                ],
                                "parameters": {}
                            },
                            {
                                "name": "adr",
                                "parameters": {
                                    "label": [
                                        "6 Cordelia St South Brisbane QLD 4101"
                                    ]
                                },
                                "type": "text",
                                "values": [
                                    "",
                                    "",
                                    "",
                                    "",
                                    "",
                                    "",
                                    ""
                                ]
                            },
                            {
                                "name": "tel",
                                "parameters": {
                                    "type": [
                                        "voice"
                                    ]
                                },
                                "type": "text",
                                "values": [
                                    "+61 7 3858 3100"
                                ]
                            },
                            {
                                "name": "email",
                                "type": "text",
                                "values": [
                                    "research@apnic.net"
                                ],
                                "parameters": {}
                            }
                        ],
                        "roles": [
                            "administrative",
                            "technical"
                        ],
                    "links": [
                        {
                            "href": "https://rdap.apnic.net/entity/AIC3-AP",
                            "rel": "self",
                            "type": "application/rdap+json",
                            "value": "https://rdap.apnic.net/ip/1.1.1.1",
                            "title": "",
                            "media": "",
                            "href_lang": []
                        }
                    ],
                    "events": [
                        {
                            "event_action": "registration",
                            "event_date": "2023-04-26T00:42:16Z",
                            "event_actor": "",
                            "links": []
                        },
                        {
                            "event_action": "last changed",
                            "event_date": "2024-07-18T04:37:37Z",
                            "event_actor": "",
                            "links": []
                        }
                    ],
                    "public_ids": [],
                    "entities": [],
                    "remarks": [],
                    "as_event_actor": [],
                    "status": [],
                    "port43": "",
                    "networks": [],
                    "autnums": [],
                    "url": "",
                    "lang": "",
                    "rdap_conformance": []
                }
            ],
            "port43": "whois.apnic.net",
            "cidr0_cidrs": [
                {
                    "v4prefix": "1.1.1.0",
                    "length": 24,
                    "v6prefix": ""
                }
            ],
            "remarks": [
                {
                    "title": "description",
                    "description": [
                        "APNIC and Cloudflare DNS Resolver project",
                        "Routed globally by AS13335/Cloudflare",
                        "Research prefix for APNIC Labs"
                    ],
                    "links": [],
                    "type": ""
                },
                {
                    "title": "remarks",
                    "description": [
                        "---------------",
                        "All Cloudflare abuse reporting can be done via",
                        "resolver-abuse@cloudflare.com",
                        "---------------"
                        ],
                        "links": [],
                        "type": ""
                    }
                ],
                "parent_handle": "",
                "arin_originas0_originautnums": []
            },
            "total_votes": {
                "harmless": 139,
                "malicious": 39
            },
            "whois": "NetRange: 1.0.0.0 - 1.255.255.255\nCIDR: 1.0.0.0/8\nNetName: APNIC-1\nNetHandle:
NET-1-0-0-0-1\nParent: ()\nNetType: Allocated to APNIC\nOriginAS: \nOrganization: Asia Pacific Network Information
Centre (APNIC)\nRegDate: \nUpdated: 2010-07-30\nComment: This IP address range is not registered in the ARIN database.
\nComment: For details, refer to the APNIC Whois Database via\nComment: WHOIS.APNIC.NET or http://wq.apnic.net/apnic-
bin/whois.pl\nComment: ** IMPORTANT NOTE: APNIC is the Regional Internet Registry\nComment: for the Asia Pacific
region. APNIC does not operate networks\nComment: using this IP address range and is not able to investigate\nComment:
spam or abuse reports relating to these addresses. For more\nComment: help, refer to http://www.apnic.net/apnic-info/
whois_search2/abuse-and-spamming\nRef: https://rdap.arin.net/registry/ip/1.0.0.0\nResourceLink: https://
apps.db.ripe.net/db-web-ui/query\nResourceLink: whois.apnic.net\nOrgName: Asia Pacific Network Information
Centre\nOrgId: APNIC\nAddress: PO Box 3646\nCity: South Brisbane\nStateProv: QLD\nPostalCode: 4101\nCountry:
AU\nRegDate: \nUpdated: 2012-01-24\nRef: https://rdap.arin.net/registry/entity/APNIC\nReferralServer: whois://
whois.apnic.net\nResourceLink: http://wq.apnic.net/whois-search/static/search.html\nOrgAbuseHandle: AWC12-
ARIN\nOrgAbuseName: APNIC Whois Contact\nOrgAbusePhone: +61 7 3858 3188 \nOrgAbuseEmail: search-apnic-not-
arin@apnic.net\nOrgAbuseRef: https://rdap.arin.net/registry/entity/AWC12-ARIN\nOrgTechHandle: AWC12-ARIN\nOrgTechName:
APNIC Whois Contact\nOrgTechPhone: +61 7 3858 3188 \nOrgTechEmail: search-apnic-not-arin@apnic.net\nOrgTechRef:
https://rdap.arin.net/registry/entity/AWC12-ARIN\ninetnum: 1.1.1.0 - 1.1.1.255\nnetname: APNIC-LABS\ndescr: APNIC and
Cloudflare DNS Resolver project\ndescr: Routed globally by AS13335/Cloudflare\ndescr: Research prefix for APNIC
Labs\ncountry: AU\norg: ORG-ARAD1-AP\nadmin-c: AIC3-AP\ntech-c: AIC3-AP\nabuse-c: AA1412-AP\nstatus: ASSIGNED
PORTABLE\nremarks: ---------------\nremarks: All Cloudflare abuse reporting can be done via\nremarks: resolver-
abuse@cloudflare.com\nremarks: ---------------\nmnt-by: APNIC-HM\nmnt-routes: MAINT-APNICRANDNET\nmnt-irt: IRT-
APNICRANDNET-AU\nlast-modified: 2023-04-26T22:57:58Z\nmnt-lower: MAINT-APNICRANDNET\nsource: APNIC\nirt: IRT-
APNICRANDNET-AU\naddress: PO Box 3646\naddress: South Brisbane, QLD 4101\naddress: Australia\ne-mail:
helpdesk@apnic.net\nabuse-mailbox: helpdesk@apnic.net\nadmin-c: AR302-AP\ntech-c: AR302-AP\nauth: # Filtered\nremarks:
helpdesk@apnic.net was validated on 2021-02-09\nmnt-by: MAINT-APNICRANDNET\nlast-modified:
2025-11-18T00:26:57Z\nsource: APNIC\norganisation: ORG-ARAD1-AP\norg-name: APNIC Research and Development\norg-type:
LIR\ncountry: AU\naddress: 6 Cordelia St\nphone: +61-7-38583100\nfax-no: +61-7-38583199\ne-mail:
helpdesk@apnic.net\nmnt-ref: APNIC-HM\nmnt-by: APNIC-HM\nlast-modified: 2023-09-05T02:15:19Z\nsource: APNIC\nrole:
ABUSE APNICRANDNETAU\ncountry: ZZ\naddress: PO Box 3646\naddress: South Brisbane, QLD 4101\naddress: Australia\nphone:
+000000000\ne-mail: helpdesk@apnic.net\nadmin-c: AR302-AP\ntech-c: AR302-AP\nnic-hdl: AA1412-AP\nremarks: Generated
from irt object IRT-APNICRANDNET-AU\nremarks: helpdesk@apnic.net was validated on 2021-02-09\nabuse-mailbox:
helpdesk@apnic.net\nmnt-by: APNIC-ABUSE\nlast-modified: 2025-05-28T03:31:35Z\nsource: APNIC\nrole: APNICRANDNET
Infrastructure Contact\naddress: 6 Cordelia St\n South Brisbane\n QLD 4101\ncountry: AU\nphone: +61 7 3858 3100\ne-
mail: research@apnic.net\nadmin-c: AIC3-AP\ntech-c: AIC3-AP\nnic-hdl: AIC3-AP\nmnt-by: MAINT-APNICRANDNET\nlast-
modified: 2024-07-18T04:37:37Z\nsource: APNIC\nroute: 1.1.1.0/24\norigin: AS13335\ndescr: APNIC Research and
Development\n 6 Cordelia St\nmnt-by: MAINT-APNICRANDNET\nlast-modified: 2023-04-26T02:42:44Z\nsource: APNIC\n",
            "whois_date": 1769963594,
            "asn": 13335,
            "last_https_certificate": {
                "cert_signature": {
                    "signature_algorithm": "1.2.840.10045.4.3.3",
                    "signature":
"306402301b2eb53f7f34ee2a79c9dc5e3fe15aeaf3fd0581b24ec6cab641ef5480d4fed03010e89c5a727e41105a889600d7cf0f023012fce5ba4
2cf30d3c2296380704acb379151ea1e24a8c1337752ea4e3bb1e2348d5d6cc2b205639cec499f8ab7323285"
                },
                "extensions": {
                    "CA": false,
                    "authority_key_identifier": {
                        "keyid": "0d74660a5e9fe22cecd5c25d25047f7532baff7d"
                    },
                    "ca_information_access": {
                        "CA Issuers": "http://cert.ssl.com/SSLcom-SubCA-SSL-ECC-384-R2.cer",
                        "OCSP": "http://ocsps.ssl.com"
                    },
                    "subject_alternative_name": [
                        "cloudflare-dns.com",
                        "*.cloudflare-dns.com",
                        "1.0.0.1",
                        "1.1.1.1",
                        "162.159.36.1",
                        "162.159.46.1",
                        "2606:4700:4700::1001",
                        "2606:4700:4700::1111",
                        "2606:4700:4700::64",
                        "2606:4700:4700::6400",
                        "one.one.one.one"
                    ],
                    "certificate_policies": [
                        "2.23.140.1.2.2",
                        "1.3.6.1.4.1.38064.1.3.1.2"
                    ],
                    "extended_key_usage": [
                        "serverAuth"
                    ],
                    "crl_distribution_points": [
                        "http://crls.ssl.com/SSLcom-SubCA-SSL-ECC-384-R2.crl"
                    ],
                    "subject_key_identifier": "2c28ec5420b686002655aa69bbb6c3652e16fa1f",
                    "key_usage": [
                        "digitalSignature"
                    ],
                    "1.3.6.1.4.1.11129.2.4.2": "0482016b0169007600c2317e574519a345ee7f38deb29041ebc7c2215a22bf7f"
                },
                "validity": {
                    "not_after": "2026-12-21 19:20:01",
                    "not_before": "2025-12-31 19:20:01"
                },
                "size": 1413,
                "version": "V3",
                "public_key": {
                    "algorithm": "EC",
                    "ec": {
                        "oid": "secp256r1",
                        "pub":
"3059301306072a8648ce3d020106082a8648ce3d030107034200046383502512ea727819eb3247afc105529c2a2b608a844e756d814847c1c7bec
f85796c12295b50b3ccec50a1949edc4408070c801a93d3bd78117bb6a3c8eaac"
                    }
                },
                "thumbprint_sha256": "e3b02826789d653d224d3edacbe4e877cb7286fc4c922672f6226741ca57ad65",
                "thumbprint": "f88635017260d40b9eb417bee73737911b630e59",
                "serial_number": "4ed03304c46b87a8c2eb5569db9eba0c",
                "issuer": {
                    "C": "US",
                    "ST": "Texas",
                    "L": "Houston",
                    "O": "SSL Corp",
                    "CN": "SSL.com SSL Intermediate CA ECC R2"
                },
                "subject": {
                    "C": "US",
                    "ST": "California",
                    "L": "San Francisco",
                    "O": "Cloudflare, Inc.",
                    "CN": "cloudflare-dns.com"
                }
            }
        }
```

```
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.id / .data.attributes.url / .data.attributes.sha256	Indicator.Value	Type-dependent	N/A	http://malicious-site...	URL uses .attributes.url; files use hash
.data.attributes.threat_severity.threat_severity_level / .data.attributes.gti_assessment.severity.value	Indicator.Attribute	Severity	.data.attributes.last_modification_date	SEVERITY_NONE	Uses only these two paths
.data.attributes.last_analysis_stats.malicious	Indicator.Attribute	Malicious Count	.data.attributes.last_modification_date	9	Optional
.data.attributes.last_analysis_stats.suspicious	Indicator.Attribute	Suspicious Count	.data.attributes.last_modification_date	1	Optional
.data.attributes.reputation	Indicator.Attribute	Reputation	.data.attributes.last_modification_date	0	Optional
.data.attributes.gti_assessment.contributing_factors.mandiant_confidence_score	Indicator.Attribute	Mandiant Score	.data.attributes.last_modification_date	70	Optional
.data.attributes.gti_assessment.contributing_factors.gti_confidence_score	Indicator.Attribute	Confidence Score	.data.attributes.last_modification_date	85	Optional
.data.attributes.gti_assessment.threat_score.value	Indicator.Attribute	Threat Score	.data.attributes.last_modification_date	65	Optional
.data.attributes.gti_assessment.threat_score.value	Indicator.Attribute	Normalised Threat Score	.data.attributes.last_modification_date	Medium	Derived from Threat Score
.data.attributes.gti_assessment.verdict.value	Indicator.Attribute	Verdict	.data.attributes.last_modification_date	malicious	Optional
.data.attributes.gti_assessment.contributing_factors.safebrowsing_verdict	Indicator.Attribute	Safe Browsing Verdict	.data.attributes.last_modification_date	UNSAFE	Optional
.data.attributes.gti_assessment.contributing_factors.pervasive_indicator	Indicator.Attribute	Is Pervasive	.data.attributes.last_modification_date	true	Stored as string
.data.attributes.gti_assessment.contributing_factors.normalised_categories[]	Indicator.Attribute	Category	.data.attributes.last_modification_date	phishing	Joined with comma
.data.attributes.asn	Indicator.Attribute	ASN	.data.attributes.last_modification_date	13335	IP/IPv6 when present

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.attributes.as_owner	Indicator.Attribute	As Organization	.data.attributes.last_modification_date	CLOUDFLARENET	IP/IPv6 when present
.data.attributes.network	Indicator.Attribute	Network	.data.attributes.last_modification_date	1.1.1.0/24	IP/IPv6 when present
.data.attributes.regional_internet_registry	Indicator.Attribute	RIR	.data.attributes.last_modification_date	APNIC	IP/IPv6 when present
.data.attributes.continent	Indicator.Attribute	Continent Code	.data.attributes.last_modification_date	OC	IP/IPv6 when present
.data.attributes.country	Indicator.Attribute	Country Code	.data.attributes.last_modification_date	AU	IP/IPv6 when present
.data.attributes.title	Indicator.Attribute	Site Title	.data.attributes.last_modification_date	malicious-site.com	URL when present
.data.attributes.last_http_response_code	Indicator.Attribute	Last HTTP Response Code	.data.attributes.last_modification_date	200	URL when present
.data.attributes.registrar	Indicator.Attribute	Registrar	.data.attributes.last_modification_date	Namecheap, Inc.	Domain when present
.data.attributes.meaningful_name	Indicator.Attribute	Meaningful Name	.data.attributes.last_modification_date	payload.exe	File when present
.data.attributes.md5	Related Indicator.Value	MD5	.data.attributes.last_modification_date	2c397d151a6137a2a9be6455d143d165	Related file hash indicator
.data.attributes.sha1	Related Indicator.Value	SHA-1	.data.attributes.last_modification_date	63d796f57f7e72ac85766034320ef01863f4a22e	Related file hash indicator
.data.attributes.sha256	Related Indicator.Value	SHA-256	.data.attributes.last_modification_date	b2ce307dfe65c188fdae169abd65b75b112522c4aqataya22e	Related file hash indicator
.data.attributes.last_submission_date	Indicator.Attribute	Last Submission Date	.data.attributes.last_modification_date	1770805401	URL/File when present
.data.attributes.tags[]	Indicator.Tag	N/A	N/A	phishing	Optional
.data.attributes.last_modification_date	Indicator.Published	N/A	.data.attributes.last_modification_date	1770805401	Timestamp

Endpoint Type Mapping

The integration will utilize Google Threat Intelligence endpoints based on the indicator type submitted for enrichment.

INDICATOR TYPE	ENDPOINT
IP Address	`ip_addresses/{value}`
IPv6 Address	`ip_addresses/{value}`
FQDN	`domains/{value}`
URL	`urls/{url_id}`
MD5, SHA-1, SHA-256	`files/{hash}`

Related Adversaries

`GET https://www.virustotal.com/api/v3/{indicator_type}/{indicator_value}/threat_actors`

Sample Response:

```
{
    "data": [
        {
            "id": "threat-actor--ae523f9a-6d22-5509-842e-127e639fb00f",
            "type": "collection",
            "links": {
                "self": "https://www.virustotal.com/api/v3/collections/threat-actor--
ae523f9a-6d22-5509-842e-127e639fb00f"
            },
            "attributes": {
                "creation_date": 1594224464,
                "first_seen": 1413158400,
                "top_icon_md5": [
                    "07c6642a9643a9354e183abdc66217a7",
                    "28bc6874df78fadd1f3bac95d82861ad",
                    "bf45249eb24fee9581e586258264704d"
                ],
                "capabilities": [],
                "description": "Temp.Traveler is an intrusion set that primarily targets the hospitality sector
globally and entities in U.S.-based education and local government sectors. TEMP.Traveler campaigns have consistently
targeted entities in these three industries, used similar social engineering tactics, reused the same infrastructure,
and relied on a customized configuration of the NetWire remote access Trojan (RAT). The ultimate motivations behind
TEMP.Traveler activity are unclear. We have some indication that the group is financially motivated, but it also may
have political or other motivations. TEMP.Traveler campaigns have been active since October 2014 and continued through
at least March 2017. We have not yet identified any confirmed TEMP.Traveler activity later in 2017, likely due to the
group shifting to unidentified tactics or temporarily pausing operations.",
                "targeted_regions_hierarchy": [
                    {
                        "region": "Americas",
                        "sub_region": "Northern America",
                        "country": "United States",
                        "country_iso2": "US",
                        "confidence": "confirmed",
                        "first_seen": 1413158400,
                        "last_seen": 1413158400,
                        "description": null,
                        "source": null
                    }
                ],
                "tags_details": [],
                "files_count": 38,
                "domains_count": 12,
                "motivations": [
                    {
                        "first_seen": null,
                        "last_seen": null,
                        "confidence": "confirmed",
                        "description": null,
                        "value": "Financial Gain"
                    }
                ],
                "collection_type": "threat-actor",
                "operating_systems": [],
                "source_regions_hierarchy": [],
                "private": true,
                "last_modification_date": 1755561600,
                "alt_names_details": [
                    {
                        "first_seen": null,
                        "last_seen": null,
                        "confidence": "confirmed",
                        "description": null,
                        "value": "TEMP.Traveler"
                    }
                ],
                "targeted_industries": [],
                "origin": "Google Threat Intelligence",
                "autogenerated_tags": [
                    "upx",
                    "attachment",
                    "contains-pe"
                ],
                "recent_activity_relative_change": 0.5451230628988148,
                "urls_count": 2,
                "counters": {
                    "files": 38,
                    "domains": 12,
                    "ip_addresses": 16,
                    "urls": 2,
                    "iocs": 68,
                    "subscribers": 4,
                    "attack_techniques": 42
                },
                "last_seen_details": [
                    {
                        "first_seen": null,
                        "last_seen": null,
                        "confidence": "confirmed",
                        "description": null,
                        "value": "2018-04-30T14:38:28Z"
                    }
                ],
                "ip_addresses_count": 16,
                "first_seen_details": [
                    {
                        "first_seen": null,
                        "last_seen": null,
                        "confidence": "confirmed",
                        "description": null,
                        "value": "2014-10-13T00:00:00Z"
                    }
                ],
                "targeted_regions": [
                    "US"
                ],
                "last_seen": 1525099108,
                "alt_names": [
                    "TEMP.Traveler"
                ],
                "collection_links": [],
                "merged_actors": [],
                "name": "TEMP.Traveler",
                "references_count": 107,
                "status": "COMPUTED",
                "subscribers_count": 4,
                "tags": [],
                "detection_names": [],
                "recent_activity_summary": [
                    777,
                    1239,
                    964,
                    772,
                    627,
                    316,
                    402,
                    761,
                    626,
                    505,
                    495,
                    454,
                    263,
                    274
                ],
                "summary_stats": {
                    "first_submission_date": {
                        "min": 1413216169.0,
                        "max": 1541443681.0,
                        "avg": 1466045340.025
                    },
                    "last_submission_date": {
                        "min": 1416968037.0,
                        "max": 1684220392.0,
                        "avg": 1495129889.25
                    },
                    "files_detections": {
                        "min": 0.0,
                        "max": 60.0,
                        "avg": 37.84210526315789
                    },
                    "urls_detections": {
                        "min": 1.0,
                        "max": 7.0,
                        "avg": 4.0
                    }
                },
                "malware_roles": [],
                "targeted_industries_tree": [],
                "aggregations": {
                }
            },
            "context_attributes": {
                "shared_with_me": false,
                "role": "viewer"
            }
        }
    ],
    "meta": {
        "count": 1
    },
    "links": {
        "self": "https://www.virustotal.com/api/v3/ip_addresses/127.0.0.1/threat_actors?limit=10"
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
`.data[].attributes.name`	Related Adversary.Value	Adversary	`UNC5840`	Core value
`.data[].attributes.description`	Related Adversary.Description	N/A	`...`	Optional
`.data[].attributes.last_modification_date`	Related Adversary.Published	N/A	`1765152000`	Timestamp

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
`.data[].attributes.alt_names_details[].value`	Related Adversary.Tag	N/A	`MuddyWater`	Only when aliases are selected

Related Campaigns

`GET https://www.virustotal.com/api/v3/{indicator_type}/{indicator_value}/campaigns`

Sample Response:

```
{
    "data": [
        {
            "id": "campaign--ea7f04c4-e2c3-59f7-996c-c82c219fe4ad",
            "type": "collection",
            "links": {
                "self": "https://www.virustotal.com/api/v3/collections/campaign--ea7f04c4-e2c3-59f7-996c-c82c219fe4ad"
            },
            "attributes": {
                "source_regions_hierarchy": [],
                "merged_actors": [],
                "alt_names": [
                    "CAMP.24.066"
                ],
                "domains_count": 9,
                "counters": {
                    "files": 45,
                    "domains": 9,
                    "ip_addresses": 12,
                    "urls": 29,
                    "iocs": 95,
                    "subscribers": 10,
                    "attack_techniques": 64
                },
                "malware_roles": [],
                "recent_activity_summary": [
                    41,
                    110,
                    31,
                    24,
                    41,
                    32,
                    21,
                    29,
                    27,
                    36,
                    32,
                    43,
                    21,
                    12
                ],
                "creation_date": 1729803514,
                "collection_links": [],
                "files_count": 45,
                "first_seen_details": [
                    {
                        "confidence": "unconfirmed",
                        "last_seen": null,
                        "value": "2024-01-01T00:00:00Z",
                        "description": "Mandiant Observed First Activity of Campaign",
                        "first_seen": null
                    }
                ],
                "urls_count": 29,
                "campaign_type": "INDIVIDUAL",
                "last_seen_details": [
                    {
                        "confidence": "unconfirmed",
                        "last_seen": null,
                        "value": "2025-12-08T00:00:00Z",
                        "description": null,
                        "first_seen": null
                    }
                ],
                "name": "Financially Motivated Threat Actor Distributing DIRTYBULK via Infected USB Devices",
                "targeted_regions": [
                    "DK",
                    "FR",
                    "PH",
                    "PK",
                    "GB",
                    "US",
                    "HK",
                    "IE",
                    "SA",
                    "CH",
                    "CZ",
                    "EG",
                    "AT",
                    "TR",
                    "AU",
                    "SG",
                    "DE"
                ],
                "top_icon_md5": [
                    "b8fabacf5f0ce868656ac7a1d38c7c99",
                    "b1e821199001f8d20b1ff93d4d6b3d40",
                    "81addaa406504038756c8f1613668203"
                ],
                "references_count": 6,
                "collection_type": "campaign",
                "last_modification_date": 1769040000,
                "ip_addresses_count": 12,
                "autogenerated_tags": [
                    "base64-embedded",
                    "contains-pe",
                    "downloads-pe"
                ],
                "alt_names_details": [
                    {
                        "confidence": "confirmed",
                        "last_seen": null,
                        "value": "CAMP.24.066",
                        "description": null,
                        "first_seen": null
                    }
                ],
                "private": true,
                "capabilities": [],
                "recent_activity_relative_change": 0.1389521640091116,
                "status": "COMPUTED",
                "summary_stats": {
                    "first_submission_date": {
                        "min": 1697750370.0,
                        "max": 1760519405.0,
                        "avg": 1731004213.4729729
                    },
                    "last_submission_date": {
                        "min": 1719954046.0,
                        "max": 1771348484.0,
                        "avg": 1750017725.1216216
                    },
                    "files_detections": {
                        "min": 0.0,
                        "max": 60.0,
                        "avg": 44.82222222222223
                    },
                    "urls_detections": {
                        "min": 0.0,
                        "max": 13.0,
                        "avg": 6.206896551724137
                    }
                },
                "subscribers_count": 10,
                "motivations": [
                    {
                        "confidence": "confirmed",
                        "last_seen": null,
                        "value": "Financial Gain",
                        "description": null,
                        "first_seen": null
                    }
                ],
                "targeted_industries": [],
                "detection_names": [],
                "tags_details": [],
                "targeted_industries_tree": [
                    {
                        "industry_group": "Automotive",
                        "industry": null,
                        "confidence": "confirmed",
                        "first_seen": null,
                        "last_seen": null,
                        "description": null,
                        "source": null
                    },
                    {
                        "industry_group": "Chemicals  Materials",
                        "industry": null,
                        "confidence": "confirmed",
                        "first_seen": null,
                        "last_seen": null,
                        "description": null,
                        "source": null
                    },
                    {
                        "industry_group": "Construction  Engineering",
                        "industry": null,
                        "confidence": "confirmed",
                        "first_seen": null,
                        "last_seen": null,
                        "description": null,
                        "source": null
                    },
                    {
                        "industry_group": "Education",
                        "industry": null,
                        "confidence": "confirmed",
                        "first_seen": null,
                        "last_seen": null,
                        "description": null,
                        "source": null
                    },
                    {
                        "industry_group": "Energy  Utilities",
                    "industry": null,
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "industry_group": "Financial Services",
                    "industry": null,
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "industry_group": "Government",
                    "industry": null,
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "industry_group": "Healthcare",
                    "industry": null,
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "industry_group": "Hospitality",
                    "industry": null,
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "industry_group": "Legal  Professional Services",
                    "industry": null,
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "industry_group": "Manufacturing",
                    "industry": null,
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "industry_group": "Media  Entertainment",
                    "industry": null,
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "industry_group": "Oil Gas",
                    "industry": null,
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "industry_group": "Pharmaceuticals",
                    "industry": null,
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "industry_group": "Retail",
                    "industry": null,
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "industry_group": "Technology",
                    "industry": null,
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "industry_group": "Telecommunications",
                    "industry": null,
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "industry_group": "Transportation",
                    "industry": null,
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                }
            ],
            "targeted_regions_hierarchy": [
                {
                    "region": "Oceania",
                        "sub_region": "Australia and New Zealand",
                        "country": "Australia",
                        "country_iso2": "AU",
                        "confidence": "confirmed",
                        "first_seen": null,
                        "last_seen": null,
                        "description": null,
                        "source": null
                    },
                    {
                        "region": "Europe",
                        "sub_region": "Western Europe",
                        "country": "Austria",
                        "country_iso2": "AT",
                        "confidence": "confirmed",
                        "first_seen": null,
                        "last_seen": null,
                        "description": null,
                        "source": null
                    },
                    {
                        "region": "Europe",
                        "sub_region": "Eastern Europe",
                        "country": "Czech Republic",
                        "country_iso2": "CZ",
                        "confidence": "confirmed",
                        "first_seen": null,
                        "last_seen": null,
                        "description": null,
                        "source": null
                    },
                    {
                        "region": "Europe",
                        "sub_region": "Northern Europe",
                        "country": "Denmark",
                        "country_iso2": "DK",
                        "confidence": "confirmed",
                        "first_seen": null,
                        "last_seen": null,
                        "description": null,
                        "source": null
                    },
                    {
                        "region": "Africa",
                        "sub_region": "Northern Africa",
                        "country": "Egypt",
                        "country_iso2": "EG",
                        "confidence": "confirmed",
                        "first_seen": null,
                        "last_seen": null,
                        "description": null,
                        "source": null
                    },
                    {
                        "region": "Europe",
                        "sub_region": "Western Europe",
                        "country": "France",
                        "country_iso2": "FR",
                        "confidence": "confirmed",
                        "first_seen": null,
                        "last_seen": null,
                        "description": null,
                        "source": null
                    },
                {
                    "region": "Europe",
                    "sub_region": "Western Europe",
                    "country": "Germany",
                    "country_iso2": "DE",
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "region": "Asia",
                    "sub_region": "Eastern Asia",
                    "country": "Hong Kong",
                    "country_iso2": "HK",
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "region": "Europe",
                    "sub_region": "Northern Europe",
                    "country": "Ireland",
                    "country_iso2": "IE",
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "region": "Asia",
                    "sub_region": "Southern Asia",
                    "country": "Pakistan",
                    "country_iso2": "PK",
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "region": "Asia",
                    "sub_region": "South-eastern Asia",
                    "country": "Philippines",
                    "country_iso2": "PH",
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                    "source": null
                },
                {
                    "region": "Asia",
                    "sub_region": "Western Asia",
                    "country": "Saudi Arabia",
                    "country_iso2": "SA",
                    "confidence": "confirmed",
                    "first_seen": null,
                    "last_seen": null,
                    "description": null,
                        "source": null
                    },
                    {
                        "region": "Asia",
                        "sub_region": "South-eastern Asia",
                        "country": "Singapore",
                        "country_iso2": "SG",
                        "confidence": "confirmed",
                        "first_seen": null,
                        "last_seen": null,
                        "description": null,
                        "source": null
                    },
                    {
                        "region": "Europe",
                        "sub_region": "Western Europe",
                        "country": "Switzerland",
                        "country_iso2": "CH",
                        "confidence": "confirmed",
                        "first_seen": null,
                        "last_seen": null,
                        "description": null,
                        "source": null
                    },
                    {
                        "region": "Asia",
                        "sub_region": "Western Asia",
                        "country": "Turkey",
                        "country_iso2": "TR",
                        "confidence": "confirmed",
                        "first_seen": null,
                        "last_seen": null,
                        "description": null,
                        "source": null
                    },
                    {
                        "region": "Europe",
                        "sub_region": "Northern Europe",
                        "country": "United Kingdom",
                        "country_iso2": "GB",
                        "confidence": "confirmed",
                        "first_seen": null,
                        "last_seen": null,
                        "description": null,
                        "source": null
                    },
                    {
                        "region": "Americas",
                        "sub_region": "Northern America",
                        "country": "United States",
                        "country_iso2": "US",
                        "confidence": "confirmed",
                        "first_seen": null,
                        "last_seen": null,
                        "description": null,
                        "source": null
                    }
                ],
                "first_seen": 1704067200,
                "tags": [],
                "description": "Beginning in September 2024, Mandiant has collected intelligence surrounding a
campaign involving widespread use of infected USB devices leading to the distribution of DIRTYBULK Dropper. Based on
available intelligence, affected organizations have been located in North America and Europe within the Construction
Engineering and Healthcare industries. The campaign is being conducted by a threat actor Mandiant tracks as UNC5840
```

```
and assesses with high confidence to have Financial motivations. The multi-stage DIRTYBULK dropper ultimately led to
installation of PUMPBENCH backdoor and XMRIG cryptominer software.",
                "operating_systems": [],
                "last_seen": 1765152000,
                "origin": "Google Threat Intelligence",
                "aggregations": {
                }
            },
            "context_attributes": {
                "shared_with_me": false,
                "role": "viewer"
            }
        }
    ],
    "meta": {
        "count": 1
    },
    "links": {
        "self": "https://www.virustotal.com/api/v3/domains/unvmainx.com/campaigns?limit=10"
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
`.data[].attributes.name`	`Related Campaign.Value`	`Campaign`	`UNC5840 USB`	`Core value`
`.data[].attributes.description`	`Related Campaign.Description`	`N/A`	`...`	`Optional`
`.data[].attributes.last_modification_date`	`Related Campaign.Published`	`N/A`	`1765152000`	`Timestamp`

Related Malware Families

`GET https://www.virustotal.com/api/v3/{indicator_type}/{indicator_value}/malware_families`

Sample Response:

```
{
    "data": [
        {
            "id": "analysis_virustotal_zenbox_ursnif",
            "type": "collection",
            "links": {
                "self": "https://www.virustotal.com/api/v3/collections/analysis_virustotal_zenbox_ursnif"
            },
            "attributes": {
                "collection_type": "malware-family",
                "targeted_industries": [],
                "operating_systems": [],
                "source_regions_hierarchy": [],
                "description": "Autogenerated malware family ursnif from detections by virustotal_zenbox",
                "recent_activity_summary": [
                    2158,
                    3885,
                    2981,
                    2657,
                    3094,
                    1652,
                    1537,
                    3342,
                    3199,
                    3244,
                    3406,
                    2864,
                    1248,
                    1487
                ],
                "merged_actors": [],
                "targeted_regions": [],
                "files_count": 1345,
                "collection_links": [],
                "ip_addresses_count": 284,
                "targeted_regions_hierarchy": [],
                "domains_count": 1055,
                "first_seen_details": [],
                "status": "COMPUTED",
                "tags_details": [
                    {
                        "last_seen": null,
                        "value": "autogenerated",
                        "confidence": "possible",
                        "description": null,
                        "first_seen": null
                    }
                ],
                "counters": {
                    "files": 1345,
                    "domains": 1055,
                    "ip_addresses": 284,
                    "urls": 148,
                    "iocs": 2832,
                    "subscribers": 0,
                    "attack_techniques": 0
                },
                "references_count": 566,
                "top_icon_md5": [
                    "d188945a3ceee1e90cae0a449ad41e5b",
                    "0ed2d599387e7d68b8489a95daf8db81",
                    "b54f34953ff8c66c225c9b6a6da1d24f"
                ],
                "malware_roles": [],
                "creation_date": 1719435980,
                "tags": [
                    "autogenerated"
                ],
                "targeted_industries_tree": [],
                "urls_count": 148,
                "last_seen_details": [],
                "name": "ursnif",
                "summary_stats": {
                    "first_submission_date": {
                        "min": 1276511498.0,
                        "max": 1762917559.0,
                        "avg": 1653199690.7756195
                    },
                    "last_submission_date": {
                        "min": 1479059163.0,
                        "max": 1771336745.0,
                        "avg": 1692793915.8278635
                    },
                    "files_detections": {
                        "min": 0.0,
                        "max": 71.0,
                        "avg": 53.54126394052043
                    },
                    "urls_detections": {
                        "min": 0.0,
                        "max": 14.0,
                        "avg": 4.445945945945943
                    }
                },
                "autogenerated_tags": [
                    "cve-2016-2569",
                    "base64-embedded",
                    "cve-2018-8440",
                    "contains-pe",
                    "nsis",
                    "opendir"
                ],
                "private": true,
                "last_modification_date": 1724199865,
                "origin": "Partner",
                "motivations": [],
                "alt_names": [
                    "ursnifv3",
                    "ursnif"
                ],
                "alt_names_details": [
                    {
                        "last_seen": null,
                        "value": "ursnifv3",
                        "confidence": "possible",
                        "description": null,
                        "first_seen": null
                    },
                    {
                        "last_seen": null,
                        "value": "ursnif",
                        "confidence": "possible",
                        "description": null,
                        "first_seen": null
                    }
                ],
                "recent_activity_relative_change": 0.08903967524963696,
                "subscribers_count": 0,
                "detection_names": [],
                "capabilities": [],
                "aggregations": {}
            },
            "context_attributes": {
                "shared_with_me": false,
                "role": "viewer"
            }
        }
    ],
    "meta": {
        "count": 1
    },
    "links": {
        "self": "https://www.virustotal.com/api/v3/urls/
cf4b367e49bf0b22041c6f065f4aa19f3cfe39c8d5abc0617343d1a66c6a26f5/malware_families?limit=10"
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
`.data[].attributes.name`	Related Malware.Value	Malware	`ursnif`	Core value
`.data[].attributes.description`	Related Malware.Description	N/A	`...`	Optional
`.data[].attributes.last_modification_date`	Related Malware.Published	N/A	`1724199865`	Timestamp
`.data[].attributes.operating_systems[].value`	Related Malware.Attribute	Operating System	`Windows`	When `operating_system` is selected
`.data[].attributes.detection_names[].value`	Related Malware.Attribute	Detection	`Trojan.*`	When `detection` is selected
`.data[].attributes.last_seen`	Related Malware.Attribute	Last Seen	`1765152000`	When `last_seen` is selected

Related Reports

`GET https://www.virustotal.com/api/v3/{indicator_type}/{indicator_value}/reports`

Sample Response:

```
{
    "data": [
        {
            "id": "report--14-00000096",
            "type": "collection",
            "links": {
                "self": "https://www.virustotal.com/api/v3/collections/report--14-00000096"
            },
            "attributes": {
                "analyst_comment": "",
                "detection_names": [],
                "threat_scape": [
                    "Cyber Crime"
                ],
                "counters": {
                    "files": 0,
                    "domains": 1,
                    "ip_addresses": 1,
                    "urls": 0,
                    "iocs": 2,
                    "subscribers": 0,
                    "attack_techniques": 0
                },
                "references_count": 191,
                "merged_actors": [],
                "autogenerated_tags": [],
                "top_icon_md5": [],
                "subscribers_count": 0,
                "tags_details": [],
                "domains_count": 1,
                "targeted_informations": [],
                "alt_names_details": [],
                "author": "",
                "report_confidence": "",
                "targeted_industries_tree": [],
                "recent_activity_summary": [
                    333,
                    336,
                    348,
                    274,
                    263,
                    149,
                    156,
                    303,
                    266,
                    254,
                    301,
                    272,
                    121,
                    128
                ],
                "technologies": [],
                "collection_links": [],
                "last_seen_details": [],
                "version": 1,
                "targeted_regions_hierarchy": [],
                "report_type": "Threat Intelligence",
                "collection_type": "report",
                "alt_names": [],
                "status": "COMPUTED",
                "mitigations": [],
                "malware_roles": [],
                "intended_effects": [],
                "report_id": "14-00000096",
                "operating_systems": [],
                "creation_date": 1418310907,
                "tmh_accuracy_ranking": "",
                "last_modification_date": 1418310907,
                "capabilities": [],
                "affected_systems": [],
                "tags": [],
                "origin": "Google Threat Intelligence",
                "recent_activity_relative_change": 0.06894447834045159,
                "source_regions_hierarchy": [],
                "files_count": 0,
                "is_content_translated": false,
                "targeted_industries": [],
                "first_seen_details": [],
                "urls_count": 0,
                "private": true,
                "ip_addresses_count": 1,
                "targeted_regions": [],
                "name": "testItrax1.2",
                "motivations": [],
                "aggregations": {}
            },
            "context_attributes": {
                "shared_with_me": false,
                "role": "viewer"
            }
        }
    ],
    "meta": {
        "count": 321,
        "cursor": "eyJsaW1pdCI6IDEwLCAib2Zmc2V0IjogMTB9"
    },
    "links": {
        "self": "https://www.virustotal.com/api/v3/ip_addresses/1.1.1.1/reports?limit=10",
        "next": "https://www.virustotal.com/api/v3/ip_addresses/1.1.1.1/reports?
limit=10cursor=eyJsaW1pdCI6IDEwLCAib2Zmc2V0IjogMTB9"
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
`.data[].attributes.name`	Related Report.Title	Report	`testItrax1.2`	Ingested as `report-sets`
`.data[].attributes.executive_summary` / `.content` / `.analyst_comment`	Related Report.Description	N/A	`...`	First non-empty value
`.data[].attributes.creation_date`	Related Report.Happened At	N/A	`1418310907`	Timestamp
`.data[].attributes.last_modification_date`	Related Report.Published	N/A	`1418310907`	Timestamp
`.data[].attributes.report_id` / `.data[].id`	Related Report.Attribute	Report ID	`14-00000096`	When `report_id` is selected

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
`.data[].attributes.report_type`	Related Report.Attribute	Report Type	`Threat Intelligence`	When `report_type` is selected
`.data[].attributes.author`	Related Report.Attribute	Author	`Google Threat Intelligence`	When `author` is selected
`.data[].attributes.analyst_comment`	Related Report.Attribute	Analyst Comment	`...`	When `analyst_comment` is selected
`.data[].attributes.executive_summary`	Related Report.Attribute	Executive Summary	`...`	When `executive_summary` is selected
`.data[].attributes.content`	Related Report.Attribute	Content	`...`	When `content` is selected
`.data[].attributes.targeted_industries[]`	Related Report.Attribute	Target Industry	`IT`	When `target_industry` is selected and present

Related Vulnerabilities

`GET https://www.virustotal.com/api/v3/{indicator_type}/{indicator_value}/malware_families`

`GET https://www.virustotal.com/api/v3/{indicator_type}/{indicator_value}/reports`

> CVE Source: `.data[].attributes.autogenerated_tags[]` entries starting with `cve-`.

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NOTES
`.data[].attributes.autogenerated_tags[]` (`cve-...`) from malware/reports	Related Vulnerability.Value or Related Indicator.Value	Vulnerability or CVE Indicator	Controlled by `Ingest CVEs As` selection

> Vulnerability context fields from `/vulnerabilities` are not currently mapped in this implementation of the integration.

Historical WHOIS

This mapping is for IP Addresses and FQDN types only.

`GET https://www.virustotal.com/api/v3/{indicator_type}/{indicator_value}/historical_whois`

Sample Response:

```
{
    "data": [
        {
            "id": "1b5bc06c95a5e14df338e124a0c518603d34a97608d3db0474b22b36ee632b81",
            "type": "whois",
            "links": {
                "self": "https://www.virustotal.com/api/v3/whois/
1b5bc06c95a5e14df338e124a0c518603d34a97608d3db0474b22b36ee632b81"
            },
            "attributes": {
                "whois_map": {},
                "first_seen_date": 1730083431,
                "registrant_country": "AU",
                "last_updated": 1730069320
            }
        }
    ],
    "meta": {
        "count": 12,
        "cursor": "CoQBChwKD2ZpcnN0X3NlZW5fZGF0ZRIJCPTngZTlmu8CEmBqEXN-
dmlydXN0b3RhbGNsb3VkcksLEgVXaG9pcyJAMzdkODI5MGM1YzgwMmNhN2MzZWU3YWNlMDFiZWJmODJjZWM1YTIyNWY1ZjRhMGU3YjU4ZDdmYjM5NTc2Nz
c2MgwYACAB"
    },
    "links": {
        "self": "https://www.virustotal.com/api/v3/ip_addresses/1.1.1.1/historical_whois?limit=10",
        "next": "https://www.virustotal.com/api/v3/ip_addresses/1.1.1.1/historical_whois?
limit=10cursor=CoQBChwKD2ZpcnN0X3NlZW5fZGF0ZRIJCPTngZTlmu8CEmBqEXN-
dmlydXN0b3RhbGNsb3VkcksLEgVXaG9pcyJAMzdkODI5MGM1YzgwMmNhN2MzZWU3YWNlMDFiZWJmODJjZWM1YTIyNWY1ZjRhMGU3YjU4ZDdmYjM5NTc2Nz
c2MgwYACAB"
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
`.data[].id`	`Indicator.Attribute`	`WHOIS`	`1b5bc06c...632b81`	`WHOIS Record ID only`
`.data[].attributes.registrant_country`	`Indicator.Attribute`	`Registrant Country`	`AU`	`Optional`
`.data[].attributes.registrar_name`	`Indicator.Attribute`	`Registrar Name`	`MarkMonitor Inc.`	`Optional`
`.data[].attributes.first_seen_date`	`Indicator.Attribute`	`Whois First Seen`	`1730083431`	`Optional`
`.data[].attributes.last_updated`	`Indicator.Attribute`	`Whois Last Updated`	`1730069320`	`Optional`

Known Issues / Limitations

- URL Lookups - URL lookups require base64 URL id with `=` removed. For example: **URL** - `http://google.com` ; **URL ID** - `aHR0cDovL2dvb2dsZS5jb20`.

Change Log

- **Version 1.0.0**
    - Initial release