ThreatQuotient

A Securonix Company

VirusTotal Action Bundle

Version 1.3.0

April 20, 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

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	1.3.0
Compatible with ThreatQ Versions	>= 5.19.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The VirusTotal Action Bundle submits a collection of FQDN and supported objects to the VirusTotal API in individual HTTP Requests. VirusTotal returns a response for each object containing any information it has about the indicator.

The integration provides the following actions:

- **VirusTotal** - enriches supported objects with attributes and related objects describing the Indicator of Compromise.
- **VirusTotal Submit URLs** - submits URL indicators to VirusTotal to be analyzed.

The action is compatible with the following indicator types:

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

The action returns the following enriched indicator objects:

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

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

Prerequisites

The action requires the following:

- A VirusTotal API Key.
- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following indicator objects:
  - FQDN
  - IP Address
  - MD5
  - SHA-256
  - SHA-1
  - 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 integration zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the zip file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration file on your local machine
6. Select the actions to install, when prompted, and click on **Install**.

   > 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(s).

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.

Virus Total Action Parameters

PARAMETER	DESCRIPTION
VirusTotal API Key	Your VirusTotal API Key.
Malicious Verdict Threshold (Deprecated)	The minimum number of AV scans reporting the IOC as malicious. Passing this threshold will result in an attribute of "Malicious: True" to be added.
AV Scan Information	The number of reports from URL scanners marking it as harmless, suspicious, malicious or undetected. Options include: ◦ Harmless Count ◦ Malicious Count (default) ◦ Suspicious Count (default)

PARAMETER	DESCRIPTION
	◦ Undetected Count ◦ VirusTotal GUI Link ◦ Return Individual AV Scan Information ◦ Fetch Related Threat Actors (GTI Enterprise or Enterprise Plus License Only)
Fetch Related Threat Actors	
Supporting Context	Select the context to include in the enrichment. Options include: ◦ Tags (default) ◦ Threat Score (GTI) (default) ◦ Severity (GTI) (default) ◦ Verdict (GTI) (default) ◦ Confidence Score (GTI) ◦ Reputation ◦ Categories (default) ◦ Safebrowsing Verdict ◦ Associated with Actor (true/false) ◦ Associated with Malware (true/false) ◦ Pervasive Indicator (true/false)
FILE HASH REPORT CONFIGURATION	
Supporting Context	Select the data used to enrich the IoC for hash submission. Options include: ◦ Basic Properties (default) ◦ Last Analysis Result ◦ Names

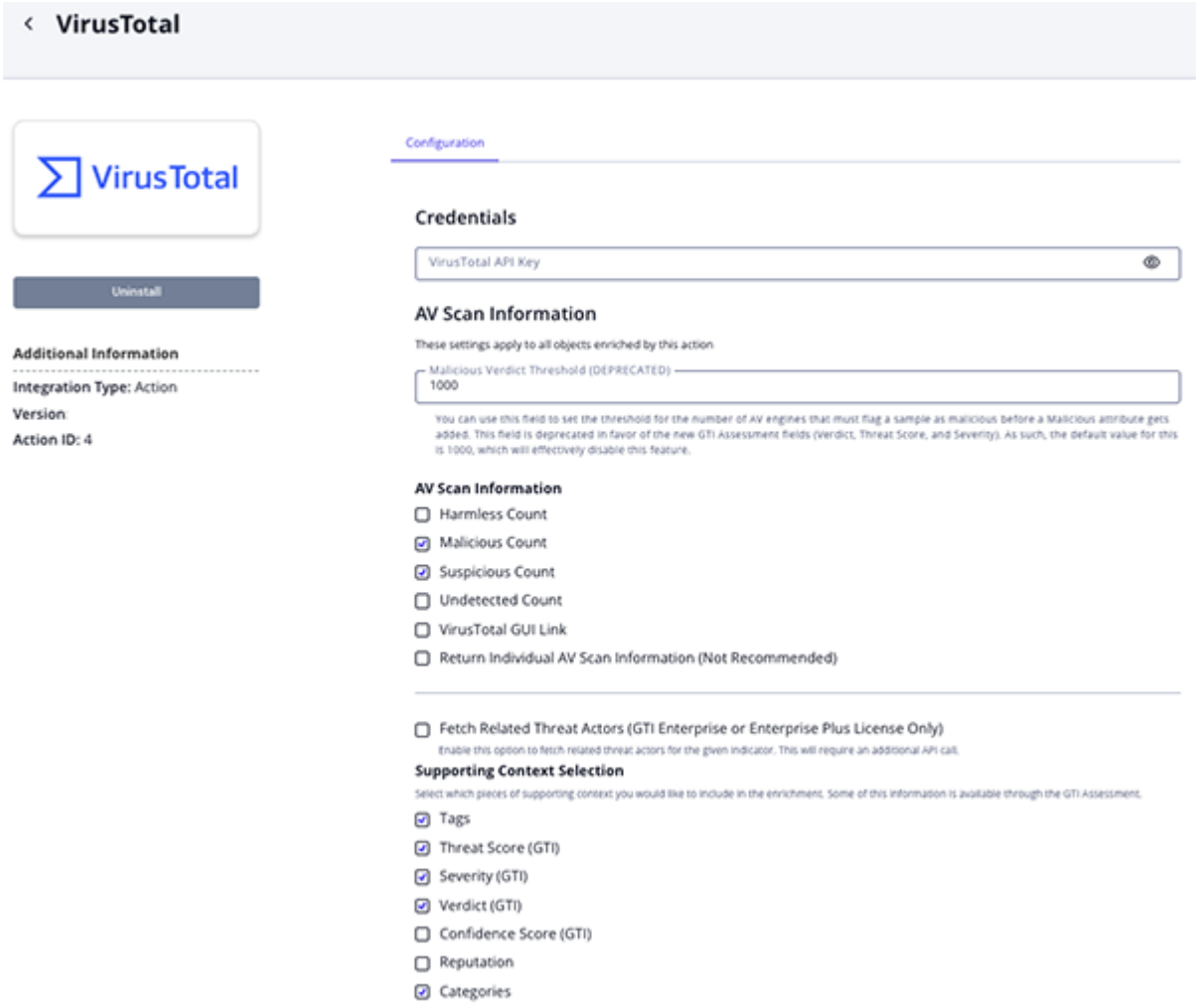
PARAMETER	DESCRIPTION
	◦ VirusTotal Link ◦ Signature Verification
Synonymous Hashes	Select the IOC types that will be ingested in ThreatQ for the file hash submission. Options include: ◦ MD5 ◦ SHA-1 ◦ SHA-256
Set Synonymous Hash Status to	Set the status of the ingested IOCs. Options include: ◦ Active (default) ◦ Expired ◦ Indirect ◦ Review ◦ Whitelisted
FQDN REPORT CONFIGURATION	
Supporting Context	Select which data should be used to enrich the IOC for FQDN Submission. Options include: ◦ WHOIS Information ◦ Registrar ◦ Last HTTPS Certificate ◦ DNS NS, SOA, and MX Records * (default)
Relationships	Select the Relationships data to be retrieved from VirusTotal. Options include: ◦ Immediate Parent ◦ Parent ◦ Siblings

PARAMETER	DESCRIPTION
	◦ Subdomains ◦ URLs *
Set Related Indicator Status to	Set the status of the related indicators. Options include: ◦ Active ◦ Expired ◦ Indirect ◦ Review ◦ Whitelisted
IP ADDRESS REPORT CONFIGURATION	
Supporting Context	Select which data should be used to enrich the IOC for IP Address Submission. Options include: ◦ Basic Properties (default) ◦ WHOIS Information ◦ Registrar ◦ Last SSL Certificate ◦ Historical SSL Certificates *
Relationships *(VT action only)*	Select the relationships data to be retrieved from VirusTotal. There is currently one option: ◦ URLs *

PARAMETER	DESCRIPTION
Set Related Indicator Status to *(VT action only)*	Set the status of the related indicators. Options include: ◦ Active ◦ Expired ◦ Indirect ◦ Review ◦ Whitelisted
URL REPORT CONFIGURATION	
Supporting Context	Select which data should be used to enrich the IOC for URL Submission. Options include: ◦ Basic Properties (default)
Relationships	Select the relationships data to be retrieved from VirusTotal. Options include: ◦ Contacted Domains * ◦ Redirecting URLs * ◦ Referrer Files * ◦ Referrer URLs *
Set Related Indicator Status to	Set the status of the related indicators. Options include: ◦ Active ◦ Expired ◦ Indirect ◦ Review ◦ Whitelisted
WORKFLOW & RATE LIMITING	

PARAMETER	DESCRIPTION
Requests per minute *(VT action only)*	Set the maximum number of requests to make to DomainTools per-minute. The default value is 100.
Objects per run	Set the maximum number of objects to send to DomainTools per-run. The default value is 5,000.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.

* Items marked with an * require an API call.

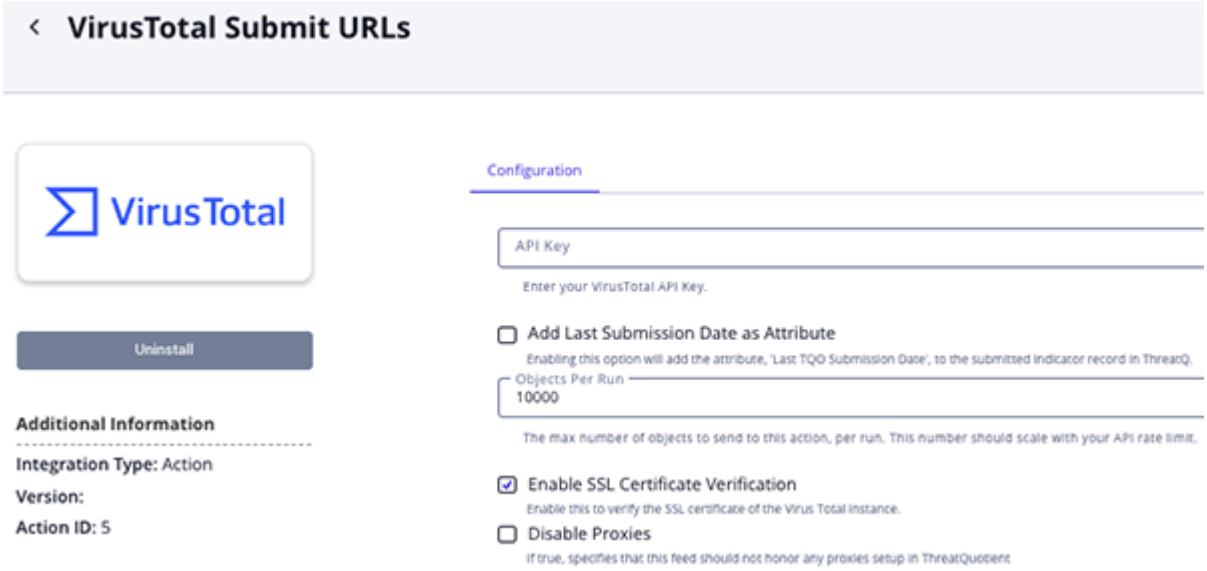


Virus Total Submit URLs Action Parameters

PARAMETER	DESCRIPTION
VirusTotal API Key	Your VirusTotal API Key.
Add Last Submission Date as Attribute	Enabling this option will add the attribute, Last TQO Submission Date, to the submitted indicator record in ThreatQ.
Objects per run	Set the maximum number of objects to send to DomainTools per-run. The default value is 5,000.

PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.

* Items marked with an * require an API call.



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

Actions

The bundle provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
VirusTotal	Queries the VirusTotal API for context.	Indicator	FQDN, IP Address, MD5, SHA-256, SHA-1, URL
VirusTotal Submit URLs	Submits a URL to VirusTotal API for analysis.	Indicator	URL

VirusTotal

The VirusTotal action enriches supported objects with attributes and related objects describing the Indicator of Compromise.

`GET https://www.virustotal.com/api/v3/{{vt_collection_name}}/{{ioc_value}}`

> `vt_collection_name` represents the plural form of the object type as it appears in VirusTotal, while `ioc_value` represents the actual value of the objects for all indicators except for URLs. The URLs are first encoded to Base64.

Sample Response:


```
{
  "data": {
    "id": "88b77a6ddc88be7a2ccfc6a518c06457656c3fdb60c9445c32aba4d24211a969",
    "type": "file",
    "links": {
      "self": "https://www.virustotal.com/api/v3/files/
88b77a6ddc88be7a2ccfc6a518c06457656c3fdb60c9445c32aba4d24211a969"
    },
    "attributes": {
      "first_submission_date": 1743422289,
      "times_submitted": 9,
      "magic": "PE32 executable (GUI) Intel 80386, for MS Windows",
      "sigma_analysis_stats": {
        "critical": 0,
        "high": 2,
        "medium": 4,
        "low": 1
      },
      "authentihash":
"a34587c0de419333ed7b19092316b91ebd0bca8b17f3f90a3c5e5298d2a9ae82",
      "last_analysis_stats": {
        "malicious": 7,
        "suspicious": 0,
        "undetected": 63,
        "harmless": 0,
        "timeout": 0,
        "confirmed-timeout": 0,
        "failure": 1,
        "type-unsupported": 6
      },
      "size": 105853912,
      "vhash": "018066655d1d15156azbe!z",
      "detectiteasy": {
        "filetype": "PE32",
        "values": [
```

```
          {
            "info": "EXE32",
            "version": "2017 v.15.5-6",
            "type": "Compiler",
            "name": "EP:Microsoft Visual C/C++"
          }
        ]
      },
      "names": [
        "NordPassSetup",
        "NordPassSetup.exe",
        "2025-04-02_62b713583c86d3440bae974aae17ed0a_black-basta_luca-stealer",
        "NordPassSetup.exe2.exe.1"
      ],
      "total_votes": {
        "harmless": 0,
        "malicious": 0
      },
      "signature_info": {
        "product": "NordPass",
        "verified": "Signed",
        "description": "NordPass Installer",
        "file version": "5.29.7.64946",
        "signing date": "07:26 PM 03/30/2025",
        "x509": [
          {
            "valid usage": "Code Signing",
            "thumbprint_sha256":
"CD0E144DD10BAC221FE2FB901058D16450A0578B3C47C770908F2E9ADA28EF12",
            "name": "GlobalSign GCC R45 EV CodeSigning CA 2020",
            "algorithm": "sha256RSA",
            "thumbprint_md5": "E6EB41AD6404317AF8A18B64F98C2BCF",
            "valid from": "2020-07-28 00:00:00",
            "valid to": "2030-07-28 00:00:00",
            "serial number": "77 BD 0E 05 B7 59 0B B6 1D 47 61 53 1E 3F 75 ED",
            "cert issuer": "GlobalSign Code Signing Root R45",
            "thumbprint": "C10BB76AD4EE815242406A1E3E1117FFEC743D4F"
          },
          {
            "valid usage": "ff",
            "thumbprint_sha256":
"3A887A951B5EB92A5EE14F6CBB768237A545D0105BF04511BDE25F82A916D1E8",
            "name": "Globalsign TSA for CodeSign1 - R6 - 202311",
            "algorithm": "sha256RSA",
            "thumbprint_md5": "B5E7F67FBE1EE346C34FE4FFDDD3ACC9",
            "valid from": "2023-11-07 17:13:40",
            "valid to": "2034-12-09 17:13:40",
            "serial number": "01 9B EA DE C8 4D 6B 8F F7 6C 3A 9F 2E 01 24 16",
            "cert issuer": "GlobalSign Timestamping CA - SHA384 - G4",
            "thumbprint": "B39F0BD99E6437DB70F4FB7D0E3A8CE5FFF5165B"
          },
          {
```

```
            "thumbprint_sha256":
"F642418E4D0C63DEC785C960EFA68BA745F38851744EF81F225CB89305314D50",
            "name": "GlobalSign Timestamping CA - SHA384 - G4",
            "algorithm": "sha384RSA",
            "thumbprint_md5": "52508C97E039D3E94D7E0B5AE8B99F8D",
            "valid from": "2018-06-20 00:00:00",
            "valid to": "2034-12-10 00:00:00",
            "serial number": "01 EC 1C 92 40 DE FD 2E 40 5D 7C 47 74",
            "cert issuer": "GlobalSign",
            "thumbprint": "F585500925786F88E721D235240A2452AE3D23F9"
          }
        ],
        "original name": "NordPassSetup.exe",
        "signers": "Shijiazhuang SUNRISE Carpet Co., Ltd.; GlobalSign GCC R45 EV
CodeSigning CA 2020; GlobalSign Code Signing Root R45",
        "counter signers details": [
          {
            "status": "Valid",
            "valid usage": "Timestamp Signing",
            "name": "Globalsign TSA for CodeSign1 - R6 - 202311",
            "algorithm": "sha256RSA",
            "valid from": "05:13 PM 11/07/2023",
            "valid to": "05:13 PM 12/09/2034",
            "serial number": "01 9B EA DE C8 4D 6B 8F F7 6C 3A 9F 2E 01 24 16",
            "cert issuer": "GlobalSign Timestamping CA - SHA384 - G4",
            "thumbprint": "B39F0BD99E6437DB70F4FB7D0E3A8CE5FFF5165B"
          },
          {
            "status": "Valid",
            "valid usage": "All",
            "name": "GlobalSign Timestamping CA - SHA384 - G4",
            "algorithm": "sha384RSA",
            "valid from": "12:00 AM 06/20/2018",
            "valid to": "12:00 AM 12/10/2034",
            "serial number": "01 EC 1C 92 40 DE FD 2E 40 5D 7C 47 74",
            "cert issuer": "GlobalSign",
            "thumbprint": "F585500925786F88E721D235240A2452AE3D23F9"
          }
        ],
        "counter signers": "Globalsign TSA for CodeSign1 - R6 - 202311; GlobalSign
Timestamping CA - SHA384 - G4; GlobalSign Root CA - R6",
        "internal name": "NordPassSetup",
        "copyright": "Copyright (C) 2025 NordPass LLC",
        "signers details": [
          {
            "status": "Trust for this certificate or one of the certificates in the
certificate chain has been revoked.",
            "valid usage": "Code Signing",
            "name": "Shijiazhuang SUNRISE Carpet Co., Ltd.",
            "algorithm": "sha256RSA",
            "valid from": "03:37 AM 03/13/2025",
            "valid to": "03:37 AM 03/14/2026",
```

```
            "serial number": "5D 35 4E A7 A5 07 F8 53 74 0B 5E 84",
            "cert issuer": "GlobalSign GCC R45 EV CodeSigning CA 2020",
            "thumbprint": "478CF418040D3AC581ED12EDA481AB39792CA73C"
          },
          {
            "status": "Valid",
            "valid usage": "Code Signing",
            "name": "GlobalSign GCC R45 EV CodeSigning CA 2020",
            "algorithm": "sha256RSA",
            "valid from": "12:00 AM 07/28/2020",
            "valid to": "12:00 AM 07/28/2030",
            "serial number": "77 BD 0E 05 B7 59 0B B6 1D 47 61 53 1E 3F 75 ED",
            "cert issuer": "GlobalSign Code Signing Root R45",
            "thumbprint": "C10BB76AD4EE815242406A1E3E1117FFEC743D4F"
          }
        ]
      },
      "sigma_analysis_results": [
        {
          "rule_level": "high",
          "rule_id":
"92acfd50d9fe4d995d6998a5346e4e031ea037d422458bb4f74555a52ffc886c",
          "rule_source": "Sigma Integrated Rule Set (GitHub)",
          "rule_title": "Script Interpreter Execution From Suspicious Folder",
          "rule_description": "Detects a suspicious script execution in temporary
folders or folders accessible by environment variables",
          "rule_author": "Florian Roth (Nextron Systems), Nasreddine Bencherchali
(Nextron Systems)",
          "match_context": [
            {
              "values": {
                "Hashes":
"SHA1=F66A592D23067C6EFF15356F874E5B61EA4DF4B5,MD5=DBA3E6449E97D4E3DF64527EF7012A10,SHA256=E0C6
                "CurrentDirectory": "C:\\Windows\\SysWOW64\\",
                "OriginalFileName": "PowerShell.EXE",
                "Product": "Microsoft\\xae Windows\\xae Operating System",
                "Description": "Windows PowerShell",
                "FileVersion": "10.0.17134.1 (WinBuild.160101.0800)",
                "ParentCommandLine": "C:\\Windows\\syswow64\\MsiExec.exe -Embedding
612992648629F41797D32ADC030D7B3B",
                "CommandLine": " -NoProfile -Noninteractive -ExecutionPolicy Bypass
-File \"C:\\Users\\george\\AppData\\Local\\Temp\\pssAB52.ps1\" -propFile \"C:\\Users\
\george\\AppData\\Local\\Temp\\msiAB3F.txt\" -scriptFile \"C:\\Users\\george\
\AppData\\Local\\Temp\\scrAB40.ps1\" -scriptArgsFile \"C:\\Users\\george\\AppData\
\Local\\Temp\\scrAB41.txt\" -propSep \" :<->: \" -lineSep \" <<:>> \" -testPrefix
\"_testValue.\"",
                "EventID": "1",
                "ParentImage": "C:\\Windows\\SysWOW64\\msiexec.exe",
                "IntegrityLevel": "High",
                "Image": "C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\
\powershell.exe",
                "Company": "Microsoft Corporation"
```

```
            }
          }
        ]
      }
    ],
    "sha256": "88b77a6ddc88be7a2ccfc6a518c06457656c3fdb60c9445c32aba4d24211a969",
    "meaningful_name": "NordPassSetup.exe",
    "sha1": "7e977e4e2cdc8176ef9bf3d1295081174f28e7b4",
    "reputation": 0,
    "last_submission_date": 1743561655,
    "last_modification_date": 1743593882,
    "type_description": "Win32 EXE",
    "last_analysis_results": {
      "Bkav": {
        "method": "blacklist",
        "engine_name": "Bkav",
        "engine_version": "2.0.0.1",
        "engine_update": "20250402",
        "category": "undetected",
        "result": null
      },
      "Lionic": {
        "method": "blacklist",
        "engine_name": "Lionic",
        "engine_version": "8.16",
        "engine_update": "20250402",
        "category": "undetected",
        "result": null
      }
    },
    "first_seen_itw_date": 1743434557,
    "type_tags": [
      "executable",
      "windows",
      "win32",
      "pe",
      "peexe"
    ],
    "popular_threat_classification": {
      "popular_threat_category": [
        {
          "count": 2,
          "value": "trojan"
        }
      ],
      "suggested_threat_label": "trojan."
    },
    "sigma_analysis_summary": {
      "Sigma Integrated Rule Set (GitHub)": {
        "critical": 0,
        "high": 2,
        "medium": 4,
```

```
          "low": 1
        }
      },
      "type_tag": "peexe",
      "magika": "PEBIN",
      "tags": [
        "long-sleeps",
        "detect-debug-environment",
        "checks-usb-bus",
        "revoked-cert",
        "signed",
        "overlay",
        "peexe"
      ],
      "creation_date": 1706027717,
      "md5": "62b713583c86d3440bae974aae17ed0a",
      "pe_info": {
        "timestamp": 1706027717,
        "imphash": "36aca8edddb161c588fcf5afdc1ad9fa",
        "machine_type": 332,
        "entry_point": 2146720,
        "resource_details": [
          {
            "lang": "ENGLISH US",
            "chi2": 42395.36,
            "filetype": "unknown",
            "entropy": 1.6825700998306274,
            "sha256":
"32673976ffb81636486cd895a3e78e45d812109fdc5c773bcd551316d0b35182",
            "type": "RT_BITMAP"
          }
        ],
        "resource_langs": {
          "ENGLISH US": 48
        },
        "resource_types": {
          "RT_DIALOG": 5,
          "RT_HTML": 10,
          "RT_ICON": 9,
          "RT_MANIFEST": 1,
          "RT_STRING": 15,
          "RT_BITMAP": 6,
          "RT_VERSION": 1,
          "RT_GROUP_ICON": 1
        },
        "overlay": {
          "chi2": 2935.24,
          "filetype": "unknown",
          "entropy": 7.999979019165039,
          "offset": 3983360,
          "md5": "2437beb2966f67d347f191e920d1b56d",
          "size": 101870552
```

```
      },
      "sections": [
        {
          "name": ".text",
          "chi2": 18583160.0,
          "virtual_address": 4096,
          "entropy": 6.46,
          "raw_size": 2716672,
          "flags": "rx",
          "virtual_size": 2716314,
          "md5": "af7d2e8220eb16ff7f03a78de226f3c6"
        }
      ],
      "compiler_product_versions": [
        "[ C ] VS2022 v17.8.0 pre 2.0 build 33030 count=20",
        "[ASM] VS2022 v17.8.0 pre 2.0 build 33030 count=25"
      ],
      "rich_pe_header_hash": "7ac02753730708fb65a242e940b712cb",
      "import_list": [
        {
          "library_name": "imagehlp.dll",
          "imported_functions": [
            "StackWalk",
            "SymCleanup",
            "SymFunctionTableAccess",
            "SymGetLineFromAddr",
            "SymGetModuleBase",
            "SymInitialize",
            "SymSetOptions",
            "SymSetSearchPath"
          ]
        }
      ]
    },
    "ssdeep":
"3145728:gNtrsYZ60ppUhkf5zYvuD5lPjDOdiBRH4cxickC:grsYJaexztzPj6gB1LbN",
    "type_extension": "exe",
    "last_analysis_date": 1743586649,
    "trid": [
      {
        "file_type": "Win64 Executable (generic)",
        "probability": 40.3
      }
    ],
    "filecondis": {
      "dhash": "0000001d0e0f0808",
      "raw_md5": "f8f2f2a0f222483eb1345ed104311e50"
    },
    "unique_sources": 6,
    "tlsh":
"T1553833E0755EC52ED56105B05A2CAA7B911CBEE90B60A0C7B3DC796E2B700CF1736E1B",
    "gti_assessment": {
```

```
            "contributing_factors": {
                "mandiant_analyst_malicious": true,
                "mandiant_confidence_score": 100,
                "associated_actor": true,
                "mandiant_association_actor": true
            },
            "verdict": {
                "value": "VERDICT_MALICIOUS"
            },
            "severity": {
                "value": "SEVERITY_HIGH"
            },
            "threat_score": {
                "value": 100
            },
            "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 and it is associated with a tracked
Mandiant threat actor. Analysts should prioritize investigation."
        }
      }
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.attributes.last_analysis_results.{key}.category	Indicator.Attribute, Related Indicator.Attribute	{key}	.attributes.creation_date or .attributes.first_submission_date	undetected	If Return Individual AV Scan Information user option is checked. For all indicator types.
.attributes.last_analysis_stats.malicious	Indicator.Attribute, Related Indicator.Attribute	Malicious Count	.attributes.creation_date or .attributes.first_submission_date	7	If Malicious Count user option is checked. For all indicator types. Updatable.
.attributes.last_analysis_stats.harmless	Indicator.Attribute, Related Indicator.Attribute	Harmless Count	.attributes.creation_date or .attributes.first_submission_date	0	If Harmless Count user option is checked. For all indicator types. Updatable.
.attributes.last_analysis_stats.suspicious	Indicator.Attribute, Related Indicator.Attribute	Suspicious Count	.attributes.creation_date or .attributes.first_submission_date	0	If Suspicious Count user option is checked. For all indicator types. Updatable.
.attributes.last_analysis_stats.undetected	Indicator.Attribute, Related Indicator.Attribute	Undetected Count	.attributes.creation_date or .attributes.first_submission_date	63	If Undetected Count user option is checked. For all indicator types. Updatable.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.attributes.last_analysis_stats.malicious	Indicator.Attribute, Related Indicator.Attribute	Malicious	.attributes.creation_date or .attributes.first_submission_date	False	If .attributes.malicious_count is greater then the Malicious Verdict Treshold user field. Updatable.
.attributes.type_description	Indicator.Attribute, Related Indicator.Attribute	File Type	.attributes.creation_date or .attributes.first_submission_date	Win32 EXE	For File Hashes. If Basic Properties user option is checked.
.attributes.first_submission_date	Indicator.Attribute, Related Indicator.Attribute	First Published Date	.attributes.creation_date or .attributes.first_submission_date	1743422289	For File Hashes and URLs. If Basic Properties user option is checked.
.attributes.last_analysis_results.result	Indicator.Attribute, Related Indicator.Attribute	Last Analysis Result	.attributes.creation_date or .attributes.first_submission_date	N/A	For File Hashes. If Last Analysis Result user option is checked.
.attributes.meaningful_name	Indicator.Attribute, Related Indicator.Attribute	Meaningful Name	.attributes.creation_date or .attributes.first_submission_date	NordPassSetup.exe	For File Hashes. If Basic Properties user option is checked.
.attributes.signature_info.verified	Indicator.Attribute, Related Indicator.Attribute	Signature Verification	.attributes.creation_date or .attributes.first_submission_date	Signed	If Signature Verification user option is checked. For File Hashes. User-configurable. Updatable.
.attributes.signature_info.signers details.status	Indicator.Attribute, Related Indicator.Attribute	Signer Status	.attributes.creation_date or .attributes.first_submission_date	Trust for this certificate or one of the certificates in the certificate chain has been revoked.	If Signature Verification user option is checked and signature_info.signers details.status is not Valid. For File Hashes. User-configurable. Updatable.
.attributes.md5	Related Indicator.Value	MD5	.attributes.creation_date or .attributes.first_submission_date	62b713583c86d3440bae974aae17ed0a	For File Hashes. If MD5 user option is checked.
.attributes.md5	Related Indicator.Attribute	VirusTotal Link	.attributes.creation_date or .attributes.first_submission_date	62b713583c86d3440bae974aae17ed0a	For File Hashes. If MD5 user option is checked, formatted as https://www.virustotal.com/gui/file/{.attributes.md5}. Updatable.
.attributes.sha1	Related Indicator.Value	SHA-1	.attributes.creation_date or .attributes.first_submission_date	7e977e4e2cdc8176ef9bf3d1295081174f28e7b4"	For File Hashes. If SHA-1 user option is checked.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.attributes.sha1	Related Indicator.Attribute	VirusTotal Link	.attributes.creation_date or .attributes.first_submission_date	7e977e4e2cdc8176ef9bf3d1295081174f28e7b4"	For File Hashes. If SHA-1 user option is checked, formatted as https://www.virustotal.com/gui/file/{.attributes.sha1}. Updatable.
.attributes.sha256	Related Indicator.Value	SHA-265	.attributes.creation_date or .attributes.first_submission_date	88b77a6ddc88be7a2ccfc6a518c06457656c3fdb60c9445c32aba4d24211a969	For File Hashes. If SHA-256 user option is checked.
.attributes.sha256	Related Indicator.Attribute	VirusTotal Link	.attributes.creation_date or .attributes.first_submission_date	88b77a6ddc88be7a2ccfc6a518c06457656c3fdb60c9445c32aba4d24211a969	For File Hashes. If SHA-256 user option is checked, formatted as https://www.virustotal.com/gui/file/{.attributes.sha256}. Updatable.
.attributes.names[]	Indicator.Attribute, Related Indicator.Attribute	Name	.attributes.creation_date or .attributes.first_submission_date	NordPassSetup	For File Hashes. If Names user option is checked.
.attributes.asn	Indicator.Attribute	ASN	.attributes.creation_date or .attributes.first_submission_date	N/A	For IP Addresses. If Basic Properties user option is checked.
.attributes.as_owner	Indicator.Attribute	AS Owner	.attributes.creation_date or .attributes.first_submission_date	N/A	For IP Addresses. If Basic Properties user option is checked.
.attributes.last_https_certificate_date	Indicator.Attribute	Last SSL certificate	.attributes.creation_date or .attributes.first_submission_date	N/A	For IP Addresses. If Last SSL certificate user option is checked.
.attributes.categories	Indicator.Attribute	Category	.attributes.creation_date or .attributes.first_submission_date	N/A	N/A
.attributes.reputation	Indicator.Attribute	Reputation	.attributes.creation_date or .attributes.first_submission_date	0	Updatable.
.attributes.tags	Indicator.Tag	N/A	N/A	long-sleeps	N/A
.attributes.gti_assessment.severity.value	Indicator.Attribute	Severity	.attributes.creation_date or .attributes.first_submission_date	HIGH	Updatable.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.attributes.gti_assessment.verdict.value	Indicator.Attribute	Verdict	.attributes.creation_date or .attributes.first_submission_date	MALICIOUS	Updatable.
.attributes.gti_assessment.contributing_factors.mandiant_confidence_score	Indicator.Attribute	Confidence Score	.attributes.creation_date or .attributes.first_submission_date	100	Updatable.
.attributes.gti_assessment.contributing_factors.associated_malware_configuration	Indicator.Attribute	Associated with Malware	.attributes.creation_date or .attributes.first_submission_date	N/A	If Associated with Malware (true/false) user option is checked. Updatable.
.attributes.gti_assessment.contributing_factors.associated_actor	Indicator.Attribute	Associated with Actor	.attributes.creation_date or .attributes.first_submission_date	true	If Associated with Actor (true/false) user option is checked. Updatable.
.attributes.gti_assessment.contributing_factors.mandiant_association_malware	Indicator.Attribute	Associated with Mandiant Malware	.attributes.creation_date or .attributes.first_submission_date	N/A	If Associated with Malware (true/false) user option is checked. Updatable.
.attributes.gti_assessment.contributing_factors.mandiant_association_actor	Indicator.Attribute	Associated with Mandiant Actor	.attributes.creation_date or .attributes.first_submission_date	true	If Associated with Actor (true/false) user option is checked. Updatable.
.attributes.gti_assessment.contributing_factors.safebrowsing_verdict	Indicator.Attribute	Safebrowsing Verdict	.attributes.creation_date or .attributes.first_submission_date	true	Updatable.
.attributes.gti_assessment.threat_score.value	Indicator.Attribute	Threat Score	.attributes.creation_date or .attributes.first_submission_date	100	Updatable.
.attributes.gti_assessment.contributing_factors.categories	Indicator.Attribute	Category	.attributes.creation_date or .attributes.first_submission_date	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.attributes.gti_assessment.contributing_factors.pervasive_indicator	Indicator.Attribute	Pervasive Indicator	.attributes.creation_date or .attributes.first_submission_date	false	If Pervasive Indicator user option is checked. Updatable.
.attributes.whois	Indicator.Description	N/A	.attributes.creation_date or .attributes.first_submission_date	N/A	If enabled for IP Addresses & Domains.
.attributes.registrar	Indicator.Attribute	Registrar	.attributes.creation_date or .attributes.first_submission_date	Xiamen 35.Com Technology Co., Ltd	For Domains and IP Addresses. If Registrar is selected in the corresponding FQDN or IP Address Supporting Context options and the structured registrar field is present. Updatable.
.attributes.last_https_certificate	Indicator.Description	N/A	.attributes.creation_date or .attributes.first_submission_date	N/A	If enabled for IP Addresses(Last SSL certificate) & Domains(Last HTTPS certificate); Raw JSON data.

IOC Type Mapping

ThreatQ provides the following ThreatQ IOC Type to VirusTotal Collection Name mapping.

THREATQ IOC TYPE	VIRUSTOTAL COLLECTION NAME
FQDN	domains
IP Address	ip_addresses
SHA-256	files
SHA-1	files
MD5	files
URL	urls

Supplemental Calls

VirusTotal objects contain relationships with other objects in the dataset that can be retrieved with the supplemental call endpoint.

```
GET https://www.virustotal.com/api/v3/{{vt_collection_name}}/
{{ioc_value}}/{{relationship}}
```

Sample Response:


```
{
    "meta": {
        "count": 1
    },
    "data": [
        {
            "attributes": {
                "last_dns_records": [
                    {
                        "type": "CNAME",
                        "value": "rigpriv.com",
                        "ttl": 599
                    },
                    {
                        "type": "NS",
                        "value": "jm2.dns.com",
                        "ttl": 21600
                    }
                ],
                "jarm":
"28d28d28d00028d1ec28d28d28d28de9ab649921aa9add8c37a8978aa3ea88",
                "whois": "Creation Date: 2022-06-29T16:00:00Z\nCreation Date:
2022-06-30T02:32:32Z\nDNSSEC: unsigned\nDomain Name: RIGPRIV.COM\nDomain Status: ok
https://icann.org/epp#ok\nName Server: JM1.DNS.COM\nName Server:
JM2.DNS.COM\nRegistrant City: 7145b6c7c70448a6\nRegistrant Country: CN\nRegistrant
Email: 5c0a26a8248bb13fs@\nRegistrant State/Province: 4f3a9c87b8ed6c6a\nRegistrar
Abuse Contact Email: domainabuse@35.cn\nRegistrar Abuse Contact Phone:
+86.4001353511\nRegistrar Abuse Contact Phone: +86.4006003535\nRegistrar IANA ID:
1316\nRegistrar Registration Expiration Date: 2023-06-30T04:00:00Z\nRegistrar URL:
http://www.35.com\nRegistrar WHOIS Server: whois.35.com\nRegistrar: Xiamen 35.Com
Technology Co., Ltd\nRegistrar: Xiamen 35.Com Technology Co., Ltd.\nRegistry Domain
ID: 2707568686_DOMAIN_COM-VRSN\nRegistry Expiry Date: 2023-06-30T02:32:32Z\nRegistry
Registrant ID: Not Available From Registry\nUpdated Date:
2022-06-30T02:43:05Z\nUpdated Date: 2022-08-21T16:00:00Z",
                "last_https_certificate_date": 1660080390,
                "tags": [],
                "popularity_ranks": {},
                "last_dns_records_date": 1660080390,
                "last_analysis_stats": {
                    "harmless": 86,
                    "malicious": 0,
```

```
                    "suspicious": 0,
                    "undetected": 8,
                    "timeout": 0
                },
                "creation_date": 1656556352,
                "reputation": 0,
                "registrar": "Xiamen 35.Com Technology Co., Ltd",
                "last_analysis_results": {
                    "CMC Threat Intelligence": {
                        "category": "harmless",
                        "result": "clean",
                        "method": "blacklist",
                        "engine_name": "CMC Threat Intelligence"
                    }
                },
                "last_update_date": 1661097600,
                "last_modification_date": 1660080390,
                "last_https_certificate": {
                    "size": 1159,
                    "public_key": {
                        "ec": {
                            "oid": "secp256r1",
                            "pub":
"0481596f6c64661ffb6a79fce6cba763d9ee961778b6e21f93eca791db1bb8fa401bbda5b35fc3874e0577444
8520d600e5f041b35257c4d7b428390afac0d514e"
                        },
                        "algorithm": "EC"
                    },
                    "thumbprint_sha256":
"2a676d52b302af217fd08e64dca3a5635bd8eea0d19ad91a50c518da2e26acc4",
                    "tags": [],
                    "cert_signature": {
                        "signature":
"6902093866e2a299575f2c04f852aaf3c2789cf53687873d4e6f599ea9140101e9be50dd8774f01b30115ca72
1561416a4d03d316b146844a3b819ec235346bb2ddc7cf3a17592a142c6b303080b18cd801d28bf7738ffb3e51
3059d8c0664783bc7edaf3711c1e6062eb20abedada8c0c8f5b2a1be20519b3056422f3c92b02c4190f649189e
a4ed07d2f9e3e87839bb180afe9a81e36f28a826400eee290775b2035bb37b681424d8224e5c8955d5ce21ecf0
475a7670f772fe16e5133176fd6dc0cc538c3d459faa72f7ffec06c4c1f9f2578cb168f82c56e10a0ffa77365d
b3378f6f55fbb1144465011a0cadb2d72658fc59b54958b0f34a89de56d640c",
                        "signature_algorithm": "sha256RSA"
                    },
                    "validity": {
                        "not_after": "2022-10-20 12:54:43",
                        "not_before": "2022-07-22 12:54:44"
                    },
                    "version": "V3",
                    "extensions": {
                        "certificate_policies": [
                            "2.23.140.1.2.1",
                            "1.3.6.1.4.1.44947.1.1.1"
                        ],
                        "extended_key_usage": [
```

```
                            "serverAuth",
                            "clientAuth"
                        ],
                        "authority_key_identifier": {
                            "keyid": "142eb317b75856cbae500940e61faf9d8b14c2c6"
                        },
                        "subject_alternative_name": [
                            "m.rigpriv.com",
                            "rigpriv.com",
                            "wap.rigpriv.com",
                            "www.rigpriv.com"
                        ],
                        "tags": [],
                        "subject_key_identifier":
"48a87063dd6dc4462b432889e1615c2ce20f118d",
                        "key_usage": [
                            "ff"
                        ],
                        "1.3.6.1.4.1.11129.2.4.2":
"0481f100ef007500dfa55eab68824f1f6cadeeb85f4e3e5aeacda212a46a5e8e",
                        "CA": true,
                        "ca_information_access": {
                            "CA Issuers": "http://r3.i.lencr.org/",
                            "OCSP": "http://r3.o.lencr.org"
                        }
                    },
                    "signature_algorithm": "sha256RSA",
                    "serial_number": "044be080e3027b8cbf43952e34f00ce03492",
                    "thumbprint": "de1cabd8d7c8b5e3b9ef2d8899b2f148390fa3d2",
                    "issuer": {
                        "C": "US",
                        "CN": "R3",
                        "O": "Let's Encrypt"
                    },
                    "subject": {
                        "CN": "m.rigpriv.com"
                    }
                },
                "categories": {},
                "total_votes": {
                    "harmless": 0,
                    "malicious": 0
                }
            },
            "type": "domain",
            "id": "wap.rigpriv.com",
            "links": {
                "self": "https://www.virustotal.com/api/v3/domains/wap.rigpriv.com"
            }
        }
    ],
    "links": {
```

```
        "self": "https://www.virustotal.com/api/v3/domains/rigpriv.com/subdomains?
limit=10"
    }
}
```

ThreatQuotient provides the following default mapping for this function:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
attributes.url	Related Indicator.Value	N/A	N/A	www.rigpriv.com/upload	For `URLs` relationships
.attributes.md5	Related Indicator.Value	N/A	N/A	e2f6cdade9be842ebd160634c30f1e16	For `Referrer File` relationship
.attributes.sha1	Related Indicator.Value	N/A	N/A	ccbbc621afe012b358ed2e13875f1581b944dd25	For `Referrer File` relationship
.attributes.sha256	Related Indicator.Value	N/A	N/A	56e784268807ee237adebd98046f0090ceecdfde6d2e1326afd3670e4e3ffd23	For `Referrer File` relationship
.context_attributes.first_seen_date	Indicator.Attribute	Historical SSL certificate	N/A	1591571057	For `Historical SSL certificate` relationship
.id	Related Indicator.Value	View the Relationships table	N/A	www.rigpriv.com	For all other relationships
N/A	Related Indicator.Attribute	VirusTotal Link	N/A	https://www.virustotal.com/gui/ip-address/194.180.191.124	Formatted based on the type of the indicator and it's value. For URL indicators the url is encoded using `base64` format
N/A	Related Indicator.Attribute	`Relationship`	N/A	True	Represents the relationship with the data collection indicator as it appears in the ThreatQ Configuration column from the Relationship table above.

Relationships Type Mapping Table

ThreatQ provides the following relationships mapping:

VIRUS TOTAL COLLECTION NAME	VIRUS TOTAL RELATIONSHIP	THREATQ CONFIGURATION	ACCESSIBILITY
domains	ns_records	DNS NS	VT Premium users only
domains	soa_records	SOA	VT Premium users only
domains	mx_records	MX Records	VT Premium users only
domains	urls	Immediate Parent	Everyone
domains	parent	Parent	Everyone
domains	siblings	Siblings	Everyone
domains	immediate_parent	Immediate Parent	Everyone
domains	subdomains	Subdomains	Everyone
domains	urls	URLs	VT Premium users only
ip_addresses	historical_ssl_certificates	Historical SSL certificates	Everyone
ip_addresses	urls	URLs	VT Premium users only

VIRUS TOTAL COLLECTION NAME	VIRUS TOTAL RELATIONSHIP	THREATQ CONFIGURATION	ACCESSIBILITY
urls	last_serving_ip_address	Last Serving IP address	Everyone
urls	contacted_domains	Contacted Domains	VT Premium users only
urls	redirecting_urls	Redirecting URLs	VT Premium users only
urls	referrer_files	Referrer Files	VT Premium users only
urls	referrer_urls	Referrer URLs	VT Premium users only
*	related_threat_actors	Fetch Related Threat Actors	GTI Enterprise or Enterprise Plus users only

Related Threat Actors

For GTI Enterprise and Enterprise Plus users, the related threat actors can be fetched using the following endpoint:

```
GET https://www.virustotal.com/api/v3/{{vt_collection_name}}/
{{ioc_value}}/related_threat_actors
```

Sample Response:


```
    {
  "data": [
    {
      "id": "threat-actor--bf5b0be5-ec7b-5f7b-985c-6aa902d2c30e",
      "type": "collection",
      "links": {
        "self": "https://www.virustotal.com/api/v3/collections/threat-actor--
bf5b0be5-ec7b-5f7b-985c-6aa902d2c30e"
      },
      "attributes": {
        "vulnerable_products": "",
        "references_count": 36,
        "malware_roles": [],
        "collection_links": [],
        "risk_factors": [],
        "files_count": 2026,
        "origin": "Google Threat Intelligence",
        "creation_date": 1624951563,
        "autogenerated_tags": [
          "downloads-pdf",
          "downloads-zip",
          "contains-pe",
          "downloads-pe",
          "downloads-doc",
          "contains-zip",
          "contains-msi",
          "base64-embedded",
          "opendir"
        ],
        "vendor_fix_references": [],
        "workarounds": [],
        "source_regions_hierarchy": [
          {
            "region": "Americas",
            "sub_region": "Central America",
            "country": "Mexico",
            "country_iso2": "MX",
            "confidence": "confirmed",
            "first_seen": null,
            "last_seen": null,
            "description": null,
```

```
      "source": null
    }
  ],
  "first_seen_details": [
    {
      "confidence": "confirmed",
      "first_seen": null,
      "last_seen": null,
      "value": "2021-06-29T07:26:03.254Z",
      "description": null
    }
  ],
  "targeted_regions_hierarchy": [
    {
      "region": "Oceania",
      "sub_region": "Australia and New Zealand",
      "country": "Australia",
      "country_iso2": "AU",
      "confidence": "confirmed",
      "first_seen": 1725949824,
      "last_seen": 1725950391,
      "description": null,
      "source": null
    }
  ],
  "targeted_informations": [],
  "subscribers_count": 10,
  "field_sources": [],
  "available_mitigation": [],
  "first_seen": 1624951563,
  "threat_scape": [],
  "private": true,
  "mitigations": [],
  "intended_effects": [],
  "recent_activity_relative_change": -0.04162936436884512,
  "targeted_industries_tree": [
    {
      "industry_group": "Chemicals and Materials",
      "industry": null,
      "confidence": "confirmed",
      "first_seen": 1628532224,
      "last_seen": 1681578143,
      "description": null,
      "source": null
    }
  ],
  "affected_systems": [],
  "operating_systems": [],
  "domains_count": 642,
  "urls_count": 2161,
  "tags": [],
  "recent_activity_summary": [129, 252],
```

```
    "last_seen": 1740170989,
    "counters": {
      "files": 2026,
      "domains": 642,
      "ip_addresses": 129,
      "urls": 2161,
      "iocs": 4958,
      "subscribers": 10,
      "attack_techniques": 110
    },
    "name": "UNC4984",
    "alt_names_details": [
      {
        "confidence": "confirmed",
        "first_seen": null,
        "last_seen": null,
        "value": "Cybercartel (Darktrace)",
        "description": null
      },
      {
        "confidence": "confirmed",
        "first_seen": null,
        "last_seen": null,
        "value": "Cybercartel (IBM)",
        "description": null
      }
    ],
    "technologies": [],
    "targeted_regions": ["CA", "MX", "FR", "US", "IN", "CL", "AU"],
    "ip_addresses_count": 129,
    "summary_stats": {
      "first_submission_date": {
        "min": 0.0,
        "max": 1741602990.0,
        "avg": 1602640150.9900086
      },
      "last_submission_date": {
        "min": 0.0,
        "max": 1742808294.0,
        "avg": 1610388669.7927492
      },
      "files_detections": {
        "min": 0.0,
        "max": 62.0,
        "avg": 12.646314221891297
      },
      "urls_detections": {
        "min": 0.0,
        "max": 20.0,
        "avg": 3.801388888888888
      }
    },
```

```
        "description": "UNC4984 is a financially motivated threat cluster that
distributes a variety of malware, including malicious browser extensions, such as
DARKWOODS and RILIDE, and the SIMPLELOADER downloader. The malicious browser
extensions often redirect to fake Mexican bank websites. The threat cluster has used
multiple distribution vectors, including phishing emails, SMS messages, malicious
advertisements, and likely search engine optimization (SEO) poisoning. These
campaigns often leverage websites that masquerade as local tax or financial-related
government websites and incorporate geofencing to limit distribution to individuals
in countries such as Mexico, Argentina, and Chile.",
        "alt_names": [
          "Manipulated Caiman (Perception Point)",
          "Cybercartel (IBM)",
          "Cybercartel (Metabaseq)",
          "Cybercartel (Darktrace)"
        ],
        "detection_names": [],
        "tags_details": [],
        "targeted_industries": [],
        "merged_actors": [
          {
            "confidence": "confirmed",
            "first_seen": 1722516815,
            "last_seen": 1722516815,
            "value": "UNC4812",
            "description": "threat-actor--abcdc639-7c95-5b42-93f0-23774776a7bb"
          },
          {
            "confidence": "confirmed",
            "first_seen": 1726509404,
            "last_seen": 1726509404,
            "value": "UNC4880",
            "description": "threat-actor--683c9d12-6d02-5953-8cba-69bd0733e958"
          }
        ],
        "motivations": [
          {
            "confidence": "confirmed",
            "first_seen": null,
            "last_seen": null,
            "value": "Financial Gain",
            "description": null
          }
        ],
        "last_seen_details": [
          {
            "confidence": "confirmed",
            "first_seen": null,
            "last_seen": null,
            "value": "2025-02-21T20:49:49Z",
            "description": null
          }
        ],
```

```
        "status": "COMPUTED",
        "exploitation_vectors": [],
        "source_region": "MX",
        "capabilities": [],
        "collection_type": "threat-actor",
        "version_history": [],
        "last_modification_date": 1742801869,
        "top_icon_md5": [
          "ac62a412f60007d190a319f9066f2890",
          "cc9984a7ffca0aa45df07e44e0245cea",
          "142af3dbfad04c3ec9a608dc70575328"
        ],
        "aggregations": {
          "files": {
            "contacted_ips": [
              {
                "value": "198.59.144.131",
                "count": 8,
                "total_related": 351,
                "prevalence": 0.022792022792022793
              }
            ],
            "execution_parents": [
              {
                "value":
"ce6215d28be085a4fb85787c9dab66ea5c5c60f4688e0f6a1760a9bf80fa9fe2",
                "count": 3,
                "total_related": 18,
                "prevalence": 0.16666666666666666
              }
            ],
            "compressed_parents": [
              {
                "value":
"d0cdf99608ba0b59a8ffb6cad9645aa1f4a15b838e098e5d64422b98ded25687",
                "count": 3,
                "total_related": 57,
                "prevalence": 0.05263157894736842
              }
            ],
            "dropped_files_sha256": [
              {
                "value":
"181a23b19109dcbece67cffabf6980980ee3e22d641a469bd80e8b991367b7b3",
                "count": 5,
                "total_related": 85381,
                "prevalence": 5.856103817008468e-5
              }
            ],
            "embedded_urls": [
              {
                "value": "http://72.5.43.188/ttt/index.php?id=10;iex",
```

```
                "count": 5,
                "total_related": 17,
                "prevalence": 0.29411764705882354
              }
            ],
            "mutexes_created": [
              {
                "value": "Hfhtrtfg24c32fjdsgFydsfjkdsfGt23",
                "count": 4,
                "total_related": 10,
                "prevalence": 0.4
              }
            ],
            "registry_keys_opened": [
              {
                "value": "HKCU\\Software\\Wow6432Node\\Microsoft\\Edge\\Extensions\
\kpcopilihnalmohknofcdijpgpmioknn\\toolbar_pin",
                "count": 2,
                "total_related": 13,
                "prevalence": 0.15384615384615385
              }
            ],
            "registry_keys_set": [
              {
                "value": "HKEY_CURRENT_USER\\Software\\Wow6432Node\\Microsoft\\Edge\
\Extensions\\kpcopilihnalmohknofcdijpgpmioknn\\installation_mode",
                "count": 2,
                "total_related": 11,
                "prevalence": 0.18181818181818182
              }
            ],
            "dropped_files_path": [
              {
                "value": "C:\\bender.txt",
                "count": 2,
                "total_related": 3,
                "prevalence": 0.6666666666666666
              }
            ],
            "pe_info_exports": [
              {
                "value": "curl_mime_encoder",
                "count": 10,
                "total_related": 58973,
                "prevalence": 0.00016956912485374662
              }
            ],
            "popular_threat_category": [
              {
                "value": "trojan",
                "count": 584
              },
```

```
            {
              "value": "downloader",
              "count": 210
            },
            {
              "value": "phishing",
              "count": 48
            }
          ],
          "popular_threat_name": [
            {
              "value": "msil",
              "count": 148
            },
            {
              "value": "furl",
              "count": 48
            },
            {
              "value": "convagent",
              "count": 36
            }
          ],
          "suggested_threat_label": "trojan.msil/furl",
          "attack_techniques": [
            {
              "value": "T1055.004",
              "count": 7,
              "total_related": 73069,
              "prevalence": 9.579986040591769e-5
            }
          ],
          "memory_pattern_urls": [
            {
              "value": "http://72.5.43.188/ttt/index.php?id=10;iex",
              "count": 5,
              "total_related": 17,
              "prevalence": 0.29411764705882354
            }
          ],
          "attack_tactics": [
            {
              "value": "TA0007",
              "count": 2332
            }
          ]
        },
        "urls": {
          "http_response_contents": [
            {
              "value":
"ec1b3fd5fdb0158078103d4e98ad5f8053663723913a78709cca842079c50f8c",
```

```
                "count": 18,
                "total_related": 172,
                "prevalence": 0.10465116279069768
              }
            ],
            "domains": [
              {
                "value": "fastify.sbs",
                "count": 20,
                "total_related": 58,
                "prevalence": 0.3448275862068966
              }
            ],
            "embedded_js": [
              {
                "value":
"20209c9e524f0f96c97c9e2aa05ef3feccb6c43786627f98c09e77b5d927aee1",
                "count": 15,
                "total_related": 38,
                "prevalence": 0.39473684210526316
              }
            ],
            "ip_addresses": [
              {
                "value": "168.100.8.151",
                "count": 12,
                "total_related": 62,
                "prevalence": 0.1935483870967742
              }
            ],
            "memory_patterns": [
              {
                "value":
"449269d0274d46bba97724d0cf296f7eedc892c3d9bd99be5aa1595ceee8c039",
                "count": 41,
                "total_related": 96,
                "prevalence": 0.4270833333333333
              }
            ],
            "outgoing_links": [
              {
                "value": "https://www.googletagmanager.com/gtag/js?
id=AW-16447205675",
                "count": 9,
                "total_related": 39,
                "prevalence": 0.23076923076923078
              }
            ],
            "path": [
              {
                "value": "/ActadeNacimiento/",
                "count": 24,
```

```
                "total_related": 40,
                "prevalence": 0.6
              }
            ],
            "prefix_paths": [
              {
                "value": "/ActadeNacimiento",
                "count": 23,
                "total_related": 75,
                "prevalence": 0.30666666666666664
              }
            ],
            "suffix_paths": [
              {
                "value": "/post.php",
                "count": 19,
                "total_related": 34123,
                "prevalence": 0.0005568091902822144
              }
            ],
            "referring_files": [
              {
                "value":
"bb9e20035d0598ba4eef8f92080c198dbff869548eed5e72672b0efb437bcbc6",
                "count": 17,
                "total_related": 58,
                "prevalence": 0.29310344827586204
              }
            ],
            "tags": [
              {
                "value": "dom-modification",
                "count": 232
              }
            ]
          },
          "domains": {
            "attributions": [
              {
                "value": "simpleloader",
                "count": 21,
                "total_related": 24,
                "prevalence": 0.875
              }
            ],
            "communicating_files": [
              {
                "value":
"0003ef8b7269acdb876bbafb741b4c3f2ad6ad2a554833e7373540b52984c548",
                "count": 1,
                "total_related": 2,
                "prevalence": 0.5
```

```
            }
          ],
          "downloaded_files": [
            {
              "value":
"f7dbeb0f4903b4712b468802a3dc385d59e23374164f58c1d38b1957fd43501a",
              "count": 3,
              "total_related": 43,
              "prevalence": 0.06976744186046512
            }
          ],
          "favicon_dhash": [
            {
              "value": "8d8d11cdcd318d8d",
              "count": 13,
              "total_related": 46,
              "prevalence": 0.2826086956521739
            }
          ],
          "favicon_raw_md5": [
            {
              "value": "ac62a412f60007d190a319f9066f2890",
              "count": 13,
              "total_related": 46,
              "prevalence": 0.2826086956521739
            }
          ],
          "urls": [
            {
              "value": "http://000.sbs/",
              "count": 1,
              "total_related": 1,
              "prevalence": 1.0
            }
          ],
          "registrant_names": [
            {
              "value": "mxonlinex.com.mx",
              "count": 3,
              "total_related": 4,
              "prevalence": 0.75
            }
          ],
          "communicating_files": [
            {
              "value":
"15d39da3087f50ea59fbea6e863b461dd60e2d6b313bdf4def2563ed228b1bfa",
              "count": 3,
              "total_related": 3,
              "prevalence": 1.0
            }
          ]
```

```
          }
        }
      },
      "context_attributes": {
        "shared_with_me": false,
        "role": "viewer"
      }
    }
  ],
  "meta": {
    "count": 1
  },
  "links": {
    "self": "https://www.virustotal.com/api/v3/ip_addresses/46.101.107.181/
related_threat_actors?limit=10"
  }
}
```


ThreatQuotient provides the following default mapping for this function:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.attributes.name	Adversary.Name	Adversary	N/A	APT32	N/A
.attributes.motivations[].value	Adversary.Attribute	Motivation	N/A	Financial Gain	N/A
.attributes.source_regions_hierarchy[].country	Adversary.Attribute	Source Region	N/A	Mexico	N/A
.attributes.targeted_regions_hierarchy[].country	Adversary.Attribute	Target Region	N/A	United States	N/A
.attributes.targeted_industries_tree[].industry_group	Adversary.Attribute	Target Sector	N/A	Construction & Engineering	N/A
.attributes.alt_names[]	Adversary.Attribute	Alias	N/A	WIZARD SPIDER	N/A
.attributes.tags[]	Adversary.Tag	N/A	N/A	N/A	N/A

VirusTotal Submit URLs

The Virus Total Submit URLS action enriches IPs using the VirusTotal API.

```
POST https://www.virustotal.com/api/v3/urls/{{ioc_value}}/analyse
```

Sample Response:

```
{
  "data": {
    "type": "analysis",
    "id": "u-
d0e196a0c25d35dd0a84593cbae0f38333aa58529936444ea26453eab28dfc86-1677067101"
  }
}
```

ThreatQ provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
run_meta.started_at	Indicator.Attribute	Last TQO Submission Date	N/A	2023-02-22 12:15:00-00:00	Only gets ingested if the user selects the Add Last Submission Date as Attribute option.

Enriched Data

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

VirusTotal

METRIC	RESULT
Run Time	1 minute
Indicators	61
Indicator Attributes	352
Adversaries	2
Adversary Attributes	40

VirusTotal Submit URLs

METRIC	RESULT
Run Time	1 minute
Indicators	57
Indicator Attributes	57

Use Case Example

1. A Threat Analyst identifies a collection of supported objects they would like to enrich.
2. The Threat Analyst adds the VirusTotal Action to a Workflow
3. The Threat Analyst configures the action with the desired parameters, and enables the Workflow
4. The Workflow executes all Actions in the graph, including VirusTotal
5. The action returns the documented Attributes from the provider, and the Workflow ingests this data into the ThreatQ platform.

Known Issues / Limitations

- The VirusTotal API is limited to 50 lookups per day.

Change Log

- **Version 1.3.0**
  - Updated the VirusTotal action to apply `VirusTotal` as the source on enriched indicator objects.
- **Version 1.2.1**
  - Updated the action to ingest additional VirusTotal context. Registrar information will now be ingested as an attribute in ThreatQ.
  - VirusTotal Action – Added `Registrar` as a new **Supporting Context** option for the FQDN and IP Address report configuration parameters.
- **Version 1.2.0**
  - Adds support for GTI Assessment Context: Threat Score, Severity, Verdict, Confidence Score, Categories, Safebrowsing Verdict, Associated with Threat Actor, Associated with Malware, and Pervasive Indicator
  - Adds support for additional VirusTotal Context:
    - Tags
    - Categories
    - Reputation
    - WHOIS Information (added to the Description of an indicator)
    - Last HTTPS Certificate Information (added to the Description of an indicator)
  - Adds support for File Signature Context: Signature Verification and Signer Status
  - Adds the ability to fetch related Threat Actors (requires GTI Enterprise or Enterprise Plus).
  - Fixes parsing errors.
  - Deprecates (but doesn't remove) the `Malicious Threshold` field. You should now use the `Verdict` and/or `Threat Score`, `Severity`, and `Confidence Score` fields to determine if an indicator is malicious
  - Adds options to Disable proxies and enable SSL Certificate Verification.
- **Version 1.1.3**
  - Hashes - the `Last Analysis Result` attribute is no longer ingested when `Basic Properties` is enabled for the **Supporting Context** configuration field. A new option is now available for this configuration: `Last Analysis Result`.

- **Version 1.1.2**
  - Resolved a filter mapping issue when the API response is missing fields.
- **Version 1.1.1**
  - You can now retrieve information about an individual AV scan.
    - Added new **AV Scan Information** option: **Return Individual AV Scan Information**.
  - Updated minimum ThreatQ version to 5.19.0.
- **Version 1.1.0**
  - Added support for resubmitting URLs to VirusTotal to be analyzed via VirusTotal Submit URL function.
- **Version 1.0.5**
  - Resolved an issue ingesting historical SSL attributes.
- **Version 1.0.4**
  - Initial release to ThreatQ Marketplace.