ThreatQuotient

abuse.ch MalwareBazaar Action Guide

Version 1.0.0

December 20, 2022

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

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

Contents

Warning and Disclaimer

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

Support

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

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

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.6.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/abuse-ch-malwarebazaar-action

Introduction

The abuse.ch Malwarebazaar action submits data collection containing MD5, SHA-1 and SHA-256 IOCs to abuse.ch MalwareBazaar and returns Indicators, TTPs and Malware. The abuse.ch MalwareBazaar queries the submitted objects for enrichment and returns related threat intelligence to be ingested into the ThreatQ library.

The action can perform the following function:

- **abuse.ch MalwareBazaar** - submits indicators to abuse.ch MalwareBazaar to be enriched with related threat intelligence.

The action is compatible with the following indicator types:

- MD5
- SHA-1
- SHA-256

The action returns the following enriched system objects:

- Indicators
  - Indicator Attributes
- Indicator Tags
- Malware
- TTP

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:

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following indicator types:
  - MD5
  - SHA-1
  - SHA-256

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 file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action 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 action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

Configuration

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

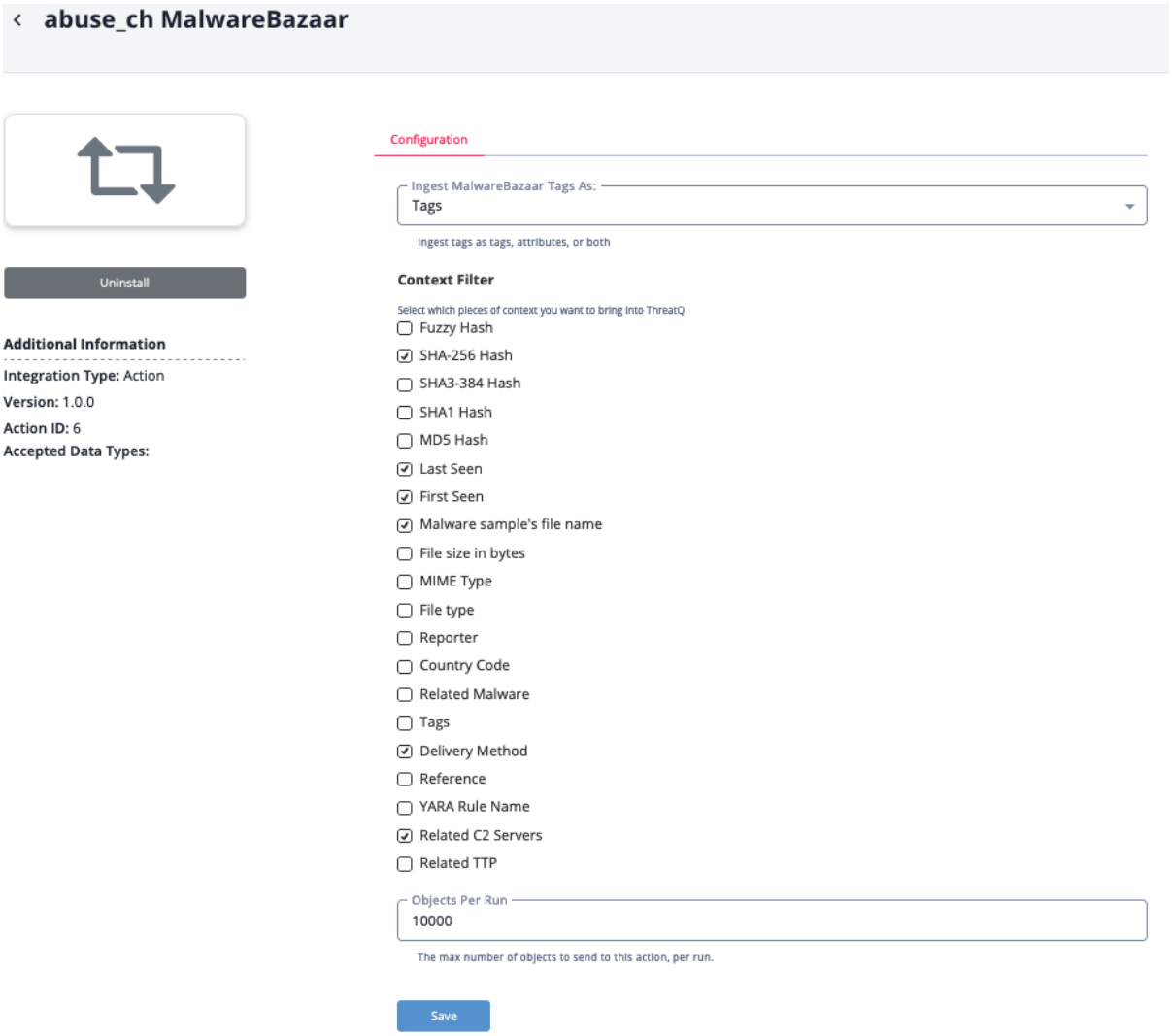
To configure the integration:

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

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

PARAMETER	DESCRIPTION
Ingest MalwareBazaar Tags As	Select how to ingest tags returned by the action. Options include: ◦ Tags (default) ◦ Attributes ◦ Both
Context Filter	Select the pieces of context to bring into ThreatQ. Options include: ◦ Fuzzy Hash ◦ SHA-256 Hash ◦ SHA-384 Hash ◦ SHA1 Hash ◦ File type ◦ Reporter ◦ Country Code

PARAMETER	DESCRIPTION
	◦ MD5 Hash ◦ Last Seen ◦ First Seen ◦ Malware sample's file name ◦ File size in bytes ◦ MIME Type ◦ Related Malware ◦ Tags ◦ Delivery Method ◦ Reference ◦ YARA Rule Name ◦ Related C2 Servers ◦ Related TTP
Objects Per Run	The max number of objects per run to send to this action. The max value for this parameter is 50,000.



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

Action Functions

The action provides the following functions

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
abuse_ch MalwareBazaar	Enriches IOCs using MalwareBazaar's API	Indicators	MD5, SHA-1, SHA-256

abuse_ch MalwareBazaar

The abuse_ch MalwareBazaar function enriches MD5, SHA-1 and SHA-256 IOCs using MalwareBazaar's API.

```
POST https://mb-api.abuse.ch/api/v1/
```

Sample Body:

```
Form URL-Encoded
query=get_info&hash=9cee5522a7ca2bfca7cd3d9daba23e9a30deb6205f56c12045839075f7627297
```

Sample Response:


```
{
  "query_status": "ok",
  "data": [
    {
      "sha256_hash": "9cee5522a7ca2bfca7cd3d9daba23e9a30deb6205f56c12045839075f7627297",
      "sha3_384_hash":
"0896178675b3349f6890ac1a270c185ca8d2ced319768f8922e9d6b967239704fa6579d61251f3b00b01d4baa
f0e9d74",
      "sha1_hash": "d1dfe82775c1d698dd7861d6dfa1352a74551d35",
      "md5_hash": "f87a2e1c3d148a67eaeb696b1ab69133",
      "first_seen": "2020-11-25 13:05:56",
      "last_seen": "2021-05-01 01:07:44",
      "file_name": "9cee5522a7ca2bfca7cd3d9daba23e9a30deb6205f56c12045839075f7627297",
      "file_size": 17408,
      "file_type_mime": "application\/x-dosexec",
      "file_type": "exe",
      "reporter": "JAMESWT_MHT",
      "origin_country": "IT",
      "anonymous": 0,
      "signature": "DarkSide",
      "imphash": "6ed4f5f04d62b18d96b26d6db7c18840",
      "tlsh": "BB72C049536D3522D20B3D36CDA29C25B086D661CB9A6DCF384EDA9DBC71D84CF7A700",
      "telfhash": null,
      "ssdeep": "384:SGyUrEk\/yEoQE+yckIYN\/pBa3AWK3T2oTboHblKR\/:l4klFypIYFpB\/x9ngb",
      "dhash_icon": null,
      "comment": null,
      "tags": [
        "DarkSide",
        "Ransomware"
      ],
      "code_sign": null,
      "delivery_method": null,
      "intelligence": {
        "clamav": null,
        "downloads": "232",
        "uploads": "2",
        "mail": null
      },
      "file_information": null,
      "ole_information": [],
      "yara_rules": [
```

```
        {
          "rule_name": "RANSOM_darkside",
          "author": "Marc Rivero | McAfee ATR Team",
          "description": "Rule to detect packed and unpacked samples of DarkSide",
          "reference": null
        },
        {
          "rule_name": "suspicious_packer_section",
          "author": "@j0sm1",
          "description": "The packer\/protector section names\/keywords",
          "reference": "http:\/\/www.hexacorn.com\/blog\/2012\/10\/14\/random-stats-
from-1-2m-samples-pe-section-names\/"
        }
      ],
      "vendor_intel": {
        "CERT-PL_MWDB": {
          "detection": null,
          "link": "https:\/\/mwdb.cert.pl\/sample\/
9cee5522a7ca2bfca7cd3d9daba23e9a30deb6205f56c12045839075f7627297\/"
        },
        "YOROI_YOMI": {
          "detection": "XPACK",
          "score": "1.00"
        },
        "vxCube": {
          "verdict": "malware2",
          "maliciousness": "100",
          "behaviour": [
            {
              "threat_level": "neutral",
              "rule": "Sending a UDP request"
            },
            {
              "threat_level": "neutral",
              "rule": "Creating a file"
            },
            {
              "threat_level": "neutral",
              "rule": "Launching a process"
            },
            {
              "threat_level": "neutral",
              "rule": "Using the Windows Management Instrumentation requests"
            },
            {
              "threat_level": "neutral",
              "rule": "Launching a service"
            },
            {
              "threat_level": "neutral",
              "rule": "Adding an access-denied ACE"
            },
            {
              "threat_level": "neutral",
              "rule": "Reading critical registry keys"
            },
            {
              "threat_level": "neutral",
              "rule": "Changing a file"
            },
            {
```

```
            "threat_level": "neutral",
            "rule": "Delayed writing of the file"
          },
          {
            "threat_level": "malicious",
            "rule": "Forced shutdown of a browser"
          },
          {
            "threat_level": "malicious",
            "rule": "Encrypting user's files"
          },
          {
            "threat_level": "suspicious",
            "rule": "Stealing user critical data"
          },
          {
            "threat_level": "suspicious",
            "rule": "Creating a file in the mass storage device "
          }
        ]
      },
      "InQuest": {
        "verdict": "MALICIOUS",
        "url": null,
        "details": [
          {
            "category": "info",
            "title": "Windows PE Executable",
            "description": "Found a Windows Portable Executable (PE) binary. Depending
on context, the presence of a binary is suspicious or malicious."
          }
        ]
      },
      "Triage": {
        "malware_family": "darkside",
        "score": "10",
        "link": "https:\/\/tria.ge\/reports\/201125-ed59r1jx9j\/",
        "tags": [
          "family:darkside",
          "ransomware",
          "spyware",
          "upx"
        ],
        "signatures": [
          {
            "signature": "DarkSide",
            "score": "10"
          },
          {
            "signature": "Modifies extensions of user files",
            "score": "8"
          },
          {
            "signature": "Reads user\/profile data of web browsers",
            "score": "7"
          },
          {
            "signature": "Suspicious behavior: EnumeratesProcesses",
            "score": null
          },
          {
```

```
              "signature": "Suspicious use of AdjustPrivilegeToken",
              "score": null
            },
            {
              "signature": "Suspicious use of WriteProcessMemory",
              "score": null
            }
          ],
          "malware_config": []
        },
        "ReversingLabs": {
          "threat_name": "Win32.Ransomware.DarkSide",
          "status": "MALICIOUS",
          "first_seen": "2020-08-08 20:29:27",
          "scanner_count": "29",
          "scanner_match": "28",
          "scanner_percent": "96.55"
        },
        "Spamhaus_HBL": [
          {
            "detection": "suspicious",
            "link": "https:\/\/www.spamhaus.org\/hbl\/"
          }
        ],
        "UnpacMe": [
          {
            "sha256_hash":
"9cee5522a7ca2bfca7cd3d9daba23e9a30deb6205f56c12045839075f7627297",
            "md5_hash": "f87a2e1c3d148a67eaeb696b1ab69133",
            "sha1_hash": "d1dfe82775c1d698dd7861d6dfa1352a74551d35",
            "detections": [],
            "link": "https:\/\/www.unpac.me\/results\/
bbccb33d-6054-4c50-970f-7e24d606e0e1\/"
          },
          {
            "sha256_hash":
"1667e1635736f2b2ba9727457f995a67201ddcd818496c9296713ffa18e17a43",
            "md5_hash": "1a700f845849e573ab3148daef1a3b0b",
            "sha1_hash": "c91ff86a88038b00d9190ebb01e6f8c94b0c83e0",
            "detections": [],
            "link": "https:\/\/www.unpac.me\/results\/
bbccb33d-6054-4c50-970f-7e24d606e0e1\/"
          }
        ],
        "VMRay": {
          "verdict": "malicious",
          "malware_family": "",
          "report_link": "https:\/\/www.vmray.com\/analyses\/9cee5522a7ca\/report\/
overview.html"
        }
      },
      "comments": null
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this function:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	
`.tags`	Indicator.Tag	N/A	N/A	N/A	`Emotet`	If enabled and 'tag' selected
`.tags`	Indicator.Attribute	Tag	N/A	`.first_seen`	`Emotet`	If enabled and 'attribute' selected
`.first_seen`	Indicator.Attribute	First Seen	N/A	`.first_seen`	`2021-01-22 15:23:01`	If enabled
`.last_seen`	Indicator.Attribute	Last Seen	N/A	`.first_seen`	`2021-05-01 01:07:44`	If enabled
`.file_size`	Indicator.Attribute	File Size (bytes)	N/A	`.first_seen`	`177664`	If enabled
`.file_type_mime`	Indicator.Attribute	MIME Type	N/A	`.first_seen`	`application\/msword`	If enabled
`.file_type`	Indicator.Attribute	File Type	N/A	`.first_seen`	`docx`	If enabled
`.reporter`	Indicator.Attribute	Reporter	N/A	`.first_seen`	`Cryptolaemus1`	If enabled
`.origin_country`	Indicator.Attribute	Origin Country	N/A	`.first_seen`	`FR`	If enabled
`.delivery_method`	Indicator.Attribute	Delivery Method	N/A	`.first_seen`	`Web Download`	If enabled
`.file_information`	Indicator.Attribute	Reference	N/A	`.first_seen`	`https://urlhaus.abuse.ch/url/972626/`	If enabled
`.yara_rules`	Indicator.Attribute	Rule Name	N/A	`.first_seen`	`SUSP_XORed_URL_in_EXE`	If enabled
`.c2`	Indicator.Attribute	Port	Split by :	`.first_seen`	N/A	If enabled, when context is 'c2'
`.md5_hash`	Related Indicator.Value	MD5	N/A	`.first_seen`	`f87a2e1c3d148a67eaeb696b1ab69133`	If enabled
`.sha1_hash`	Related Indicator.Value	SHA-1	N/A	`.first_seen`	`d1dfe82775c1d698dd7861d6dfa1352a74551d35`	If enabled
`.sha256_hash`	Related Indicator.Value	SHA-256	N/A	`.first_seen`	`9cee5522a7ca2bfca7cd3d9daba23e9a30deb6205f56c12045839075f7627297`	If enabled
`.sha3_384_hash`	Related Indicator.Value	SHA-384	N/A	`.first_seen`	`0896178675b3349f6890ac1a270c185ca8d2ced319768f8922e9d6b967239704fa6579d61251f3b00b01d4baaf0`	If enabled

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	
					`e9d 74`	
`.file_name`	Related Indicator.Value	Filename	N/A	`.first_seen`	`emotet_e2_9e2c5e 3ffc 4db3771082aa0ed3 a6c3 0821f0545c540f65 41d0 87d1e65e733cde_2 021`	If enabled
`.c2`	Related Indicator.Value	URL	N/A	`.first_seen`	N/A	If enabled, when context is 'dropper'
`.c2`	Related Indicator.Value	Ip Address	Split by :	`.first_seen`	N/A	If enabled, when context is 'c2'
`.triage_ttp`	Related TTP.Value	N/A	N/A	`.first_seen`	`Process spawned unexpected child process`	If enabled
`.signature`	Related Malware.Value	N/A	N/A	`.first_seen`	`Heodo`	If enabled
`.ssdeep`	Related Indicator.Value	Fuzzy Hash	N/A	`.first_seen`	`384:SGyUrEk\/ yEoQE+yc kIYN\/ pBa3AWK3T2oTbo HblKR\/:l4klFypI YFpB \/x9ngb`	If enabled

Enriched Data

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

METRIC	RESULT
Run Time	2 minute
Indicators	150
Indicator Attributes	1,456
Indicator Tags	25
Malware	76
TTP	35

Use Case Example

1. A user submits a data collection using the abuse.ch MalwareBazaar action to the abuse.ch MalwareBazaar with a data collection containing 350 system objects (100 MD5, 75 SHA-1, 75 SHA-256).
2. The abuse.ch MalwareBazaar queries the submitted data.
3. The action returns the submitted data collection enriched with the following:
    - 99 Indicators
    - 30 Indicator Attributes
    - 20 Indicator Tags
    - 3 Malware
    - 5 TTP

Change Log

- **Version 1.0.0**
  - Initial release