ThreatQuotient

Malpedia Implementation Guide

Version 1.0.0

Wednesday, April 22, 2020

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.

Last Updated: Wednesday, April 22, 2020

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.25.0`

Introduction

The Malpedia Integration for ThreatQ allows a user to ingest Malware, Actors, and YARA Rules from Malpedia.

Endpoints:

- `https://malpedia.caad.fkie.fraunhofer.de/api/get/families`
- `https://malpedia.caad.fkie.fraunhofer.de/api/list/actors`
- `https://mal-pedia.caad.fkie.fraunhofer.de/api/get/yara/after`

Installation

Perform the following steps to install the feed:

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

1. Log into https://marketplace.threatq.com/.
2. Locate and download the **Malpedia** feeds file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Incoming feeds**.
5. Click on the **Add New Feed** button.
6. Upload the feed file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the feed 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.

The feeds will be added to the **OSINT** tab for Incoming Feeds. You will still need to configure and then enable the feed.

ThreatQ UI 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. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feed under the **OSINT** tab.
3. Click on the **Feed Settings** link for the feed.
4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
API Token	This parameter is optional. Malpedia does not require an API token; however, more threat intelligence can be ingested by having one.

5. Click on **Save Changes**.
6. Click on the toggle switch to the left of the feed name to enable it.

ThreatQ Mapping

Malpedia Malware (Feed)

This feed will ingest malware and related actors and YARA rules into ThreatQ.

```
GET https://malpedia.caad.fkie.fraunhofer.de/api/get/families
```


```
      {
  "win.sparksrv": {
       "updated": "2020-01-23",
       "library_entries": [
              "team:20120326:luckycat:b7b4f63"
       ],
       "attribution": [],
       "description": "",
       "notes": [],
       "alt_names": [],
       "sources": [],
       "urls": [
              "https://www.trendmicro.com/vinfo/us/security/news/cyber-
attacks/luckycat-redux-campaign-attacks-multiple-targets-in-
india-and-japan"
       ],
       "common_name": "Sparksrv",
       "uuid": "1937c3e0-569d-4eb4-b769-ae5d9cc27755"
},
"win.sslmm": {
       "updated": "",
       "library_entries": [
```

```
        "baumgartner:20150514:naikon:9edea2f",
        "baumgartner:201505:msnmm:13a9145",
        "fireeye:201504:apt30:0129bf7"
      ],
      "attribution": [
        "Naikon"
      ],
      "description": "",
      "notes": [],
      "alt_names": [],
      "sources": [],
      "urls": [
        "https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf",
        "https://securelist.com/analysis/publications/69953/the-naikon-apt/",
        "https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/TheNaikonAPT-MsnMM1.pdf"
      ],
      "common_name": "SslMM",
      "uuid": "009db412-762d-4256-8df9-eb213be01ffd"
      }
}
```


Enrichment data is also polled from the following URL for each Malware name, (Eg `win.s-parksrv`):

```
GET https://malpedia.caad.fkie.fraunhofer.de/api/get/yara/{{Mal-ware Name}}
```

```
{
       "tlp_white": {
         "win.poulight_stealer_w0.yar": "rule win_poulight_w0 {\r\n
  meta:\r\n        description = \"Poullight stealer\"\r\n
   author = \"James_inthe_box\"\r\n        reference =
\"https://app.any.run/tasks/d9e4933b-3229-4cb4-84e6-
c45a336b15be/\"\r\n        date = \"2020/03\"\r\n
maltype = \"Stealer\"\r\n        malpedia_reference =
\"https://malpedia.caad.fkie.fraunhofer.de/details/win.pouligh
t_stealer\"\r\n        malpedia_version = \"20200325\"\r\n
   malpedia_sharing = \"TLP:WHITE\"\r\n        \r\n
strings:\r\n        $string1 = \"[LOGS]\" wide\r\n
$string2 = \"Org.BouncyCastle.Crypto.Prng\" ascii\r\n
$string3 = \"lookupPowX2\" ascii\r\n\r\n    condition:\r\n
   uint16(0) == 0x5A4D and \r\n        all of ($string*) and
\r\n        filesize < 400KB\r\n}",
         "win.vidar_w0.yar": "rule win_vidar_w0 {\n    meta:\n
 description = \"Yara rule for detecting Vidar stealer\"\n
   author = \"Fumik0_\"\n        malpedia_reference =
\"https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar\"
\n        malpedia_version = \"2019-01-06\"\n        malpedia_
license = \"CC BY-NC-SA 4.0\"\n        malpedia_sharing =
\"TLP:WHITE\"\n\n    strings:\n        $s1 = { 56 69 64 61 72
}\n        $s2 = { 31 42 45 46 30 41 35 37 42 45 31 31 30 46
44 34 36 37 41 }\n        \n    condition:\n        all of
them\n}"
       }
}
```

ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
key.common_name	Malware	N/A	Trickbot	N/A
key.alt_names[]	Malware	N/A	NanoCore RAT	These are inter-related with the "common name"
key.attribution	Adversary	N/A	APT1	All APT names have spaces stripped from them for consistency
key.description	Malware.Attribute	Description	Some Text	
key.notes	Malware.Attribute	Note	Some Note	N/A
key.urls	Malware.Attribute	Reference	N/A	N/A
key	Malware.Attribute	Malpedia Link	N/A	This key is formatted into a URL like `https://malpedia.caad.fkie.fraunhofer.de/details/{{data.name}}`

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
key.key	Signature	YARA	See rules above	Each returned YARA rule for the Malware in question will be parsed as a Signature
key.key.attributes	Signature.Attribute	<varies>	N/A	YARA metadata is converted to attributes

Average Feed Run

Metric	Result
Run Time	36 minutes
Adversaries	157
Malware	2210
Malware Attributes	11601
Signatures	1199
Signature Attributes	10559

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

Malpedia Threat Actors (Feed)

This feed will ingest threat actors into ThreatQ.

```
GET https://malpedia.caad.fkie.fraunhofer.de/api/list/actors
```

```
[
	"[unnamed_group]",
	"[vault_7_8]",
	"_stealth_mango_and_tangelo_",
	"allanite",
	"anchor_panda",
	"andromeda_spider",
	"anthropoid_spider"
]
```

Enrichment data is then polled from:

```
GET https://malpedia.caad.fkie.fraunhofer.de/api/get/actor/
{{Actor Name}}
```

```
{
	"uuid" : "9f133738-935f-11e9-aa5e-bbf8d91abb46",
	"families" :
		{
		},
	"description" : "An unnamed source leaked almost 10,000
documents describing a large number of 0-day vulnerabilities,
methodologies and tools that had been collected by the CIA.
This leaking was done through WikiLeaks, since March 2017. In
```

weekly publications, the dumps were said to come from Vault 7 and later Vault 8, until his arrest in 2018.\nMost of the published vulnerabilities have since been fixed by the respective vendors, by many have been used by other threat actors. This actor turned out to be a former CIA software engineer.\n(WikiLeaks) Today, Tuesday 7 March 2017, WikiLeaks begins its new series of leaks on the U.S. Central Intelligence Agency. Code-named \"Vault 7\" by WikiLeaks, it is the largest ever publication of confidential documents on the agency.\nThe first full part of the series, \"Year Zero\", comprises 8,761 documents and files from an isolated, high-security network situated inside the CIA\"s Center for Cyber Intelligence in Langley, Virgina. It follows an introductory disclosure last month of CIA targeting French political parties and candidates in the lead up to the 2012 presidential election.\nRecently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized \"zero day\" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive.\n\"Year Zero\" introduces the scope and direction of the CIA\"s global covert hacking program, its malware arsenal and dozens of \"zero day\" weaponized exploits against a wide range of U.S. and European company products, include Apple\"s iPhone, Google\"s Android and Microsoft\"s

```
Windows and even Samsung TVs, which are turned into covert
microphones.",
       "meta" :
         {
               "refs" :
                       [
                         "https://wikileaks.org/ciav7p1/",
                         "https://www.justice.gov/opa/pr/joshua-adam-sch
charged-unauthorized-disclosure-classified-information-and-
other-offenses"
                       ],
               "victimology": "Government, Military",
               "mode-of-operation": "Discrete",
               "capabilities": "Control, Infiltration",
               "synonyms":
                       [
                         "Vault 7",
                         "Vault 8"
                       ],
               "cfr-suspected-victims": [],
               "country": "USA",
               "cfr-target-category": [],
               "cfr-type-of-incident": "",
               "attribution-confidence": "",
               "cfr-suspected-state-sponsor": ""
               },
       "value" : "[Vault 7/8]"
}
```

ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.value	Adversary	N/A	APT1	All APT names have spaces stripped from them for consistency
.meta.synonyms	Adversary	N/A	APT15	These are inter-related with the parent adversary
.meta.capabilities	Malware	N/A	Mimikatz	
.description	Adversary.Attribute	Description	An unnamed source leaked almost 10,000 documents describing a large number of 0-day ...	
.meta.victimology	Adversary.Attribute	Victimology	Europe	This is a comma-separated list, parsed
.meta.refs	Adversary.Attribute	Reference	https://wikileaks.org/ciav7p1/	
.meta.mode-of-operation	Adversary.Attribute	Mode of Operation	N/A	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.meta.cfr-suspected-victims	Adversary.Attribute	Suspected Victim	Sweden	
.meta.country	Adversary.Attribute	Country	CN	
.meta.cfr-target-category	Adversary.Attribute	Target Sector	Government	
.meta.cfr-type-of-incident	Adversary.Attribute	Incident Type	Espionage	
.meta.attribution-confidence	Adversary.Attribute	Confidence	N/A	
.meta.cfr-suspected-state-sponsor	Adversary.Attribute	Suspected State Sponsor	China	

Average Feed Run

Metric	Result
Run Time	7 minutes
Adversaries	769
Adversary Attributes	13513
Malware	20

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

Malpedia YARA Rules (Feed)

This feed will ingest YARA Signatures into ThreatQ.

```
GET https://malpedia.caad.fkie.fraunhofer.de/api/get/yara/after
```


```
{
       "tlp_white": {
         "win.poulight_stealer_w0.yar": "rule win_poulight_w0 {\r\n
  meta:\r\n        description = \"Poullight stealer\"\r\n
   author = \"James_inthe_box\"\r\n        reference =
\"https://app.any.run/tasks/d9e4933b-3229-4cb4-84e6-
c45a336b15be/\"\r\n        date = \"2020/03\"\r\n
maltype = \"Stealer\"\r\n        malpedia_reference =
\"https://malpedia.caad.fkie.fraunhofer.de/details/win.pouligh
t_stealer\"\r\n        malpedia_version = \"20200325\"\r\n
   malpedia_sharing = \"TLP:WHITE\"\r\n        \r\n
strings:\r\n        $string1 = \"[LOGS]\" wide\r\n
$string2 = \"Org.BouncyCastle.Crypto.Prng\" ascii\r\n
$string3 = \"lookupPowX2\" ascii\r\n\r\n    condition:\r\n
   uint16(0) == 0x5A4D and \r\n        all of ($string*) and
\r\n        filesize < 400KB\r\n}",
         "win.vidar_w0.yar": "rule win_vidar_w0 {\n    meta:\n
 description = \"Yara rule for detecting Vidar stealer\"\n
   author = \"Fumik0_\"\n        malpedia_reference =
\"https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar\"
\n        malpedia_version = \"2019-01-06\"\n        malpedia_
license = \"CC BY-NC-SA 4.0\"\n        malpedia_sharing =
\"TLP:WHITE\"\n\n    strings:\n        $s1 = { 56 69 64 61 72
}\n        $s2 = { 31 42 45 46 30 41 35 37 42 45 31 31 30 46
```

```
44 34 36 37 41 }\n        \n    condition:\n        all of
them\n}"
        }
}
```

ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
key.key	Signature	YARA	See rules above	
key.key.attributes	Signature.Attribute	<varies>	N/A	YARA metadata is converted to attributes

Average Feed Run

Metric	Result
Run Time	1 minute
Signatures	2
Signature Attributes	14

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

Known Issues/Limitations

- Both the Threat Actor and Malware feeds ingest the entire dataset each time. This is due to a Malpedia API limitation. It is advised you schedule this to run daily, not hourly.

Change Log

- **Version 1.0.0**
  - Initial Release