ThreatQuotient

FireEye Intelligence Reports CDF Guide

Version 1.3.5

January 04, 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: `1.3.5`
- Supported on ThreatQ versions >= `4.34.0`

Introduction

The FireEye Intelligence Reports integration allows a user to ingest threat intelligence reports from FireEye's API using the following endpoints:

- `https://api.isightpartners.com/help/settings`
- `https://api.isightpartners.com/report/index`
- `https://api.isightpartners.com/report/{reportID}`

Notes

- Time constrained data fetching is possible.
  - The time range specified should not exceed 90 days.
- The FireEye API uses HMAC-based HTTP auth.

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
FireEye API Public Key	The FireEye account API Key
FireEye API Private Key	The FireEye account Secret Key
Ingest CPEs	When checked, the feed will ingest CPEs. Unchecked by default.

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

FireEye Intelligence Reports (Feed)

```
GET https://api.isightpartners.com/help/settings
```

For manual runs, the request will contain `startDate` and `endDate` parameters to determine which reports to return for the specified time range. If the time range exceeds 90 days, the `endDate` parameter will automatically be set to 90 days from the `startDate`.

For every run, this feed makes a call to the API User Settings endpoint to determine the user's `totalRemainingQueries`. If `totalRemainingQueries` is below 2,000 queries, the feed run will complete without making any additional API calls or ingesting any threat intelligence data to avoid having the user's account blacklisted. If the user's `totalRemainingQueries` is above the threshold, the feed will make a call to the API Report Index endpoint to retrieve a list of all of the report IDs for the specified time range. A subsequent API call is made to the Report Download endpoint to retrieve an intelligence report for each report ID in the list.

FireEye Reports Index (Supplemental)

```
GET https://api.isightpartners.com/report/index
```


```
{
    "success": true,
    "message": [
        {
            "reportId": "20-00004785",
            "title": "Adobe Photoshop 2020 21.1 Out-of-Bounds Write Vulnerability",
            "ThreatScape": [
                "Vulnerability"
            ],
            "audience": [
                "Vulnerability"
            ],
            "publishDate": 1584565920,
            "version": "1",
            "version1PublishDate": 1584565920,
            "intelligenceType": "vulnerability",
            "reportType": "Vulnerability Report",
            "reportLink": "https://api.isightpartners.com/report/20-00004785",
            "webLink": "https://intelligence.fireeye.com/reports/20-00004785"
        },
        {
            "reportId": "19-00017683",
            "title": "Oracle Java SE 13 2D Input Validation Vulnerability",
            "ThreatScape": [
                "Vulnerability"
            ],
            "audience": [
                "Vulnerability"
            ],
            "publishDate": 1584564780,
            "version": "25",
            "version1PublishDate": 1571231760,
            "intelligenceType": "vulnerability",
            "reportType": "Vulnerability Report",
            "reportLink": "https://api.isightpartners.com/report/19-00017683",
            "webLink": "https://intelligence.fireeye.com/reports/19-00017683"
        },
        {
            "reportId": "19-00017679",
            "title": "Oracle Java SE 13 Serialization Uncaught Exception Vulnerability",
            "ThreatScape": [
                "Vulnerability"
            ],
            "audience": [
                "Vulnerability"
            ],
            "publishDate": 1584564780,
            "version": "42",
            "version1PublishDate": 1571231700,
            "intelligenceType": "vulnerability",
            "reportType": "Vulnerability Report",
            "reportLink": "https://api.isightpartners.com/report/19-00017679",
            "webLink": "https://intelligence.fireeye.com/reports/19-00017679"
        }
    ]
```

```
}
```


Report Download (Supplemental)

```
GET https://api.isightpartners.com/report/{reportID}
```


```
{
    "success": true,
    "message": {
        "report": {
            "accessComplexity": "AC:M",
            "accessVector": "AV:N",
            "analysis": "<div>Smoke Loader builds are offered at varying degrees of functionality based on price...",
            "attackingEase": "Moderate",
            "audience": [
                "Operational"
            ],
            "authentication": "Au:S",
            "availabilityImpact": "A:P",
            "confidentialityImpact": "C:C",
            "copyright": "© Copyright 2020 FireEye, Inc. All rights reserved.",
            "cveIds": {
                "cveId": [
                    "CVE-2020-14296"
                ]
            },
            "cvssBaseScore": "7.5",
            "cvssTemporalScore": "5.5",
            "dateOfDisclosure": "August 02, 2020 11:00:00 PM",
            "execSummary": "<p>Smoke Loader (aka Smoke Bot or Dofoil) is a modular downloader that can serve a range
of...",
            "exploitability": "E:U",
            "exploitation": {
                "inTheWild": false,
                "zeroDay": false
            },
            "exploitationConsequence": "Code Execution",
            "exploitationVectors": {
                "exploitationVector": [
                    "General Network Connectivity"
                ]
            },
            "exploitRating": "No Known",
            "integrityImpact": "I:P",
            "intelligenceType": "malware",
            "mitigations": {
                "mitigation": [
                    "Patch"
                ]
            },
            "mitigationDetails": "\u003cp\u003eMandiant has not evaluated this vulnerability...",
            "previousVersionSection": {
                "previousVersion": [
                    {
                        "versionNumber": "1.0",
                        "title": "Indicator Report: Smoke Loader Activity Report (Mar 23, 2020)",
                        "publishDate": "March 24, 2020 05:44:00 AM"
                    }
                ]
```

```
},
"publishDate": "March 24, 2020 05:44:00 AM",
"remediationLevel": "RL:OF",
"reportConfidence": "RC:C",
"reportId": "20-00005120",
"reportType": "Indicator Report",
"riskRating": "LOW",
"sourceSection": {
    "source": [
        {
            "title": "Red Hat Inc.",
            "urls": {
                "url": [
                    "https://access.redhat.com/errata/RHSA-2020:3358"
                ]
            },
            "description": "RHSA-2020:3358",
            "date": "August 06, 2020 07:00:00 AM"
        },
        ...
    ]
},
"tagSection": {
    "files": {
        "file": [
            {
                "identifier": "Related",
                "type": "fileType",
                "md5": "01d0862ab2b38b3395d255dc34b4a476",
                "malwareFamily": "smokeloader",
                "malwareFamilyId": "95223862-dbf0-4ad9-b2f0-358c6013f227"
            },
            {
                "identifier": "Related",
                "type": "fileType",
                "md5": "06037d2fdb18ab0ad7e9c6ab0b90f6f2",
                "malwareFamily": "smokeloader",
                "malwareFamilyId": "95223862-dbf0-4ad9-b2f0-358c6013f227"
            },
            {
                "identifier": "Related",
                "type": "fileType",
                "md5": "0d8106afb39f7f49342c68f1e09e6f24",
                "malwareFamily": "smokeloader",
                "malwareFamilyId": "95223862-dbf0-4ad9-b2f0-358c6013f227"
            },
            ...
        ]
    },
    "main": {
        "actors": {
            "actor": [
                  {
                      "name": "Till Kottmann",
                      "id": "cead5ff2-4356-460d-9b27-e31f9fdce650"
                  }
            ]
        },
        "affectedIndustries": {
            "affectedIndustry": [
              "Telecommunications",
              "Technology",
              "Financial Services"
```

```
            ]
        },
        "affectedSystems": {
            "affectedSystem": [
                "Users/Application and Software"
            ]
        },
        "intendedEffects": {
            "intendedEffect": [
                "Disruption",
                "Identity Theft",
                "IP or Business Information Theft",
                "Degradation"
            ]
        },
        "malwareFamilies": {
            "malwareFamily": [
                {
                    "id": "95223862-dbf0-4ad9-b2f0-358c6013f227",
                    "name": "smokeloader"
                }
            ]
        },
        "targetGeographies": {
            "targetGeography": [
                "Mexico",
                "Peru",
                "Chile",
                "Colombia"
            ]
        },
        "ttps": {
            "ttp": [
                "Malware Propagation and Deployment",
                "Enabling Infrastructures",
                "Distributed Denial-of-Service (DDoS) Attack",
                "Domain Registration/DNS Abuse and Manipulation"
            ]
        },
    },
    "networks": {
        "network": [
            {
                "ip": "185.35.137.147",
                "identifier": "Attacker",
                "networkType": "network",
                "malwareFamily": "smokeloader",
                "malwareFamilyId": "95223862-dbf0-4ad9-b2f0-358c6013f227"
            },
            {
                "domain": "shopandpop.su",
                "identifier": "Attacker",
                "networkType": "network",
                "malwareFamily": "smokeloader",
                "malwareFamilyId": "95223862-dbf0-4ad9-b2f0-358c6013f227"
            },
            {
                "identifier": "Attacker",
                "networkType": "url",
                "url": "http://185.35.137.147/mlp/",
                "malwareFamily": "smokeloader",
                "malwareFamilyId": "95223862-dbf0-4ad9-b2f0-358c6013f227"
            },
```

```
                    ...
                ]
            }
        },
        "technologySection": {
            "technologies": [
                {
                    "vendor": "redhat",
                    "cpe": "cpe:2.3:a:redhat:cloudforms:5.0:*:*:*:*:*:*:*",
                    "technologyName": "cloudforms 5.0",
                    "cpeTitle": "redhat cloudforms 5.0"
                },
                ...
            ]
        },
        "title": "Indicator Report: Smoke Loader Activity Report (Mar 23, 2020)",
        "threatDetail": "\u003cp style\u003d\"margin: 0in 0in 0.0001pt; font-size: 10pt; font-family: ...",
        "ThreatScape": {
            "product": [
                "ThreatScape Cyber Crime"
            ]
        },
        "vendorFix": "\u003cp\u003eAll known fixes, or information on obtaining the fixes...",
        "vendorFixUrls": {
            "vendorFixUrl": [
                {
                    "name": "CloudForms Management Engine 5.11 (RHSA-2020:3358) Security Update Information",
                    "url": "https://access.redhat.com/errata/RHSA-2020:3358"
                }
            ]
        },
        "version": "1",
        "version1PublishDate": "March 24, 2020 05:44:00 AM",
        "vulnerableProducts": "\u003cp\u003eThe following vendors/products have been...",
        "vulnerabilityTypes": {
            "vulnerabilityType": "Unknown"
        }
    }
},
"user_name": "ThreatQAPI2Dev"
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.message.report.title	report.value	N/A	.message.report.publishDate	Apache Thrift 0.12.0 Infinite Loop Vulnerability	N/A
.message.report.overview	report.description	N/A	N/A	An authentication issues vulnerability exists within IBM WebSphere eXtreme Scale 8.6 and earlier that, when exploited, allows an attacker to remotely conduct brute force attacks and bypass password security restrictions. Exploit code is not publicly available. Mitigation options include a vendor fix. Exploitation Rating: No Known. iSIGHT Partners considers this a Low-risk vulnerability due to the limited impact of exploitation. Customers with specific questions regarding this vulnerability can contact the Vulnerability & Exploitation Team at analystaccess@isightpartners.com.	The object description is formatted from `.message.report.overview`, as well as `.message.report.reportType`, `.message.report.vulnerabilityTypes`, `.message.report.analysis`, `.message.report.threatDetail`, `.message.report.threatDescription`, `.message.report.vendorFix`, `.message.report.vulnerableProducts`, and `.message.report.mitigationDetails` (when these fields are present). If a description's length exceeds 32,760 characters, it will be truncated and the string `...[Truncated - see full report]` will be appended to the description.
.message.report.publishDate	report.attribute	Published At	N/A	March 24, 2020 05:44:00 AM	N/A
.message.report.ThreatScape.product[]	report.attribute / indicator.attribute	Threat Scape	.message.report.publishDate	ThreatScape Cyber Crime	N/A
.message.report.execSummary	report.attribute	Executive Summary	.message.report.publishDate	Smoke Loader (aka Smoke Bot or Dofoil) is a modular downloader that can serve a range of malicious purposes for a cyber crime actor. Smoke Loader is widely available on underground Russian forums by the user "SmokeLdr" and has been in distribution since as early as June 2011. Smoke Loader developers steadily continue to add functionality to the bot, typically in the form of new modules or plugins. The majority of these modules	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
				are focused on stealing information and credentials from infected bots, but there are also plugins designed for hidden surveillance, loading additional malware and distributed denial-of-service (DDoS) attacks.	
.message.report.execSummary	attack_pattern.value	N/A	N/A	A spear-phishing campaign targeting U.S.-based academics is leveraging a novel technique to deliver a malicious payload (probably BEACON) via an archive hosted on GitHub.The incident highlights the risk to academics and global organizations with relationships or interests in Central Asia, especially Uyghur communities.Please see the Technical Annex for YARA rules and suggested mitigations and detections (MITRE ATT&CK T1002, T1027, T1032, T1035, T1050, T1071, T1038, and T1056).	If `.message.report.execSummary` contains any MITRE ATT&CK attack pattern IDs for MITRE ATT&CK attack patterns that already exist in the ThreatQ system, the associated attack patterns are related to the report.
.message.report.audience[]	report.attribute	Audience	.message.report.publishDate	Operational	N/A
.message.report.version	report.attribute	Audience	.message.report.publishDate	1	N/A
.message.report.reportType	report.attribute	Report Type	.message.report.publishDate	Current Intelligence	N/A
.message.report.reportId	report.attribute	Report ID	.message.report.publishDate	19-00019601	N/A
(see `Notes` column)	report.attribute	Report Link	.message.report.publishDate	https://api.isightpartners.com/report/19-00019601	API URL of the report, generated from the Report ID
(see `Notes` column)	report.attribute	Web Link	.message.report.publishDate	https://intelligence.fireeye.com/reports/19-00019601	Web URL of the report, generated from the Report ID
.message.report.previousVersionSection.previousVersion[].versionNumber	report.attribute	Previous Version Number	.message.report.publishDate	1.0	If multiple `previousVersion` objects exist, only the most recent `previousVersion` object is reported.
.message.report.previousVersionSection.previousVersion[].title	report.attribute	Previous Version Title	.message.report.publishDate	Indicator Report: Smoke Loader Activity Report (Mar 23, 2020)	N/A
.message.report.previousVersionSection.previousVersion[].publishDate	report.attribute	Previous Version Date	.message.report.publishDate	March 24, 2020 05:44:00 AM	N/A
.message.report.sourceSection.source[].urls.url[]	report.attribute	Source URL	.message.report.publishDate	https://www-304.ibm.com/support/docview.wss?uid=swg21966045	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.message.report.technologySection.technologies[].cpe	report.attribute / adversary.attribute / malware.attribute	CPE	.message.report.publishDate	cpe:2.3:a:ibm:websphere_extreme_scale:8.5.0:::::::*	Ingestion is conditional, depending on whether the **Ingest CPEs** user field is checked.
.message.report.vulnerableProducts	report.attribute / adversary.attribute / malware.attribute	Vulnerable Products	.message.report.publishDate	IBM reports that WebSphere eXtreme Scale versions 7.1.0, 7.1.1, 8.5 and 8.6 are vulnerable.	N/A
.message.report.mitigations.mitigation[]	report.attribute / adversary.attribute / malware.attribute	Mitigation	.message.report.publishDate	Patch	N/A
.message.report.mitigationDetails	report.attribute / adversary.attribute / malware.attribute	Mitigation Details	.message.report.publishDate	Aside from the available vendor fix, iSIGHT Partners is unaware of any alternate mitigation procedures for this vulnerability.	N/A
.message.report.vulnerabilitytypes.vulnerabilityType	report.attribute / adversary.attribute / malware.attribute	Vulnerability Types	.message.report.publishDate	Authentication Issues	N/A
.message.report.vendorFix	report.attribute / adversary.attribute / malware.attribute	Vendor Fix	.message.report.publishDate	IBM released a fix that reportedly addresses this vulnerability. The fix, or information on obtaining the fix, can be retrieved from the following location:	N/A
.message.report.vendorFixUrls.VendorFixUrl[].name	report.attribute / adversary.attribute / malware.attribute	Vendor Fix Name	.message.report.publishDate	IBM WebSphere eXtreme Scale (1966045) Security Update Information	N/A
.message.report.vendorFixUrls.VendorFixUrl[].url	report.attribute / adversary.attribute / malware.attribute	Vendor Fix URL	.message.report.publishDate	https://www-304.ibm.com/support/docview.wss?uid=swg21966045	N/A
.message.report.confidentialityImpact	report.attribute / adversary.attribute / malware.attribute	Confidentiality Impact	.message.report.publishDate	C:N	N/A
.message.report.accessVector	report.attribute / adversary.attribute / malware.attribute	Access Vector	.message.report.publishDate	AV:N	N/A
.message.report.accessComplexity	report.attribute / adversary.attribute / malware.attribute	Access Complexity	.message.report.publishDate	AC:L	N/A
.message.report.authentication	report.attribute / adversary.attribute / malware.attribute	Authentication	.message.report.publishDate	Au:N	N/A
.message.report.integrityImpact	report.attribute / adversary.attribute / malware.attribute	Integrity Impact	.message.report.publishDate	I:P	N/A
.message.report.availabilityImpact	report.attribute / adversary.attribute / malware.attribute	Availability Impact	.message.report.publishDate	A:N	N/A
.message.report.exploitability	report.attribute / adversary.attribute / malware.attribute	Exploitability	.message.report.publishDate	E:U	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.message.report.remediationLevel	report.attribute / adversary.attribute / malware.attribute	Remediation Level	.message.report.publishDate	RL:OF	N/A
.message.report.reportConfidence	report.attribute / adversary.attribute / malware.attribute	Report Confidence	.message.report.publishDate	RC:C	N/A
.message.report.cvssBaseScore	report.attribute / adversary.attribute / malware.attribute	CVSS Base Score	.message.report.publishDate	5	N/A
.message.report.cvssBaseVector	report.attribute / adversary.attribute / malware.attribute	CVSS Base Vector	.message.report.publishDate	(AC:L/A:N/Au:N/I:P/C:N/AV:N)	N/A
.message.report.cvssBaseScoreLink	report.attribute / adversary.attribute / malware.attribute	CVSS Base Score Link	.message.report.publishDate	http://nvd.nist.gov/cvss.cfm?version=2&name=&vector=(AC:L/A:N/Au:N/I:P/C:N/AV:N)	N/A
.message.report.cvssTemporalScore	report.attribute / adversary.attribute / malware.attribute	CVSS Temporal Score	.message.report.publishDate	3.7	N/A
.message.report.cvssTemporalVector	report.attribute / adversary.attribute / malware.attribute	CVSS Temporal Vector	.message.report.publishDate	(RL:OF/RC:C/E:U)	N/A
.message.report.cvssTemporalScoreLink	report.attribute / adversary.attribute / malware.attribute	CVSS Temporal Score Link	.message.report.publishDate	http://nvd.nist.gov/cvss.cfm?version=2&name=&vector=(AC:L/A:N/Au:N/I:P/C:N/AV:N/RL:OF/RC:C/E:U)	N/A
.message.report.riskRating	report.attribute / adversary.attribute / malware.attribute	Risk Rating	.message.report.publishDate	LOW	N/A
.message.report.exploitRating	report.attribute / adversary.attribute / malware.attribute	Exploit Rating	.message.report.publishDate	No Known	N/A
.message.report.cveIds.cveId[]	Value	Indicator	.message.report.publishDate	CVE-2015-2030	Indicator type is CVE. Indicator objects are related to the primary Report object.
.message.report.dateOfDisclosure	report.attribute / adversary.attribute / malware.attribute	Date Of Disclosure	.message.report.publishDate	September 07, 2015 01:00:00 AM	N/A
.message.report.attackingEase	report.attribute / adversary.attribute / malware.attribute	Attacking Ease	.message.report.publishDate	Easy	N/A
.message.report.exploitationConsequence	report.attribute / indicator.attribute / adversary.attribute / malware.attribute	Exploitation Consequence	.message.report.publishDate	Security Bypass	N/A
.message.report.exploitationVectors.exploitationVector[]	report.attribute / adversary.attribute / malware.attribute	Exploitation Vectors	.message.report.publishDate	General Network Connectivity	N/A
.message.report.exploitation.zeroDay	report.attribute / adversary.attribute / malware.attribute	Exploitation: Zero Day	.message.report.publishDate	false	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.message.report.exploitation.inTheWild	report.attribute / adversary.attribute / malware.attribute	Exploitation: In The Wild	.message.report.publishDate	false	N/A
.message.report.copyright	report.attribute / adversary.attribute / malware.attribute	Copyright	.message.report.publishDate	Copyright 2016 FireEye, Inc. All rights reserved.	N/A
.message.report.intelligenceType	report.attribute / adversary.attribute / malware.attribute	Intelligence Type	.message.report.publishDate	malware	N/A
.message.report.tagSection.main.languages.language[]	report.attribute / adversary.attribute / malware.attribute	Language	.message.report.publishDate	English	N/A
.message.report.tagSection.main.affectedIndustries.affectedIndustry[]	report.attribute / adversary.attribute / malware.attribute	Affected Industry	.message.report.publishDate	Consumer Goods >> Automobiles & Parts >> Automobile & Parts >> Automobiles	N/A
.message.report.tagSection.main.affectedSystems.affectedSystem[]	report.attribute / adversary.attribute / malware.attribute	Affected System	.message.report.publishDate	Enterprise System >> Database Layer	N/A
.message.report.tagSection.main.impacts.impact[]	report.attribute / adversary.attribute / malware.attribute	Impact	.message.report.publishDate	Data Breach or Compromise	N/A
.message.report.tagSection.main.intents.intent[]	report.attribute / adversary.attribute / malware.attribute	Intent	.message.report.publishDate	Disruption	N/A
.message.report.tagSection.main.motivations.motivation[]	report.attribute / adversary.attribute / malware.attribute	Motivation	.message.report.publishDate	Ideological >> Religious	N/A
.message.report.tagSection.main.sourceGeographies.sourceGeography[]	report.attribute / adversary.attribute / malware.attribute	Source Geography	.message.report.publishDate	Saudi Arabia	N/A
.message.report.tagSection.main.targetGeographies.targetGeography[]	report.attribute / adversary.attribute / malware.attribute	Target Geography	.message.report.publishDate	Global	N/A
.message.report.tagSection.main.targetInformations.targetInformation[]	report.attribute / adversary.attribute / malware.attribute	Targeted Information	.message.report.publishDate	Information Assets >> Email Lists / Archives	N/A
.message.report.tagSection.main.ttps.ttp[]	report.attribute / adversary.attribute / malware.attribute	TTP	.message.report.publishDate	Social Engineering	N/A
.message.report.tagSection.main.threatSources.threatSource[]	report.attribute / adversary.attribute / malware.attribute	Threat Source	.message.report.publishDate	Hacktivist	N/A
.message.report.tagSection.main.operatingSystems.operatingSystem[]	report.attribute / adversary.attribute / malware.attribute	Operating System	.message.report.publishDate	Linux	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.message.report.tagSection.main.roles.role[]	report.attribute / adversary.attribute / malware.attribute	Role	.message.report.publishDate	Backdoor	N/A
.message.report.tagSection.main.malwareCapabilities.malwareCapability[]	report.attribute / adversary.attribute / malware.attribute	Malware Capability	.message.report.publishDate	Anti-forensic capabilities	N/A
.message.report.tagSection.main.detectionNames.detectionName[]	report.attribute / adversary.attribute / malware.attribute	Detection Name	.message.report.publishDate	Anti-AV capabilities	N/A
.message.report.threatDescription	report.attribute / malware.attribute	Threat Description	.message.report.publishDate	ZXSHELL is a backdoor that can be downloaded from the internet, particularly Chinese hacker websites. The backdoor has features including launching port scans, running a keylogger, capturing screen shots, setting up an HTTP or SOCKS proxy, launching a reverse command shell, causing SYN floods, and transferring/deleting/running files. The publicly available version of the tool provides a graphical user interface that attackers can use to interact with victim backdoors. The language used for the bundled ZXSHELL documentation is Simplified Chinese.	N/A
.message.report.abstract	report.attribute / adversary.attribute / malware.attribute	Abstract	.message.report.publishDate	Sality is a venerable family of malicious software that allows for persistent remote control over a Windows machine. The malware has features to persist on victim systems, evade anti-virus software and spread to additional machines. The malware's primary function is to act as a flexible and resilient platform for other actors in the underground economy to install malware on Sality-infected machines, including credential theft malware, fake anti-virus, spam tools and ransomware.	N/A
.message.report.analysis	report.attribute / adversary.attribute / malware.attribute	Analysis	.message.report.publishDate	Many similarities between TrickBot and the now-defunct https://mysight.isightpartners.com/report/full/15-00000436 banking Trojan exist, including web-inject types, code structure, and check-in types for command and control communications. Like Dyre, TrickBot also uses compromised infrastructure for some of the communications. Although we believe that the two projects (Dyre and TrickBot) are related, the code for TrickBot has been completely rewritten so we do not believe this is a new variant, but instead its own code family. The TrickBot indicators in the report include controller URLs and nodes. These nodes or controllers are used for command and control communications, downloads, and configuration downloads (including injects). IOCs marked as "Attacker" are	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
				purely malicious. Any IOC marked as "Compromised" has been malicious at one point but may have been remediated. IP addresses marked as "Related" often include controller nodes hosted on legitimate infrastructure, possibly containing hundreds or thousands of additional hosts.	
.message.report.tagSection.main.actors.actor[].name	adversary.name	N/A	.message.report.publishDate	APT28	Adversary objects are related to the primary Report object.
.message.report.tagSection.main.actors.actor[].id	adversary.attribute	ID	.message.report.publishDate	685c8fdd-2ab4-4709-b7fc-29ce2dde4695	N/A
.message.report.tagSection.main.malwareFamilies.malwareFamily[].name	malware.value	N/A	.message.report.publishDate	trickbot	Malware objects are related to the primary Report object and all other Adversary, Malware, and Indicator objects parsed from the Report object.
.message.report.tagSection.main.malwareFamilies.malwareFamily[].id	malware.attribute	ID	.message.report.publishDate	ab06ecb9-cd4b-4232-852c-21daa187b8e7	N/A
.message.report.tagSection.main.malwareFamilies.malwareFamily[].aliases[]	malware.attribute	Alias	.message.report.publishDate	Silver128	N/A
.message.report.relations.actors[].name	adversary.name	N/A	.message.report.publishDate	Tailgater Team	Adversary objects are related to the primary Report object.
.message.report.relations.actors[].id	adversary.attribute	ID	.message.report.publishDate	8c31fdeb-22e2-4e6b-99a7-cfb87392537b	N/A
.message.report.relations.malwareFamilies[].name	malware.value	N/A	.message.report.publishDate	ZXSHELL	Malware objects are related to the primary Report object and all other Adversary, Malware, and Indicator objects parsed from the Report object.
.message.report.relations.malwareFamilies[].id	malware.attribute	ID	.message.report.publishDate	1b2dfdbe-c04e-411a-a46e-517e1fcabf72	N/A
.message.report.relations.	malware.attribute	Alias	.message.report.publishDate	Viper	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
malwareFamilies[] .aliases[]					
.message.report. tagSection. networks.network[].ip	indicator.value	N/A	.message.report. publishDate	114.8.133.71	Indicator type is `IP Address` or `IPv6 Address` depending on the value of `ip`. Indicator objects are related to the primary Report object.
.message.report. tagSection. networks.network[]. domain	indicator.value	N/A	.message.report. publishDate	comune.villasantostefano.fr.it	Indicator type is `FQDN`. Indicator objects are related to the primary Report object.
.message.report. tagSection. networks.network[]. asn	indicator.value	N/A	.message.report. publishDate	AS24940	Indicator type is `ASN`. Indicator objects are related to the primary Report object.
.message.report. tagSection. networks.network[]. url	indicator.value	N/A	.message.report. publishDate	https://114.8.133.71:449	Indicator type is `URL`. Indicator objects are related to the primary Report object.
.message.report. tagSection. networks.network[]. cidr	indicator.value	N/A	.message.report. publishDate	1.179.132.0/24	Indicator type is `CIDR Block`. Indicator objects are related to the primary Report object.
.message.report. tagSection. networks.network[]. identifier	indicator.attribute	Identifier	.message.report. publishDate	Compromised	N/A
.message.report. tagSection. networks.network[]. domainTimeOfLookup	indicator.attribute	Domain Time of Lookup	.message.report. publishDate	1371573858	Value represented as epoch date time.
.message.report. tagSection. networks.network[]. malwareFamily	indicator.attribute	Malware Family	.message.report. publishDate	smokeloader	N/A
.message.report. tagSection. networks.network[]. malwareFamilyId	indicator.attribute	Malware Family ID	.message.report. publishDate	95223862-dbf0-4ad9-b2f0-358c6013f227	N/A
.message.report. tagSection. networks.network[]. networkType	indicator.attribute	Network Type	.message.report. publishDate	url	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.message.report.tagSection.networks.network[].port	indicator.attribute	Port Number	.message.report.publishDate	8834	N/A
.message.report.tagSection.emails.email[].senderAddress	indicator.value	N/A	.message.report.publishDate	celestino@cdmferri.it	Indicator type is `Email Address`. Indicator objects are related to the primary Report object.
.message.report.tagSection.emails.email[].sourceDomain	indicator.value	N/A	.message.report.publishDate	samyongonc.com	Indicator type is `FQDN`. Indicator objects are related to the primary Report object.
.message.report.tagSection.emails.email[].sourceIp	indicator.value	N/A	.message.report.publishDate	184.105.137.110	Indicator type is `IP Address` or `IPv6 Address` depending on the value of `sourceIp`. Indicator objects are related to the primary Report object.
.message.report.tagSection.emails.email[].subject	indicator.value	N/A	.message.report.publishDate	I need more bees	Indicator type is `Email Subject`. Indicator objects are related to the primary Report object.
.message.report.tagSection.emails.email[].recipient	indicator.value	N/A	.message.report.publishDate	yeh@cwb.gov.tw	Indicator type is `Email Address`. Indicator objects are related to the primary Report object.
.message.report.tagSection.emails.email[].emailIdentifier	indicator.attribute	Email Identifier	.message.report.publishDate	Attacker	N/A
.message.report.tagSection.emails.email[].senderName	indicator.attribute	Sender Name	.message.report.publishDate	llssddzz	N/A
.message.report.tagSection.emails.email[].language	indicator.attribute	Language	.message.report.publishDate	English	N/A
.message.report.tagSection.emails.email[].malwareFamily	indicator.attribute	Malware Family	.message.report.publishDate	smokeloader	N/A
.message.report.tagSection.	indicator.attribute	Malware Family ID	.message.report.publishDate	95223862-dbf0-4ad9-b2f0-358c6013f227	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
emails.email[].malwareFamilyId					
.message.report.tagSection.files.file[].fileName	indicator.value	N/A	.message.report.publishDate	info.exe	Indicator type is `Filename`. Indicator objects are related to the primary Report object.
.message.report.tagSection.files.file[].fuzzyHash	indicator.value	N/A	.message.report.publishDate	1536:RFFgWOBN33zBLLCJ3qpgAXb84sXyA7oi0klOEI6toKtdw:9NEJlLLzLb4I6toKtdw	Indicator type is `Fuzzy Hash`. Indicator objects are related to the primary Report object.
.message.report.tagSection.files.file[].sha1	indicator.value	N/A	.message.report.publishDate	2f2fcfc8f5f23e3e5d7487b656dd9c6c23c79c22	Indicator type is `SHA-1`. Indicator objects are related to the primary Report object.
.message.report.tagSection.files.file[].sha256	indicator.value	N/A	.message.report.publishDate	2b0964359491854078650044 3a68e08d0c272c956f5091cf31 9efe430255002c	Indicator type is `SHA-256`. Indicator objects are related to the primary Report object
.message.report.tagSection.files.file[].md5	indicator.value	N/A	.message.report.publishDate	f691231016739d8bf1fb0020b98f06b5	Indicator type is `MD5`. Indicator objects are related to the primary Report object
.message.report.tagSection.files.file[].description	indicator.attribute	File Description	N/A	Keylogger	N/A
.message.report.tagSection.files.file[].fileSize	indicator.attribute	File Size	.message.report.publishDate	572054	N/A
.message.report.tagSection.files.file[].fileIdentifier	indicator.attribute	File Indentifier	.message.report.publishDate	Attacker	N/A
.message.report.tagSection.files.file[].fileType	indicator.attribute	File Type	.message.report.publishDate	PDF document	N/A
.message.report.tagSection.files.file[].malwareFamily	indicator.attribute	Malware Family	.message.report.publishDate	trickbot	N/A
.message.report.tagSection.files.file[].malwareFamilyId	indicator.attribute	Malware Family ID	.message.report.publishDate	6ff93884-2004-4696-84e3-3d21e1e918ff	N/A

Average Feed Run

METRIC	RESULT
Run Time	15 minutes
Reports	117
Report Attributes	5,482
Adversaries	39
Adversary Attributes	1,427
Indicators	3,995
Indicator Attributes	23,695
Malware	29
Malware Attributes	596

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. Manual feed runs may take significantly longer than scheduled runs to complete due to ingesting one or multiple years' worth of data in a single feed run.

Known Issues/Limitations

- It is possible for a user to specify a time range that does not include any intelligence reports. In this case, the feed run will complete, but no threat intelligence will be ingested.
- MITRE ATT&CK attack patterns must have already been ingested by a previous run of the MITRE ATT&CK feeds in order for MITRE ATT&CK attack patterns extracted from a report's Executive Summary to be related to the report. MITRE ATT&CK attack patterns are ingested from the following feeds:
  - MITRE Enterprise ATT&CK
  - MITRE Mobile ATT&CK
  - MITRE PRE-ATT&CK

Change Log

- **Version 1.3.5**
  - Removed `Threat Detail` attribute.
- **Version 1.3.4**
  - Fixed bug that caused silent errors to be thrown when a query range resulted in only 1 Report
- **Version 1.3.3**
  - Fixed bug that would remove too much text from Description, Threat Detail, Analysis, and Executive Summary attributes
- **Version 1.3.2**
  - Added `Threat Scape` attribute to indicators
  - Removed Description from indicators, malware, and adversaries
  - Truncated Report Description at 32,760 characters
  - Related file and network indicators to adversaries
  - Related file indicators to reports
  - Removed logic to interrelate file indicators
  - Dropped Email Address indicators with an empty value
  - Added feed run metrics
- **Version 1.3.1**
  - Added support for MITRE Attack Pattern Sub-Techniques
- **Version 1.0.0**
  - Initial release