

ThreatQuotient



FireEye Intelligence Reports Feed Implementation Guide

Version 1.3.3

Thursday, October 15, 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.

Copyright © 2020 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Last Updated: Thursday, October 15, 2020

Contents

Versioning	4
Introduction	5
Installation	6
Configuration	7
ThreatQ Mapping	8
FireEye Intelligence Reports (Feed)	8
FireEye Reports Index (Supplemental)	9
Report Download (Supplemental)	12
Average Feed Run	64
Known Issues/Limitations	65
Change Log	66

Versioning

- Current integration version: 1.3.3
- Supported on ThreatQ versions $\geq$ 4.34.0

Introduction

The FireEye Intelligence Reports integration allows a FireEye 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.
- API uses HTTP with HMAC.

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 **FireEye Intelligence** feed 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 feed will be added to the **Commercial** tab for Incoming Feeds. 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. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feed under the **Commercial** tab.
3. Click on the **Feed Settings** link for the feed.
4. Under the **Connection** tab, enter the following configuration parameters:

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.  This parameter is unchecked by default.

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

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 Dofail) 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	Threat-Q 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 regard-	The object description is formatted from <code>.message.report.overview</code> , as well as <code>.message.report.reportType</code> , <code>.message.report.vulnerabilityTypes</code> , <code>.message.report.analysis</code> ,

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
				ing this vulnerability can contact the Vulnerability & Exploitation Team at analystaccess@isightpartners.com .	<pre>.mes- sage.re- port.threatDetail, .mes- sage.re- port.threatDescription , .mes- sage.report.vendorFix, .mes- sage.re- port.vul- nerableProducts, and .mes- sage.re- port.mitigationDetails (when these fields are present). If a description's length exceeds 32,760 char-</pre>

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
					acters, it will be truncated and the string <code>... [Truncated - see full report]</code> 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	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
				"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 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 aca-	If <code>.message.report.execSummary</code> contains any MITRE ATT&CK attack pattern IDs for MITRE ATT&CK attack patterns that

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
				demics 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).	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.re-	Current Intelligence	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
			port.publishDate		
.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.
.mes-	report.at-	Previous	.mes-	Indicator Report: Smoke Loader Activ-	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
sage.report.previousVersionSection.previousVersion[].title	tribute	Version Title	sage.report.publishDate	ity Report (Mar 23, 2020)	
.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
.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.

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
.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 /	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

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
	mal-ware.at-tribute				
.message.report.vulnerabilitytypes.vulnerabilityType	report.at-tribute / adversary.-attribute / mal-ware.at-tribute	Vul-ner-ability Types	.mes-sage.re-port.publishDate	Authentication Issues	N/A
.message.report.vendorFix	report.at-tribute / adversary.-attribute / mal-ware.at-tribute	Vendor Fix	.mes-sage.re-port.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

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
.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 /	Confidentiality Impact	.message.report.publishDate	C:N	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
	mal-ware.at-tribute				
.message.report.accessVector	report.at-tribute / adversary.-attribute / mal-ware.at-tribute	Access Vector	.mes-sage.re-port.publishDate	AV:N	N/A
.message.report.accessComplexity	report.at-tribute / adversary.-attribute / mal-ware.at-tribute	Access Complexity	.mes-sage.re-port.publishDate	AC:L	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
.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 /	Availability Impact	.message.report.publishDate	A:N	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
	mal-ware.at-tribute				
.message.report.exploitability	report.at-tribute / adversary.-attribute / mal-ware.at-tribute	Exploit-ability	.mes-sage.re-port.publishDate	E:U	N/A
.message.report.remediationLevel	report.at-tribute / adversary.-attribute / mal-ware.at-tribute	Remedi-ation Level	.mes-sage.re-port.publishDate	RL:OF	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
.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 /	CVSS Base Vector	.message.report.publishDate	(AC:L/A:N/Au:N/I:P/C:N/AV:N)	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
	mal-ware.at-tribute				
.message.report.cvssBaseScoreLink	report.at-tribute / adversary.-attribute / mal-ware.at-tribute	CVSS Base Score Link	.mes-sage.re-port.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.at-tribute / adversary.-attribute / mal-ware.at-tribute	CVSS Temporal Score	.mes-sage.re-port.publishDate	3.7	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
.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 /	Risk Rating	.message.report.publishDate	LOW	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
	mal-ware.at-tribute				
.message.report.exploitRating	report.at-tribute / adversary.-attribute / mal-ware.at-tribute	Exploit Rating	.mes-sage.re-port.publishDate	No Known	N/A
.message.report.cvelDs.cvelD[]	Value	Indicator	.mes-sage.re-port.publishDate	CVE-2015-2030	Indicator type is CVE . Indicator objects are related to the primary Report object.
.message.report.dateOfDisclosure	report.at-tribute / adversary.-attribute /	Date Of Dis-closure	.mes-sage.re-port.publishDate	September 07, 2015 01:00:00 AM	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
	mal-ware.at-tribute				
.message.report.attackingEase	report.at-tribute / adversary.-attribute / mal-ware.at-tribute	Attack-ing Ease	.mes-sage.re-port.publishDate	Easy	N/A
.message.report.exploitationConsequence	report.at-tribute / indic-ator.at-tribute / adversary.-attribute / mal-	Exploit-ation Con-sequenc-e	.mes-sage.re-port.publishDate	Security Bypass	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
	ware.attribute				
.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
.message.report.exploitation.inTheWild	report.attribute	Exploit-	.mes-	false	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
	tribute / adversary.- attribute / mal- ware.at- tribute	ation: In The Wild	sage.re- port.publishDate		
.message.report.copyright	report.at- tribute / adversary.- attribute / mal- ware.at- tribute	Copy- right	.mes- sage.re- port.publishDate	Copyright 2016 FireEye, Inc. All rights reserved.	N/A
.message.report.intelligenceType	report.at- tribute / adversary.- attribute / mal-	Intel- ligence Type	.mes- sage.re- port.publishDate	malware	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
	ware.attribute				
.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
.mes-	report.at-	Affected	.mes-	Enterprise System >> Database	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
sage.re- port.tagSec- tion.main.affectedSystems.affectedSystem[]	tribute / adversary.- attribute / mal- ware.at- tribute	System	sage.re- port.publishDate	Layer	
.mes- sage.report.tagSection.main.impacts.impact[]	report.at- tribute / adversary.- attribute / mal- ware.at- tribute	Impact	.mes- sage.re- port.publishDate	Data Breach or Compromise	N/A
.message.report.tagSection.main.intents.intent[]	report.at- tribute / adversary.- attribute / mal-	Intent	.mes- sage.re- port.publishDate	Disruption	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
	ware.attribute				
.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
.mes-	report.at-	Target	.mes-	Global	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
sage.re-port.tagSection.main.targetGeographies.targetGeography[]	tribute / adversary.-attribute / malware.attribute	Geography	sage.re-port.publishDate		
.message.re-port.tagSection.main.targetInformations.targetInformation[]	report.attribute / adversary.-attribute / malware.attribute	Targeted Information	.message.re-port.publishDate	Information Assets >> Email Lists / Archives	N/A
.message.report.tagSection.main.ttps.ttp[]	report.attribute / adversary.-attribute / malware.	TTP	.message.re-port.publishDate	Social Engineering	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
	ware.attribute				
.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
.message.report.tagSection.main.roles.role[]	report.attribute	Role	.mes-	Backdoor	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
	tribute / adversary.-attribute / malware.attribute		sage.re-port.publishDate		
.message.re-port.tagSection.-main.malwareCapabilities.malwareCapability[]	report.attribute / adversary.-attribute / malware.attribute	Malware Capability	.message.re-port.publishDate	Anti-forensic capabilities	N/A
.message.re-port.tagSection.main.detectionNames.detectionName[]	report.attribute / adversary.-attribute / mal-	Detection Name	.message.re-port.publishDate	Anti-AV capabilities	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
	ware.attribute				
.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

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
.message.report.abstract	report.attribute / adversary.attribute / malware.attribute	Abstract	.message.report.publishDate	Salicy 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 Salicy-infected machines, including credential theft malware, fake anti-virus, spam tools and ransomware.	N/A
.message.report.analysis	report.attribute / adversary.attribute /	Analysis	.message.report.publishDate	Many similarities between TrickBot and the now-defunct https://mysight.isight-	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
	mal-ware.attribute			partners.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, Trick-Bot also uses compromised infrastructure for some of the communications. Although we believe that the two projects (Dyre and Trick-Bot) 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	

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
				injects). IOCs marked as "Attacker" are 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.threatDetail	report.attribute / adversary.-attribute / malware.attribute	Threat Detail	.message.report.publishDate	On March 7, 2020, on the popular Russian-language forum exploit.in, "Buffer" advertised access allegedly to a major U.S. domain registrar. According to the actor, the company operates registries for the top-level domains (TLDs) lol, mom, sexy, link,	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
				click, help, photo, and more. The actor also claims to have found domain names containing the words "casino" and "crypto." The starting bid is listed at \$50,000 USD, with \$1,000 USD increments, and \$100,000 USD to purchase immediately. Buffer joined the forum on July 2, 2018, has 96 posts, and 46 points of reputation. The actor was recently observed advertising data from a UK operator (20-00003545). Reliability: C Credibility: 3 Threat Activity Alerts relay immediate observations of notable activities within the cyber threat environment. Accompanying reliability (A-F) and credibility (1-6) scores are based on the NATO	

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
				us actors or conducted in-depth analysis of malware or malicious infrastructure. Any indicators of compromise (IOCs) provided may contain only minimal context. Activities continue to be monitored and may result in additional alerts or reports if anything significant occurs, or the issue warrants further analysis. Please rate this product by taking a short four question survey	
.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

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
.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.

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
.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.malwareFamilies[].aliases[]	malware.attribute	Alias	.message.report.publishDate	Viper	N/A
.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

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
					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	indicator	Identifier	.mes-	Compromised	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
[].identifier	ator.attribute		sage.report.publishDate		
.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
.message.report.tagSection.networks.network [].port	indicator.attribute	Port Number	.message.re-	8834	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
	tribute		port.publishDate		
.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.

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
.message.report.tagSection.emails.email[].recipient	indicator.value	N/A	.message.report.publishDate	yeh@cwbgov.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

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.message.report.tagSection.emails.email[].malwareFamilyId	indicator.attribute	Malware Family ID	.message.report.publishDate	95223862-dbf0-4ad9-b2f0-358c6013f227	N/A
.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:RFFgWOBN33zBLLCJ3qpgAXb84sXyA7oi0kIOEI6toKtdw:9NEJILLzLb4I6toKtdw	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	2b09643594918540786500443a68e08d0c272c956f5091cf319efe430255002c	Indicator type is SHA-256 . Indicator objects are related to the primary Report object

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
.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 Identifier	.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[].mal-	indicator	Malware	.mes-	trickbot	N/A

Feed Data Path	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Published Date	Examples	Notes
wareFamily	ator.attribute	Family	sage.report.publishDate		
.message.report.tagSection.files.file[].malwareFamilyId	indicator.attribute	Malware Family ID	.message.report.publishDate	6ff93884-2004-4696-84e3-3d21e1e918ff	N/A

Average Feed Run



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.

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

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 1.3.3**
 - Fixed a 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.
- **Version 1.3.1**
 - Added support for MITRE Attack Pattern Sub-Techniques.
- **Version 1.3.0**
 - Added rich formatting to object descriptions
 - Fixed bug where some attributes would sometimes be ingested even if they were not included in the provider response.
 - Added the option to enable/disable the ingestion of CPEs and related indicators.
 - Added relationships between hash indicators that refer to the same file.
- **Version 1.2.0**
 - Added support for MITRE ATT&CK Attack Patterns.

- **Version 1.1.0**
 - Fixed possible bug with reports from 2013 and back.
 - Fixed issue with not all HTML tags being stripped from description content.
 - Added new Attributes - Web Link, Report Link, & Report ID.
- **Version 1.0.0**
 - Initial Release