ThreatQuotient

Accenture iDefense Feeds Implementation Guide

Version 1.0.0

Thursday, February 6, 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: Thursday, February 6, 2020

Contents

Versioning

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

Introduction

iDefense IntelGraph is a security intelligence platform that allows users to search, manipulate, visualize and contextualize relationships between elements within the iDefense Security Intelligence knowledge base.

Accenture iDefense empowers its customers' environments with contextual, timely and actionable security intelligence, enabling businesses and governments to make smarter decisions to defend against new and evolving threats.

The following feeds are shared by Accenture iDefense:

- Accenture iDefense Vulnerabilities
- Accenture iDefense Threat Actors
- Accenture iDefense Domains
- Accenture iDefense IPs
- Accenture iDefense Hashes
- Accenture iDefense Campaigns
- Accenture iDefense Global Events
- Accenture iDefense Malicious Events
- Accenture iDefense Malware Families
- Accenture iDefense Malicious Tools

Time constrained data fetching is possible, but these feeds only support a Start Date for manual runs and will use the current time as the End Date.

Installation

Accenture iDefense Integration on the ThreatQ Marketplace is designed to replace the Verisign iDefense IntelGraph Feed currently seeded with the ThreatQ platform.

Verisign iDefense IntelGraph Feed users are highly encouraged to review exisiting workflows when installing the new integration.

> 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 **Accenture IDefense** 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 **Commerical** tab for Incoming Feeds. You will still need to configure and then enable the feeds.

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 feeds under the **Commercial** tab.
3. Click on the **Feed Settings** link for each feed.
4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
API Key	The iDefense API Key used for authentication.
Feed URL	The iDefense API Endpoint URL used by the feed. This field is for display purposes only.

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

ThreatQ Mapping

With the exception of Accenture iDefense Malware Families, the feeds follow the same attribute and object mapping. Additional mapping, specific to the feed, are listed at the end of each sample provided in this section.

Accenture iDefense Vulnerabilities

JSON response sample:

```
{
  "results": [
    {
      "created_on": "2020-01-27T15:25:40.000Z",
      "index_timestamp": "2020-01-27T15:27:05.411Z",
      "key": "CVE-2019-17651",
      "last_modified": "2020-01-27T15:25:40.000Z",
      "last_published": "2020-01-27T15:25:40.000Z",
      "links": [
        {
          "key": "cpe:/a:fortinet:fortisiem:5.2.5",
          "relationship": "affects",
          "type": "vuln_tech",
          "uuid": "bc52b449-f0e4-4871-936c-15bec7258857",
          "href": "/rest/fundamental/v0/bc52b449-f0e4-4871-936c-15bec7258857"
        }
      ],
      "replication_id": 1580138740392000000,
      "sources_external": [
        {
          "datetime": "2020-01-27T15:24:40.000Z",
          "description": "Security Advisory FG-IR-19-197",
          "name": "Fortinet",
          "reputation": 5,
          "url": "https://fortiguard.com/psirt/FG-IR-19-197"
        }
      ],
      "type": "vulnerability",
      "uuid": "77a12a69-204b-4c75-bb79-4e545bfb48e4",
      "analysis": "Exploitation could allow an attacker to
execute arbitrary script code on the targeted host.\n\nAn
attacker can successfully exploit this vulnerability by enticing
a potential victim to visit a malicious site. This is normally
accomplished with social engineering techniques. A
mitigating factor against exploitation includes practicing
safe browsing habits, such as not visiting untrusted
sites.\n\niDefense considers this a LOW-severity vulnerability
due to the minimal impact potential.",
      "cvss2": "AV:N/AC:M/Au:N/C:N/I:P/A:N/E:U/RL:OF/RC:C",
      "cvss2_base_score": 4.3,
      "cvss2_temporal_score": 3.2,
      "cvss3":
"CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:U/RL:O/RC:C",
      "cvss3_base_score": 6.1,
      "cvss3_temporal_score": 5.3,
      "cwe": "CWE-79",
      "description": "Remote exploitation of an input validation
vulnerability in Fortinet's FortiSIEM, could allow an
```

```
attacker to execute arbitrary script code on the targeted host.\n\nAn input validation vulnerability has been identified in FortiSIEM. The application fails to properly sanitize user-supplied data via a parameter description field of a Device Maintenance schedule. \n\nFurther details are not available at the time of this writing. iDefense will update this report as more details become available.",
      "severity": 2,
      "threat_types": [
        "Vulnerability"
      ],
      "title": "Fortinet FortiSIEM Input Validation XSS Vulnerability",
      "vendor_fix_external": [
        {
          "advisory_id": "Fortinet update information",
          "datetime": "2020-01-06T05:00:00.000Z",
          "url": "https://fortiguard.com/psirt/FG-IR-19-197"
        }
      ]
    }
  ],
  "total_size": 5,
  "page": 1,
  "page_size": 25,
  "more": false
}
```

Feed Specific Mapping

In addition to the attribute mapping listed on **Shared Attribute Mapping** and related object mapping listed on **Shared Related Object Mapping**, ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Example
.results[].key	Indicator.value	CVE	.results[].created_on	CVE-2020-0001

Accenture iDefense Threat Actors

JSON response sample:

```
{
  "results": [
    {
      "created_on": "2020-01-24T17:49:58.000Z",
      "index_timestamp": "2020-01-27T09:37:28.223Z",
      "key": "@_naifu666",
      "last_modified": "2020-01-25T12:13:26.000Z",
      "last_published": "2020-01-24T17:49:58.000Z",
      "links": [
        {
          "key": "DKB AG",
          "relationship": "impacts",
          "type": "target_organization",
          "uuid": "85027bd1-4afe-4dcf-bebb-23cee7d43e3b",
          "href": "/rest/fundamental/v0/85027bd1-4afe-4dcf-
bebb-23cee7d43e3b"
        },
        {
          "key": "Sparkasse",
          "relationship": "impacts",
          "type": "target_organization",
          "uuid": "642e3e5c-8f10-40d4-9951-17730eb80381",
          "href": "/rest/fundamental/v0/642e3e5c-8f10-40d4-
9951-17730eb80381"
        }
      ],
      "replication_id": 1579954406915000000,
      "sources_external": [
        {
          "datetime": "2020-01-24T16:58:59.000Z",
          "name": "Twitter",
          "reputation": 1,
          "url": "https://twitter.com/_naifu666"
        }
      ],
      "type": "threat_actor",
      "uuid": "431e47f1-df34-4d86-865a-e0615015c15e",
      "first_seen": "2020-01-08T00:00:00.000Z",
      "severity": 2,
      "threat_types": [
        "Cyber Crime"
      ],
      "description": "Twitter handle `@_naifu911` claimed to
have carried out two distributed denial of service (DDoS)
```

```
attacks affecting German-based Das kann Bank (DKB), and one on
Sparkasse Bank Malta plc, which both occurred in January 2020.
This Twitter account was suspended and a new handle created in
its place: `@_naifu666`. The threat actor using this handle
shared screenshots on Twitter of check-host.net, a site used
for checking website availability, showing the DKB and Spar-
kasse sites being unreachable. \n\n`@_naifu666` is a German-
language speaker but claims to be from Japan, using a Twitter
profile picture of a character called Shiro from the anime
\"No Game No Life\" (\"shiro\" means \"white\"). As of January
24, 2020, the account has nine followers and follows 14 Twit-
ter users.\n\nThe Twitter profile shares links to the Telegram
account `@naifu1337`, Discord account `.naifu#3596` and Key-
base account `keybase.io/naifu`. The Keybase profile contains
the Bitcoin address `1Bf36QV91Q9jyyyyw3KyoCUYkQ79JaYWLd` and a
single machine called `NaifuVM`. The Bitcoin wallet has zero
transactions as of January 24, 2020.\n\nTwitter provides the
following additional data: Phone number ending in 95,\nEmail
`un***************@p**********.***`",
      "skill_lvl": "Unknown",
      "ttps": [
        "DDoS"
      ]
    }
  ],
  "total_size": 9,
  "page": 1,
  "page_size": 25,
  "more": false
```

```
}
```

Feed Specific Mapping

In addition to the attribute mapping listed on **Shared Attribute Mapping** and related object mapping listed on **Shared Related Object Mapping**, ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Examples
.results[].key	Adversary.name	N/A	.results[].created_on	Mikhail Rytikov

Accenture iDefense Domains

JSON response sample:

```
{
  "results": [
    {
      "created_on": "2020-01-27T14:20:09.000Z",
      "index_timestamp": "2020-01-27T14:22:28.904Z",
      "key": "lightway.duckdns.org",
      "last_modified": "2020-01-27T14:20:09.000Z",
      "last_published": "2020-01-27T14:20:09.000Z",
      "links": [
        {
          "key": "NanoCore RAT",
          "relationship": "seenAt",
          "type": "malware_family",
          "uuid": "d388ac19-8ffb-46ba-9fc6-c94fc1bb80f5",
          "href": "/rest/fundamental/v0/d388ac19-8ffb-46ba-
9fc6-c94fc1bb80f5"
        }
      ],
      "replication_id": 1580134809889000001,
      "type": "domain",
      "uuid": "edf28d27-cff1-490a-845b-2282694c744d",
      "last_seen_as": [
        "MALWARE_C2"
      ],
      "severity": 3,
      "threat_types": [
        "Cyber Crime"
      ]
    }
  ],
  "total_size": 134,
  "page": 1,
  "page_size": 25,
  "more": true
}
```

Feed Specific Mapping

In addition to the attribute mapping listed on **Shared Attribute Mapping** and related object mapping listed on **Shared Related Object Mapping**, ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Example
.results [].key	Indicator.value	FQDN	.results [].created_on	subdomain.example.com

Accenture iDefense IPs

JSON response sample:

```
{
  "results": [
    {
      "created_on": "2020-01-27T14:20:01.000Z",
      "index_timestamp": "2020-01-27T14:21:57.692Z",
      "key": "67.215.9.236",
      "last_modified": "2020-01-27T14:20:01.000Z",
      "last_published": "2020-01-27T14:20:01.000Z",
      "links": [
        {
          "key": "NanoCore RAT",
          "relationship": "seenAt",
          "type": "malware_family",
          "uuid": "d388ac19-8ffb-46ba-9fc6-c94fc1bb80f5",
          "href": "/rest/fundamental/v0/d388ac19-8ffb-46ba-
9fc6-c94fc1bb80f5"
        }
      ],
      "replication_id": 1580134801570000000,
      "type": "ip",
      "uuid": "acdd1524-bdee-4bf8-93a2-21e1a44ca9de",
      "last_seen_as": [
        "MALWARE_C2"
      ],
      "severity": 3,
      "threat_types": [
        "Cyber Crime"
      ],
      "ip_int": 1138166252,
      "ip_type": 4
    }
  ],
  "total_size": 25,
  "page": 1,
  "page_size": 25,
  "more": false
}
```

Feed Specific Mapping

In addition to the attribute mapping listed on **Shared Attribute Mapping** and related object mapping listed on **Shared Related Object Mapping**, ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Example
.results[].key	Indicator.value	IP Address	.results[].created_on	192.168.0.1

Accenture iDefense Hashes

JSON response sample:

```
{
  "results": [
       {
         "created_on": "2020-01-27T03:29:20.000Z",
         "index_timestamp": "2020-01-27T16:19:17.460Z",
         "key": "f6d18361f19fa5b917a8b021596fa293",
         "last_modified": "2020-01-27T16:17:46.000Z",
         "last_published": "2020-01-27T03:29:20.000Z",
         "links": [
               {
                 "key": "http://177.103.159.44:80",
                 "relationship": "contactsC2At",
                 "type": "url",
                 "uuid": "63c65f6d-5862-4544-b6bf-960501e61a3a",
                 "href": "/rest/fundamental/v0/63c65f6d-5862-4544-b6bf-
960501e61a3a"
               }
         ],
         "replication_id": 1580141866793000010,
         "type": "file",
         "uuid": "6e568b84-c3a3-4bc2-9c59-db42dcd7b430",
         "file_class": "gzip compressed data, from Unix",
         "file_extension": "gzip",
         "filenames": [
               "w80e3z3n36726.exe"
         ],
         "filetype": "Archive",
         "severity": 3,
         "sha1": "b8e44e7e54edd35ab601ca2578a9ce5f45683028",
         "sha256": "426ca154e8e99de86d-
c63c3d45ae6a1ab88b49442964ca7896f1eb7d8c6d30b6",
         "size": 286374,
         "ssdeep": "6144:xjf/UcrD2g3py3ILr3dJYZq5V9Lz-
a2rPdN2U1ygkaOvB+N50ghGXt:Zf/UcXR+o3dJ3VpW2r/2WygkaOvEN50R",
         "threat_types": [
               "Cyber Crime"
         ]
       }
  ],
  "total_size": 10,
  "page": 1,
  "page_size": 25,
  "more": false
}
```

Feed Specific Mapping

In addition to the attribute mapping listed on **Shared Attribute Mapping** and related object mapping listed on **Shared Related Object Mapping**, ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Example
.res-	Indic-	MD5	.results	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Example
ults[].key	ator.value		[].created_on	1a79a4d60de6718e8e5b326e338ae533

Accenture iDefense Campaigns

JSON response sample:

```
{
  "results": [
    {
      "created_on": "2015-06-05T00:00:00.000Z",
      "index_timestamp": "2020-01-27T04:30:45.354Z",
      "key": "OPM Breach",
      "last_modified": "2020-01-03T14:26:58.000Z",
      "last_published": "2015-06-05T00:00:00.000Z",
      "links": [
        {
          "key": "50c24aa1-c90b-4874-93fe-b98f9e5f264e",
          "relationship": "mentions",
          "type": "intelligence_alert",
          "uuid": "901a3856-35b6-41ac-82fa-ca660dc4527c",
          "href": "/rest/document/v0/901a3856-35b6-41ac-82fa-
ca660dc4527c"
```

```
        }
      ],
      "replication_id": 1578061618402000000,
      "type": "threat_campaign",
      "uuid": "9330f7f0-7d13-4645-92fc-61f8ca3ee7b7",
      "description": "See [OPM Data Breach](/#/node/in-
telligence_alert/view/4e9afda9-cda5-4de6-bc87-50970c1bc550)",
      "intent": "Espionage",
      "motive": [
        "political"
      ],
      "severity": 4,
      "threat_types": [
        "Cyber Espionage"
      ]
    }
  ],
  "total_size": 1,
  "page": 1,
  "page_size": 25,
  "more": false
}
```

Feed Specific Mapping

In addition to the attribute mapping listed on **Shared Attribute Mapping** and related object mapping listed on **Shared Related Object Mapping**, ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Example
.results[].key	Campaign.value	N/A	.results[].created_on	OPM Breach
.results[].event_start_date	Campaign.started_at	N/A	N/A	

Accenture iDefense Global Events

JSON response sample:

```
{
  "results": [
    {
      "created_on": "2020-01-23T20:15:47.000Z",
      "index_timestamp": "2020-01-27T05:37:00.630Z",
      "key": "2019-nCoV Novel Coronavirus Outbreak",
      "last_modified": "2020-01-23T21:05:18.000Z",
      "last_published": "2020-01-23T20:15:47.000Z",
      "links": [
        {
          "key": "Taiwan",
          "relationship": "hasLocation",
          "type": "country",
          "uuid": "8e7da585-04b8-4c5f-80f1-891040557002",
          "href": "/rest/fundamental/v0/8e7da585-04b8-4c5f-
80f1-891040557002"
        },
      ],
      "replication_id": 1579813518213000000,
      "sources_external": [
        {
          "datetime": "2020-01-23T17:50:49.000Z",
          "description": "Freedom of the Press and the 2002-
2003 SARS Outbreak",
          "name": "Congressional-Executive Commission on
China",
          "reputation": 5,
          "url": "https://www.cecc.gov/freedom-of-the-press-
and-the-2002-2003-sars-outbreak"
        }
      ],
      "type": "global_event",
      "uuid": "c6b8b9d6-004d-45d4-af22-67fbfb3df53c",
      "description": "On Thursday, January 23 Chinese author-
ities quarantined the cities of Wuhan (武汉) and its eastern
suburbs of Huanggang (黄冈) and Ezhou (鄂州) in response to an
outbreak of what has been named Novel Coronavirus (2019-nCoV),
shutting down public transportation, roads and highways, rail
stations, and the city's airport. \n\nReported infection rates
varied. As of January 21, the World Health Organization (WHO)
had identified 314 confirmed cases (309 in China, two in Thai-
land, one in Japan, and one in South Korea) and six confirmed
deaths. By January 22, the Chinese State Council Information
Office was reporting a total 444 cases of infection and 17
deaths in Wuhan's Hubei Province. Citing the China National
Health Commission, on January 23 media sources were reporting
17 dead, all in Wuhan's Hubei Province, from a total of 571
```

```
cases in China, three in Thailand, and one each in the United
States (Washington State), Japan, South Korea, Taiwan, Hong
Kong and Macau for a total of 580. By the early hours of Janu-
ary 24 Beijing local time, Chinese news source _iFeng_ repor-
ted a total of 658 infections also including cases in Vietnam,
the UK, Singapore, and the Philippines, and 18 dead. Chinese
news outlet _Caixin_ late on January 23 cited an estimate by
Chinese health authorities that cases would eventually reach
up to 6000 in Wuhan alone, and that up to seven cities had
been placed under transportation bans.\n\nChinese authorities
first reported cases to the WHO on December 31, 2019, and
within 24 hours had identified the probable source as an infec-
ted animal offered for sale at the Wuhan Huanan Wholesale Sea-
food Market (武汉华南海鲜批发市场, _Wuhan Huanan Haixian Pifa
Shichang_) in the city's central district not far from the
Yangtze River. Media reports have described the market as a
trading post for exotic game meat, listing species such as
ostrich, peacock, civet, crocodile, camel, koala and wolf pup
on posted menus, along with live slaughtering ser-
vices.\n\nMany Chinese citizens praised authorities for their
firm handling of the outbreak, including the quarantine
actions and the relaxing of state censorship on media report-
ing about the virus. The media policy contrasted with state
suppression of reporting on the SARS virus in 2002 and Asian
H7N9 avian flu epidemic in 2013.\n\nAs of January 23, sig-
nificant global effort is being made to contain the outbreak
but will continue to cause concern and even panic until new
cases are no longer emerging. Like any large-scale global
event, the epidemic is ripe for exploitation in phishing e-
```

```
mail subject lines and lure documents. iDefense suggests organ-
izations rely only on verifiable and authoritative sources for
news and status updates about the virus, and remind their
staff about the likelihood of increased phishing attempts and
ways to protect against them.",
      "event_start_date": "2019-12-31T05:00:00.000Z",
      "event_type": "Epidemic"
    }
  ],
  "total_size": 1,
  "page": 1,
  "page_size": 25,
  "more": false
}
```

Feed Specific Mapping

In addition to the attribute mapping listed on **Shared Attribute Mapping** and related object mapping listed on **Shared Related Object Mapping**, ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Example
.results[].key	Event.title	Global Event	.results[].created_on	2019-nCoV Novel Coronavirus Outbreak
.results[].event_start_date	Event.happened_at	N/A	N/A	

Accenture iDefense Malicious Events

JSON response sample:

```
{
  "results": [
    {
      "created_on": "2020-01-22T20:59:24.000Z",
      "index_timestamp": "2020-01-27T09:37:16.485Z",
      "key": "28615db1-5110-4765-9154-df559473c195",
      "last_modified": "2020-01-26T20:08:29.000Z",
      "last_published": "2020-01-22T20:59:24.000Z",
      "links": [
        {
          "key": "Amazon",
          "relationship": "impacts",
          "type": "target_organization",
          "uuid": "d7448fb7-dc25-45f0-b42b-ed24f1f644c3",
          "href": "/rest/fundamental/v0/d7448fb7-dc25-45f0-
b42b-ed24f1f644c3"
        }
      ],
      "replication_id": 1580069309367000000,
      "sources_external": [
        {
          "datetime": "2020-01-22T05:00:00.000Z",
          "description": "British public news source",
          "name": "British Broadcasting Corporation",
          "reputation": 5,
          "url": "https://www.bbc.com/news/world-asia-india-
50245209"
```

```
        }
      ],
      "type": "malicious_event",
      "uuid": "863ed17d-4f49-4185-ade6-a414d6162e6c",
      "attack_type": "Information Exfiltration",
      "description": "##Overview\n\nThe 2018 breach of Amazon
founder Jeff Bezos' cell phone, which led to a scandalous 2019
leak of details about Bezos' private life, traces back to
Saudi Arabia's royal family, according to a forensic study the
_Financial Times_ and the _Guardian_ reported on January 21.
Anthony J Ferrante of the firm FTI Consulting found with
"medium to high confidence" that Bezos's phone began exporting
masses of data soon after he received an encrypted video file
from the WhatsApp account of Saudi Prince Mohammad bin Salman
in May 2018. \n\nThe forensic analysis, judging from a summary
UN Special Rapporteurs for Human Rights Agnes Callamard and
David Kaye publicized, showed no evidence of known malware.
The report did note that the suspect video had been delivered
via an encrypted downloader host on WhatsApp's media server,
which analysts were unable to decrypt for analysis. Analysts
suspected that the threat actors used mobile spyware such as
the Israeli cyberwarfare firm [NSO Group's Pegasus](/#/node/in-
telligence_alert/view/88269b38-c791-4fcb-8abf-36e67a9f8a48)
software or possibly the [Hacking Team](/#/node/threat_
group/view/5e590c8b-8e29-45ae-be74-c9610e91a0c0)'s Galileo
Remote Control System. They suspect that Saudi security chief
Saud al-Qahtani, who has procured surveillance software from
the [Hacking Team](/#/node/intelligence_alert/view/6f454716-
545f-4e39-a5fa-e16466d1cf53) in the past, procured such
```

```
surveillance software.\n\n##iDefense Insight and Assessment \n\niDefense notes that the Saudi Prince and al-Qahtani have had a strong incentive to discredit Bezos after _The Washington Post_ published articles by journalist Jamal Khashoggi, critical of the Saudi government. A Saudi Twitter campaign targeted Bezos after the paper published articles blaming a Saudi hit squad for the October 2018 murder of Khashoggi. \n\nHowever, publicly available evidence in the case remains less than complete. The attribution rests on massive spikes in egress from Bezos’ phone and on the use of malicious .mp4 files distributed via WhatsApp. \n\niDefense and [others](https://twitter.com/KimZetter/status/1219990065314762752) caution that third-party threat actors may have hacked the Saudi prince’s phone and used it as a launchpad. Both [Iranian](/#/node/intelligence_alert/view/2c8cba51-7eae-4052-b595-77646b7aab16) and [Russian](/#/node/intelligence_alert/view/6f668357-bd6a-4a04-876d-20bd840e0788) governments have targeted Saudi Arabia in the past and have strong incentives to discredit the country so it will not gain too much leverage in the precarious balance among Middle Eastern powers. In addition, if indeed the malware used was Galileo, that code has been available since after the 2015 Hacking Team breach, allowing a variety of threat actors to have used it.\n\n##Action\n\niDefense recommends that organizations and individuals:\n\n* Remain aware that even an encrypted messaging applications like Signal will not ensure privacy of communications.\n* Exercise caution when opening e-mails and clicking on links, even from known contacts.",
      "event_end_date": "2019-01-01T05:00:00.000Z",
      "event_start_date": "2018-05-01T04:00:00.000Z",
      "intent": "Discredit Jeff Bezos and The Washington Post",
      "motive": [
        "Political"
      ],
      "severity": 3,
      "threat_types": [
        "Cyber Espionage"
      ],
      "ttps": [
        "Information disclosure",
        "Mobile malware",
        "malicious .mp4 file"
      ],
      "title": "Saudi Prince Likely Linked to 2018 Breach of Amazon Founder Jeff Bezos’ Phone"
    }
  ],
  "total_size": 1,
  "page": 1,
  "page_size": 25,
  "more": false
}
```

Feed Specific Mapping

In addition to the attribute mapping listed on **Shared Attribute Mapping** and related object mapping listed on **Shared Related Object Mapping**, ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Example
.results[].key	Event.title	Malicious Event	.results [].created_ on	28615db1-5110-4765-9154-df559473c195
.results [].event_ start_date	Event.happened_ at	N/A	N/A	

Accenture iDefense Malware Families

JSON response sample:

```
{
  "results": [
    {
      "created_on": "2015-01-29T07:52:47.000Z",
      "index_timestamp": "2020-01-27T16:42:14.233Z",
      "key": "VB Downloader",
      "last_modified": "2020-01-27T16:40:51.000Z",
      "last_published": "2016-05-19T14:47:54.000Z",
      "links": [
        {
          "key": "793005fd07e7ae0c5bd2064d4d3a4766",
          "relationship": "belongsTo",
          "type": "file",
          "uuid": "076486ac-b810-4ee9-a0f7-4965c57e8470",
          "href": "/rest/fundamental/v0/076486ac-b810-4ee9-
a0f7-4965c57e8470"
        }
      ],
      "replication_id": 1580134608020000000,
      "type": "malware_family",
      "uuid": "511c3d3b-cff3-4263-b236-269deabab7c4",
      "description": "IoT botnet designed to conduct large-scale DDoS attacks.",
      "severity": 3,
      "threat_types": [
        "Hacktivism",
        "Cyber Crime"
      ],
      "variety": [
        "Brute force"
      ],
      "vector": [
        "Network propagation"
      ]
    }
  ],
  "total_size": 20,
  "page": 1,
  "page_size": 25,
  "more": false
}
```

Feed Specific Mapping

In addition to the attribute mapping listed on **Shared Attribute Mapping**, ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Example
.results[].key	Malware.value	N/A	.results[].created_on	VB Downloader

Accenture iDefense Malicious Tools

JSON response sample:

```
{
  "results": [
    {
      "created_on": "2019-11-07T14:17:23.000Z",
      "index_timestamp": "2020-01-27T04:58:59.837Z",
      "key": "Try2check",
      "last_modified": "2019-11-07T14:17:23.000Z",
      "last_published": "2019-11-07T14:17:23.000Z",
      "links": [
        {
          "key": "bb585868-39c5-41e1-b74c-7237db813bfe",
          "relationship": "mentions",
          "type": "intelligence_alert",
          "uuid": "57a05947-86f7-40ce-96a2-481eaa1de160",
          "href": "/rest/document/v0/57a05947-86f7-40ce-96a2-
481eaa1de160"
        }
      ],
      "replication_id": 1573136243827000000,
      "type": "malicious_tool",
      "uuid": "2b5b4975-e65b-4d6f-ad0a-63ad11919c5d",
      "description": "Service used by threat actors to check the validity of compromised card data, by using it to make small transactions. Also referred to as Try2services",
      "severity": 2,
      "threat_types": [
        "Cyber Crime"
      ]
    }
  ],
  "total_size": 8,
  "page": 1,
  "page_size": 25,
  "more": false
}
```

Feed Specific Mapping

In addition to the attribute mapping listed on **Shared Attribute Mapping** and related object mapping listed on **Shared Related Object Mapping**, ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Example
.results [].key	Tool.value	N/A	.results[].created_on	Try2check

Shared Attribute Mapping

With the exception of **Accenture iDefense Malware Families** (see Known Issues/Limitations), the following attribute mapping applies to all feeds:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Examples	Notes
.results[].title	Object.attribute	iDefense Title	.results[].created_on	Kernel.Org Kernel Input Validation Error information Disclosure Vulnerability	
.results[].links	Object.attribute	Targeted Vertical	.results[].created_on		Includes objects from `.results[].links` for which `relationship` is `'target'` and `type` is `'vertical'`.
.results[].links	Object.attribute	Targeted Organization	.results[].created_on		Includes objects from `.results[].links` for which `relationship` is `'target'` and `type` is `'target_organ-`

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Examples	Notes
					`ization'`.
.results[].links	Object.attribute	Targeted Country	.results[].created_on		Includes objects from `.results[].links` for which `relationship` is `'target'` and `type` is `'country'`.
.results[].links	Object.attribute	Impacted Vertical	.results[].created_on		Includes objects from `.results[].links` for which `relationship` is `'impacts'` and `type` is `'vertical'`.
.results[].links	Object.attribute	Impacted Organization	.results[].created_on		Includes objects from `.results[].links` for which `relationship` is `'impacts'` and `type` is `'target_organization'`.
.results[].links	Object.attribute	Impacted Country	.results[].created_		Includes objects from `.results[].links` for which `rela-`

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Examples	Notes
			on		`tionship` is `'impacts'` and `type` is `'country'`.
.results[].alias	Object.attribute	Alias	.results[].created_on	`['Alias 1', 'Alias 2']`	
.results[].pocs	Object.attribute	Proof of Concept	.results[].created_on		
.results[].popularity	Object.attribute	Popularity	.results[].created_on	`3`	In range `1` (Prototype) - `5` (Almost Always)
.results[].severity	Object.attribute	Severity	.results[].created_on	`3`	In range `1` (Minimal) - `5` (Extreme)
.results	Object.attribute	Has Zero Day	.results	`True`	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Examples	Notes
[].zero_day			[].created_on		
.results[].mitigation	Object.attribute	Mitigation	.results[].created_on	iDefense recommends using Microsoft Corp.'s Enhanced Mitigation experience toolkit (EMET) tool to help mitigate this vulnerability. While...	
.results[].threat_types	Object.attribute	Threat Type	.results[].created_on	Vulnerability	
.results[].last_seen_as	Object.attribute	Last Seen As	.results[].created_on		
.results[].meta_data	Object.attribute	Metadata	.results[].created_on		

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Examples	Notes
.results[].cwe	Object.attribute	CWE	.results[].created_on	CWE-200	
.results[].cvss2_base_score	Object.attribute	CVSS v2 Base Score	.results[].created_on	3.3	
.results[].cvss2_temporal_score	Object.attribute	CVSS v2 Temporal Score	.results[].created_on	2.4	
.results[].cvss3_base_score	Object.attribute	CVSS v3 Base Score	.results[].created_on	5.1	
.results[].cvss3_temporal_score	Object.attribute	CVSS v3 Temporal Score	.results[].created_on	7.9	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Examples	Notes
.results[].motivations	Object.attribute	Motivation	.results[].created_on		
.results[].nationalities	Object.attribute	Nationality	.results[].created_on		
.results[].languages	Object.attribute	Language	.results[].created_on		
.results[].capabilities	Object.attribute	Capability	.results[].created_on		
.results[].hashtags	Object.attribute	Hashtag	.results[].created_on		

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Examples	Notes
.results[].religions	Object.attribute	Religion	.results [].created_on		
.results[].real_name	Object.attribute	Real Name	.results [].created_on		
.results[].skill_lvl	Object.attribute	Skill Level	.results [].created_on		
.results[].attack_type	Object.attribute	Attack Type	.results [].created_on		
.results [].motive	Object.attribute	Motive	.results [].created_on		

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Examples	Notes
.results[].location	Object.attribute	Location	.results[].created_on		
.results[].links	Object.attribute	Location	.results[].created_on		Includes objects from `.results[].links` for which `relationship` is `'hasLocation'` and `type` is `'country'`
.results[].event_type	Object.attribute	Event Type	.results[].created_on		
.results[].variety	Object.attribute	Variety	.results[].created_on		
.results[].vector	Object.attribute	Vector	.results[].created_on		

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Examples	Notes
.results[].sources_external	Object.attribute	Reference	.results[].created_on		
.results[].vendor_fix_external	Object.attribute	Vendor Fix	.results[].created_on		
.results[].links	Object.attribute	Affected Technology	.results[].created_on		Includes objects from `.results[].links` for which `relationship` is `'affects'` and `type` is `'vuln_tech'`.
.results[].description	Object.attribute	Description	.results[].created_on	Remote exploitation of an input validation error vulnerability in Kernel.Org's Kernel could allow an attacker to steal sensitive information...	
.results[].ana-	Object.attribute	Analysis	.results	Exploitation could allow an attacker	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Examples	Notes
lysis			[].created_on	to steal sensitive information on the targeted host. An attacker...	
.results[].interesting_characteristics	Object.attribute	Interesting Characteristics	.results [].created_on		

Shared Related Object Mapping

With the exception of **Accenture iDefense Malware Families** (see Known Issues/Limitations), the following shared object mapping applies to all feeds:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Examples	Notes
.results [].links	Object.indicators [].value	IP Address	.results [].created_on	192.168.0.1	Includes objects from `.results[].links` for which `type` is `'ip'`.
.results [].links	Object.indicators [].value	FQDN	.results [].created_on	somesubdomain.example.com	Includes objects from `.results[].links` for which `type` is `'domain'`.
.results [].links	Object.indicators [].value	MD5	.results [].created_on	1a79a4d60de6718e8e5b326e338ae533	Includes objects from `.results[].links` for which `type` is `'file'`, with a length of 32.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Examples	Notes
.results[].links	Object.indicators[].value	URL	.results[].created_on	example.com	Includes objects from `.results[].links` for which type is `'url'`.
.results[].filenames	Object.indicators[].value	Filename	.results[].created_on	example.txt	
.results[].sha1	Object.indicators[].value	SHA-1	.results[].created_on	c3499c2729730a7f807efb8676a92dcb6f8a3f8f	
.results[].sha256	Object.indicators[].value	SHA-256	.results[].created_on	50d858e0985ecc7f60418aaf0cc5ab587f42c2570a884095a9e8ccacd0f6545c	
.results[].links	Object.adversaries[].name	N/A	.results[].created_on		Includes objects from `.results[].links` for which

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Examples	Notes
					`relationship` is one of `'alias', 'talksWith', 'advertiserOf'` and key does not start with `'CVE-'`.
.results[].links	Object.adversaries[].name	N/A	.results[].created_on		Includes objects from `.results[].links` for which `type` is `'threat_group'`.
.results[].links	Object.malware[].value	N/A	.results[].created_on		Includes objects from `.results[].links` for which `type` is `'malware_family'`.
.results[].links	Object.campaigns[].value	N/A	.results[].created_		Includes objects from `.results[].links` for which

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published At	Examples	Notes
			on		`type` is `'threat_campaign'`.
.results[].links	Object.tools[].value	N/A	.results[].created_on		Includes objects from `.results[].links` for which `type` is `'malicious_tool'`.
.results[].ttps	Object.ttps[].value	N/A	.results[].created_on		

Known Issues/Limitations

While **Accenture iDefense Malware Families** does not ingest all possible relationships, using this Feed in conjunction with the other Accenture iDefense feeds will result in relationships being built between the Malware objects ingested by **Accenture iDefense Malware Families** and the other threat intelligence offered by Accenture iDefense.