ThreatQuotient

Digital Shadows Intelligence Feed Implementation Guide

Version 1.0.0

Tuesday, September 1, 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: Tuesday, September 1, 2020

Contents

Digital Shadows Intelligence Feed Implementation Guide 1

Warning and Disclaimer 2

Contents 3

Versioning 4

Introduction 5

Installation 6

Configuration 7

ThreatQ Mapping 9

Digital Shadows Intelligence Threats 9

Digital Shadows Intelligence Incidents 30

Average Feed Runs 48

Known Issues/Limitations 50

Change Log 51

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.28.0`

Introduction

The feeds fetch data from the Digital Shadows Intelligence Threats endpoint and the Digital Shadows Intelligence Incidents endpoint.

- Time constrained data fetching is possible.
    - This feed only supports a Start Date for manual runs and will use the current time as the End Date.
- Uses basic HTTP authentication based on API ID and API key.

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 **Digital Shadows 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 parameter:

Digital Shadows Intelligence Threats

Parameter	Description
API ID	API ID provided by Digital Shadows. Necessary for authentication.
API Key	API key provided by Digital Shadows. Necessary for authentication.
Threat Types	One or more threat types to be ingested.
Threat Levels	One or more threat levels to be ingested.
Save CVE Data as	The ThreatQ object types to be created from CVE data.
Ingest Events as Incidents Objects	If checked, ingests fetched incidents as ThreatQ incident objects. Otherwise, ingests them as Event objects. Checked by default.

Parameter	Description
Relevant to Organization Only	If checked, ingests only threats that are flagged as relevant to your organization. Otherwise, ingests all threats.

Digital Shadows Intelligence Incidents

Parameter	Description
API ID	API ID provided by Digital Shadows. Necessary for authentication.
API Key	API key provided by Digital Shadows. Necessary for authentication.
Threat Types	One or more threat types to be ingested.
Severities	One or more severities to be ingested.
Save CVE Data as	The ThreatQ object types to be created from CVE data.
Ingest Events as Incident Objects	If checked, ingests fetched incidents as ThreatQ incident objects. Otherwise, ingests them as Event objects. Checked 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

Digital Shadows Intelligence Threats

This feed ingests adversaries, malware, events, campaigns, indicators, tools, and TTPs from Digital Shadows.

`GET https://portal-digitalshadows.com/api/intel-threats/find` Sample JSON response:

```
{
  "content": [
    {
      "id": 4049,
      "primaryTag": {
        "id": 5642
      },
      "type": "SPECIFIC_TTP",
      "threatLevel": {
        "type": "MEDIUM"
      },
      "activityLevel": "RECENT",
      "overview": "The TrickBot banking trojan was first reported publicly on 15 Oct 2016 by the
security firm Fidelis. The malware was developed to enable its users to harvest online banking
credentials from customers of banks targeted in the malware configuration file. This is achieved
through the use of webinjects which are inserted into an infected user's browser. The objective
of banking trojans is generally unauthorized access into customer bank accounts to facilitate
fraudulent transactions, but TrickBot has also targeted users of services such as SalesForce and
crypto-currency entities.[[trickbot configs 2017-11-07][https://pastebin.com/ZnU7tuvB]].[[Trick-
Bot expands targeting][https://f5.com/labs/articles/threat-intelligence/malware/trickbot-expands-
global-targets-beyond-banks-and-payment-processors-to-crms]]. On 13 Oct 2016, the first samples
of TrickBot were detected, which included a webinject module; the configuration files of these
samples showed that customers of four Australian banks and one Canadian bank had been affected.
[[TrickBot: We missed you, Dyre][http://www.threatgeek.com/2016/10/trickbot-the-dyre-con-
nection.html]] Subsequent reporting also identified the targeting of bank customers in the United
Kingdom, New Zealand and Germany.[[Aggressive launch of TrickBot][https://se-
curityintelligence.com/an-aggressive-launch-trickbot-trojan-rises-with-redirection-attacks-in-
the-uk]] Further to this, the following locations were known to have been affected by TrickBot
activity:[[TrickBot targeting developments][https://www.digitalshadows.com/blog-and-research/-
coming-to-a-country-near-you-the-rapid-development-of-the-trickbot-trojan/]]\r\n\r\n- Argentina
(see incident ${incident:23821757})\r\n- Australia\r\n- Canada\r\n- Chile (see incident ${in-
cident:23821757})\r\n- Colombia (see incident ${incident:23821757})\r\n- Denmark (see incident
${incident:19594419})\r\n- Finland (see incident ${incident:19594419})\r\n- France\r\n-
```

```
Germany\r\n- Isle of Man\r\n- Ireland\r\n- India\r\n- Israel (see incident ${incident:19594419})\r\n- Italy (see incident ${incident:19594419})\r\n- Malaysia \r\n- New Zealand\r\n- Netherlands[[TrickBot config from 11 Apr 2017][https://pastebin.com/SedUcQ2X]]\r\n-
Norway (see incident ${incident:19594419})\r\n- Peru (see incident ${incident:23821757})\r\n-
Singapore\r\n- Sweden (see incident ${incident:19594419})\r\n- Switzerland (see incident ${incident:19594419})\r\n- United Kingdom\r\n- United States\r\n\r\nTrickBot has been distributed via
the use of spam emails containing malicious Microsoft Office attachments (see incident ${incident:13475074}), malicious JavaScript files (see incident ${incident:13657353}) and the RIG
exploit kit (see incident ${incident:13475074}). On 09 Jun 2017, distribution was reported via
the Necurs botnet; between 0900 and 1800 BST on 07 Jun 2017, 9.6 million emails were detected by
Forcepoint (see incident ${incident:19594419}). Distribution of TrickBot via Necurs has been a
consistent trend since mid-2017. Despite the number of reported distribution methods, the number
of infections associated with TrickBot and any amount of losses resulting from this activity was
not known. \r\n\r\nFollowing distribution, TrickBot was downloaded and installed via the use of a
downloader called TrickLoader, reportedly crypted via  a cryptor also used for Vawtrak, Pushdo
and Cutwail malware. The downloader analysed system bit information before decoding appropriate
resources. TrickBot has contained modules enumerating an infected system's information, and to
exflitrate data to attackers, as well as a webinject configuration stored in an injectDLL module.
\r\n\r\nTrickBot used at least two methods to propagate between machines and network shares on a
local network. On 26 Jul 2017, individual researchers discovered a sample of TrickBot that used
the EternalBlue exploit for a server message block (SMB) vulnerability (CVE-2017-0144) to
```

```
propagate between machines (see incident ${incident:21129761}). Furthermore, in Sep 2017, a Trick-
Bot sample reportedly implemented a new module named “WormShare” that used Windows API calls to
create copies of the malware on network shares.[[TrickBot adds WormShare module][http://www.vkre-
mez.com/2017/09/lets-learn-reversing-trickbot-banking.html]]\r\n\r\nTrickBot was reportedly very
similar to the Dyre banking trojan in relation to the functions and activities it carried out.
However, the \"code styles\" of issuing command to the bot were reportedly different, Trickbot
engaged TaskScheduler, with Dyre deploying direct communication. Furthermore, there was
reportedly more use of the C++ programming language in TrickBot than Dyre. Overall, Fidelis
assessed with \"strong confidence\" that there was a link between Dyre and TrickBot, but that
there had been a considerable amount of new development invested into TrickBot. Fidelis assessed
with a \"moderate confidence\" that one or more of the original Dyre developers had been involved
in the development of TrickBot[[TrickBot: We missed you, Dyre][http://www.-
threatgeek.com/2016/10/trickbot-the-dyre-connection.html]] While the similarities presented by
Fidelis were probably true, we had not confirmed the links between TrickBot and Dyre at the time
of writing. In Feb 2016, reporting on arrests of individuals in Russia in Nov 2015, coupled with
a cessation of Dyre activity, led to speculation that the group behind the Dyre banking trojan
had been arrested and the operations disrupted (see incident ${incident:6471059}). \r\n\r\nSince
its inception TrickBot has undergone a considerable level of development, with the incorporation
of webinject modules and configuration for targeting banks and other services. Additionally,
TrickBot reportedly targeted private and business banks, as well as eight building societies.
[[TrickBot targeting private banks][https://securityintelligence.com/trickbot-is-hand-picking-
private-banks-for-targets-with-redirection-attacks-in-tow/]] Based on our analysis of the con-
figuration files for TrickBot, Australian banks were the most commonly included in these con-
figuration files, showing a realistic possibility customers of these banks were predominantly
affected. It was assessed that at least in the near future TrickBot would continue to expand its
targeting within these locations and likely target further locations in future (see incident ${in-
cident:14305506}). ",
      "lastActive": "2020-04-06T23:00:00.000Z",
      "overviewTags": [],
      "imageThumbnailId": "378e90ec-b4d3-41cc-b071-4bbdf545733b"
    }
  ],
  "currentPage": {
    "offset": 0,
    "size": 12
  },
  "total": 1
}
```

`GET https://portal-digitalshadows.com/api/intel-threats/{ID}` Sample JSON response:

```
{
  "id": 4049,
  "primaryTag": {
    "id": 5642,
    "name": "TrickBot",
    "type": "SPECIFIC_TTP"
  },
  "type": "SPECIFIC_TTP",
  "threatLevel": {
    "type": "MEDIUM",
    "reason": "The TrickBot banking trojan has targeted customers from a large number of banks, financial services and online platforms. The rapid development and global reach of Trickbot indicates that developers are well resourced. The group behind the malware is likely to have access to mule infrastructure to facilitate cash out and money laundering operations. The multiple delivery methods used by its operators showed they were willing to invest resources into its widespread distribution. As a result of these indicators, TrickBot was assessed to represent a Medium threat level at the time of writing."
  },
  "activityLevel": "RECENT",
  "summary": "TrickBot is a banking trojan that was first detected in Sep 2016 and since that time had been developed to incorporate the targeting of multiple geographies and online services. The malware was developed to gain unauthorized access to customer bank accounts to facilitate fraudulent transactions, but also targeted users of online services such as SalesForce and
```

```
cryptocurrency services. The malware was reportedly delivered via spam emails containing mali-
cious attachments, including those distributed by the Necurs botnet, and via the RIG exploit kit.
In some cases, TrickBot used an exploit called EternalBlue (affects CVE-2017-0144) or Windows API
calls to propagate in a local network. The functions and activities of TrickBot are reportedly
very similar to the Dyre banking trojan, and it was assessed by researchers to be linked to this
trojan, including that at least one of the developers of Dyre was involved in the development of
TrickBot. The widespread targeting and rapid, continuing development meant that the malware rep-
resented a Medium threat level at the time of writing.",
  "overview": "The TrickBot banking trojan was first reported publicly on 15 Oct 2016 by the
security firm Fidelis. The malware was developed to enable its users to harvest online banking
credentials from customers of banks targeted in the malware configuration file. This is achieved
through the use of webinjects which are inserted into an infected user's browser. The objective
of banking trojans is generally unauthorized access into customer bank accounts to facilitate
fraudulent transactions, but TrickBot has also targeted users of services such as SalesForce and
crypto-currency entities.[[trickbot configs 2017-11-07][https://pastebin.com/ZnU7tuvB]].[[Trick-
Bot expands targeting][https://f5.com/labs/articles/threat-intelligence/malware/trickbot-expands-
global-targets-beyond-banks-and-payment-processors-to-crms]]. On 13 Oct 2016, the first samples
of TrickBot were detected, which included a webinject module; the configuration files of these
samples showed that customers of four Australian banks and one Canadian bank had been affected.
[[TrickBot: We missed you, Dyre][http://www.threatgeek.com/2016/10/trickbot-the-dyre-con-
nection.html]] Subsequent reporting also identified the targeting of bank customers in the United
```

```
Kingdom, New Zealand and Germany.[[Aggressive launch of TrickBot][https://se-
curityintelligence.com/an-aggressive-launch-trickbot-trojan-rises-with-redirection-attacks-in-
the-uk]] Further to this, the following locations were known to have been affected by TrickBot
activity:[[TrickBot targeting developments][https://www.digitalshadows.com/blog-and-research/-
coming-to-a-country-near-you-the-rapid-development-of-the-trickbot-trojan/]]\r\n\r\n- Argentina
(see incident ${incident:23821757})\r\n- Australia\r\n- Canada\r\n- Chile (see incident ${in-
cident:23821757})\r\n- Colombia (see incident ${incident:23821757})\r\n- Denmark (see incident
${incident:19594419})\r\n- Finland (see incident ${incident:19594419})\r\n- France\r\n- Ger-
many\r\n- Isle of Man\r\n- Ireland\r\n- India\r\n- Israel (see incident ${in-
cident:19594419})\r\n- Italy (see incident ${incident:19594419})\r\n- Malaysia \r\n- New
Zealand\r\n- Netherlands[[TrickBot config from 11 Apr 2017][https://pastebin.com/SedUcQ2X]]\r\n-
Norway (see incident ${incident:19594419})\r\n- Peru (see incident ${incident:23821757})\r\n-
Singapore\r\n- Sweden (see incident ${incident:19594419})\r\n- Switzerland (see incident ${in-
cident:19594419})\r\n- United Kingdom\r\n- United States\r\n\r\nTrickBot has been distributed via
the use of spam emails containing malicious Microsoft Office attachments (see incident ${in-
cident:13475074}), malicious JavaScript files (see incident ${incident:13657353}) and the RIG
exploit kit (see incident ${incident:13475074}). On 09 Jun 2017, distribution was reported via
the Necurs botnet; between 0900 and 1800 BST on 07 Jun 2017, 9.6 million emails were detected by
Forcepoint (see incident ${incident:19594419}). Distribution of TrickBot via Necurs has been a
consistent trend since mid-2017. Despite the number of reported distribution methods, the number
of infections associated with TrickBot and any amount of losses resulting from this activity was
```

```
not known. \r\n\r\nFollowing distribution, TrickBot was downloaded and installed via the use of a
downloader called TrickLoader, reportedly crypted via  a cryptor also used for Vawtrak, Pushdo
and Cutwail malware. The downloader analysed system bit information before decoding appropriate
resources. TrickBot has contained modules enumerating an infected system's information, and to
exflitrate data to attackers, as well as a webinject configuration stored in an injectDLL module.
\r\n\r\nTrickBot used at least two methods to propagate between machines and network shares on a
local network. On 26 Jul 2017, individual researchers discovered a sample of TrickBot that used
the EternalBlue exploit for a server message block (SMB) vulnerability (CVE-2017-0144) to propag-
ate between machines (see incident ${incident:21129761}). Furthermore, in Sep 2017, a TrickBot
sample reportedly implemented a new module named “WormShare” that used Windows API calls to cre-
ate copies of the malware on network shares.[[TrickBot adds WormShare module][http://www.vkre-
mez.com/2017/09/lets-learn-reversing-trickbot-banking.html]]\r\n\r\nTrickBot was reportedly very
similar to the Dyre banking trojan in relation to the functions and activities it carried out.
However, the \"code styles\" of issuing command to the bot were reportedly different, Trickbot
engaged TaskScheduler, with Dyre deploying direct communication. Furthermore, there was
reportedly more use of the C++ programming language in TrickBot than Dyre. Overall, Fidelis
assessed with \"strong confidence\" that there was a link between Dyre and TrickBot, but that
there had been a considerable amount of new development invested into TrickBot. Fidelis assessed
with a \"moderate confidence\" that one or more of the original Dyre developers had been involved
in the development of TrickBot[[TrickBot: We missed you, Dyre][http://www.-
threatgeek.com/2016/10/trickbot-the-dyre-connection.html]] While the similarities presented by
```

```
Fidelis were probably true, we had not confirmed the links between TrickBot and Dyre at the time
of writing. In Feb 2016, reporting on arrests of individuals in Russia in Nov 2015, coupled with
a cessation of Dyre activity, led to speculation that the group behind the Dyre banking trojan
had been arrested and the operations disrupted (see incident ${incident:6471059}). \r\n\r\nSince
its inception TrickBot has undergone a considerable level of development, with the incorporation
of webinject modules and configuration for targeting banks and other services. Additionally,
TrickBot reportedly targeted private and business banks, as well as eight building societies.
[[TrickBot targeting private banks][https://securityintelligence.com/trickbot-is-hand-picking-
private-banks-for-targets-with-redirection-attacks-in-tow/]] Based on our analysis of the con-
figuration files for TrickBot, Australian banks were the most commonly included in these con-
figuration files, showing a realistic possibility customers of these banks were predominantly
affected. It was assessed that at least in the near future TrickBot would continue to expand its
targeting within these locations and likely target further locations in future (see incident ${in-
cident:14305506}). ",
  "lastActive": "2020-04-06T23:00:00.000Z",
  "overviewTags": [],
  "imageId": "9a155fe2-a2c1-4561-a4a7-1c59098e975e",
  "imageThumbnailId": "378e90ec-b4d3-41cc-b071-4bbdf545733b",
  "tacticTags": [
    {
      "id": 2694,
      "name": "Credential Harvesters",
      "type": "GENERAL_TTP",
      "parent": {
        "id": 2682
      }
    }
  ],
  "motivationTags": [
    {
      "id": 443,
      "name": "Financial or Economic",
      "type": "MOTIVATION"
    }
  ],
  "primaryLanguageTags": [
    {
      "id": 467,
      "name": "English",
      "type": "LANGUAGE"
    }
  ],
"sourceGeographyTags": [],
"actorTypeTags": [
  {
    "id": 1112,
    "name": "eCrime Actor - Malware Developer",
    "type": "ACTOR_TYPE"
  }
],
"targetGeographyTags": [
  {
    "id": 855,
    "name": "Canada",
    "type": "TARGET_GEOGRAPHY",
    "parent": {
      "id": 990
    }
  }
],
"targetSectorTags": [
  {
    "id": 1080,
      "name": "Banks",
      "type": "TARGET_SECTORS"
    }
  ],
  "intendedEffectTags": [
    {
      "id": 401,
      "name": " Theft - Credential Theft",
      "type": "INTENDED_EFFECTS"
    }
  ],
  "impactEffectTags": [
    {
      "id": 428,
      "name": "Financial Loss",
      "type": "IMPACT_EFFECTS"
    }
  ],
  "associatedActorTags": [
    {
      "id": 7732,
      "name": "Lazarus Group",
      "type": "ACTOR"
    }
  ],
  "associatedCampaignTags": [],
  "associatedEvents": [],
  "latestIncident": {
    "id": 61058206,
    "scope": "GLOBAL"
  },
  "sites": [],
  "detailLevel": "FULL",
  "indicatorOfCompromiseCount": 355,
  "aptReports": [
    {
      "id": "39c68dd0-f9ed-472f-b46b-4d9153ae5442"
    },
    {
      "id": "109c2b6b-3c2e-4e6c-bd58-16d38c4c1dba"
    }
  ],
  "mitigation": "Mitigations against malware such as this should be focused on deploying a defense-in-depth strategy to protect against initial infection and for post infection. A strategy for defense should use a blend of technical and non-technical controls in order to be most effective, some of the components that should be used include:\r\n\r\n• Security awareness training, staff should be educated on the risks associated with clicking on links and attachments within emails.\r\n\r\n• Filter email and attachments, it may be wise to block executable file types including those compressed within archives such as zip and RAR.\r\n\r\n• Advanced malware detection devices should be deployed to monitor incoming email streams as well as subsequent downloads.\r\n\r\n• End point controls should be implemented on the end users’ computers to help limit opening of malicious file attachments and to catch malware installations/executions.\r\n\r\n• Apply post-infection controls such as firewall policies, web proxies, and log monitoring to identify abnormalities.\r\n\r\n• Keep antivirus databases, operating systems and applications up to date.\r\n",
  "toolTags": [],
  "cveNumberTags": []
}
```

`GET https://portal-digitalshadows.com/api/intel-threats/{ID}/iocs` Sample JSON response:

```
{
  "content": [
    {
      "id": 5666,
      "type": "MD5",
      "value": "0804499dba4090c439e580f5693660e0",
      "aptReport": {
        "id": "109c2b6b-3c2e-4e6c-bd58-16d38c4c1dba"
      }
    },
  ]
}
```

The mapping below maps the JSON responses above from the `Digital Shadows Intelligence Threats` Feed.

Feed Data Path	ThreatQ Entity	ThreatQ Object.Type or Attribute Key	Published Date	Examples	Notes
.content[].primaryTag.name	Adversary.Value	N/A	N/A	N/A	Ingested when .content[].primaryTag.type is ACTOR
.content[].primaryTag.name	Event.Title/Incident.Value	Incident	N/A	N/A	Ingested when .content[].primaryTag.type is EVENT.

Feed Data Path	ThreatQ Entity	ThreatQ Object.Type or Attribute Key	Published Date	Examples	Notes
					ThreatQ object type varies depending on the **Ingest Events as Incident Objects** setting
.content[].primaryTag.name	Malware.Value	N/A	Trickbot	N/A	Ingested when .content[].primaryTag.type is SPECIFIC_TTP
.content[].primaryTag.name	Tool.Value	N/A	N/A	N/A	Ingested when .content[].primaryTag.type is TOOLS
.content[].primaryTag.name	Campaign.Value	N/A	N/A	N/A	Ingested when .content[].primaryTag.type is CAMPAIGN
.content[].lastActive	Event.HappenedAt/Incident.OccurredAt	N/A	N/A	N/A	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object.Type or Attribute Key	Published Date	Examples	Notes
.content[].threatLevel.type	Object.Attribute	Threat Level	N/A	MEDIUM	N/A
.content[].threatLevel.reason	Object.Attribute	Threat Level Reason	N/A	N/A	N/A
.content[].activityLevel	Object.Attribute	Activity Level	N/A	RECENT	N/A
.content[].recurring	Object.Attribute	Recurring Event	N/A	True	N/A
.content[].actorTypeTags [].name	Object.Attribute	Actor Type	N/A	Hacker	N/A
.content[].impactEffectTags [].name	Object.Attribute	Impact Effect	N/A	Financial Loss	N/A
.content[].intendedEffectTags [].name	Object.Attribute	Intended Effect	N/A	Theft - Credential Theft	N/A
.content[].primaryLanguageTags[].name	Object.Attribute	Language	N/A	English	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object.Type or Attribute Key	Published Date	Examples	Notes
.content[].sourceGeographyTags[].name	Object.Attribute	Source Geography	N/A	Canada	N/A
.content[].specifiedTargetTags[].name	Object.Attribute	Specified Target	N/A	N/A	N/A
.content[].targetGeographyTags[].name	Object.Attribute	Target Geography	N/A	Canada	N/A
.content[].targetSectorTags[].name	Object.Attribute	Target Sector	N/A	Banks	N/A
.content[].overview	Object.Attribute	Overview	N/A	The TrickBot banking trojan was first reported publicly on 15 Oct 2016...	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object.Type or Attribute Key	Published Date	Examples	Notes
.content[].knownMembersDescription	Object.Attribute	Known Members Description	N/A	N/A	N/A
.content[].mitigation	Object.Attribute	Recommended Action	N/A	Mitigations against malware such as this should...	N/A
.content[].tacticDescription	Object.Attribute	Tactic Description	N/A	N/A	N/A
.content[].id	Object.Attribute	Digital Shadows portal Link	N/A	N/A	Formatted with portal URL
.content[].value	Indicator.Value	.content[].type	N/A	N/A	`iocs` are from the supplemental feed
.content[].cveNumberTags [].name	Indicator.Value/Vulnerability.Value	CVE for Indicator, N/A for	N/A	N/A	ThreatQ object types vary depending on

Feed Data Path	ThreatQ Entity	ThreatQ Object.Type or Attribute Key	Published Date	Examples	Notes
		Vulnerability			the **Save CVE Data as** settings
.content[].associatedActorTags[].name	Adversary.Name	N/A	N/A	N/A	Above attributes do not apply
.content[].tacticTags[].name	TTP.Value	N/A	N/A	Credential Harvesters	Filtered down to only CATEGORY_TTP and GENERAL_TTP types
.content[].tacticTags[].name	Malware.Value	N/A	N/A	N/A	Filtered down to only SPECIFIC_TTP types
.content[].associatedCampaignTags[].name	Campaign.Value	Campaign	N/A	N/A	Above attributes do not apply
.content[].toolTags[].name	Tool.Value	Tool	N/A	N/A	N/A

Digital Shadows Intelligence Incidents

This feed ingests public intelligence incidents from Digital Shadows.

`GET https://portal-digitalshadows.com/api/intel-incidents/find` Sample JSON response:

```
{
  "content": [
    {
      "id": 61133184,
      "scope": "GLOBAL",
      "type": "CYBER_THREAT",
      "severity": "LOW",
      "title": "xHelper Android malware remains active",
      "published": "2020-04-14T08:38:57.835Z",
      "closedSource": false,
      "summary": "Cyber-security researchers reported that the xHelper Android malware variants has remained highly active in 2020.",
      "modified": "2020-04-14T08:38:57.842Z",
      "occurred": "2020-04-06T23:00:00.000Z",
      "verified": "2020-04-14T08:38:20.851Z",
      "tags": [
        {
          "id": 8710,
          "name": "Mobile malware",
          "type": "GENERAL_TTP"
        },
        {
          "id": 170,
          "name": "Industry News",
          "type": "GENERAL"
        },
        {
          "id": 9532,
          "name": "Android",
          "type": "SPECIFIED_TARGETS"
        },
        {
          "id": 2701,
          "name": "Remote Access Trojan",
          "type": "GENERAL_TTP"
        },
        {
          "id": 3181,
          "name": "Secondary source",
          "type": "GENERAL"
        },
        {
          "id": 1903,
          "name": "Social Engineering",
          "type": "GENERAL_TTP"
        }
      ],
      "version": 5,
      "score": 0,
      "entitySummary": {
        "source": "https://threatpost.com/xhelper-russian-nesting-doll-android-malware/154519/",
        "summaryText": "Ultimately delivering the Triada payload, xHelper goes to great lengths to become virtually indestructible once installed on a smartphone.",
        "domain": "threatpost.com",
        "sourceDate": "2020-04-06T23:00:00.000Z",
        "type": "WEB_PAGE",
        "contentRemoved": false
      },
      "description": "On 07 Apr 2020 cyber-security researchers reported that the xHelper Android
```

```
malware variant (see incident 57711200) has remained highly active in 2020. This has included
operations where it has been used to deliver the \"Triada\" trojan. \r\n\r\nThe infection chain
starts by convincing a victim to download a malicious trojanized app. This has included an operation
where xHelper was embedded in an app that masqueraded as a popular cleaner and speed-up
utility for smartphones.\r\n\r\nFurther technical details are available in the additional source
included below. \r\n\r\nSource evaluation: Threat Post is usually reliable; the information is
probably true. \r\n\r\nAdditional source: \r\n- https://securelist.com/unkillable-xhelper-and-a-
trojan-matryoshka/96487/",
      "linkedContentIncidents": [],
      "internal": false,
      "restrictedContent": false,
      "indicatorOfCompromiseCount": 18
    }
  ]
}
```

`GET https://portal-digitalshadows.com/api/intel-incidents/{ID}` Sample JSON response:

```
{
  "id": 61133184,
  "scope": "GLOBAL",
  "type": "CYBER_THREAT",
  "severity": "LOW",
  "title": "xHelper Android malware remains active",
  "published": "2020-04-14T08:38:57.835Z",
  "closedSource": false,
  "summary": "Cyber-security researchers reported that the xHelper Android malware variants has
remained highly active in 2020.",
  "modified": "2020-04-14T08:38:57.842Z",
  "occurred": "2020-04-06T23:00:00.000Z",
  "verified": "2020-04-14T08:38:20.851Z",
  "tags": [
    {
      "id": 8710,
      "name": "Mobile malware",
      "type": "GENERAL_TTP"
    },
    {
      "id": 170,
      "name": "Industry News",
      "type": "GENERAL"
    },
    {
      "id": 9532,
      "name": "Android",
      "type": "SPECIFIED_TARGETS"
    },
    {
      "id": 2701,
      "name": "Remote Access Trojan",
      "type": "GENERAL_TTP"
    },
    {
      "id": 3181,
      "name": "Secondary source",
      "type": "GENERAL"
    },
    {
      "id": 1903,
      "name": "Social Engineering",
      "type": "GENERAL_TTP"
    }
  ],
  "version": 5,
  "score": 0,
  "entitySummary": {
    "source": "https://threatpost.com/xhelper-russian-nesting-doll-android-malware/154519/",
    "summaryText": "Ultimately delivering the Triada payload, xHelper goes to great lengths to become virtually indestructible once installed on a smartphone.",
    "domain": "threatpost.com",
    "sourceDate": "2020-04-06T23:00:00.000Z",
    "type": "WEB_PAGE",
    "contentRemoved": false
  },
  "description": "On 07 Apr 2020 cyber-security researchers reported that the xHelper Android malware variant (see incident 57711200) has remained highly active in 2020. This has included operations where it has been used to deliver the \"Triada\" trojan. \r\n\r\nThe infection chain starts by convincing a victim to download a malicious trojanized app. This has included an operation where xHelper was embedded in an app that masqueraded as a popular cleaner and speed-up utility for smartphones.\r\n\r\nFurther technical details are available in the additional source included below. \r\n\r\nSource evaluation: Threat Post is usually reliable; the information is probably true. \r\n\r\nAdditional source: \r\n- https://securelist.com/unkillable-xhelper-and-a-trojan-matryoshka/96487/",
  "linkedContentIncidents": [],
  "internal": false,
  "restrictedContent": false,
  "indicatorOfCompromiseCount": 18
}
```

`GET https://portal-digitalshadows.com/api/intel-threats/{ID}/iocs` Sample JSON response:

```
{
  "content": [
    {
      "id": 18306,
      "type": "IP",
      "value": "172.104.215.170",
      "source": "https://securelist.com/unkillable-xhelper-and-a-trojan-matryoshka/96487/",
      "lastUpdated": "2020-04-07T00:00:00.000Z"
    }
  ]
}
```

The mapping below maps the JSON responses above from the `Digital Shadows Intelligence Incidents` Feed.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.content[].title	Event.Title/Incident.Value	Incident	.content[].published	xHelper Android malware remains active	
.content[].occurred	Event.HappenedAt/Incident.OccurredAt	N/A	N/A	N/A	ThreatQ object type varies depending on user field settings
.content[].tags[].name	TTP.Value	N/A	.content[].published	N/A	Filtered down to only CATEGORY_TTP and

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
					GENERAL_TTP types
.content[].tags[].name	Malware.Value	N/A	.content[].published	N/A	Filtered down to only SPECIFIC_TTP types
.content[].tags[].name	Adversary.Name	N/A	.content[].published	N/A	Filtered down to only ACTOR types
.content[].tags[].name	Indicator.Value/Vulnerability.Value	CVE for Indicator,	.content[].pub-	N/A	Filtered down to

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
		N/A for Vulnerability	lished		only CVE_ NUMBER types. ThreatQ object types vary depending on user field settings
.content[].tags[].name	Tool.Value	N/A	.content [].published	N/A	Filtered down to only TOOLS types

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.content[].tags[].name	Object.Attribute	.content[].tags.type	.content[].published	N/A	See table below for attribute type mapping
.content[].severity	Event.Attribute	Severity	.content[].published	LOW	
.content[].type	Event.Attribute	Type	.content[].published	CYBER_THREAT	
.content[].subType	Event.Attribute	Subtype	.content[].puslibhed	N/A	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.content[].summary	Event.Attribute	Summary	.content[].published	Cyber-security researchers reported that the xHelper Android malware variants have remained highly active in 2020.	
.content[].scope	Event.Attribute	Scope	.content[].published	GLOBAL	
.content[].verified	Event.Attribute	Verified At	.content[].published	2020-04-14T09:31:33.991Z	
.content[].internal	Event.Attribute	Is Internal	.content[].published	N/A	
.content[].version	Event.Attribute	Version	.content	5	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
			[].published		
.content[].entitySummary.summaryText	Event.Attribute	Entity Summary	.content [].published	Ultimately deilvering the Triada payload, xHelper goes to great lengths to become virtually indestructible once installed on a smartphone.	
.content[].entitySummary.source	Event.Attribute	Entity Source	.content [].published	https://-threatpost.com/xhelper-russian-nesting-doll-android-malware/154519	
.content[].entitySummary.domain	Event.Attribute	Entity Domain	.content [].published	threatpost.com	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.content[].entitySummary.sourceDate	Event.Attribute	Entity Source Date	.content[].published	2020-04-06T23:00:00.000Z	
.content[].entitySummary.screenshotThumbnailId	Event.Attribute	Entity Screenshot ID	.content[].published	N/A	
.content[].entitySummary.type	Event.Attribute	Entity Type	.content[].puslibhed	WEB_PAGE	
.content[].entitySummary.fullText	Event.Attribute	Entity Text	.content[].published	N/A	
.content[].entitySummary.contentRemoved	Event.Attribute	Entity Content Removed	.content[].published	false	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.content[].alerted	Event.Attribute	Alerted At	.content[].published	N/A	
.content[].mitigation	Event.Attribute	Mitigation	.content[].published	N/A	
.content[].impactDescription	Event.Attribute	Impact Description	.content[].published	N/A	
.content[].takedownRequestCount	Event.Attribute	Takedown Request Count	.content[].published	N/A	
.content[].restrictedContent	Event.Attribute	Restricted Content	.content[].published	false	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.content[].score	Event.Attribute	Score	.content[].published	N/A	

The values in .content[].tags which are ingested as attributes are as follows:

Digital Shadows Type	ThreatQ Attribute Key
TARGET_GEOGRAPHY	Target Geography
INTENDED_EFFECTS	Intended Effect
SOURCE_GEOGRAPHY	Source Geography
GENERAL	Tag
DATA_BREACH	Breached Data
IMPACT EFFECTS	Impact Effect

Digital Shadows Type	ThreatQ Attribute Key
EVENT_TYPE	Event Type
ACTOR_TYPE	Actor Type
LANGUAGE	Language
TARGET_SECTORS	Target Sector
SPECIFIED_TARGETS	Specified Target

Average Feed Runs

Digital Shadows Intelligence Threats

Average Feed Run results for Digital Shadows Intelligence Threats (with default user field settings):

Metric	Result
Run Time	1 minute
Adversaries	3
Incidents	2
Incident Attributes	90
Indicators	35
Indicator Attributes	5
Malwares	10
Malware Attributes	90
TTPs	20

Digital Shadows Intelligence Incidents

Average Feed Run results for Digital Shadows Intelligence Incidents (with default user field settings):

Metric	Result
Run Time	< 1 minute
Incidents	20
Incident Attributes	550
Indicators	10
Malwares	1
TTPs	10

Known Issues/Limitations

Currently, the `Digital Shadows Intelligence Incidents` feed *does not* ingest related events or incidents.

Change Log

- **Version 1.0.0**
    - Initial release