ThreatQuotient

McAfee MVISION CDF Guide Guide

Version 1.0.0

February 28, 2022

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

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.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Versioning

- Current integration version `1.0.0`
- Compatible with ThreatQ versions >= `4.35.0`

Introduction

The McAfee MVISION CDF for ThreatQ enables analysts to automatically ingest campaigns provided by McAfee MVISION Cloud.

The McAfee MVISION CDF integration for ThreatQ provides the following feeds:

- **McAfee MVISION Insights Campaigns** - brings in campaigns & related context from the McAfee MVISION Insights App.
- **McAfee Insights IOC Data (Supplemental)** - fetches related IOCs to a given Campaign.
- **McAfee Insights Galaxies Data (Supplemental)** - fetches related Galaxy Data to a given Campaign.
- **McAfee MVISION ePO Events** - brings in assets (hosts/devices) with threat events from McAfee MVISION ePO.
- **McAfee ePO Device by Agent ID (Supplemental)** - fetches a single device by its' ID, from McAfee MVISION via the ePO endpoint.
- **McAfee MVISION Insights Events** - ingests assets (hosts/devices) with threat events relating to a campaign within the McAfee MVISION Insights App.
- **McAfee Insights Campaign by ID (Supplemental)** - fetches a single campaign by its' ID, from McAfee MVISION via the Insights endpoint.
- **McAfee MVISION Threat Research** - brings in reports from McAfee's Threat Research RSS feed.

The integration ingests the following system objects:

- Adversaries
- Assets (custom object)
- Campaigns
- Events
- Indicators
- Malware
- Reports
- Tools

Prerequisites

Review and complete the following prerequisites before installing the McAfee MVISION CDF integration.

Asset Custom Object

McAfee MVISION CDF requires the installation of the `Assets` custom object. Before installing the custom object, be sure that you unzipped the **McAfee MVISION.zip**. The zip file will contain the following:

- asset.json - the assets definition file.
- asset.svg - the assets icon file.
- install.sh - the assets installation script.
- McAfee MVISION CDF yaml - the integration file to install the CDF in ThreatQ.

ThreatQuotient provides two methods to install the required custom objects: via script and manual installation.

> When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

1. Download the custom object zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Install the custom objects using the one of the following methods:

   Via Script

   ThreatQuotient provides a script that will copy the SVG icon and JSON definition file to the correct directories and automatically install the required custom object.

   a. Navigate to tmp directory:

   ```
   <> cd /tmp/
   ```

b. Create a new directory:

c.
```
<> mkdir mcafee_mvision_cdf
```

d. Upload the **asset.json**, **asset.svg file**, and **install.sh** script into this new directory.

e. Navigate to the new directory, **/tmp/mcafee_mvision_cdf**, if you have not done so yet.

The directory should resemble the following:

- tmp
  - **mcafee_mvision_cdf**
    - **asset.json**
    - **install.sh**
    - **asset.svg**

f. Run the following command:

```
<> sudo bash install.sh
```

> You must be in the directory that houses the install.sh, SVG, and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

```
[root@localhost mcafee_mvision_cdf]# sudo bash install.sh
----- Installing Asset Custom Object -----

'/tmp/mcafee_mvision_cdf/asset.svg' -> '/var/www/api/database/seeds/data/ico
ns/images/custom_objects/asset.svg'
'/tmp/mcafee_mvision_cdf/asset.json' -> '/var/www/api/database/seeds/data/cu
stom_objects/asset.json'
Installing Custom Objects - Step 1 of 5 (Entering Maintenance Mode)

Application is now in maintenance mode.
Installing Custom Objects - Step 2 of 5 (Installing the Asset Custom Object)
Installing Custom Objects - Step 3 of 5 (Configuring image for Asset Custom
Object)
Installing Custom Objects - Step 4 of 5 (Updating Permissions in ThreatQ)
Installing Custom Objects - Step 5 of 5 (Exiting Maintenance Mode)

Application is now live.
[root@localhost mcafee_mvision_cdf]#
```

g. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
<> rm -rf mcafee_mvision_cdf
```

Manually

Use the following commands to manually install the required custom object.

a. Navigate to the API directory:

```
<> cd /var/www/api/
```

b. Put your ThreatQ instance into maintenance mode:

```
<> sudo php artisan down
```

c. Upload the asset.json file to the following directory:

`/var/www/api/database/seeds/data/custom_objects/`

d. Upload the asset.svg icon file to the following directory:

`/var/www/api/database/seeds/data/icons/images/custom_objects/`

e. Run the following command to install the Custom Object Definition:

```
<> sudo php artisan threatq:make-object-set --file=/var/www/
   api/database/seeds/data/custom_objects/asset.json
```

f. Run the following commands to assign the SVG icons to the custom objects:

```
<> sudo php artisan threatq:object-settings --code=asset --
   icon=/var/www/api/database/seeds/data/icons/images/
   custom_objects/asset.svg --background-color='#0A9D85'
```

g. Update the ThreatQ object permissions:

```
<> sudo php /var/www/api/artisan threatq:update-permissions
```

h. Take your ThreatQ instance out of maintenance mode and restart Dynamo:

```
<> sudo php artisan up

   sudo systemctl restart threatq-dynamo
```

Client ID / Secret Credentials Access

Confirm that your Client ID/Secret Credentials have access to the following scopes:

- ins.user
- ins.suser
- ins.ms.r
- epo.device.r
- epo.device.w
- epo.tags.r
- epo.tags.w
- epo.evt.r
- epo.taggroup.r

Generating MVISION Client Credentials (API Keys)

Client Credentials (API Keys) are obtained via McAfee's MVISION Marketplace, found here:

https://www.mcafee.com/enterprise/en-us/solutions/mvision/marketplace.html

> As of the date of this publication, ThreatQuotient does not have a configurable entry on the MVISION Marketplace. You can use the IBM Security App for QRadar to generate the Client Credentials that are required to use ThreatQ integrations.

Perform the following steps to generate these Client Credentials using QRadar:

1. Navigate to the McAfee MVISION Marketplace: https://www.mcafee.com/enterprise/en-us/solutions/mvision/marketplace.html.
2. Enter **McAfee MVISION App for IBM QRadar** in the search bar and select the auto-completed entry.
3. Click on the **Configure** button for the marketplace entry.
4. Complete the **Instance URL** field.

   > The URL can be any value as you are not actually connecting to a QRadar instance.
   >
   > Recommendation: Enter `https://127.0.0.1` if you do not have a QRadar instance.

5. Click on the **Refresh** button located above the Client Credential fields.
6. Use the checkboxes to agree to McAfee's user-agreements.
7. Click the **Connect** button to save the configuration.
8. Copy your **McAfee API Key**, **Cloud Client ID**, and **Cloud Client Secret**, and store them in a safe location.

Installation

> The CDF requires the installation of a custom object before installing the actual CDF. See the Prerequisites chapter for more details. The custom object must be installed prior to installing the CDF. Attempting to install the CDF without the custom object will cause the CDF install process to fail.

Perform the following steps to install the integration:

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

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration file on your local machine

   > ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.
6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

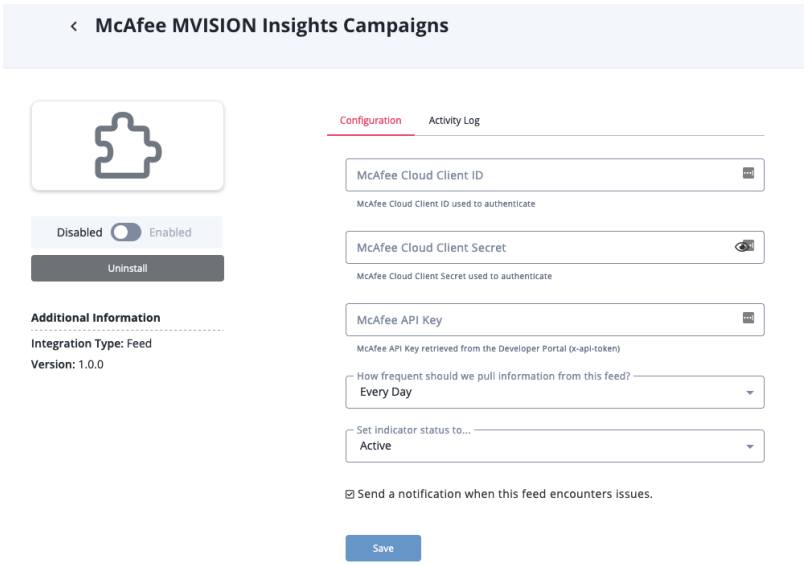
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
McAfee API Key	Your McAfee API Key retrieved from the Developer Portal (x-api-token).
McAfee Cloud Client ID	Your McAfee Cloud Client ID used to authenticate. See the Generating MVISION Client Credentials (API Keys) section of the Prerequisites chapter for steps to obtain McAfee Cloud credentials.
McAfee Cloud Client Secret	Your McAfee Cloud Client Secret used to authenticate. See the Generating MVISION Client Credentials (API Keys) section of the Prerequisites chapter for steps to obtain McAfee Cloud credentials.



5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

McAfee MVISION Insights Campaigns

The McAfee MVISION Insights Campaigns feed brings in campaigns & related context from the McAfee MVISION Insights App.

`GET https://api.mvision.mcafee.com/insights/v2/campaigns`

Sample Response:


```
{
    "links": {
        "self": "https://api.mvision.mcafee.com/insights/v2/campaigns/0026519b-ad7b-11ea-9477-02d538d9640e?
include=prevalence,last_detected_on&page[limit]=1000&page[sort]=updated-on"
    },
    "data": [
      {
            "type": "campaigns",
            "id": "0026519b-ad7b-11ea-9477-02d538d9640e",
            "links": {
                "self": "https://api.mvision.mcafee.com/insights/v2/campaigns/0026519b-ad7b-11ea-9477-02d538d9640e"
            },
            "attributes": {
                "name": "The Stealthy Email Stealer in the TA505 Arsenal",
                "description": "The TA505 threat group targeted the banking sector with spear-phishing emails that
contained a malicious attachment and installed the FlawedAmmyy remote access trojan. The RAT was used to drop an
email stealer to harvest credentials from multiple software applications.",
                "threat-level-id": 2,
                "kb-article-link": null,
                "coverage": {
                    "dat_version": {
                        "min": 4388
                    }
                },
                "updated-on": "2021-05-07T09:35:25.000Z",
                "external-analysis": {
                    "links": [
                        "https://blog.yoroi.company/research/the-stealthy-email-stealer-in-the-ta505-arsenal/"
                    ]
                },
                "is-coat": 1,
                "prevalence": {
                    "nodes": 4.53,
                    "events": 10.5,
                    "sectors": [
                        {
                            "sector": "Unknown",
                            "affected": 19.76,
                            "events": 45.81,
                            "total": 1000000
                        }
                    ],
```

```
                    "countries": [
                        {
                            "iso_code": "IT",
                            "affected": 94.31,
                            "events": 270.24,
                            "total": 1000000
                        }
                    ],
                    "countriesTotalDevices": 1000000
                }
            },
            "relationships": {
                "iocs": {
                    "links": {
                        "self": "https://api.mvision.mcafee.com/insights/v2/campaigns/0026519b-
ad7b-11ea-9477-02d538d9640e/relationships/iocs",
                        "related": "https://api.mvision.mcafee.com/insights/v2/campaigns/0026519b-
ad7b-11ea-9477-02d538d9640e/iocs"
                    }
                },
                "galaxies": {
                    "links": {
                        "self": "https://api.mvision.mcafee.com/insights/v2/campaigns/0026519b-
ad7b-11ea-9477-02d538d9640e/relationships/galaxies",
                        "related": "https://api.mvision.mcafee.com/insights/v2/campaigns/0026519b-
ad7b-11ea-9477-02d538d9640e/galaxies"
                    }
                }
            }
        }
    ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.name	Campaign.Value	N/A	.data[].attributes.created-on	The Stealthy Email Stealer in the TA505 Arsenal	N/A
.data[].attributes.description	Campaign.Description	N/A	N/A	The TA505 threat group targeted the banking sector..	Gets the first 64000 characters of the description and adds .data[].attributes.kb-article-link
.data[].attributes.updated-on	Campaign.Ended_at	N/A	N/A	2021-05-07T09:35:25	N/A
.data[].attributes.kb-article-link	Campaign.Attribute	Knowledgebase Article Link	.data[].attributes.created-on	https://kc.mcafee.com/corporate/index?page=content&id=KB93433	N/A
.data[].attributes.threat-level-id	Campaign.Attribute	Threat Level	.data[].attributes.created-on	1	Mapped by using the `Threat Level` mapping table below
.data[].attributes.prevalence.countries[].iso_code	Campaign.Attribute	Affected Country Code	.data[].attributes.created-on	IT	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.external-analysis.links[]	Campaign.Attribute	External Analysis	.data[].attributes.created-on	N/A	N/A
.data[].attributes.is-coat	Campaign.Attribute	Analysed by Coat Team	.data[].attributes.created-on	0	Mapped to bool (1 => True, 0 => False)

The feed calls the `McAfee Insights IOC Data` and `McAfee Insights Galaxies Data` supplemental feeds using `.data[].id` as `campaign_id` parameter.

McAfee Threat Level to ThreatQ Mapping

The Threat Level (as found in `.data[].attributes.threat.severity`) to ThreatQ Type mapping is as follows:

MCAFEE THREAT LEVEL	THREATQ INDICATOR TYPE
1	Unverified
2	Low
3	Medium
4	High
5	Very High

McAfee Insights IOC Data (Supplemental)

The McAfee Insights IOC Data feed fetches related IOCs to a given Campaign.

`GET https://api.mvision.mcafee.com/insights/v2/campaigns/{{campaign_id}}/iocs`

Sample Response:


```
{
    "links": {
        "self": "https://api.mvision.mcafee.com/insights/v2/campaigns/0026519b-ad7b-11ea-9477-02d538d9640e/iocs",
        "first": "https://api.mvision.mcafee.com/insights/v2/campaigns/0026519b-ad7b-11ea-9477-02d538d9640e/iocs?
page[limit]=500&page[offset]=0",
        "last": "https://api.mvision.mcafee.com/insights/v2/campaigns/0026519b-ad7b-11ea-9477-02d538d9640e/iocs?
page[limit]=500&page[offset]=0",
        "prev": null,
        "next": null
    },
    "data": [
        {
            "type": "iocs",
            "id": "00936f77-ad7b-11ea-9477-02d538d9640e",
            "links": {
                "self": "https://api.mvision.mcafee.com/insights/v2/iocs/00936f77-ad7b-11ea-9477-02d538d9640e"
            },
            "attributes": {
                "type": "ip",
                "value": "178.48.154.38",
                "coverage": null,
                "uid": "32aa0246-385d-4aae-b4f7-3bf68c1620a9",
                "is-coat": 0,
                "is-sdb-dirty": 0,
                "category": "Network activity",
                "comment": "",
                "lethality": null,
                "determinism": null,
                "created-on": "2020-06-13T13:37:19.000Z"
            },
            "relationships": {
                "campaigns": {
                    "links": {
                        "self": "https://api.mvision.mcafee.com/insights/v2/iocs/00936f77-
ad7b-11ea-9477-02d538d9640e/relationships/campaigns",
                        "related": "https://api.mvision.mcafee.com/insights/v2/iocs/00936f77-
ad7b-11ea-9477-02d538d9640e/campaigns"
                    }
                }
            }
        }
    ]
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.value	Indicator.Value	N/A	.data[].attributes.created-on	4746854f043cdde2d28420e3d733f5d916bef929	N/A
.data[].attributes.type	Indicator.Type	N/A	N/A	sha1	Mapped by using the `IOC Type` mapping table below
.data[].attributes.is-sdb-dirty	Indicator.Attribute	Potentially Malicious	.data[].attributes.created-on	1	Mapped to bool (1 => True, 0 => False)
.data[].attributes.lethality	Indicator.Attribute	Lethality	.data[].attributes.created-on	20	N/A
.data[].attributes.comment	Indicator.Attribute	Comment	.data[].attributes.created-on	RIG EK redirecting host	N/A
.data[].attributes.category	Indicator.Attribute	Category	.data[].attributes.created-on	Network activity	N/A
.data[].attributes.is-coat	Indicator.Attribute	Analysed by Coat Team	.data[].attributes.created-on	0	Mapped to bool (1 => True, 0 => False)
.data[].attributes.threat.name	Indicator.Attribute	Threat Name	.data[].attributes.created-on	pinksbot-hn	N/A
.data[].attributes.threat.classification	Indicator.Attribute	Classification	.data[].attributes.created-on	Trojan	N/A
.data[].attributes.threat.severity	Indicator.Attribute	Severity	.data[].attributes.created-on	1	Mapped by using the `Threat Severity` mapping table below

McAfee IOC Type to ThreatQ Mapping

The IOC Type (as found in `.data[].attributes.type`) to ThreatQ Type mapping is as follows:

MCAFEE INDICATOR TYPE	THREATQ INDICATOR TYPE
sha1	SHA-1
sha256	SHA-256
sha384	SHA-384
sha512	SHA-512
ip	IP Address
md5	MD5
fqdn	FQDN
url	URL

McAfee Threat Severity to ThreatQ Mapping

The Threat Severity (as found in `.data[].attributes.threat.severity`) to ThreatQ Type mapping is as follows:

MCAFEE THREAT SEVERITY	THREATQ INDICATOR TYPE
1	Unverified
2	Low

MCAFEE THREAT SEVERITY	THREATQ INDICATOR TYPE
3	Medium
4	High
5	Very High

McAfee Insights Galaxies Data (Supplemental)

The McAfee Insights Galaxies Data feed fetches related Galaxy Data to a given Campaign.

`GET https://api.mvision.mcafee.com/insights/v2/campaigns/{{campaign_id}}/galaxies`

Sample Response:


```
{
    "data": [
        {
            "attributes": {
                "category": "mcafee-tool",
                "description": "The RIG exploit kit (EK) has been in operation since at least 2013. The EK directs
users from legitimate sites to the actor's landing page using malicious iframes or malvertising campaigns. Adobe
Flash and Microsoft Internet Explorer vulnerabilities are targeted and used to drop ransomware, botnets, trojans,
loaders, stealers, and crypto miners. Use of RIG started to decline in 2017 but is still used in campaigns throughout
the world.",
                "name": "Rig Exploit Kit"
            },
            "id": "05b53e57-b97a-11eb-9d72-02d538d9640e",
            "links": {
                "self": "https://api.mvision.mcafee.com/insights/v2/galaxies/05b53e57-b97a-11eb-9d72-02d538d9640e"
            },
            "relationships": {
                "campaigns": {
                    "links": {
                        "related": "https://api.mvision.mcafee.com/insights/v2/galaxies/05b53e57-
b97a-11eb-9d72-02d538d9640e/campaigns",
                        "self": "https://api.mvision.mcafee.com/insights/v2/galaxies/05b53e57-
b97a-11eb-9d72-02d538d9640e/relationships/campaigns"
                    }
                }
            },
            "type": "galaxies"
        }
    ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.name	Adversary.Name	N/A	N/A	UNC2452	Ingested if `.data[].attributes.category` contains `threat-actor`
.data[].attributes.description	Adversary.Description	N/A	N/A	Has been in operation since at least 2013	Ingested if `.data[].attributes.category` contains `threat-actor`
.data[].attributes.name	Malware.Value	N/A	N/A	KhRAT	Ingested if `.data[].attributes.category` ends with `malware` or is one of: `rat`, `tool`, `malpedia`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.description	Malware.Description	N/A	N/A	Has been in operation since at least 2013	Ingested if `.data[].attributes.category` ends with `malware` or is one of: `rat`, `tool`, `malpedia`
.data[].attributes.name	Tool.Value	N/A	N/A	Campo Loader	Ingested if `.data[].attributes.category` is `mcafee-tool`
.data[].attributes.description	Tool.Description	N/A	N/A	Has been in operation since at least 2013	Ingested if `.data[].attributes.category` is `mcafee-tool`
.data[].attributes.name	Campaign.Attribute	Affected Sector	N/A	Political party	Ingested if `.data[].attributes.category` is `sector`
.data[].attributes.name	Value	Attack Pattern	N/A	Exploitation for Privilege Escalation	Ingested if `.data[].attributes.category` is `mcafee-attack-pattern`

McAfee MVISION ePO Events

The McAfee MVISION ePO Events feed brings in assets (hosts/devices) with threat events from McAfee MVISION ePO.

```
GET https://api.mvision.mcafee.com/epo/v2/events
```

Sample Response:


```
{
    "data": [
        {
            "agent_id": "be3879aa-2836-4901-a016-dd40316e9094",
            "attributes": {
                "agentguid": "be3879aa-2836-4901-a016-dd40316e9094",
                "analyzer": "ENDP_AM_1070",
                "analyzerdatversion": "4519.0",
                "analyzerdetectionmethod": "On-Access Scan",
                "analyzerengineversion": "6300.9389",
                "analyzerhostname": "DESKTOP-RIS67BS",
                "analyzeripv4": "192.168.15.128",
                "analyzeripv6": "/0:0:0:0:0:ffff:c0a8:f80",
                "analyzermac": "000c29960917",
                "analyzername": "McAfee Endpoint Security",
                "analyzerversion": "10.7.0.2787",
                "autoguid": "bc4fddc4-a679-491a-bd0b-fa552f6db45c",
                "detectedutc": "1629466300000",
                "nodepath": "1\\970278\\970481",
                "receivedutc": "1629466357375",
                "sourcefilepath": null,
                "sourcehostname": null,
                "sourceipv4": "192.168.15.128",
                "sourceipv6": "/0:0:0:0:0:ffff:c0a8:f80",
                "sourcemac": null,
                "sourceprocesshash": null,
                "sourceprocessname": "C:\\Windows\\explorer.exe",
                "sourceprocesssigned": null,
                "sourceprocesssigner": null,
                "sourceurl": null,
                "sourceusername": null,
                "targetfilename": "C:\\Users\\Admin\\Downloads\\Keylogger.Ardamax\
\ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18",
                "targethash": "e33af9e602cbb7ac3634c2608150dd18",
                "targethostname": null,
                "targetipv4": "192.168.15.128",
                "targetipv6": "/0:0:0:0:0:ffff:c0a8:f80",
                "targetmac": null,
                "targetport": null,
                "targetprocessname": null,
                "targetprotocol": null,
                "targetusername": null,
                "threatactiontaken": "IDS_ALERT_ACT_TAK_DEL",
                "threatcategory": "av.detect",
                "threateventid": 1027,
                "threathandled": true,
                "threatname": "Spy-Agent.cv",
```

```
                "threatseverity": "2",
                "threattype": "trojan",
                "timestamp": "2021-08-20T13:32:37.376Z"
            },
            "id": "59974a79-f887-47eb-ae22-52ca30e47a6f",
            "links": {
                "self": "/epo/v2/events/59974a79-f887-47eb-ae22-52ca30e47a6f"
            },
            "type": "MVEvents"
        }
    ],
    "links": {
        "next": "/epo/v2/events?page[limit]=1&page[cursor]=514aa1b5-3303-4be8-
ae76-7904b2810bc3_%3A_2021-08-04T04%3A15%3A03.648Z&filter[timestamp][GT]=2021-05-07T09%3A35%3A25.000Z"
    }
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.[analyzername, threatname, threatseverity, analyzeripv4]	Event.Title	Sighting	.data[].attributes.detectedutc	McAfee Endpoint Security detected a threat - None (Severity: Info) - 172.16.113.58	N/A
.data[].attributes.agentguid	Event.Attribute	Agent GUID	.data[].attributes.timestamp	be3879aa-2836-4901-a016-dd40316e9094	N/A
.data[].attributes.analyzername	Event.Attribute	Analyzer	.data[].attributes.timestamp	McAfee Endpoint Security	N/A
.data[].attributes.analyzerdetectionmethod	Event.Attribute	Analyzed Detection Method	.data[].attributes.timestamp	On-Access Scan	N/A
.data[].attributes.threatactiontaken	Event.Attribute	Action Taken	.data[].attributes.timestamp	IDS_ALERT_ACT_TAK_DEL	N/A
.data[].attributes.targetusername	Event.Attribute	Target Username	.data[].attributes.timestamp	root	N/A
.data[].attributes.targetport	Event.Attribute	Target Port	.data[].attributes.timestamp	21	N/A
.data[].attributes.targetfilename	Indicator.Value	File Path	.data[].attributes.timestamp	C:\Users\Admin\Downloads\Keylogger	N/A
.data[].attributes.targethash	Indicator.Value	MD5	.data[].attributes.timestamp	e33af9e602cbb7ac3634c2608150dd18	N/A
.data[].attributes.sourceipv4	Indicator.Value	IP Address	.data[].attributes.timestamp	192.168.15.128	As long as it's not the same as the device IP
.data[].attributes.targetipv4	Indicator.Value	IP Address	.data[].attributes.timestamp	192.168.15.128	As long as it's not the same as the device IP
.data[].attributes.targetprocessname	Indicator.Value	Filename	.data[].attributes.timestamp	Keylogger	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.threatname	Event.Attribute, Indicator.Attribute	Threat Name	.data[].attributes.timestamp	Spy-Agent.cv	N/A
.data[].attributes.threatcategory	Event.Attribute, Indicator.Attribute	Threat Category	.data[].attributes.timestamp	av.detect	N/A
.data[].attributes.threattype	Event.Attribute, Indicator.Attribute	Threat Type	.data[].attributes.timestamp	trojan	N/A
.data[].attributes.threatseverity	Event.Attribute, Indicator.Attribute	Severity	.data[].attributes.timestamp	2	Mapped by using the Threat Severity mapping table below

The feed calls the `McAfee ePO Device by Agent ID` supplemental feed using `.data[].attributes.agentguid` parameter.

McAfee Threat Severity to ThreatQ Type Mapping

The Threat Severity (as found in `.data[].attributes.threatseverity`) to ThreatQ Type mapping is as follows:

MCAFEE THREAT SEVERITY	THREATQ INDICATOR TYPE
1	Alert
2	Critical
3	Warning
4	Unknown
5	Notice
6	Info

McAfee ePO Device by Agent ID (Supplemental)

The McAfee ePO Device by Agent ID feed fetches a single device by its' ID, from McAfee MVISION via the ePO endpoint.

`GET https://api.mvision.mcafee.com/epo/v2/devices`

Sample Response:


```
{
    "data": [
        {
            "attributes": {
                "agentGuid": "77B72506-C48A-11EB-2B4F-000C29960917",
                "agentPlatform": "Windows 10:10:0:0",
                "agentState": 0,
                "agentVersion": "5.7.2.162",
                "computerName": "DESKTOP-RIS67BS",
                "cpuSpeed": 2304,
                "cpuType": "Intel(R) Core(TM) i9-9880H CPU @ 2.30GHz",
                "domainName": "WORKGROUP",
                "excludedTags": "",
                "ipAddress": "192.168.15.128",
                "ipHostName": "DESKTOP-RIS67BS.localdomain",
                "isPortable": "portable",
                "lastUpdate": "2021-06-03T18:15:54.533+00:00",
                "macAddress": "000C29960917",
                "managed": "1",
                "managedState": 1,
                "name": "DESKTOP-RIS67BS",
                "nodeCreatedDate": "2021-06-03T17:13:34.347+00:00",
                "nodePath": null,
                "numOfCpu": 4,
                "osPlatform": "Workstation",
                "osType": "Windows 10",
                "osVersion": "10.0",
                "parentId": 113382,
                "tags": "Escalated, Workstation",
                "tenantId": 5643,
                "totalPhysicalMemory": 8588865536,
                "userName": "Admin"
            },
            "id": "180385",
            "links": {
                "self": "https://api.mvision.mcafee.com/epo/v2/devices/180385"
            },
            "relationships": {
                "assignedTags": {
                    "links": {
                        "related": "https://api.mvision.mcafee.com/epo/v2/devices/180385/assignedTags",
                        "self": "https://api.mvision.mcafee.com/epo/v2/devices/180385/relationships/assignedTags"
                    }
                },
                "epoGroup": {
                    "links": {
                        "related": "https://api.mvision.mcafee.com/epo/v2/devices/180385/epoGroup",
```

```
                        "self": "https://api.mvision.mcafee.com/epo/v2/devices/180385/relationships/epoGroup"
                    }
                },
                "installedProducts": {
                    "links": {
                        "related": "https://api.mvision.mcafee.com/epo/v2/devices/180385/installedProducts",
                        "self": "https://api.mvision.mcafee.com/epo/v2/devices/180385/relationships/
installedProducts"
                    }
                }
            },
            "type": "devices"
        }
    ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.domainName + '/' + .data[].attributes.name]	Asset.Value	N/A	.data[].attributes.nodeCreatedAt	WORKGROUP/ DESKTOP-RIS67BS	Keys concatenated together
.data[].attributes.tags	Asset.Tag	N/A	N/A	Workstation, Escalated	N/A
.data[].attributes.agentGuid	Asset.Attribute	Agent GUID	.data[].attributes.nodeCreatedAt	N/A	N/A
.data[].attributes.agentPlatform	Asset.Attribute	Agent Platform	.data[].attributes.nodeCreatedAt	Windows 10:10:0:0	N/A
.data[].attributes.agentState	Asset.Attribute	Agent State	.data[].attributes.nodeCreatedAt	0	`Online` if .data[].attributes.agentState = 1, else is `Offline`
.data[].attributes.computerName	Asset.Attribute	Computer Name	.data[].attributes.nodeCreatedAt	DESKTOP-RIS67BS	N/A
.data[].attributes.cpuType	Asset.Attribute	CPU Type	.data[].attributes.nodeCreatedAt	Intel(R) Core(TM) i9-9880H CPU @ 2.30GHz	N/A
.data[].attributes.domainName	Asset.Attribute	Domain Name	.data[].attributes.nodeCreatedAt	WORKGROUP	N/A
.data[].attributes.ipAddress	Asset.Attribute	IP Address	.data[].attributes.nodeCreatedAt	192.168.15.102	N/A
.data[].attributes.numOfCpu	Asset.Attribute	Number of CPUs	.data[].attributes.nodeCreatedAt	4	N/A
.data[].attributes.osPlatform	Asset.Attribute	OS Platform	.data[].attributes.nodeCreatedAt	Workstation	N/A
.data[].attributes.osType	Asset.Attribute	Operating System	.data[].attributes.nodeCreatedAt	Windows 10	N/A
.data[].attributes.userName	Asset.Attribute	Username	.data[].attributes.nodeCreatedAt	Admin	N/A
.data[].attributes.managedState	Asset.Attribute	Is Managed	.data[].attributes.nodeCreatedAt	True	bool -> string

McAfee MVISION Insights Events

The McAfee MVISION Insights Events feed ingests assets (hosts/devices) with threat events relating to a campaign within the McAfee MVISION Insights App.

```
GET https://api.mvision.mcafee.com/insights/v2/events
```

Sample Response:


```
{
    "data": [
        {
            "attributes": {
                "campaign-id": "df7a511d-ad7a-11ea-9477-02d538d9640e",
                "customer-details": {
                    "epo_server_id": null,
                    "epo_tenant_id": "6c9e422fae3d45089d772838daab4142",
                    "ma_id": "77b72506c48a11eb2b4f000c29960917"
                },
                "exec-uid": "992b96c2c48f11eba49706354c5c4b89",
                "md5": "84c82835a5d21bbcf75a61706d8ab549",
                "timestamp": "2021-06-03T17:17:33.000Z"
            },
            "links": {},
            "type": "events"
        }
    ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.md5	Indicator.Value	MD5	.data[].attributes.timestamp	84c82835a5d21bbcf75a61706d8ab549	N/A
.data[].attributes.sha1	Indicator.Value	SHA-1	.data[].attributes.timestamp	61c65d46eb23d8064692865f80e02f1b3bdac245	N/A
.data[].attributes.sha256	Indicator.Value	SHA-256	.data[].attributes.timestamp	3ce665e28a4626973d252af6d1a6d969f378e2d9aaf120c0f862061fd6384b5e	N/A

The feed calls the `McAfee Insights Campaign by ID` supplemental feed using `.data[].attributes['campaign-id']` as `campaign_id` parameter.

McAfee Insights Campaign by ID (Supplemental)

The McAfee Insights Campaign by ID feed fetches a single campaign by its' ID, from McAfee MVISION via the Insights endpoint.

`GET https://api.mvision.mcafee.com/insights/v2/campaigns/{{campaign_id}}`

Sample Response:


```
{
    "links": {
        "self": "https://api.mvision.mcafee.com/insights/v2/campaigns/0026519b-ad7b-11ea-9477-02d538d9640e"
    },
    "data": {
        "type": "campaigns",
        "id": "0026519b-ad7b-11ea-9477-02d538d9640e",
        "links": {
            "self": "https://api.mvision.mcafee.com/insights/v2/campaigns/0026519b-ad7b-11ea-9477-02d538d9640e"
        },
        "attributes": {
            "name": "The Stealthy Email Stealer in the TA505 Arsenal",
            "description": "The TA505 threat group targeted the banking sector with spear-phishing emails that
contained a malicious attachment and installed the FlawedAmmyy remote access trojan. The RAT was used to drop an
email stealer to harvest credentials from multiple software applications.",
            "threat-level-id": 2,
            "kb-article-link": null,
            "coverage": {
                "dat_version": {
                    "min": 4388
                }
            },
            "updated-on": "2021-05-07T09:35:25.000Z",
            "external-analysis": {
                "links": [
                    "https://blog.yoroi.company/research/the-stealthy-email-stealer-in-the-ta505-arsenal/"
                ]
            },
            "is-coat": 1,
            "created-on": "2020-06-13T13:37:18.000Z"
        },
        "relationships": {
            "iocs": {
                "links": {
                    "self": "https://api.mvision.mcafee.com/insights/v2/campaigns/0026519b-
ad7b-11ea-9477-02d538d9640e/relationships/iocs",
                    "related": "https://api.mvision.mcafee.com/insights/v2/campaigns/0026519b-
ad7b-11ea-9477-02d538d9640e/iocs"
                }
            },
            "galaxies": {
                "links": {
                    "self": "https://api.mvision.mcafee.com/insights/v2/campaigns/0026519b-
ad7b-11ea-9477-02d538d9640e/relationships/galaxies",
                    "related": "https://api.mvision.mcafee.com/insights/v2/campaigns/0026519b-
ad7b-11ea-9477-02d538d9640e/galaxies"
                }
```

```
            }
        }
    }
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.attributes.name	Campaign.Value	N/A	.data.attributes.created-on	WannaCry Ransomware	N/A
.data.attributes.description	Campaign.Description	N/A	N/A	Over the course of Friday, May 12, 2017 McAfee received reports ..	N/A
.data.attributes.kb-article-link	Campaign.Attribute	Knowledgebase Article Link	.data.attributes.created-on	https://kc.mcafee.com/corporate/index?page=content&id=KB93433	N/A
.data.attributes.threat-level-id	Campaign.Attribute	Threat Level	.data.attributes.created-on	1	Mapped by using the `Threat Level` mapping table below
.data.attributes.external-analysis.links[]	Campaign.Attribute	External Analysis	.data.attributes.created-on	N/A	N/A
.data.attributes.is-coat	Campaign.Attribute	Analyzed by Coat Team	.data.attributes.created-on	1	N/A

McAfee Threat Level to ThreatQ Type Mapping

The Threat Level (as found in `.data[].attributes.threat-level-id`) to ThreatQ Type mapping is as follows:

MCAFEE THREAT LEVEL	THREATQ INDICATOR TYPE
1	Unverified
2	Low
3	Medium
4	High
5	Very High

McAfee MVISION Threat Research

The McAfee MVISION Threat Research feed brings in reports from McAfee's Threat Research RSS feed.

```
GET https://ui-mcafee.mvision.mcafee.com/rest/contentfeed/v1/mcafeelabs
```

Sample Response:


```
[
    {
      "link": "https://www.mcafee.com/blogs/other-blogs/mcafee-labs/the-rise-of-deep-learning-for-detection-and-
classification-of-malware/",
      "dc:creator": "McAfee Labs",
      "guid": {
        "isPermaLink": false,
        "content": "/blogs/?p=126041"
      },
      "description": "<div><img width=\"300\" height=\"200\" src=\"https://www.mcafee.com/wp-content/uploads/
2021/08/300x200_RiseofDeepLearning.jpg\" class=\"attachment-medium size-medium wp-post-image\" alt=\"\"
loading=\"lazy\" style=\"margin-bottom: 15px;\" srcset=\"https://www.mcafee.com/wp-content/uploads/
2021/08/300x200_RiseofDeepLearning.jpg 300w, https://www.mcafee.com/wp-content/uploads/
2021/08/300x200_RiseofDeepLearning-194x129.jpg 194w\" sizes=\"(max-width: 300px) 100vw, 300px\" /><\/div>\n<p>Co-
written by Catherine Huang, Ph.D. and Abhishek Karnik  Artificial Intelligence (AI) continues to evolve and has made
huge progress over the last decade. AI shapes our daily lives. Deep learning is a subset of techniques in AI
that...<\/p>\n<p>The post <a rel=\"nofollow\" href=\"https://www.mcafee.com/blogs/other-blogs/mcafee-labs/the-rise-
of-deep-learning-for-detection-and-classification-of-malware/\">The Rise of Deep Learning for Detection and
Classification of Malware<\/a> appeared first on <a rel=\"nofollow\" href=\"https://www.mcafee.com/blogs\">McAfee
Blogs<\/a>.<\/p>\n",
      "title": "The Rise of Deep Learning for Detection and Classification of Malware",
      "category": "McAfee Labs",
      "content:encoded": "<div><img width=\"300\" height=\"200\" src=\"https://www.mcafee.com/wp-content/uploads/
2021/08/300x200_RiseofDeepLearning.jpg\" class=\"attachment-medium size-medium wp-post-image\" alt=\"\"
loading=\"lazy\" style=\"margin-bottom: 15px;\" srcset=\"https://www.mcafee.com/wp-content/uploads/
2021/08/300x200_RiseofDeepLearning.jpg 300w, https://www.mcafee.com/wp-content/uploads/
2021/08/300x200_RiseofDeepLearning-194x129.jpg 194w\" sizes=\"(max-width: 300px) 100vw, 300px\" /><\/div><p><span
data-contrast=\"auto\">C<\/span><span data-contrast=\"auto\">o-written by Catherine Huang,
Ph.D. and Abhishek Karnik<\/span><span data-ccp-props=\"{}\"> <\/span><\/p>\n<p><span data-
contrast=\"auto\">Artificial Intelligence (AI) continues to evolve and has made huge progress over the
last decade. AI shapes our daily lives. Deep learning is a subset of techniques in AI that extract patterns from data
using neural networks. Deep learning has been applied to image segmentation, protein structure, machine translation,
speech recognition and robotics. It has outperformed human champions in the game of <\/span><i><span data-
contrast=\"auto\">Go<\/span><\/i><span data-contrast=\"auto\">. In recent years, deep learning has been applied to
malware analysis. Different types of deep learning algorithms, such as convolutional neural networks (CNN), recurrent
neural networks and Feed-Forward networks, have been applied to a variety of use cases in malware analysis using
bytes sequence, gray-scale image, structural entropy, API call sequence, HTTP traffic and network behavior. <\/
span><span data-ccp-props=\"{}\"> <\/span><\/p>\n<p><span data-contrast=\"auto\">Most traditional machine learning
malware classification and detection approaches rely on handcrafted features. These features are selected based on
experts with domain knowledge. Feature engineering can be a very time-consuming process, and handcrafted features may
not generalize well to novel malware. In this blog, we briefly describe how we apply CNN on raw bytes for malware
detection and classification in real-world data.<\/span><span data-ccp-props=\"{}\"> <\/span><\/p>\n<ol>\n<li data-
leveltext=\"%1.\" data-font=\"Calibri\" data-listid=\"1\" aria-setsize=\"-1\" data-aria-posinset=\"1\" data-aria-
level=\"1\">\n<h4><strong>CNN on Raw Bytes <\/strong><\/h4>\n<\/li>\n<\/ol>\n<p><img loading=\"lazy\" class=\"size-
full wp-image-126044\" src=\"/wp-content/uploads/2021/08/Figure-1-CNNs-on-raw-bytes-for-malware-detection-and-
classification.png\" alt=\"Figure 1: CNNs on raw bytes for malware detection and classification\" width=\"846\"
height=\"241\" srcset=\"https://www.mcafee.com/wp-content/uploads/2021/08/Figure-1-CNNs-on-raw-bytes-for-malware-
```

detection-and-classification.png 846w, https://www.mcafee.com/wp-content/uploads/2021/08/Figure-1-CNNs-on-raw-bytes-for-malware-detection-and-classification-300x85.png 300w, https://www.mcafee.com/wp-content/uploads/2021/08/Figure-1-CNNs-on-raw-bytes-for-malware-detection-and-classification-768x219.png 768w, https://www.mcafee.com/wp-content/uploads/2021/08/Figure-1-CNNs-on-raw-bytes-for-malware-detection-and-classification-205x58.png 205w\" sizes=\"(max-width: 846px) 100vw, 846px\" /><\/p>\n<p><span data-contrast=\"auto\">The motivation for applying deep learning is to identify new patterns in raw bytes. The novelty of this work is threefold. First, there is no domain-specific feature extraction and pre-processing. Second, it is an end-to-end deep learning approach. It can also perform end-to-end classification. And it can be a feature extractor for feature augmentation. Third, the explainable AI (XAI) provides insights on the CNN decisions and help human identify interesting patterns across malware families. As shown in Figure 1, the input is only raw bytes and labels. CNN performs representation learning to automatically learn features and classify malware. <\/span><span data-ccp-props=\"{}\"> <\/span><\/p>\n<h4 style=\"padding-left: 40px;\">2. Experimental Results <\/strong><\/h4>\n<p><span data-contrast=\"auto\">For the purposes of our experiments with malware detection, we first gathered 833,000 distinct binary samples (Dirty and Clean) across multiple families, compilers and varying \u201cfirst-seen\u201d time periods. There were large groups of samples from common families although they did utilize varying packers, obfuscators. Sanity checks were performed to discard samples that were corrupt, too large or too small, based on our experiment. From samples that met our sanity check criteria, we extracted raw bytes from these samples and utilized them for conducting multiple experiments. The data was randomly divided into a training and a test set with an 80% / 20% split. We utilized this data set to run the three experiments. <\/span><span data-ccp-props=\"{}\"> <\/span><\/p>\n<p><span data-contrast=\"auto\">In our first experiment, raw bytes from the 833,000 samples were fed to the CNN and the performance accuracy in terms of area under receiver operating curve (ROC) was 0.9953. <\/span><span data-ccp-props=\"{"335559731":720}\"> <\/span><\/p>\n<p><span data-contrast=\"auto\">One observation with the initial run was that, after raw byte extraction from the 833,000 unique samples, we did find duplicate raw byte entries. This was primarily due to malware families that utilized hash-busting as an approach to polymorphism. Therefore, in our second experiment, we deduplicated the extracted raw byte entries. This reduced the raw byte input vector count to 262,000 samples. The test area under ROC was 0.9920.<\/span><span data-ccp-props=\"{"335559731":720}\"> <\/span><\/p>\n<p><span data-contrast=\"auto\">In our third experiment, we attempted multi-family malware classification. We took a subset of 130,000 samples from the original set and labeled 11 categories \u2013 the 0<\/span><span data-contrast=\"auto\">th<\/span><span data-contrast=\"auto\"> were bucketed as Clean, 1-9 of which were malware families,<\/span><span data-contrast=\"auto\"> <\/span><span data-contrast=\"auto\">and the 10<\/span><span data-contrast=\"auto\">th<\/span><span data-contrast=\"auto\"> were bucketed as Others. Again, these 11 buckets contain samples with varying packers and compilers. We performed another 80 / 20% random split for the training set and test set. For this experiment, we achieved a test accuracy of 0.9700. The training and test time on one GPU was 26 minutes. <\/span><span data-ccp-props=\"{}\"> <\/span><\/p>\n<h4 style=\"padding-left: 40px;\">3. Visual Explanation <\/strong><\/h4>\n<figure id=\"attachment_126047\" aria-describedby=\"caption-attachment-126047\" style=\"width: 928px\" class=\"wp-caption aligncenter\"><figcaption id=\"caption-attachment-126047\" class=\"wp-caption-text\">Figure 2: A visual explanation using T-SNE and PCA before and after the CNN training<\/figcaption><\/figure>\n<p><span data-contrast=\"auto\">To understand the CNN training process, we performed a visual analysis for the CNN training. Figure 2 shows the t-Distributed Stochastic Neighbor Embedding (t-SNE) and Principal Component Analysis (PCA) for before and after CNN training. We can see that after training, CNN is able to extract useful representations to capture characteristics of different types of malware as shown in different clusters. There was a good separation for most categories, lending us to believe that the algorithm was useful as a multi-class classifier.<\/span><span data-ccp-props=\"{}\"> <\/span><\/p>\n<p><span data-contrast=\"auto\">We then performed XAI to understand CNN\u2019s decisions. Figure 3 shows XAI heatmaps for one sample of Fareit and one sample of Emotet. The brighter the color is the more important the bytes contributing to the gradient activation in neural networks. Thus, those bytes are important to CNN\u2019s decisions. We were interested in understanding the bytes that weighed in heavily on the decision-making and reviewed some samples manually.<\/span><span data-ccp-props=\"{"335559731":720}\"> <\/span><\/p>\n<figure id=\"attachment_126050\" aria-describedby=\"caption-attachment-126050\" style=\"width: 829px\" class=\"wp-caption aligncenter\"><img loading=\"lazy\" class=\"size-full wp-image-126050\" src=\"/wp-content/uploads/2021/08/Figure-3-XAI-heatmaps-on-Fareit-left-and-Emotet-right.png\" alt=\"Figure 3: XAI heatmaps on Fareit (left) and Emotet (right)\" width=\"829\" height=\"603\" srcset=\"https://www.mcafee.com/wp-content/uploads/2021/08/Figure-3-XAI-heatmaps-on-Fareit-left-and-Emotet-right.png 829w, https://www.mcafee.com/wp-content/uploads/2021/08/Figure-3-XAI-heatmaps-on-Fareit-left-and-Emotet-right-300x218.png 300w,

https://www.mcafee.com/wp-content/uploads/2021/08/Figure-3-XAI-heatmaps-on-Fareit-left-and-Emotet-right-768x559.png 768w, https://www.mcafee.com/wp-content/uploads/2021/08/Figure-3-XAI-heatmaps-on-Fareit-left-and-Emotet-right-177x129.png 177w\" sizes=\"(max-width: 829px) 100vw, 829px\" /><figcaption id=\"caption-attachment-126050\" class=\"wp-caption-text\">Figure 3: XAI heatmaps on Fareit (left) and Emotet (right)<\/figcaption><\/figure>\n<h4 style=\"padding-left: 40px;\"><span class=\"TextRun Underlined SCXW196196725 BCX0\" lang=\"EN-US\" xml:lang=\"EN-US\" data-contrast=\"auto\"><span class=\"NormalTextRun SCXW196196725 BCX0\">4. Human analysis<\/span><span class=\"NormalTextRun SCXW196196725 BCX0\"> to understand the ML decision and XAI <\/span><\/span><span class=\"EOP SCXW196196725 BCX0\" data-ccp-props=\"{"134233279":true}\"> <\/span><\/strong><\/h4>\n<figure id=\"attachment_126053\" aria-describedby=\"caption-attachment-126053\" style=\"width: 1024px\" class=\"wp-caption aligncenter\"><figcaption id=\"caption-attachment-126053\" class=\"wp-caption-text\">Figure 4: Human analysis on CNN\u2019s predictions<\/figcaption><\/figure>\n<p><span class=\"TextRun SCXW174722149 BCX0\" lang=\"EN-US\" xml:lang=\"EN-US\" data-contrast=\"auto\"><span class=\"NormalTextRun SCXW174722149 BCX0\">To verify if the CNN can learn new patterns, <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">we fed a<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\"> few <\/span><span class=\"NormalTextRun ContextualSpellingAndGrammarErrorV2 SCXW174722149 BCX0\">never before seen<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\"> samples to the CNN<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">,<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\"> and requested a <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">human expert to <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">verify the <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">CNN\u2019s decision<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\"> <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">on<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\"> <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">some<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\"> random <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">samples<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">. The human <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">analysis <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">verified<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\"> <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">that <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">the <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">CNN <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">was able to <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">correctly <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">identify <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">many <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">malware families<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">. <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">In some cases, it identified samples accurately before the to<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">p 15 <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">AV <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">vendors based on our internal tests<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">. Figure 4 shows a subset of samples that belong to the <\/span><span class=\"NormalTextRun SpellingErrorV2 SCXW174722149 BCX0\">Nabucur<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\"> family that <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">were correctly ca<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">tegorized by the CNN despite having no <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">vendor detection<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\"> at that point in time<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">. <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">It<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">\u2019s<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\"> <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">also <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">interesting to note that o<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">ur results <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">showed that the CNN was able to <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">currently <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">categorize <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">malware <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">samples <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">across families utilizing common packers<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\"> into an accurate family <\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">bucket<\/span><span class=\"NormalTextRun SCXW174722149 BCX0\">.<\/span><\/span><span class=\"EOP SCXW174722149 BCX0\" data-ccp-props=\"{}\"> <\/span><\/p>\n<figure id=\"attachment_126056\" aria-describedby=\"caption-attachment-126056\" style=\"width: 1024px\" class=\"wp-caption aligncenter\"><img loading=\"lazy\" class=\"size-large wp-image-126056\" src=\"/wp-content/uploads/2021/08/Figure-5-domain-analysis-on-sample-compiler-1024x155.png\" alt=\"Figure 5: domain analysis on sample compiler\" width=\"1024\" height=\"155\" srcset=\"https://www.mcafee.com/wp-content/uploads/2021/08/Figure-5-domain-analysis-on-sample-compiler-1024x155.png 1024w, https://www.mcafee.com/wp-content/uploads/2021/08/Figure-5-domain-analysis-on-sample-compiler-300x45.png 300w, https://www.mcafee.com/wp-content/uploads/

```
2021/08/Figure-5-domain-analysis-on-sample-compiler-768x116.png 768w, https://www.mcafee.com/wp-content/uploads/
2021/08/Figure-5-domain-analysis-on-sample-compiler-205x31.png 205w, https://www.mcafee.com/wp-content/uploads/
2021/08/Figure-5-domain-analysis-on-sample-compiler.png 1239w\" sizes=\"(max-width: 1024px) 100vw, 1024px\" /
><figcaption id=\"caption-attachment-126056\" class=\"wp-caption-text\">Figure 5: domain analysis on sample
compiler<\/figcaption><\/figure>\n<p><span data-contrast=\"auto\">We ran domain analysis on the same sample complier
VB files. As shown in Figure 5, CNN was able to identify two samples of a threat family before other vendors. CNN
agreed with MSMP/other vendors on two samples. In this experiment, the CNN incorrectly identified one sample as
Clean. <\/span><span data-ccp-props=\"{}\"> <\/span><\/p>\n<figure id=\"attachment_126059\" aria-
describedby=\"caption-attachment-126059\" style=\"width: 523px\" class=\"wp-caption aligncenter\"><img
loading=\"lazy\" class=\"wp-image-126059 size-full\" src=\"/wp-content/uploads/2021/08/Figure-6-human-analysis-on-an-
XAI-heatmap.-Left-is-the-result-disassembly-of-part-of-decryption-tea-algorithm-from-Hiew-tool..png\" alt=\"Figure 6:
Human analysis on an XAI heatmap. Above is the resulting disassembly of part of the decryption tea algorithm from the
Hiew tool.\" width=\"523\" height=\"221\" srcset=\"https://www.mcafee.com/wp-content/uploads/2021/08/Figure-6-human-
analysis-on-an-XAI-heatmap.-Left-is-the-result-disassembly-of-part-of-decryption-tea-algorithm-from-Hiew-tool..png
523w, https://www.mcafee.com/wp-content/uploads/2021/08/Figure-6-human-analysis-on-an-XAI-heatmap.-Left-is-the-
result-disassembly-of-part-of-decryption-tea-algorithm-from-Hiew-tool.-300x127.png 300w, https://www.mcafee.com/wp-
content/uploads/2021/08/Figure-6-human-analysis-on-an-XAI-heatmap.-Left-is-the-result-disassembly-of-part-of-
decryption-tea-algorithm-from-Hiew-tool.-205x87.png 205w\" sizes=\"(max-width: 523px) 100vw, 523px\" /><figcaption
id=\"caption-attachment-126059\" class=\"wp-caption-text\">Figure 6: Human analysis on an XAI heatmap. Above is the
resulting disassembly of part of the decryption tea algorithm from the Hiew tool.<\/figcaption><\/figure>\n<figure
id=\"attachment_126062\" aria-describedby=\"caption-attachment-126062\" style=\"width: 418px\" class=\"wp-caption
aligncenter\"><img loading=\"lazy\" class=\"wp-image-126062 size-full\" src=\"/wp-content/uploads/2021/08/Figure-6-
Right-is-an-XAI-heatmap-for-one-sample..png\" alt=\"Above is XAI heatmap for one sample.\" width=\"418\"
height=\"484\" srcset=\"https://www.mcafee.com/wp-content/uploads/2021/08/Figure-6-Right-is-an-XAI-heatmap-for-one-
sample..png 418w, https://www.mcafee.com/wp-content/uploads/2021/08/Figure-6-Right-is-an-XAI-heatmap-for-one-
sample.-259x300.png 259w, https://www.mcafee.com/wp-content/uploads/2021/08/Figure-6-Right-is-an-XAI-heatmap-for-one-
sample.-111x129.png 111w\" sizes=\"(max-width: 418px) 100vw, 418px\" /><figcaption id=\"caption-attachment-126062\"
class=\"wp-caption-text\">Above is XAI heatmap for one sample.<\/figcaption><\/figure>\n<p><span data-
contrast=\"auto\">We asked a human expert to inspect an XAI heatmap and verify if those bytes in bright color are
associated with the malware family classification. Figure 6 shows one sample which belongs to the Sodinokibi family.
The bytes identified by the XAI (c3 8b 4d 08 03 d1 66 c1) are interesting because the byte sequence belongs to part
of the Tea decryption algorithm. This indicates these bytes are associated with the malware classification, which
confirms the CNN can learn and help identify useful patterns which humans or other automation may have overlooked.
Although these experiments were rudimentary, they were indicative of the effectiveness of the CNN in identifying
unknown patterns of interest. <\/span><span data-ccp-props=\"{}\"> <\/span><\/p>\n<p><span data-contrast=\"auto\">In
summary, the experimental results and visual explanations demonstrate that CNN can automatically learn PE raw byte
representations. CNN raw byte model can perform end-to-end malware classification. CNN can be a feature extractor for
feature augmentation. The CNN raw byte model has the potential to identify threat families before other vendors and
identify novel threats. These initial results indicate that CNN\u2019s can be a very useful tool to assist automation
and human researcher in analysis and classification. Although we still need to conduct a broader range of
experiments, it is encouraging to know that our findings can already be applied for early threat triage,
identification, and categorization which can be very useful for threat prioritization. <\/span><span data-ccp-
props=\"{&quot;335559731&quot;:720}\"> <\/span><\/p>\n<p><span data-contrast=\"auto\">We believe that McAfee\u2019s
ongoing AI research, such as deep learning-based approaches, leads the security industry to tackle the evolving
threat landscape, and we look forward to continuing to share our findings in this space with the security
community.<\/span><span data-ccp-props=\"{&quot;335559731&quot;:720}\"> <\/span><\/p>\n<p>The post <a
rel=\"nofollow\" href=\"https://www.mcafee.com/blogs/other-blogs/mcafee-labs/the-rise-of-deep-learning-for-detection-
and-classification-of-malware/\">The Rise of Deep Learning for Detection and Classification of Malware<\/a> appeared
first on <a rel=\"nofollow\" href=\"https://www.mcafee.com/blogs\">McAfee Blogs<\/a>.<\/p>\n",
      "pubDate": "Fri, 13 Aug 2021 00:50:48 +0000"
    }
]
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].title	Report.Value	N/A	[].pubDate	The Rise of Deep Learning for Detection and Classification of Malware	N/A
[].description	Report.Description	N/A	N/A		Formatted using generic description formatter
[].link	Report.Attribute	Reference	[].pubDate	https://www.mcafee.com/blogs/other-blogs/mcafee-labs/detection-and-classification-of-malware/	N/A
[].dc:creator	Report.Attribute	Creator	[].pubDate	McAfee Labs	N/A
[].category	Report.Attribute	Category	[].pubDate	McAfee Labs	N/A
[].description	Indicator.Value	MD5	[].pubDate	3449523cdf7ef61bfa8e86eac05ad27b	Parsed out of the description. The status of the indicator is `Review`.
[].description	Indicator.Value	SHA-1	[].pubDate	61c65d46eb23d8064692865f80e02f1b3bdac245	Parsed out of the description. The status of the indicator is `Review`.
[].description	Indicator.Value	SHA-256	[].pubDate	3ce665e28a4626973d252af6d1a6d969f378e2d9aaf120c0f862061fd6384b5e	Parsed out of the description. The status of the indicator is `Review`.
[].description	Indicator.Value	SHA-512	[].pubDate	827e4ba7de2b18d2a5a2ae0b03fd3933bf1fd0557b2de8a6a36d0f54c96c645fbec9bbcae18804bc619d537363d297415797cdaac7727e81e5035c5fb58ee9c4	Parsed out of the description. The status of the indicator is `Review`.
[].description	Indicator.Value	CVE	[].pubDate	CVE-2019-1458	Parsed out of the description. The status of the indicator is `Review`.
[].description	Indicator.Value	IP Address	[].pubDate	172.17.0.31	Parsed out of the description. The status of the indicator is `Review`.

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.

McAfee MVISION Insights Campaigns

METRIC	RESULT
Run Time	9 minutes
Campaigns	6
Campaign Attributes	116
Adversaries	2
Indicators	7,211
Indicator Attributes	42,476
Malware	4
Tools	19

McAfee MVISION ePO Events

METRIC	RESULT
Run Time	1 minute
Assets	2
Asset Attributes	26
Indicators	2
Events	2
Event Attributes	10

McAfee MVISION Insights Events

METRIC	RESULT
Run Time	1 minute
Assets	2
Asset Attributes	26
Indicators	2
Campaigns	2
Campaign Attributes	10

McAfee MVISION Threat Research

METRIC	RESULT
Run Time	1 minute
Reports	10
Report Attributes	32
Indicators	53

Known Issues / Limitations

- If the MvAfee MVISION ePO Events feed is run for multiple days, the Activity Log will display one run per day.

  > Performing a run for January 17-19, the Activity Log will display two runs, one for January 17-18 and one for January 18-19.

Change Log

- **Version 1.0.0**
  - Initial release