ThreatQuotient

MITRE ATT&CK CDF Guide

Version 1.0.0 rev-a

February 23, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 4.3.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/mitre-att-ck-cdf

Introduction

The MITRE ATT&CK CDF retrieves a list of adversaries, intrusion set, course of actions, malware objects, attack partners and tools, along with their attributes.

The CDF provides the following feeds:

- **MITRE Enterprise ATT&CK** - retrieves the content of the `Enterprise ATT&CK` collection. It retrieves a list of adversaries, intrusion set, course of actions, malware objects, attack partners and tools, along with their attributes.
- **MITRE PRE-ATT&CK** - retrieves the content of the `PRE-ATT&CK` collection. It retrieves a list of adversaries, intrusion sets and attack patterns, along with their attributes.
- **MITRE Mobile ATT&CK** - retrieves the content of the `Mobile ATT&CK` collection. It retrieves a list of adversaries, intrusion set, course of actions, malware objects, attack partners and tools, along with their attributes.

The integration ingests the following system objects:

- Adversaries / Intrusion Sets
  - Adversary /Intrusion Set Attributes
- Attack Patterns
  - Attack Pattern Attributes
- Course of Action
  - Course of Action Attributes
- Malware
  - Malware Attributes
- Tools
  - Tool Attributes

Installation

Perform the following steps to install the integration:

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

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

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

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

Configuration

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

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** 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 entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Verify SSL	Enable or disable verification of the server's SSL certificate.
Host CA	Enter your base64 PEM encoded CA Certificate bundle to verify against the provider's SSL. You can leave this field blank if you did not enable the Verify SSL option listed above.
Disable Proxies	Select whether the feed should honor the proxies set on the ThreatQ platform.
Save Intrusion Set as	MITRE provides Threat Actor data as Intrusion Sets. Select how you will save the information. Options include: ◦ Adversaries (default) ◦ Intrusion Sets

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

All feeds access the same endpoint, `https://cti-taxii.mitre.org/taxii/`, each requesting the content of a specific collection.

MITRE Enterprise ATT&CK

The MITRE Enterprise ATT&CK feed retrieves the content of the `Enterprise ATT&CK` collection. It retrieves a list of adversaries, intrusion set, course of actions, malware objects, attack patterns, and tools, along with their attributes.

Sample Response:


```
{
  "objects": [
    {
      "created": "2021-10-08T14:06:28.212Z",
      "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
      "description": "Adversaries may downgrade or use a version of system features that may be outdated, vulnerable, and/or does not support updated security controls..",
      "external_references": [
        {
          "external_id": "T1562.010",
          "source_name": "mitre-attack",
          "url": "https://attack.mitre.org/techniques/T1562/010"
        },
        {
          "description": "Falcon Complete Team. (2021, May 11). Response When Minutes Matter: Rising Up Against Ransomware. Retrieved October 8, 2021.",
          "source_name": "CrowdStrike BGH Ransomware 2021",
          "url": "https://www.crowdstrike.com/blog/how-falcon-complete-stopped-a-big-game-hunting-ransomware-attack/"
        }
      ],
      "id": "attack-pattern--824add00-99a1-4b15-9a2d-6c5683b7b497",
      "kill_chain_phases": [
        {
          "kill_chain_name": "mitre-attack",
          "phase_name": "defense-evasion"
        }
      ],
      "modified": "2021-10-15T00:48:06.723Z",
      "name": "Downgrade Attack",
      "object_marking_refs": [
        "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
      ],
      "type": "attack-pattern",
      "x_mitre_data_sources": [
        "Command: Command Execution",
        "Process: Process Creation"
      ],
      "x_mitre_detection": "Monitor for commands or other activity that may be indicative of attempts to abuse older or deprecated technologies (ex: <code>powershell –v 2</code>). ",
```

```
      "x_mitre_is_subtechnique": true,
      "x_mitre_permissions_required": [
        "User"
      ],
      "x_mitre_platforms": [
        "Windows"
      ],
      "x_mitre_version": "1.0",
      "x_mitre_system_requirements": [
        "Some folders may require Administrator, SYSTEM or specific user depending on permission levels and access
controls"
      ],
      "x_mitre_is_subtechnique:" true,
      "x_mitre_network_requirements": true
    },
    {
      "created": "2021-03-18T13:39:27.676Z",
      "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
      "description": "[ConnectWise](https://attack.mitre.org/software/S0591) is a legitimate remote administration
tool that has been used since at least 2016 by threat actors including [MuddyWater](https://attack.mitre.org/groups/
G0069) and [GOLD SOUTHFIELD](https://attack.mitre.org/groups/G0115) to connect to and conduct lateral movement in
target environments.(Citation: Anomali Static Kitten February 2021)(Citation: Trend Micro Muddy Water March 2021)",
      "external_references": [
        {
          "external_id": "S0591",
          "source_name": "mitre-attack",
          "url": "https://attack.mitre.org/software/S0591"
        },
        {
          "description": "Peretz, A. and Theck, E. (2021, March 5). Earth Vetala – MuddyWater Continues to Target
Organizations in the Middle East. Retrieved March 18, 2021.",
          "source_name": "Trend Micro Muddy Water March 2021",
          "url": "https://www.trendmicro.com/en_us/research/21/c/earth-vetala---muddywater-continues-to-target-
organizations-in-t.html"
        }
      ],
      "id": "tool--842976c7-f9c8-41b2-8371-41dc64fbe261",
      "labels": [
        "tool"
      ],
      "modified": "2021-03-18T14:54:01.053Z",
      "name": "ConnectWise",
      "object_marking_refs": [
        "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
      ],
      "type": "tool",
      "x_mitre_aliases": [
        "ScreenConnect"
      ],
      "x_mitre_platforms": [
        "Windows"
      ],
      "x_mitre_version": "1.0"
    },
    {
        "created":"2020-10-19T14:57:58.771Z",
        "created_by_ref":"identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
        "description":"This category is used for any applicable mitigation activities that apply to techniques
occurring before an adversary gains Initial Access, such as Reconnaissance and Resource Development techniques.",
        "external_references":[
          {
```

```
            "external_id":"M1056",
            "source_name":"mitre-attack",
            "url":"https://attack.mitre.org/mitigations/M1056"
          }
        ],
        "id":"course-of-action--78bb71be-92b4-46de-acd6-5f998fedf1cc",
        "modified":"2020-10-20T19:52:32.439Z",
        "name":"Pre-compromise",
        "object_marking_refs":[
          "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
        ],
        "type":"course-of-action",
        "x_mitre_version":"1.0"
      },
    {
        "created":"2018-04-18T17:59:24.739Z",
        "created_by_ref":"identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
        "description":"[Hydraq](https://attack.mitre.org/software/S0203) is a data-theft trojan first used by
[Elderwood](https://attack.mitre.org/groups/G0066) in the 2009 Google intrusion ...",
        "external_references":[
          {
            "external_id":"S0203",
            "source_name":"mitre-attack",
            "url":"https://attack.mitre.org/software/S0203"
          },
          {
            "description":"Falcone, R. & Miller-Osborn, J. (2015, September 23). Chinese Actors Use \u20183102\u2019
Malware in Attacks on US Government and EU Media. Retrieved March 19, 2018.",
            "source_name":"PaloAlto 3102 Sept 2015",
            "url":"https://researchcenter.paloaltonetworks.com/2015/09/chinese-actors-use-3102-malware-in-attacks-on-
us-government-and-eu-media/"
          }
        ],
        "id":"malware--73a4793a-ce55-4159-b2a6-208ef29b326f",
        "labels":[
          "malware"
        ],
        "modified":"2021-01-06T19:32:28.374Z",
        "name":"Hydraq",
        "object_marking_refs":[
          "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
        ],
        "type":"malware",
        "x_mitre_aliases":[
       "Hydraq",
          "9002 RAT"
        ],
        "x_mitre_platforms":[
          "Windows"
        ],
        "x_mitre_version":"1.1"
      },
    {
      "aliases": [
        "APT33",
        "Elfin"
      ],
      "created": "2018-04-18T17:59:24.739Z",
      "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
      "description": "[APT33](https://attack.mitre.org/groups/G0064) is a suspected Iranian threat group that has
carried out operations since at least 2013.",
```

```
      "external_references": [
        {
          "external_id": "G0064",
          "source_name": "mitre-attack",
          "url": "https://attack.mitre.org/groups/G0064"
        },
        {
          "description": "(Citation: FireEye APT33 Sept 2017) (Citation: FireEye APT33 Webinar Sept 2017)",
          "source_name": "APT33"
        }
      ],
      "id": "intrusion-set--fbd29c89-18ba-4c2d-b792-51c0adee049f",
      "modified": "2021-05-26T12:40:42.907Z",
      "name": "APT33",
      "object_marking_refs": [
        "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
      ],
      "type": "intrusion-set",
      "x_mitre_version": "1.4"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.objects[].external_references[].external_id - .objects[].name	Attack Pattern / Course Of Action / Malware.Value	N/A	.objects[].created	T0803 - Block Command Message	If .objects[].type is `attack-pattern`
.objects[].name	Adversary / Intrusion set / Malware.Value	N/A	.objects[].created	APT17	If .objects[].type is `intrusion-set`
.objects[].description	All objects.Description	N/A	.objects[].created	Adversaries may block a command message from reaching..	N/A
.objects[].external_references[].external_id	Attack Pattern.Attribute	Technique ID	.objects[].created	T1546.009	N/A
.objects[].external_references[].external_id	Related Adversary/ Intrusion Set.Attribute	Group ID	.objects[].created	G0034	If .objects[].external_references[].source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[].external_id	Course Of Action.Attribute	Mitigation ID	.objects[].created	M1014	If .objects[].external_references[].source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[].external_id	Tool.Attribute	Tool ID	.objects[].created	S0298	If .objects[].external_references[].source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[].external_id	Malware.Attribute	Malware ID	.objects[].created	S0321	If .objects[].external_references[].source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[].description	All objects.Attribute	External Reference	.objects[].created	Gregory Scasny. (2015, September 14). Understanding Open Source Intelligence (OSINT) ..	N/A
.objects[].external_references[].url	All objects.Attribute	External Reference	.objects[].created	https://attack.mitre.org/mitigations/M1009	N/A
.objects[].object_marking_refs	All objects.Attribute	Statement Marking	.objects[].created	marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168	If .objects[].external_references[].source_name is `marking-definition`. Used to filter in to obtain the marking definition (`Copyright 2015-2021, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.`)
.objects[].x_mitre_contributors[]	All objects.Attribute	Contributor	.objects[].created	Dragos Threat Intelligence	N/A
.objects[].modified	All objects.Attribute	Modified At	.objects[].created	2020-10-26T13:42:49.342Z	N/A
.objects[].x_mitre_deprecated	All objects.Attribute	Deprecated	.objects[].created	true	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.objects[].kill_chain_phases[].phase_name	Attack Pattern.Attribute	Tactic	.objects[].created	Privilege Escalation	N/A
.objects[].x_mitre_difficulty_for_adversary	Attack Pattern.Attribute	Effective Permissions	.objects[].created	Administrator	N/A
.objects[].x_mitre_detection	Attack Pattern.Attribute	Detection	.objects[].created	Monitor DLL loads by processes, specifically looking for DLLs that are not recognized or not normally loaded into a process.	N/A
.objects[].x_mitre_data_sources[]	Attack Pattern.Attribute	Data Source	.objects[].created	Command: Command Execution	N/A
.objects[].x_mitre_permissions_required[]	Attack Pattern.Attribute	Permissions Required	.objects[].created	System	N/A
.objects[].x_mitre_system_requirements	Attack Pattern.Attribute	System Requirements	.objects[].created	Some Folders May Require Administrator, System Or Specific User Depending On Permission Levels And Access Controls	N/A
.objects[].x_mitre_defense_bypassed	Attack Pattern.Attribute	Defense Bypassed	.objects[].created	Application Control	N/A
.objects[].x_mitre_effective_permissions[]	Attack Pattern.Attribute	Effective Permissions	.objects[].created	Administrator	N/A
.objects[].x_mitre_network_requirements	Attack Pattern.Attribute	Network Requirements	.objects[].created	true	N/A
.objects[].x_mitre_remote_support	Attack Pattern.Attribute	Remote Support	.objects[].created	true	N/A
.objects[].x_mitre_platforms[]	Attack Pattern / Tool / Malware.Attribute	Platform	.objects[].created	Android	N/A
.objects[].revoked	Attack Pattern / Intrusion set / Malware.Attribute	Revoked	.objects[].created	true	N/A
.objects[].aliases[]	Related Adversary/ Intrusion Set.Value	Alias	.objects[].created	Palmetto Fusion	N/A
.objects[].labels[]	Tool / Malware.Attribute	Label	.objects[].created	tool	N/A

MITRE PRE-ATT&CK

This feed retrieves the content of the `PRE-ATT&CK` collection. It retrieves a list of adversaries, intrusion sets and attack patterns, along with their attributes.

Sample Response:


```
{
  "objects": [
    {
      "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
      "kill_chain_phases": [
        {
          "phase_name": "organizational-information-gathering",
          "kill_chain_name": "mitre-pre-attack"
        }
      ],
      "x_mitre_old_attack_id": "PRE-T1058",
      "x_mitre_detectable_by_common_defenses_explanation": "Adversary may download templates or branding from
publicly available presentations that the defender cannot monitor.",
      "type": "attack-pattern",
      "x_mitre_detectable_by_common_defenses": "No",
      "external_references": [
        {
          "external_id": "T1281",
          "source_name": "mitre-pre-attack",
          "url": "https://attack.mitre.org/techniques/T1281"
        },
        {
          "source_name": "Scasny2015",
          "description": "Gregory Scasny. (2015, September 14). Understanding Open Source Intelligence (OSINT) and
its relationship to Identity Theft. Retrieved March 1, 2017."
        }
      ],
      "modified": "2020-10-26T13:42:49.342Z",
      "x_mitre_deprecated": true,
      "x_mitre_version": "1.0",
      "created": "2017-12-14T16:46:06.044Z",
      "id": "attack-pattern--68b45999-bb0c-4829-bbd0-75d6dac57c94",
      "x_mitre_difficulty_for_adversary": "Yes",
      "description": "This object is deprecated as its content has been merged into the enterprise domain. Please see
the...",
      "x_mitre_difficulty_for_adversary_explanation": "Some branding information is publicly available when a
corporation publishes their briefings to the internet which provides insight into branding information and template
materials.  An exhaustive list of templating and branding is likely not available on the internet.",
      "name": "Obtain templates/branding materials",
      "object_marking_refs": [
        "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
      ]
    },
    {
      "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
      "external_references": [
        {
          "source_name": "mitre-attack",
          "url": "https://attack.mitre.org/groups/G0025",
          "external_id": "G0025"
```

```
        },
        {
          "source_name": "APT17",
          "description": "(Citation: FireEye APT17)"
        },
        {
          "source_name": "Deputy Dog",
          "description": "(Citation: FireEye APT17)"
        },
        {
          "source_name": "FireEye APT17",
          "url": "https://www2.fireeye.com/rs/fireye/images/APT17_Report.pdf",
          "description": "FireEye Labs/FireEye Threat Intelligence. (2015, May 14). Hiding in Plain Sight: FireEye
and Microsoft Expose Obfuscation Tactic. Retrieved January 22, 2016."
        }
      ],
      "x_mitre_version": "1.1",
      "type": "intrusion-set",
      "object_marking_refs": [
        "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
      ],
      "created": "2017-05-31T21:31:57.307Z",
      "id": "intrusion-set--090242d7-73fc-4738-af68-20162f7a5aae",
      "aliases": [
        "APT17",
        "Deputy Dog"
      ],
      "description": "[APT17](https://attack.mitre.org/groups/G0025) is a China-based threat group that has conducted
network intrusions against U.S. government entities, the defense industry, law firms, information technology
companies, mining companies, and non-government organizations. (Citation: FireEye APT17)",
      "name": "APT17",
      "modified": "2020-10-13T22:33:14.018Z"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.objects[].external_references[].external_id - .objects[].name	Attack Pattern.Value	N/A	.objects[].created	T0803 - Block Command Message	If .objects[].type is `attack-pattern`
.objects[].name	Adversary / Intrusion set.Value	N/A	.objects[].created	APT17	If .objects[].type is `intrusion-set`
.objects[].description	All objects.Description	N/A	.objects[].created	Adversaries may block a command message from reaching..	N/A
.objects[].external_references[].external_id	Related Adversary/ Intrusion Set.Value	Group ID	.objects[].created	G0034	If .objects[].external_references[].source_name is `mitre-attack`
.objects[].external_references[].external_id	Attack Pattern.Attribute	Technique ID	.objects[].created	T1281	N/A
.objects[].external_references[].description	All objects.Attribute	External Reference	.objects[].created	Gregory Scasny. (2015, September 14). Understanding Open Source Intelligence (OSINT) ..	N/A
.objects[].modified	Adversary/ Intrusion set.Attribute, Attack Pattern.Attribute	Modified At	.objects[].created	2020-10-26T13:42:49.342Z	N/A
.objects[].x_mitre_deprecated	All objects.Attribute	Deprecated	.objects[].created	true	N/A
.objects[].x_mitre_detectable_by_common_defenses	Attack Pattern.Attribute	Detectable by Common Defenses	.objects[].created	Do	N/A
.objects[].x_mitre_detectable_by_common_defenses_explanation	Attack Pattern.Attribute	Detectable by Common Defenses Explanation	.objects[].created	Adversary may download templates or branding from publicly available presentations that the defender can't monitor.	N/A
.objects[].x_mitre_difficulty_for_adversary	Attack Pattern.Attribute	Difficulty for Adversary	.objects[].created	Dragos Threat Intelligence	N/A
.objects[].x_mitre_difficulty_for_adversary_explanation	Attack Pattern.Attribute	Difficulty for Adversary Explanation	.objects[].created	Some branding information is publicly available when a corporation publishes...	N/A
.objects[].kill_chain_phases[].phase_name	Attack Pattern.Attribute	Tactic	.objects[].created	organizational-information-gathering	N/A
.objects[].object_marking_refs	Adversary/ Intrusion set.Attribute, Attack Pattern.Attribute	Statement Marking	.objects[].created	marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168	If .objects[].external_references[].source_name is `marking-definition`. Used to filter in to obtain the marking definition (`Copyright 2015-2021, The MITRE Corporation.`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					`MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.`
.objects[].x_mitre_contributors[]s	Adversary/ Intrusion Set.Attribute	Contributor	.objects[].created	Dragos Threat Intelligence	N/A
.objects[].aliases[]	Related Adversary/ Intrusion Set.Value	Alias	.objects[].created	Palmetto Fusion	N/A

MITRE Mobile ATT&CK

This feed retrieves the content of the `Mobile ATT&CK` collection. It retrieves a list of adversaries, intrusion set, course of actions, malware objects, attack partners and tools, along with their attributes.

Sample Response:


```
{
  "objects": [
    {
      "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
      "x_mitre_version": "1.1",
      "external_references": [
        {
          "source_name": "mitre-attack",
          "url": "https://attack.mitre.org/groups/G0112",
          "external_id": "G0112"
        },
        {
          "source_name": "Bahamut",
          "description": "(Citation: SANS Windshift August 2018)"
        },
        {
          "url": "https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1554718868.pdf",
          "source_name": "SANS Windshift August 2018",
          "description": "Karim, T. (2018, August). TRAILS OF WINDSHIFT. Retrieved June 25, 2020."
        }
      ],
      "object_marking_refs": [
        "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
      ],
      "created": "2020-06-25T17:16:39.168Z",
      "id": "intrusion-set--afec6dc3-a18e-4b62-b1a4-5510e1a498d1",
      "aliases": [
        "Windshift",
        "Bahamut"
      ],
      "modified": "2021-04-26T14:37:33.234Z",
      "type": "intrusion-set",
      "name": "Windshift",
      "description": "[Windshift](https://attack.mitre.org/groups/G0112) is a threat group that has been active since
at least 2017..."
    },
    {
      "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
      "kill_chain_phases": [
        {
          "phase_name": "persistence",
          "kill_chain_name": "mitre-mobile-attack"
        }
      ],
      "created": "2017-10-25T14:48:31.294Z",
      "x_mitre_old_attack_id": "MOB-T1001",
      "x_mitre_platforms": [
        "Android",
```

```
        "iOS"
      ],
      "type": "attack-pattern",
      "external_references": [
        {
          "external_id": "T1398",
          "source_name": "mitre-mobile-attack",
          "url": "https://attack.mitre.org/techniques/T1398"
        },
        {
          "external_id": "APP-26",
          "source_name": "NIST Mobile Threat Catalogue",
          "url": "https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-26.html"
        },
        {
          "source_name": "Apple-iOSSecurityGuide",
          "url": "https://www.apple.com/business/docs/iOS_Security_Guide.pdf",
          "description": "Apple. (2016, May). iOS Security. Retrieved December 21, 2016."
        }
      ],
      "modified": "2018-10-17T00:14:20.652Z",
      "x_mitre_version": "1.0",
      "x_mitre_tactic_type": [
        "Post-Adversary Device Access"
      ],
      "x_mitre_detection": "The Android SafetyNet APIs remote attestation capability could potentially be used to
identify...",
      "id": "attack-pattern--46d818a5-67fa-4585-a7fc-ecf15376c8d5",
      "description": "If an adversary can escalate privileges, he or she may be able to use those privileges to
place...",
      "name": "Modify OS Kernel or Boot Partition",
      "object_marking_refs": [
        "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
      ]
    },
    {
      "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
      "x_mitre_version": "1.0",
      "type": "course-of-action",
      "external_references": [
        {
          "external_id": "M1014",
          "source_name": "mitre-attack",
          "url": "https://attack.mitre.org/mitigations/M1014"
        },
        {
          "source_name": "CSRIC5-WG10-FinalReport",
          "url": "https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf",
          "description": "Communications Security, Reliability, Interoperability Council (CSRIC). (2017, March)."
        }
      ],
      "created": "2017-10-25T14:48:50.181Z",
      "x_mitre_old_attack_id": "MOB-M1014",
      "id": "course-of-action--e829ee51-1caf-4665-ba15-7f8979634124",
      "object_marking_refs": [
        "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
      ],
      "modified": "2018-10-17T00:14:20.652Z",
      "name": "Interconnection Filtering",
      "description": "In order to mitigate Signaling System 7 (SS7) exploitation, the Communications, Security,
Reliability, and Interoperability ..."
```

```
    },
    {
      "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
      "labels": [
        "tool"
      ],
      "x_mitre_old_attack_id": "MOB-S0014",
      "x_mitre_platforms": [
        "Android"
      ],
      "type": "tool",
      "external_references": [
        {
          "external_id": "S0298",
          "source_name": "mitre-mobile-attack",
          "url": "https://attack.mitre.org/software/S0298"
        },
        {
          "source_name": "Xbot",
          "description": "(Citation: PaloAlto-Xbot)"
        }
      ],
      "modified": "2018-12-11T20:40:31.461Z",
      "x_mitre_version": "1.1",
      "created": "2017-10-25T14:48:48.609Z",
      "id": "tool--da21929e-40c0-443d-bdf4-6b60d15448b4",
      "object_marking_refs": [
        "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
      ],
      "x_mitre_aliases": [
        "Xbot"
      ],
      "name": "Xbot",
      "description": "[Xbot](https://attack.mitre.org/software/S0298) is an Android malware family that was observed
in 2016 primarily targeting Android users in Russia and Australia. (Citation: PaloAlto-Xbot)"
    },
    {
      "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
      "labels": [
        "malware"
      ],
      "x_mitre_old_attack_id": "MOB-S0027",
      "x_mitre_platforms": [
        "iOS"
      ],
      "type": "malware",
      "external_references": [
        {
          "external_id": "S0311",
          "source_name": "mitre-mobile-attack",
          "url": "https://attack.mitre.org/software/S0311"
        },
        {
          "source_name": "YiSpecter",
          "description": "(Citation: PaloAlto-YiSpecter)"
        }
      ],
      "modified": "2018-12-11T20:40:31.461Z",
      "x_mitre_version": "1.1",
      "created": "2017-10-25T14:48:48.301Z",
      "id": "malware--a15c9357-2be0-4836-beec-594f28b9b4a9",
```

```
      "object_marking_refs": [
        "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
      ],
      "x_mitre_aliases": [
        "YiSpecter"
      ],
      "name": "YiSpecter",
      "description": "[YiSpecter](https://attack.mitre.org/software/S0311) iOS malware that affects both jailbroken
and non-jailbroken iOS devices."
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.objects[].external_references[].external_id - .objects[].name	Attack Pattern / Course Of Action / Malware.Value	N/A	.objects[].created	T0803 - Block Command Message	If .objects[].type is `attack-pattern`
.objects[].name	Adversary / Intrusion set / Malware.Value	N/A	.objects[].created	APT17	If .objects[].type is `intrusion-set`
.objects[].description	All objects.Description	N/A	.objects[].created	Adversaries may block a command message from reaching..	N/A
.objects[].external_references[].external_id	Course Of Action.Attribute	Mitigation ID	.objects[].created	M1014	If .objects[].external_references[].source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[].external_id	Tool.Attribute	Tool ID	.objects[].created	S0298	If .objects[].external_references[].source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[].external_id	Malware.Attribute	Malware ID	.objects[].created	S0321	If .objects[].external_references[].source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[].external_id	Related Adversary/ Intrusion Set.Attribute	Group ID	.objects[].created	G0034	If .objects[].external_references[].source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[].description	All objects.Attribute	External Reference	.objects[].created	Gregory Scasny. (2015, September 14). Understanding Open Source Intelligence (OSINT) ..	N/A
.objects[].external_references[].url	All objects.Attribute	External Reference	.objects[].created	https://attack.mitre.org/mitigations/M1009	N/A
.objects[].modified	All objects.Attribute	Modified At	.objects[].created	2020-10-26T13:42:49.342Z	N/A
.objects[].object_marking_refs	All objects.Attribute	Statement Marking	.objects[].created	marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168	If .objects[].external_references[].source_name is `marking-definition`. Used to filter in to obtain the marking definition (`Copyright 2015-2021, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.`
.objects[].x_mitre_deprecated	All objects.Attribute	Deprecated	.objects[].created	true	N/A
.objects[].x_mitre_contributors[]	All objects.Attribute	Contributor	.objects[].created	Dragos Threat Intelligence	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.objects[].x_mitre_detection	Attack Pattern.Attribute	Detection	.objects[].created	Monitor DLL loads by processes, specifically looking for DLLs that are not recognized or not normally loaded into a process.	N/A
.objects[].kill_chain_phases[].phase_name	Attack Pattern.Attribute	Tactic	.objects[].created	organizational-information-gathering	N/A
.objects[].external_references[].external_id	Attack Pattern.Attribute	Technique ID	.objects[].created	T1281	N/A
.objects[].x_mitre_platforms[]	Attack Pattern / Tool / Malware.Attribute	Platform	.objects[].created	Android	N/A
.objects[].x_mitre_tactic_type	Attack Pattern.Attribute	Tactic Type	.objects[].created	Post-Adversary Device Access	N/A
.objects[].revoked	Attack Pattern.Attribute	Revoked	.objects[].created	true	N/A
.objects[].aliases[]	Related Adversary/ Intrusion Set.Value	Alias	.objects[].created	Palmetto Fusion	N/A
.objects[].labels[]	Tool / Malware.Attribute	Label	.objects[].created	tool	N/A

Average Feed Run

Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

MITRE Enterprise ATT&CK

METRIC	RESULT
Run Time	10 minutes
Attack Pattern	707
Attack Pattern Attributes	11,139
Course Of Action	267
Course Of Action Attributes	1,635
Malware	474
Malware Attributes	4,155
Adversaries / Intrusion Set	344
Adversaries / Intrusion Set Attributes	5,106
Tool	72
Tool Attributes	603

MITRE PRE-ATT&CK

METRIC	RESULT
Run Time	3 minutes
Attack Pattern	174
Attack Pattern Attributes	2,040
Adversaries / Intrusion Set	25
Adversaries / Intrusion Set Attributes	594

MITRE Mobile ATT&CK

METRIC	RESULT
Run Time	10 minutes
Attack Pattern	110
Attack Pattern Attributes	1,144
Course Of Action	13
Course Of Action Attributes	55
Malware	92
Malware Attributes	731
Adversaries / Intrusion Set	23

METRIC	RESULT
Adversaries / Intrusion Set Attributes	673
Tool	2
Tool Attributes	18

Change Log

- **Version 1.0.0 rev-a**
  - Updated the Configuration chapter to cover the **Host CA** parameter field.
- **Version 1.0.0**
  - Initial release