

ThreatQuotient



CrowdStrike Falcon X Sandbox Operation Guide

Version 1.0.0

January 07, 2021

ThreatQuotient

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

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2021 ThreatQuotient, Inc.

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

Contents

- Versioning 4
- Introduction 5
- Installation 6
- Configuration 7
- Actions 8
 - Get Reports 9
 - api.crowdstrike.com/falconx/queries/reports/v1 9
 - api.crowdstrike.com/falconx/entities/reports/v1?ids={report-id} 10
 - Submit File 18
 - api.crowdstrike.com/samples/entities/samples/v2 18
 - api.crowdstrike.com/falconx/entities/submissions/v1 18
- Change Log 20

Versioning

- **Operation Version:** 1.0.0
- **Minimum ThreatQ Version:** 4.41.0

Introduction

The CrowdStrike Falcon X Sandbox Operation submits files to Falcon X Sandbox for analysis and fetches detonation reports.

The **CrowdStrike Falcon X Sandbox CDF**, available on the ThreatQ Marketplace, is recommended to ingest reports and retrieve more context on submitted samples from Falcon X Sandbox.

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 operation 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 operation and will require user confirmation before proceeding.

6. You will still need to [configure and then enable the operation](#).

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 operation:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Operation** option from the *Type* 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
Client ID	The Falcon X Client Id used for authentication.
Client Secret	The Falcon X Secret used for authentication.

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

Actions

The CrowdStrike Falcon X Sandbox operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Get Reports	Fetches existing reports for previous detonations of file; optionally, adds Report Links and other data as attributes, and Malquery hashes as related indicators	Attachment, Indicator	Any (Attachment), SHA-256 (Indicator)
Submit File	Uploads and submits a file for detonation with the Falcon X Sandbox service	Attachment	Any

Get Reports

Fetches reports for a given file. For reports to be fetched, the file must have been submitted (i.e., either through ThreatQ or directly through CrowdStrike Falcon X Sandbox), and detonation must have completed (typically takes around 10-15 minutes).

api.crowdstrike.com/falconx/queries/reports/v1

This action makes requests to the following endpoint:

GET <https://api.crowdstrike.com/falconx/queries/reports/v1>

Sample JSON response:

```
{
  "meta": {
    "query_time": 0.038525809,
    "pagination": {
      "offset": 0,
      "limit": 10,
      "total": 75
    },
    "powered_by": "falconx-api",
    "trace_id": "b30e8593-179f-457f-aad4-47d0152771ca",
    "quota": {
      "total": 100,
      "used": 35,
      "in_progress": 0
    }
  },
  "resources": [
    "ace79a13936f4ec8ad4de36606814bfc_3f51f9d65ea34f348c1d70b5d2a54f98",
    "ace79a13936f4ec8ad4de36606814bfc_e140385178184090bd58ed105ba8703c",
    "ace79a13936f4ec8ad4de36606814bfc_b532180309fb47b7a0dae6be27afebcb",
    "ace79a13936f4ec8ad4de36606814bfc_485bf65f80f245c9901af9e718c1c93b",
    "ace79a13936f4ec8ad4de36606814bfc_92cbe2b5fcee44bdb6b8f436399f6a69",
    "ace79a13936f4ec8ad4de36606814bfc_750e30c94fff40798d78d924742a24b7",
    "ace79a13936f4ec8ad4de36606814bfc_f93360a892df43f6ae3e3add5b56186f",
    "ace79a13936f4ec8ad4de36606814bfc_4d49dd7582be4a02a47966667280716d",
    "ace79a13936f4ec8ad4de36606814bfc_cfc5b9956c6e4958bafa989abb6fdd4a",
    "ace79a13936f4ec8ad4de36606814bfc_95b49b6f295b41619b4a127022fb4f3b"
  ],
  "errors": []
}
```

api.crowdstrike.com/falconx/entities/reports/v1? ids={report-id}

Additionally, each report's details are fetched from the following endpoint:

GET <https://api.crowdstrike.com/falconx/entities/reports/v1?ids={report-id}>

Sample JSON response:

```
{
  "meta": {
    "query_time": 0.050169045,
    "powered_by": "falconx-api",
    "trace_id": "a58fe97c-3ca5-4c7c-a400-465381318d80",
    "quota": {
      "total": 100,
      "used": 40,
      "in_progress": 0
    }
  },
  "resources": [
    {
      "id": "ace79a13936f4ec8ad4de36606814bfc_9026dc9993a940c1b5e0a2a320de2307",
      "cid": "ace79a13936f4ec8ad4de36606814bfc",
      "created_timestamp": "2020-09-17T15:25:12Z",
      "origin": "apigateway",
      "verdict": "malicious",
      "ioc_report_strict_csv_artifact_id": "cb1aed69e6f4b1ebd2c59ad4470353328e103ef99013094cb823cfee3d63e1b4",
      "ioc_report_broad_csv_artifact_id": "5f47aa91082a5f534007a766b675debe41f03ede9da75126fd0956e15bd6973c",
      "ioc_report_strict_json_artifact_id": "584089ced7394f0304b12cc432e0c123f9775ae607ba2afeb5ce093cb969b9e3",
      "ioc_report_broad_json_artifact_id": "9eb0acde3ac1e75f91e880fb924e4b93126b54709b8e1dbb4a87727d1e591260",
      "ioc_report_strict_stix_artifact_id": "f62cab644b83372efa7ba2e20042ba798b05c6694b78e14f53aed5116b071ad5",
      "ioc_report_broad_stix_artifact_id": "87c6f4802fa4eaa85b33d6c707ebb9c879b36639e6a9d7ca9ec0824ce7420ac9",
      "ioc_report_strict_maec_artifact_id": "fff4482b39642d93e3a07071ed6c2243bb506be5745ebf0f73d7b9e5187928b8",
      "ioc_report_broad_maec_artifact_id": "c200269ffaca437f8e8b8b43977f87441ae0fec317e5512f7a567ef1e1c3e015",
      "sandbox": [
        {
          "sha256": "4e87a0794bf73d06ac1ce4a37e33eb832ff4c89fb9e4266490c7cef9229d27a7",
          "environment_id": 100,
          "environment_description": "Windows 7 32 bit",
          "file_size": 786432,
          "file_type": "PE32 executable (GUI) Intel 80386, for MS Windows",
          "file_type_short": [
            "peexe",
            "executable"
          ],
          "classification_tags": [
            "criminal",
            "informationstealer",
            "kpotstealer"
          ],
          "submit_name": "trojan_ponystealer",
          "submission_type": "file",
          "verdict": "malicious",
          "threat_score": 99,
          "windows_version_name": "Windows 7",

```

```
"windows_version_edition": "Professional",
"windows_version_service_pack": "Service Pack 1",
"windows_version_version": "6.1 (build 7601)",
"windows_version_bitness": 32,
"incidents": [
  {
    "name": "Remote Access",
    "details": [
      "Reads terminal service related keys (often RDP related)"
    ]
  }
],
"file_metadata": {
  "file_compositions": [
    "1 .BAS (Pseudo-Code) Files compiled with C2.EXE 6.0 (Visual Basic 6) (build: 9782)",
    "16 .BAS Files compiled with C2.EXE 5.0 (Visual Basic 6) (build: 8783)",
    "1 .ASM Files assembled with MASM 6.13 (Visual Studio 6 SP1) (build: 7299)"
  ],
  "file_analysis": [
    "File contains Visual Basic code",
    "File contains assembly code",
    "File is the product of a medium codebase (18 files)"
  ]
},
"classification": [
  "82.7% (.EXE) Win32 Executable Microsoft Visual Basic 6",
  "6.6% (.DLL) Win32 Dynamic Link Library (generic)",
  "4.5% (.EXE) Win32 Executable (generic)",
  "2.0% (.EXE) OS/2 Executable (generic)",
  "2.0% (.EXE) Generic Win/DOS Executable"
],
"dns_requests": [
  {
    "domain": "ajax.googleapis.com",
    "address": "172.217.9.138",
    "country": "United States"
  }
],
"contacted_hosts": [
  {
    "address": "172.217.5.14",
    "port": 443,
    "protocol": "TCP",
    "associated_runtime": [
      {
        "name": "iexplore.exe",
        "pid": 2424
      }
    ],
    "country": "United States"
  }
],
"http_requests": [
  {
    "host": "seeyouonlineservice.com",
    "host_ip": "173.239.5.6",
    "host_port": 80,
    "url": "/config.php",
    "method": "GET",
    "header": "GET /config.php HTTP/1.1\nAccept: text/html, application/xhtml+xml, */*\nHost: seeyouonlineservice.com\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nAccept-Encoding: gzip, deflate\nDNT: 1\nConnection: Keep-Alive"
  }
]
```

```
],
"extracted_files": [
  {
    "name": "Kipl.exe",
    "file_path": "%ALLUSERSPROFILE%\\Kipl.exe",
    "file_size": 786432,
    "sha256": "callb8ffbc782df697f34a26df930970b1ced2efbf89a34c506ae80a1cdc43bf",
    "md5": "b211348f8784ea450e1364c053046a6c",
    "sha1": "70df9df1ffe20e7eac54e424c2e76242696904d2",
    "runtime_process": "trojan_ponystealer.exe",
    "type_tags": [
      "peexe",
      "executable"
    ],
    "threat_level_readable": "no specific threat",
    "description": "PE32 executable (GUI) Intel 80386, for MS Windows"
  }
],
"extracted_interesting_strings": [
  {
    "value": "!1;for(w=0;w<t.length;w++)C=h(t[w]),null!=C&&(F=!0,M.appendChild(C));if(!F)return null)return u?(t=document.createDocumentFragment(),t.appendChild(M),t.appendChild(u),t):M)d=void 0===d?!1:d;e=void 0===e?null:e;f=void 0===f?[]:f;var k=lk(a.s),l=[],m=!Sj(c,b,\"ctc.cott\"),p=!Sj(c,b,\"ctd\"),r={},v=(r[l]=[],r[2]=[],r);r=S();a=h(a.l||{}),r,f.join(\" \"));a||(a=document.createElement(\"span\"),a.id=r);return{rootElement:a,ej:l,vi:r}}\",
    "type": "Ansi",
    "source": "Dropped File",
    "filename": "caf_1.js"
  },
  {
    "value": "Version",
    "type": "Unicode",
    "source": "Runtime Data",
    "process": "iexplore.exe"
  }
],
"signatures": [
  {
    "threat_level_human": "informative",
    "category": "General",
    "identifier": "mutant-0",
    "type": 4,
    "relevance": 3,
    "name": "Creates mutants",
    "description": "\"\\Sessions\\1\\BaseNamedObjects\\Local\\ZonesCacheCounterMutex\\\"\\n \\Sessions\\1\\BaseNamedObjects\\Local\\ZonesLockedCacheCounterMutex\\\"\\n \\Local\\ZonesLockedCacheCounterMutex\\\"\\n \\Local\\ZonesCacheCounterMutex\\\"\\n \\Sessions\\1\\BaseNamedObjects\\IsoScope_a60_IE_EarlyTabStart_0x7e0_Mutex\\\"\\n \\Sessions\\1\\BaseNamedObjects\\{5312EE61-79E3-4A24-BFE1-132B85B23C3A}\\\"\\n \\Sessions\\1\\BaseNamedObjects\\IsoScope_a60_IESQMMUTEX_0_303\\\"\\n \\Sessions\\1\\BaseNamedObjects\\IsoScope_a60_IESQMMUTEX_0_331\\\"\\n \\Sessions\\1\\BaseNamedObjects\\{66D0969A-1E86-44CF-B4EC-3806DDDA3B5D}\\\"\\n \\IsoScope_a60_IESQMMUTEX_0_303\\\"\\n \\{5312EE61-79E3-4A24-BFE1-132B85B23C3A}\\\"\\n \\IsoScope_a60_IESQMMUTEX_0_519\\\"\\n \\Local\\URLBLOCK_FILEMAPSWITCH_MUTEX_2656\\\"\\n \\{66D0969A-1E86-44CF-B4EC-3806DDDA3B5D}\\\"\",
    "origin": "Created Mutant"
  }
],
"processes": [
  {
    "uid": "00152739-00003312",
    "parent_uid": "00152502-00003404",
    "name": "schtasks.exe",
    "normalized_path": "%WINDIR%\\System32\\schtasks.exe",
    "command_line": "/Create /SC MINUTE /TN \"Eburin\" /TR \"\\\"%ALLUSERSPROFILE%\\Kipl.exe\\\"\"\",

```

```
"sha256": "15018d0093befabba8b927743191030d1f8c17bb97fdb48c2fc3eab20e2d4b3d",
"pid": 3312,
"process_flags": [
  {
    "name": "Reduced Monitoring"
  }
],
"registry": [
  {
    "operation": "Open",
    "path": "HKLM\\SYSTEM\\CURRENTCONTROLSET\\CONTROL\\SESSION MANAGER\\"
  }
],
"mutants": [
  "Local\\ZonesLockedCacheCounterMutex",
  "Local\\ZonesCacheCounterMutex"
],
"handles": [
  {
    "id": 4,
    "type": "KeyHandle",
    "path": "HKLM\\SYSTEM\\ControlSet001\\Control\\Session Manager"
  }
],
"file_accesses": [
  {
    "type": "CREATE",
    "path": "%WINDIR%\\Globalization\\Sorting\\SortDefault.nls",
    "mask": "GENERIC_READ | FILE_READ_ATTRIBUTES"
  }
]
},
"screenshots_artifact_ids": [
  "bf278d0febd27579a9f181dc369b9eb3f56cf6581f291e2193f5812385d061b7",
  "ac574d7f094cc9e096a1f04ab9b93fba19c15081d41c1f2c225da0247545a658",
  "dcea35624ebfba0376db2d0cddfa4f4351944936389fea32898d1713245f1dd4"
],
"file_imports": [
  {
    "module": "MSVBVM60.DLL",
    "functions": [
      "__vbaAryDestruct",
      "__vbaChkstk",
      "__vbaCopyBytes"
    ]
  }
],
"architecture": "32 Bit",
"version_info": [
  {
    "id": "InternalName",
    "value": "dagdrmmen"
  },
  {
    "id": "FileVersion",
    "value": "3.04.0001"
  }
],
"sample_flags": [
  "Multi-Process",
  "Network Traffic",
  "Extracted Files",
```

```
"Sample Crashed",
"Decrypted SSL traffic"
],
"mitre_attacks": [
  {
    "tactic": "Persistence",
    "technique": "Kernel Modules and Extensions",
    "attack_id": "T1215",
    "informative_identifiers": [
      "Opens the Kernel Security Device Driver (KsecDD) of Windows"
    ]
  },
  {
    "tactic": "Persistence",
    "technique": "Hooking",
    "attack_id": "T1179",
    "suspicious_identifiers": [
      "Installs hooks/patches the running process"
    ]
  },
  {
    "tactic": "Privilege Escalation",
    "technique": "Process Injection",
    "attack_id": "T1055",
    "malicious_identifiers": [
      "Writes data to a remote process",
      "Allocates virtual memory in a remote process"
    ],
    "suspicious_identifiers": [
      "Scans for the windows taskbar (may be used for explorer injection)",
      "Found a string that may be used as part of an injection method"
    ]
  },
  {
    "tactic": "Privilege Escalation",
    "technique": "Hooking",
    "attack_id": "T1179",
    "suspicious_identifiers": [
      "Installs hooks/patches the running process"
    ]
  },
  {
    "tactic": "Defense Evasion",
    "technique": "Process Injection",
    "attack_id": "T1055",
    "malicious_identifiers": [
      "Writes data to a remote process",
      "Allocates virtual memory in a remote process"
    ],
    "suspicious_identifiers": [
      "Scans for the windows taskbar (may be used for explorer injection)",
      "Found a string that may be used as part of an injection method"
    ]
  },
  {
    "tactic": "Lateral Movement",
    "technique": "Remote Desktop Protocol",
    "attack_id": "T1076",
    "suspicious_identifiers": [
      "Reads terminal service related keys (often RDP related)"
    ]
  },
  {
```

```
        "tactic": "Command and Control",
        "technique": "Data Encoding",
        "attack_id": "T1132",
        "informative_identifiers": [
            "HTTP request contains Base64 encoded artifacts"
        ]
    },
    {
        "tactic": "Command and Control",
        "technique": "Commonly Used Port",
        "attack_id": "T1043",
        "suspicious_identifiers": [
            "Sends traffic on typical HTTP outbound port, but without HTTP header"
        ]
    }
],
"pcap_report_artifact_id": "55c83b8e854766d3988fd9cc514f0c5f20d5b926d672c2ce7704eda866d6918e",
"memory_strings_artifact_id": "9d09b343414be8031ba6aabc5fd5d025b12d8276c53e740370c26fef7bb4e087"
},
"malquery": [
    {
        "verdict": "unknown",
        "input": "7.14.22.69",
        "type": "ip",
        "resources": [
            {
                "sha256": "009609f749677e0dfd71efd4cadfa91c41738bc304f34b235514be3e9731ab93",
                "md5": "7a1a988de1c9d8fc6ef69be1d032e1c4",
                "sha1": "43f72c02249131f3890915d983f8d5ddd080080f",
                "label": "unknown",
                "file_size": 65536,
                "file_type": "TEXT",
                "first_seen_timestamp": "2020-09-10T00:00:00Z"
            }
        ]
    },
    {
        "verdict": "whitelisted",
        "input": "http://a.ad",
        "type": "url"
    },
    {
        "verdict": "unknown",
        "input": "http://a.gg",
        "type": "url",
        "resources": [
            {
                "sha256": "0602d9de2e545e6a34349f2c5802d360f2b01f7968eaf52b5c283713ed24591d",
                "md5": "67720774f58d7dde07aec038764400b9",
                "sha1": "8712ab7a736f257b4e2b831fec47419a4982947a",
                "label": "unknown",
                "file_size": 753836,
                "file_type": "DALVIK",
                "first_seen_timestamp": "2014-10-01T00:00:00Z"
            }
        ]
    }
],
"threat_graph": {
    "indicators": [
        {
            "type": "sha256",
```

```
        "value": "ca11b8ffbc782df697f34a26df930970b1ced2efbf89a34c506ae80a1cdc43bf",
        "global_prevalence": "common"
      }
    ],
    "tags": [
      "informationstealer",
      "kpotstealer",
      "occamy",
      "iframeref",
      "criminal"
    ]
  },
  "errors": []
}
```

The ingested indicators and attributes are displayed as defined in the following mapping:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.resources[].id	Object.Attribute	Falcon X Sandbox Report Summary Link	https://falcon.crowdstrike.com/intelligence/sandbox/report/ace79a13936f4ec8ad4de36606814bfc_9026dc9993a940c1b5e0a2a320de2307/report-summary	Report URL is formatted from the Report ID sent by CrowdStrike
.resources[].sandbox[].sha256	Indicator.Value	SHA-256	4e87a0794bf73d06ac1ce4a37e33eb832ff4c89fb9e4266490c7cef9229d27a7w	Only displayed if the Action is executed on a file object
.resources[].malquery[].resources[].sha256	Indicator.Value	SHA-256	4e87a0794bf73d06ac1ce4a37e33eb832ff4c89fb9e4266490c7cef9229d27a7	
.resources[].malquery[].resources[].sha1	Indicator.Value	SHA-1	dee01d843ebb9c51ae17386f7be7a0ad4d6387fe	
.resources[].malquery[].resources[].md5	Indicator.Value	MD5	dd16ac44f33559f1bf194133d15bceba	
.resources[].sandbox[].resources[].origin	Object.Attribute	Origin	apigateway	
.resources[].sandbox[].classification_tags[]	Object.Attribute	Tag	APT	
.resources[].sandbox[].verdict	Object.Attribute	Verdict	malicious	
.resources[].sandbox[].file_type	Object.Attribute	File Type	PE32 executable (GUI) Intel 80386, for MS Windows	

Submit File

Uploads a file to CrowdStrike Falcon X Sandbox and submits it for detonation. Note that while this action completes quickly, the detonation and report generation typically take 10-15 minutes.

api.crowdstrike.com/samples/entities/samples/v2

This action makes requests to the following endpoints:

POST <https://api.crowdstrike.com/samples/entities/samples/v2>

Sample JSON response:

```
{
  "meta": {
    "query_time": 1.16e-7,
    "trace_id": "b3f2142f-eec7-4394-aba9-6ba2e815acce"
  },
  "resources": [
    {
      "sha256": "4e87a0794bf73d06ac1ce4a37e33eb832ff4c89fb9e4266490c7cef9229d27a7",
      "file_name": "trojan-ponystealer"
    }
  ],
  "errors": []
}
```

api.crowdstrike.com/falconx/entities/submissions/v1

POST <https://api.crowdstrike.com/falconx/entities/submissions/v1>

Sample JSON response:

```
{
  "meta": {
    "query_time": 0.116349733,
    "powered_by": "falconx-api",
    "trace_id": "29aad17d-001c-4d47-9d5a-cd54f96b77de",
    "quota": {
      "total": 100,
      "used": 35,
      "in_progress": 2
    }
  },
  "resources": [
    {
      "id": "ace79a13936f4ec8ad4de36606814bfc_eebc849ccc8646fba61f1580eeb384ec",
      "cid": "ace79a13936f4ec8ad4de36606814bfc",

```

```
"origin": "apigateway",
"state": "created",
"created_timestamp": "2020-09-17T15:25:14Z",
"sandbox": [
  {
    "sha256": "4e87a0794bf73d06ac1ce4a37e33eb832ff4c89fb9e4266490c7cef9229d27a7",
    "environment_id": 100,
    "submit_name": "trojan_ponystealer"
  }
]
},
"errors": []
}
```

Change Log

- **Version 1.0.0**
 - Initial release