ThreatQuotient

PolySwarm Operation Guide

Version 1.0.0

December 13, 2021

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

Not Supported

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 **Not Supported**.

Integrations, apps, and add-ons designated as **Not Supported** are not supported by ThreatQuotient's Customer Support team.

While you can report issues to ThreatQ's Customer Support team regarding the integration/app/add-on, you are solely responsible for ensuring proper functionality and version compatibility of Not Supported designations with the applicable ThreatQuotient software.

If unresolvable functional or compatibility issues are encountered, you may be required to uninstall the integration/app/add-on from your ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

> ⚠ For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply to issues caused by Not Supported integrations/apps/add-ons.

Versioning

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

Introduction

The PolySwarm Operation for ThreatQ enables analysts to interact with PolySwarm by performing scans on files/URLs, enriching indicators, submitting YARA rules, and more.

The operation provides the following actions:

- **Lookup** - Performs a lookup on a hash or URL to find context from PolySwarm.
- **Rescan** - Performs a Rescan for a particular hash.
- **Metadata Search** - Searches for scans using the metadata search.
- **Live Hunt** - Starts a live hunt in PolySwarm using a YARA Signature.
- **Historical Hunt** - Starts a historical hunt in PolySwarm using a YARA Signature.
- **Add Rule** - Creates a Ruleset to PolySwarm using YARA Signature.
- **Scan** - Scans a file or URL using PolySwarm.

See the Actions chapter for more information on the actions listed above.

The operation is compatible with the following object types:

- File
- Indicator (MD5, SHA-1, SHA-256, URL, FQDN, IP Address, IPv6, CVE
- Signature

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 integration:

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 parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
PolySwarm API Key	Your PolySwarm API Key found in your PolySwarm Settings.

5. Click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable the operation.

Actions

The PolySwarm Operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPES	OBJECT SUB-TYPES
Lookup	Perform a lookup on a hash or URL to find context from PolySwarm	Indicator	MD5, SHA-1, SHA-256, URL, FQDN
Rescan	Perform a Rescan for a particular hash	Indicator	MD5, SHA-1, SHA-256
Metadata Search	Search for scans using the metadata search	Indicator	IP Address, IPv6 Address, FQDN, URL, CVE
Live Hunt	Start a live hunt in PolySwarm using a YARA Signature	Signature (YARA)	N/A
Historical Hunt	Start a historical hunt in PolySwarm using a YARA Signature	Signature (YARA)	N/A
Add Rule	Create a Ruleset to PolySwarm using YARA Signature	Signature (YARA)	N/A
Scan	Scan a file or URL using PolySwarm	File, Indicator	URL, FQDN

Lookup

The Lookup action performs a lookup on a hash or URL to find context from PolySwarm.

```
GET https://api.polyswarm.network/v2/search/hash/{hash_type}?hash={hash}
```


```
{
    "sha1": "7fe6c8191749767254513b03da03cfbf6dd6c139",
    "sha256": "fadf362a52dcf884f0d41ce3df9eaa9bb30227afda50c0e0657c096baff501f0",
    "assertions": [
        {
            "engine": {
                "description": "Engine based on cloud computing, big data technologies and a database with massive
collection of confirmed malware and safe files. Multiple subsystems included, such as preprocessing, static analysis,
dynamic analysis, and counterfeit software detection.",
                "name": "Alibaba"
            },
            "metadata": {
                "malware_family": "Backdoor:Win32/ChChes.5a1edf5c",
                "scanner": {}
            },
            "bid": "1000000000000000000",
            "verdict": true,
            "mask": true,
            "author": "0x10A9eE8552f2c6b2787B240CeBeFc4A4BcB96f27",
            "author_name": "Alibaba"
        }
    ],
    "id": "19861351221101223",
    "result": null,
    "created": "2021-02-23T16:17:35.100939",
    "failed": false,
    "size": 430304,
    "last_scanned": "2021-02-23T16:17:35.100939",
    "extended_type": "PE32 executable (GUI) Intel 80386, for MS Windows",
    "votes": [],
    "community": "rho",
    "mimetype": "application/x-dosexec",
    "md5": "db212129be94fe77362751c557d0e893",
    "filename": "fadf362a52dcf884f0d41ce3df9eaa9bb30227afda50c0e0657c096baff501f0",
    "metadata": [
        {
            "tool_metadata": {
                "dropped": [],
                "ttp": [],
                "detections": "ChChes",
                "extracted_c2_ips": [
                    "kawasaki.unhamj.com"
                ],
                "signatures": [
                    {
                        "families": [],
                        "confidence": 100,
                        "severity": 1,
                        "weight": 1,
                        "description": "SetUnhandledExceptionFilter detected (possible anti-debug)",
                        "name": "antidebug_setunhandledexceptionfilter",
```

```
            "alert": false
        },
        {
            "families": [],
            "confidence": 100,
            "severity": 1,
            "weight": 1,
            "description": "Behavioural detection: Executable code extraction - unpacking",
            "name": "Unpacker",
            "alert": false
        },
        {
            "families": [],
            "confidence": 100,
            "severity": 1,
            "weight": 0,
            "description": "Attempts to connect to a dead IP:Port (1 unique times)",
            "name": "dead_connect",
            "alert": false
        },
        {
            "families": [],
            "confidence": 30,
            "severity": 1,
            "weight": 1,
            "description": "Communicates with IPs located across a large number of unique countries",
            "name": "network_country_distribution",
            "alert": false
        },
        {
            "families": [],
            "confidence": 100,
            "severity": 1,
            "weight": 1,
            "description": "Yara rule detections observed from a process memory dump/dropped files/CAPE",
            "name": "procmem_yara",
            "alert": false
        },
        {
            "families": [],
            "confidence": 50,
            "severity": 2,
            "weight": 1,
            "description": "Creates RWX memory",
            "name": "injection_rwx",
            "alert": false
        },
        {
            "families": [],
            "confidence": 100,
            "severity": 2,
            "weight": 1,
            "description": "Mimics the system's user agent string for its own requests",
            "name": "mimics_agent",
            "alert": false
        },
        {
            "families": [],
            "confidence": 100,
            "severity": 2,
            "weight": 1,
```

```
            "description": "Performs HTTP requests potentially not found in PCAP.",
            "name": "http_request",
            "alert": false
        },
        {
            "families": [],
            "confidence": 100,
            "severity": 2,
            "weight": 1,
            "description": "CAPE extracted potentially suspicious content",
            "name": "cape_extracted_content",
            "alert": false
        },
        {
            "families": [],
            "confidence": 30,
            "severity": 2,
            "weight": 1,
            "description": "Multiple direct IP connections",
            "name": "network_multiple_direct_ip_connections",
            "alert": false
        },
        {
            "families": [],
            "confidence": 100,
            "severity": 3,
            "weight": 1,
            "description": "CAPE detected the ChChes malware family",
            "name": "cape_detected_threat",
            "alert": false
        }
    ],
    "network": {
        "udp": [
            {
                "offset": 5033699,
                "sport": 137,
                "dport": 137,
                "src": "192.168.144.131",
                "time": -21.314763069152832,
                "dst": "192.168.144.255"
            },
            {
                "offset": 5035168,
                "sport": 49781,
                "dport": 53,
                "src": "192.168.144.131",
                "time": -23.094773054122925,
                "dst": "193.138.218.74"
            },
            {
                "offset": 5036096,
                "sport": 49981,
                "dport": 53,
                "src": "192.168.144.131",
                "time": -23.33778691291809,
                "dst": "193.138.218.74"
            },
            {
                "offset": 5036467,
                "sport": 50116,
```

```
        "dport": 53,
        "src": "192.168.144.131",
        "time": -24.01390790939331,
        "dst": "193.138.218.74"
    },
    {
        "offset": 5037047,
        "sport": 53203,
        "dport": 53,
        "src": "192.168.144.131",
        "time": -24.971735954284668,
        "dst": "193.138.218.74"
    },
    {
        "offset": 5037584,
        "sport": 53891,
        "dport": 53,
        "src": "192.168.144.131",
        "time": -8.775880098342896,
        "dst": "193.138.218.74"
    },
    {
        "offset": 5038155,
        "sport": 54855,
        "dport": 53,
        "src": "192.168.144.131",
        "time": 7.031538963317871,
        "dst": "193.138.218.74"
    },
    {
        "offset": 5038692,
        "sport": 54893,
        "dport": 53,
        "src": "192.168.144.131",
        "time": 2.5382208824157715,
        "dst": "193.138.218.74"
    },
    {
        "offset": 5039041,
        "sport": 55335,
        "dport": 53,
        "src": "192.168.144.131",
        "time": 33.19151592254639,
        "dst": "193.138.218.74"
    },
    {
        "offset": 5039379,
        "sport": 55665,
        "dport": 53,
        "src": "192.168.144.131",
        "time": 26.147763967514038,
        "dst": "193.138.218.74"
    },
    {
        "offset": 5040371,
        "sport": 56063,
        "dport": 53,
        "src": "192.168.144.131",
        "time": 5.498383045196533,
        "dst": "193.138.218.74"
    },
```

```
            {
                "offset": 5040908,
                "sport": 56147,
                "dport": 53,
                "src": "192.168.144.131",
                "time": -1.5909569263458252,
                "dst": "193.138.218.74"
            },
            {
                "offset": 5041500,
                "sport": 57499,
                "dport": 53,
                "src": "192.168.144.131",
                "time": -22.53717803955078,
                "dst": "193.138.218.74"
            },
            {
                "offset": 5042120,
                "sport": 58354,
                "dport": 53,
                "src": "192.168.144.131",
                "time": -2.2449920177459717,
                "dst": "193.138.218.74"
            },
            {
                "offset": 5042458,
                "sport": 61701,
                "dport": 53,
                "src": "192.168.144.131",
                "time": 23.250617027282715,
                "dst": "193.138.218.74"
            },
            {
                "offset": 5043043,
                "sport": 61748,
                "dport": 53,
                "src": "192.168.144.131",
                "time": 30.856555938720703,
                "dst": "193.138.218.74"
            },
            {
                "offset": 5043432,
                "sport": 63905,
                "dport": 53,
                "src": "192.168.144.131",
                "time": 6.423388957977295,
                "dst": "193.138.218.74"
            },
            {
                "offset": 5043914,
                "sport": 64655,
                "dport": 53,
                "src": "192.168.144.131",
                "time": 36.79194688796997,
                "dst": "193.138.218.74"
            }
        ],
        "tcp": [
            {
                "offset": 24,
                "sport": 60176,
```

```
            "dport": 80,
            "src": "192.168.144.131",
            "time": 0,
            "dst": "153.248.125.4"
        },
        {
            "offset": 784,
            "sport": 60190,
            "dport": 80,
            "src": "192.168.144.131",
            "time": 22.581259965896606,
            "dst": "153.248.125.4"
        },
        {
            "offset": 1544,
            "sport": 60203,
            "dport": 80,
            "src": "192.168.144.131",
            "time": 48.86009192466736,
            "dst": "153.248.125.4"
        },
        {
            "offset": 2304,
            "sport": 60204,
            "dport": 80,
            "src": "192.168.144.131",
            "time": 80.23402905464172,
            "dst": "153.248.125.4"
        },
        {
            "offset": 3064,
            "sport": 60205,
            "dport": 80,
            "src": "192.168.144.131",
            "time": 96.18023490905762,
            "dst": "153.248.125.4"
        },
        {
            "offset": 3824,
            "sport": 60179,
            "dport": 443,
            "src": "192.168.144.131",
            "time": 6.530672073364258,
            "dst": "191.232.139.2"
        },
        {
            "offset": 7423,
            "sport": 60193,
            "dport": 443,
            "src": "192.168.144.131",
            "time": 27.41287589073181,
            "dst": "191.232.139.2"
        },
        {
            "offset": 2090534,
            "sport": 60201,
            "dport": 443,
            "src": "192.168.144.131",
            "time": 42.54734396934509,
            "dst": "191.232.139.2"
        },
```

```
{
    "offset": 5044494,
    "sport": 60160,
    "dport": 443,
    "src": "192.168.144.131",
    "time": -23.10044503211975,
    "dst": "20.54.110.119"
},
{
    "offset": 5060861,
    "sport": 60171,
    "dport": 443,
    "src": "192.168.144.131",
    "time": -19.384203910827637,
    "dst": "20.54.110.119"
},
{
    "offset": 5074577,
    "sport": 49336,
    "dport": 80,
    "src": "192.168.144.131",
    "time": -11.905674934387207,
    "dst": "205.185.216.10"
},
{
    "offset": 5075557,
    "sport": 49353,
    "dport": 80,
    "src": "192.168.144.131",
    "time": -11.905407905578613,
    "dst": "205.185.216.10"
},
{
    "offset": 5076537,
    "sport": 49363,
    "dport": 80,
    "src": "192.168.144.131",
    "time": -11.90530800819397,
    "dst": "205.185.216.10"
},
{
    "offset": 5077517,
    "sport": 49373,
    "dport": 80,
    "src": "192.168.144.131",
    "time": 35.993048906326294,
    "dst": "205.185.216.10"
},
{
    "offset": 5078497,
    "sport": 49993,
    "dport": 80,
    "src": "192.168.144.131",
    "time": 35.99315404891968,
    "dst": "205.185.216.10"
},
{
    "offset": 5079477,
    "sport": 50013,
    "dport": 80,
    "src": "192.168.144.131",
```

```
        "time": -25.046306133270264,
        "dst": "205.185.216.10"
    },
    {
        "offset": 5181840,
        "sport": 50002,
        "dport": 80,
        "src": "192.168.144.131",
        "time": -25.04945397377014,
        "dst": "205.185.216.42"
    },
    {
        "offset": 5188209,
        "sport": 49376,
        "dport": 443,
        "src": "192.168.144.131",
        "time": 79.64388608932495,
        "dst": "35.186.224.25"
    },
    {
        "offset": 5236768,
        "sport": 60163,
        "dport": 443,
        "src": "192.168.144.131",
        "time": -22.436357021331787,
        "dst": "40.126.31.7"
    },
    {
        "offset": 5807864,
        "sport": 60158,
        "dport": 443,
        "src": "192.168.144.131",
        "time": -23.2328679561615,
        "dst": "40.127.240.158"
    },
    {
        "offset": 5825282,
        "sport": 60162,
        "dport": 443,
        "src": "192.168.144.131",
        "time": -22.88087010383606,
        "dst": "40.127.240.158"
    },
    {
        "offset": 5837771,
        "sport": 60183,
        "dport": 443,
        "src": "192.168.144.131",
        "time": 13.149832010269165,
        "dst": "40.127.240.158"
    },
    {
        "offset": 5853280,
        "sport": 60185,
        "dport": 443,
        "src": "192.168.144.131",
        "time": 20.091070890426636,
        "dst": "40.127.240.158"
    },
    {
        "offset": 5865848,
```

```
        "sport": 60187,
        "dport": 443,
        "src": "192.168.144.131",
        "time": 21.165966987609863,
        "dst": "40.127.240.158"
    },
    {
        "offset": 5887450,
        "sport": 60189,
        "dport": 443,
        "src": "192.168.144.131",
        "time": 22.355721950531006,
        "dst": "40.127.240.158"
    },
    {
        "offset": 5901567,
        "sport": 49345,
        "dport": 443,
        "src": "192.168.144.131",
        "time": -21.881307125091553,
        "dst": "40.67.254.36"
    },
    {
        "offset": 5903646,
        "sport": 54245,
        "dport": 443,
        "src": "192.168.144.131",
        "time": 33.19041609764099,
        "dst": "40.67.254.36"
    },
    {
        "offset": 5919221,
        "sport": 60194,
        "dport": 443,
        "src": "192.168.144.131",
        "time": 28.79618000984192,
        "dst": "51.11.168.232"
    },
    {
        "offset": 5932191,
        "sport": 60197,
        "dport": 443,
        "src": "192.168.144.131",
        "time": 36.1934609413147,
        "dst": "51.11.168.232"
    },
    {
        "offset": 5945992,
        "sport": 60202,
        "dport": 443,
        "src": "192.168.144.131",
        "time": 43.02833008766174,
        "dst": "51.11.168.232"
    },
    {
        "offset": 6313404,
        "sport": 60155,
        "dport": 443,
        "src": "192.168.144.131",
        "time": -24.837090969085693,
        "dst": "52.242.101.226"
```

```
    },
    {
        "offset": 6323890,
        "sport": 60168,
        "dport": 443,
        "src": "192.168.144.131",
        "time": -20.30522394180298,
        "dst": "52.242.101.226"
    },
    {
        "offset": 6367103,
        "sport": 60178,
        "dport": 443,
        "src": "192.168.144.131",
        "time": 5.602633953094482,
        "dst": "52.242.101.226"
    },
    {
        "offset": 6377158,
        "sport": 60181,
        "dport": 443,
        "src": "192.168.144.131",
        "time": 7.959491014480591,
        "dst": "52.242.101.226"
    },
    {
        "offset": 6382314,
        "sport": 60150,
        "dport": 80,
        "src": "192.168.144.131",
        "time": -25.03634810447693,
        "dst": "67.26.109.254"
    },
    {
        "offset": 6382804,
        "sport": 60152,
        "dport": 80,
        "src": "192.168.144.131",
        "time": -25.03581690788269,
        "dst": "67.27.153.254"
    },
    {
        "offset": 6383294,
        "sport": 65172,
        "dport": 80,
        "src": "192.168.144.131",
        "time": -25.0423800945282,
        "dst": "67.27.153.254"
    },
    {
        "offset": 6383784,
        "sport": 65170,
        "dport": 80,
        "src": "192.168.144.131",
        "time": -25.04357600212097,
        "dst": "8.247.205.126"
    },
    {
        "offset": 6384274,
        "sport": 60151,
        "dport": 80,
```

```
        "src": "192.168.144.131",
        "time": -25.036755084991455,
        "dst": "8.247.206.126"
    },
    {
        "offset": 6384764,
        "sport": 65171,
        "dport": 80,
        "src": "192.168.144.131",
        "time": -25.042897939682007,
        "dst": "8.247.206.126"
    },
    {
        "offset": 6385254,
        "sport": 60149,
        "dport": 80,
        "src": "192.168.144.131",
        "time": -25.037235021591187,
        "dst": "8.248.5.254"
    },
    {
        "offset": 6385744,
        "sport": 65173,
        "dport": 80,
        "src": "192.168.144.131",
        "time": -25.041805028915405,
        "dst": "8.248.5.254"
    },
    {
        "offset": 6386234,
        "sport": 49330,
        "dport": 443,
        "src": "192.168.144.131",
        "time": -11.905869960784912,
        "dst": "88.221.170.156"
    },
    {
        "offset": 6386724,
        "sport": 49377,
        "dport": 443,
        "src": "192.168.144.131",
        "time": 35.99293494224548,
        "dst": "88.221.170.156"
    },
    {
        "offset": 6387214,
        "sport": 49331,
        "dport": 443,
        "src": "192.168.144.131",
        "time": -11.90766191482544,
        "dst": "88.221.170.212"
    },
    {
        "offset": 6387704,
        "sport": 49333,
        "dport": 443,
        "src": "192.168.144.131",
        "time": -11.906913042068481,
        "dst": "88.221.170.212"
    },
    {
```

```
        "offset": 6388194,
        "sport": 49346,
        "dport": 443,
        "src": "192.168.144.131",
        "time": -11.906773090362549,
        "dst": "88.221.170.212"
    },
    {
        "offset": 6388684,
        "sport": 49352,
        "dport": 443,
        "src": "192.168.144.131",
        "time": -11.906322956085205,
        "dst": "88.221.170.212"
    },
    {
        "offset": 6389174,
        "sport": 49357,
        "dport": 443,
        "src": "192.168.144.131",
        "time": -11.906147003173828,
        "dst": "88.221.170.212"
    },
    {
        "offset": 6389664,
        "sport": 49359,
        "dport": 443,
        "src": "192.168.144.131",
        "time": -11.90605902671814,
        "dst": "88.221.170.212"
    },
    {
        "offset": 6390154,
        "sport": 49364,
        "dport": 443,
        "src": "192.168.144.131",
        "time": -11.906007051467896,
        "dst": "88.221.170.212"
    },
    {
        "offset": 6390644,
        "sport": 49372,
        "dport": 443,
        "src": "192.168.144.131",
        "time": 35.99201703071594,
        "dst": "88.221.170.212"
    },
    {
        "offset": 6391134,
        "sport": 49378,
        "dport": 443,
        "src": "192.168.144.131",
        "time": 35.99233293533325,
        "dst": "88.221.170.212"
    },
    {
        "offset": 6391624,
        "sport": 49992,
        "dport": 443,
        "src": "192.168.144.131",
        "time": 35.99257493019104,
```

```
            "dst": "88.221.170.212"
        },
        {
            "offset": 6392114,
            "sport": 50007,
            "dport": 443,
            "src": "192.168.144.131",
            "time": 35.99274802207947,
            "dst": "88.221.170.212"
        },
        {
            "offset": 6463066,
            "sport": 60157,
            "dport": 80,
            "src": "192.168.144.131",
            "time": -23.541767120361328,
            "dst": "89.249.74.41"
        },
        {
            "offset": 6470794,
            "sport": 60199,
            "dport": 80,
            "src": "192.168.144.131",
            "time": 38.21606993675232,
            "dst": "89.249.74.48"
        },
        {
            "offset": 6536039,
            "sport": 60164,
            "dport": 80,
            "src": "192.168.144.131",
            "time": -22.166570901870728,
            "dst": "93.184.220.29"
        },
        {
            "offset": 6539109,
            "sport": 54573,
            "dport": 80,
            "src": "192.168.144.131",
            "time": -24.519613027572632,
            "dst": "93.184.221.240"
        },
        {
            "offset": 6539179,
            "sport": 54574,
            "dport": 80,
            "src": "192.168.144.131",
            "time": -24.003917932510376,
            "dst": "93.184.221.240"
        },
        {
            "offset": 6539389,
            "sport": 80,
            "dport": 60209,
            "src": "89.249.74.41",
            "time": 21.33832597732544,
            "dst": "192.168.144.131"
        }
    ],
    "http": [],
    "sorted_pcap_sha256": "29f67e250d881239bcc169ddb7c4628b06ca30aeab84568edf24b12d1f75a0db",
```

```
"dns": [
    {
        "type": "A",
        "request": "kawasaki.unhamj.com",
        "answers": [
            {
                "data": "a.sinkhole.yourtrap.com",
                "type": "CNAME"
            },
            {
                "data": "sinkhole.dynu.net",
                "type": "CNAME"
            },
            {
                "data": "153.248.125.4",
                "type": "A"
            }
        ]
    }
],
"pcap_sha256": "1377ce7b432b69f9f5a458cea49b7224dcf62da79111d5eff6e74eb138a02f7c",
"hosts": [
    {
        "hostname": "",
        "inaddrarpa": "",
        "ip": "93.184.221.240",
        "country_name": "United Kingdom"
    },
    {
        "hostname": "",
        "inaddrarpa": "",
        "ip": "93.184.220.29",
        "country_name": "United Kingdom"
    },
    {
        "hostname": "",
        "inaddrarpa": "",
        "ip": "88.221.170.212",
        "country_name": "Europe"
    },
    {
        "hostname": "",
        "inaddrarpa": "",
        "ip": "88.221.170.156",
        "country_name": "Europe"
    },
    {
        "hostname": "",
        "inaddrarpa": "",
        "ip": "8.248.5.254",
        "country_name": "United States"
    },
    {
        "hostname": "",
        "inaddrarpa": "",
        "ip": "8.247.206.126",
        "country_name": "United States"
    },
    {
        "hostname": "",
        "inaddrarpa": "",
```

```
            "ip": "8.247.205.126",
            "country_name": "United States"
        },
        {
            "hostname": "",
            "inaddrarpa": "",
            "ip": "67.27.153.254",
            "country_name": "United States"
        },
        {
            "hostname": "",
            "inaddrarpa": "",
            "ip": "67.26.109.254",
            "country_name": "United States"
        },
        {
            "hostname": "",
            "inaddrarpa": "",
            "ip": "40.67.254.36",
            "country_name": "Ireland"
        },
        {
            "hostname": "",
            "inaddrarpa": "",
            "ip": "35.186.224.25",
            "country_name": "United States"
        },
        {
            "hostname": "",
            "inaddrarpa": "",
            "ip": "20.54.110.119",
            "country_name": "United States"
        },
        {
            "hostname": "",
            "inaddrarpa": "",
            "ip": "193.138.218.74",
            "country_name": "Sweden"
        },
        {
            "hostname": "",
            "inaddrarpa": "",
            "ip": "191.232.139.2",
            "country_name": "Ireland"
        },
        {
            "hostname": "kawasaki.unhamj.com",
            "inaddrarpa": "",
            "ip": "153.248.125.4",
            "country_name": "Japan"
        }
    ],
    "icmp": [
        {
            "src": "192.168.144.131",
            "data": "",
            "dst": "193.138.218.74",
            "type": 3
        },
        {
            "src": "192.168.144.131",
```

```
            "data": "",
            "dst": "193.138.218.74",
            "type": 3
        }
    ],
    "ja3": [
        {
            "desc": "unknown",
            "sport": 60179,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "191.232.139.2"
        },
        {
            "desc": "unknown",
            "sport": 60193,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "191.232.139.2"
        },
        {
            "desc": "unknown",
            "sport": 60201,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "191.232.139.2"
        },
        {
            "desc": "unknown",
            "sport": 60160,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "20.54.110.119"
        },
        {
            "desc": "unknown",
            "sport": 60171,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "20.54.110.119"
        },
        {
            "desc": "unknown",
            "sport": 60175,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "40.126.31.5"
        },
        {
            "desc": "unknown",
            "sport": 60163,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "40.126.31.7"
```

```
    },
    {
        "desc": "unknown",
        "sport": 60169,
        "dport": 443,
        "src": "192.168.144.131",
        "ja3": "28a2c9bd18a11de089ef85a160da29e4",
        "dst": "40.126.31.7"
    },
    {
        "desc": "unknown",
        "sport": 60158,
        "dport": 443,
        "src": "192.168.144.131",
        "ja3": "28a2c9bd18a11de089ef85a160da29e4",
        "dst": "40.127.240.158"
    },
    {
        "desc": "unknown",
        "sport": 60159,
        "dport": 443,
        "src": "192.168.144.131",
        "ja3": "28a2c9bd18a11de089ef85a160da29e4",
        "dst": "40.127.240.158"
    },
    {
        "desc": "unknown",
        "sport": 60162,
        "dport": 443,
        "src": "192.168.144.131",
        "ja3": "28a2c9bd18a11de089ef85a160da29e4",
        "dst": "40.127.240.158"
    },
    {
        "desc": "unknown",
        "sport": 60182,
        "dport": 443,
        "src": "192.168.144.131",
        "ja3": "28a2c9bd18a11de089ef85a160da29e4",
        "dst": "40.127.240.158"
    },
    {
        "desc": "unknown",
        "sport": 60183,
        "dport": 443,
        "src": "192.168.144.131",
        "ja3": "28a2c9bd18a11de089ef85a160da29e4",
        "dst": "40.127.240.158"
    },
    {
        "desc": "unknown",
        "sport": 60184,
        "dport": 443,
        "src": "192.168.144.131",
        "ja3": "28a2c9bd18a11de089ef85a160da29e4",
        "dst": "40.127.240.158"
    },
    {
        "desc": "unknown",
        "sport": 60185,
        "dport": 443,
```

```
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "40.127.240.158"
        },
        {
            "desc": "unknown",
            "sport": 60186,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "40.127.240.158"
        },
        {
            "desc": "unknown",
            "sport": 60187,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "40.127.240.158"
        },
        {
            "desc": "unknown",
            "sport": 60188,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "40.127.240.158"
        },
        {
            "desc": "unknown",
            "sport": 60189,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "40.127.240.158"
        },
        {
            "desc": "unknown",
            "sport": 60177,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "3b5074b1b5d032e5620f69f9f700ff0e",
            "dst": "40.67.251.132"
        },
        {
            "desc": "unknown",
            "sport": 60191,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "51.11.168.232"
        },
        {
            "desc": "unknown",
            "sport": 60194,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "51.11.168.232"
        },
        {
```

```
            "desc": "unknown",
            "sport": 60196,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "51.11.168.232"
        },
        {
            "desc": "unknown",
            "sport": 60197,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "51.11.168.232"
        },
        {
            "desc": "unknown",
            "sport": 60200,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "51.11.168.232"
        },
        {
            "desc": "unknown",
            "sport": 60202,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "51.11.168.232"
        },
        {
            "desc": "unknown",
            "sport": 60192,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "52.142.21.137"
        },
        {
            "desc": "unknown",
            "sport": 60155,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "52.242.101.226"
        },
        {
            "desc": "unknown",
            "sport": 60167,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
            "dst": "52.242.101.226"
        },
        {
            "desc": "unknown",
            "sport": 60168,
            "dport": 443,
            "src": "192.168.144.131",
            "ja3": "28a2c9bd18a11de089ef85a160da29e4",
```

```
                        "dst": "52.242.101.226"
                    },
                    {
                        "desc": "unknown",
                        "sport": 60172,
                        "dport": 443,
                        "src": "192.168.144.131",
                        "ja3": "28a2c9bd18a11de089ef85a160da29e4",
                        "dst": "52.242.101.226"
                    },
                    {
                        "desc": "unknown",
                        "sport": 60178,
                        "dport": 443,
                        "src": "192.168.144.131",
                        "ja3": "28a2c9bd18a11de089ef85a160da29e4",
                        "dst": "52.242.101.226"
                    },
                    {
                        "desc": "unknown",
                        "sport": 60180,
                        "dport": 443,
                        "src": "192.168.144.131",
                        "ja3": "28a2c9bd18a11de089ef85a160da29e4",
                        "dst": "52.242.101.226"
                    },
                    {
                        "desc": "unknown",
                        "sport": 60181,
                        "dport": 443,
                        "src": "192.168.144.131",
                        "ja3": "28a2c9bd18a11de089ef85a160da29e4",
                        "dst": "52.242.101.226"
                    }
                ],
                "domains": [
                    {
                        "ip": "153.248.125.4",
                        "domain": "kawasaki.unhamj.com"
                    }
                ],
                "smtp": [],
                "irc": []
            },
            "extracted_c2_ip_port": [
                "kawasaki.unhamj.com"
            ],
            "cape_filter": [
                {
                    "sha512":
"e40c33ca4140db7cd9a783a303f79f5ba73fdad1cf2fdfef0b4fb0645df7f76d43a775d147cdf40ef53f4f767c31dbd0a5d589c2e918e1ebc7c9
f8b12e6a541e",
                    "size": 61236,
                    "sha1": "3e556d29ff1a61b3dd32d78cd1c986243db84f05",
                    "sha256": "ee04fb9e8f24d7fe05a239d107ef830730ce3d87185b1807dd73ec7694c4abea",
                    "path": "/opt/CAPEv2/storage/analyses/15/CAPE/
ee04fb9e8f24d7fe05a239d107ef830730ce3d87185b1807dd73ec7694c4abea",
                    "process_name": "file.exe",
                    "cape_type_code": 9,
                    "type": "DOS executable (COM)",
                    "module_path": "C:\\Users\\shelly\\AppData\\Local\\Temp\\file.exe",
```

```
                        "pid": 4348,
                        "cape_type": "ChChes Payload",
                        "crc32": "718899D1",
                        "ssdeep": "1536:OmSTkiVmSH3BqDmsOHX0ywwFR22oSpKHLkeYf:iggm8Rqalky9DKRHLW",
                        "guest_paths": "9;?C:\\Users\\shelly\\AppData\\Local\\Temp\\file.exe;?C:\\Users\\shelly\
\AppData\\Local\\Temp\\file.exe;?0x006E0000;?",
                        "virtual_address": "0x006E0000",
                        "name": "ee04fb9e8f24d7fe05a239d107ef830730ce3d87185b1807dd73ec7694c4abea",
                        "process_path": "C:\\Users\\shelly\\AppData\\Local\\Temp\\file.exe",
                        "md5": "57b0ff04d256a8edb2de0ca64c5bbfc3"
                    }
                ],
                "cape_config": [
                    {
                        "address": [
                            "kawasaki.unhamj.com"
                        ],
                        "detections": "ChChes",
                        "urlpath": [
                            "/%r.htm"
                        ],
                        "c2_address": [
                            "kawasaki.unhamj.com"
                        ],
                        "url": [
                            "http://kawasaki.unhamj.com/%r.htm"
                        ],
                        "c2_url": [
                            "http://kawasaki.unhamj.com/%r.htm"
                        ]
                    }
                ],
                "signature_names": [
                    "antidebug_setunhandledexceptionfilter",
                    "Unpacker",
                    "dead_connect",
                    "network_country_distribution",
                    "procmem_yara",
                    "injection_rwx",
                    "mimics_agent",
                    "http_request",
                    "cape_extracted_content",
                    "network_multiple_direct_ip_connections",
                    "cape_detected_threat"
                ]
            },
            "updated": "2021-02-23T19:51:42.606126",
            "tool": "cape_sandbox_v2",
            "created": "2021-02-23T19:51:42.606126"
        },
        {
            "tool_metadata": {
                "has_export_table": false,
                "force_integrity": false,
                "high_entropy_aslr": false,
                "terminal_server_aware": true,
                "is_driver": false,
                "signed": true,
                "warnings": [],
                "certificate": [
                    {
```

```
            "public": {
                "algorithm": "rsa",
                "sha256": "708f94656ead77166be933385b37b7d58f7f10b28c126c64a7861bc66bb667c4",
                "sha1": "7fd365a7c2ddecbbf03009f34339fa02af333133",
                "bit_size": 2048
            },
            "sha1": "453ab3276f4c16717c64d2d90c054ce288770351",
            "sha256": "893780c6d4c09c6d5523d1d5ffae0cc63ce1329050bf5d1bb69e3758b1499897",
            "signature_algo": "rsassa_pkcs1v15",
            "not_valid_before": "2006-11-08T00:00:00+00:00",
            "not_valid_after": "2021-11-07T23:59:59+00:00",
            "serial_number": "359370927573585894971116214966566641 84",
            "subject": {
                "organization": "VeriSign, Inc.",
                "country": "US",
                "common_name": "VeriSign Class 3 Public Primary Certification Authority - G5"
            },
            "is_ca": true,
            "hash_algo": "sha1"
        },
        {
            "public": {
                "algorithm": "rsa",
                "sha256": "c5b404fa65e10e3358c077dfee4e5db38d7416b27a6ab1720cb342dc65056ad3",
                "sha1": "4046d6e5d3c83a0f8de968c0599a7a4068402c56",
                "bit_size": 2048
            },
            "sha1": "b366dbe8b3e81915ca5c5170c65dcad8348b11f0",
            "sha256": "840b05526d4754ddb1f9f785aff4353165433f1b349248861dc2c082fb95faf1",
            "signature_algo": "rsassa_pkcs1v15",
            "not_valid_before": "2011-08-05T00:00:00+00:00",
            "not_valid_after": "2012-08-04T23:59:59+00:00",
            "serial_number": "85054602239157067351845372565600594873",
            "subject": {
                "organization": "HT Srl",
                "locality": "Milan",
                "country": "IT",
                "common_name": "HT Srl",
                "state_province": "Italy"
            },
            "is_ca": false,
            "hash_algo": "sha1"
        },
        {
            "public": {
                "algorithm": "rsa",
                "sha256": "4b741c5eacc3b518b0e6ef1ab3ae210e1bf7c82e803cd691216f90b0c7461d3a",
                "sha1": "cf99a9ea7b26f44bc98e8fd7f00526efe3d2a79d",
                "bit_size": 2048
            },
            "sha1": "495847a93187cfb8c71f840cb7b41497ad95c64f",
            "sha256": "0cfc19db681b014bfe3f23cb3a78b67208b4e3d8d7b6a7b1807f7cd6ecb2a54e",
            "signature_algo": "rsassa_pkcs1v15",
            "not_valid_before": "2010-02-08T00:00:00+00:00",
            "not_valid_after": "2020-02-07T23:59:59+00:00",
            "serial_number": "1090013538065060687451449014490451936 71",
            "subject": {
                "organization": "VeriSign, Inc.",
                "country": "US",
                "common_name": "VeriSign Class 3 Code Signing 2010 CA"
            },
```

```
            "is_ca": true,
            "hash_algo": "sha1"
        }
    ],
    "exports": [],
    "is_dll": false,
    "force_no_isolation": false,
    "verify_checksum": true,
    "pdb_guids": [
        "{ebfe4de5-da9a-a04d-abae5a84f2832ab4}"
    ],
    "is_valid": null,
    "is_exe": true,
    "uses_seh": true,
    "libraries": [
        "KERNEL32.dll",
        "USER32.dll",
        "ADVAPI32.dll"
    ],
    "uses_cfg": false,
    "uses_aslr": true,
    "wdm_driver": false,
    "is_probably_packed": false,
    "pdb": [
        "D:\\Projects\\ByPassAV\\Win32Project2\\Release\\Win32Project2.pdb"
    ],
    "imphash": "c4e3543b5b9bb91158628c64a57f9863",
    "compile_date": "2011-11-21 23:51:44",
    "is_suspicious": null,
    "no_bind": false,
    "imported_functions": [
        "VirtualAlloc",
        "lstrcpynA",
        "lstrcmpA",
        "SetUnhandledExceptionFilter",
        "lstrlenA",
        "WaitForSingleObject",
        "GetCurrentProcess",
        "VirtualFree",
        "SetErrorMode",
        "DecodePointer",
        "HeapReAlloc",
        "HeapSize",
        "WriteConsoleW",
        "SetFilePointerEx",
        "CreateFileW",
        "FlushFileBuffers",
        "GetStringTypeW",
        "SetStdHandle",
        "GetProcessHeap",
        "GetModuleFileNameW",
        "FreeEnvironmentStringsW",
        "UnhandledExceptionFilter",
        "TerminateProcess",
        "IsProcessorFeaturePresent",
        "IsDebuggerPresent",
        "GetStartupInfoW",
        "GetModuleHandleW",
        "QueryPerformanceCounter",
        "GetCurrentProcessId",
        "GetCurrentThreadId",
```

```
            "GetSystemTimeAsFileTime",
            "InitializeSListHead",
            "GetLastError",
            "RaiseException",
            "SetLastError",
            "RtlUnwind",
            "EnterCriticalSection",
            "LeaveCriticalSection",
            "DeleteCriticalSection",
            "InitializeCriticalSectionAndSpinCount",
            "TlsAlloc",
            "TlsGetValue",
            "TlsSetValue",
            "TlsFree",
            "FreeLibrary",
            "GetProcAddress",
            "LoadLibraryExW",
            "ExitProcess",
            "GetModuleHandleExW",
            "MultiByteToWideChar",
            "WideCharToMultiByte",
            "GetStdHandle",
            "WriteFile",
            "GetACP",
            "HeapFree",
            "HeapAlloc",
            "GetFileType",
            "LCMapStringW",
            "GetConsoleCP",
            "GetConsoleMode",
            "CloseHandle",
            "FindClose",
            "FindFirstFileExW",
            "FindNextFileW",
            "IsValidCodePage",
            "GetOEMCP",
            "GetCPInfo",
            "GetCommandLineA",
            "GetCommandLineW",
            "GetEnvironmentStringsW",
            "PostQuitMessage",
            "EndPaint",
            "BeginPaint",
            "DefWindowProcW",
            "UpdateWindow",
            "ShowWindow",
            "RegisterClassExW",
            "LoadCursorW",
            "LoadIconW",
            "DispatchMessageW",
            "TranslateMessage",
            "TranslateAcceleratorW",
            "GetMessageW",
            "LoadAcceleratorsW",
            "LoadStringW",
            "CreateWindowExW",
            "SystemFunction036"
        ],
        "app_container": false,
        "uses_dep": true,
        "has_debug_info": true,
```

```
            "has_import_table": true
        },
        "updated": "2021-02-23T16:17:35.863200",
        "tool": "pefile",
        "created": "2021-02-23T16:17:35.863200"
    },
    {
        "tool_metadata": {
            "urls": [
                "http://csc3-2010-aia.verisign.com/CSC3-2010.cer0",
                "http://crl.verisign.com/pca3.crl0",
                "https://www.verisign.com/cps0",
                "https://www.verisign.com/cps0*",
                "https://www.verisign.com/rpa",
                "1.0.0.1",
                "https://www.verisign.com/rpa0",
                "http://csc3-2010-crl.verisign.com/CSC3-2010.crl0D"
            ],
            "domains": [
                "",
                "csc3-2010-aia.verisign.com",
                "www.verisign.com",
                "csc3-2010-crl.verisign.com",
                "crl.verisign.com"
            ],
            "ipv4": [
                "1.0.0.1"
            ],
            "ipv6": [
                "::442"
            ]
        },
        "updated": "2021-02-23T16:17:35.731050",
        "tool": "strings",
        "created": "2021-02-23T16:17:35.731050"
    },
    {
        "tool_metadata": {
            "libraries": [
                "KERNEL32.dll",
                "USER32.dll",
                "ADVAPI32.dll"
            ],
            "imported_functions": [
                "VirtualAlloc",
                "lstrcpynA",
                "lstrcmpA",
                "SetUnhandledExceptionFilter",
                "lstrlenA",
                "WaitForSingleObject",
                "GetCurrentProcess",
                "VirtualFree",
                "SetErrorMode",
                "DecodePointer",
                "HeapReAlloc",
                "HeapSize",
                "WriteConsoleW",
                "SetFilePointerEx",
                "CreateFileW",
                "FlushFileBuffers",
                "GetStringTypeW",
```

```
"SetStdHandle",
"GetProcessHeap",
"GetModuleFileNameW",
"FreeEnvironmentStringsW",
"UnhandledExceptionFilter",
"TerminateProcess",
"IsProcessorFeaturePresent",
"IsDebuggerPresent",
"GetStartupInfoW",
"GetModuleHandleW",
"QueryPerformanceCounter",
"GetCurrentProcessId",
"GetCurrentThreadId",
"GetSystemTimeAsFileTime",
"InitializeSListHead",
"GetLastError",
"RaiseException",
"SetLastError",
"RtlUnwind",
"EnterCriticalSection",
"LeaveCriticalSection",
"DeleteCriticalSection",
"InitializeCriticalSectionAndSpinCount",
"TlsAlloc",
"TlsGetValue",
"TlsSetValue",
"TlsFree",
"FreeLibrary",
"GetProcAddress",
"LoadLibraryExW",
"ExitProcess",
"GetModuleHandleExW",
"MultiByteToWideChar",
"WideCharToMultiByte",
"GetStdHandle",
"WriteFile",
"GetACP",
"HeapFree",
"HeapAlloc",
"GetFileType",
"LCMapStringW",
"GetConsoleCP",
"GetConsoleMode",
"CloseHandle",
"FindClose",
"FindFirstFileExW",
"FindNextFileW",
"IsValidCodePage",
"GetOEMCP",
"GetCPInfo",
"GetCommandLineA",
"GetCommandLineW",
"GetEnvironmentStringsW",
"PostQuitMessage",
"EndPaint",
"BeginPaint",
"DefWindowProcW",
"UpdateWindow",
"ShowWindow",
"RegisterClassExW",
"LoadCursorW",
```

```
                "LoadIconW",
                "DispatchMessageW",
                "TranslateMessage",
                "TranslateAcceleratorW",
                "GetMessageW",
                "LoadAcceleratorsW",
                "LoadStringW",
                "CreateWindowExW",
                "SystemFunction036"
            ],
            "is_pie": true,
            "has_nx": true,
            "exported_functions": [],
            "entrypoint": 4204466,
            "virtual_size": 446464
        },
        "updated": "2021-02-23T16:17:35.662558",
        "tool": "lief",
        "created": "2021-02-23T16:17:35.662558"
    },
    {
        "tool_metadata": {
            "subsystemversion": 5.1,
            "imagefilecharacteristics": "Executable, 32-bit",
            "fileflags": "(none)",
            "internalname": "TODO: <Internal name>",
            "timestamp": "2011:11:21 23:51:44+00:00",
            "originalfilename": "TODO: <Original filename>",
            "fileflagsmask": "0x003f",
            "exiftoolversion": 11.16,
            "legalcopyright": "Copyright (C) 2016",
            "codesize": 68096,
            "productversion": "1.0.0.1",
            "linkerversion": 14,
            "subsystem": "Windows GUI",
            "filepermissions": "rw-r--r--",
            "objectfiletype": "Unknown",
            "filemodifydate": "2021:02:23 16:17:35+00:00",
            "sourcefile": "/tmp/tmpycqwrz7q",
            "companyname": "TODO: <Company name>",
            "mimetype": "application/octet-stream",
            "productversionnumber": "1.0.0.1",
            "machinetype": "Intel 386 or later, and compatibles",
            "filesubtype": 0,
            "petype": "PE32",
            "fileversionnumber": "1.0.0.1",
            "filename": "tmpycqwrz7q",
            "filetypeextension": "exe",
            "fileos": "Windows NT 32-bit",
            "characterset": "Unicode",
            "directory": "/tmp",
            "productname": "TODO: <Product name>",
            "fileinodechangedate": "2021:02:23 16:17:35+00:00",
            "filedescription": "TODO: <File description>",
            "languagecode": "English (U.S.)",
            "uninitializeddatasize": 0,
            "fileversion": "1.0.0.1",
            "filetype": "Win32 EXE",
            "imageversion": 0,
            "initializeddatasize": 360448,
            "entrypoint": "0x27b2",
```

```
                "filesize": "420 kB",
                "osversion": 5.1,
                "fileaccessdate": "2021:02:23 16:17:35+00:00"
            },
            "updated": "2021-02-23T16:17:35.596176",
            "tool": "exiftool",
            "created": "2021-02-23T16:17:35.596176"
        },
        {
            "tool_metadata": {
                "sha3_256": "d641402a2ddc65fab2c6c5400994b4b0cdd1a548dd6b9bca0ec24afa56f83682",
                "sha512":
"44e9a2dbd327aef0892660a527139088ac65a4863a8ea7e72ab5a5b463bd77f0b31a12453813dd2d0894249b47ab57688c84916914148dd5edd8
3dbf1d9103e2",
                "sha1": "7fe6c8191749767254513b03da03cfbf6dd6c139",
                "sha256": "fadf362a52dcf884f0d41ce3df9eaa9bb30227afda50c0e0657c096baff501f0",
                "ssdeep": "3072:MiPK+qCOhn+wJyh/
FQgnzPNY+2JdkFn4T8BQVvi0yfYn+6uRoHSXBKBlQ3JQ2Iok:9PqCkn+wJyhzPUd24T8zcn+y0BiQqok",
                "sha3_512":
"cd45f0b7a037118daa677b35102246c3ce5862c175d85a9ff8b0629a5b70bd4f9209a82e64d90ab892e7e91e881588ba92efa0fcc25d0d804a4b
995d7707c992",
                "authentihash": "c81ecdd6639199718dcc9b70195ee60b56f94f6ca97e3f463f1d1510550b6bfe",
                "tlsh": "e294b053aadc3cd7c0385770377b87d0c72eed6455a2c41ea6d022aad8bd0537a227e9",
                "md5": "db212129be94fe77362751c557d0e893"
            },
            "updated": "2021-02-23T16:17:35.496612",
            "tool": "hash",
            "created": "2021-02-23T16:17:35.496612"
        }
    ],
    "last_seen": "2021-02-23T16:17:35.100939",
    "type": "FILE",
    "first_seen": "2021-02-23T16:17:35.100939",
    "artifact_id": "19861351221101223",
    "country": "",
    "detections": {
        "malicious": 7,
        "total": 9,
        "benign": 2
    },
    "polyscore": 0.999864868853413,
    "window_closed": true,
    "upload_url": null
}
```

Parameters

ThreatQ provides the following parameters for this Action:

PARAMETER	DESCRIPTION
Default HTTP Schema (for URLs & FQDNs)	Select the default HTTP schema to apply to indicators without one. The default setting is HTTP.
Automatically Upload Related TTPs to ThreatQ	Select whether detected signatures/TTPs are automatically uploaded & related within ThreatQ. This parameter is selected by default.

ThreatQ Mapping

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.sha1	Indicator Value	SHA-1	N/A	7fe6c81917497672545 13b03da03cfbf6dd6c139	N/A
.sha256	Indicator Value	SHA-256	N/A	fadf362a52dcf884f0d41 ce3df9eaa9bb30227afda 50c0e0657c096baff501f0	N/A
.md5	Indicator Value	MD5	N/A	db212129be94fe7736275 1c557d0e893	N/A
.filename	Indicator Value	Filename	N/A	N/A	N/A
.metadata[].tool_metadata.network.domains[].ip	Indicator Value	IP Address	N/A	`153[.]248.125.4`	N/A
.metadata[].tool_metadata.network.domains[].domain	Indicator Value	FQDN	N/A	`kawasaki[.]unhamj.com`	N/A
.metadata[].tool_metadata.cape_config[].c2_url[]	Indicator Value	URL	N/A	`http://kawasaki[.]unhamj[.]com/%r.htm`	N/A
.strings.urls[]	Indicator Value	URL	N/A	N/A	N/A
.strings.domains[]	Indicator Value	FQDN	N/A	N/A	N/A
.strings.ipv4[]	Indicator Value	IP Address	N/A	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.strings.ipv6[]	Indicator Value	IPv6	N/A	N/A	N/A
.metadata[].tool_metadata.signatures[].name	Object Value	TTP	N/A	N/A	N/A
.size	Attribute	File Size	N/A	430304	N/A
.type	Attribute	Polyswarm Type	N/A	FILE	N/A
.extended_type	Attribute	Extended Type	N/A	PE32 executable (GUI) Intel 80386, for MS Windows	N/A
.community	Attribute	PolySwarm Community	N/A	rho	N/A
.mimetype	Attribute	MIME Type	N/A	application/x-dosexec	N/A
.metadata[].tool_metadata.sha512	Indicator Value	SHA-512	N/A	N/A	N/A
.metadata[].tool_metadata.malware_family	Attribute	Malware Family	N/A	N/A	N/A
.metadata[].tool_metadata.operating_system[]	Attribute	Operating System	N/A	N/A	N/A
.metadata[].tool_metadata.labels[]	Attribute	Label	N/A	N/A	N/A
.metadata[].tool_metadata.detections	Attribute	Detection	N/A	ChChes	N/A
.metadata[].polyscore	Attribute	Polyscore	N/A	0.99	N/A
.metadata[].country	Attribute	Country Code	N/A	US	N/A
.metadata[].last_scanned	Attribute	Last Scanned	N/A	N/A	Date is parsed and re-formatted
.metadata[].last_seen	Attribute	Last Seen	N/A	N/A	Date is parsed and re-formatted
.metadata[].detections.[malicious/total]	Attribute	Detection Rate	N/A	100%	N/A
.metadata[].detections.[malicious/total]	Attribute	Detections	N/A	5/10	N/A

Rescan

The Rescan action perform a Rescan for a particular hash.

```
POST https://api.polyswarm.network/v2/consumer/submission/{community}/{hash_type}/{hash_value}
```

There is no sample API response to show.

Parameters

ThreatQ provides the following parameter for this Action:

PARAMETER	DESCRIPTION
Wait for Response	Select if the operation will wait for the rescan to finish its process. This parameter is selected by default.

ThreatQ Mapping

There is no mapping for this Action

Metadata Search

Search for scans using the metadata search

```
POST https://api.polyswarm.network/v2/search/metadata/query
```

There is no sample API response to show

ThreatQ Mapping

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.artifact.sha1	Indicator Value	SHA-1	N/A	7fe6c8191749767254513b03da03cfbf6dd6c139	N/A
.artifact.sha256	Indicator Value	SHA-256	N/A	N/A	N/A
.artifact.md5	Indicator Value	MD5	N/A	N/A	N/A
.hash.sha256	Indicator Value	SHA-256	N/A	N/A	N/A
.scan.filename[]	Indicator Value	Filename	N/A	N/A	N/A
.scan.countries[]	Attribute	Country Code	N/A	US	N/A
.scan.mimetype.mime	Attribute	MIME Type	N/A	N/A	N/A
.scan.mimetype.extended	Attribute	Extended Type	N/A	N/A	N/A
.scan.first_seen	Attribute	First Seen	N/A	N/A	Converted to the TQ date format
.scan.last_seen	Attribute	Last Seen	N/A	N/A	Converted to the TQ date format
.scan.latest_scan[malicious/total]	Attribute	Detection Rate	N/A	N/A	Rate is calculated
.scan.latest_scan[malicious/total]	Attribute	Detections	N/A	N/A	Ratio is formatted
.id	Attribute	Scan Link	N/A	N/A	N/A
.strings.urls[]	Indicator Value	URL	N/A	N/A	N/A
.strings.domains[]	Indicator Value	FQDN	N/A	N/A	N/A
.strings.ipv4[]	Indicator Value	IP Address	N/A	N/A	N/A
.strings.ipv6[]	Indicator Value	IPv6 Address	N/A	N/A	N/A
.metadata.malware_family	Attribute	Malware Family	N/A	N/A	N/A

Live Hunt

The Live Hunt action start a live hunt in PolySwarm using a YARA Signature.

```
POST https://api.polyswarm.network/v2/hunt/live
```

There is no sample API response to show.

Parameters

ThreatQ provides the following parameters for this Action:

PARAMETER	DESCRIPTION
Name (Override)	Enter a rule name to override the existing name.
Is Active	Select if this rule will be set to Active. This parameter is selected by default.

ThreatQ Mapping

There is no mapping for this Action

Historical Hunt

The Historical Hunt action start a historical hunt in PolySwarm using a YARA Signature.

```
POST https://api.polyswarm.network/v2/hunt/historical
```

There is no sample API response to show.

Parameters

ThreatQ provides the following parameter for this Action:

PARAMETER	DESCRIPTION
Name (Override)	Enter a rule name to override the existing name.

ThreatQ Mapping

There is no mapping for this Action.

Add Rule

The Add Rule action creates a Ruleset to PolySwarm using YARA Signature.

```
POST https://api.polyswarm.network/v2/hunt/rule
```

There is no sample API response to show.

Parameters

ThreatQ provides the following parameters for this Action:

PARAMETER	DESCRIPTION
Name (Override)	Enter a rule name to override the existing name.
Description (Override)	Enter a description to override the existing description.

ThreatQ Mapping

There is no mapping for this Action.

Scan

The Scan action scans a file or URL using PolySwarm.

```
POST https://api.polyswarm.network/v2/consumer/submission/{community}
```

There is no sample API response to show.

Parameters

ThreatQ provides the following parameters for this Action:

PARAMETER	DESCRIPTION
Scan Config	• Select the configuration to use for the scan. Options include: ◦ Default (Default) ◦ More Time ◦ Most Time
Default HTTP Schema (for URLs & FQDNs)	• Select the default HTTP schema to apply to indicators without one. Options include: ◦ HTTP (Default) ◦ HTTPS
Wait for Response	Select if the operation will wait for the rescan to finish its process. This parameter is selected by default.

ThreatQ Mapping

There is no mapping for this Action.

Change Log

- **Version 1.0.0**
  - Initial Release