

Juniper Advanced Threat Prevention Appliance

HTTP API Guide

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA

408-745-2000

www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Juniper Advanced Threat Prevention HTTP API Guide
Copyright© 2018 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical document consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes. Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>.
- Search for known bugs: <https://prsearch.juniper.net/>.
- Find product documentation: <http://www.juniper.net/documentation/>.
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>.
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>.
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>.
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>.
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>.

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>.

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).
- For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>

Inside This Guide

- JUNIPER ATP APPLIANCE API HTTP REQUEST PROPERTIES
- API AUTHORIZATION KEY
- SEVERITY CONSTANTS
- API FUNCTIONS

add_incident_comments	get_iocs
add_license	get_ipv
add_user	get_reports*
analysis_details	get_unchecked_exposures
backup	get_users
behavior_details	get_whitelist_rules
behavior_features	get_zones*
bit9_config	history_details
blocked_ips	incident_comments
bluecoat_config	incidents*
change_password	incident_details*
collector_details	ingestion_vendor_details*
collector_performance	license_details
collectors_summary	login
delete_whitelist_rules	logout
events*	network_traffic
event_details	set_auto_mitigation_settings*
file_submit	set_whitelist_rules
get_auto_mitigation_settings*	test_configuration
get_blocked_emails_ex*	top_incidents
get_blocked_ips_ex	trace_log
get_blocked_signatures	trace_pcap
get_blocked_urls_ex	test_configuration
	update_report*
	verify

* new or recently modified APIs

The Juniper ATP Appliance supports an HTTP-based API for accessing all threat and processing data as well as device and software configuration. All functionality available from the Central Manager Web UI is also accessible via the Juniper ATP Appliance HTTP API. JSON is returned in all responses from the API, including errors.

NOTE All Juniper ATP Appliance detection engine Cores support the same API. Juniper ATP Appliance Traffic Collectors do not currently support APIs.

Juniper ATP Appliance defines “incidents” as a group of events that share the same enterprise endpoint. In other words, a Juniper ATP Appliance incident contains events that are likely part of the same attack. Currently, the grouping of events into an incident is primarily a measure of co-occurrence in time; the events occurred at or from the same endpoint within a 5-minute timespan.

In recent releases, Juniper ATP Appliance separated correlation results into incident groups and now provides an “events” API that retrieves the raw data accrued during the detection and analysis process.

Events include:

- a download
- a CnC detection via signature
- a phishing detection
- a malicious email URL or attachment
- exploits from chain heuristics
- a user upload

Juniper ATP Appliance API HTTP Request Properties

All Juniper ATP Appliance HTTP requests share the following properties:

The base URL is: <https://HOST/admin/api.php>

A function is given as an “op” query string parameter.

Function parameters are provided via form url-encoded content in a POST request.

Response data is in JSON except where noted with each JSON response always containing the “status” field, where 0 indicates success, and negative indicates failure. If the status field is negative, another field “error_msg” is set with a string describing the error.

Authentication is either via the “SESSID” or via an API key supplied in the “Authorization” HTTP header. The “SESSID” cookie is generated using the “login” request. This cookie is set with a configurable server-side timeout. API keys are generated from the Config>User configuration page in the Central Manager Web UI.

Every successful request resets the cookie timeout to zero.

Example

```
curl -k -d "user_name=admin&password=12345"  
"https://HOST/admin/api.php?op=login"
```

API Authorization Key

Generate a new API key for a specified user from the Juniper ATP Appliance Central Manager Web UI to provide authorized programmatic access to the Juniper ATP Appliance REST API. Supply the Authorization Key each time an API request is made via the HTTP “Authorization” header or via the query string parameter “api_key”; this action removes the requirement for API session logins.

Generate an API key as follows:

1. At the Juniper ATP Appliance Central Manager Web UI Config> System Profiles> Users page.
2. Click on an existing user account to open the Update User window.
3. Check the “Generate New API Key” option, then click the Update User button. Open that user update window one more time to view and copy the new API Key.

As part of each API call, enter the key as shown below:

Example

```
curl -k -H "Authorization: bbc940ccdc795813d1c2d21c60d51a4b"  
"https://HOST/admin/api.php?op=country_counts"
```

Optional Query String Parameters

Init:

Any request may add a value “init” to the query string. If the value is non-zero the response will also contain initialization data including a “constant_map” which provides values for symbolic constants used by the other requests. For example, the error status values are defined in this map (see [Error Status Values](#)).

noop:

This value prevents the cookie’s server-side session timeout from resetting.

error status values:

Descriptions of API error values are delineated as follows:

Table 3-1 API error values

Error Codes	Description
-1	Invalid or missing parameter.
-2	Internal error
-3	Duplicate configuration already exists
-4	No results available.
-5	Database error
-6	The current user does not have permissions to access this API
-7	Results are not yet available
-8	Session timeout
-11	User not logged in
-12	Service not available
-13	Invalid CSRF token
-14	Invalid input

NOTE Each API call also returns an error string containing a detailed text description of the error; each API will define the meaning of each error case.

Severity Constants

In recent releases, a new severity and risk indicator range was employed such that severity is now defined as a value (including decimals) between 0 and 1. The previous range was a positive integer value between 1-4.

The new severity range mapping is as follows:

- Previous alert severity 1 (high) now maps to [0.75, 1.0]
- Previous alert severity 2 (medium) maps to [0.5, 0.75]
- Previous alert severity 3 (low) maps to [0, 0.5]

In the “incident” and “event” search queries the results will have a severity/risk greater than or equal to the minimum severity/risk value, and strictly less than the severity/risk value, except when the minimum severity/risk value is 0 or the maximum severity risk value is 1, in which case the results will have severity/risk greater than 0 and less than or equal to 1.

For example, to return all non-benign incidents or events, set the minimum risk/severity value to 0 and the maximum value to 1.

As a special case, to search for all clean/benign events, specify a minimum severity of 0 and maximum severity of 0.

NOTE For a report of all mitigation devices, use the API `get_reports`. To test connectivity to mitigation devices, use the API `test_configuration`.

API Functions

The available APIs for the current Juniper ATP Appliance release are provided in the following sections. This list of APIs is updated as new features are developed.

[add_incident_comments on page 5](#)

[add_license on page 6](#)

[add_user on page 6](#)

[analysis_details on page 7](#)

[backup on page 10](#)

[behavior_details on page 10](#)

[behavior_features on page 56](#)

[bit9_config on page 58](#)

[blocked_ips on page 59](#)

[bluecoat_config on page 60](#)

[change_password on page 61](#)

[collector_details on page 62](#)

[collector_performance on page 63](#)

[collectors_summary on page 65](#)

[delete_whitelist_rules on page 67](#)

[events on page 68](#)

[event_details on page 73](#)

[file_submit on page 81](#)

[get_auto_mitigation_settings on page 86](#)

[get_blocked_emails_ex on page 86](#)

[get_blocked_ips_ex on page 87](#)

[get_blocked_signatures on page 88](#)

[get_blocked_urls_ex on page 89](#)

[get_iocs on page 91](#)

[get_ivp on page 118](#)

[get_reports on page 118](#); includes argument for obtaining a list of zones, mitigation devices, ingestion vendors, and a `test_configuration` option for testing connectivity to mitigation devices.

[get_unchecked_exposures on page 122](#)

[get_users on page 123](#)

[get_whitelist_rules on page 125](#)

[get_zones on page 126](#)

[history_details on page 127](#)

[incident_comments on page 128](#)

[incidents on page 129](#)

[incident_details on page 136](#)

[ingestion vendor details on page 146](#)

[license details on page 162](#)

[login on page 163](#)

[logout on page 165](#)

[network traffic on page 165](#)

[set auto mitigation settings on page 169](#)

[set whitelist rules on page 170](#)

[test configuration on page 170](#)

[top incidents on page 171](#)

[trace log on page 173](#)

[trace pcap on page 173](#)

[update report on page 173](#)

[verify on page 174](#)

NOTE Use of the return values "monitored" and "scanned" are deprecated in this release; refer instead to outputs for offered_traffic or inspected_traffic.

add_incident_comments

https://HOST/admin/api.php?op=add_incident_comments

HTTP Post Parameters	Description
last_status	Last incident status information
status	Current Status: options are "new," "acknowledged," "in_progress" or "complete"
comments	Comment or update
incident_id	ID of the incident for which a comment is to be added or updated

Example

```
curl -k -H "Authorization:0d5b240487eb5abcaf987ab04e8a1411" "https://192.168.2.25/admin/api.php?op=add_incident_comments" --data "last_status=new&status=complete&comments=Test%20Comment&incident_id=134"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any configured User to generate or obtain their API Key.

Sample Response

```
{"session_timeout_sec":36000,"status":0}
```

add_license

This API adds a product or support license to the current Juniper ATP Appliance system.

https://HOST/admin/api.php?op=add_license

HTTP Post Parameters	Description
filename	Name of the license key file to be uploaded and added as a new license
license_type	Product or Support license type

Example

```
curl -k -b SESSID=fhffc90prmu9dte2bu4mv3od11 -d  
"filename=licenseKey&license_type=product"  
"https://HOST/admin/api.php?op=add\_license"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any configured User to generate or obtain their API Key.

Sample Response

There is no response for this API request.

add_user

This API adds a new user to the Juniper ATP Appliance system.

https://HOST/admin/api.php?op=add_user

HTTP Post Parameters	Description
user_name	Username of new user to be added to system
full_name	Full name of the new user
is_admin	New user's admin access profile; 1 is enabled
has_debug	New user's debug access privilege; 1 is enabled
generate_api_key	0 for no; 1 for yes
api_key	key definition or _is_disabled if not enabled

password	Password for the new user
csrf_token	unique token ID for the new user
remote_authentication	Valid values are true or false. This key determines whether the user being created will be authenticated using the remote system or not.
remote_authorization	Valid values are true or false. This key determines whether the user being created will be authorized using the remote system or not.

Example

```
curl -k -H "Authorization:d7e6d14140fc944fc4ba287f88f42d45"
"https://10.2.20.107/admin/api.php?op=add_user" -d user_name=test2 -d
full_name=test2 -d role_name='Default Admin Role' -d
generate_api_key=0 -d api_key_is_disabled=0 -d password=JATPlz2 -d
remote_authentication=false -d remote_authorization=false
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

There is no response from this API call.

analysis_details

Use the analysis_details API to retrieve the analysis details associated with a particular file object. The analysis_details API takes either an event_id, md5sum or sha1sum as a parameter.

TIP As of Release 4.1.1 and later, Juniper ATP Appliance now limits the upload to the actual processing limit and throws an error if the file is greater than 16MB.

Unlike the “event” API, analysis_details does not return any context about how and when the file object was discovered.

An additional boolean parameter “get_components” set to 1 will cause the return of all the components of the specified file. This option is only meaningful if the md5sum/sha1sum corresponds to a zip, tar, or other archive.

https://HOST/admin/api.php?op=analysis_details

HTTP Post Parameters	Description
event_id or md5sum/ sha1sum	[Required] Unique identifier for this event. One of these parameters is a mandatory parameter. Get this from the output of the API <a href="https://<Host>/admin/api.php?op=events">https://<Host>/admin/api.php?op=events The md5sum & sha1sum are the hashes of the objects.

get_components	1 indicates components are available. When the get_components value is set, analysis details for all the sub-components are also returned.
----------------	---

API Access: To demonstrate the analysis_details API from the Central Manager Web UI Incidents page: select an incident from the Incidents table then scroll down the page and click Downloads or Uploads tab. Expand the row to view details and with this action, you will see a call to the analysis_details API.

See also [behavior_details on page 10](#)

Example

```
curl -k -H "Authorization:7c71c218662411a5c857042053acca8f"
"https://10.2.20.37/admin/api.php?op=analysis_details" -d
event_id=672
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

NOTE The request should include one of event-id or md5 or sha1. If both are specified, then the server only considers the event-id.

Sample Response

```
{
  analysis_array:
  [
    1]
    0:
    {
      local_path: "/var/spool/c-icap/download/CI_TMPFP9jYz"
      file_md5_string: "7be866d691c3da79f51240bf8963e210"
      file_sha1_string:
        "1f707b2fe77691ee91aa5da0a326aec40182bb0d"
      file_sha256_string:
        "fada509542437360aeaa73a6256a9f1c8
        8764e823f0f0a6a78fb66e419b5f389"
      file_size: "893977"
      file_type_string: "PE32 executable (GUI) Intel 80386,
        for MS Windows"
      file_suffix: "exe"
      mime_type_string: "FILE_UPLOAD"
      has_components: null
      packer_name: null
      malware_name: "TROJAN_YAKES.CY"
      malware_severity: "0.75"
      malware_category: "Trojan_Generic"
      malware_classname: "malware"
      has_static_detection: "1"
      has_behavioral_detection: "0"
```

```

        user_whitelisted: null
        JATP_whitelisted: null
        has_cnc: null
        dig_cert_name: null
        analysis_start_time: "2016-06-02 08:34:40.513488+00"
        analysis_done_time: "2016-06-02 08:35:03.877626+00"
        source_url_rank: "-1"
        reputation_score: "35"
        microsoft_name: "None"
        has_behavior_log: "1"
        screen_shots:
        [
        3]
            0:  "/analysis/897/qemu-results/screenshots-
            winxp/screenshot_00.jpg"
            1:  "/analysis/897/qemu-results/screenshots-
            winxp/screenshot_01.jpg"
            2:  "/analysis/897/qemu-results/screenshots-
            winxp/screenshot_02.jpg"
        -
    }
    -
-
analysis_details:
{
    local_path: "/var/spool/c-icap/download/CI_TMPFP9jYz"
    file_md5_string: "7be866d691c3da79f51240bf8963e210"
    file_sha1_string: "1f707b2fe77691ee91aa5da0a326aec40182bb0d"
    file_sha256_string: "fada509542437360aeaa73a6256a9f1c88
764e823f0f0a6a78fb66e419b5f389"
    file_size: "893977"
    file_type_string: "PE32 executable (GUI) Intel 80386, for MS
Windows"
    file_suffix: "exe"
    mime_type_string: "FILE_UPLOAD"
    has_components: null
    packer_name: null
    malware_name: "TROJAN_YAKES.CY"
    malware_severity: "0.75"
    malware_category: "Trojan_Generic"
    malware_classname: "malware"
    has_static_detection: "1"
    has_behavioral_detection: "0"
    user_whitelisted: null
    JATP_whitelisted: null
    has_cnc: null
    dig_cert_name: null
    analysis_start_time: "2016-06-02 08:34:40.513488+00"
    analysis_done_time: "2016-06-02 08:35:03.877626+00"
    source_url_rank: "-1"

```

```
    reputation_score: "35"
    microsoft_name: "None"
    has_behavior_log: "1"
    screen_shots:
    [
    3]
      0:  "/analysis/897/qemu-results/screenshots-winxp/
          screenshot_00.jpg"
      1:  "/analysis/897/qemu-results/screenshots-winxp/
          screenshot_01.jpg"
      2:  "/analysis/897/qemu-results/screenshots-winxp/
          screenshot_02.jpg"
    -
  }
  -
  status: 0
}
```

backup

Use this API performs a backup of the running config for the current Juniper ATP Appliance system. This API uses no parameters, and the response for this API is the file containing the backup.

<https://HOST/admin/api.php?op=backup>

Example

```
curl -k -v -b "Authorization:7c71c218662411a5c857042053acca8f"-d
"https://HOST/admin/api.php?op=backup"
```

Authorization - The device user API key.
Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

There is no response generated for this API.

behavior_details

This API retrieves per-event analysis details from the Juniper ATP Appliance behavior analysis engine. Use this API to capture all behavioral analysis details for a selected incident event, including all registry changes, mutexes created, and so on.

HTTP Post Parameters	Description
event_id	[Required] Obtain this ID from the of the API <a href="https://<Host>/admin/api.php?op=events">https://<Host>/admin/api.php?op=events

collector_id	ID of the Collector that processed the malicious traffic.
--------------	---

API Access: To demonstrate the behavior_details API from the Central Manager Web UI Incidents page: select an incident from the Incidents table then scroll down the page and click Downloads or Uploads tab. Expand the row to view details and with this action, you will see a call to the behavior_details API.

See also [analysis_details on page 7](#)

Example

```
curl -k -H "Authorization:7c71c218662411a5c857042053acca8f"
"https://10.2.20.37/admin/api.php?op=behavior_details" -d
event_id=672&collector_id=aaaa-bbbb-cccc-ddddd"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

NEW: Additional JSON objects are available for obtaining third party ingestion vendor information:

[memory_artifact_details](#) This contains all the memory artifact strings that are recognized for the executable from which Juniper ATP Appliance is able to take a memory dump when certain Windows API calls are used. This corresponds to Memory Artifacts information displayed in the Juniper ATP Appliance Central Manager Web UI incident displays.

[behavior_details](#) uses an object called malware_actions that lists all the actions exhibited by detected malware. This corresponds to the Malware Traits information displayed in the Juniper ATP Appliance Central Manager Web UI incident displays.

Sample Output

```
curl 'https://10.2.25.21/admin/
api.php?op=behavior_details&sha1sum=c174ed87d658110b1596e30a827a810f0
e1bc102' -H 'Host: 10.2.25.24' -H
"Authorization:292fef0472b25dd9e1c032c69a4c9a18" --insecure |
json_pp

{
  "behavior_details": {
    "has_ivp": true,
    "cnc_array": [
      {
        "host": "teredo.ipv6.microsoft.com",
        "string": "port 53 DNS",
        "response": ""
      }
    ],
    "registry_changes": [
```

```
{
  "key_path":
  "\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet001\\services\\Disk\\Enum",
  "was_created": 0
},
{
  "key_path": "\\REGISTRY\\MACHINE\\HARDWARE\\DESCRIPTION\\System",
  "was_created": 0
},
{
  "key_path": "\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion",
  "was_created": 0
},
{
  "key_path": "\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\AeDebug",
  "was_created": 0
},
{
  "key_path":
  "\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\U
ninstall",
  "was_created": 0
},
{
  "key_path":
  "\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet001\\services\\Disk\\Enum",
  "was_created": 0
},
{
  "key_path": "\\REGISTRY\\MACHINE\\HARDWARE\\DESCRIPTION\\System",
  "was_created": 0
},
{
  "key_path": "\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion",
  "was_created": 0
}
```



```
    },
    {
      "key_path": "\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\AeDebug",
      "was_created": 0
    },
    {
      "key_path":
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\U
ninstall",
      "was_created": 0
    },
    {
      "key_path":
"\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet001\\services\\Disk\\Enum",
      "was_created": 0
    },
    {
      "key_path": "\\REGISTRY\\MACHINE\\HARDWARE\\DESCRIPTION\\System",
      "was_created": 0
    },
    {
      "key_path": "\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion",
      "was_created": 0
    },
    {
      "key_path": "\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\AeDebug",
      "was_created": 0
    },
    {
      "key_path":
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\U
ninstall",
      "was_created": 0
    }
  ],
  "malware_actions": [
```

```
{
  "line_number": 10,
  "new_pid": null,
  "description": "Checks the disk enum registry key to see if it
contains virtual, vmware, vbox, qemu, etc.",
  "file_name": "JATP-000-1556.txt",
  "group_priority": 20,
  "pid": 1556,
  "group_name": "anti_sandbox",
  "value_details":
  "\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet001\\services\\Disk\\Enum",
  "group_description": "Anti Sandbox",
  "action_name": "regkey_open"
},
{
  "line_number": 11,
  "new_pid": null,
  "description": "Checks the disk enum registry key to see if it
contains virtual, vmware, vbox, qemu, etc.",
  "file_name": "JATP-000-1556.txt",
  "group_priority": 20,
  "pid": 1556,
  "group_name": "anti_sandbox",
  "value_details":
  "\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet001\\services\\Disk\\Enum\\\\"
  "0\\",
  "group_description": "Anti Sandbox",
  "action_name": "regval_query"
},
{
  "line_number": 13,
  "new_pid": null,
  "description": "Accesses a suspicious registry key",
  "file_name": "JATP-000-1556.txt",
  "group_priority": 100,
  "pid": 1556,
  "group_name": "suspicious_reg_access",
  "value_details":
```

```
"\\REGISTRY\\MACHINE\\HARDWARE\\DESCRIPTION\\System",
  "group_description": "Suspicious Registry Accesses",
  "action_name": "regkey_open"
},
{
  "line_number": 14,
  "new_pid": null,
  "description": "Checks the System BIOS/Processor registry key to
see if it contains virtual, vmware, vbox, qemu, etc.",
  "file_name": "JATP-000-1556.txt",
  "group_priority": 20,
  "pid": 1556,
  "group_name": "anti_sandbox",
  "value_details":
"\\REGISTRY\\MACHINE\\HARDWARE\\DESCRIPTION\\System\\SystemBiosVers
ion\\",
  "group_description": "Anti Sandbox",
  "action_name": "regval_query"
},
{
  "line_number": 16,
  "new_pid": null,
  "description": "Accesses a registry key",
  "file_name": "JATP-000-1556.txt",
  "group_priority": 130,
  "pid": 1556,
  "group_name": "other_reg_access",
  "value_details":
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion",
  "group_description": "All Other Registry Accesses",
  "action_name": "regkey_open"
},
{
  "line_number": 17,
  "new_pid": null,
  "description": "Checks the ProductId/InstallDate to see if it's
on the known sandbox list",
```

```
    "file_name": "JATP-000-1556.txt",
    "group_priority": 20,
    "pid": 1556,
    "group_name": "anti_sandbox",
    "value_details":
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\\\"ProductId\\",
    "group_description": "Anti Sandbox",
    "action_name": "regval_query"
},
{
    "line_number": 19,
    "new_pid": null,
    "description": "Checks to see if the Just In Time debugger is set
(also known as post mortem debugger)",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 30,
    "pid": 1556,
    "group_name": "anti_debug",
    "value_details":
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\AeDebug",
    "group_description": "Anti Debug",
    "action_name": "regkey_open"
},
{
    "line_number": 21,
    "new_pid": null,
    "description": "Checks the registry to get a list of installed
apps",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 20,
    "pid": 1556,
    "group_name": "anti_sandbox",
    "value_details":
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\U
ninstall",
    "group_description": "Anti Sandbox",
    "action_name": "regkey_open"
```

```
    },
    {
      "line_number": 24,
      "new_pid": null,
      "description": "Creates a new file",
      "file_name": "JATP-000-1556.txt",
      "group_priority": 110,
      "pid": 1556,
      "group_name": "misc_file_creation",
      "value_details":
"C:\\Users\\John\\AppData\\Local\\Temp\\csrss.exe",
      "group_description": "All Other File Drops",
      "action_name": "new_file"
    },
    {
      "line_number": 35,
      "new_pid": null,
      "description": "Creates a new file",
      "file_name": "JATP-000-1556.txt",
      "group_priority": 110,
      "pid": 1556,
      "group_name": "misc_file_creation",
      "value_details":
"C:\\Users\\John\\AppData\\Local\\Temp\\svnhost.exe",
      "group_description": "All Other File Drops",
      "action_name": "new_file"
    },
    {
      "line_number": 46,
      "new_pid": null,
      "description": "Creates a new file",
      "file_name": "JATP-000-1556.txt",
      "group_priority": 110,
      "pid": 1556,
      "group_name": "misc_file_creation",
      "value_details":
"C:\\Users\\John\\AppData\\Local\\Temp\\isass.exe",
```

```
    "group_description": "All Other File Drops",
    "action_name": "new_file"
  },
  {
    "line_number": 57,
    "new_pid": null,
    "description": "Allocates committed memory with execute bit set -
could be a process of injecting code",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 105,
    "pid": 1556,
    "group_name": "code_injection",
    "value_details": "4096",
    "group_description": "Suspicious Code Injection Behaviors",
    "action_name": "allocate_committed_mem_exec"
  },
  {
    "line_number": 59,
    "new_pid": null,
    "description": "Sets a page of memory to enable execution",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 105,
    "pid": 1556,
    "group_name": "code_injection",
    "value_details": null,
    "group_description": "Suspicious Code Injection Behaviors",
    "action_name": "set_mem_execute"
  },
  {
    "line_number": 10,
    "new_pid": null,
    "description": "Checks the disk enum registry key to see if it
contains virtual, vmware, vbox, qemu, etc.",
    "file_name": "JATP-001-1268.txt",
    "group_priority": 20,
    "pid": 1268,
    "group_name": "anti_sandbox",
```

```
    "value_details":
"\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Disk\Enum",
    "group_description": "Anti Sandbox",
    "action_name": "regkey_open"
},
{
    "line_number": 11,
    "new_pid": null,
    "description": "Checks the disk enum registry key to see if it
contains virtual, vmware, vbox, qemu, etc.",
    "file_name": "JATP-001-1268.txt",
    "group_priority": 20,
    "pid": 1268,
    "group_name": "anti_sandbox",
    "value_details":
"\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Disk\Enum\\"
0\",
    "group_description": "Anti Sandbox",
    "action_name": "regval_query"
},
{
    "line_number": 13,
    "new_pid": null,
    "description": "Accesses a suspicious registry key",
    "file_name": "JATP-001-1268.txt",
    "group_priority": 100,
    "pid": 1268,
    "group_name": "suspicious_reg_access",
    "value_details":
"\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System",
    "group_description": "Suspicious Registry Accesses",
    "action_name": "regkey_open"
},
{
    "line_number": 14,
    "new_pid": null,
    "description": "Checks the System BIOS/Processor registry key to
see if it contains virtual, vmware, vbox, qemu, etc.",
```

```
    "file_name": "JATP-001-1268.txt",
    "group_priority": 20,
    "pid": 1268,
    "group_name": "anti_sandbox",
    "value_details":
"\\REGISTRY\\MACHINE\\HARDWARE\\DESCRIPTION\\System\\\\"SystemBiosVers
ion\\",
    "group_description": "Anti Sandbox",
    "action_name": "regval_query"
},
{
    "line_number": 16,
    "new_pid": null,
    "description": "Accesses a registry key",
    "file_name": "JATP-001-1268.txt",
    "group_priority": 130,
    "pid": 1268,
    "group_name": "other_reg_access",
    "value_details":
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion",
    "group_description": "All Other Registry Accesses",
    "action_name": "regkey_open"
},
{
    "line_number": 17,
    "new_pid": null,
    "description": "Checks the ProductId/InstallDate to see if it's
on the known sandbox list",
    "file_name": "JATP-001-1268.txt",
    "group_priority": 20,
    "pid": 1268,
    "group_name": "anti_sandbox",
    "value_details":
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\\\"ProductId\\",
    "group_description": "Anti Sandbox",
    "action_name": "regval_query"
```



```
    },
    {
      "line_number": 19,
      "new_pid": null,
      "description": "Checks to see if the Just In Time debugger is set
(also known as post mortem debugger)",
      "file_name": "JATP-001-1268.txt",
      "group_priority": 30,
      "pid": 1268,
      "group_name": "anti_debug",
      "value_details":
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\AeDebug",
      "group_description": "Anti Debug",
      "action_name": "regkey_open"
    },
    {
      "line_number": 21,
      "new_pid": null,
      "description": "Checks the registry to get a list of installed
apps",
      "file_name": "JATP-001-1268.txt",
      "group_priority": 20,
      "pid": 1268,
      "group_name": "anti_sandbox",
      "value_details":
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\U
ninstall",
      "group_description": "Anti Sandbox",
      "action_name": "regkey_open"
    },
    {
      "line_number": 10,
      "new_pid": null,
      "description": "Checks the disk enum registry key to see if it
contains virtual, vmware, vbox, qemu, etc.",
      "file_name": "JATP-003-1044.txt",
      "group_priority": 20,
```

```
    "pid": 1044,
    "group_name": "anti_sandbox",
    "value_details":
"\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Disk\Enum",
    "group_description": "Anti Sandbox",
    "action_name": "regkey_open"
},
{
    "line_number": 11,
    "new_pid": null,
    "description": "Checks the disk enum registry key to see if it
contains virtual, vmware, vbox, qemu, etc.",
    "file_name": "JATP-003-1044.txt",
    "group_priority": 20,
    "pid": 1044,
    "group_name": "anti_sandbox",
    "value_details":
"\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Disk\Enum\\"
0\",
    "group_description": "Anti Sandbox",
    "action_name": "regval_query"
},
{
    "line_number": 13,
    "new_pid": null,
    "description": "Accesses a suspicious registry key",
    "file_name": "JATP-003-1044.txt",
    "group_priority": 100,
    "pid": 1044,
    "group_name": "suspicious_reg_access",
    "value_details":
"\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System",
    "group_description": "Suspicious Registry Accesses",
    "action_name": "regkey_open"
},
{
    "line_number": 14,
    "new_pid": null,
```

```

        "description": "Checks the System BIOS/Processor registry key to
see if it contains virtual, vmware, vbox, qemu, etc.",
        "file_name": "JATP-003-1044.txt",
        "group_priority": 20,
        "pid": 1044,
        "group_name": "anti_sandbox",
        "value_details":
"\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\SystemBiosVers
ion",
        "group_description": "Anti Sandbox",
        "action_name": "regval_query"
    },
    {
        "line_number": 16,
        "new_pid": null,
        "description": "Accesses a registry key",
        "file_name": "JATP-003-1044.txt",
        "group_priority": 130,
        "pid": 1044,
        "group_name": "other_reg_access",
        "value_details":
"\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion",
        "group_description": "All Other Registry Accesses",
        "action_name": "regkey_open"
    },
    {
        "line_number": 17,
        "new_pid": null,
        "description": "Checks the ProductId/InstallDate to see if it's
on the known sandbox list",
        "file_name": "JATP-003-1044.txt",
        "group_priority": 20,
        "pid": 1044,
        "group_name": "anti_sandbox",
        "value_details":
"\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\ProductId",
        "group_description": "Anti Sandbox",

```

```
    "action_name": "regval_query"
  },
  {
    "line_number": 19,
    "new_pid": null,
    "description": "Checks to see if the Just In Time debugger is set
(also known as post mortem debugger)",
    "file_name": "JATP-003-1044.txt",
    "group_priority": 30,
    "pid": 1044,
    "group_name": "anti_debug",
    "value_details":
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\AeDebug",
    "group_description": "Anti Debug",
    "action_name": "regkey_open"
  },
  {
    "line_number": 21,
    "new_pid": null,
    "description": "Checks the registry to get a list of installed
apps",
    "file_name": "JATP-003-1044.txt",
    "group_priority": 20,
    "pid": 1044,
    "group_name": "anti_sandbox",
    "value_details":
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\U
ninstall",
    "group_description": "Anti Sandbox",
    "action_name": "regkey_open"
  },
  {
    "line_number": 7,
    "new_pid": null,
    "description": "Checks to see if a remote debugger is attached",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 30,
```

```
    "pid": 1556,
    "group_name": "anti_debug",
    "value_details": null,
    "group_description": "Anti Debug",
    "action_name": "check_remote_debugger"
  },
  {
    "line_number": 7,
    "new_pid": null,
    "description": "Checks to see if a remote debugger is attached",
    "file_name": "JATP-001-1268.txt",
    "group_priority": 30,
    "pid": 1268,
    "group_name": "anti_debug",
    "value_details": null,
    "group_description": "Anti Debug",
    "action_name": "check_remote_debugger"
  },
  {
    "line_number": 7,
    "new_pid": null,
    "description": "Checks to see if a remote debugger is attached",
    "file_name": "JATP-003-1044.txt",
    "group_priority": 30,
    "pid": 1044,
    "group_name": "anti_debug",
    "value_details": null,
    "group_description": "Anti Debug",
    "action_name": "check_remote_debugger"
  },
  {
    "line_number": 57,
    "new_pid": null,
    "description": "Sets a page of memory to enable execution",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 109,
```

```
    "pid": 1556,
    "group_name": "misc_suspicious_behavior",
    "value_details": "4096",
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
  },
  {
    "line_number": 59,
    "new_pid": null,
    "description": "Sets a page of memory to enable execution",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 109,
    "pid": 1556,
    "group_name": "misc_suspicious_behavior",
    "value_details": null,
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
  },
  {
    "line_number": 43,
    "new_pid": 1344,
    "description": "Creates a spoofed system process",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 40,
    "pid": 1556,
    "group_name": "suspicious_processes",
    "value_details": "svnhost.exe",
    "group_description": "Suspicious Processes",
    "action_name": "fake_system_process"
  },
  {
    "line_number": 54,
    "new_pid": 1044,
    "description": "Creates a spoofed system process",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 40,
```

```
    "pid": 1556,
    "group_name": "suspicious_processes",
    "value_details": "isass.exe",
    "group_description": "Suspicious Processes",
    "action_name": "fake_system_process"
  },
  {
    "line_number": 32,
    "new_pid": null,
    "description": "Creates a spoofed system process from a non-
standard path",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 40,
    "pid": 1556,
    "group_name": "suspicious_processes",
    "value_details":
"C:\\Users\\John\\AppData\\Local\\Temp\\csrss.exe",
    "group_description": "Suspicious Processes",
    "action_name": "known_process_not_in_known_path"
  },
  {
    "line_number": 11,
    "new_pid": null,
    "description": "Queries suspicious registry value - anti-vm/anti-
sandbox behaviors",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 109,
    "pid": 1556,
    "group_name": "misc_suspicious_behavior",
    "value_details":
"\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet001\\services\\Disk\\Enum\\\\"
0\\",
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
  },
  {
    "line_number": 14,
    "new_pid": null,
```

```
    "description": "Queries suspicious registry value - anti-vm/anti-
sandbox behaviors",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 109,
    "pid": 1556,
    "group_name": "misc_suspicious_behavior",
    "value_details":
"\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\\"SystemBiosVers
ion\\"",
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
},
{
    "line_number": 17,
    "new_pid": null,
    "description": "Queries suspicious registry value - anti-vm/anti-
sandbox behaviors",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 109,
    "pid": 1556,
    "group_name": "misc_suspicious_behavior",
    "value_details":
"\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\\"ProductId\\"",
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
},
{
    "line_number": 11,
    "new_pid": null,
    "description": "Queries suspicious registry value - anti-vm/anti-
sandbox behaviors",
    "file_name": "JATP-001-1268.txt",
    "group_priority": 109,
    "pid": 1268,
    "group_name": "misc_suspicious_behavior",
    "value_details":
"\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Disk\Enum\\"
0\\"",
```



```
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
  },
  {
    "line_number": 14,
    "new_pid": null,
    "description": "Queries suspicious registry value - anti-vm/anti-
sandbox behaviors",
    "file_name": "JATP-001-1268.txt",
    "group_priority": 109,
    "pid": 1268,
    "group_name": "misc_suspicious_behavior",
    "value_details":
"\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\\"SystemBiosVers
ion\\"",
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
  },
  {
    "line_number": 17,
    "new_pid": null,
    "description": "Queries suspicious registry value - anti-vm/anti-
sandbox behaviors",
    "file_name": "JATP-001-1268.txt",
    "group_priority": 109,
    "pid": 1268,
    "group_name": "misc_suspicious_behavior",
    "value_details":
"\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\\"ProductId\\"",
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
  },
  {
    "line_number": 11,
    "new_pid": null,
    "description": "Queries suspicious registry value - anti-vm/anti-
sandbox behaviors",
```

```
    "file_name": "JATP-003-1044.txt",
    "group_priority": 109,
    "pid": 1044,
    "group_name": "misc_suspicious_behavior",
    "value_details":
"\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Disk\Enum\\"
0\",
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
},
{
    "line_number": 14,
    "new_pid": null,
    "description": "Queries suspicious registry value - anti-vm/anti-
sandbox behaviors",
    "file_name": "JATP-003-1044.txt",
    "group_priority": 109,
    "pid": 1044,
    "group_name": "misc_suspicious_behavior",
    "value_details":
"\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\\"SystemBiosVers
ion\",
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
},
{
    "line_number": 17,
    "new_pid": null,
    "description": "Queries suspicious registry value - anti-vm/anti-
sandbox behaviors",
    "file_name": "JATP-003-1044.txt",
    "group_priority": 109,
    "pid": 1044,
    "group_name": "misc_suspicious_behavior",
    "value_details":
"\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\\"ProductId\",
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
```

```
},
{
  "line_number": 57,
  "new_pid": null,
  "description": "Allocates and commits memory",
  "file_name": "JATP-000-1556.txt",
  "group_priority": 140,
  "pid": 1556,
  "group_name": "other_behavior",
  "value_details": null,
  "group_description": "All Other Behaviors",
  "action_name": "allocate_committed_mem"
},
{
  "line_number": 61,
  "new_pid": null,
  "description": "Calls sleep API",
  "file_name": "JATP-000-1556.txt",
  "group_priority": 109,
  "pid": 1556,
  "group_name": "misc_suspicious_behavior",
  "value_details": null,
  "group_description": "Other Suspicious Behaviors",
  "action_name": "suspicious_action"
},
{
  "line_number": 8,
  "new_pid": null,
  "description": "Outputs to debug port",
  "file_name": "JATP-000-1556.txt",
  "group_priority": 30,
  "pid": 1556,
  "group_name": "anti_debug",
  "value_details": null,
  "group_description": "Anti Debug",
  "action_name": "output_debug_string"
```

```
    },
    {
      "line_number": 8,
      "new_pid": null,
      "description": "Outputs to debug port",
      "file_name": "JATP-001-1268.txt",
      "group_priority": 30,
      "pid": 1268,
      "group_name": "anti_debug",
      "value_details": null,
      "group_description": "Anti Debug",
      "action_name": "output_debug_string"
    },
    {
      "line_number": 8,
      "new_pid": null,
      "description": "Outputs to debug port",
      "file_name": "JATP-003-1044.txt",
      "group_priority": 30,
      "pid": 1044,
      "group_name": "anti_debug",
      "value_details": null,
      "group_description": "Anti Debug",
      "action_name": "output_debug_string"
    },
    {
      "line_number": 32,
      "new_pid": null,
      "description": "Creates a process that runs in a suspicious
path",
      "file_name": "JATP-000-1556.txt",
      "group_priority": 40,
      "pid": 1556,
      "group_name": "suspicious_processes",
      "value_details":
"C:\\Users\\John\\AppData\\Local\\Temp\\csrss.exe",
      "group_description": "Suspicious Processes",
    }
```

```
    "action_name": "create_process_in_suspicious_path"
  },
  {
    "line_number": 43,
    "new_pid": null,
    "description": "Creates a process that runs in a suspicious
path",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 40,
    "pid": 1556,
    "group_name": "suspicious_processes",
    "value_details":
"C:\\Users\\John\\AppData\\Local\\Temp\\svnhost.exe",
    "group_description": "Suspicious Processes",
    "action_name": "create_process_in_suspicious_path"
  },
  {
    "line_number": 54,
    "new_pid": null,
    "description": "Creates a process that runs in a suspicious
path",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 40,
    "pid": 1556,
    "group_name": "suspicious_processes",
    "value_details":
"C:\\Users\\John\\AppData\\Local\\Temp\\isass.exe",
    "group_description": "Suspicious Processes",
    "action_name": "create_process_in_suspicious_path"
  },
  {
    "line_number": 24,
    "new_pid": null,
    "description": "Creates a suspicious file",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 50,
    "pid": 1556,
```

```
    "group_name": "suspicious_file_creation",
    "value_details":
"C:\\Users\\John\\AppData\\Local\\Temp\\csrss.exe",
    "group_description": "Suspicious File Drops",
    "action_name": "new_suspicious_file"
},
{
    "line_number": 35,
    "new_pid": null,
    "description": "Creates a suspicious file",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 50,
    "pid": 1556,
    "group_name": "suspicious_file_creation",
    "value_details":
"C:\\Users\\John\\AppData\\Local\\Temp\\svnhost.exe",
    "group_description": "Suspicious File Drops",
    "action_name": "new_suspicious_file"
},
{
    "line_number": 46,
    "new_pid": null,
    "description": "Creates a suspicious file",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 50,
    "pid": 1556,
    "group_name": "suspicious_file_creation",
    "value_details":
"C:\\Users\\John\\AppData\\Local\\Temp\\isass.exe",
    "group_description": "Suspicious File Drops",
    "action_name": "new_suspicious_file"
},
{
    "line_number": 61,
    "new_pid": null,
    "description": "Sleeps for an excessive amount of time",
    "file_name": "JATP-000-1556.txt",
```

```
    "group_priority": 20,
    "pid": 1556,
    "group_name": "anti_sandbox",
    "value_details": null,
    "group_description": "Anti Sandbox",
    "action_name": "sleep_5min+"
  },
  {
    "line_number": 10,
    "new_pid": null,
    "description": "Opens suspicious registry key",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 109,
    "pid": 1556,
    "group_name": "misc_suspicious_behavior",
    "value_details":
    "\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet001\\services\\Disk\\Enum",
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
  },
  {
    "line_number": 13,
    "new_pid": null,
    "description": "Opens suspicious registry key",
    "file_name": "JATP-000-1556.txt",
    "group_priority": 109,
    "pid": 1556,
    "group_name": "misc_suspicious_behavior",
    "value_details":
    "\\REGISTRY\\MACHINE\\HARDWARE\\DESCRIPTION\\System",
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
  },
  {
    "line_number": 19,
    "new_pid": null,
    "description": "Opens suspicious registry key",
```

```

        "file_name": "JATP-000-1556.txt",
        "group_priority": 109,
        "pid": 1556,
        "group_name": "misc_suspicious_behavior",
        "value_details":
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\AeDebug",
        "group_description": "Other Suspicious Behaviors",
        "action_name": "suspicious_action"
    },
    {
        "line_number": 21,
        "new_pid": null,
        "description": "Opens suspicious registry key",
        "file_name": "JATP-000-1556.txt",
        "group_priority": 109,
        "pid": 1556,
        "group_name": "misc_suspicious_behavior",
        "value_details":
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\U
ninstall",
        "group_description": "Other Suspicious Behaviors",
        "action_name": "suspicious_action"
    },
    {
        "line_number": 10,
        "new_pid": null,
        "description": "Opens suspicious registry key",
        "file_name": "JATP-001-1268.txt",
        "group_priority": 109,
        "pid": 1268,
        "group_name": "misc_suspicious_behavior",
        "value_details":
"\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet001\\services\\Disk\\Enum",
        "group_description": "Other Suspicious Behaviors",
        "action_name": "suspicious_action"
    },
    {

```



```
    "line_number": 13,
    "new_pid": null,
    "description": "Opens suspicious registry key",
    "file_name": "JATP-001-1268.txt",
    "group_priority": 109,
    "pid": 1268,
    "group_name": "misc_suspicious_behavior",
    "value_details":
"\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System",
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
},
{
    "line_number": 19,
    "new_pid": null,
    "description": "Opens suspicious registry key",
    "file_name": "JATP-001-1268.txt",
    "group_priority": 109,
    "pid": 1268,
    "group_name": "misc_suspicious_behavior",
    "value_details":
"\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AeDebug",
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
},
{
    "line_number": 21,
    "new_pid": null,
    "description": "Opens suspicious registry key",
    "file_name": "JATP-001-1268.txt",
    "group_priority": 109,
    "pid": 1268,
    "group_name": "misc_suspicious_behavior",
    "value_details":
"\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall",
    "group_description": "Other Suspicious Behaviors",
```

```
    "action_name": "suspicious_action"
  },
  {
    "line_number": 10,
    "new_pid": null,
    "description": "Opens suspicious registry key",
    "file_name": "JATP-003-1044.txt",
    "group_priority": 109,
    "pid": 1044,
    "group_name": "misc_suspicious_behavior",
    "value_details":
"\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet001\\services\\Disk\\Enum",
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
  },
  {
    "line_number": 13,
    "new_pid": null,
    "description": "Opens suspicious registry key",
    "file_name": "JATP-003-1044.txt",
    "group_priority": 109,
    "pid": 1044,
    "group_name": "misc_suspicious_behavior",
    "value_details":
"\\REGISTRY\\MACHINE\\HARDWARE\\DESCRIPTION\\System",
    "group_description": "Other Suspicious Behaviors",
    "action_name": "suspicious_action"
  },
  {
    "line_number": 19,
    "new_pid": null,
    "description": "Opens suspicious registry key",
    "file_name": "JATP-003-1044.txt",
    "group_priority": 109,
    "pid": 1044,
    "group_name": "misc_suspicious_behavior",
    "value_details":
```

```
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\AeDebug",
  "group_description": "Other Suspicious Behaviors",
  "action_name": "suspicious_action"
},
{
  "line_number": 21,
  "new_pid": null,
  "description": "Opens suspicious registry key",
  "file_name": "JATP-003-1044.txt",
  "group_priority": 109,
  "pid": 1044,
  "group_name": "misc_suspicious_behavior",
  "value_details":
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\U
ninstall",
  "group_description": "Other Suspicious Behaviors",
  "action_name": "suspicious_action"
}
],
"cook_env": "win7-winapi",
"processes_spawned": [
  {
    "command_ppid": 1556,
    "command_pid": 1268,
    "command_name": "csrss.exe",
    "command_args": "C:\\Users\\John\\AppData\\Local\\Temp\\csrss.exe
--anti-sandbox",
    "command_path":
"C:\\Users\\John\\AppData\\Local\\Temp\\csrss.exe"
  },
  {
    "command_ppid": 1556,
    "command_pid": 1344,
    "command_name": "svnhost.exe",
    "command_args":
"C:\\Users\\John\\AppData\\Local\\Temp\\svnhost.exe --do-nothing",
    "command_path":
```

```
"C:\\Users\\John\\AppData\\Local\\Temp\\svnhost.exe"
},
{
  "command_ppid": 1556,
  "command_pid": 1044,
  "command_name": "isass.exe",
  "command_args": "C:\\Users\\John\\AppData\\Local\\Temp\\isass.exe
--anti-sandbox",
  "command_path":
"C:\\Users\\John\\AppData\\Local\\Temp\\isass.exe"
}
],
"os_type": "win7",
"shalsum": "c174ed87d658110b1596e30a827a810f0e1bc102"
},
"memory_artifact_details": {
"JATPdum-000-1556-CreateProcessInternalW.windump": {
  "display_names": {
    "security_tools": "Security Tools Detected",
    "ips": "IP Strings",
    "vm_tools": "Virtual Machines Detected",
    "urls": "URL Strings",
    "embedded_public_key": "Encryption Keys"
  },
  "embedded_public_key": "",
  "vm_tools": [],
  "ips": [],
  "urls": [],
  "security_tools": []
}
},
"session_timeout_sec": 18000,
"status": 0,
"server_ip": "10.2.25.21",
"server_name": "10.2.25.21",
"max_cook_size": 15000001,
"status_fc_on": 0,
```

```

    "status_sigeng_on": 1,
    "status_hre_on": 1,
    "status_sc_on": 1,
    "status_correlation_on": 1,
    "status_internet_on": 1,
    "status_mode": 0,
    "status_web_collector": 0,
    "status_downstream_web_collector": 0
  }

```

Sample Response Fields

Output Field	Description
behavior_details	The analysis result of Juniper ATP Appliance's behavioral analysis engine for an event.
has_ivp	Indicates whether the infection verification package (IVP) was available for the event.
cnc_array	Command and Control (CNC) activities involved in the event.
processes_spawned	Processes that were created during the event.
registry_changes	Modification(s) to system registry during the malware event.
mutexes	Mutexes used during the event.
file_opened	Files opened during the malware event.
csrf_token	Token ID for this request.

```

{
  behavior_details:
  {
    has_ivp: true
    cnc_array:
    [
      0]
  }
}

```

```
registry_changes:
[
51]
    0:
    {
        key_path: "\REGISTRY\USER\S-1-5-21-842925246-
484763869-117609710-500\Control Panel\Mouse"
        was_created: 0
    }
    -
    1:
    {
        key_path: "\REGISTRY\USER\S-1-5-21-842925246-
484763869-117609710-
500\Software\Microsoft\Windows\CurrentVersion
\ThemeManager"
        was_created: 0
    }
    -
    2:
    {
        key_path: "\REGISTRY\USER\S-1-5-21-842925246-
484763869-117609710-500\Control Panel\Desktop"
        was_created: 0
    }
    -
    3:
    {
        key_path: "\REGISTRY\USER\S-1-5-21-842925246-
484763869-117609710-
500\Software\Microsoft\Windows\CurrentVersion
\Policies\Explorer"
        was_created: 0
    }
    -
    4:
    {
        key_path: "\REGISTRY\USER\S-1-5-21-842925246-
484763869-117609710-
500\Software\Microsoft\Windows\Current
Version\Policies\Explorer"
        was_created: 0
    }
    -
    5:
    {
        key_path: "\REGISTRY\USER\S-1-5-21-842925246-
484763869-117609710-
500\Software\Microsoft\Windows\Current
Version\Policies\Explorer"
        was_created: 0
    }
```

```
}
-
6:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-842925246-
484763869-117609710-
500\\Software\\Microsoft\\Windows\\Current
Version\\Policies\\Explorer"
    was_created: 0
}
-
7:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-842925246-
484763869-117609710-
500\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\Explorer"
    was_created: 0
}
-
8:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-842925246-
484763869-117609710-
500\\Software\\Microsoft\\Windows\\CurrentVersion\\
Policies\\Explorer"
    was_created: 0
}
-
9:
{
    key_path: "\\REGISTRY\\MACHINE\\SOFTWARE\\Classes\\
CLSID\\{20D04FE0-3AEA-1069-A2D8-
08002B30309D}\\InProcServer32"
    was_created: 0
}
-
10:
{
    key_path: "\\REGISTRY\\MACHINE\\SOFTWARE\\
Microsoft\\Rpc"
    was_created: 0
}
-
11:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-842925246-
484763869-117609710-
500\\Software\\Microsoft\\Windows\\CurrentVersion\\
Explorer\\MountPoints2\\CPC\\Volume"
    was_created: 0
}
```

```
}
-
12:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-842925246-484763869-117609710-500\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\MountPoints2\\CPC\\Volume\\{9cd0ccd9-900f-11e2-ba02-525400123456}"
    was_created: 0
}
-
13:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-842925246-484763869-117609710-500\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\MountPoints2\\CPC\\Volume"
    was_created: 0
}
-
14:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-842925246-484763869-117609710-500\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\MountPoints2\\CPC\\Volume\\{9cd0ccd9-900f-11e2-ba02-525400123456}"
    was_created: 0
}
-
15:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-842925246-484763869-117609710-500\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\MountPoints2\\CPC\\Volume"
    was_created: 0
}
-
16:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-842925246-484763869-117609710-500\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\MountPoints2\\CPC\\Volume\\{59dfa098-9b09-11e2-9897-806d6172696f}"
    was_created: 0
}
-
17:
```



```
{
  key_path: "\\REGISTRY\\USER\\S-1-5-21-842925246-
484763869-117609710-
500\\Software\\Microsoft\\Windows\\CurrentVersion\\
Explorer\\MountPoints2\\CPC\\Volume"
  was_created: 0
}
-
18:
{
  key_path: "\\REGISTRY\\USER\\S-1-5-21-842925246-
484763869-117609710-
500\\Software\\Microsoft\\Windows\\CurrentVersion\\
Explorer\\MountPoints2\\CPC\\Volume\\{59dfa098-9b09-
11e2-9897-806d6172696f}"
  was_created: 0
}
-
19:
{
  key_path: "\\REGISTRY\\USER\\S-1-5-21-842925246-
484763869-117609710-
500\\Software\\Microsoft\\Windows\\CurrentVersion\\
Explorer\\MountPoints2\\CPC\\Volume"
  was_created: 0
}
-
20:
{
  key_path: "\\REGISTRY\\USER\\S-1-5-21-842925246-
484763869-117609710-
500\\Software\\Microsoft\\Windows\\CurrentVersion\\
Explorer\\MountPoints2\\CPC\\Volume\\
{dc3e8588-366a-11e1-9c6d-806d6172696f}"
  was_created: 0
}
-
21:
{
  key_path: "\\REGISTRY\\USER\\S-1-5-21-842925246-
484763869-117609710-
500\\Software\\Microsoft\\Windows\\CurrentVersion\\
Explorer\\MountPoints2\\CPC\\Volume"
  was_created: 0
}
-
22:
{
  key_path: "\\REGISTRY\\USER\\S-1-5-21-842925246-
484763869-117609710-
500\\Software\\Microsoft\\Windows\\CurrentVersion\\
```

```
        Explorer\MountPoints2\CPC\Volume\
        {dc3e8588-366a-11e1-9c6d-806d6172696f}"
        was_created: 0
    }
-
23:
{
    key_path: "\REGISTRY\USER\S-1-5-21-842925246-
484763869-117609710-
500\Software\Microsoft\Windows\CurrentVersion\
Explorer\MountPoints2\{dc3e8588-366a-11e1-9c6d-
806d6172696f}"
    was_created: 0
}
-
24:
{
    key_path: "\REGISTRY\USER\S-1-5-21-842925246-
484763869-117609710-
500\Software\Microsoft\Windows\CurrentVersion\
Explorer\MountPoints2\{59dfa098-9b09-11e2-9897-
806d6172696f}"
    was_created: 0
}
-
25:
{
    key_path: "\REGISTRY\USER\S-1-5-21-842925246-
484763869-117609710-
500\Software\Microsoft\Windows\CurrentVersion\
Explorer\MountPoints2\{9cd0ccd9-900f-11e2-ba02-
525400123456}"
    was_created: 0
}
-
26:
{
    key_path: "\REGISTRY\USER\S-1-5-21-842925246-
484763869-117609710-
500\Software\Microsoft\Windows\CurrentVersion\
Explorer\MountPoints2\CPC\Volume"
    was_created: 0
}
-
27:
{
    key_path: "\REGISTRY\USER\S-1-5-21-842925246-
484763869-117609710-
500\Software\Microsoft\Windows\CurrentVersion\
Explorer\MountPoints2\CPC\Volume\
{dc3e8588-366a-11e1-9c6d-806d6172696f}"
```

```
        was_created: 0
    }
    -
28:
{
    key_path: "\\REGISTRY\\MACHINE\\SOFTWARE\\Classes\\
Drive\\shellex\\FolderExtensions"
    was_created: 0
}
-
29:
{
    key_path: "\\REGISTRY\\MACHINE\\SOFTWARE\\Classes\\
Drive\\shellex\\FolderExtensions\\
{fbeb8a05-beee-4442-804e-409d6c4515e9}"
    was_created: 0
}
-
30:
{
    key_path: "\\REGISTRY\\MACHINE\\SOFTWARE\\
Classes\\Directory"
    was_created: 0
}
-
31:
{
    key_path: "\\REGISTRY\\MACHINE\\SOFTWARE\\
Classes\\Directory"
    was_created: 0
}
-
32:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-842925246
-484763869-117609710-500\\Software\\Microsoft\\
Windows\\CurrentVersion\\Policies\\Explorer"
    was_created: 0
}
-
33:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-8429
25246-484763869-117609710-
500\\Software\\Microsoft\\Windows\\
CurrentVersion\\Explorer"
    was_created: 0
}
-
34:
```

```
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-8429
25246-484763869-117609710-
500\\Software\\Microsoft\\Windows\\
CurrentVersion\\Explorer"
    was_created: 0
}
-
35:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-8429
25246-484763869-117609710
500\\Software\\Microsoft\\Windows\\
CurrentVersion\\Policies\\Explorer"
    was_created: 0
}
-
36:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-8429
25246-484763869-117609710-
500\\Software\\Microsoft\\Windows\\CurrentVersion
\\Policies\\Explorer"
    was_created: 0
}
-
37:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-8429
25246-484763869-117609710-500\\Software\\
Microsoft\\Windows\\CurrentVersion\\Policies\\
Explorer"
    was_created: 0
}
-
38:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-8429
5246-484763869-117609710-
500\\Software\\Microsoft\\Windows\\
CurrentVersion\\Policies\\Explorer"
    was_created: 0
}
-
39:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-8429
25246-484763869-117609710-500\\Software\\
Microsoft\\Windows\\CurrentVersion\\
Policies\\Explorer"
    was_created: 0
}
```

```
}
-
40:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-8429
25246-484763869-117609710-500\\Software\\
Microsoft\\Windows\\CurrentVersion\\
Policies\\Explorer"
    was_created: 0
}
-
41:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-8429
25246-484763869-117609710-500\\Software\\
Microsoft\\Windows\\CurrentVersion
\\Policies\\Explorer"
    was_created: 0
}
-
42:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-8429
25246-484763869-117609710-500\\Software\\
Microsoft\\Windows
\\CurrentVersion\\Explorer\\Advanced"
    was_created: 0
}
-
43:
{
    key_path: "\\REGISTRY\\MACHINE\\SOFTWARE\\
Classes\\Folder"
    was_created: 0
}
-
44:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-8429
25246-484763869-117609710-
500\\Software\\Microsoft\\Windows\\CurrentVersion
\\Policies\\Explorer"
    was_created: 0
}
-
45:
{
    key_path: "\\REGISTRY\\USER\\S-1-5-21-8429
25246-484763869-117609710-
500\\Software\\Microsoft\\Windows\\CurrentVersion
\\Policies\\Explorer"
```

```
        was_created: 0
    }
    -
46:
{
    key_path: "\REGISTRY\USER\S-1-5-21-8429
25246-484763869-117609710-
500\Software\Microsoft\Windows\CurrentVersion
\Explorer\FileExts"
    was_created: 0
}
    -
47:
{
    key_path: "\REGISTRY\MACHINE\SOFTWARE\
Classes\.exe"
    was_created: 0
}
    -
48:
{
    key_path: "\REGISTRY\MACHINE\SOFTWARE\Classes
\exefile"
    was_created: 0
}
    -
49:
{
    key_path: "\REGISTRY\MACHINE\SOFTWARE\Classes
\exefile"
    was_created: 0
}
    -
50:
{
    key_path: "\REGISTRY\MACHINE\SOFTWARE\Classes\*"
    was_created: 0
}
    -
-
files_opened:
[
2]
    0:
    {
        file_name: "\\.\PIPE\lsarpc"
        for_pipe: 1
    }
    -
    1:
```

```

        {
            file_name: "\\.\PIPE\lsarpc"
            for_pipe: 1
        }
    -
-
}
-
session_timeout_sec: 31536000
status: 0
server_ip: "10.2.20.37"
server_name: "10.2.20.37"
status_fc_on: 1
status_sigeng_on: 1
status_hre_on: 1
status_sc_on: 1
status_correlation_on: 1
status_internet_on: 1
status_mode: 0
"status_downstream_web_collector": 1,
"status_downstream_slave_core": 0
}

```

TIP To obtain Behavior information via API, [1] query `analysis_details` for the event with `get_components=1` set; this returns the array of all child elements of the zip that includes the sha1sum for the child element(s). Next, query `behavior_details` using the sha1sum.

Example:

```

curl -k -H "Authorization:c6b5493ewr35yt4e7f51bc1b5f5556ef521d84"
"https://demo-upload.JATP.net/admin/api.php?op=analysis_details" -d
"event_id=18138" -d get_components=1

```

Then, querying `behavior_details`, something like the following is returned:

```

{
    "behavior_details": {
        "has_ivp": false,
        "cnc_array": [],
        "processes_spawned": [],
        "mutexes": [],
        "registry_changes": [],
        "files_opened": []
    },
    "session_timeout_sec": 31536000,
    "status": 0,
}

```

```
"server_ip": "192.168.1.21",
"server_name": "test-upload.JATP.net",
"max_cook_size": 15000001,
"status_fc_on": 0,
"status_sigeng_on": 1,
"status_hre_on": 1,
"status_sc_on": 1,
"status_correlation_on": 1,
"status_internet_on": 1,
"status_mode": 0,
"status_web_collector": 1
}
```

TIP Sample APIs for obtaining behavioral details from a Zip file.

1. Get components of the Zip file:

Example

URL: https://host1.JATP.net/admin/api.php?op=analysis_details

Data:

shasum:5ac9a76d3057cd40f33bf8698028ed9928badb04 (shasum of the Zip file)

get_components:1

Response:

```
{
  "status" : 0,
  "session_timeout_sec" : 900,
  "analysis_array" : [
    {
      "malware_classname" : "malware",
      "mime_type_string" : "application/x-dosexec",
      "file_size" : "61952",
      "packer_name" : "UPX v0.89.6 - v1.02 / v1.05 -v1.24 -> Markus
& Laszlo [overlay]",
      "microsoft_name" : "",
      "malware_name" : "WORM_GAMARUE.DC",
      "dig_cert_name" : null,
      "has_embedded_code" : null,
    }
  ]
}
```



```

        "file_sha1_string" :
"1bca4f69ec98ff9b65f75d1ef8d611493a231e73",
        "has_static_detection" : null,
        "custom_image_array" : [],
        "yara_rule_array" : [],
        "file_md5_string" : "acfc43903491ec6beeea552965ef7f8d",
        "has_cnc" : "1",
        "screen_shots" : [],
        "dig_cert_override" : null,
        "file_type_string" : "PE32 executable (GUI) Intel 80386, for
MS Windows",
        "file_sha256_string" :
"103c02f980f7518299999ffff64555b74be54ef1fef86265e48f7233c5ac39d7",
        "has_behavioral_detection" : "1",
        "analysis_done_time" : "2016-01-05 22:27:29.769217+00",
        "local_path" : "/var/spool/c-icap/download/ZF_ILPSAN",
        "malware_severity" : "0.75",
        "reputation_score" : "30",
        "has_components" : null,
        "malware_category" : "Trojan_Generic",
        "analysis_start_time" : "2016-01-05 22:17:12.508474+00",
        "has_yara_match" : null,
        "source_url_rank" : "-1",
        "has_behavior_log" : "1",
        "pcap_size" : "1144",
        "file_suffix" : "exe",
        "has_reputation_detection" : "1"
    }
]
}

```

2. Get behavioral details:

URL: https://test.juniper.net/admin/api.php?op=behavior_details

Data:

sha1sum:1bca4f69ec98fb9b65f75d1ef8d611493a231e73 (sha1sum from the previous response)

Response:

```
{
```

```
"status_downstream_slave_core" : 1,
"status_correlation_on" : 0,
"max_cook_size" : 6000001,
"status_sigeng_on" : 1,
"status" : 0,
"session_timeout_sec" : 900,
"status_sc_on" : 1,
"status_hre_on" : 1,
"status_fc_on" : 0,
"status_internet_on" : 1,
"behavior_details" : {
  "cnc_array" : [
    {
      "response" : "HTTP/1.0 200 OK",
      "string" : "POST /oliver.php HTTP/1.1",
      "host" : "euspeed.pl"
    },
    {
      "response" : "HTTP/1.0 200 OK",
      "string" : "POST /moonlight.php HTTP/1.1",
      "host" : "mobcity.pl"
    },
    {
      "response" : "",
      "string" : "port 53 DNS",
      "host" : "mobcity.pl"
    },
    {
      "response" : "",
      "string" : "port 53 DNS",
      "host" : "pumade.ru"
    },
    {
      "response" : "",
      "string" : "port 53 DNS",
      "host" : "update.microsoft.com"
```

```
    }
  ],
  "processes_spawned" : [
    {
      "command_args" : "C:\\Windows\\system32\\msiexec.exe",
      "command_name" : "C:\\Windows\\System32\\msiexec.exe"
    }
  ],
  "has_ivp" : false,
  "registry_changes" : [
    {
      "was_created" : 0,
      "key_path" :
"\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet001\\services\\Disk\\Enum"
    },
    {
      "was_created" : 0,
      "key_path" :
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\FontLink\\SystemLink"
    },
    {
      "was_created" : 0,
      "key_path" :
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\LanguagePack\\DataStore_V1.0"
    },
    {
      "was_created" : 0,
      "key_path" :
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\LanguagePack\\SurrogateFallback"
    },
    {
      "was_created" : 0,
      "key_path" :
"\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\LanguagePack\\SurrogateFallback"
    },
  ],

```

```
{
  "was_created" : 0,
  "key_path" :
  "\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows
  NT\\CurrentVersion\\LanguagePack\\SurrogateFallback"
}
],
"os_type" : "win7"
},
"status_web_collector" : 1,
"status_mode" : 0,
"server_ip" : "10.2.2.2",
"server_name" : "host.JATP.net"
}
```

behavior_features

Use this API to retrieve the top five suspicious behaviors and anomalies associated with a captured file, or a file submitted for analysis.

https://host/admin/api.php?op=behavior_features

HTTP Post Parameters	Description
shalsum	SHA1Sum of the object.

Example

An example of a shalsum request:

```
curl 'https://10.2.25.52/admin/
api.php?op=behavior_features&shalsum=ac8b956cf20f605a1027cccf1125e793
31d83f71' -H 'Host: 10.2.25.52' -H
"Authorization:54c20d76c5fcff62cccf2208b45712be" --insecure
```

An example of an md5sum request:

```
curl 'https://10.2.25.52/admin/
api.php?op=behavior_features&md5=fd9a81793182e414cae17975ebb0610e' -H
'Host: 10.2.25.52' -H
"Authorization:54c20d76c5fcff62cccf2208b45712be" --insecure
```

An example of an event_id request:

```
curl 'https://10.2.25.52/admin/
api.php?op=behavior_features&event_id=1005' -H 'Host: 10.2.25.52' -H
"Authorization:54c20d76c5fcff62cccf2208b45712be" --insecure
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

This API's response displays the top 5 suspicious behaviors of the object identified by its SHA1SUM. The response would be a behavior_features json dictionary that will have array of top features that caused the incident. It will be in the following format.

```
behavior_features = [
[
{
"Description": "description of malware action"
"value_string": "value representing malware action such as
registry key creation, modification, file creation etc.."
},
{
"Description": "description of malware action"
"value_string": "value representing malware action such as registry
key creation, modification, file creation etc.."
}
]
```

Example output follows:

```
{
"description": "Opens suspicious registry key",
"value_string":
".+\\\\\\\\SOFTWARE\\\\\\\\Microsoft\\\\\\\\Windows\\\\\\\\CurrentVersion\\\\\\\\Explorer
\\\\\\\\(Shell Folders|User Shell Folders)",
"value_details": "\"\\\\\\\\\\\\\\\\REGISTRY\\\\\\\\\\\\\\\\USER\\\\\\\\\\\\\\\\S-1-5-21-816955493-
887784245-1659347409-
1001\\\\\\\\Software\\\\\\\\Microsoft\\\\\\\\Windows\\\\\\\\CurrentVersion\\\\\\\\Explore
r\\\\\\\\Shell Folders\\\\\\\\\""
},
{
"description": "Queries suspicious registry value - anti-vm/
```

```
anti-sandbox behaviors",
    "value_string":
".+\\\\\\SOFTWARE\\\\\\Microsoft\\\\\\Windows\\\\\\CurrentVersion\\\\\\Explorer
\\\\\\(Shell Folders|User Shell Folders)\\\\\\.+",
    "value_details": "\"\\\\\\REGISTRY\\\\\\USER\\\\\\S-1-5-21-816955493-
887784245-1659347409-
1001\\\\\\Software\\\\\\Microsoft\\\\\\Windows\\\\\\CurrentVersion\\\\\\Explore
r\\\\\\Shell Folders\\\\\\\\\\\\\\\"Cache\\\\\\\\\\\\\\\"\""
},
{
    "description": "Count of system calls to num-traced-calls",
    "value_string": null,
    "value_details": null
},
{
    "description": "Size of the file",
    "value_string": null,
    "value_details": null
},
{
    "description": "Generates filtered kernel traces",
    "value_string": null,
    "value_details": null
}
```

bit9_config

This API configures Bit9 server integration with the Juniper ATP Appliance system for real-time threat mitigation and blocking.

https://HOST/admin/api.php?op=bit9_config

HTTP Post Parameters	Description
bit9_enabled	Enables Bit9 integration
bit9_host_name	Host name of the Bit9 server

bit9_api_key	API key obtained from Bit9
csrf_token	unique ID for the configuration

Example

```
curl -k -b SESSID=fhffc90prmu9dte2bu4mv3od11 -d
"bit9_enabled=true&bit9_host_name=bit9Server&bit9_api_key=234i78t23o1
7t34523t4&csrf_token=5459498c95a6b8.48953273"
"https://10.2.11.54/admin/api.php?op=bit9_config"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

There is no response generated for the bit9_config API.

blocked_ips

This API retrieves a list of IP addresses with corresponding malware details that can be blocked.

The API for blocked IPS data retrieval is as follows (there are no required parameters):

```
https://HOST/admin/api.php?op=blocked_ips
```

Example

```
curl -k -v -b "Authorization:7c71c218662411a5c857042053acca8f"
"https://10.2.2.2/admin/api.php?op=blocked_ips"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Output

An object is returned for each incident involving a malicious source IP which includes the following fields:

HTTP Post Parameters	Description
malware_ip	IP address associated with the malware
incident_id	Incident ID assigned to this incident
endpoint_ip	IP Address of the targeted endpoint

malware_name	Name of the malware
last_seen	Date the malware was processed by the Collector
collector_id	ID of the Collector that processed the malicious traffic

```
{
  "infection_array": [
    {
      "malware_ip": "31.170.165.131",
      "event_id": "28",
      "endpoint_ip": "10.1.1.48",
      "malware_name": "TROJAN_Vertexbot.32755.CY",
      "last_seen": "2016-06-16 07:14:34.06+00",
      "collector_id": "00000000-0000-0000-0000-000000000000"
    },
    {
      "malware_ip": "64.20.35.186",
      "event_id": "25",
      "endpoint_ip": "10.1.1.56",
      "malware_name": "TROJAN_Malex.CY",
      "last_seen": "2016-06-16 07:14:34.264+00",
      "collector_id": "00000000-0000-0000-0000-000000000000"
    },
  ],
  "blocked_ip_array": [],
  "session_timeout_sec": 900,
  "status": 0
}
```

bluecoat_config

Use this API to configure bluecoat integration for threat mitigation.

https://10.1.1.1/admin/api.php?op=bluecoat_config

HTTP Post Parameters	Description
availability	Availability of a bluecoat server port
blocked_term	IP address of the blocked terminal

cache_age	Cache aging limit
allowed_ips	IP addresses specified as "allowed" during configuration
csrf_token	unique ID for the configuration

Example

```
curl -k -v -b "Authorization:7c71c218662411a5c857042053acca8f"
"availability=1&blocked_term=content_filter_denied&cache_age=10&allow
ed_ips=&csrf_token=545a308a2731c8.84186293"
"https://10.1.1.1/admin/api.php?op=bluecoat_config"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

There is no response generated for this API call.

change_password

Use this API to change the admin password for the Juniper ATP Appliance Central Manager Web UI.

https://10.1.1.1/admin/api.php?op=change_password

HTTP Post Parameters	Description
old_password	The password to be changed.
new_password	The new password.
csrf_token	unique ID for the configuration

Example

```
curl -k -v -b "Authorization:7c71c218662411a5c857042053acca8f"
"old_password=JATPSecure98&new_password=JATPAPI978&csrf_token=545a308
a2731c8.84186293" "https://10.1.1.1/admin/api.php?op=change_password"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

There is no response generated for this API call.

collector_details

Use this API to retrieve details for a particular Web Collector.

https://10.1.1.1/admin/api.php?op=collector_details

Example

```
curl "https://localhost/admin/api.php?op=collector_details"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

An example response follows.

```
{
  "service_status": {
    "LOADOMETER": "1",
    "GSS": "1",
    "CHAINHEUR": "0",
    "SURICATA": "0",
    "OVERALL HEALTH": "0",
    "Last Refresh TimeStamp": 1436190063,
    "CONFIG": "1",
    "PCAP-TAP-ICAP (ETH1)": "0",
    "COLLECTOR-AGENT": "1",
    "HEALTHMONITOR": "1"
  },
  "session_timeout_sec": 36000,
  "status": 0
}
```

collectors_summary

Use this API to retrieve summary information from all Web Collectors connected to the Core.

https://10.1.1.1/admin/api.php?op=collectors_summary

HTTP Post Parameters	Description
collector_id	The ID of the collector for which details information is to be retrieved.

Example

```
curl "https://localhost/admin/api.php?op=collector_details" --data  
"collector_id=03020100-0504-0706-0809-0a0b0c0d0e0f"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

An example response follows.

```
{  
  "service_status": {  
    "LOADOMETER": "1",  
    "GSS": "1",  
    "CHAINHEUR": "0",  
    "SURICATA": "0",  
    "OVERALL HEALTH": "0",  
    "Last Refresh TimeStamp": 1436190063,  
    "CONFIG": "1",  
    "PCAP-TAP-ICAP (ETH1)": "0",  
    "COLLECTOR-AGENT": "1",  
    "HEALTHMONITOR": "1"  
  },  
  "session_timeout_sec": 36000,  
  "status": 0  
}
```

collector_performance

Use this API to retrieve the performance trend data for a specified collector.

https://10.1.1.1/admin/api.php?op=collector_performance

HTTP Post Parameters	Description
interval_sec	The number of seconds in the time frame of interest, ending in "end_time_sec"
num_intervals	The number of intervals.
tz_offset_sec	The tz offset in seconds.
collector_id	The ID of the collector for which performance information is to be retrieved.
metric_name	Name of the metric
offered_traffic	Traffic processed for every 5min in kbps.
offered_traffic_rate	Total bandwidth of traffic being analyzed.
inspected_traffic_rate	The traffic objects inspected by the analysis and detection engines.

Example

```
curl 'https://localhost/admin/api.php?op=collector_performance' --data 'interval_sec=27000&num_intervals=96&tz_offset_sec=19800&collector_id=03020100-0504-0706-0809-0a0b0c0d0e0f&metric_name=offered_traffic_rate'
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

A sample response follows:

```
{
  "data": [
    {
      "time_window": 1433602247,
      "inspected_traffic_rate": 426,
```

```
    "offered_traffic_rate": 426,  
    "cpu_usage": 10,  
    "mem_usage": 96,  
    "total_objects": 9163,  
    "malware_objects": 4610  
  },  
  
  {  
    "time_window": 1436167247,  
    "inspected_traffic_rate": 5371,  
    "offered_traffic_rate": 5371,  
    "cpu_usage": 93,  
    "mem_usage": 57,  
    "total_objects": 355,  
    "malware_objects": 77  
  }  
],  
  "session_timeout_sec": 36000,  
  "status": 0  
}
```

collectors_summary

Use this API to retrieve summary information from all Web Collectors connected to the Core.

https://10.1.1.1/admin/api.php?op=collectors_summary

Example

```
curl "https://localhost/admin/api.php?op=collectors_summary"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

An example response follows.

```
{
  "collectors_stats": [
    {
      "id": "03020100-0504-0706-0809-0a0b0c0d0e0f",
      "name": "tap37",
      "ip": "10.2.20.37",
      "enabled": true,
      "cpu_usage": "3",
      "peak_cpu_usage": "5",
      "disk_partition": "/dev/sda1",
      "disk_size": "483813253120",
      "disk_used": "86680829952",
      "disk_avail": "372556058624",
      "disk_usage": 19,
      "mem_total": "8230207488",
      "mem_free": "3539337216",
      "mem_usage": 57,
      "inspected_traffic_rate": 3,
      "offered_traffic_rate": 3,
      "offered_traffic": "960",
      "offered_traffic": "960",
      "inspected_traffic": "0",
      "num_packets_dropped": "0",
      "total_objects": "23",
      "malware_objects": "22",
      "status_ts": 1436192153,
      "status": "OK",
      "last_event_time": 1435225814,
      "last_event_type": "exploit",
      "last_event_severity": "0.25"
    }
  ],
  "session_timeout_sec": 36000,
  "status": 0
}
```

delete_whitelist_rules

Use this API to delete configured whitelist rules by name.

https://<Host>/admin/api.php?op=delete_whitelist_rules

<Host> - the IP Address of the device

HTTP Post Parameters	Description
type	[optional] Specifies the type; possible value "incident"
name	Name of the rule to be deleted

An example follows.

Example

```
curl "https://10.2.20.84/admin/api.php?op=delete_whitelist_rules"
-data "name=NewRule&type=incident"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

There is no response available for this API.

download_matched_yara

Use this API to download matched yara rule detections.

https://<Host>/admin/api.php?op=download_matched_yara

<Host> - the IP Address of the device

HTTP Post Parameters	Description
type	[optional] Specifies the type; possible value "incident"
name	Name of the yara rule.

An example follows.

Example

```
curl "https://10.2.20.84/admin/api.php?op=download_matched_yara"
-data "name=NewRule&type=incident"
```

Authorization – The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

events

Use this API to retrieve the raw data accrued during the detection and analysis process.

The “events” API provides two API calls: one that provides an array of events, and another that presents the details of the event.

Get Events API: [events](#)

Get Events Details: [event_details](#) [For information about this API, go to [event_details](#)]

To recap: Juniper ATP Appliance defines “incidents” as a group of events that share the same enterprise endpoint. In other words, a Juniper ATP Appliance incident contains events that are likely part of the same attack. Currently, the grouping of events into an incident is primarily a measure of co-occurrence in time; the events occurred at or from the same endpoint within a 5-minute timespan. In recent releases, Juniper ATP Appliance separated correlation results into incident groups and now provides an “events” API that retrieves the raw data accrued during the detection and analysis process.

Events include:

- a download
- a CnC detection via signature
- a phishing detection
- a malicious email URL or attachment
- exploits from chain heuristics
- a user upload

Get Events

Use the following “events” API to get events. This API returns an event_array which contains the fields listed below.

<https://<Host>/admin/api.php?op=events>

where <Host> is The IP address of the device

The inputs to the “events” API are as follows and except for the parameter “export_csv” are used to select which events to return:

HTTP Post Parameters for “events” API	Description
api_key	[Optional] The API authorization key.
custom_snort_event	[Optional] Provides data for custom SNORT events that have been recognized in this application.
end_time_sec	[Optional] The UTC timestamp of the end of the time frame of interest.
export_csv	[Optional] Displays the incident report in comma separated values (CSV) format: 0 indicates no CSV export; 1 indicates export CSV.
filetype_value	[Optional] The file type of interest: exe, pdf, dll
geo_value	[Optional] A two-letter country code representing the threat source.

interval_sec	[Required] The number of seconds in the time frame of interest, ending in "end_time_sec"
local_ip_value	[Optional] IP address of the threat target.
malwarename_value	[Optional] The name of the detected malware.
max_results	[Optional] The maximum number of results to return.
max_severity_value	[Required] Maximum risk of the events of interest, range 0-1; maximum severity; see explanation of min_severity_value for more details.
min_severity_value	<p>[Optional] The minimum severity of the events of interest, which ranges from 0 to 1.0, where 0 indicates a benign event and 1.0 indicates the highest severity.</p> <p>The query will return all events greater or equal to the given min_severity_value and strictly less than the max_severity_value except when the min_severity_value is 0 and/or the max_severity_value is 1, in which case all events with severity greater than zero and/or less than or equal to one will be returned.</p> <p>To return all benign events set both the min_severity_value and max_severity_value to zero.</p>
remote_ip_value	[Optional] The IP address of the threat source.
total_events	[Optional] The total number of events returned.
collector_id	[Optional] ID of the Collector that processed the malicious traffic.
third_party_info	[Optional] For every event in an event_array, a third_party_info attribute can be added. It has a unique structure shown below in this section when the event_type is set as third_party. If the event_type is not set as third_party, the value of this attribute will be null.
zone_uuid	The tenant zone_uuid in the incident_array elements

The "events" API will return zone_uuid in the event_array json response elements.

Example

```
curl -k -H "Authorization:d5d0e4e71c9ab6d7bfa8fff4dab341a5" "https://
10.2.9.43/admin/api.php?op=events" -d
"interval_sec=2592000&max_severity_value=1"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

Sample output for this API is provided further below. Output field definitions are provided here:

Output Field	Definition
analysis_done_time	Timestamp for the completion of event analysis.
app_protocol_array	HTTP or Email protocol instance, as in: "app_protocol_array": ["EMAIL"],
collector_id_array	Collector(s) that observed this event. A string enclosed in curly braces { }; as in: "collector_id_array": ["00000000-0000-0000-0000-000000000001"],
collector_name	Name of the collector that observed the event.
destination_email_id	The destination email ID.
endpoint_hostname	The hostname of the endpoint.
endpoint_id	The ID associated with the endpoint.
endpoint_ip	The IP address of the endpoint.
endpoint_name	The DNS-resolved name of the endpoint.
endpoint_os_type	The target OS determined by observing the traffic on the appliance.
endpoint_username	The username for the endpoint device.
event_category	Malware category associated with this event, for example: Adware, Trojan_DDOS, Trojan_Backdoor, etc.
event_id	The ID of this event.
event_name	Name of the threat or malware.
event_severity	Ranges from 0 (clean) to 1.0 (critical).
event_type	Type of event: "exploit", "http", "email", "cnc", "submission" (for file submission), "fsp" (for lateral detection).
has_phishing	Indication of a phishing event: "1" = true, as in "has_phishing": "1",
incident_id	The ID of the incident for which this event is correlated.
incident_risk	Risk level of the incident containing this event.
initial_done_time	Timestamp for completion of the heuristics-level analysis of the event; for example: 2016-06-31 09:45:28.670764+00
last_activity_time	The timestamp at which this event was last observed.
last_activity_epoch	Duration values in seconds; for example: 1441014034.66748
normalized_name	Normalized malware name
search_data	Search criteria applied to analysis.
source_country_code	The country code using a geoIP lookup of the threat source IP.
source_country_name	The country name using a geoIP lookup of the threat source IP.
source_email_id	The threat source email ID.

source_hostname	The threat source device hostname.
source_id	The ID for the threat source device.
source_ip	Threat source IP address.
source_name	The DNS-resolved name of the threat source IP address.
source_username	The threat source device username.
threat_source	The threat source qualifier: "threat_source":"newcard.dyndns.biz"
threat_target	A string enclosed in curly braces { }, as in: "threat_target":{"switch-54.corp.biz.com."},

Response to the “events” example call:

```
{
  "event_id": "506",
  "event_type": "http",
  "event_category": "Trojan_Generic",
  "event_name": "Njrat",
  "normalized_name": "Njrat",
  "event_severity": "0.2",
  "last_activity_time": "2016-06-03 08:35:01.462934+00",
  "last_activity_epoch": "1464942901.46293",
  "initial_done_time": "2016-06-03 08:35:40.751017+00",
  "analysis_done_time": "2016-06-03 08:35:40.751017+00",
  "endpoint_ip": "192.168.2.23",
  "endpoint_name": "192.168.2.23",
  "endpoint_os_type": "windows",
  "source_ip": "65.1.1.2",
  "source_name": "balckanweb.com",
  "source_country_code": "US",
  "source_country_name": "USA",
  "incident_id": "237",
  "incident_risk": "0.250",
  "user_ack_status": "new",
  "collector_name": "shiva-ui-automation-galileo",
  "search_data": "http://balckanweb.com/raghav/dotnetfiles/samples/e/e8e173b4eebae4a2bc2f49819e71349df373cf9ecd3b338ff6c28cc91632bb2b192.168.2.23 Njrat 87f7cbd6db62bdc55ddee57a106508a9 421ef5fb-9d57-5f23-261b-d51458356fa6 0a63ebf67461f81616851bf2407d3c5b2ce75647 65.1.1.2 e8e173b4eebae4a2bc2f49819e71349df373cf9ecd3b338ff6c28cc91632bb2bbalckanweb.comTrojan_Generic",
  "endpoint_hostname": null,
  "endpoint_username": null,
  "endpoint_id": ["192.168.2.23"],
  "source_email_id": null,
  "destination_email_id": [],
  "source_hostname": null,
  "source_id": "65.1.1.2",
  "source_username": null,
  "has_phishing": null,
  "has_download": "1",
  "threat_target": ["192.168.2.23"],
  "threat_source": "balckanweb.com",
  "collector_id_array": ["421ef5fb-9d57-5f23-261b-d51458356fa6"],
  "app_protocol_array": ["HTTP"]
},
{
  "session_timeout_sec" : 31536000,
  "status" : 0,
  "server_ip" : "10.2.9.43",
  "server_name" : "10.2.9.43",
  "max_cook_size" : 15000001,
  "status_fc_on" : 0,
  "status_sigeng_on" : 1,
  "status_hre_on" : 1,
  "status_sc_on" : 1,
  "status_correlation_on" : 1,
  "status_internet_on" : 1
}
```

```
, "status_mode" : 0
, "status_web_collector" : 1
}
```

Example: Third Party Ingestion Vendor

```
"third_party_info": {
  "device_host": "cbtest",
  "raw":
    "{ \"alert_severity\": \"67.5\", \"alert_type\": \"watchlist.hit.ingress.
process\", \"cb_server\": \"cbserver\", \"childproc_count\": \"0\", \"comm
s_ip\": \"10.7.1.205\", \"computer_name\": \"TEST-
2F0DDD7E5F\", \"created_time\": \"2017-05-
31T05:31:22.095903Z\", \"crossproc_count\": \"0\", \"feed_id\": \"4\", \"f
eed_name\": \"virustotal\", \"feed_rating\": \"3.0\", \"filemod_count\": \"
1\", \"group\": \"Default Group\", \"hostname\": \"TEST-
2F0DDD7E5F\", \"interface_ip\": \"0.0.0.0\", \"ioc_confidence\": \"0.5\",
\"ioc_type\": \"md5\", \"ioc_value\": \"7016a5d74459577060366f7d1e44f495
\", \"ioc_value_facet\": \"7016a5d74459577060366f7d1e44f495\", \"md5\": \"
7016A5D74459577060366F7D1E44F495\", \"modload_count\": \"56\", \"netcon
n_count\": \"0\", \"os_type\": \"windows\", \"process_guid\": \"00000006-
0000-0f08-01d2-d972777c31da\", \"process_id\": \"00000006-0000-0f08-
01d2-
d972777c31da\", \"process_name\": \"sup_games_notification_service.exe\
\", \"process_path\": \"c:\\\\documents and settings\\\\analyst\\\\local
settings\\\\application data\\\\sup
games\\\\sup_games_notification_service.exe\", \"regmod_count\": \"43\",
\"report_score\": \"100\", \"segment_id\": \"1\", \"sensor_criticality\":
\"3.0\", \"sensor_id\": \"6\", \"status\": \"Unresolved\", \"timestamp\":
1496208697.046, \"type\": \"alert.watchlist.hit.ingress.process\", \"uni
que_id\": \"5c02d994-f12f-4753-ad0d-
d0c4d3c17f30\", \"username\": \"SYSTEM\", \"watchlist_id\": \"7016a5d7445
9577060366f7d1e44f495\", \"watchlist_name\": \"7016a5d74459577060366f7d
1e44f495\" }",
  "severity": "high"
}
```

Example: Direct Ingestion from a Third Party Vendor

When the device_host is the source of the event, raw event data is ingested into Juniper ATP Appliance.

Example

```
curl 'https://10.2.25.24/admin/api.php?op=events' -H 'Host:
10.2.25.24' -H "Authorization:fb4f4fff2841a784fb21aa864af5e8fa" --
insecure | json_pp
```

It is possible to get events for a given hostname or IP address by passing these values in the request parameter, for example:

```
curl 'https://10.2.25.24/admin/api.php?op=events' -H 'Host:
10.2.25.24' -H "Authorization:fb4f4fff2841a784fb21aa864af5e8fa" --
data
'min_severity_value=0&normalize_names=0&has_endpoint_meta=true&get_al
l_events=false&get_lateral_and_phishing_as_events=true&endpoint_hostn
ame_value=TEST-2F0DDD7E5F' --insecure | json_pp
```

`min_severity_value` can be 0, 0.25, 0.5, 0.75 or 1.

`get_all_events`, when true, will get all the events from the time Juniper ATP Appliance is installed. It can be very slow depending on the size of data.

`get_lateral_and_phishing_as_events` can be true or false. If true, this will get the lateral events from the `endpoint_hostname_value` as events. If false, the lateral events are excluded in the response.

`endpoint_hostname_value` is the name of the host for which events are being fetched. It is case sensitive and should exactly match with the `host_name` of the real system.

NOTE You can also pass the IP address of the endpoint `local_ip_value` or `username_value` instead of `endpoint_hostname_value`.

event_details

Use the following “[event_details](#)” API to retrieve event details.

A new `event_details` API key is provided in the response: `custom_snort_event_details`.

The `event_details` API takes only an `event_id` as a parameter.

NOTE The “`events`” API returns a set of events matching the query parameters, whereas, currently, the “`event_details`” API returns the details of a specific event.

https://<HOST>/admin/api.php?op=event_details

An event can be one of several different types:

Types of events	Description
cnc	The event is a signature match on network traffic
email	The event is an email attachment.
exploit	The event is an HTTP exploit sequence.

fsp	The event is a lateral spread.
http	The event is an http download
upload	The event is a manual file upload, i.e. an appliance user uploaded a file for analysis.

HTTP Post Parameters	Description
event_id	[Required] The ID set for the incident during malware analysis. Get this id from the output of the API: <a href="https://<Host>/admin/api.php?op=events">https://<Host>/admin/api.php?op=events

Example

```
curl -k -H "Authorization:7c71c218662411a5c857042053acca8f" "https://10.1.1.1/admin/api.php?op=event_details" -d event_id=604
```

Authorization – The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

Sample output for this API is provided further below. Output field definitions are provided here. The general details are shared by each event type per these fields:

Output Field	Definition
app_protocol_array	HTTP or Email protocol instance, as in: "app_protocol_array": ["EMAIL"],
analysis_done_time	Timestamp for analysis engine detonation completion.
cnc_details	Details of a detected CnC event.
collector_id_array	The collector ID(s) associated with observing this event. A string enclosed in curly braces { }; as in: "collector_id_array": ["00000000-0000-0000-0000-000000000001"]
collector_name	Name of the collector that observed the event.
custom_snort_event_details	Details of the custom SNORT rule match.
destination_email_id	The destination email ID.
download_details	Details about a detected download.
endpoint_hostname	The hostname of the endpoint.
endpoint_id	The ID associated with the endpoint.
endpoint_ip	The IP address of the endpoint.
endpoint_name	The host name of the endpoint, if available.

endpoint_os_type	The endpoint OS type, if available.
endpoint_username	The username for the endpoint device.
event_category	The event category, for example Adware, Exploit, Trojan_Generic, etc.
event_id	The ID of this event
event_name	The event name, such as: "WORM.GAMARUE.CY"
event_severity	The severity of the event: 0 is benign, 1 is critical, 0.75 is high, 0.5 is medium.
event_type	Type of event: "exploit", "http", "email", "cnc", "submission" (for file submission).
exploit_details	Details of a detected exploit event.
file_md5_string	The MD5 checksum for the event, such as: "340c860492c5ee5f708dfee57f650cd3"
file_sha1_string	The SHA1 for the event, such as: "a0bd2ee698848dc40f41ce593c9668ccf7dd1993"
file_sha256_string	The SHA256 associated with the event, such as: "e482ea7bdbfd42dbf1c33cb0b4a57920f40e8ccba52a8ba57cf6191700fb6751"
file_size	The file size in bytes, such as: "55808"
file_type_string	The file type associated with the event, such as: "PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed"

file_submission_details	<p>The data associated with the file submission event, for example:</p> <pre> event_id: "604" submission_time_string: "2016-06-01 08:12:17.618365+00" local_path: "/var/spool/c-icap/download/CL_TMPoSYYjt" file_md5_string: "340c860492c5ee5f708dfee57f650cd3" file_sha1_string: "a0bd2ee698848dc40f41ce593c9668ccf7dd1993" file_sha256_string: "e482ea7bdbfd42dbf1c33cb0b4a57920f40e8ccba52a8ba57cf6191700fb 6751" file_size: "55808" file_type_string: "PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed" file_suffix: "exe" mime_type_string: "FILE_UPLOAD" has_components: null packer_name: "UPX" malware_name: "WORM_GAMARUE." malware_severity: "0.75" malware_category: "Trojan_Generic" malware_classname: "malware" has_static_detection: "1" has_behavioral_detection: "0" user_whitelisted: null JATP_whitelisted: null has_cnc: null dig_cert_name: null analysis_start_time: "2016-06-01 08:12:17.607846+00" analysis_done_time: "2016-06-01 08:12:46.504487+00" source_url_rank: "-1" reputation_score: "44" microsoft_name: "Worm:Win32/Gamarue.I" has_behavior_log: "1" file_meta: </pre>
file_suffix	The file suffix, such as: "exe"
has_download	Indication of a download event.
has_phishing	Indication of a phishing event: "1" = true, as in "has_phishing": "1"
http_details	Details of the HTTP detection.
incident_id	The incident id of the related incident if the event was not benign.
incident_risk	The risk of the related incident on the same scale as event_severity.
initial_done_time	Timestamp for completion of the heuristics-level analysis of the event; for example: 2016-06-31 09:45:28.670764+00
last_activity_time	The most recent time this event had any activity.
last_activity_epoch	The epoch ID for the event, such as: "1417421537.61837"

local_path	The path to the malware download.
mime_type_string	MIME type for the event, such as: "FILE_UPLOAD"
normalized_name	Normalized name that qualifies the event (for example: "Phishing").
phishing_details	Details of a detected phishing event.
search_data	A display of the search data for the event, such as: "a0bd2ee698848dc40f41ce593c9668ccf7dd1993 340c860492c5ee5f708dfef57f650cd3 Trojan_Generic e482ea7bdbfd42dbf1c33cb0b4a57920f40e8ccba52a8ba57cf6191700fb6 751 WORM_GAMARUE.CY"
source_country_code	The country code using a geoIP lookup of the threat source IP.
source_country_name	The country name using a geoIP lookup of the threat source IP.
source_email_id	The threat source email ID.
source_hostname	The threat source device hostname.
source_id	The ID for the threat source device.
source_ip	Threat source IP address.
source_name	The host name of the threat source IP address, if available.
source_username	The threat source device username.
submission_time_string	The date and time of the file upload for malware analysis.
threat_source	The threat source qualifier: "threat_source":"newcard.dyndns.biz"
threat_target	A string enclosed in square braces [], as in: "threat_target":"[10.1.1.26]"
user_ack_status	Status of the current user (for example: "new").

A Sample response for an HTTP download:

```
curl -k -H "Authorization:d5d0e4e71c9ab6d7bfa8fff4dab341a5" "https://
10.2.9.43/admin/api.php?op=event_details" -d event_id=506
```

```
{"event_details":{"event_id":"506","event_type":"http","event_category":
"Trojan_Generic","event_name":"Njrat","normalized_name":"Njrat","event_s
everity":"0.2","last_activity_time":"2016-06-03
08:35:01.462934+00","last_activity_epoch":"1464942901.46293","initial_do
ne_time":"2016-06-03 08:35:40.751017+00","analysis_done_time":"2016-06-
03
08:35:40.751017+00","endpoint_ip":"192.168.2.23","endpoint_name":"192.16
8.2.23","endpoint_os_type":"windows","source_ip":"65.1.1.2","source_name
":"balckanweb.com","source_country_code":"US","source_country_name":"USA
","incident_id":"237","incident_risk":"0.250","user_ack_status":"new","c
ollector_name":"shiva-ui-automation-galileo","search_data":"http:\\\\
balckanweb.com\\raghav\\dotnetfiles\\samples\\e\\
e8e173b4eebae4a2bc2f49819e71349df373cf9ecd3b338ff6c28cc91632bb2b
192.168.2.23 Njrat 87f7cbd6db62bdc55ddee57a106508a9 421ef5fb-9d57-5f23-
261b-d51458356fa6 0a63ebf67461f81616851bf2407d3c5b2ce75647 65.1.1.2
```

```
e8e173b4eebae4a2bc2f49819e71349df373cf9ecd3b338ff6c28cc91632bb2b
balckanweb.com
Trojan_Generic","endpoint_hostname":null,"endpoint_username":null,"endpo
int_id":["192.168.2.23"],"source_email_id":null,"destination_email_id":[
""],"source_hostname":null,"source_id":"65.1.1.2","source_username":null
,"has_phishing":null,"has_download":"1","threat_target":["192.168.2.23"]
,"threat_source":"balckanweb.com","collector_id_array":["421ef5fb-9d57-
5f23-261b-
d51458356fa6"],"app_protocol_array":["HTTP"],"http_details":{"event_id":
"506","has_execution":"0","app_protocol":"HTTP","capture_time_string":"2
016-06-03
08:35:01.462934+00","endpoint_id":"192.168.2.23","endpoint_ip":"192.168.
2.23","endpoint_name":"192.168.2.23","endpoint_hostname":null,"source_id
":"65.1.1.2","source_ip":"65.1.1.2","source_name":"balckanweb.com","sour
ce_hostname":null,"source_url":"http://balckanweb.com/raghav\
dotnetfiles\samples\e\
e8e173b4eebae4a2bc2f49819e71349df373cf9ecd3b338ff6c28cc91632bb2b","clien
t_os":"windows","appliance_id":"421ef5fb-9d57-5f23-261b-
d51458356fa6","source_email_id":null,"destination_email_id":null,"req_he
aders":{"host":"balckanweb.com","connection":"Keep-Alive","accept":"*/
*","user-agent":"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:25.0)
Gecko/20100101 Firefox\
25.0"},"req_referer":null,"country_code":"us","country_name":"USA","sha1
sum":"0a63ebf67461f81616851bf2407d3c5b2ce75647","md5sum":"87f7cbd6db62bd
c55ddee57a106508a9","sha256sum":"e8e173b4eebae4a2bc2f49819e71349df373cf9
ecd3b338ff6c28cc91632bb2b","file_type":"PE32 executable (GUI) Intel
80386 Mono\/.Net assembly, for MS Windows","local_path":"/var/spool\
c-icap/download\
CI_TMP9iFhM9","file_md5_string":"87f7cbd6db62bdc55ddee57a106508a9","file
_sha1_string":"0a63ebf67461f81616851bf2407d3c5b2ce75647","file_sha256_st
ring":"e8e173b4eebae4a2bc2f49819e71349df373cf9ecd3b338ff6c28cc91632bb2b"
,"file_size":"9867264","file_type_string":"PE32 executable (GUI) Intel
80386 Mono\/.Net assembly, for MS
Windows","file_suffix":"exe","mime_type_string":"N\
A","has_components":null,"packer_name":null,"malware_name":"Njrat","malw
are_severity":"0.2","malware_category":"Trojan_Generic","malware_classna
me":"malware","malware_confidence":"1.0","has_static_detection":"1","has
_behavioral_detection":"1","has_reputation_detection":null,"has_embedded
_code":null,"has_cnc":null,"dig_cert_name":null,"dig_cert_override":null
,"has_yara_match":"1","pcap_size":"283","analysis_start_time":"2016-06-
03 08:35:02.150144+00","analysis_done_time":"2016-06-03
08:35:40.608563+00","source_url_rank":"-
1","reputation_score":"0","has_behavior_log":"1","user_agent":"windows",
"custom_image_array":[],"yara_rule_array":[{"rule_file_name":"Njrat.yar"
,"scan_time":"2016-06-03
01:35:09.519801","rule_name":"Njrat","rule_severity":"0.2","rule_descrip
tion":"Njrat","is_customer_rule":"0"}]},"download_details":{"event_id":
"506","has_execution":"0","app_protocol":"HTTP","capture_time_string":"20
16-06-03
08:35:01.462934+00","endpoint_id":"192.168.2.23","endpoint_ip":"192.168.
2.23","endpoint_name":"192.168.2.23","endpoint_hostname":null,"source_id
":"65.1.1.2","source_ip":"65.1.1.2","source_name":"balckanweb.com","sour
ce_hostname":null,"source_url":"http://balckanweb.com/raghav\
dotnetfiles\samples\e\
```

```
e8e173b4eebae4a2bc2f49819e71349df373cf9ecd3b338ff6c28cc91632bb2b","client_os":"windows","appliance_id":"421ef5fb-9d57-5f23-261b-d51458356fa6","source_email_id":null,"destination_email_id":null,"req_headers":{"host":"balckanweb.com","connection":"Keep-Alive","accept":"*/","user-agent":"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:25.0) Gecko/20100101 Firefox/25.0"},"req_referer":null,"country_code":"us","country_name":"USA","sha1sum":"0a63ebf67461f81616851bf2407d3c5b2ce75647","md5sum":"87f7cbd6db62bdc55ddee57a106508a9","sha256sum":"e8e173b4eebae4a2bc2f49819e71349df373cf9ecd3b338ff6c28cc91632bb2b","file_type":"PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows","local_path":"\\var\\spool\\c-icap\\download\\CI_TMP9iFhM9","file_md5_string":"87f7cbd6db62bdc55ddee57a106508a9","file_shal_string":"0a63ebf67461f81616851bf2407d3c5b2ce75647","file_sha256_string":"e8e173b4eebae4a2bc2f49819e71349df373cf9ecd3b338ff6c28cc91632bb2b","file_size":"9867264","file_type_string":"PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows","file_suffix":"exe","mime_type_string":"N/A","has_components":null,"packer_name":null,"malware_name":"Njrat","malware_severity":"0.2","malware_category":"Trojan_Generic","malware_classname":"malware","malware_confidence":"1.0","has_static_detection":"1","has_behavioral_detection":"1","has_reputation_detection":null,"has_embedded_code":null,"has_cnc":null,"dig_cert_name":null,"dig_cert_override":null,"has_yara_match":"1","pcap_size":"283","analysis_start_time":"2016-06-03 08:35:02.150144+00","analysis_done_time":"2016-06-03 08:35:40.608563+00","source_url_rank":"-1","reputation_score":"0","has_behavior_log":"1","user_agent":"windows","custom_image_array":[],"yara_rule_array":[{"rule_file_name":"Njrat.yar","scan_time":"2016-06-03 01:35:09.519801","rule_name":"Njrat","rule_severity":"0.2","rule_description":"Njrat","is_customer_rule":"0"}],"screen_shots":["\\analysis\\185\\cooker-results\\win7-winapi\\screenshots\\screenshot_00.jpg","\\analysis\\185\\cooker-results\\win7-winapi\\screenshots\\screenshot_01.jpg","\\analysis\\185\\cooker-results\\win7-winapi\\screenshots\\screenshot_02.jpg"]},"status":0}
```

NOTE The specific details for each event change for each event type and are contained in the sub-object download_details, cnc_details, exploit_details, etc. of the event_details object.

A Sample Response for Phishing:

```
curl -k -H "Authorization:d5d0e4e71c9ab6d7bfa8fff4dab341a5" "https://10.2.9.43/admin/api.php?op=event_details" -d event_id=504

{"event_details":{"event_id":"504","event_type":"email","event_category":null,"event_name":"Phishing","normalized_name":"Phishing","event_severity":"0.75","last_activity_time":"2016-06-03 06:33:39+00","last_activity_epoch":"1464935619","initial_done_time":"2016-06-03 06:33:50.126422+00","analysis_done_time":"2016-06-03 06:37:59.299276+00","endpoint_ip":null,"endpoint_name":null,"endpoint_os_type":null,"source_ip":null,"source_name":null,"source_country_code":null}}
```

```
11,"source_country_name":null,"incident_id":"234","incident_risk":"0.750",
,"user_ack_status":"new","collector_name":null,"search_data":"http:\\\\
greatfilesarey.asia\\QA\\files_to_pcaps\\
79ea1163c0844a2d2b6884a31fc32cc4.bin xyz@gmail.com
abc@gmail.com","endpoint_hostname":null,"endpoint_username":null,"endpoi
nt_id":["abc@gmail.com"],"source_email_id":"xyz@gmail.com","destination_
email_id":["abc@gmail.com"],"source_hostname":null,"source_id":"xyz@gmai
l.com","source_username":null,"has_phishing":"1","has_download":"0","thr
eat_target":["abc@gmail.com"],"threat_source":"xyz@gmail.com","collector
_id_array":["00000000-0000-0000-0000-
000000000001"],"app_protocol_array":["EMAIL"],"phishing_details":{"metad
ata_array":[{"email_msg_id":"CAK9CQGddX3LL-
2oFNWHZUM1cncqoSasKbH3npeLJEe9LXGnGmQ@mail.gmail.com","destination_email
_id":["abc@gmail.com"],"source_email_id":"xyz@gmail.com","email_recv_tim
e":"2016-06-03
06:33:39+00","event_id":"504","event_severity":"0.75","url_array":[{"url
":"http:\\\\greatfilesarey.asia\\QA\\files_to_pcaps\\
79ea1163c0844a2d2b6884a31fc32cc4.bin","url_severity":"0.75","description
":"Downloads Sha1:
acf69d292d2928c5ddfe5e6af562cd482e6812dc"}]}]}},{"status":0}
```

A sample response for custom snort event details:

```
{
  "custom_snort_event_details": {
    "collector" : "4C4C4544-0036-3010-8036-C3C04F465831",
    "create_time": "2016-04-07 07:26:06.76+00",
    "data_payload" :
    "474554202F51412F66696C65735F746F5F70636170732F2F37396561313136336330
383434613264326236383834613331666333326363342E62696E20485454502F312E3
10D0A557365722D4167656E743A204D6F7A696C6C612F352E30202857696E646F7773
204E5420362E323B2057696E36343B2078363429204170706C655765624B69742F353
3372E333620284B48544D4C2C206C696B65204765636B6F29204368726F6D652F3332
2E302E313636372E30205361666172692F3533372E33360D0A4163636570743A202A2
F2A0D0A486F73743A20677265617466696C6573617265792E617369610D0A436F6E6E
656374696F6E3A204B6565702D416C6976650D0A0D0A",
    "description": "Alert 3 ",
    "signature": "alert tcp 10.1.1.26 any -> 172.16.0.14 80
(msgs:\\\"Alert 3\\\"; classtype: web-application-activity;
reference:url,http://www.junk.com/no.html; sid:5500004; rev:1; )",
    "severity": "0.0",
    "source": "10.1.1.26",
    "destination": "172.16.0.14",
    "threat_source" : "172.16.0.14",
    "threat_target" : "{10.1.1.26}"
  }
}
```

file_submit

Use this API function to submit a file to the Juniper ATP Appliance threat detection system for analysis.

The API format for file submission is as follows:

https://<HOST>/admin/cgi-bin/file_submit

The file_submit API returns the event_id; use to event_details API to get the malware analysis results for the submitted file. "File Upload" (from the Central Manager Incidents page) is the Web UI equivalent of the file_submit API.

This API requires a form data "file" designation that specifies the file to be submitted. In addition, the user may submit an optional form data segment named "file_meta_json" as the meta to the submitted file. The JSON string "file_meta_json" as shown below:

HTTP Post Parameters	Description
file_meta_json	Name of the file to be submitted for analysis. The simple key value pair data when sent will show on the File Uploads tab in the Central Manager.
file	[Required] Path of the file to be submitted for analysis.

Following a successful file submission, an HTTP 200 response is returned. The content of the response is a JSON string containing the status code 0, the event id of the file submission, and the SHA1 sum of the submitted file. Various HTTP codes are returned for different error cases. The content of the response is a JSON string that includes the status code -1 and the reason for the failure with details.

NOTE Be aware that in the example below that the "file" and "file_meta_json" fields are required form names (the file_meta_json field is required when you want to specify a name for the file when it appears in the analysis results), and the red highlighted text below in the Example ("file_name": "customer_file1") calls out the required key:value pair in the meta.

The designator "fada509542437360aeaa73a6256a9f1c88764e823f0f0a6a78fb66e419b5f389" is the name of the malware file used for testing.

The file_meta_json is recently enhanced; when all required endpoint metadata is available to process, the incident is shown in the Central Manager Incident tab.

Metadata JSON Structure

```
{
  "file_name": "<fileName>",
  "comment": "<free text for future use>",
  "file_capture_time": <epoch time>,
  threat_target_data: {
    "endpoint_ip": null,
```

```
        "endpoint_hostname":null,
        "endpoint_os_type":null,
        "endpoint_username":null,
    }
    "threat_source_data": {
        "source_ip":null,
        "source_hostname":null,
        "source_username":null,
        "source_uri": null
    }
}
```

NOTE File submissions that include an endpoint IP address or endpoint hostname can be correlated with other file submissions or malicious events that originated from the same endpoint IP address or endpoint hostname. These file submissions are displayed on the Central Manager Web UI Incidents tab. File submissions that do not include an endpoint IP address or endpoint hostname are displayed on the File Uploads tab.

Additionally, the file upload username is persistent and derived from the session data.

Examples

- Example 1 Uploading a file using CURL without end point and source metadata
- Example 2: Uploading a file with source and destination endpoint data

Example 1 Uploading a file using CURL without end point and source metadata

```
curl -k -H "Authorization:7c71c218662411a5c857042053acca8f" -F
file=@fada509542437360aeaa73a6256a9f1c88764e823f0f0a6a78fb66e419b5f38
9
-F file_meta_json='{ "file_name": "customer_file1" }'
"https://10.2.20.37/admin/cgi-bin/file_submit"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

```
curl "https://10.2.25.56/admin/cgibin/ file_submit.py" -insecure -H
"Authorization:99de8c2290eaf126054f126c2ce18708" -F file="@/tmp/
f34922f0cdf5160f389c73f3ec99f5693ccb0fee3039187020da8a89d7d7fcd5" F
file_meta_json='{ "file_name": "f34922f0cdf5160f389c73f3ec99f5693ccb0fe
e3039187020da8a89d7d7fcd5" } '
```

The analysis result will be returned to the Central Manager Web UI File Upload tab because there is no source and end point data.

Sample Output

```
{ "status": 0, "detail": { "event_id": 672, "shasum":
"1f707b2fe77691ee91aa5da0a326aec40182bb0d" } }
```

Example 2: Uploading a file with source and destination endpoint data

NOTE Refer to [Metadata JSON Structure](#) section for more information.

```
curl "https://10.2.25.56/admin/cgibin/file_submit.py" -insecure -H
"Authorization:99de8c2290eaf126054f126c2ce18708" -F file="@/tmp/
f34922f0cdf5160f389c73f3ec99f5693ccb0fee3039187020da8a89d7d7fcd5" -F
file_meta_json='{ "file_name": "f34922f0cdf5160f389c73f3ec99f5693ccb0fe
e3039187020da8a89d7d7fcd5", "file_capture_time": 1471683137, "threat_tar
get_data": { "endpoint_ip": "10.1.1.10", "endpoint_hostname": "labpc", "end
point_os_type": "windows", "endpoint_username": "testuser" }, "threat_sour
ce_data": { "source_ip": "3.23.31.3", "source_hostname": "rogue_interneth
ost", "source_uri": " www.rogue_internethost.com/index.html " } }'
```

The formatted JSON for this example is shown below:

```
{
  "file_name": "f34922f0cdf5160f389c73f3ec99f5693ccb0fee3039187
{20da8a89d7d7fcd5",
  "file_capture_time": 1471683137,
  "threat_target_data": {
    "endpoint_ip": "10.1.1.10",
    "endpoint_hostname": "labpc",
    "endpoint_os_type": "windows",
    "endpoint_username": "testuser"
  },
  "threat_source_data": {
    "source_ip": "3.23.31.3",
    "source_hostname": "rogue_internethost",
    "source_uri": "www.rogue_internethost.com/index.html"
  }
}
```

The `file_capture_time` is epoch time. (Optional): Convert human readable time to epoch and vice versa at <http://www.epochconverter.com/> If specified, this will be treated as the file capture time. The `endpoint_os_type` might be "windows" for windows hosts and "macos" for OSX; these are optional as well, as are `endpoint_hostname` and `source_hostname` are optional. Because endpoint data is present, the analysis result is provided in the Incident tab, not the File Upload tab. Depending on whether the file is benign or malware, the analysis will appear as Threat, Suspicious or Benign in the Incident table.

Example 3: Uploading a file with source and destination email IDs

```
curl "https://10.2.25.56/admin/cgibin/file_submit.py" -insecure -H
"Authorization:99de8c2290eaf126054f126c2ce18708" -F file="@/tmp/
problem_pcap1.pcap" -F
file_meta_json='{"file_name":"problem_pcap","file_capture_time":14716
83137,"threat_target_data":{"destination_email_id":[" user1@JATP.net
","user2@JATP.net"]},"threat_source_data":{"source_email_id":"interne
tuser@JATP.net"}}'
```

There is no change in the response format for this file upload API example from previous releases. A successful fileupload returns the following JSON:

```
{"status": 0, "detail": {"event_id": 1135, "shasum":
"feb6e1615d0b61f6f40c487ca3154f368b0041c3"}}
```

The non zero status indicates failure.

Retrieving the submitted file analysis results

Now use the event_details API to get the result of the submitted file.

```
curl -k -H "Authorization:7c71c218662411a5c857042053acca8f" "https://
10.2.20.37/admin/api.php?op=event_details" -d event_id=672
```

Note that the returned JSON matches the existing events API except that only data specific to file upload is returned. The user who uploaded the file is also returned. Files are displayed that are still being analyzed because the API returns all the events without the status finalized.

```
{
  event_details:
  {
    event_id: "672"
    event_type: "submission"
    event_category: "Trojan_Generic"
    event_name: "TROJAN_YAKES.CY"
    event_severity: "0.75"
    last_activity_time: "2016-06-02 09:03:11.008311+00"
    last_activity_epoch: "1417510991.00831"
    analysis_done_time: "2016-06-02 09:03:11.072094+00"
    endpoint_ip: null
    endpoint_name: null
    endpoint_os_type: null
  }
}
```



```
source_ip: null
source_name: "User Uploaded"
source_country_code: null
source_country_name: null
incident_id: "205"
incident_risk: "0.75000000000000000000"
collector_id: "00000000-0000-0000-0000-000000000002"
search_data: "1f707b2fe77691ee91aa5da0a326aec40182bb0d
TROJAN_YAKES.CY Trojan_Generic
fada509542437360aeaa73a6256a9f1c88764e823f0f0a6a78f
b66e419b5f389 7be866d691c3da79f51240bf8963e210"
file_submission_details:
{
    event_id: "672"
    submission_time_string: "2016-06-02
09:03:11.008311+00"
    local_path: "/var/spool/c-icap/download/CI_TMPFP9jYz"
    file_md5_string: "7be866d691c3da79f51240bf8963e210"
    file_sha1_string:
"1f707b2fe77691ee91aa5da0a326aec40182bb0d"
    file_sha256_string:
"fada509542437360aeaa73a6256a9f1c887
64e823f0f0a6a78fb66e419b5f389"
    file_size: "893977"
    file_type_string: "PE32 executable (GUI) Intel 80386,
for MS Windows"
    file_suffix: "exe"
    mime_type_string: "FILE_UPLOAD"
    has_components: null
    packer_name: null
    malware_name: "TROJAN_YAKES.CY"
    malware_severity: "0.75"
    malware_category: "Trojan_Generic"
    malware_classname: "malware"
    has_static_detection: "1"
    has_behavioral_detection: "0"
    user_whitelisted: null
    JATP_whitelisted: null
    has_cnc: null
```

```
        dig_cert_name: null
        analysis_start_time: "2016-06-02 08:34:40.513488+00"
        analysis_done_time: "2016-06-02 08:35:03.877626+00"
        source_url_rank: "-1"
        reputation_score: "35"
        microsoft_name: "None"
        has_behavior_log: "1"
        file_meta:
        {
            file_name: "customer_file1"
        }
    }
    status: 0}
```

NOTE All file uploads performed by integrations such as Carbon Black/Bit9 are returned with available metadata in the Incident tab's Incident table.

`get_auto_mitigation_settings`

This API retrieves configured auto-mitigation settings.

https://HOST/admin/api.php?op=get_auto_mitigation_settings

Example

```
curl 'https://10.1.1.1/admin/api.php?op=get_auto_mitigation_settings'
-H 'Host: 10.1.1.1' -H
"Authorization:ae5bab7c3a2241a89a435d3671e29f92"
```

See Also: [set auto mitigation settings on page 169](#).

`get_blocked_emails_ex`

Use this API to retrieve all blocked emails.

The API for retrieving all blocked emails is shown as follows:

https://HOST/admin/api.php?op=get_blocked_emails_ex

Example

```
curl 'https://10.1.1.1/admin/api.php?op=get_blocked_emails_ex' -H
'Host: 10.1.1.1' -H "Authorization:ae5bab7c3a2241a89a435d3671e29f92"
```

get_blocked_ips_ex

Use this API to retrieve all the mitigation rules and their status for firewalls. This API replaces “get_blocked_ips” in the previous release.

The API for retrieving blocked IPS rules and status is shown as follows:

https://HOST/admin/api.php?op=get_blocked_ips_ex

Example

```
curl "https://10.2.20.84/admin/api.php?op=get_blocked_ips_ex" -H
"Host: 10.2.20.84" -H "Authorization:54c20d76c5fcff62cccf2208b45712be
--insecure"
```

The returned JSON is an array in the following format:

HTTP Post Parameters	Description
threat_actor	An attacker's IP address.
confidence	The mitigation rule confidence determination. The values range from 0 to 1. Automatic mitigation is based on the confidence score, and can be set from the Central Manager Config > System Settings page under "Auto Mitigation Settings."
threat_source	Source information created as a result of an incident, or created by Juniper ATP Appliance ATA.
event_array	A set of individual events derived from incidents, including their details as a JSON dictionary.

The following attributes report the action taken by Juniper ATP Appliance for mitigation. These actions are used by the Juniper ATP Appliance Central Manager to provide status:

Mitigation Attributes	Description
push_to_device	Shows whether the rule is required to be pushed to the configured firewall device.
who	Shows who created the rule; USER is displayed if the incident created the attribute; Juniper ATP is displayed if the incident is created by the Juniper ATP Appliance as part of ATA.
limit	A 'limit' is shown as 't' if and only if the threat has been "limited", for example, the threat should be pushed based on the threat's confidence, but the number of threats to be pushed exceeds the configured threat capacity of the device, and so this threat has been held back ("limited"). A "limit" is shown as 'f' if it has not been limited. The limits for the number of auto mitigation rules configured is defined in Config > System Settings under Auto Mitigation Settings.

Sample Output

```
{
  "threat_actor": "115.47.49.181",
  "push_to_device": "f",
  "who": "USER",
  "confidence": "0.75",
  "severity": "1.0",
  "threat_source": "Local",
  "limit": "f",
  "event_array": [
    {
      "event_id": "25367",
      "confidence": "0.5",
      "endpoint_ip": "10.1.1.44",
      "malware_name": "TROJAN_FAREIT.CY",
      "last_seen": "2016-11-03 12:15:37.134+00",
      "collector_id": "421ea7c0-029c-4907-e4c0-51741936b882",
      "threat_target": "switch-44.corp.JATP.net."
    },
    {
      "event_id": "25368",
      "confidence": "0.75",
      "endpoint_ip": "10.1.1.44",
      "malware_name": "TROJAN_Fareit.CY",
      "last_seen": "2016-11-03 12:15:37.138+00",
      "collector_id": "421ea7c0-029c-4907-e4c0-51741936b882",
      "threat_target": "switch-44.corp.JATP.net."
    }
  ]
},
{
  "threat_actor": "23.254.165.61",
  "push_to_device": "f",
  "who": "JATP",
  "confidence": "1",
  "severity": "0.65",
  "threat_source": "JATP ATA",
  "limit": "f"
}
```

get_blocked_signatures

Use this API to obtain a list of blocked signatures.

The API for getting blocked signatures is as follows (there are no required parameters):

https://HOST/admin/api.php?op=get_blocked_signatures

Example

```
curl "https://10.2.20.84/admin/api.php?op=get_blocked_signatures"
```

Sample Output

```
{
  "blocked_signature_array": [
    {
      "malware_name": "TROJAN_Malex.CY",
      "event_id": "25",
      "endpoint_ip": "10.1.1.56",
      "endpoint_name": "switch-56.corp.JATP.net.",
      "last_seen": "2016-06-16 07:14:34.264+00",
      "snort_sid": "2803971",
      "snort_group_id": "983",
      "collector_id": "00000000-0000-0000-0000-000000000000"
    },
    {
      "malware_name": "TROJAN_Gippers.CY",
      "event_id": "26",
      "endpoint_ip": "10.1.1.54",
      "endpoint_name": "switch-54.corp.JATP.net.",
      "last_seen": "2016-06-16 07:17:35.003+00",
      "snort_sid": "2805993",
      "snort_group_id": "3019",
      "collector_id": "00000000-0000-0000-0000-000000000000"
    }
  ],
  "session_timeout_sec": 900,
  "status": 0
}
```

get_blocked_urls_ex

Use this API to obtain a list of the mitigation rules applicable to web gateways; this replaces the “get_blocked_url” available from a previous release.

The API for getting blocked gateway rules data is as follows:

https://HOST/admin/api.php?op=get_blocked_urls_ex

Example

```
curl "https://10.1.1.1/admin/api.php?op=get_blocked_urls_ex" -H
"Host: 10.1.1.1" -H "Authorization:54c20d76c5fcff62cccf2208b45712be"
--insecure
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

HTTP Post Parameters	Description
threat_actor	The returned value "threat_actor" is a regular expression of URL, URI or the URL itself.
limit	A "limit" is returned as "t" for true or "f" for false; "f" indicates also that the limit it is less than "Max URL Threats" configured at the Central Manager Config>System Settings page.

Sample Output

```
{
  "threat_actor": ".*clickpapa.com/*",
  "push_to_device": "f",
  "who": "JATP",
  "confidence": "1",
  "severity": "0.65",
  "threat_source": "JATP ATA",
  "limit": "f"
},
{
  "threat_actor": ".*exoclick.com/*",
  "push_to_device": "f",
  "who": "JATP",
  "confidence": "1",
  "severity": "0.65",
  "threat_source": "JATP ATA",
  "limit": "f"
},
{
  "threat_actor": "http://die-tradlers.de/malware_vault/malware/newton_qa/file_samples/malware_msoffice/99b87945f1ecb646b517f64fb8c3ff4826fcelc7",
  "push_to_device": "f",
  "who": "JATP",
  "confidence": "1.0",
  "severity": "0.25",
  "threat_source": "Local",
  "limit": "f",
  "event_array": [
    {
      "confidence": "1.0",
      "event_id": "25478",
      "endpoint_ip": "172.17.1.128",
      "threat_target": "172.17.1.128",
      "malware_name": "Suspicious.DC",
      "last_seen": "2016-11-03 12:16:05.407351+00",
```

```

        "collector_id": "421ea7c0-029c-4907-e4c0-51741936b882"
    }
]
}

```

get_iocs

Use this API to retrieve Indicators of Compromise (IoCs) in STIX format.

Structured Threat Information Expression (STIX™) is a language used to qualify cyber threat data and intel so it can be exchanged, stored, and analyzed. The “get_iocs” API allows users to query Juniper ATP Appliance to obtain Indicators of Compromise (IoC) in a standard STIX format.

The API for returning IoCs is as follows:

https://HOST/admin/api.php?op=get_iocs

Examples

```
curl -k -H "Authorization: 24cec5e4d9e117f6737f82582a3eeff0" -d
"max_results=500&end_time_sec=1438713859&interval_sec=2592000" -X
POST "https://10.2.20.78/admin/api.php?op=get_iocs"
```

```
curl -k -H "Authorization: 24cec5e4d9e117f6737f82582a3eeff0" -d
"event_id=12345" -X POST "https://10.2.20.78/admin/
api.php?op=get_iocs"
```

HTTP Post Parameters	Description
max_results	The maximum number of indicators that the API will return. A default number of 500 maximum is applied if “max_results” is unspecified.
end_time_sec	The end of the time range for which the indicators are selected. The current time is used if “end_time_sec” is unspecified.
interval_sec	The length of the time range for which the indicators are selected. A default of 24 hours is applied if “interval_sec” is unspecified.
begin_time_sec	The beginning of the time range for which the indicators are selected. The argument “end_time_sec” and “interval_sec” are used if “begin_time_sec” is unspecified. Note that “begin_time_sec” overrides “interval_sec” if both arguments are present in the request.
event_id	The event ID relative to all returned indicators of compromise. All other arguments are ignored if “event_id” is provided in the API request.
NOTE Querying large datasets can require a long response time; see the Tip provided on the following page for optional query management strategies.	

IoC Filtering

Filtering IoCs with the “get_iocs” API can be implemented in either of two ways:

1. Time based Filtering

As indicated in the HTTP POST Parameters table above, time-based filtering can be implemented by pairing the arguments “beginning_time_sec” and “end_time_sec,” or by pairing “end_time_sec” and “interval_sec,” in order to specify the time range of IoCs you would like to receive.

2. Event ID based Filtering

Another filtering option is event_id filtering; specify the “event_id” argument in the request and the response will only contain IoCs that are related to that particular event, regardless of the time that the event took place.

NOTE The get_iocs API generates a response based on events with a severity of > 0 and are not whitelisted.

Query the API by specifying the time range and the maximum number of indicators to be fetched. The time range can be of arbitrary size. You can choose to fetch on any intervals as long as the joint of all intervals covers the entire timeline. Any overlap in the results of different queries can be identified by the event ID embedded in the indicators.

TIP The STIX API query might take a long time to generate the response result against very large data-base. The default “max_results” parameter is 500 indicators and the default time range is 24 hours. But you can increase and decrease those arguments as necessary. It is a good practice to specify your time range at a relatively small interval so that the total number of returned indicators is small. Then repeat the request with a sliding window to eventually retrieve all indicators.

It is possible to request a maximum number of indicators that is smaller than the actual number of indicators within a specified time range. An error message will be returned displaying the actual number of indicators so that the set can be adjusted accordingly. The API will not select the requested number of indicators.

NOTE Indicators may get updated when an event is updated due to rescan. Within the results of multiple queries, indicators with recent timestamp are preferred unless a complete history is required. The event ID in the indicator can be used to replace an outdated result on the client side.

Sample Responses

Sample responses for the “get_iocs” API are provided below for the following categories:

- [HTTP without IVP on page 93 \(below\)](#)
- [HTTP with IVP on page 95](#)
- [Submission with IVP on page 98](#)
- [Submission Zip on page 102](#)
- [Email without IVP on page 105](#)
- [Email with IVP on page 107](#)
- [CnC on page 111](#)
- [Exploit on page 112](#)

NOTE For more information about STIX indicators, refer to [Sample STIX Data on page 114](#).

Sample Response for get_jocs

HTTP without IVP

```

<JATP:JATP_Package xmlns:JATP="www.JATP.net" version="1.0">
  <JATP:JATP_Header>
    <JATP:Title>JATP Indicators</JATP:Title>
    <JATP:Description>JATP Indicators 1 of 4810, last indicator time 2016-
06-11 14:48:23.716894-07:00</JATP:Description>
  </JATP:JATP_Header>
  <stix:STIX_Package xmlns:AddressObj="http://atpbox.mitre.org/
objects#AddressObject-2" xmlns:FileObj="http://atpbox.mitre.org/
objects#FileObject-2" xmlns:NetworkConnectionObj="http://
JATPbox.mitre.org/objects#NetworkConnectionObject-2"
xmlns:SocketAddressObj="http://atpbox.mitre.org/
objects#SocketAddressObject-1" xmlns:URIObj="http://atpbox.mitre.org/
objects#URIObject-2" xmlns:atpbox="http://atpbox.mitre.org/JATPbox-2"
xmlns:atpboxCommon="http://atpbox.mitre.org/common-2"
xmlns:atpboxVocabs="http://atpbox.mitre.org/default_vocabularies-2"
xmlns:JATP="http://JATP.net" xmlns:indicator="http://stix.mitre.org/
Indicator-2" xmlns:stix="http://stix.mitre.org/stix-1"
xmlns:stixCommon="http://stix.mitre.org/common-1"
xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="1.2">
<stix:Indicators>
  <stix:Indicator id="e16914-s14522" timestamp="2016-06-
11T14:48:23.716894-07:00" xsi:type="indicator:IndicatorType">
    <indicator:Title>Common indicator for event 16914</indicator:Title>
    <indicator:Description>Context of the threat activities. Event type:
http. Event category: Trojan_Generic. Event name: WORM_DORKBOT.CY.</
indicator:Description>
    <indicator:Observable>
      <JATPbox:Observable_Composition operator="AND">
        <JATPbox:Observable>
          <JATPbox:Object>
            <JATPbox:Properties
xsi:type="NetworkConnectionObj:NetworkConnectionObjectType">
              <NetworkConnectionObj:Source_Socket_Address
xsi:type="SocketAddressObj:SocketAddressObjectType">
                <SocketAddressObj:IP_Address
xsi:type="AddressObj:AddressObjectType">
                  <AddressObj:Address_Value
condition="Equals">172.16.0.2</AddressObj:Address_Value>
                </SocketAddressObj:IP_Address>
              </NetworkConnectionObj:Source_Socket_Address>
              <NetworkConnectionObj:Destination_Socket_Address
xsi:type="SocketAddressObj:SocketAddressObjectType">
                <SocketAddressObj:IP_Address
xsi:type="AddressObj:AddressObjectType">
                  <AddressObj:Address_Value
condition="Equals">172.16.0.1</AddressObj:Address_Value>

```

```
        </SocketAddressObj:IP_Address>
        </NetworkConnectionObj:Destination_Socket_Address>
    </JATPbox:Properties>
</JATPbox:Object>
</JATPbox:Observable>
<JATPbox:Observable>
    <JATPbox:Object>
        <JATPbox:Properties xsi:type="URIObj:URIObjectType">
            <URIObj:Value>greatfilesarey.asia</URIObj:Value>
        </JATPbox:Properties>
    </JATPbox:Object>
</JATPbox:Observable>
<JATPbox:Observable>
    <JATPbox:Object>
        <JATPbox:Properties xsi:type="URIObj:URIObjectType">
            <URIObj:Value>172.16.0.2</URIObj:Value>
        </JATPbox:Properties>
    </JATPbox:Object>
</JATPbox:Observable>
</JATPbox:Observable_Composition>
</indicator:Observable>
<indicator:Related_Indicators>
    <indicator:Related_Indicator>
        <stixCommon:Indicator id="s14522" timestamp="2016-06-
25T21:23:14.083690+00:00" xsi:type="indicator:IndicatorType">
            <indicator:Title>File indicator for storage object 14522</
indicator:Title>
            <indicator:Observable>
                <JATPbox:Object>
                    <JATPbox:Properties xsi:type="FileObj:FileObjectType">
                        <FileObj:Hashes>
                            <JATPboxCommon:Hash>
                                <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">SHA256</JATPboxCommon:Type>

                                <JATPboxCommon:Simple_Hash_Value>0f2b176ed787c286cb7708f2fb62328cfd0874e
3ac7a79afcc9369bc612a4556</JATPboxCommon:Simple_Hash_Value>
                            </JATPboxCommon:Hash>
                            <JATPboxCommon:Hash>
                                <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">SHA1</JATPboxCommon:Type>

                                <JATPboxCommon:Simple_Hash_Value>0cc656bf166343ff07b346bf2ae6d5983067cd1
7</JATPboxCommon:Simple_Hash_Value>
                            </JATPboxCommon:Hash>
                            <JATPboxCommon:Hash>
                                <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">MD5</JATPboxCommon:Type>

                                <JATPboxCommon:Simple_Hash_Value>2d8d9a261c4673a9965b78817911a1fd</
```

```

JATPboxCommon:Simple_Hash_Value>
    </JATPboxCommon:Hash>
  </FileObj:Hashes>
</JATPbox:Properties>
</JATPbox:Object>
</indicator:Observable>
</stixCommon:Indicator>
</indicator:Related_Indicator>
</indicator:Related_Indicators>
</stix:Indicator>

```

Sample Response for get_jocs

HTTP with IVP

```

<JATP:JATP_Package xmlns:JATP="http://www.JATP.net" version="1.0">
  <JATP:JATP_Header>
    <JATP:Title>JATP Indicators</JATP:Title>
    <JATP:Description>JATP Indicators 1 of 4810, last indicator time 2016-
06-04 16:00:54.135901-07:00</JATP:Description>
  </JATP:JATP_Header>
  <stix:STIX_Package xmlns:AddressObj="http://atpbox.mitre.org/
objects#AddressObject-2" xmlns:FileObj="http://atpbox.mitre.org/
objects#FileObject-2" xmlns:NetworkConnectionObj="http://
atpbox.mitre.org/objects#NetworkConnectionObject-2"
xmlns:SocketAddressObj="http://atpbox.mitre.org/
objects#SocketAddressObject-1" xmlns:URIObj="http://atpbox.mitre.org/
objects#URIObject-2" xmlns:atpbox="http://atpbox.mitre.org/JATPbox-2"
xmlns:JATPboxCommon="http://atpbox.mitre.org/common-2"
xmlns:JATPboxVocabs="http://atpbox.mitre.org/default_vocabularies-2"
xmlns:JATP="http://atpphort.com" xmlns:indicator="http://stix.mitre.org/
Indicator-2" xmlns:stix="http://stix.mitre.org/stix-1"
xmlns:stixCommon="http://stix.mitre.org/common-1"
xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="1.2">
<stix:Indicators>
  <stix:Indicator id="e16862-s14930" timestamp="2016-06-
04T16:00:54.135901-07:00" xsi:type="indicator:IndicatorType">
    <indicator:Title>Common indicator for event 16862</indicator:Title>
    <indicator:Description>Context of the threat activities. Event type:
http. Event category: Trojan_Generic. Event name: TROJAN_MIUREF.Rep.</
indicator:Description>
    <indicator:Observable>
      <atpbox:Observable_Composition operator="AND">
        <atpbox:Observable>
          <atpbox:Object>
            <atpbox:Properties
xsi:type="NetworkConnectionObj:NetworkConnectionObjectType">
              <NetworkConnectionObj:Source_Socket_Address
xsi:type="SocketAddressObj:SocketAddressObjectType">
                <SocketAddressObj:IP_Address
xsi:type="AddressObj:AddressObjectType">

```

```
        <AddressObj:Address_Value
condition="Equals">192.168.50.18</AddressObj:Address_Value>
        </SocketAddressObj:IP_Address>
        </NetworkConnectionObj:Source_Socket_Address>
        <NetworkConnectionObj:Destination_Socket_Address
xsi:type="SocketAddressObj:SocketAddressObjectType">
        <SocketAddressObj:IP_Address
xsi:type="AddressObj:AddressObjectType">
        <AddressObj:Address_Value
condition="Equals">134.19.180.195</AddressObj:Address_Value>
        </SocketAddressObj:IP_Address>
        </NetworkConnectionObj:Destination_Socket_Address>
        </JATPbox:Properties>
    </JATPbox:Object>
</JATPbox:Observable>
<JATPbox:Observable>
    <JATPbox:Object>
        <JATPbox:Properties xsi:type="URIObj:URIObjectType">
            <URIObj:Value>582330430-6.idgromo.ru</URIObj:Value>
        </JATPbox:Properties>
    </JATPbox:Object>
</JATPbox:Observable>
<JATPbox:Observable>
    <JATPbox:Object>
        <JATPbox:Properties xsi:type="URIObj:URIObjectType">
            <URIObj:Value>192.168.50.18</URIObj:Value>
        </JATPbox:Properties>
    </JATPbox:Object>
</JATPbox:Observable>
</JATPbox:Observable_Composition>
</indicator:Observable>
<indicator:Related_Indicators>
    <indicator:Related_Indicator>
        <stixCommon:Indicator id="s14930" timestamp="2016-06-
25T21:26:01.403485+00:00" xsi:type="indicator:IndicatorType">
            <indicator:Title>File indicator for storage object 14930</
indicator:Title>
            <indicator:Observable>
                <JATPbox:Object>
                    <JATPbox:Properties xsi:type="FileObj:FileObjectType">
                        <FileObj:Hashes>
                            <JATPboxCommon:Hash>
                                <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">SHA256</JATPboxCommon:Type>

                                <JATPboxCommon:Simple_Hash_Value>9db690015a4684b03c7f19c443f8a02588abebb
900edc1bb9fac635ae12e9528</JATPboxCommon:Simple_Hash_Value>
                            </JATPboxCommon:Hash>
                            <JATPboxCommon:Hash>
                                <JATPboxCommon:Type
```

```

xsi:type="JATPboxVocabs:HashNameVocab-1.0">SHA1</JATPboxCommon:Type>

<JATPboxCommon:Simple_Hash_Value>71500fb9e9877cae9652e534d76b3fbb9dbfa6b
f</JATPboxCommon:Simple_Hash_Value>
    </JATPboxCommon:Hash>
    <JATPboxCommon:Hash>
        <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">MD5</JATPboxCommon:Type>

<JATPboxCommon:Simple_Hash_Value>b999d1ad460bd367275a798b5f334f37</
JATPboxCommon:Simple_Hash_Value>
    </JATPboxCommon:Hash>
    </FileObj:Hashes>
    </JATPbox:Properties>
    </JATPbox:Object>
    </indicator:Observable>
    </stixCommon:Indicator>
    </indicator:Related_Indicator>
    <indicator:Related_Indicator>
        <stixCommon:Indicator id="b14930" timestamp="2016-06-
25T21:26:01.404784+00:00" xsi:type="indicator:IndicatorType">
            <indicator:Title>Behavior indicator for storage object 14930</
indicator:Title>
            <indicator:Observable>
                <JATPbox:Observable_Composition operator="OR">
                    <JATPbox:Observable>
                        <JATPbox:Event>
                            <JATPbox:Type xsi:type="JATPboxVocabs:EventTypeVocab-
1.0.1">File Ops (CRUD)</JATPbox:Type>
                                <JATPbox:Actions>
                                    <JATPbox:Action>
                                        <JATPbox:Type
xsi:type="JATPboxVocabs:ActionTypeVocab-1.0">Create</JATPbox:Type>
                                            <JATPbox:Associated_Objects>
                                                <JATPbox:Associated_Object>
                                                    <JATPbox:Properties
xsi:type="FileObj:FileObjectType">
                                                        <FileObj:File_Path
fully_qualified="true">C:\Documents and Settings\Administrator\Local
Settings\Temp\NRWConfig.exe</FileObj:File_Path>
                                                            </JATPbox:Properties>
                                                                </JATPbox:Associated_Object>
                                                                    </JATPbox:Associated_Objects>
                                                                        </JATPbox:Action>
                                                                            </JATPbox:Actions>
                                                                                </JATPbox:Event>
                                                                                    </JATPbox:Observable>
                                                                                        </JATPbox:Observable_Composition>
                                                                                            </indicator:Observable>
                                                                                                </stixCommon:Indicator>
                                                                                                    </indicator:Related_Indicator>

```

```

    </indicator:Related_Indicators>
  </stix:Indicator>
</stix:Indicators>
</stix:STIX_Package>
</JATP:JATP_Package>

```

Sample Response for get_iocs

Submission with IVP

```

<JATP:JATP_Package xmlns:JATP="http://www.JATP.net" version="1.0">
  <JATP:JATP_Header>
    <JATP:Title>JATP Indicators</JATP:Title>
    <JATP:Description>JATP Indicators 1 of 4810, last indicator time 2016-06-11 17:20:22.545253-07:00</JATP:Description>
  </JATP:JATP_Header>
  <stix:STIX_Package xmlns:AddressObj="http://JATPbox.mitre.org/objects#AddressObject-2" xmlns:FileObj="http://JATPbox.mitre.org/objects#FileObject-2" xmlns:NetworkConnectionObj="http://JATPbox.mitre.org/objects#NetworkConnectionObject-2" xmlns:SocketAddressObj="http://JATPbox.mitre.org/objects#SocketAddressObject-1" xmlns:URIObj="http://JATPbox.mitre.org/objects#URIObject-2" xmlns:JATPbox="http://JATPbox.mitre.org/JATPbox-2" xmlns:JATPboxCommon="http://JATPbox.mitre.org/common-2" xmlns:JATPboxVocabs="http://JATPbox.mitre.org/default_vocabularies-2" xmlns:JATP="http://JATP.net" xmlns:indicator="http://stix.mitre.org/Indicator-2" xmlns:stix="http://stix.mitre.org/stix-1" xmlns:stixCommon="http://stix.mitre.org/common-1" xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="1.2">
    <stix:Indicators>
      <stix:Indicator id="e17026-s14703" timestamp="2016-06-11T17:20:22.545253-07:00" xsi:type="indicator:IndicatorType">
        <indicator:Title>Common indicator for event 17026</indicator:Title>
        <indicator:Description>Context of the threat activities. Event type: submission. Event category: Trojan_Generic. Event name: WORM_GAMARUE.DC.</indicator:Description>
        <indicator:Observable>
          <JATPbox:Object>
            <JATPbox:Properties xsi:type="URIObj:URIObjectType">
              <URIObj:Value>User Uploaded</URIObj:Value>
            </JATPbox:Properties>
          </JATPbox:Object>
        </indicator:Observable>
        <indicator:Related_Indicators>
          <indicator:Related_Indicator>
            <stixCommon:Indicator id="s14703" timestamp="2016-06-25T21:23:16.066539+00:00" xsi:type="indicator:IndicatorType">
              <indicator:Title>File indicator for storage object 14703</indicator:Title>
              <indicator:Observable>
                <JATPbox:Object>

```

```

    <JATPbox:Properties xsi:type="FileObj:FileObjectType">
      <FileObj:Hashes>
        <JATPboxCommon:Hash>
          <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">SHA256</JATPboxCommon:Type>

          <JATPboxCommon:Simple_Hash_Value>103c02e980f7518299999fdaf64555b74be54ef
1fef86265e48f7233c5ac39d7</JATPboxCommon:Simple_Hash_Value>
          </JATPboxCommon:Hash>
          <JATPboxCommon:Hash>
            <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">SHA1</JATPboxCommon:Type>

            <JATPboxCommon:Simple_Hash_Value>1bca4f69ec98fb9b65f75d1ef8d611493a231e7
3</JATPboxCommon:Simple_Hash_Value>
            </JATPboxCommon:Hash>
            <JATPboxCommon:Hash>
              <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">MD5</JATPboxCommon:Type>

              <JATPboxCommon:Simple_Hash_Value>acfc43903491ec6bccea552965ef7f8d</
JATPboxCommon:Simple_Hash_Value>
              </JATPboxCommon:Hash>
            </FileObj:Hashes>
          </JATPbox:Properties>
        </JATPbox:Object>
      </indicator:Observable>
    </stixCommon:Indicator>
  </indicator:Related_Indicator>
<indicator:Related_Indicator>
  <stixCommon:Indicator id="b14703" timestamp="2016-06-
25T21:23:16.073337+00:00" xsi:type="indicator:IndicatorType">
    <indicator:Title>Behavior indicator for storage object 14703</
indicator:Title>
    <indicator:Observable>
      <JATPbox:Observable_Composition operator="OR">
        <JATPbox:Observable>
          <JATPbox:Event>
            <JATPbox:Type xsi:type="JATPboxVocabs:EventTypeVocab-
1.0.1">Registry Ops</JATPbox:Type>
            <JATPbox:Actions>
              <JATPbox:Action>
                <JATPbox:Type
xsi:type="JATPboxVocabs:ActionTypeVocab-1.0">Create</JATPbox:Type>
                <JATPbox:Associated_Objects>
                  <JATPbox:Associated_Object>
                    <JATPbox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

                    <WinRegistryKeyObj:Key>\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\S
haredAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplicat

```

```

ions\List</WinRegistryKeyObj:Key>
    <WinRegistryKeyObj:Values>
        <WinRegistryKeyObj:Value>

<WinRegistryKeyObj:Name>C:\WINDOWS\system32\msiexec.exe</
WinRegistryKeyObj:Name>

<WinRegistryKeyObj:Data>C:\WINDOWS\system32\msiexec.exe:*.Generic Host
Process</WinRegistryKeyObj:Data>
    <WinRegistryKeyObj:Datatype>REG_SZ</
WinRegistryKeyObj:Datatype>
    </WinRegistryKeyObj:Value>
    </WinRegistryKeyObj:Values>
    </JATPbox:Properties>
    </JATPbox:Associated_Object>
    </JATPbox:Associated_Objects>
    </JATPbox:Action>
    </JATPbox:Actions>
    </JATPbox:Event>
    </JATPbox:Observable>
    <JATPbox:Observable>
    <JATPbox:Event>
        <JATPbox:Type xsi:type="JATPboxVocabs:EventTypeVocab-
1.0.1">Registry Ops</JATPbox:Type>
        <JATPbox:Actions>
            <JATPbox:Action>
                <JATPbox:Type
xsi:type="JATPboxVocabs:ActionTypeVocab-1.0">Create</JATPbox:Type>
                <JATPbox:Associated_Objects>
                <JATPbox:Associated_Object>
                <JATPbox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

<WinRegistryKeyObj:Key>\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\Curr
entVersion\policies\Explorer\Run</WinRegistryKeyObj:Key>
    <WinRegistryKeyObj:Values>
        <WinRegistryKeyObj:Value>
        <WinRegistryKeyObj:Name>23252</
WinRegistryKeyObj:Name>

<WinRegistryKeyObj:Data>c:\docume~1\alluse~1\dxnvrflgl.exe</
WinRegistryKeyObj:Data>
    <WinRegistryKeyObj:Datatype>REG_SZ</
WinRegistryKeyObj:Datatype>
    </WinRegistryKeyObj:Value>
    </WinRegistryKeyObj:Values>
    </JATPbox:Properties>
    </JATPbox:Associated_Object>
    </JATPbox:Associated_Objects>
    </JATPbox:Action>
    </JATPbox:Actions>

```



```

        </JATPbox:Event>
    </JATPbox:Observable>
    <JATPbox:Observable>
        <JATPbox:Event>
            <JATPbox:Type xsi:type="JATPboxVocabs:EventTypeVocab-
1.0.1">Registry Ops</JATPbox:Type>
            <JATPbox:Actions>
                <JATPbox:Action>
                    <JATPbox:Type
xsi:type="JATPboxVocabs:ActionTypeVocab-1.0">Create</JATPbox:Type>
                    <JATPbox:Associated_Objects>
                        <JATPbox:Associated_Object>
                            <JATPbox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">

                            <WinRegistryKeyObj:Key>\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\S
haredAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplicat
ions\List</WinRegistryKeyObj:Key>
                                <WinRegistryKeyObj:Values>
                                    <WinRegistryKeyObj:Value>

                                </WinRegistryKeyObj:Values>
                                </WinRegistryKeyObj:Value>

                            <WinRegistryKeyObj:Name>C:\WINDOWS\system32\svchost.exe</
WinRegistryKeyObj:Name>

                            <WinRegistryKeyObj:Data>C:\WINDOWS\system32\svchost.exe:*:Generic Host
Process</WinRegistryKeyObj:Data>
                                <WinRegistryKeyObj:Datatype>REG_SZ</
WinRegistryKeyObj:Datatype>

                                </WinRegistryKeyObj:Value>
                                </WinRegistryKeyObj:Values>
                            </JATPbox:Properties>
                            </JATPbox:Associated_Object>
                            </JATPbox:Associated_Objects>
                        </JATPbox:Action>
                    </JATPbox:Actions>
                </JATPbox:Event>
            </JATPbox:Observable>
        <JATPbox:Observable>
            <JATPbox:Observable_Composition operator="OR">
                <JATPbox:Observable>
                    <JATPbox:Event>
                        <JATPbox:Type
xsi:type="JATPboxVocabs:EventTypeVocab-1.0.1">File Ops (CRUD)</
JATPbox:Type>

                        <JATPbox:Actions>
                            <JATPbox:Action>
                                <JATPbox:Type
xsi:type="JATPboxVocabs:ActionTypeVocab-1.0">Create</JATPbox:Type>
                                <JATPbox:Associated_Objects>
                                    <JATPbox:Associated_Object>

                                    <JATPbox:Properties>

```

```
xsi:type="FileObj:FileType">
    <FileObj:File_Path
fully_qualified="true">c:\Documents and Settings\All
Users\dxnvrflgl.exe</FileObj:File_Path>
    </JATPbox:Properties>
    </JATPbox:Associated_Object>
    </JATPbox:Associated_Objects>
    </JATPbox:Action>
    </JATPbox:Actions>
    </JATPbox:Event>
    </JATPbox:Observable>
    </JATPbox:Observable_Composition>
    </JATPbox:Observable>
    </JATPbox:Observable_Composition>
    </indicator:Observable>
    </stixCommon:Indicator>
    </indicator:Related_Indicator>
    </indicator:Related_Indicators>
    </stix:Indicator>
</stix:Indicators>
    </stix:STIX_Package>
</JATP:JATP_Package>
```

Sample Response for get_jocs

Submission Zip

```
<JATP:JATP_Package xmlns:JATP="http://www.JATP.net" version="1.0">
  <JATP:JATP_Header>
    <JATP:Title>JATP Indicators</JATP:Title>
    <JATP:Description>JATP Indicators 2 of 4810, last indicator time 2016-
06-15 16:17:28.821249-07:00</JATP:Description>
  </JATP:JATP_Header>
  <stix:STIX_Package xmlns:AddressObj="http://JATPbox.mitre.org/
objects#AddressObject-2" xmlns:FileObj="http://JATPbox.mitre.org/
objects#FileObject-2" xmlns:NetworkConnectionObj="http://
JATPbox.mitre.org/objects#NetworkConnectionObject-2"
xmlns:SocketAddressObj="http://JATPbox.mitre.org/
objects#SocketAddressObject-1" xmlns:URIObj="http://JATPbox.mitre.org/
objects#URIObject-2" xmlns:JATPbox="http://JATPbox.mitre.org/JATPbox-2"
xmlns:JATPboxCommon="http://JATPbox.mitre.org/common-2"
xmlns:JATPboxVocabs="http://JATPbox.mitre.org/default_vocabularies-2"
xmlns:JATP="http://JATP.net" xmlns:indicator="http://stix.mitre.org/
Indicator-2" xmlns:stix="http://stix.mitre.org/stix-1"
xmlns:stixCommon="http://stix.mitre.org/common-1"
xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="1.2">
    <stix:Indicators>
      <stix:Indicator id="e17256-s15004" timestamp="2016-06-
15T16:17:28.821249-07:00" xsi:type="indicator:IndicatorType">
        <indicator:Title>Common indicator for event 17256</indicator:Title>
        <indicator:Description>Context of the threat activities. Event type:
```

```

submission. Event category: None. Event name: None.</
indicator:Description>
  <indicator:Observable>
    <JATPbox:Object>
      <JATPbox:Properties xsi:type="URIObj:URIObjectType">
        <URIObj:Value>User Uploaded</URIObj:Value>
      </JATPbox:Properties>
    </JATPbox:Object>
  </indicator:Observable>
  <indicator:Related_Indicators>
    <indicator:Related_Indicator>
      <stixCommon:Indicator id="s15004" timestamp="2016-06-
25T21:23:16.479160+00:00" xsi:type="indicator:IndicatorType">
        <indicator:Title>File indicator for storage object 15004</
indicator:Title>
        <indicator:Observable>
          <JATPbox:Object>
            <JATPbox:Properties xsi:type="FileObj:FileObjectType">
              <FileObj:Hashes>
                <JATPboxCommon:Hash>
                  <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">SHA256</JATPboxCommon:Type>

                <JATPboxCommon:Simple_Hash_Value>535b541550973f18f6f6498d2adc0908a117884
1df14be8a97366d320d033599</JATPboxCommon:Simple_Hash_Value>
                </JATPboxCommon:Hash>
                <JATPboxCommon:Hash>
                  <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">SHA1</JATPboxCommon:Type>

                <JATPboxCommon:Simple_Hash_Value>a75f64ec687dd2d969d9c9c67ac41fd8ee6f2fa
c</JATPboxCommon:Simple_Hash_Value>
                </JATPboxCommon:Hash>
                <JATPboxCommon:Hash>
                  <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">MD5</JATPboxCommon:Type>

                <JATPboxCommon:Simple_Hash_Value>59b2b3720591e37e33f7946cb12ed74e</
JATPboxCommon:Simple_Hash_Value>
                </JATPboxCommon:Hash>
              </FileObj:Hashes>
            </JATPbox:Properties>
          </JATPbox:Object>
        </indicator:Observable>
      </stixCommon:Indicator>
    </indicator:Related_Indicator>
    <indicator:Related_Indicator>
      <stixCommon:Indicator id="b15004" timestamp="2016-06-
25T21:23:16.495466+00:00" xsi:type="indicator:IndicatorType">
        <indicator:Title>Behavior indicator for storage object 15004</
indicator:Title>

```

```

<indicator:Observable>
  <JATPbox:Observable_Composition operator="OR">
    <JATPbox:Observable>
      <JATPbox:Event>
        <JATPbox:Type xsi:type="JATPboxVocabs:EventTypeVocab-
1.0.1">File Ops (CRUD)</JATPbox:Type>
        <JATPbox:Actions>
          <JATPbox:Action>
            <JATPbox:Type
xsi:type="JATPboxVocabs:ActionTypeVocab-1.0">Create</JATPbox:Type>
            <JATPbox:Associated_Objects>
              <JATPbox:Associated_Object>
                <JATPbox:Properties
xsi:type="FileObj:FileType">
                  <FileObj:File_Path
fully_qualified="true">C:\Documents and
Settings\Administrator\Application
Data\Adobe\Acrobat\8.0\UserCache.bin</FileObj:File_Path>
                </JATPbox:Properties>
              </JATPbox:Associated_Object>
            </JATPbox:Associated_Objects>
          </JATPbox:Action>
        </JATPbox:Actions>
      </JATPbox:Event>
    </JATPbox:Observable>
  </JATPbox:Observable_Composition>
</indicator:Observable>
</stixCommon:Indicator>
</indicator:Related_Indicator>
</indicator:Related_Indicators>
</stix:Indicator>
<stix:Indicator id="e17256-s15005" timestamp="2016-06-
15T16:17:28.821249-07:00" xsi:type="indicator:IndicatorType">
  <indicator:Title>Common indicator for event 17256</indicator:Title>
  <indicator:Description>Context of the threat activities. Event type:
submission. Event category: None. Event name: None.</
indicator:Description>
  <indicator:Observable>
    <JATPbox:Object>
      <JATPbox:Properties xsi:type="URIObj:URIObjectType">
        <URIObj:Value>User Uploaded</URIObj:Value>
      </JATPbox:Properties>
    </JATPbox:Object>
  </indicator:Observable>
  <indicator:Related_Indicators>
    <indicator:Related_Indicator>
      <stixCommon:Indicator id="s15005" timestamp="2016-06-
25T21:23:16.505289+00:00" xsi:type="indicator:IndicatorType">
        <indicator:Title>File indicator for storage object 15005</
indicator:Title>

```

```

<indicator:Observable>
  <JATPbox:Object>
    <JATPbox:Properties xsi:type="FileObj:FileObjectType">
      <FileObj:Hashes>
        <JATPboxCommon:Hash>
          <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">SHA256</JATPboxCommon:Type>

          <JATPboxCommon:Simple_Hash_Value>370ef1a8b59e721c08b6d1b5c3def23f98f97a2
fca81045fce48fd800888b13</JATPboxCommon:Simple_Hash_Value>
        </JATPboxCommon:Hash>
        <JATPboxCommon:Hash>
          <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">SHA1</JATPboxCommon:Type>

          <JATPboxCommon:Simple_Hash_Value>1fc12d33627bb3f3adde85e831af97d97a173a7
a</JATPboxCommon:Simple_Hash_Value>
        </JATPboxCommon:Hash>
        <JATPboxCommon:Hash>
          <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">MD5</JATPboxCommon:Type>

          <JATPboxCommon:Simple_Hash_Value>0d418fb846db353305deddfa886a8985</
JATPboxCommon:Simple_Hash_Value>
        </JATPboxCommon:Hash>
      </FileObj:Hashes>
    </JATPbox:Properties>
  </JATPbox:Object>
</indicator:Observable>
</stixCommon:Indicator>
</indicator:Related_Indicator>
</indicator:Related_Indicators>
</stix:Indicator>
</stix:Indicators>
</stix:STIX_Package>
</JATP:JATP_Package>

```

Sample Response for get_iocs

Email without IVP

```

<JATP:JATP_Package xmlns:JATP="http://www.JATP.net" version="1.0">
  <JATP:JATP_Header>
    <JATP:Title>JATP Indicators</JATP:Title>
    <JATP:Description>JATP Indicators 1 of 4810, last indicator time 2016-
06-17 20:16:43-07:00</JATP:Description>
  </JATP:JATP_Header>
  <stix:STIX_Package xmlns:AddressObj="http://JATPbox.mitre.org/
objects#AddressObject-2" xmlns:FileObj="http://JATPbox.mitre.org/
objects#FileObject-2" xmlns:NetworkConnectionObj="http://
JATPbox.mitre.org/objects#NetworkConnectionObject-2"
xmlns:SocketAddressObj="http://JATPbox.mitre.org/

```

```

objects#SocketAddressObject-1" xmlns:URIObj="http://JATPbox.mitre.org/
objects#URIObject-2" xmlns:JATPbox="http://JATPbox.mitre.org/JATPbox-2"
xmlns:JATPboxCommon="http://JATPbox.mitre.org/common-2"
xmlns:JATPboxVocabs="http://JATPbox.mitre.org/default_vocabularies-2"
xmlns:JATP="http://JATP.net" xmlns:indicator="http://stix.mitre.org/
Indicator-2" xmlns:stix="http://stix.mitre.org/stix-1"
xmlns:stixCommon="http://stix.mitre.org/common-1"
xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="1.2">
<stix:Indicators>
  <stix:Indicator id="e17259-s14700" timestamp="2016-06-17T20:16:43-
07:00" xsi:type="indicator:IndicatorType">
    <indicator:Title>Common indicator for event 17259</indicator:Title>
    <indicator:Description>Context of the threat activities. Event type:
email. Event category: Worm. Event name: WORM_CONFICKER.CY.</
indicator:Description>
    <indicator:Observable>
      <JATPbox:Object>
        <JATPbox:Properties
xsi:type="EmailMessageObj:EmailMessageObjectType">
          <EmailMessageObj:Header>
            <EmailMessageObj:To>
              <EmailMessageObj:Recipient
xsi:type="AddressObj:AddressObjectType" category="e-mail">

<AddressObj:Address_Value>central_user5@biz_central.JATP.net</
AddressObj:Address_Value>
                </EmailMessageObj:Recipient>
              </EmailMessageObj:To>
            <EmailMessageObj:From
xsi:type="AddressObj:AddressObjectType" category="e-mail">

<AddressObj:Address_Value>central_user6@biz_central.JATP.net</
AddressObj:Address_Value>
                </EmailMessageObj:From>
              </EmailMessageObj:Header>
            </JATPbox:Properties>
          </JATPbox:Object>
        </indicator:Observable>
      <indicator:Related_Indicators>
        <indicator:Related_Indicator>
          <stixCommon:Indicator id="s14700" timestamp="2016-06-
25T21:23:16.524354+00:00" xsi:type="indicator:IndicatorType">
            <indicator:Title>File indicator for storage object 14700</
indicator:Title>
            <indicator:Observable>
              <JATPbox:Object>
                <JATPbox:Properties xsi:type="FileObj:FileObjectType">
                  <FileObj:Hashes>
                    <JATPboxCommon:Hash>
                      <JATPboxCommon:Type

```

```

xsi:type="JATPboxVocabs:HashNameVocab-1.0">SHA256</JATPboxCommon:Type>

<JATPboxCommon:Simple_Hash_Value>896eb5f146817aae8981c31063029531caba959
437ff610a7e096436f97300fe</JATPboxCommon:Simple_Hash_Value>
    </JATPboxCommon:Hash>
    <JATPboxCommon:Hash>
        <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">SHA1</JATPboxCommon:Type>

<JATPboxCommon:Simple_Hash_Value>627bef790e3b265260389d33979cf9e9e8deb8c
d</JATPboxCommon:Simple_Hash_Value>
    </JATPboxCommon:Hash>
    <JATPboxCommon:Hash>
        <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">MD5</JATPboxCommon:Type>

<JATPboxCommon:Simple_Hash_Value>393e2e61ff08a8f7439e3d2cfcb8056f</
JATPboxCommon:Simple_Hash_Value>
    </JATPboxCommon:Hash>
</FileObj:Hashes>
</JATPbox:Properties>
</JATPbox:Object>
</indicator:Observable>
</stixCommon:Indicator>
</indicator:Related_Indicator>
</indicator:Related_Indicators>
</stix:Indicator>
</stix:Indicators>
</stix:STIX_Package>
</JATP:JATP_Package>

```

Sample Response for get_iocs

Email with IVP

```

<JATP:JATP_Package xmlns:JATP="http://www.JATP.net" version="1.0">
  <JATP:JATP_Header>
    <JATP:Title>JATP Indicators</JATP:Title>
    <JATP:Description>JATP Indicators 1 of 4810, last indicator time 2016-
06-17 20:16:43-07:00</JATP:Description>
  </JATP:JATP_Header>
  <stix:STIX_Package xmlns:AddressObj="http://JATPbox.mitre.org/
objects#AddressObject-2" xmlns:FileObj="http://JATPbox.mitre.org/
objects#FileObject-2" xmlns:NetworkConnectionObj="http://
JATPbox.mitre.org/objects#NetworkConnectionObject-2"
xmlns:SocketAddressObj="http://JATPbox.mitre.org/
objects#SocketAddressObject-1" xmlns:URIObj="http://JATPbox.mitre.org/
objects#URIObject-2" xmlns:JATPbox="http://JATPbox.mitre.org/JATPbox-2"
xmlns:JATPboxCommon="http://JATPbox.mitre.org/common-2"
xmlns:JATPboxVocabs="http://JATPbox.mitre.org/default_vocabularies-2"
xmlns:JATP="http://JATP.net" xmlns:indicator="http://stix.mitre.org/
Indicator-2" xmlns:stix="http://stix.mitre.org/stix-1"

```

```

xmlns:stixCommon="http://stix.mitre.org/common-1"
xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="1.2">
<stix:Indicators>
  <stix:Indicator id="e17257-s14732" timestamp="2016-06-17T20:16:43-
07:00" xsi:type="indicator:IndicatorType">
    <indicator:Title>Common indicator for event 17257</indicator:Title>
    <indicator:Description>Context of the threat activities. Event type:
email. Event category: Trojan_Generic. Event name: TROJAN_VUNDO.DC.</
indicator:Description>
    <indicator:Observable>
      <JATPbox:Object>
        <JATPbox:Properties
xsi:type="EmailMessageObj:EmailMessageObjectType">
          <EmailMessageObj:Header>
            <EmailMessageObj:To>
              <EmailMessageObj:Recipient
xsi:type="AddressObj:AddressObjectType" category="e-mail">

<AddressObj:Address_Value>central_user5@biz_central.JATP.net</
AddressObj:Address_Value>
                </EmailMessageObj:Recipient>
              </EmailMessageObj:To>
              <EmailMessageObj:From
xsi:type="AddressObj:AddressObjectType" category="e-mail">

<AddressObj:Address_Value>central_user6@biz_central.JATP.net</
AddressObj:Address_Value>
                </EmailMessageObj:From>
              </EmailMessageObj:Header>
            </JATPbox:Properties>
          </JATPbox:Object>
        </indicator:Observable>
      <indicator:Related_Indicators>
        <indicator:Related_Indicator>
          <stixCommon:Indicator id="s14732" timestamp="2016-06-
25T21:23:16.525198+00:00" xsi:type="indicator:IndicatorType">
            <indicator:Title>File indicator for storage object 14732</
indicator:Title>
            <indicator:Observable>
              <JATPbox:Object>
                <JATPbox:Properties xsi:type="FileObj:FileObjectType">
                  <FileObj:Hashes>
                    <JATPboxCommon:Hash>
                      <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">SHA256</JATPboxCommon:Type>

<JATPboxCommon:Simple_Hash_Value>6d88308a029653c56e2f1d84eb7c4b2ebc588f6
5a108f3c98203a089bf3692ca</JATPboxCommon:Simple_Hash_Value>
                    </JATPboxCommon:Hash>
                  <JATPboxCommon:Hash>

```



```

        <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">SHA1</JATPboxCommon:Type>

<JATPboxCommon:Simple_Hash_Value>c01e057e6b7115057d9465311346f198a7fed57
4</JATPboxCommon:Simple_Hash_Value>
    </JATPboxCommon:Hash>
    <JATPboxCommon:Hash>
        <JATPboxCommon:Type
xsi:type="JATPboxVocabs:HashNameVocab-1.0">MD5</JATPboxCommon:Type>

<JATPboxCommon:Simple_Hash_Value>efed1115deb7d3c67bfe4921b82bd86b</
JATPboxCommon:Simple_Hash_Value>
    </JATPboxCommon:Hash>
    </FileObj:Hashes>
    </JATPbox:Properties>
    </JATPbox:Object>
</indicator:Observable>
</stixCommon:Indicator>
</indicator:Related_Indicator>
<indicator:Related_Indicator>
    <stixCommon:Indicator id="b14732" timestamp="2016-06-
25T21:23:16.525708+00:00" xsi:type="indicator:IndicatorType">
        <indicator:Title>Behavior indicator for storage object 14732</
indicator:Title>
        <indicator:Observable>
            <JATPbox:Observable_Composition operator="OR">
                <JATPbox:Observable>
                    <JATPbox:Event>
                        <JATPbox:Type xsi:type="JATPboxVocabs:EventTypeVocab-
1.0.1">Registry Ops</JATPbox:Type>
                        <JATPbox:Actions>
                            <JATPbox:Action>
                                <JATPbox:Type
xsi:type="JATPboxVocabs:ActionTypeVocab-1.0">Create</JATPbox:Type>
                                <JATPbox:Associated_Objects>
                                    <JATPbox:Associated_Object>
                                        <JATPbox:Properties
xsi:type="WinRegistryKeyObj:WindowsRegistryKeyObjectType">
                                            <WinRegistryKeyObj:Key>\REGISTRY\USER\S-1-5-
21-842925246-484763869-117609710-
500\Software\Microsoft\Windows\CurrentVersion\Run</
WinRegistryKeyObj:Key>
                                                <WinRegistryKeyObj:Values>
                                                    <WinRegistryKeyObj:Value>
                                                        <WinRegistryKeyObj:Name>~backup~</
WinRegistryKeyObj:Name>
                                                            <WinRegistryKeyObj:Data>C:\Documents and
Settings\Administrator\My Documents\Application Data\explorer.exe</
WinRegistryKeyObj:Data>
                                                                <WinRegistryKeyObj:Datatype>REG_SZ</
WinRegistryKeyObj:Datatype>

```

```

        </WinRegistryKeyObj:Value>
        </WinRegistryKeyObj:Values>
    </JATPbox:Properties>
    </JATPbox:Associated_Object>
    </JATPbox:Associated_Objects>
    </JATPbox:Action>
    </JATPbox:Actions>
    </JATPbox:Event>
</JATPbox:Observable>
<JATPbox:Observable>
    <JATPbox:Observable_Composition operator="OR">
        <JATPbox:Observable>
            <JATPbox:Event>
                <JATPbox:Type
xsi:type="JATPboxVocabs:EventTypeVocab-1.0.1">File Ops (CRUD)</
JATPbox:Type>
                <JATPbox:Actions>
                    <JATPbox:Action>
                        <JATPbox:Type
xsi:type="JATPboxVocabs:ActionTypeVocab-1.0">Create</JATPbox:Type>
                        <JATPbox:Associated_Objects>
                            <JATPbox:Associated_Object>
                                <JATPbox:Properties
xsi:type="FileObj:FileObjectType">
                                    <FileObj:File_Path
fully_qualified="true">C:\Documents and Settings\Administrator\My
Documents\Application Data\explorer.exe</FileObj:File_Path>
                                </JATPbox:Properties>
                            </JATPbox:Associated_Object>
                        </JATPbox:Associated_Objects>
                    </JATPbox:Action>
                </JATPbox:Actions>
            </JATPbox:Event>
        </JATPbox:Observable>
    <JATPbox:Observable>
        <JATPbox:Event>
            <JATPbox:Type
xsi:type="JATPboxVocabs:EventTypeVocab-1.0.1">File Ops (CRUD)</
JATPbox:Type>
            <JATPbox:Actions>
                <JATPbox:Action>
                    <JATPbox:Type
xsi:type="JATPboxVocabs:ActionTypeVocab-1.0">Create</JATPbox:Type>
                    <JATPbox:Associated_Objects>
                        <JATPbox:Associated_Object>
                            <JATPbox:Properties
xsi:type="FileObj:FileObjectType">
                                <FileObj:File_Path
fully_qualified="true">C:\Documents and Settings\Administrator\My
Documents\Application Data\explorer.dat</FileObj:File_Path>
                            </JATPbox:Properties>

```

```

        </JATPbox:Associated_Object>
        </JATPbox:Associated_Objects>
        </JATPbox:Action>
        </JATPbox:Actions>
        </JATPbox:Event>
        </JATPbox:Observable>
        </JATPbox:Observable_Composition>
        </JATPbox:Observable>
        </JATPbox:Observable_Composition>
    </indicator:Observable>
</stixCommon:Indicator>
</indicator:Related_Indicator>
</indicator:Related_Indicators>
</stix:Indicator>
</stix:Indicators>
</stix:STIX_Package>
</JATP:JATP_Package>

```

Sample Response for get_iocs

CnC

```

<JATP:JATP_Package xmlns:JATP="http://www.JATP.net" version="1.0">
  <JATP:JATP_Header>
    <JATP:Title>JATP Indicators</JATP:Title>
    <JATP:Description>JATP Indicators 1 of 4810, last indicator time 2016-06-04 21:55:25.050000-07:00</JATP:Description>
  </JATP:JATP_Header>
  <stix:STIX_Package xmlns:AddressObj="http://JATPbox.mitre.org/objects#AddressObject-2" xmlns:FileObj="http://JATPbox.mitre.org/objects#FileObject-2" xmlns:NetworkConnectionObj="http://JATPbox.mitre.org/objects#NetworkConnectionObject-2" xmlns:SocketAddressObj="http://JATPbox.mitre.org/objects#SocketAddressObject-1" xmlns:URIObj="http://JATPbox.mitre.org/objects#URIObject-2" xmlns:JATPbox="http://JATPbox.mitre.org/JATPbox-2" xmlns:JATPboxCommon="http://JATPbox.mitre.org/common-2" xmlns:JATPboxVocabs="http://JATPbox.mitre.org/default_vocabularies-2" xmlns:JATP="http://JATP.net" xmlns:indicator="http://stix.mitre.org/Indicator-2" xmlns:stix="http://stix.mitre.org/stix-1" xmlns:stixCommon="http://stix.mitre.org/common-1" xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="1.2">
    <stix:Indicators>
      <stix:Indicator id="e16861" timestamp="2016-06-04T21:55:25.050000-07:00" xsi:type="indicator:IndicatorType">
        <indicator:Title>Common indicator for event 16861</indicator:Title>
        <indicator:Description>Context of the threat activities. Event type: cnc. Event category: Suspicious. Event name: TROJAN_Miuref.CY.</indicator:Description>
        <indicator:Observable>
          <JATPbox:Observable_Composition operator="AND">
            <JATPbox:Observable>

```

```

    <JATPbox:Object>
      <JATPbox:Properties
xsi:type="NetworkConnectionObj:NetworkConnectionObjectType">
        <NetworkConnectionObj:Source_Socket_Address
xsi:type="SocketAddressObj:SocketAddressObjectType">
          <SocketAddressObj:IP_Address
xsi:type="AddressObj:AddressObjectType">
            <AddressObj:Address_Value
condition="Equals">192.168.50.203</AddressObj:Address_Value>
          </SocketAddressObj:IP_Address>
        </NetworkConnectionObj:Source_Socket_Address>
        <NetworkConnectionObj:Destination_Socket_Address
xsi:type="SocketAddressObj:SocketAddressObjectType">
          <SocketAddressObj:IP_Address
xsi:type="AddressObj:AddressObjectType">
            <AddressObj:Address_Value
condition="Equals">46.165.222.218</AddressObj:Address_Value>
          </SocketAddressObj:IP_Address>
        </NetworkConnectionObj:Destination_Socket_Address>
      </JATPbox:Properties>
    </JATPbox:Object>
  </JATPbox:Observable>
  <JATPbox:Observable>
    <JATPbox:Object>
      <JATPbox:Properties xsi:type="URIObj:URIObjectType">
        <URIObj:Value>46.165.222.218</URIObj:Value>
      </JATPbox:Properties>
    </JATPbox:Object>
  </JATPbox:Observable>
  <JATPbox:Observable>
    <JATPbox:Object>
      <JATPbox:Properties xsi:type="URIObj:URIObjectType">
        <URIObj:Value>192.168.50.203</URIObj:Value>
      </JATPbox:Properties>
    </JATPbox:Object>
  </JATPbox:Observable>
</JATPbox:Observable_Composition>
</indicator:Observable>
</stix:Indicator>
</stix:Indicators>
</stix:STIX_Package>
</JATP:JATP_Package>

```

Sample Response for get_iocs

Exploit

```

<JATP:JATP_Package xmlns:JATP="www.JATP.com" version="1.0">
  <JATP:JATP_Header>
    <JATP:Title>JATP Indicators</JATP:Title>
    <JATP:Description>JATP Indicators 1 of 4810, last indicator time 2016-

```

```

06-04 21:55:45.285867-07:00</JATP:Description>
  </JATP:JATP_Header>
  <stix:STIX_Package xmlns:AddressObj="http://JATPbox.mitre.org/
objects#AddressObject-2" xmlns:FileObj="http://JATPbox.mitre.org/
objects#FileObject-2" xmlns:NetworkConnectionObj="http://
JATPbox.mitre.org/objects#NetworkConnectionObject-2"
xmlns:SocketAddressObj="http://JATPbox.mitre.org/
objects#SocketAddressObject-1" xmlns:URIObj="http://JATPbox.mitre.org/
objects#URIObject-2" xmlns:JATPbox="http://JATPbox.mitre.org/JATPbox-2"
xmlns:JATPboxCommon="http://JATPbox.mitre.org/common-2"
xmlns:JATPboxVocabs="http://JATPbox.mitre.org/default_vocabularies-2"
xmlns:JATP="http://JATP.net" xmlns:indicator="http://stix.mitre.org/
Indicator-2" xmlns:stix="http://stix.mitre.org/stix-1"
xmlns:stixCommon="http://stix.mitre.org/common-1"
xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="1.2">
<stix:Indicators>
  <stix:Indicator id="e16864" timestamp="2016-06-04T21:55:45.285867-
07:00" xsi:type="indicator:IndicatorType">
    <indicator:Title>Common indicator for event 16864</indicator:Title>
    <indicator:Description>Context of the threat activities. Event type:
exploit. Event category: None. Event name: Exploit.</
indicator:Description>
    <indicator:Observable>
      <JATPbox:Observable_Composition operator="AND">
        <JATPbox:Observable>
          <JATPbox:Object>
            <JATPbox:Properties
xsi:type="NetworkConnectionObj:NetworkConnectionObjectType">
              <NetworkConnectionObj:Source_Socket_Address
xsi:type="SocketAddressObj:SocketAddressObjectType">
                <SocketAddressObj:IP_Address
xsi:type="AddressObj:AddressObjectType">
                  <AddressObj:Address_Value
condition="Equals">192.168.50.203</AddressObj:Address_Value>
                </SocketAddressObj:IP_Address>
              </NetworkConnectionObj:Source_Socket_Address>
              <NetworkConnectionObj:Destination_Socket_Address
xsi:type="SocketAddressObj:SocketAddressObjectType">
                <SocketAddressObj:IP_Address
xsi:type="AddressObj:AddressObjectType">
                  <AddressObj:Address_Value
condition="Equals">64.202.116.124</AddressObj:Address_Value>
                </SocketAddressObj:IP_Address>
              </NetworkConnectionObj:Destination_Socket_Address>
            </JATPbox:Properties>
          </JATPbox:Object>
        </JATPbox:Observable>
      </JATPbox:Observable>
    </indicator:Observable>
  </stix:Indicator>
</stix:Indicators>

```

```

        <URIObj:Value>64.202.116.124</URIObj:Value>
      </JATPbox:Properties>
    </JATPbox:Object>
  </JATPbox:Observable>
<JATPbox:Observable>
  <JATPbox:Object>
    <JATPbox:Properties xsi:type="URIObj:URIObjectType">
      <URIObj:Value>192.168.50.203</URIObj:Value>
    </JATPbox:Properties>
  </JATPbox:Object>
</JATPbox:Observable>
</JATPbox:Observable_Composition>
</indicator:Observable>
</stix:Indicator>
</stix:Indicators>
  </stix:STIX_Package>
</JATP:JATP_Package>

```

Sample STIX Data

STIX validator is used as the minimal validation.

Sample STIX Data are provided in this section for:

- HTTP Event
- Submission Event
- Email Event
- CnC Event
- Exploit Event
- IVP

Sample STIX Data for an HTTP Event

```

event_id           | 16603
event_type         | http
event_category     | Trojan_Generic
event_name         | TROJAN_ZEGOST.DC
event_severity     | 0.75
endpoint_ip        | 172.16.0.2
endpoint_name      | 172.16.0.2
endpoint_os_type   |
source_ip          | 172.16.0.1
source_name        | greatfilesarey.asia
source_country_code |
source_uri         |
collector_id       | 03000200-0400-0500-0006-000700080009
event_start_time   | 2016-06-29 11:39:03.921156-07
last_activity_time | 2016-06-29 11:39:03.921156-07
incident_id        | 2578

```

```

incident_risk      | 0.750
event_status      | done
event_processed_time | 2016-06-29 12:24:28.957648-07
dependent_done_time | 2016-06-29 12:24:28.931417-07
event_relevance   | 1.0
search_data       | Trojan_Generic 03000200-0400-0500-0006-000700080009
4272ad068d1259d377f8300efd395ddc greatfilesarey.asia 172.16.0.2
172.16.0.1 http://greatfilesarey.asia/malware_vault/malware/newton_qa/
file_samples/malware_exe/WL-61e7ee84986355cf85beb079e6cb623f-0
f6bf35ac0db072661356bbfd8911c783208c0820fab281e4b9520298234386b1
TROJAN_ZEGOST.DC 0394a458e68fe508ee0b773ef6fb5401b870dd1c
has_valid_av      |
has_os_match      |
has_execution     | f
whitelisted       | f
analysis_done_time | 2016-06-29 12:24:24.898253-07
custom_img_infected |
initial_done_time | 2016-06-29 12:24:24.898253-07
Submission Event
event_id          | 16868
event_type        | submission
event_category    | Worm
event_name        | WORM_LOVGATE.DC
event_severity    | 0.75
endpoint_ip       |
endpoint_name     |
endpoint_os_type  |
source_ip         |
source_name       | User Uploaded
source_country_code |
source_uri        |
collector_id      | 00000000-0000-0000-0000-000000000002
event_start_time  | 2016-06-04 22:05:59.451969-07
last_activity_time | 2016-06-04 22:05:59.451969-07
incident_id       | 2586
incident_risk     | 0.750
event_status      | done
event_processed_time | 2016-06-04 22:07:35.021933-07
dependent_done_time | 2016-06-04 22:07:35.002534-07
event_relevance   | 1.0
search_data       | WORM_LOVGATE.DC Worm
fd52b4134c4b6c4ec42ca2cb1efa919303bcda83
5d73aba7169ebfd2bdfd99437d5d8b11
31d66f99962c353c44f310b69a576aef7b8e82e6b18a99d61927711a3f76fd32
has_valid_av      |
has_os_match      |
has_execution     | f
whitelisted       | f
analysis_done_time | 2016-06-04 22:07:08.859399-07
custom_img_infected |

```

initial_done_time| 2016-06-04 22:07:08.859399-07

Sample STIX Data for an Email Event

```

event_id           | 16877
event_type         | email
event_category     | Worm
event_name         | WORM_CONFICKER.CY
event_severity     | 0.75
endpoint_ip        |
endpoint_name      | central_user7@biz_central.JATP.net
endpoint_os_type   |
source_ip          |
source_name        | central_user8@biz_central.JATP.net
source_country_code |
source_uri         |
collector_id       | 00000000-0000-0000-0000-000000000001
event_start_time   | 2016-06-06 16:17:06-07
last_activity_time | 2016-06-06 16:17:06-07
incident_id        | 2602
incident_risk      | 0.750
event_status       | done
event_processed_time | 2016-06-06 16:19:58.395234-07
dependent_done_time | 2016-06-04 17:04:38.713595-07
event_relevance    | 1.0
search_data        | 10.2.10.7 1a1eea36108cc35942a39a3e9d0e22c0 10.2.10.4
Worm central_user7@biz_central.JATP.net 00000000-0000-0000-0000-
000000000001 central_user8@biz_central.JATP.net email://
<20160806231706.4610.32986.central_user8@biz_central.JATP.net@replay1.JA
TP-world.com> 58bb58b1c18017455d5353b3fc31e32c94b1ea1d
3617ab1b94cf881aeeca16b8146cb566767bd66d134779851d4a2acf241e6a1f
WORM_CONFICKER.CY
has_valid_av       |
has_os_match       |
has_execution      | f
whitelisted        | f
analysis_done_time | 2016-06-06 16:20:10.108402-07
custom_img_infected |
initial_done_time  | 2016-06-06 16:20:10.108402-07
CNC Event
event_id           | 16859
event_type         | cnc
event_category     | Trojan_Generic
event_name         | TROJAN_Malex.CY
event_severity     | 0.75
endpoint_ip        | 10.0.2.15
endpoint_name      | 10.0.2.15
endpoint_os_type   |
source_ip          | 64.20.35.186
source_name        | nhatlinh98.net

```



```
source_country_code | US
source_uri          |
collector_id        | 00000000-0000-0000-0000-000000000000
event_start_time    | 2016-06-30 11:37:51.979-07
last_activity_time  | 2016-06-30 11:40:53.022-07
incident_id         | 2579
incident_risk       | 0.750
event_status        | done
event_processed_time | 2016-06-30 11:58:36.235653-07
dependent_done_time | 2016-06-30 11:58:35.859673-07
event_relevance     | 1.0
search_data         | 00000000-0000-0000-0000-000000000000 TROJAN_Malex.CY
Trojan_Generic 64.20.35.186 10.0.2.15
has_valid_av        |
has_os_match        |
has_execution       | f
whitelisted         |
analysis_done_time   | 2016-06-30 11:43:30.353565-07
custom_img_infected |
initial_done_time    | 2016-06-30 11:43:30.353565-07
Exploit Event
event_id            | 16863
event_type          | exploit
event_category      |
event_name          | Exploit
event_severity      | 0.25
endpoint_ip         | 192.168.50.203
endpoint_name       | 192.168.50.203
endpoint_os_type    | windows
source_ip           | 64.202.116.124
source_name         | 64.202.116.124
source_country_code | US
source_uri          |
collector_id        | 03000200-0400-0500-0006-000700080009
event_start_time    | 2016-06-04 21:52:16.097747-07
last_activity_time  | 2016-06-04 21:52:16.097747-07
incident_id         | 2582
incident_risk       | 0.250
event_status        | done
event_processed_time | 2016-06-04 21:57:22.211961-07
dependent_done_time | 2016-06-04 21:57:22.194591-07
event_relevance     | 1.0
search_data         | 64.202.116.124 Exploit 192.168.50.203 03000200-0400-
0500-0006-000700080009
has_valid_av        |
has_os_match        |
has_execution       | f
whitelisted         |
analysis_done_time   | 2016-06-04 21:57:23.910671-07
custom_img_infected |
```

```
initial_done_time| 2016-06-04 21:57:23.910671-07
```

get_ivp

Use this API to generate and download an IVP for a given event_id, MD5sum or SHA1SUM.

The API for getting blocked URLs is as follows (there are no required parameters):

```
https://HOST/admin/api.php?op=get_ivp
```

Example

```
curl "https://10.2.20.84/admin/api.php?op=get_ivp" --data
"event_id=24"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

HTTP Post Parameters	Description
event_id md5sum sha1sum	[Required] Provide one of these event identifiers.

Sample Output

A file containing the IVP.

get_reports

Use this API to retrieve configuration information.

Reports include: siem, email-coll, network-value, auto-mitigation, dlp-configuration, av-configuration, golden image results, configured zones and all configured mitigation devices.

The API for report retrieval is as follows (there are no required parameters):

```
https://HOST/admin/api.php?op=get_reports
```

An example of the API for retrieving configured tenant zones is as follows:

```
curl 'https://10.1.1.1/admin/
api.php?op=get_reports&report_group=zones-configuration' -H 'Host:
10.1.1.1' -H "Authorization:ae5bab7c3a2241a89a435d3671e29f92"
```

The API for retrieving information about a specific tenant zone is as follows:

```
curl 'https://10.1.1.1/admin/
api.php?op=get_reports&report_group=zones-
configuration&report_id=4F12B367-5983-4D6E-8719-B9C84A01F043' -H
'Host: 10.1.1.1' -H "Authorization:ae5bab7c3a2241a89a435d3671e29f92"
```

The API for retrieving all mitigation devices, "[op=get_reports&report_group=auto-mitigation](#)", is shown as follows:

https://HOST/admin/api.php?op=get_reports&report_group=auto-mitigation

The returned value is same as that displayed in Config > Environmental Settings > Firewall Mitigation Settings at the Central Manager.

The API response contains a "report_table" field which is a JSON object/map keyed on report id. Each value is a report object that constrains the following common fields as well as fields specific to each report group:

Report Field	Description
report_group	Retrieve configuration for "report", "siem", "av-configuration", "email-coll", "network-value", "auto-mitigation", "dlp-configuration", "custom-image",
report_id	The ID of the report to display.
time_created	Time of report file creation.
time_modified	Time report was last modified
user_id	User who created the report
zones-configuration	currently configured zones

Example

```
curl -k -v -b "Authorization:7c71c218662411a5c857042053acca8f"
"https://10.2.2.2/admin/api.php?op=get_report"
```

```
curl "https://10.2.20.84/admin/api.php?op=show_report&report_id=<>"
```

```
curl "https://10.2.20.84/admin/api.php?op=get_reports" --data
"report_group=custom-image&csrf_token=54e5b5916c43f1.42854640"
```

```
curl "https://10.2.20.84/admin/api.php?op=show_report&report_id=<>"
[Displays HTML for the corresponding report.]
```

```
curl "https://10.2.25.52/admin/
api.php?op=get_reports&report_group=auto-mitigation" -H "Host:
10.2.25.52" -H "Authorization:54c20d76c5fcff62cccf2208b45712be"
--insecure
```

[Displays all mitigation devices in the corresponding report. The returned json report_table dictionary contains elements for each configured device. The ID is provided in UUID format, such as 4F12B367-5983-4D6E-8719-B9C84A01F043 in the report_id. This can be used in other APIs such as "test connection." You can ignore other

attributes returned as they are used mainly by the JATPJATP Web UI. Note that the attribute `host_name` is the name or IP address of the mitigation device, and `mitigate_type` is the device type.]

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Output

```
{
  "status" : 0,
  "session_timeout_sec" : 36000,
  "report_table" : {
    "3CD2D2D6-D826-4CB0-887B-31983CACAF96" : {
      "time_modified_ms" : "1384391241000",
      "report_format" : "html",
      "time_created" : "Wed Nov 13 2013 17:07:21 GMT-0800 (PST)",
      "report_group" : "report",
      "alert_severity" : "0.0",
      "report_type" : "downloads_by_server",
      "report_category" : "technical",
      "date_range" : "year",
      "report_id" : "3CD2D2D6-D826-4CB0-887B-31983CACAF96",
      "delivery_mechanism" : "on_demand",
      "max_num_results" : "25",
      "user_id" : "2d9d5a23-a309-0a09-2dfa-4585b2e5f851",
      "time_modified" : "Wed Jul 16 2016 18:18:10 -0700"
    },

    "5A0572D7-89D3-488A-8C47-3AC98C7627C1" : {
      "report_format" : "html",
      "time_created" : "Wed Nov 13 2013 17:06:04 GMT-0800 (PST)",
      "report_group" : "report",
      "report_type" : "recent_malware",
      "report_category" : "executive",
      "date_range" : "day",
      "report_id" : "5A0572D7-89D3-488A-8C47-3AC98C7627C1",
      "delivery_mechanism" : "on_demand",
      "max_num_results" : "2500",
      "user_id" : "2d9d5a23-a309-0a09-2dfa-4585b2e5f851",
      "time_modified" : "Wed Nov 13 2013 17:06:04 GMT-0800 (PST)"
    }
  }
}
```

To get custom Golden Image results information:

```
{
  "report_table": {
```

```

"C34B0155-EA5E-4C46-982C-F5C9BDEE6236": {
  "report_id": "C34B0155-EA5E-4C46-982C-F5C9BDEE6236",
  "time_created": "Thu Feb 19 2016 15:36:47 GMT+0530 (IST)",
  "time_modified": "Thu Feb 19 2016 15:36:47 GMT+0530 (IST)",
  "vm_image_name": "Test",
  "description": "Test",
  "vnc_id": "1",
  "disk_size": "20",
  "risk_reduction": "0",
  "network_cidr": "default",
  "report_group": "custom-image",
  "arch_type": "32bit",
  "os_type": "win7",
  "enabled_time": "",
  "finalized_time": "",
  "last_modified_time": "",
  "last_boot_time": "",
  "enabled": false,
  "running": false,
  "read_only": false,
  "user_id": "be7c484c-ad72-06b0-81f7-cfeb8cd7222a"
}
},
"session_timeout_sec": 900,
"status": 0
}

```

To get mitigation device data:

```

{
  "report_table": {
    "4F12B367-5983-4D6E-8719-B9C84A01F043": {
      "mitigation_plugin_device_plain_text_label": "ASA : 10.1.1.1;
Group: asds",
      "host_name": "1.1.1.1",
      "mitigate_type": "ASA",
      "report_group": "auto-mitigation",

```

```
    "report_id": "4F12B367-5983-4D6E-8719-B9C84A01F043"
  },
  "status": 0
}
```

get_unchecked_exposures

This API retrieves a list of infections that have not yet been verified..

The API for unverified infection retrieval is as follows:

https://HOST/admin/api.php?op=get_unchecked_exposures

No parameters are required.

Example

```
curl -k -v -b "Authorization:7c71c218662411a5c857042053acca8f"
"https://10.2.2.2/admin/api.php?op=get_unchecked_exposures"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Output

```
{
  "unchecked_array": [
    {
      "endpoint_ip": "10.1.1.20",
      "malware_name": "SUSP_KRADDARE.DC",
      "malware_severity": "0.25",
      "event_id": "19",
      "capture_time": "2016-06-16 07:14:07.152759+00"
    },
    {
      "endpoint_ip": "10.1.1.38",
      "malware_name": "TROJAN_GIPPERS.DC",
      "malware_severity": "0.75",
      "event_id": "22",
      "capture_time": "2016-06-16 07:14:26.152144+00"
    },
    {
      "endpoint_ip": "10.1.1.24",
      "malware_name": "TROJAN_GIPPERS.DC",
      "malware_severity": "0.75",
      "event_id": "18",

```

```
    "capture_time": "2016-06-16 07:14:07.932812+00"
  },
  {
    "endpoint_ip": "10.1.1.40",
    "malware_name": "TROJAN_ORSAM.DC",
    "malware_severity": "0.75",
    "event_id": "24",
    "capture_time": "2016-06-16 07:14:30.951377+00"
  },
  {
    "endpoint_ip": "10.1.1.2",
    "malware_name": "TROJAN_PHDET.DC",
    "malware_severity": "0.75",
    "event_id": "17",
    "capture_time": "2016-06-16 07:14:03.24189+00"
  },
  {
    "endpoint_ip": "10.1.1.26",
    "malware_name": "TROJAN_GIPPERS.DC",
    "malware_severity": "0.75",
    "event_id": "21",
    "capture_time": "2016-06-16 07:14:15.332106+00"
  },
  {
    "endpoint_ip": "10.1.1.44",
    "malware_name": "TROJAN_FAREIT.DC",
    "malware_severity": "1.0",
    "event_id": "23",
    "capture_time": "2016-06-16 07:14:31.890184+00"
  }
],
"session_timeout_sec": 900,
"status": 0
}
```

get_users

This API retrieves current user profiles.

The API for user profile retrieval is as follows (there are no required parameters):

https://HOST/admin/api.php?op=get_users

The response includes:

```
user_id
user_name
user_fullname
api_key
```

```
api_key_is_disabled [status]  
role_array
```

Example

```
curl -k -v -b "Authorization:7c71c218662411a5c857042053acca8f"  
"https://10.2.2.2/admin/api.php?op=get_users"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Output

```
{  
  "user_table": {  
    "2d9d5a23-a309-0a09-2dfa-4585b2e5f851": {  
      "user_id": "2d9d5a23-a309-0a09-2dfa-4585b2e5f851",  
      "user_name": "admin",  
      "user_fullname": "View Admin",  
      "api_key": "2af0de6832dc43d8a1a347ee8ad93f97",  
      "api_key_is_disabled": 0,  
      "role_array": [  
        0,  
        1,  
        2,  
        3  
      ]  
    },  
    "9cd3e22f-aeff-0f16-7516-2bd2c449bc8b": {  
      "user_id": "9cd3e22f-aeff-0f16-7516-2bd2c449bc8b",  
      "user_name": "fhe",  
      "user_fullname": "Frank He",  
      "api_key": "56030ac8f0c74a8f32068d0e61094757",  
      "api_key_is_disabled": 0,  
      "role_array": [  
        0,  
        1,  
        2  
      ]  
    },  
    "f4b41198-6202-0a77-fd4e-4da1d3fb6a90": {  
      "user_id": "f4b41198-6202-0a77-fd4e-4da1d3fb6a90",  
      "user_name": "kalyan",  
      "user_fullname": "Kalyan",  
      "api_key": null,  
      "api_key_is_disabled": 0,  
      "role_array": [  
        0,  
        1,  
        2,  
      ]  
    }  
  }  
}
```



```

        3
    ]
},
"b11c3213-df11-0eb6-dd6e-786079c97958": {
    "user_id": "b11c3213-df11-0eb6-dd6e-786079c97958",
    "user_name": "temp",
    "user_fullname": "temp",
    "api_key": "ef8327d6e8a423193bbc214125278442",
    "api_key_is_disabled": 0,
    "role_array": [
        0,
        1,
        2
    ]
}
},
"session_timeout_sec": 36000,
"status": 0
}

```

get_whitelist_rules

Use this API to retrieve all configured whitelist rules.

https://<Host>/admin/api.php?op=get_whitelist_rules

<Host> - the IP Address of the device

HTTP Post Parameters	Description
type	[optional] Specifies the type; possible value "incident"

An example follows.

Example

```

curl -k -H "Authorization:7c71c218662411a5c857042053acca8f" "https://
10.2.20.37/admin/api.php?op=get_whitelist_rules" --data
"type=incident"

```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

```

{
    "content": [
        {

```

```

        "name": "rr",
        "uri": "http:\\\\greatfilesarey.asia\\shivaram\\vt\\
intelligencefiles\\Archive.zip",
        "src_ip": "65.1.1.2",
        "host": "greatfilesarey.asia",
        "dst_ip": "65.1.1.1",
        "shalsum": "a0bd2ee698848dc40f41ce593c9668ccf7dd1993"
    },
    {
        "name": "are",
        "uri": "http:\\\\greatfilesarey.asia\\shivaram\\vt\\
intelligencefiles\\Archive.zip",
        "src_ip": "65.1.1.2",
        "host": "greatfilesarey.asia",
        "dst_ip": "65.1.1.1",
        "shalsum": "bf36eed9c2ff4d907d5a72e6c96ade0e59ef8623"
    }
],
"status_detail": "",
"status_string": "Currently configured rules",
"success": 1,
"error": 0,
"session_timeout_sec": 900,
"status": 0
}

```

get_zones

Use this API to retrieve all MSSP tenant-specific “zones” information.

https://<Host>/admin/api.php?op=get_zones

<Host> - the IP Address of the device

HTTP Post Parameters	Description
type	[optional] Specifies the type; possible value “incident”

An example follows.

Example

```
curl -k -H "Authorization:7c71c218662411a5c857042053acca8f" "https://
10.1.1.1/admin/api.php?op=get_zones"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

```
{
  "content": [
```

history_details

Retrieve detection history for a given SHA1 SUM hash.

See also [incident_details](#); [incidents](#); [add_incident_comments](#)

https://<Host>/admin/api.php?op=history_details

<Host> - the IP Address of the device

HTTP Post Parameters	Description
sha1sum	SHA1 SUM hash

An example follows.

Example

```
curl "https://localhost/admin/api.php?op=history_details" --data
"sha1sum=4a44203b88d1936f8774619d7d5fccba8922ee0"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

```
{
  "history_details": [
    {
      "hre_donetime": "2016-06-06 11:23:26.986239+00",
      "hre_reputation_score": "41",
      "hre_is_malware": "t",
      "hre_classname": "malware",
      "hre_results": "ANALYZED",
```

```

        "hre_malware_category": "Trojan_Generic",
        "malware_name": "TROJAN_MALEX.DC",
        "hre_severity": "0.75"
    }
],
    "session_timeout_sec": 900,
    "status": 0
}

```

incident_comments

Retrieve incident comments associated with an incident.

See also [incident_details](#); [incidents](#); [add incident comments](#)

https://<Host>/admin/api.php?op=incident_comments

<Host> - the IP Address of the device

HTTP Post Parameters	Description
incident_id	ID of the incident for which comments are to be retrieved.

An example follows.

Example

```
curl "https://localhost/admin/api.php?op=incident_comments" --data
"incident_id=1031"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

```

{
    "incident_comments": {
        "comments_array": [
            {
                "user_ack_status": "new",
                "comments": "Event 1759 was added to this incident",
                "create_time": "2016-06-25 09:54:40.345961+00",
                "user_id": null,
            }
        ]
    }
}

```

```

        "user_name": null
    }
]
},
"session_timeout_sec": 36000,
"status": 0
}

```

incidents

Retrieving incidents from a Juniper ATP Appliance. Use this API to retrieve incidents from the Central Manager.
[incident comments](#); [add incident comments](#)

```

curl "https://localhost/admin/api.php?op=incidents" -k -H
"Authorization:d5d0e4e71c9ab6d7bfa8fff4dab341a5" --data
"max_results=500&end_time_sec=0&interval_sec=2592000&min_risk_value=0
&max_risk_value=1&collector_id=aaaa-bbbb-cccc-ddddd"

```

<Host> - the IP Address of the device

The current release includes the following changes:

- App_protocol_array uses "LOG" as the protocol in addition to other protocols in the incident. And collector_id_array will have UUID of the third party ingestion collector, as in:

```
"collector_id_array": ["LOG","HTTP"]
```

```

curl 'https://10.2.25.24/admin/api.php?op=incidents' -H 'Host:
10.2.25.24' -H "Authorization:fb4f4fff2841a784fb21aa864af5e8fa" --
insecure | json_pp

```

HTTP Post Parameters	Description
collector_id	[optional] ID of the Collector that processed the malicious traffic; can include LOG or Protocol
endpoint_id	Identification of the endpoint(s) in an array contained in square brackets [].
end_time_sec	[optional] The UTC timestamp of the end of the time frame of interest.
export_csv	[optional] Displays the incident report in comma separated values (CSV) format: 0 indicates no CSV export; 1 indicates export CSV.
filetype_value	[optional] The file type of interest: exe, pdf, dll

geo_value	[optional] A two-letter country code representing the threat source.
interval_sec	[required] The number of seconds in the time frame of interest, ending in "end_time_sec"
local_ip_value	[optional] IP address of the threat target.
malwarename_value	[optional] The name of the detected malware.
max_results	[optional] The maximum number of results to return.
max_risk_value	[required] maximum risk of the events of interest, range 0-1; see explanation of min_risk_value for details.
min_risk_value	<p>[optional] The minimum risk of the events of interest, which ranges from 0 to 1, where 0 indicates a benign event and 1 indicates the highest risk.</p> <p>The query will return all events greater or equal to the given min_risk_value and strictly less than the max_risk_value except when the min_risk_value is 0 and/or the max_risk_value is 1, in which case all events with risk greater than zero and/or less than or equal to one will be returned.</p> <p>To return all benign events set both the min_risk_value and max_risk_value to zero.</p>
remote_ip_value	[optional] The IP address of the threat source.
threat_target	Identification of the targeted endpoint(s) in an array displayed in square brackets [].
zone_uuid	The tenant zone_uuid in the incident_array elements

NOTE If an exploit is present, the incident_details>exploit_array object displays a new attribute called dst_ip.

Examples follow.

Example 1

```
curl 'https://10.1.1.1/admin/api.php?op=incidents&zone_uuid=D4636024-8E9B-4B8E-9095-D693716B583E' -H 'Host: 10.1.1.1' -H "Authorization:ae5bab7c3a2241a89a435d3671e29f92" --insecure
```

The response of op=incidents will have the tenant zone_uuid in the incident_array elements.

Zone_uuid can be passed to op=incidents API to fetch incidents from a particular zone. If zone_uuid is not passed, incidents from all zones are retrieved. If a zone is not configured, the default zone UUID of '00000000-0000-0000-0000-000000000000' is returned.

Example 2

```
curl "https://localhost/admin/api.php?op=incidents" --data "max_results=500&end_time_sec=0&interval_sec=2592000&min_risk_value=0"
```

```
&max_risk_value=1&collector_id=aaaa-bbbb-cccc-ddddd"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

```
{
  first_dummy_value: 0
  incident_array:
  [
    2]
    0:
    {
      incident_id: "175"
      incident_risk: "0.75000000000000000000"
      incident_category: "Worm"
      incident_name: "WORM_BRONTOK@MM.DC"
      incident_severity: "0.75"
      incident_relevance: "1.0"
      last_activity_time: "2016-06-01 08:11:48.921628+00"
      endpoint_ip: "172.16.0.2"
      endpoint_name: "172.16.0.2"
      endpoint_value: "0.75"
      endpoint_os_type: null
      source_ip: "172.16.0.1"
      source_name: "greatfilesarey.asia"
      source_country_code: null
      source_country_name: null
      has_valid_av: null
      has_os_match: null
      has_exploit: "0"
      has_download: "1"
      has_phishing: "1"
      has_execution: "0"
      has_infection: "0"
      has_data_theft: "0"
      has_file_submission: "0"
```

```

        collector_id: "03020100-0504-0706-0809-0a0b0c0d0e0f"
        collector_type: null
        search_data: "greatfilesarey.asia 172.16.0.2
172.16.0.1 159c01d7bc1f99bcb5caf0783e2f18e Worm
WORM_BRONTOK@MM.DC
08b7111f46244377eeb208a2356da9fef85abeba6
8d94aa3e984faa3e9c08592 03020100-0504-
0706-0809-0a0b0c0d0e0f http://greatfilesarey.asia/
malware_vault/malware/newton_qa/file_samples/
malware_exe/WL-ff165005bce579a24beb91b6253d21d3-0
ecb21879d091b6a990c0ea60f8b22b2fd13c43ac"
        search_collector_id: "03020100-0504-0706-0809-
0a0b0c0d0e0f"
    }
-
1:
{
    incident_id: "176"
    incident_risk: "0.75000000000000000000"
    incident_category: "Trojan_Generic"
    incident_name: "WORM_GAMARUE.CY"
    incident_severity: "0.75"
    incident_relevance: "1.0"
    last_activity_time: "2016-06-01 08:12:17.618365+00"
    "collector_id_array": ["00000000-0000-0000-0000-
000000000001"],
    endpoint_ip: null
    endpoint_name: null
    endpoint_value: "0.75"
    endpoint_os_type: null
    "endpoint_hostname": "emailuser-host",
    "endpoint_username": "emailuser",
    "endpoint_id": "{user5@biz_central.com}",
    "source_email_id": "user6@biz_central.com",
    "destination_email_id": "user5@biz_central.com",
    "source_hostname": null,
    "source_id": "user6@biz_central.com",
    "source_username": null,
    "app_protocol_array": ["EMAIL"],

```



```
        "threat_target": "{switch-54.corp.com.}",
        "threat_source": "newcard.dyndns.biz"
        source_ip: null
        source_name: "User Uploaded"
        source_country_code: null
        source_country_name: null
        has_valid_av: null
        has_os_match: null
        has_exploit: "0"
        has_download: "0"
        has_phishing: "1"
        has_execution: "0"
        has_infection: "0"
        has_data_theft: "0"
        has_file_submission: "1"
        collector_id: "00000000-0000-0000-0000-000000000002"
        collector_type: null

        search_data: "a0bd2ee698848dc40f41ce593c9668ccf7dd1993
340c860492c5ee5f708dfec57f650cd3 Trojan_Generic
e482ea7bdbfd42dbf1c33cb0b4a57920f40
e8ccba52a8ba57cf6191700fb6751 WORM_GAMARUE.CY"
        search_collector_id: "00000000-0000-0000-0000-
000000000002"
    }
-
-
total_incidents: 2
session_timeout_sec: 31536000
user_ack_status: 0
server_ip: "10.2.20.37"
server_name: "10.2.20.37"
status_fc_on: 1
status_sigeng_on: 1
status_hre_on: 1
status_sc_on: 1
status_correlation_on: 1
status_internet_on: 1
```

```

    status_mode: 0
    "status_downstream_web_collector": 1,
    "status_downstream_slave_core": 0
  }

```

A Sample Response Showing Endpoint Identity

```

{
  "has_phishing": "1",
  "collector_id_array": [
    "00000000-0000-0000-0000-000000000001"
  ],
  "endpoint_hostname": "emailuser-host",
  "endpoint_username": "emailuser",
  "endpoint_id": "[central_user5@JATP_central.eng.JATP.net]",
  "source_email_id": "central_user6@JATP_central.eng.JATP.net",
  "destination_email_id": "central_user5@JATP_central.eng.JATP.net",
  "source_hostname": null,
  "source_id": "central_user6@JATP_central.eng.JATP.net",
  "source_username": null,
  "app_protocol_array": [
    "EMAIL"
  ],
  "threat_target": "[switch-54.corp.JATP.net.]",
  "threat_source": "newcard.dyndns.biz"
}

```

A Sample Response for an HTTP Download

```

{"incident_id":"233","incident_risk":"0.750","incident_category":"Trojan_Generic","incident_name":"Trojan_Generic.DC","incident_severity":"0.75","incident_relevance":"1.0","last_activity_time":"2016-06-03 06:37:15.816192+00","endpoint_ip":"10.2.11.74","endpoint_name":"eng-dhcp-10-2-11-74.eng.JATP.net","endpoint_value":"0.5","endpoint_os_type":"windows","source_ip":"172.16.0.1","source_name":"greatfilesarey.asia","source_count_ry_code":null,"source_country_name":null,"has_valid_av":null,"has_os_match":"1","has_exploit":"0","has_download":"1","has_execution":"0","has_infection":"0","has_data_theft":"0","has_file_submission":"0","has_lateral":"0","has_phishing":"1","collector_id_array":["421ef5fb-9d57-5f23-261b-d51458356fa6"],"collector_type":null,"search_data":"http://greatfilesarey.asia/QA/files_to_pcaps/79ea1163c0844a2d2b6884a31fc32cc4.bin tomhanks greatfilesarey.asia 172.16.0.1 acf69d292d2928c5ddfe5e6af562cd482e6812dc 421ef5fb-9d57-5f23-261b-d51458356fa6 79ea1163c0844a2d2b6884a31fc32cc4 0d694aa0c12f7a11b6ce29eaf17173c8f0acb168de4738f633db8eca46c3885d Trojan_Generic.DC UIAUTO1 Trojan_Generic 10.2.11.74","search_collector_id":"421ef5fb-9d57-5f23-261b-d51458356fa6","user_ack_status":"new","endpoint_hostname":"UIAUTO1","end

```

```
point_username":"tomhanks","endpoint_id":["UIAUTO1"],"source_email_id":null,"destination_email_id":[""],"source_hostname":null,"source_id":"172.16.0.1","source_username":null,"threat_target":["UIAUTO1"],"threat_source":"greatfilesarey.asia","app_protocol_array":["HTTP"]}
```

A Sample Response for a Phishing Email:

```
{"incident_id":"234","incident_risk":"0.750","incident_category":null,"incident_name":"Phishing","incident_severity":"0.75","incident_relevance":"1.0","last_activity_time":"2016-06-03 06:33:39+00","endpoint_ip":null,"endpoint_name":null,"endpoint_value":"0.5","endpoint_os_type":null,"source_ip":null,"source_name":null,"source_country_code":null,"source_country_name":null,"has_valid_av":null,"has_os_match":null,"has_exploit":"0","has_download":"0","has_execution":"0","has_infection":"0","has_data_theft":"0","has_file_submission":"0","has_lateral":"0","has_phishing":"1","collector_id_array":["00000000-0000-0000-0000-000000000001"],"collector_type":null,"search_data":"http:\\\\greatfilesarey.asia\\QA\\files_to_pcaps\\79ea1163c0844a2d2b6884a31fc32cc4.bin xyz@gmail.com abc@gmail.com","search_collector_id":"00000000-0000-0000-0000-000000000001","user_ack_status":"new","endpoint_hostname":null,"endpoint_username":null,"endpoint_id":["abc@gmail.com"],"source_email_id":"xyz@gmail.com","destination_email_id":["abc@gmail.com"],"source_hostname":null,"source_id":"xyz@gmail.com","source_username":null,"threat_target":["abc@gmail.com"],"threat_source":"xyz@gmail.com","app_protocol_array":["EMAIL"]}
```

A Sample Response for a Lateral Detection

```
{"incident_id":"235","incident_risk":"0.250","incident_category":"Trojan_Generic","incident_name":"Njrat","incident_severity":"0.2","incident_relevance":"1.0","last_activity_time":"2016-06-03 08:35:01.948034+00","endpoint_ip":"192.168.2.69","endpoint_name":"192.168.2.69","endpoint_value":"0.5","endpoint_os_type":null,"source_ip":"192.168.2.23","source_name":null,"source_country_code":null,"source_country_name":null,"has_valid_av":null,"has_os_match":null,"has_exploit":"0","has_download":"1","has_execution":"0","has_infection":"0","has_data_theft":"0","has_file_submission":"0","has_lateral":"1","has_phishing":null,"collector_id_array":["421ef5fb-9d57-5f23-261b-d51458356fa6"],"collector_type":null,"search_data":"192.168.2.23 \\\\192.168.2.23\\d$\\SMB_sample_Raghav_dot_net 87f7cbd6db62bdc55ddee57a106508a9 421ef5fb-9d57-5f23-261b-d51458356fa6 192.168.2.69 Njrat e8e173b4eebae4a2bc2f49819e71349df373cf9ecd3b338ff6c28cc91632bb2b 0a63ebf67461f81616851bf2407d3c5b2ce75647 Trojan_Generic","search_collector_id":"421ef5fb-9d57-5f23-261b-d51458356fa6","user_ack_status":"new","endpoint_hostname":null,"endpoint_username":null,"endpoint_id":["192.168.2.69"],"source_email_id":null,"destination_email_id":[""],"source_hostname":null,"source_id":"192.168.2.23","source_username":null,"threat_target":["192.168.2.69"],"threat_source":"192.168.2.23","app_protocol_array":["SMB"]}
```

incident_details

Retrieving details of an Incident in Juniper ATP Appliance.

Use this API function to retrieve incident details from the Juniper ATP Appliance threat detection system, including OS changes such as mutexes, process starts or registry changes associated with a file object.

The API for incident detail retrieval is as follows:

https://<HOST>/admin/api.php?op=incident_details

<HOST> - The IP address of the Juniper ATP Appliance.

HTTP Post Parameters	Description
incident_id	[required] The ID set for the incident during malware analysis; get this ID in the output of API <a href="https://<Host>/admin/api.php?op=incidents">https://<Host>/admin/api.php?op=incidents
zone_uuid	The tenant zone_uuid in the incident_array elements

The response of op=incident_details will have the tenant zone_uuid in the incident_array elements.

Zone_uuid can be passed to the op=incident_details API to fetch incident details from a particular zone. If zone_uuid is not passed, incidents from all zones are retrieved. If a zone is not configured, the default zone UUID of '00000000-0000-0000-0000-000000000000' is returned.

Example

```
curl -k -H "Authorization:7c71c218662411a5c857042053acca8f" "https://10.2.20.37/admin/api.php?op=incident_details" -d incident_id=142
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

A new field third_party_event_array lists all third party events correlated as part of the incident.

Example

```
[
  {
    "event_type": "third_party",
    "event_category": null,
    "event_name": "Execution",
    "event_severity": "0.25",
    "endpoint_ip": null,
    "endpoint_name": null,
    "endpoint_os_type": null,
    "endpoint_hostname": "TEST-2F0DDD7E5F",
```

```

"endpoint_username": null,
"last_activity_time": "2017-05-31 08:27:27+00",
"last_activity_time_epoch": "1496219247",
"source_ip": null,
"third_party_info": {
  "device_host": "cbtest",
  "raw":
    "{ \"alert_severity\": \"67.5\", \"alert_type\": \"watchlist.hit.ingress.
process\", \"cb_server\": \"cbserver\", \"childproc_count\": \"0\", \"comm
s_ip\": \"10.7.1.234\", \"computer_name\": \"TEST-
2F0DDD7E5F\", \"created_time\": \"2017-05-
31T08:27:12.790080Z\", \"crossproc_count\": \"0\", \"feed_id\": \"4\", \"f
eed_name\": \"virustotal\", \"feed_rating\": \"3.0\", \"filemod_count\": \"
0\", \"group\": \"Default Group\", \"hostname\": \"TEST-
2F0DDD7E5F\", \"interface_ip\": \"0.0.0.0\", \"ioc_confidence\": \"0.5\",
\"ioc_type\": \"md5\", \"ioc_value\": \"23f3b2b0f5840dfaa8abd35655658828
\", \"ioc_value_facet\": \"23f3b2b0f5840dfaa8abd35655658828\", \"md5\": \"
23F3B2B0F5840DFAA8ABD35655658828\", \"modload_count\": \"25\", \"netcon
n_count\": \"0\", \"os_type\": \"windows\", \"process_guid\": \"00000006-
0000-6968-01d2-d9e71d94425a\", \"process_id\": \"00000006-0000-6968-
01d2-d9e71d94425a\", \"process_name\": \"plus-hd-9.6-
nova.exe\", \"process_path\": \"c:\\\\program files\\\\plus-hd-
9.6\\\\plus-hd-9.6-
nova.exe\", \"regmod_count\": \"6\", \"report_score\": \"100\", \"segment_
id\": \"1\", \"sensor_criticality\": \"3.0\", \"sensor_id\": \"6\", \"statu
s\": \"Unresolved\", \"timestamp\": 1496219247.822, \"type\": \"alert.watc
hlist.hit.ingress.process\", \"unique_id\": \"e1244756-6312-4b4f-be84-
3b9788d6c111\", \"username\": \"SYSTEM\", \"watchlist_id\": \"23f3b2b0f58
40dfaa8abd35655658828\", \"watchlist_name\": \"23f3b2b0f5840dfaa8abd356
55658828\" }",
  "severity": "high"
},
"vendor_product": "carbon_black",
"action_response": "allowed",
"event_action": "Execution",
"detection_method": "alert.watchlist.hit.ingress.process",
"event_signature": null,
"device_host": "cbtest"
}
]

```

Optional Curl Command Options:

```

curl 'https://10.2.25.24/admin/api.php?op=incident_details' --data
'incident_uuid=515e2faa-d57c-40ce-abca-7be0b13e5987' -H 'Host:

```

```
10.2.25.24' -H "Authorization:fb4f4fff2841a784fb21aa864af5e8fa" --insecure | json_pp
```

Or

```
curl 'https://10.2.25.24/admin/api.php?op=incident_details&incident_uuid=515e2faa-d57c-40ce-abca-7be0b13e5987' -H 'Host: 10.2.25.24' -H "Authorization:fb4f4fff2841a784fb21aa864af5e8fa" --insecure | json_pp
```

Or

```
curl 'https://10.2.25.24/admin/api.php?op=incident_details&incident_id=6094' -H 'Host: 10.2.25.24' -H "Authorization:fb4f4fff2841a784fb21aa864af5e8fa" --insecure | json_pp
```

In the above examples, the first curl command sends the incident_uuid as post param and in the next two examples it is sent as a get parameter. You can pass incident_id or incident_uuid. Incident_uuid is suggested.

Sample Outputs

Several samples are provided below:

- [Sample Response for a Phishing Event on page 138](#)
- [Sample STIX Data for an Email Event on page 116](#)
- [Sample Response for an SMB Lateral Detection on page 139](#)
- [Sample Incident Details for an Exploit on page 142](#)
- [Sample Incident Details with YARA Rule Matching on page 145](#)

Sample Response for a Phishing Event

Sample output for an incident with Phishing detection:

Apart from the above new keys, phishing_array has been introduced in this API

```
{
  "phishing_array": [{
    "metadata_array": [{
      "destination_email_id": "{central_user5@central.JATP.net}",
      "Email_msg_id" :
      "<CAK9CQGcUhnjFuOPZhye94=F3r5d=0Sxz2kX27XBYLMPdQ8VHPw@mail.gmail.com>"
      "source_email_id": "central_user6@biz_central.JATP.net",
      "email_recv_time": "2016-04-07 22:45:59+00",
```

```

    "event_id": "729",
    "event_severity": "0.75",
    "url_array": [{
      "url": "http://google.com/74280968a4917.bin",
      "description" : "Downloads Sha1:
acf69d292d2928c5ddfe5e6af562cd482e6812dc"
      "url_severity": null
    }]
  }]
}],
}

```

Sample Response for an SMB Lateral Detection

Sample output for an incident with SMB lateral detection:

```

{
  "fsp_array": [
    {
      "event_id": "36",
      "has_execution": "0",
      "app_protocol": "SMB",
      "capture_time_string": "2016-06-05 09:46:15.11862+00",
      "endpoint_ip": "192.168.2.69",
      "endpoint_name": null,
      "source_ip": "192.168.2.23",
      "source_name": null,
      "source_url":
"\\\\"192.168.2.23\\d\$\\SMB sample Raghav dot net",
      "client_os": null,
      "appliance_id": "03aa02fc-0414-05e3-3406-920700080009",
      "country_code": null,
      "country_name": null,
      "sha1sum": "0a63ebf67461f81616851bf2407d3c5b2ce75647",
      "md5sum": "87f7cbd6db62bdc55ddee57a106508a9",
      "sha256sum":
      "e8e173b4eebae4a2bc2f49819e71349df373cf9ecd3b338ff6c28cc91632bb2b",
      "file_type": "PE32 executable (GUI) Intel 80386 Mono/.Net
assembly, for MS Windows",
    }
  ]
}

```

```
"local_path": "/var/spool/c-icap/download/CI_TMPvd6nzP",
"file_md5_string": "87f7cbd6db62bdc55ddee57a106508a9",
"file_sha1_string": "0a63ebf67461f81616851bf2407d3c5b2ce75647",
"file_sha256_string":
"e8e173b4eebae4a2bc2f49819e71349df373cf9ecd3b338ff6c28cc91632bb2b",
"file_size": "9867264",
"file_type_string": "PE32 executable (GUI) Intel 80386 Mono/
.Net assembly, for MS Windows",
"file_suffix": "exe",
"mime_type_string": "N/A",
"has_components": null,
"packer_name": null,
"malware_name": "TROJAN_BLADABINDI.CY",
"malware_severity": "0.75",
"malware_category": "Trojan_Generic",
"malware_classname": "malware",
"has_static_detection": "1",
"has_behavioral_detection": null,
"has_reputation_detection": "1",
"has_embedded_code": null,
"has_cnc": null,
"dig_cert_name": null,
"dig_cert_override": null,
"has_yara_match": null,
"pcap_size": null,
"analysis_start_time": "2016-06-05 09:46:18.056625+00",
"analysis_done_time": "2016-06-05 09:47:02.333223+00",
"source_url_rank": "-1",
"reputation_score": "22",
"microsoft_name": "Backdoor:MSIL/Bladabindi.AP",
"has_behavior_log": null,
"custom_image_array": [],
"yara_rule_array": []
}
],
"lateral_array":[
{
```



```
"event_id":"35",
"event_type":"fsp",
"event_category":"Trojan_Generic",
"event_name":"TROJAN_BLADABINDI.CY",
"event_severity":"0.75",
"endpoint_ip":"192.168.2.70",
"endpoint_name":"192.168.2.70",
"endpoint_os_type":"null",
"source_ip":"192.168.2.69",
"source_name":"null",
"source_country_code":"null",
"source_uri":"null",
"collector_id":"03aa02fc-0414-05e3-3406-920700080009",
"event_start_time":"2016-06-05 09:46:23.658417+00",
"last_activity_time":"2016-06-05 09:46:23.658417+00",
"incident_id":"15",
"incident_risk":"0.750",
"event_status":"done",
"event_processed_time":"2016-06-06 09:53:40.036999+00",
"dependent_done_time":"2016-06-06 09:53:39.78763+00",
"initial_done_time":"2016-06-05 09:47:03.329563+00",
"analysis_done_time":"2016-06-05 09:47:03.329563+00",
"event_relevance":"1.0",
"search_data":"03aa02fc-0414-05e3-3406-920700080009
TROJAN_BLADABINDI.CY 87f7cbd6db62bdc55ddee57a106508a9
\\\\\\192.168.2.69\\\\d$\\\\SMB sample Raghav dot net 192.168.2.69
0a63ebf67461f81616851bf2407d3c5b2ce75647 192.168.2.70
e8e173b4eebae4a2bc2f49819e71349df373cf9ecd3b338ff6c28cc91632bb2b
Trojan_Generic",
"has_valid_av":"null",
"has_os_match":"null",
"custom_img_infected":"null",
"has_execution":"f",
"whitelisted":"f"
}
]
}
```

Sample Incident Details for an Exploit

Sample output for an incident with exploit:

```
{
  "incident_details": {
    "incident_id": "501",
    "incident_risk": "0.250",
    "incident_category": null,
    "incident_name": "Exploit",
    "incident_severity": "0.25",
    "incident_relevance": "1.0",
    "last_activity_time": "2016-02-03 04:56:26.347902+00",
    "endpoint_ip": "192.168.50.203",
    "endpoint_name": "192.168.50.203",
    "endpoint_value": "0.5",
    "endpoint_os_type": "windows",
    "source_ip": "64.202.116.124",
    "source_name": null,
    "source_country_code": "US",
    "source_country_name": "USA",
    "has_valid_av": null,
    "has_os_match": null,
    "has_exploit": "1",
    "has_download": "0",
    "has_execution": "0",
    "has_infection": "0",
    "has_data_theft": "0",
    "has_file_submission": "0",
    "collector_id": "4c4c4544-0036-3010-8035-c3c04f465831",
    "collector_type": null,
    "search_data": "64.202.116.124 Exploit 192.168.50.203 4c4c4544-0036-3010-8035-c3c04f465831",
    "search_collector_id": "4c4c4544-0036-3010-8035-c3c04f465831",
    "exploit_array": [
      {
```

```

    "req_referer": "http://www.christianforums.com/",
    "mime_uri": "http://64.202.116.124/5butqfk/?2",
    "timestamp": "2016-02-03 04:56:26.347902+00",
    "event_description": "Suspicious download sequence and
Shellcode",
    "chain_id": "0219e8d6-ab61-11e4-9a69-90b11c46a0fd",
    "dst_ip": "64.202.116.124",
    "chain_array": [
        {
            "req_referer": "http://www.christianforums.com/",
            "mime_uri": "http://64.202.116.124/5butqfk/?2",
            "timestamp": "2016-02-03 04:56:26.347902+00",
            "event_id": "1468",
            "req_headers": "{\"Host\": \"czipso.in.ua\", \"Accept-
Language\": \"en-US\", \"Accept-Encoding\": \"gzip, deflate\",
\"Referer\": \"http://www.christianforums.com/\", \"Connection\":
\"Keep-Alive\", \"Accept\": \"application/x-ms-application, image/
jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-
xbap, */*\", \"User-Agent\": \"Mozilla/4.0 (compatible; MSIE 8.0;
Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET
CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\"}",
            "resp_headers": "{\"X-Powered-By\": \"PHP/5.3.27-
1~dotdeb.0\", \"Transfer-Encoding\": \"chunked\", \"Expires\": \"Mon,
26 Jul 1997 05:00:00 GMT\", \"Server\": \"nginx/1.4.4\", \"Last-
Modified\": \"Thu, 03 Apr 2016 18:48:24 GMT\", \"Pragma\": \"no-
cache\", \"Cache-Control\": \"no-store, no-cache, must-revalidate\",
\"Date\": \"Thu, 03 Apr 2016 18:48:24 GMT\", \"Content-Type\":
\"text/html\", \"Content-Encoding\": \"gzip\"}",
            "file_type": "HTML document, ASCII text, with very long
lines, with CRLF line terminators"
        },
        {
            "req_referer": "http://czipso.in.ua/5butqfk/?2",
            "mime_uri": "http://64.202.116.124/5butqfk/
?1a8c1e8d2aa9837a58045458035e0050095701580507085f04520b0750065e5c",
            "timestamp": "2016-02-03 04:56:26.349189+00",
            "event_id": "1466",
            "req_headers": "{\"Host\": \"czipso.in.ua\", \"Accept-
Language\": \"en-US\", \"Accept-Encoding\": \"gzip, deflate\",
\"Referer\": \"http://czipso.in.ua/5butqfk/?2\", \"Connection\":
\"Keep-Alive\", \"Accept\": \"application/x-ms-application, image/
jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-
xbap, */*\", \"User-Agent\": \"Mozilla/4.0 (compatible; MSIE 8.0;

```

```

Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET
CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\"}",

    "resp_headers": "{\"X-Powered-By\": \"PHP/5.3.27-
1~dotdeb.0\", \"Transfer-Encoding\": \"chunked\", \"Expires\": \"Mon,
26 Jul 1997 05:00:00 GMT\", \"Server\": \"nginx/1.4.4\", \"Last-
Modified\": \"Thu, 03 Apr 2016 18:48:28 GMT\", \"Pragma\": \"no-
cache\", \"Cache-Control\": \"no-store, no-cache, must-revalidate\",
\"Date\": \"Thu, 03 Apr 2016 18:48:28 GMT\", \"Content-Type\":
\"text/html\", \"Content-Encoding\": \"gzip\"}\",

    "file_type": "HTML document, ASCII text, with very long
lines, with CRLF line terminators"

},

{

    "req_referer": "<unknown>",

    "mime_uri": "http://64.202.116.124/5butqfk/
?2e8f5ae222a208fc5115535d075a5d060a53015d0103550907560b0254020351;5",

    "timestamp": "2016-02-03 04:56:26.351379+00",

    "event_id": "1467",

    "req_headers": "{\"Accept-Encoding\": \"gzip, deflate\",
\"Host\": \"czipso.in.ua\", \"Connection\": \"Keep-Alive\",
\"Accept\": \"*/*\", \"User-Agent\": \"Mozilla/4.0 (compatible; MSIE
8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727;
.NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\"}",

    "resp_headers": "{\"Date\": \"Thu, 03 Apr 2016 18:48:30
GMT\", \"Content-Length\": \"138357\", \"X-Powered-By\": \"PHP/
5.3.27-1~dotdeb.0\", \"Content-Type\": \"application/octet-stream\",
\"Server\": \"nginx/1.4.4\"}\",

    "file_type": "data"

},

{

    "req_referer": "<unknown>",

    "mime_uri": "http://64.202.116.124/5butqfk/
?2e8f5ae222a208fc5115535d075a5d060a53015d0103550907560b0254020351;5;1
",

    "timestamp": "2016-02-03 04:56:26.352701+00",

    "event_id": null,

    "req_headers": "{\"Accept-Encoding\": \"gzip, deflate\",
\"Host\": \"czipso.in.ua\", \"Connection\": \"Keep-Alive\",
\"Accept\": \"*/*\", \"User-Agent\": \"Mozilla/4.0 (compatible; MSIE
8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727;
.NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\"}",

    "resp_headers": "{\"Date\": \"Thu, 03 Apr 2016 18:48:34
GMT\", \"Content-Encoding\": \"gzip\", \"Transfer-Encoding\":
\"chunked\", \"X-Powered-By\": \"PHP/5.3.27-1~dotdeb.0\", \"Content-

```

```

Type\: \"text/html\", \"Server\: \"nginx/1.4.4\"}\",
      \"file_type\": null
    }
  ]
}
],
\"download_array\": [],
\"infection_array\": [],
\"second_order_array\": [],
\"file_submission_array\": [],
\"custom_image_array\": [],
\"snort_event_array\": []
},
\"session_timeout_sec\": 36000,
\"status\": 0
}

```

Sample Incident Details with YARA Rule Matching

Sample response for an incident with YARA rule matching ("yara_rule_array" has been added to the download_array). In this example, "has_yara_match": "1" and "yara_rule_array" are the sample values:

```

{
  \"download_array\": [
    {
      ...
      ...
      \"has_yara_match\": \"1\",
      \"yara_rule_array\": [
        {
          \"scan_time\": \"2016-06-02 23:56:21.990669\",
          \"rule_name\": \"mz_executable\",
          \"rule_severity\": null,
          \"rule_description\": null,
          \"rule_file_name\": \"Yara1.txt\"
        }
      ]
      ...
      ...
    }
  ]
}

```

```
}
```

ingestion_vendor_details

Use this API function to obtain log ingestion and event details per integrated vendor. This API returns all the ingestion vendors and various fields of ingested data supported by Juniper ATP Appliance. A typical response is provided below. Some of the fields are used by Juniper ATP Appliance for acquiring events information.

https://<HOST>/admin/api.php?op=ingestion_vendor_details

<HOST> - The IP address of the Juniper ATP Appliance.

See Also: [op=get_incident](#) | [op=incident_details](#) | [op=behavior_details](#)

Example

```
curl -k -H "Authorization:7c71c218662411a5c857042053acca8f" 'https://  
10.2.25.24/admin/api.php?op=ingestion_vendor_details' -H 'Host:  
10.2.25.24' -H "Authorization:fb4f4fff2841a784fb21aa864af5e8fa" --  
insecure | json_pp
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Output

```
{ "vendor_array" : [  
  {  
    "vendor_name": "bluecoat",  
    "vendor_display_name": "Bluecoat Secure Web Gateway",  
    "vendor_category": "web_gateway",  
    "require_exclusive_port": true,  
    "parser_config": {  
      "parse_actions": [  
        {  
          "type": "grok",  
          "config_file": "grok.conf"  
        },  
        {  
          "type": "filter"  
        },  
        {  
          "type": "normalize_field_names"
```

```

    },
    {
        "type": "normalize_field_values",
        "config_file": "normalize.yaml"
    },
    {
        "type": "format_field_values"
    }
],
"field_mappings": {
    "event_start_time": "record[\"date\"] + \"T\" +
record[\"timestamp\"] + \"Z\"",
    "endpoint_ip": "record[\"c_ip\"]",
    "source_ip": "record[\"s_ip\"]",
    "source_hostname": "record[\"cs_host\"]",
    "event_action": "\"Web\"",
    "detection_method": "record[\"category\"]",
    "is_blocked": "record[\"filter_result\"]",
    "action_response": "record[\"filter_result\"]",
    "third_party_info.web_url": "record[\"cs_uri_scheme\"] + \"://\" +
record[\"cs_host\"] + record[\"cs_uri_path\"]",
    "third_party_info.url_query": "record[\"cs_uri_query\"]",
    "third_party_info.http_content_type":
record[\"http_content_type\"],
    "third_party_info.http_referrer": "record[\"http_referrer\"]",
    "third_party_info.http_status": "record[\"sc_status\"]",
    "third_party_info.device_host": "record[\"host\"]"
},
"field_formats": {
    "event_start_time": {
        "type": "time"
    }
},
"filter": [
    {
        "rules": {
            "filter_result": ".*"
        }
    }
]

```

```
        },
        "excludes": {
            "filter_result": "DENIED"
        }
    }
]
}
,
{
    "vendor_name": "carbon_black",
    "vendor_display_name": "Carbon Black Response",
    "vendor_category": "etdr",
    "require_exclusive_port": true,
    "parser_config": {
        "parse_actions": [
            {
                "type": "json"
            },
            {
                "type": "filter"
            },
            {
                "type": "normalize_field_names"
            },
            {
                "type": "normalize_field_values",
                "config_file": "normalize.yaml"
            },
            {
                "type": "format_field_values"
            }
        ],
        "field_mappings": {
            "endpoint_ip": "record[\"interface_ip\"] if
record[\"interface_ip\"] != \"0.0.0.0\"",
```



```

"endpoint_hostname": [
    "record[\"hostname\"]",
    "record[\"computer_name\"]",
    "record[\"server_name\"]",
"endpoint_username": [
    "record[\"docs\"][0][\"username\"] if record[\"docs\"]",
    "record[\"username\"]"
],
"event_start_time": [
    "record[\"docs\"][0][\"start\"] if record[\"docs\"]",
    "record[\"docs\"][0][\"server_added_timestamp\"] if
record[\"docs\"]",
    "Time.at(record[\"timestamp\"]).to_s if
record[\"timestamp\"]",
"event_action": "record[\"type\"]",
"detection_method": "record[\"type\"]",
"is_blocked": "false",
"action_response": "\"allowed\"",
"third_party_info.device_host": "record[\"host\"]",
"third_party_info.file_path": [
    "record[\"docs\"][0][\"path\"] if record[\"docs\"]",
    "record[\"observed_filename\"][0] if
record[\"observed_filename\"]",
    "record[\"process_path\"]"
],
"third_party_info.file_name": [
    "record[\"docs\"][0][\"process_name\"] if
record[\"docs\"]",
    "record[\"process_name\"]"
],
"third_party_info.file_hash": [
    "record[\"docs\"][0][\"process_md5\"] if record[\"docs\"]",
    "record[\"md5\"]"
]
},
"field_formats": {
"event_start_time": {

```

```
        "type": "time"
    }
},
"filter": [
{
    "rules": {
        "type": ".*"
    },
    "excludes": {
        "type": "alert.*"
    }
}
]
}
}
,
{
    "vendor_name": "JATP",
    "vendor_display_name": "JATP",
    "vendor_category": "JATP",
    "parser_config": {
        "parse_actions": [
        ],
        "field_mappings": {
        },
        "filter": []
    }
}
,
{
    "vendor_name": "mcafee_epo",
    "vendor_display_name": "McAfee ePO",
    "vendor_category": "endpoint_av",
    "parser_config": {
        "parse_actions": [
        {
```

```
        "type": "xml"
    },
    {
        "type": "normalize_field_names"
    },
    {
        "type": "normalize_field_values",
        "config_file": "normalize.yaml"
    },
    {
        "type": "filter"
    },
    {
        "type": "format_field_values"
    }
],
"xml_mappings": [
    {
        "field": "message",
        "match": "<VirusDetectionEvent>",
        "mapping": {
            "is_valid": {
                "value_path": "VirusDetectionEvent/
ScannerSoftware/DetectionInfo/EventID"
            },
            "action_response": {
                "value_path": "VirusDetectionEvent/
ScannerSoftware/DetectionInfo/EventID"
            },
            "event_action": {
                "value_path": "VirusDetectionEvent/
ScannerSoftware/TaskName"
            },
            "detection_method": {
                "value_path": "VirusDetectionEvent/
ScannerSoftware/ProductName"
            }
        }
    },
```

```

        "third_party_info.file_name": {
            "value_path": "VirusDetectionEvent/
ScannerSoftware/DetectionInfo/FileName"
        },
        "third_party_info.file_hash": {
            "value_path": "VirusDetectionEvent/
ScannerSoftware/DetectionInfo/MD5"
        },
        "third_party_info.severity": {
            "value_path": "VirusDetectionEvent/
ScannerSoftware/DetectionInfo/Severity"
        },
        "event_start_time": {
            "value_path": "VirusDetectionEvent/
ScannerSoftware/DetectionInfo/UTCTime"
        },
        "endpoint_ip": {
            "value_path": "VirusDetectionEvent/MachineInfo/
IPAddress"
        },
        "endpoint_username": {
            "value_path": "VirusDetectionEvent/MachineInfo/
UserName"
        },
        "endpoint_hostname": {
            "value_path": "VirusDetectionEvent/MachineInfo/
MachineName"
        }
    },
    {
        "field": "message",
        "match": "<PortBlockEvent>",
        "mapping": {
            "is_valid": {
                "value_path": "PortBlockEvent/ScannerSoftware/
BlockedPortInfo/EventID"
            },
            "action_response": {

```

```

        "value_path": "PortBlockEvent/ScannerSoftware/
BlockedPortInfo/EventID"
    },
    "event_action": {
        "value_path": "PortBlockEvent/ScannerSoftware/
TaskName"
    },
    "detection_method": {
        "value_path": "PortBlockEvent/ScannerSoftware/
ProductName"
    },
    "third_party_info.file_name": {
        "value_path": "PortBlockEvent/ScannerSoftware/
BlockedPortInfo/ProcessName"
    },
    "third_party_info.severity": {
        "value_path": "PortBlockEvent/ScannerSoftware/
BlockedPortInfo/Severity"
    },
    "event_start_time": {
        "value_path": "PortBlockEvent/ScannerSoftware/
BlockedPortInfo/UTCTime"
    },
    "endpoint_ip": {
        "value_path": "PortBlockEvent/MachineInfo/
IPAddress"
    },
    "endpoint_username": {
        "value_path": "PortBlockEvent/MachineInfo/
UserName"
    },
    "endpoint_hostname": {
        "value_path": "PortBlockEvent/MachineInfo/
MachineName"
    }
}

],

```

```
"field_mappings": {
  "third_party_info.device_host": "record[\"host\"]",
  "event_start_time": "record[\"event_start_time\"] + \"Z\"",
  "is_blocked": "record[\"action_response\"]"
},
"field_formats": {
  "event_start_time": {
    "type": "time"
  }
},
"filter": [
{
  "rules": {
    "is_valid": "false"
  }
}
]
}
,
{
  "vendor_name": "pan",
  "vendor_display_name": "PAN Next Gen Firewall",
  "vendor_category": "ngfw",
  "parser_config": {
    "parse_actions": [
      {
        "type": "grok",
        "config_file": "trim_grok.conf"
      },
      {
        "type": "csv"
      },
      {
        "type": "filter"
      }
    ]
  }
}
```

```
{
  "type": "normalize_field_names"
},
{
  "type": "normalize_field_values",
  "config_file": "normalize.yaml"
},
{
  "type": "format_field_values"
}
],
"csv_mappings": [
  "future_use_1",
  "receive_time",
  "serial",
  "type",
  "subtype",
  "future_use_2",
  "gen_time",
  "source_ip",
  "endpoint_ip",
  "nat_source_ip",
  "nat_endpoint_ip",
  "rule_name",
  "source_username",
  "endpoint_username",
  "application",
  "virtual_system",
  "source_zone",
  "destination_zone",
  "ingress_ifc",
  "egress_ifc",
  "log_forwarding_profile",
  "future_use_3",
  "session_id",
  "repeat_cnt",
```

```
"source_port",
"endpoint_port",
"nat_source_port",
"nat_endpoint_port",
"flags",
"protocol",
"action",
"misc",
"threat_id",
"category",
"severity",
"direction",
"seq_num",
"action_flags",
"endpoint_loc",
"source_loc",
"future_use_4",
"content_type",
"pcap_id",
"filedigest",
"cloud",
"future_use_5",
"user_agent",
"file_type",
"xff",
"referrer",
"sender",
"subject",
"recipient",
"report_id"
],
"field_mappings": {
  "third_party_info.raw": "record[\"message\"]",
  "event_start_time": "record[\"receive_time\"]",
  "event_action": "\"Download\"",
  "detection_method": "record[\"rule_name\"]",
```



```
"is_blocked": "record[\"action\"]",
"action_response": "record[\"action\"]",
"third_party_info.http_content_type": "record[\"content_type\"]",
"third_party_info.http_referrer": "record[\"referrer\"]",
"third_party_info.severity": "record[\"severity\"]",
"third_party_info.file_name": "record[\"misc\"]",
"third_party_info.file_hash": "record[\"file_digest\"]"
},
"field_formats": {
"event_start_time": {
    "type": "time"
}
},
"filter": [
{
    "rules": {
        "type": ".*"
    },
    "excludes": {
        "type": "THREAT"
    }
},
{
    "rules": {
        "severity": "informational"
    }
},
{
    "rules": {
        "action": "wildfire-upload-success|wildfire-upload-
skip|forward"
    }
}
]
}
```

```
,
{
  "vendor_name": "symantec_ep",
  "vendor_display_name": "Symantec EP",
  "vendor_category": "endpoint_av",
  "parser_config": {
    "parse_actions": [
      {
        "type": "grok",
        "config_file": "trim_grok.conf"
      },
      {
        "type": "grok",
        "config_file": "grok.conf"
      },
      {
        "type": "filter"
      },
      {
        "type": "normalize_field_names"
      },
      {
        "type": "normalize_field_values",
        "config_file": "normalize.yaml"
      },
      {
        "type": "format_field_values"
      }
    ],
    "field_mappings": {
      "third_party_info.raw": "record[\"message\"]",
      "action_response": "record[\"actual_action\"]",
      "is_blocked": "record[\"actual_action\"]",
      "event_action": "\"Virus Scan\"",
      "detection_method": "record[\"action\"]",
      "third_party_info.file_path": "record[\"file_path\"]",
```

```
    "third_party_info.file_name": "record[\"file_name\"]",
    "third_party_info.file_hash": "record[\"file_hash\"]"
  },
  "field_formats": {
    "event_start_time": {
      "type": "time"
    }
  },
  "filter": [
    {
      "rules": {
        "type": ".*"
      },
      "excludes": {
        "type": "Virus.*"
      }
    }
  ]
},
"status" : 0
, "session_timeout_sec" : 36000
, "server_ip" : "10.2.25.24"
, "server_name" : "10.2.25.24"
, "max_cook_size" : 15000001
, "status_fc_on" : 0
, "status_sigeng_on" : 1
, "status_hre_on" : 1
, "status_sc_on" : 1
, "status_correlation_on" : 1
, "status_internet_on" : 1
, "status_mode" : 0
, "status_web_collector" : 1
}
```

Creating or Updating an External Event Collector Source

Use the following settings:

`report_group=third-party-source`

This setting holds the configured third party event sources listed under External Event Collectors in the Juniper ATP Appliance. Central Manager Web UI Config > Environmental Settings page.

Get `vendor_category`, `vendor_name` values from the `op=ingestion_vendor_details` API for the source you are configuring.

Parameters differ slightly based on the whether ingestion will be coming from Splunk or via Direct Log collection. Be sure to supply the following sample parameters in POST or GET:

```
coll_log_ssl=disabled | enabled
create_incident=disabled | enabled
authorization=<auth key>
default_severity=0.0|0.25|0.5|0.75|1.0
ingest_transport=splunk | log_collector
report_group=third-party-sources
report_id=<report_id>
splunk_index=<Optional splunk index.
Applicable only when ingest_transport is splunk>
coll_log_port =
Applicable for sources such as Bluecoat to specify listen port for receiving events
vendor_category=<Vendor category (web_gateway | etdr | endpoint_av |
ngfw | ips)>
vendor_name=<Vendor name (bluecoat | carbon_black | mcafee_epo |
symantec_ep | pan)>
```

Example for Splunk Ingestion

```
curl 'https://10.2.25.24/admin/
api.php?op=update_report&report_group=third-party-
sources&report_id=21AB723E-AD7F-48BB-87CA-
9E547596E04B&vendor_category=endpoint_av&vendor_name=mcafee_epo&defau
lt_severity=0.50&create_incident=enabled&ingest_transport=splunkl_log
_ssl=enabled' -H 'Host: 10.2.25.24' -H
"Authorization:fb4f4fff2841a784fb21aa864af5e8fa" --insecure
```

Example for Direct Log Ingestion

```
curl 'https://10.2.25.24/admin/
api.php?op=update_report&report_group=third-party-
sources&report_id=21AB723E-AD7D-48BB-87CA-
9E547596E04B&vendor_category=endpoint_av&vendor_name=mcafee_epo&defau
lt_severity=0.50&create_incident=enabled&ingest_transport=log_collect
or&coll_log_ident=MCAFEE-EPO.eng.JATP.net&coll_log_ssl=enabled' -H
'Host: 10.2.25.24' -H
"Authorization:fb4f4fff2841a784fb21aa864af5e8fa" --insecure
```

Response will be {"status":0} for success.

Where:

[report_id](#) (which is a UUID). A random UUID can be generated and used with this API.

[vendor_category](#), [vendor_name](#) are the values from [op=ingestion_vendor_details](#) for the source being configured.

Other values map to the equivalent values shown in the Juniper ATP Appliance Web UI.

Getting All Configured External Event Collector Event Sources

The third party external event sources are stored in the reports framework. Pass

[op=get_reports&report_group=third-party-sources](#) to obtain all configured third party sources.

Example

```
curl 'https://10.2.25.24/admin/
api.php?op=get_reports&report_group=third-party-sources' -H 'Host:
10.2.25.56' -H "Authorization:fb4f4fff2841a784fb21aa864af5e8fa" --
insecure | json_pp
```

Output will display in the following format:

```
{
  "status" : 0,
  "report_table" : {
    "843AD6D7-99D5-4C6F-A194-58C0A98AABCD" : {
      "ingest_transport" : "splunk",
      "splunk_index" : "",
      "report_id" : "843AD6D7-99D5-4C6F-A194-58C0A98AABCD",
      "vendor_category" : "etdr",
      "user_id" : "fafbc8fe-1583-04cf-b985-a597472fc4ef",
      "time_created" : "Tue Apr 04 2017 12:30:57 GMT+0530 (IST)",
      "time_modified" : "Tue May 16 2017 13:45:31 GMT+0530 (IST)",
      "source_type" : "Splunk",
      "report_group" : "third-party-sources",
      "port_number" : "8089",
      "default_severity" : "0.25",
      "devices" : "carbon_black",
      "password" : "goJATP1",
      "create_incident" : "enabled",
```

```
    "host_name" : "10.2.14.219",
    "username" : "admin",
    "vendor_name" : "carbon_black"
  },
  "21AB723E-AD7D-48BB-87CA-9E547596E04B" : {
    "user_id" : "fafbc8fe-1583-04cf-b985-a597472fc4ef",
    "create_incident" : "enabled",
    "vendor_name" : "mcafee_epo",
    "coll_log_ident" : "MCAFEE-EPO",
    "ingest_transport" : "log_collector",
    "report_group" : "third-party-sources",
    "report_id" : "21AB723E-AD7D-48BB-87CA-9E547596E04B",
    "coll_log_ssl" : "enabled",
    "vendor_category" : "endpoint_av",
    "default_severity" : "0.50"
  }
}
```

license_details

Use this API function to obtain current license status and details for Juniper ATP Appliance support, content and product licenses.

The API for a license details request is as follows:

https://<HOST>/admin/api.php?op=license_details

Example

```
curl -v -k -d "csrf_token=5461a5c0e68990.85292892"
"https://10.2.2.2/admin/api.php?op=license_details"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample JSON Request

```
{
  "licenses": {
    "product": {
      "regular_checking_failed_cap": 1,
```

```
    "status": "valid",
    "expiry_date": "NEVER",
    "warning_cap": 14,
    "data_services_stopped": false,
    "data_services_stopped_reason": "",
    "regular_checking_failed": false
  },
  "support": {"status": "valid", "expiry_date": "2024-10-04
05:34:34+00", "warning_cap": 14},
  "content": {"status": "valid", "expiry_date": "2024-10-04
05:34:34+00", "warning_cap": 14}
}, "session_timeout_sec": 36000, "status": 0
}
```

login

Use the login API function to set the SESSID cookie when login is successful. This API also returns basic user and configuration information.

HTTP Post Parameters	Description
init	When non-zero, this augments the result with constants and configuration tables that are useful in displaying values returned by other API requests
password	cleartext password of login request
user_name	User name of login request

Example

```
curl -v -k -d "Authorization:7c71c218662411a5c857042053acca8f"
"user_name=admin&password=12345"
"https://HOST/admin/api.php?op=login&init=1"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

```
{
  "status" : 0,
  "session_timeout_sec" : 0,
  "user_info" : {
    "user_id" : "5520fa4b-73a2-0a63-1597-2bc8e99897b7",
    "config_table" : {
```

```
    "system_config" : {
      "has_license" : 0,
      "hostname" : "frank",
      "autoupdate_enabled" : "0",
      "remote_shell_enabled" : "0",
      "spanning_tree" : "0"
    },
    "display" : {
      "account_lockout_duration_sec" : 600,
      "account_lockout_threshold" : 10,
      "account_lockout_observation_sec" : 600,
      "alerts_refresh_sec" : 60,
      "max_alerts" : 500
    }
  },
  "user_fullname" : "JATPView Admin",
  "role_array" : [
    0,
    1,
    2
  ],
  "user_name" : "JATPadmin"
},
"JATP_version" : "2.0",
"server_fqdn" : "",

"role_map" : {
  "JATP_ADMIN_ROLE" : {
    "role_desc" : "Administrator",
    "role_value" : 2
  },
  "JATP_PUBLIC_ROLE" : {
    "role_desc" : "General Public",
    "role_value" : 0
  },
  "JATP_DEBUG_ROLE" : {
    "role_desc" : "Debugging",
    "role_value" : 3
  },
  "JATP_USER_ROLE" : {
    "role_desc" : "User",
    "role_value" : 1
  }
},
"status_network_on" : 0,
"status_fc_on" : 0,
"status_mode" : 0,
"status_sc_on" : 0,
"status_hre_on" : 0,
"status_sigeng_on" : 0,
```



```
"status_net_on" : 1,  
"status_correlation_on" : 0,  
"server_ip" : "127.0.0.1",  
"server_name" : "HOST"  
}
```

logout

Use the login API function to log out and invalidate the session.

Example

```
curl 'https://10.2.20.84/admin/api.php?op=logout' --data  
'csrf_token=54acc54b99ba37.93795519'
```

Sample Response

There is no response available for this API.

network_traffic

Use this API to display a per-object summary of network traffic object statistics and usage stats of the data displayed in the Central Manager Dashboard, including Core detection utilization information. This API provides various runtime metrics typically seen on the Central manager Dashboard for the last n units of time. The returned data contains information about inspected traffic, cluster utilization, analysis times and details about malwares detected recorded at various points in time. The duration is time is specified using the interval_sec and the num_intervals param.

The API for obtaining network traffic summaries from the Central Manager Web UI Dashboard is as follows:

https://<HOST>/admin/api.php?op=network_traffic

HTTP Post Parameters	Description
interval_sec	Time interval in seconds. Network traffic during this time will be returned.
num_intervals	The number of intervals.
tz_offset_sec	The tz offset in seconds.
collector_id	(Optional) UUID of the Collector

NOTE If an incorrect collector_id is given, the offered_traffic and inspected_traffic values are displayed as zero (0). If no collector_id parameter is passed, then the values shown for offered_traffic and inspected_traffic is representative of aggregate traffic.

Example

```
curl "Authorization:7c71c218662411a5c857042053acca8f" "https://
10.1.1.1/admin/api.php?op=network_traffic" --data
"interval_sec=5400&num_intervals=480&tz_offset_sec=19800&Collector_id
=aaaa-bbbb-cccc-ddddd"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Output

The response includes a count_array attribute which is an array of various metrics (not all of which we display on the dashboard). Each element in the array indicates the value of various metrics for the specified timestamp. Consequently, to graph them, attributes are aggregated (certain attributes are averaged while others are summed up) for display. The response output fields include:

Response Field	Description
timestamp	Timestamp for the traffic collection
num_clean	Number of clean objects.
num_low	Number of low risk objects
num_med	Number of medium risk objects
num_high	Number of high risk traffic objects
total_objects	Total number of objects in network traffic
offered_traffic	Traffic processed for every 5min in kbps
offered_traffic_rate	Total bandwidth of traffic being analyzed.

inspected_traffic	Bandwidth used for scanning and inspecting traffic in Bytes per Second (Bps)
num_malware	Number of malicious objects detected
winxp_util_factor_short	Utilization data for Windows Cores
osx_util_factor_short	Utilization data for OSX Secondary Cores
winxp_duration	Analysis delay for winxp OS
osx_duration	Analysis delay for OSX

The following is an example response:

```
{
  "count_array": [
    {
      "timestamp": 1413093828,
      "num_clean": 0,
      "num_low": 0,
      "num_med": 0,
      "num_high": 0,
      "total_objects": 0,
      "offered_traffic": 0,
      "inspected_traffic": 0,
      "winxp_util_factor_short": 0,
      "osx_util_factor_short": 0,
      "winxp_duration": 0,
      "osx_duration": 0,
      "num_malware": 0
    },
    {
      "timestamp": 1413099228,
      "num_clean": 0,
      "num_low": 0,
      "num_med": 0,
      "num_high": 0,
      "total_objects": 0,
      "offered_traffic": 0,
      "inspected_traffic": 0,
      "winxp_util_factor_short": 0,
```

```

        "osx_util_factor_short": 0,
        "winxp_duration": 0,
        "osx_duration": 0,
        "num_malware": 0
    },
    {
        "timestamp": 1415540028,
        "num_clean": 0,
        "num_low": 0,
        "num_med": 0,
        "num_high": 0,
        "total_objects": 0,
        "offered_traffic": 0,
        "inspected_traffic": 0,
        "winxp_util_factor_short": 0,
        "osx_util_factor_short": 0,
        "winxp_duration": 0,
        "osx_duration": 0,
        "num_malware": 0
    },
    {
        "timestamp": 1415545428,
        "num_clean": 0,
        "num_low": 0,
        "num_med": 0,
        "num_high": 0, {
"count_array": [
    {
        "timestamp": 1415855407,
        "num_clean": 0,
        "num_low": 0,
        "num_med": 0,
        "num_high": 0,
        "total_objects": 0, /// indicates the total object processed
        "offered_traffic": 0, /// offered traffic
        "inspected_traffic": 0, /// inspected traffic
    }

```

```
        "winxp_util_factor_short": 0,                /// utilization for
win Cores
        "osx_util_factor_short": 0,                /// utilization for
osx cores
        "winxp_duration": 0,                      /// Analysis delay for
winxp
        "osx_duration": 0, /// Analysis delay for osx
        "num_malware": 0                          /// indicates the
total number of malware
    },
    ....
}
```

set_auto_mitigation_settings

This API configures auto-mitigation.

https://HOST/admin/api.php?op=set_auto_mitigation_settings

Example

```
curl 'https://10.1.1.1/admin/
api.php?op=set_auto_mitigation_settings&web_auto_mitigation_enabled=t
rue&aggressiveness=moderate&max_ip_threats=500&email_auto_mitigation_
enabled=true&max_url_threats=500' -H 'Host: 10.1.1.1' -H
"Authorization:ae5bab7c3a2241a89a435d3671e29f92" --insecure
```

HTTP Post Parameters	Description
web_auto_mitigation_enabled	true false
email_auto_mitigation_enabled	true false
aggressiveness	moderate always
max_url_threats	Number of threats to return

NOTE The parameters `web_auto_mitigation_enabled` and `email_auto_mitigation_enabled` can be false if they are not required to be enabled.

Aggressiveness can be moderate or always. If it is always, all the threats are auto mitigated. For moderate only, only Max and High Threat confidence level threats are automatically mitigated.

See Also: [get_auto_mitigation_settings on page 86](#).

set_whitelist_rules

This API adds a new whitelist rule or updates an existing rule. Rename a rule by specifying the old_name parameter. A rule can have one or more attributes.

https://HOST/admin/api.php?op=set_whitelist_rule

HTTP Post Parameters	Description
type	Specifies type; possible value "incident"
name	New name for the rule; used while changing the name of a rule.
old_name	Old name of the rule; set when re-naming a whitelist rule.
src_ip	Source IP
dst_ip	Destination IP
domain	Domain name
host:	Host name
uri	URI
sha1sum	SHA1 Sum

Example

```
curl "Authorization:7c71c218662411a5c857042053acca8f" "https://  
10.2.20.84/admin/api.php?op=set_whitelist_rules" -data  
"src_ip=10.10.10.10&name=NewRule&type=incident"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

No response is available for this API.

test_configuration

Use this API to test the Juniper ATP Appliance configuration.

https://HOST/admin/api.php?op=test_configuration

Example

```
curl 'https://tap21/admin/api.php?op=test_configuration'
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Parameters

HTTP Post Parameters	Description
interval_sec	[Required] The number of seconds in the time frame of interest, ending in "end_time_sec"
min_severity_value	[Required] The minimum severity value of the incident.
max_severity_value	[Required] The maximum severity value of the incident.

Sample Response

```
{
```

top_incidents

Use this API to retrieve the latest incidents.

Identification of the endpoint is provided in this API response, when available.

https://HOST/admin/api.php?op=top_incidents

Example

```
curl -k -H "Authorization:d5d0e4e71c9ab6d7bfa8fff4dab341a5" 'https://  
10.2.9.43/admin/api.php?op=top_incidents' --data  
'end_time_sec=0&interval_sec=2592000&max_severity_value=1&min_severity_v  
alue=0'
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Parameters

HTTP Post Parameters	Description
interval_sec	[Required] The number of seconds in the time frame of interest, ending in "end_time_sec"
min_severity_value	[Required] The minimum severity value of the incident.
max_severity_value	[Required] The maximum severity value of the incident.

Sample Response

```
{
  "top_incidents": [
    {
      "user_ack_status": "new",
      "incident_id": "2001",
      "incident_category": "Trojan_Generic",
      "incident_name": "TROJAN_MIUREF.DC",
      "normalized_name": "Trojan_Miuref",
      "incident_risk": "1.00",
      "incident_severity": "1.0",
      "incident_relevance": "1.0",
      "endpoint_ip": "192.168.50.18",
      "endpoint_id": "192.168.50.18""{user5@biz_central.com}",,
      "endpoint_name": "192.168.50.18",
      "endpoint_value": "0.5",
      "endpoint_os_type": "windows",
      "source_ip": "134.19.180.195",
      "source_name": "582330430-6.idgromo.ru",
      "last_activity_time": "2016-06-02 08:23:43.123692+00"
    },
    {
      "user_ack_status": "new",
      "incident_id": "2010",
      "incident_category": "Suspicious",
      "incident_name": "TROJAN_Miuref.CY",
      "normalized_name": "Trojan_Miuref",
      "incident_risk": "1.00",
      "incident_severity": "1.0",
      "incident_relevance": "1.0",
      "endpoint_ip": "192.168.50.203",
      "endpoint_id": 0,
      "endpoint_name": "192.168.50.203",
      "endpoint_value": "0.5",
      "endpoint_os_type": "windows",
      "source_ip": "46.165.222.218",
      "source_name": "46.165.222.218",
      "last_activity_time": "2016-06-02 08:23:52.166731+00"
```



```
    } ],  
    "session_timeout_sec": 36000,  
    "status": 0  
  }
```

trace_log

Use this API to retrieve the trace log for an event.

https://HOST/admin/api.php?op=trace_log

Example

```
curl -k -b "Authorization:7c71c218662411a5c857042053acca8f"  
"https://HOST/admin/api.php?op=trace_log" -d "event_id=624"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

Response includes the trace log for the specified event.

trace_pcap

Use this API to retrieve the trace log for an event.

https://HOST/admin/api.php?op=trace_pcap

Example

```
curl -k -b "Authorization:7c71c218662411a5c857042053acca8f"  
"https://HOST/admin/api.php?op=trace_pcap" -d "event_id=624"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

Response includes display of the pcap for the specified event.

update_report

Use this API to update report settings and include zone configuration.

https://HOST/admin/api.php?op=update_report

Parameters

HTTP Post Parameters	Description
report_group	zones-configuration
report_id	A UUID;a random UUID can be generated and used with this API.
zone_description	Description of the zone.
zone_name	Name of the zone.

Example

```
curl 'https://10.1.1.1/admin/
api.php?op=update_report&report_group=zones-
configuration&report_id=4F12B367-5983-4D6E-8719-
B9C84A01F043&zone_description=test&zone_name=zonetest' -H 'Host:
10.1.1.1' -H "Authorization:ae5bab7c3a2241a89a435d3671e29f92"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

verify

Use this API to verify and update the session cookie.

<https://HOST/admin/api.php?op=verify>

This is a verification and update function that is successful if the session cookie is valid. On success, it returns the same result as a successful login with the parameter "init" set to non-zero.

Example

```
curl -k -b "Authorization:7c71c218662411a5c857042053acca8f"
"https://HOST/admin/api.php?op=verify"
```

Authorization - The device user API key.

Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

```
{
  "error_msg" : "not logged in",
  "status" : -11,
  "session_timeout_sec" : 0
}
```

What to Do Next?

- Refer to the Juniper ATP Appliance Core/CM Quick Start Guide or Juniper ATP Appliance All-in-One Quick Start Guide for more information about installing and managing Juniper ATP Appliance's distributed, virtual and/or clustered threat protection.
- Refer to the Juniper ATP Appliance Mac Mini OS X Engine Quick Start Guide for information about installing a Mac Mini Secondary Core Detection Engine.
- Refer to the Juniper ATP Appliance Core/CM Quick Start Guide for information about installing virtual Core or clustered Core deployments.
- Refer to the Juniper ATP Appliance Traffic Collector Quick Start Guide for information about installing a Traffic Collector.
- Refer to the Juniper ATP Appliance CLI Command Reference for information about Collector CLI commands.
- Refer to the Juniper ATP Appliance Operator's Guide for information about all products and usage.
- Refer to the Juniper ATP Appliance CEF Logging Support for SIEM Integration Guide for information about CEF logging

