



# Malware Detection API

User Guide

Version 3.5

February 16, 2021

## Table of Contents

Get Started.....	3
Malware Detection API .....	3
Making API calls.....	4
URL to Qualys API server .....	6
Qualys user account .....	7
Output pagination and truncation.....	8
JSON support .....	11
Know your portal version .....	15
MD APIs.....	18
Current malware detection count.....	18
Search malware detections .....	20
View malware detection details .....	23
Troubleshooting .....	25
MD error messages.....	25

# Get Started

## Malware Detection API

The Malware Detection API supports the download of information from the Malware Detection module, when this module is enabled your Qualys account.

### Modules supported

MD

### Authentication

Authentication to your Qualys account with valid Qualys credentials is required for making Qualys API requests to the Qualys API servers. Learn more about authentication to your Qualys account

### Get API Notifications

We recommend you join our Community and subscribe to our API Notifications RSS Feeds for announcements and discussions.

<https://community.qualys.com/community/developer/notifications-api>

### About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated Cloud Apps deliver businesses critical security intelligence continuously, enabling them to automate the full spectrum of auditing, compliance and protection for IT systems and web applications on premises, on endpoints and elastic clouds. For more information, please visit [www.qualys.com](http://www.qualys.com)

Qualys and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies

## **Making API calls**

### **Curl samples in our API doc**

We use curl in our API documentation to show an example how to form REST API calls, and it is not meant to be an actual production example of implementation.

### **GET and POST Methods**

Qualys API unctions allow API users to submit parameters (name=value pairs) using the GET and/or POST method. There are known limits for the amount of data that can be sent using the GET method, and these limits are dependent on the toolkit used. Please refer to the individual descriptions of the API function calls to learn about the supported methods for each function

### **Parameters in URLs**

API parameters, as documented in this user guide, should be specified one time for each URL. In the case where the same parameter is specified multiple times in a single URL, the last parameter takes effect and the previous instances are silently ignored. URL elements are case sensitive.

### **Date format in API Results**

The Qualys API has adopted a date/time format to provide consistency and interoperability of the Qualys API with third-party applications. The date format follows standards published in RFC 3339 and ISO 8601, and applies throughout the Qualys API. The date format is: yyyy-mm-ddThh-mm-ssZ This represents a UTC value (GMT time zone).

### **URL Encoding in API Code**

You must URL encode variables when using the Qualys API. This is standard practice for HTTP communications. If your application passes special characters, like the single quote ('), parentheses, and symbols, they must be URL encoded. For example, the pound (#) character cannot be used as an input parameter in URLs. If “#” is specified, the Qualys API returns an error. To

specify the “#” character in a URL you must enter the encoded value “%23”. The “#” character is considered by browsers and other Internet tools as a separator between the URL and the results page, so whatever follows an un-encoded “#” character is not passed to the Qualys API server and returns an error.

## **Making requests with URL payload**

While it is still possible to create simple API requests using the GET method, you can create API requests using the POST method with an XML payload to make an advanced request.

The XML payloads can be compared to a scripting language that allows user to make multiple actions within one single API request, like adding a parameter to an object and updating another parameter.

The XML structure of the payload is described in the XSD files.

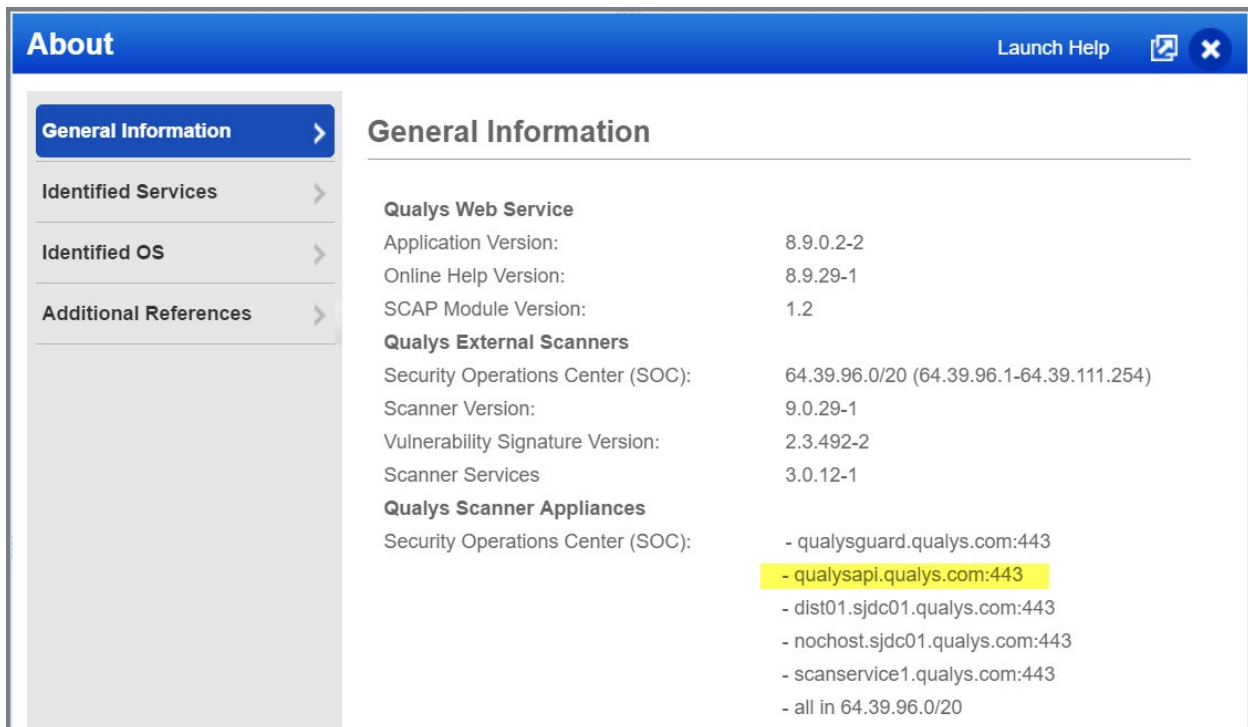
## URL to Qualys API server

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

[Click here to identify your Qualys platform and get the API URL](#)

This documentation uses the API server URL for Qualys US Platform 1 (<https://qualysapi.qualys.com>) in sample API requests. If you're on another platform, please replace this URL with the appropriate server URL for your account.

Looking for your API server URL for your account? You can find this easily. Just log in to your Qualys account and go to Help > About. You'll see this information under Security Operations Center (SOC).



The screenshot shows the 'About' page in a Qualys account. The page has a blue header with 'About' on the left and 'Launch Help' with a help icon on the right. A left sidebar contains a menu with 'General Information' (selected), 'Identified Services', 'Identified OS', and 'Additional References'. The main content area is titled 'General Information' and lists various service versions and IP addresses. The 'Qualys External Scanners' section lists the Security Operations Center (SOC) IP address as 64.39.96.0/20 (64.39.96.1-64.39.111.254) and the Scanner Version as 9.0.29-1. The 'Qualys Scanner Appliances' section lists the Security Operations Center (SOC) IP addresses as - qualysguard.qualys.com:443, - qualysapi.qualys.com:443 (highlighted in yellow), - dist01.sjdc01.qualys.com:443, - nohost.sjdc01.qualys.com:443, - scanservice1.qualys.com:443, and - all in 64.39.96.0/20.

Qualys Web Service	
Application Version:	8.9.0.2-2
Online Help Version:	8.9.29-1
SCAP Module Version:	1.2

Qualys External Scanners	
Security Operations Center (SOC):	64.39.96.0/20 (64.39.96.1-64.39.111.254)
Scanner Version:	9.0.29-1
Vulnerability Signature Version:	2.3.492-2
Scanner Services	3.0.12-1

Qualys Scanner Appliances	
Security Operations Center (SOC):	- qualysguard.qualys.com:443
	- qualysapi.qualys.com:443
	- dist01.sjdc01.qualys.com:443
	- nohost.sjdc01.qualys.com:443
	- scanservice1.qualys.com:443
	- all in 64.39.96.0/20

## Qualys user account

The application must authenticate using Qualys account credentials (user name and password) as part of the HTTP request. The credentials are transmitted using the “Basic Authentication Scheme” over HTTPS.

For more information, see the “Basic Authentication Scheme” section of RFC #2617:

<http://www.faqs.org/rfcs/rfc2617.html>

The exact method of implementing authentication will vary according to which programming language is used.

Basic authentication - recommended option:

```
curl -u "USERNAME:PASSWORD"  
https://qualysapi.qualys.com/qps/rest/1.0/download/cm/alert
```

where qualysapi.qualys.com is the base URL to the Qualys API server where your account is located.

## Output pagination and truncation

The XML output of a search API request is paginated and the default page size is 100 object records. The page size can be customized to a value between 1 and 1,000. If the number of records is greater than the page size then the `<ServiceResponse>` element shows the response code SUCCESS with the element `<hasMoreRecords>>true</hasMoreRecords>` as shown below.

Follow the simple process below to obtain the first two the XML pages for an API request. Please apply the same logic to get all the next (n+1) pages until all records are returned. This is indicated when `<hasMoreRecords>>false</hasMoreRecords>`.

### Step 1 - Search for malware detection alerts of type behavioral.

#### API request

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/qps/rest/1.0/search/md/detection/" <
file.xml
```

Note: "file.xml" contains the request POST data.

#### Request POST data

```
<ServiceRequest>
  <preferences>
    <limitResults>5</limitResults>
  </preferences>
  <filters>
    <Criteria field="type" operator="EQUALS">BEHAVIORAL</Criteria>
  </filters>
</ServiceRequest>
```

In the response, the number of records is greater than the default pagination value so the `<ServiceResponse>` element identifies the last ID of the object in the current page output.



## Response

```
<ServiceResponse ...>
  <responseCode>SUCCESS</responseCode>
  <COUNT>5</COUNT>
  <hasMoreRecords>true</hasMoreRecords>
  <lastId>123</lastId>
  <data>
    <!--here you will find 5 alert records-->
  </data>
</ServiceResponse>
```

## Step 2 - Search alerts and get next batch of results

To get the next page of results, you need to edit your service request in “file.xml” that will be passed to API request as a POST payload. According to the <lastId> element returned in the first page, you want the next page of results to start with the object ID 124 or greater.

## API request

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/ps/rest/1.0/search/md/detection/" <
file.xml
```

Note: “file.xml” contains the request POST data.

You’ll notice the operator field value is set to 123, which is the value returned in <lastId> of the previous page output. The GREATER operator is a logical “greater than” (it does not mean greater than or equal to).

## Request POST data

```
<ServiceRequest>
  <filters>
    <Criteria field="type"operator="EQUALS">BEHAVIORAL </Criteria>
    <Criteria field="id" operator="GREATER">123</Criteria>
  </filters>
</ServiceRequest>
```

## Set custom page size

The service request needs to contain the <preferences> section with the <limitResults> parameter. For the <limitResults> parameter you can enter a value from 1 to 1,000.

### Response

```
<ServiceRequest>
  <filters>
    <Criteria> ... </Criteria>
  </filters>
  <preferences>
    <limitResults>200</limitResults>
  </preferences>
</ServiceRequest>
```

## JSON support

The Qualys Malware Detection API supports JSON requests and responses. Headers used in samples below.

Send JSON request - "Content-Type: application/json"

Get response in JSON - "Accept: application/json"

### Sample - Search Malware Detections

#### API request

```
cat {json} | curl -s -k -X POST -H "Accept: application/json" -H  
"Content-Type: application/json" -H "user:{USERNAME}" -H  
"password:{PASSWORD}" -d @-  
https://qualysapi.qualys.com/qps/rest/1.0/search/md/detection
```

#### Request POST data

```
{  
  "ServiceRequest": {  
    "preferences": { "limitResults": "100" },  
    "filters": {  
      "Criteria": [  
        {  
          "-field": "id",  
          "-operator": "EQUALS",  
          "#text": "37747097"  
        },  
        {  
          "-field": "url",  
          "-operator": "CONTAINS",  
          "#text": "http://www.mwtest.info/malware-demos-named/"  
        },  
        {  
          "-field": "type",  
          "-operator": "EQUALS",  
          "#text": "BEHAVIORAL"  
        }  
      ]  
    }  
  }  
}
```

```
    ]  
  }  
}  
}
```

## Response

```
{  
  "ServiceResponse": {  
    "-xmlns:xsi": "http://www.w3.org/2001/XMLSchema-instance",  
    "-xsi:noNamespaceSchemaLocation":  
      "https://qualysapi.qualys.com/qps/xsd/1.0/md/detection.xsd",  
    "responseCode": "SUCCESS",  
    "count": "1",  
    "hasMoreRecords": "false",  
    "data": {  
      "Detection": {  
        "id": "37747097",  
        "qid": "206012",  
        "name": "  
          A Malicious Process Launch Was Detected  
        ",  
        "type": "BEHAVIORAL",  
        "severity": "HIGH",  
        "url": "  
          http://www.mwtest.info/malware-demos-named/  
          MS06-014-RemotePayload/MS06-014-DEMO.html  
        "  
      }  
    }  
  }  
}
```

## Sample - Get details for malware detection

### API request

```
curl -X GET -s -k -H "Accept: application/json" -n -u  
"{USERNAME}:{PASSWORD}" "  
https://qualysapi.qualys.com/qps/rest/1.0/get/md/detection/37747097"
```

### Response

```
{
```

```

"ServiceResponse": {
  "-xmlns:xsi": "http://www.w3.org/2001/XMLSchema-instance",
  "-xsi:noNamespaceSchemaLocation":
"https://qualysapi.qualys.com/qps/xsd/1.0/md/detection.xsd",
  "responseCode": "SUCCESS",
  "count": "1",
  "data": {
    "Detection": {
      "id": "37747097",
      "qid": "206012",
      "name": "
        A Malicious Process Launch Was Detected
      ",
      "type": "BEHAVIORAL",
      "description": "
        Upon visiting the Web page, a process launch was
detected by the malware detection service. External process launches
should never occur in normal Web browsing activity. This is an
indication of malicious behavior. The process launched is noted in the
Results section.
      ",
      "severity": "HIGH",
      "url": "
        http://www.mwtest.info/malware-demos-named/MS06-014-
RemotePayload/MS06-014-DEMO.html
      ",
      "result": "
        Process creation was attempted on application
C:\\DOCUME~1\\ADMINI~1\\LOCALS~1\\Temp\\hgivV.exe with parameters
(Undefined)
      ",
      "asset": {
        "id": "2688083",
        "name": "
          http://www.mwtest.info/malware-demos-named/
        ",
        "deactivated": "false"
      }
    }
  }
}

```



## Know your portal version

/qps/rest/portal/version/

[GET] [POST]

Using the Version API you can find out the installed version of Portal and its sub-modules that are available in your subscription.

Sample XML

### API request

```
curl -u "USERNAME:PASSWORD" -X "GET" -H "Accept: application/xml"
https://qualysapi.qualys.com/qps/rest/portal/version
```

### Response

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/ve
rsion.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <PortalApplication-VERSION>3.5.0.0-SNAPSHOT-1 DEVELOP #92
(2021-01-19T01:51:21Z)
    </PortalApplication-VERSION>
    <ITAM-VERSION>1.3.1.0-18</ITAM-VERSION>
    <CS-VERSION>1.9.0.0-SNAPSHOT</CS-VERSION>
    <CA-VERSION>3.4.0.0</CA-VERSION>
    <QGS-VERSION>1.2.0.0-6</QGS-VERSION>
    <QUESTIONNAIRE-VERSION>2.26.0.0</QUESTIONNAIRE-VERSION>
    <SAC-VERSION>1.0.0-SNAPSHOT</SAC-VERSION>
    <WAF-VERSION>2.12.6.0</WAF-VERSION>
    <QUESTIONNAIRE__V2-VERSION>1.13.1.0-
SNAPSHOT</QUESTIONNAIRE__V2-VERSION>
    <WAS-VERSION>6.17.0.0-SNAPSHOT-32</WAS-VERSION>
    <FIM-VERSION>2.6.0.0-23</FIM-VERSION>
    <ICS-VERSION>0.9.1.0-12</ICS-VERSION>
```

```

    <VM-VERSION>1.0.3</VM-VERSION>
    <CERTVIEW-VERSION>2.8.0.0-20</CERTVIEW-VERSION>
    <CLOUDVIEW-VERSION>1.9.2.0-SNAPSHOT</CLOUDVIEW-VERSION>
    <CM-VERSION>1.31.0.0</CM-VERSION>
    <MDS-VERSION>2.16.1.0-SNAPSHOT-2</MDS-VERSION>
    <PM-VERSION>1.5.0.0-2</PM-VERSION>
    <PS-VERSION>1.3.0.0-16</PS-VERSION>
    <IOC-VERSION>1.2.0-15</IOC-VERSION>
    <THREAT__PROTECT-VERSION>1.5.0-SNAPSHOT</THREAT__PROTECT-
VERSION>
    <AV2-VERSION>0.1.0</AV2-VERSION>
    <UD-VERSION>1.0.0</UD-VERSION>
  </Portal-Version>
  <QWeb-Version>
    <WEB-VERSION>10.7.0.0-1</WEB-VERSION>
    <SCANNER-VERSION>12.1.68-1</SCANNER-VERSION>
    <VULNSIGS-VERSION>2.5.84-2</VULNSIGS-VERSION>
  </QWeb-Version>
</data>
</ServiceResponse>

```

Sample JSON

### API request

```
curl -u "USERNAME:PASSWORD" -X "GET" -H "Accept: application/json"
https://qualysapi.qualys.com/qps/rest/portal/version
```

### Response

```

{
  "ServiceResponse": {
    "data": [
      {
        "Portal-Version": {
          "PortalApplication-VERSION": "3.5.0.0-SNAPSHOT-1 DEVELOP #92
(2021-01-19T01:51:21Z)",
          "WAS-VERSION": "6.17.0.0-SNAPSHOT-32",
          "VM-VERSION": "1.0.3",
          "CM-VERSION": "1.20.1",
          "MDS-VERSION": "2.16.1.0-SNAPSHOT-2",
          "CA-VERSION": "2.9.1.0",

```



```
        "QUESTIONNAIRE-VERSION": "2.14.0.4",  
        "WAF-VERSION": "2.7.0.0"  
    },  
    ...  
    }  
  ],  
  "responseCode": "SUCCESS",  
  "count": 1  
}
```

# MD APIs

## Current malware detection count

`/qps/rest/1.0/count/md/detection/`

[POST]

Returns the total number of malware detections in the user's account. Input elements are optional and are used to filter the number of detections in the count.

Permissions required - Managers with full scope. Other users must have these permissions: Access Permission "API Access" and Asset Management Permission "Read Asset". Output includes web sites within the user's scope.

### Input Parameters

Allowed input elements are listed below. The associated data type for each element appears in parentheses. These elements are optional and act as filters. When multiple elements are specified, parameters are combined using a logical AND.

Available operators

Parameter	Description
id	(integer)
qid	(integer)
url	(text)
type	(keyword)
showDeactivatedSite	(boolean)

severity (keyword)

## Sample - Get malware detection count

### API request

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --  
data-binary @-  
"https://qualysapi.qualys.com/qps/rest/1.0/count/md/detection" <  
file.xml
```

Note: "file.xml" contains the request POST data.

### Request POST data

```
<ServiceRequest>  
  <filters>  
    <Criteria field="id" operator="GREATER">37747097</Criteria>  
  </filters>  
</ServiceRequest>
```

### Response

```
<?xml version="1.0" encoding="UTF-8"?>  
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/1.  
0/md/detection.xsd">  
  <responseCode>SUCCESS</responseCode>  
  <count>41</count>  
</ServiceResponse>
```

### XSD

[platform API server](https://qualysapi.qualys.com/qps/xsd/2.0/md/detection.xsd)/qps/xsd/2.0/md/detection.xsd

## Search malware detections

/qps/rest/1.0/search/md/detection/

[POST]

Returns a list of malware detections in the user's account.

Limit your results - Use the optional "fields" parameter to limit the amount of information returned. [Learn more about limiting your results](#)

Permissions required - Managers with full scope. Other users must have requested asset in their scope and these permissions: Access Permission "API Access" and Asset Management Permission "Read Asset"

### Input Parameters

Allowed input elements are listed below. The associated data type for each element appears in parentheses. These elements are optional and act as filters. When multiple elements are specified, parameters are combined using a logical AND.

Available operators

Parameter	Description
id	(integer)
qid	(integer)
url	(text)
type	(keyword)
showDeactivatedSite	(boolean)
severity	(keyword)

## Sample - Search detections

### API request

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --  
data-binary @-  
"https://qualysapi.qualys.com/qps/rest/1.0/search/md/detection" <  
file.xml
```

### Request POST data

```
<ServiceRequest>  
  <preferences>  
    <limitResults>100</limitResults>  
  </preferences>  
  <filters>  
    <Criteria field="id" operator="EQUALS">37747097</Criteria>  
    <Criteria field="url"  
      operator="CONTAINS">http://www.mwtest.info/  
      malware-demos-named/</Criteria>  
    <Criteria field="type"  
      operator="EQUALS">BEHAVIORAL</Criteria>  
  </filters>  
</ServiceRequest>
```

### Response

```
<?xml version="1.0" encoding="UTF-8"?>  
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
  xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/1.  
  0/md/detection.xsd">  
  <responseCode>SUCCESS</responseCode>  
  <count>1</count>  
  <hasMoreRecords>>false</hasMoreRecords>  
  <data>  
    <Detection>  
      <id>37747097</id>  
      <qid>206012</qid>  
      <name>  
        <![CDATA[A Malicious Process Launch Was Detected]]>  
      </name>  
      <type>BEHAVIORAL</type>  
      <severity>HIGH</severity>  
      <url>
```

```
<![CDATA[http://www.mwtest.info/  
malware-demos-named/MS06-014-RemotePayload/  
MS06-014-DEMO.html]]>  
  </url>  
</Detection>  
</data>  
</ServiceResponse>
```

## XSD

[<platform API server>/qps/xsd/2.0/md/detections.xsd](#)

## View malware detection details

/qps/rest/1.0/get/md/detection/<id>

[GET] [POST]

Returns details of a malware detection.

Limit your results - Use the optional “fields” parameter to limit the amount of information returned. [Learn more about limiting your results](#)

Permissions required - Managers with full scope. Other users must have requested asset in their scope and these permissions: Access Permission “API Access” and Asset Management Permission “Read Asset”. Output includes web sites in the user’s scope.

### Input Parameter

The element “id” (Integer) is required, where “id” identifies the alert.

### Sample - Get detection details

#### API request

```
curl -u "USERNAME:PASSWORD" -X GET  
https://qualysapi.qualys.com/qps/rest/1.0/get/md/detection/37747097
```

#### Response

```
<?xml version="1.0" encoding="UTF-8"?>  
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/1.  
0/md/detection.xsd">  
  <responseCode>SUCCESS</responseCode>  
  <count>1</count>  
  <data>  
    <Detection>  
      <id>37747097</id>  
      <qid>206012</qid>  
      <name>
```

```

        <![CDATA[A Malicious Process Launch Was Detected]]>
    </name>
    <type>BEHAVIORAL</type>
    <description>
        <![CDATA[Upon visiting the Web page, a process
        launch was detected by the malware detection
        service. External process launches should never
        occur in normal Web browsing activity. This is an
        indication of malicious behavior. The process
        launched is noted in the Results section.]]>
    </description>
    <severity>HIGH</severity>
    <url>
        <![CDATA[http://www.mwtest.info/malware-demos
        -named/MS06-014-RemotePayload/MS06-014-DEMO.html]]>
    </url>
    <result>
        <![CDATA[Process creation was attempted on
        application
        C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\hgivV.exe
        with parameters (Undefined)]]>
    </result>
    <asset>
        <id>2688083</id>
        <name>
            <![CDATA[http://www.mwtest.info/
            malware-demos-named/]]>
        </name>
        <deactivated>>false</deactivated>
    </asset>
    </Detection>
</data>
</ServiceResponse>

```

## XSD

[platform API server/qps/xsd/2.0/md/detection.xsd](http://platform API server/qps/xsd/2.0/md/detection.xsd)



# Troubleshooting

## MD error messages

Error messages returned from MD API requests are described below by category.

Error categories: [Element](#) | [Criteria](#) | [Authorization](#) | [Report Storage Limit](#)

### Element

Error message	Resolution
url: Invalid URL format (<value>)	URL format must be as follows:  http://<baseUrl>/rest/1.0/?parameters
Url: Element is required	Element “Url” is required.
uris.<field>: Invalid URL format (<value>).	For the uri.<field> sub element, specify a URL like http://domain.name/base/url/?parameters
uris.<field>: Length of the field must not be greater than 2048 characters. (<value>).	For the uri.<field> sub element, the maximum field length is 2048 characters.
Attribute.category: Element is required.	The element Attribute.category is required.
Attribute.category:	Element Attribute.category must be set to one of

Invalid value (<value>).	these values: Business Function, Business Location, Business Description.
Attribute.value: Element is required.	Element Attribute.category must be set to one of these values: Business Function, Business Location, Business Description.
Attribute.value: Element is required.	Provide a value for the attribute in the Attribute.value element: function, location or description.
The attribute length cannot be greater than 64 characters.	The value for this attribute cannot exceed 64 characters.
The attribute length cannot be greater than 2048 characters.	The value for this attribute cannot exceed 2048 characters.
<element>: Element must not be set.	This element does not apply to this request.
set: Element must contain at least one child.	The set element requires at least one sub element.
headers: Length of all headers cannot exceed 2048 characters.	The values of all headers cannot exceed 2048 characters.
At least one of the following elements must be set: set, add, remove.	For an “update” request you must set at least one of these elements: set, add or remove.
UrlEntry: Element	The element UrlEntry must be provided.

is required.

UrlEntry: Invalid URL format (value). Specify a URL like `http://domain.name/base/url/?parameters`

<parent>: Length of all [URLs, regular expressions] cannot exceed 2048 characters The list of entries for a given type shall not exceed 2048 characters.

UrlEntry: Only regular expressions are accepted for this element. You must provide regular expressions for the element `postDataBlackList`.

tags.<element>: Element must not be set. The tags element does not apply for this request

tags.set: Element must contain at least one child. At least one sub element must be provided for the element `tag.set`.

Tag.id: Element is required. Provide a value for the element `Tag.id`

Tag.id: Invalid value (value). Value must be an integer set at least to 1.

Tag: Tag specified by ID <id> does not exist or is not available. Provide a value for the element id that corresponds to a valid tag.

## Criteria

Error message	Resolution
Criteria: Field is required.	Specify the name of the criteria to search against.
Criteria: Invalid criteria (<field name>).	Please search against one of the following criteria: %s.
Criteria: Invalid operator for criteria '<field>' (<operator>).	Allowed operations for this criteria are: %s.
Criteria: Value is required for criteria '<field>'.	Specify a value for a field name for search criteria.
Criteria: Invalid value format for criteria '<field>': <value>.	Boolean (true, false). Date and Time in UTC format. Enumeration (allowed options separated by comma). Other: Specify criteria value(s) as <type>.

## Authorization

Error message	Resolution
You are not authorized to access the application through the API.	You must be granted the API Access permission in your roles and scopes.
No data shall be passed for this	The POST request does not specify a data element.

operation.

User is not authorized to perform this operation on specified object(s).

You must be granted access to these objects in your user scope.

Operation %s does not support search filters.

Do not provide search filters for this operation.

## Report storage limit

Error message	Resolution
Your [subscription user] storage limit of <NB> Mb has been reached.	Delete existing reports and try again.