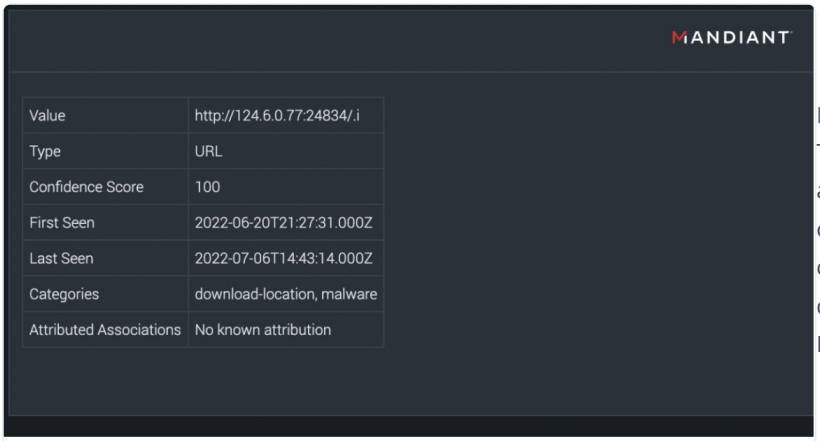
SPLUNK SOAR INTEGRATION

Developed By:	Mandiant
Latest Version:	1.0.0
Last Released:	May 2023
Key Contact:	**Support (https://docs.mandiant.com/home/mandiant-support-cases)**
Download:	**Splunk SOAR Integration (https://splunkbase.splunk.com/app/6858)** (md5: 9d519a219bce0b867b4a4326297c6d45)

Splunk SOAR provides security infrastructure orchestration, case management, playbook automation, and integrated threat intelligence. The solution can ingest security events from various sources, letting security teams track, analyze, and triage events, and use playbooks to automate responses from one interface.



Indicator of Compromise Lookup

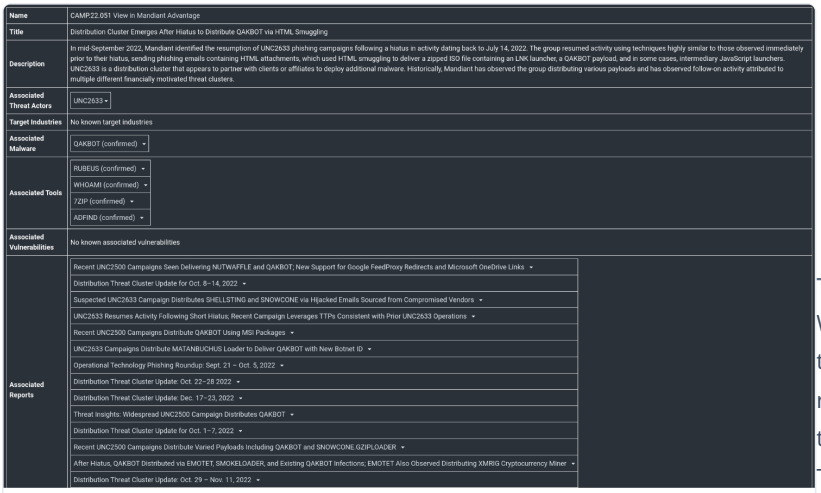
Indicator of Compromise Lookup

The integration lets you look up details about an indicator of compromise, based on the value of the indicator. An indicator can be specified by URL, fully qualified domain name (FQDN), IP Address, or File Hash (MD5/SHA1/SHA256).

Campaign Lookup

Campaign Lookup

The integration lets you look up details about a campaign that has been associated with an Indicator of Compromise (IOC).

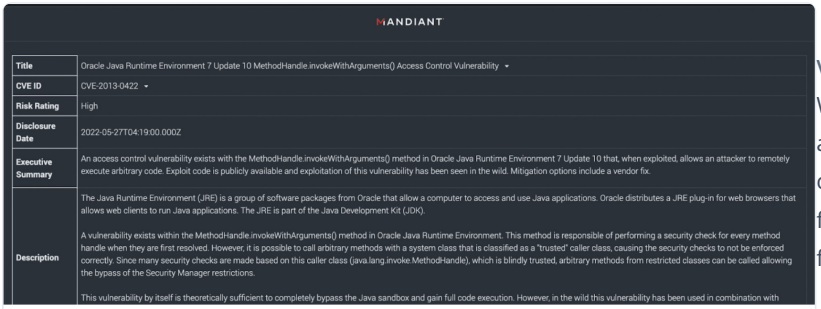


Name	CAMP22.051 View in Mandiant Advantage
Title	Distribution Cluster Emerges After Hiatus to Distribute QAKBOT via HTML Smuggling
Description	In mid-September 2022, Mandiant identified the resumption of UNC2633 phishing campaigns following a hiatus in activity dating back to July 14, 2022. The group resumed activity using techniques highly similar to those observed immediately prior to their hiatus, sending phishing emails containing HTML attachments, which used HTML smuggling to deliver a zipped ISO file containing an LNK launcher, a QAKBOT payload, and in some cases, intermediary JavaScript launchers. UNC2633 is a distribution cluster that appears to partner with clients or affiliates to deploy additional malware. Historically, Mandiant has observed the group distributing various payloads and has observed follow-on activity attributed to multiple different financially motivated threat clusters.
Associated Threat Actors	UNC2633
Target Industries	No known target industries
Associated Malware	QAKBOT (confirmed)
Associated Tools	RUBEUS (confirmed) WHOAMI (confirmed) 7ZIP (confirmed) ADFIND (confirmed)
Associated Vulnerabilities	No known associated vulnerabilities
Associated Reports	Recent UNC2500 Campaigns Seen Delivering NUTWAFFLE and QAKBOT; New Support for Google FeedProxy Redirects and Microsoft OneDrive Links Distribution Threat Cluster Update for Oct. 8–14, 2022 Suspected UNC2633 Campaign Distributes SHELLSTING and SNOWCONE via Hijacked Emails Sourced from Compromised Vendors UNC2633 Resumes Activity Following Short Hiatus; Recent Campaign Leverages TTPs Consistent with Prior UNC2633 Operations Recent UNC2500 Campaigns Distribute QAKBOT Using MSI Packages UNC2633 Campaigns Distribute MATANBUCHUS Loader to Deliver QAKBOT with New Botnet ID Operational Technology Phishing Roundup: Sept. 21 – Oct. 5, 2022 Distribution Threat Cluster Update: Oct. 22–28 2022 Distribution Threat Cluster Update: Dec. 17–23, 2022 Threat Insights: Widespread UNC2500 Campaign Distributes QAKBOT Distribution Threat Cluster Update for Oct. 1–7, 2022 Recent UNC2500 Campaigns Distribute Varied Payloads Including QAKBOT and SNOWCONE.G2IPLOADER After Hiatus, QAKBOT Distributed via EMOTET, SMOKELOADER, and Existing QAKBOT Infections; EMOTET Also Observed Distributing XMRIG Cryptocurrency Miner Distribution Threat Cluster Update: Oct. 29 – Nov. 11, 2022

Threat Actor Lookup

Threat Actor Lookup

When a threat actor is identified as part of the output of the integration, you can request further information about the threat actor from Mandiant Advantage Threat Intelligence (MATI).



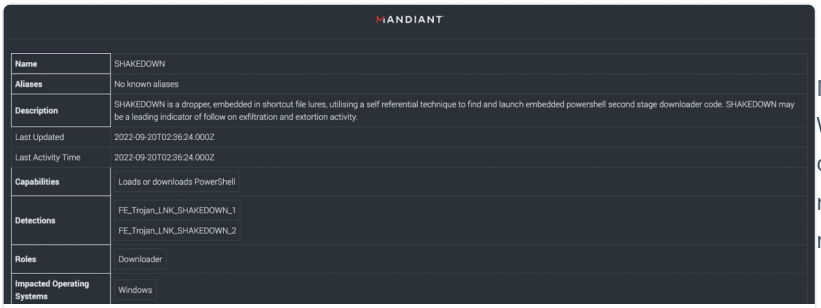
MANDIANT

Title	Oracle Java Runtime Environment 7 Update 10 MethodHandle.invokeWithArguments() Access Control Vulnerability
CVE ID	CVE-2013-0422
Risk Rating	High
Disclosure Date	2022-05-27T04:19:00.000Z
Executive Summary	An access control vulnerability exists with the MethodHandle.invokeWithArguments() method in Oracle Java Runtime Environment 7 Update 10 that, when exploited, allows an attacker to remotely execute arbitrary code. Exploit code is publicly available and exploitation of this vulnerability has been seen in the wild. Mitigation options include a vendor fix.
Description	The Java Runtime Environment (JRE) is a group of software packages from Oracle that allow a computer to access and use Java applications. Oracle distributes a JRE plug-in for web browsers that allows web clients to run Java applications. The JRE is part of the Java Development Kit (JDK). A vulnerability exists within the MethodHandle.invokeWithArguments() method in Oracle Java Runtime Environment. This method is responsible of performing a security check for every method handle when they are first resolved. However, it is possible to call arbitrary methods with a system class that is classified as a "trusted" caller class, causing the security checks to not be enforced correctly. Since many security checks are made based on this caller class (java.lang.invoke.MethodHandle), which is blindly trusted, arbitrary methods from restricted classes can be called allowing the bypass of the Security Manager restrictions. This vulnerability by itself is theoretically sufficient to completely bypass the Java sandbox and gain full code execution. However, in the wild this vulnerability has been used in combination with

Vulnerability/CVE Lookup

Vulnerability/CVE Lookup

When a CVE ID or vulnerability is identified as part of the output from any command/integration, you can request further information about the vulnerability from MATI.



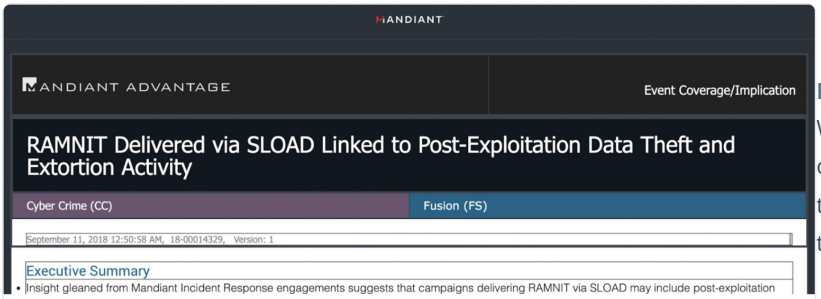
MANDIANT

Name	SHAKEDOWN
Aliases	No known aliases
Description	SHAKEDOWN is a dropper, embedded in shortcut file lures, utilising a self referential technique to find and launch embedded powershell second stage downloader code. SHAKEDOWN may be a leading indicator of follow on exfiltration and extortion activity.
Last Updated	2022-09-20T02:36:24.000Z
Last Activity Time	2022-09-20T02:36:24.000Z
Capabilities	Loads or downloads PowerShell
Detections	FE_Trojan_LNK_SHAKEDOWN_1 FE_Trojan_LNK_SHAKEDOWN_2
Roles	Downloader
Impacted Operating Systems	Windows

Malware Family Lookup

Malware Family Lookup

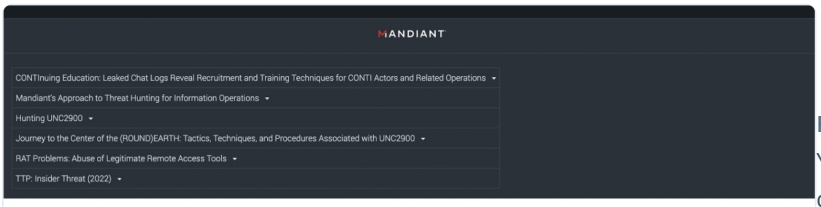
When a malware family is identified as part of the output of the integration, you can request further information about the malware family from MATI.



Report Lookup

Report Lookup

When a report is referenced as part of the output of the integration, you can retrieve the report from MATI and display it within the Splunk SOAR console.



Reports List

Reports List

You can query for reports within a specified date range and with additional Report Type filters, which can then be displayed within the Splunk SOAR console.

Overview

Splunk SOAR provides security infrastructure orchestration, case management, playbook automation, and integrated threat intelligence.

This integration requires three steps:

1. Generate credentials in the MATI platform for Splunk SOAR access using the API.
2. Add the MATI Integration to your Splunk SOAR Configuration.
3. Verify connectivity.

Prerequisites

- A server with Splunk SOAR installed
- Network connectivity to **https://api.intelligence.mandiant.com** over port 443 (HTTPS)
- Network connectivity to your Splunk SOAR instance over port 443 (HTTPS)

> This integration will work with any edition of Splunk SOAR, but limits and restrictions may apply to which features are available. Please see the **Splunk SOAR Documentation (https://docs.splunk.com/Documentation/SOAR/current/User/Intro)** for additional information on limits and restrictions.

Get API Key and Secret

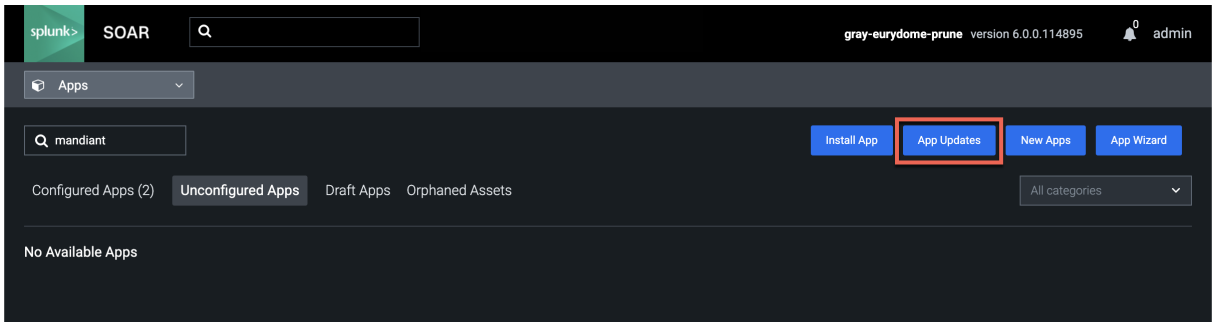
> To obtain a **Service API Key** (which is tied to an organization rather than an individual user) for use with third-party security technologies such as a SIEM, contact **Support (https://www.mandiant.com/support)**.

To obtain an API Key ID and Secret for an individual user account, perform the following:

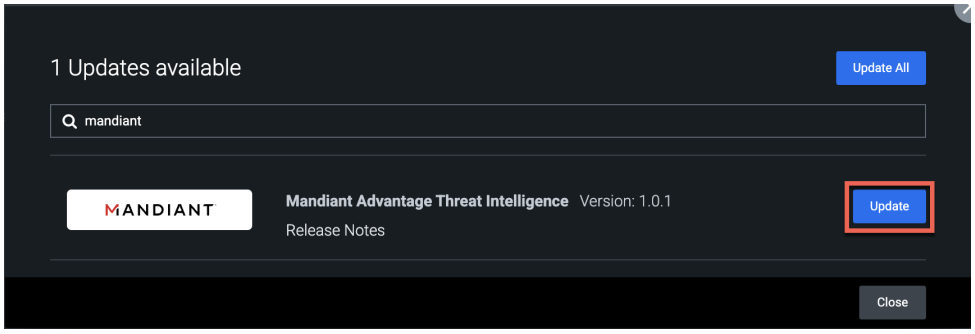
1. Navigate to the Mandiant Threat Intelligence web console.
2. Click **Account Settings**.
3. Select **API Access and Keys** from the navigation menu.
4. Click **Get Key ID and Secret**.
5. Copy and store the displayed values in a secure location.

Setup and installation

1. Log into Splunk SOAR as an Administrator, go to the Apps page and click **App Updates**.



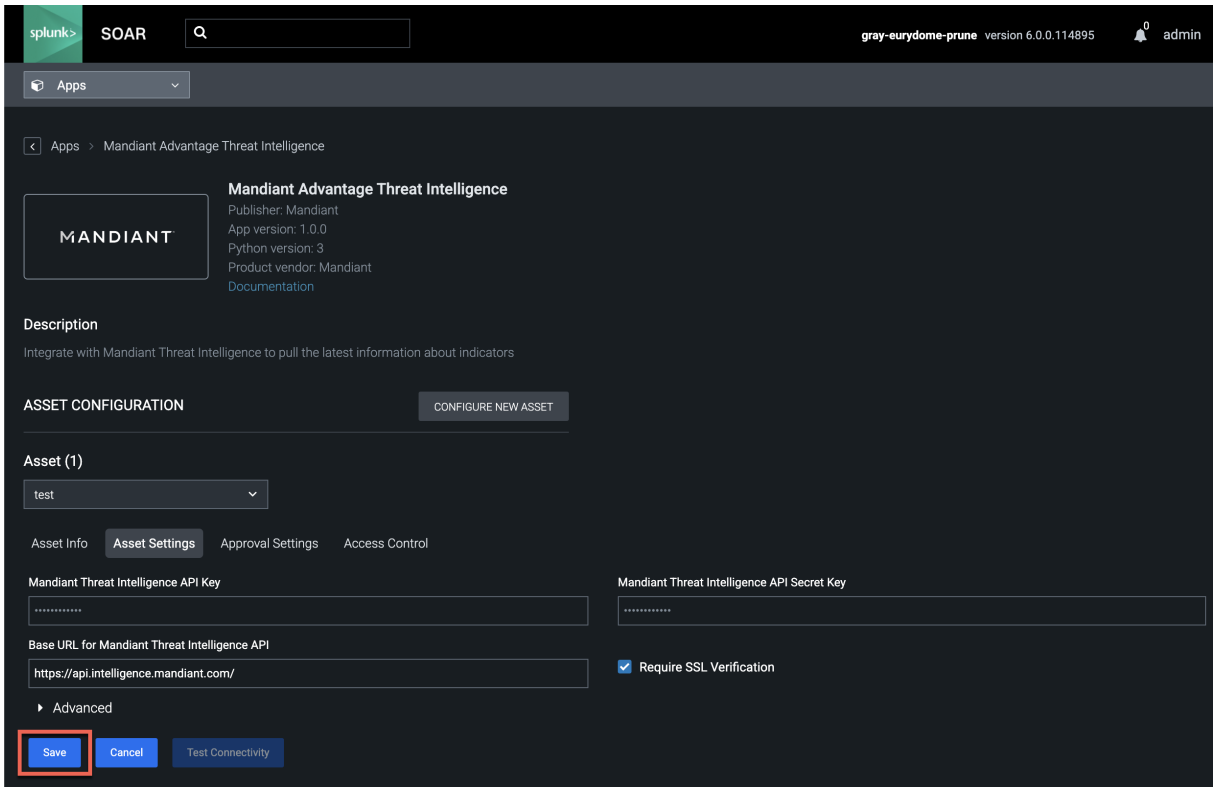
2. Search for "Mandiant" and click **Update** for **Mandiant Advantage Threat Intelligence**.



3. Upload the provided tar file from Step 1 and click **Install.**
4. Search for 'Mandiant' and click **Configure New Asset**.

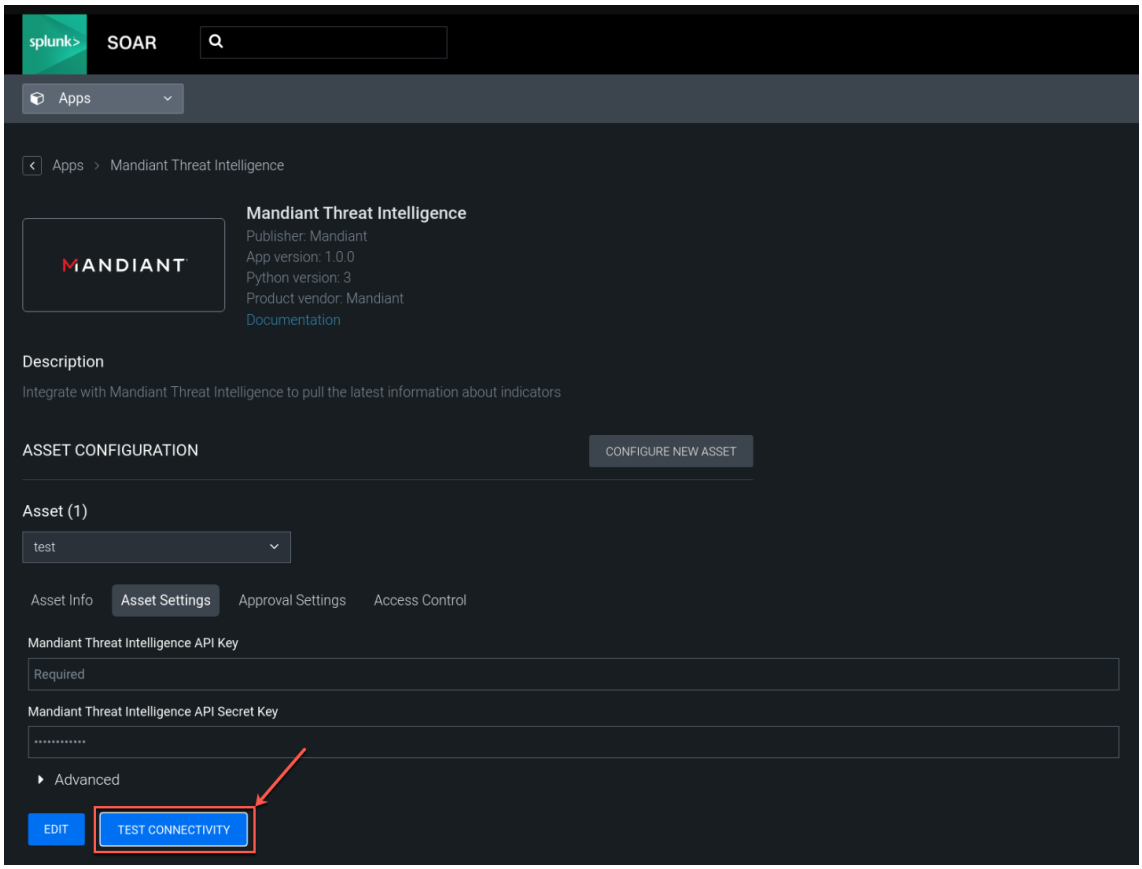
> If **Mandiant Advantage Threat Intelligence** has not been previously configured, it may appear in **Unconfigured Apps**. If a previous configuration exists, it will appear in **Configured Apps**.

5. Fill in an **Asset Name**, then navigate to the **Asset Settings** tab.
6. Fill in your MATI API Key and Secret Key, then click **Save.**



Verify connectivity

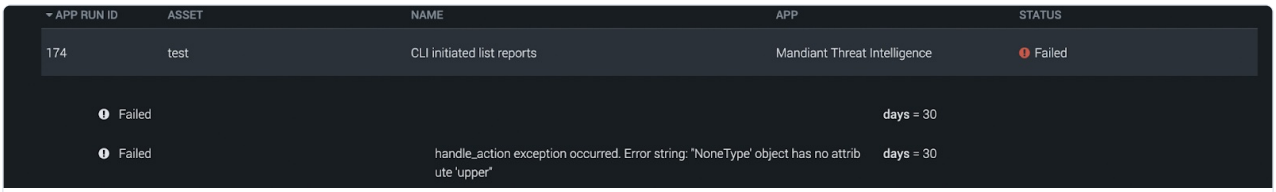
1. Navigate to the **Asset Settings** tab and click **Test Connectivity**.



Troubleshooting

If an error occurs, provide the following information to **Support (https://docs.mandiant.com/home/mandiant-support-cases)**:

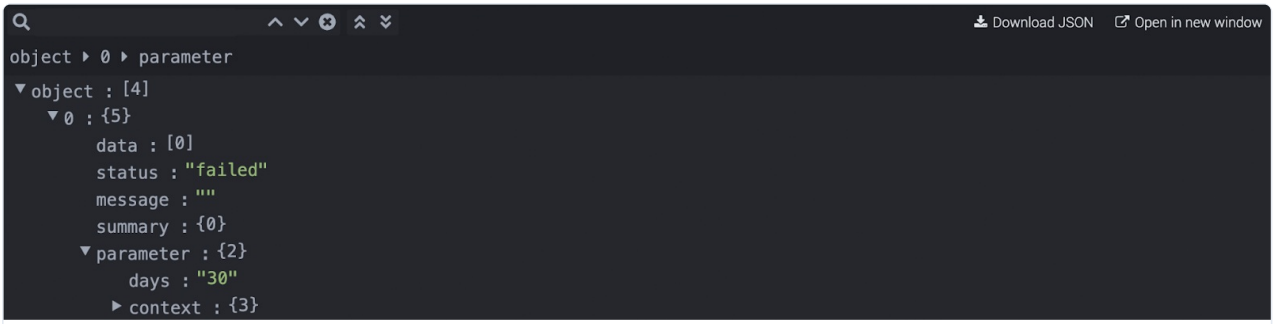
- The text of the exception:



Error Text

- The JSON output of the command:

> Click **Download JSON** to get the entire output as a file.



Error JSON