Frequently Asked Questions

# HYAS **Insight Intel Feed**

## Contents


[How do I get access to the feed?]

[I have registered for the feed but I have not received any information to get started.  Why not?]

[My API key is not working or I have forgotten it - what should I do?]

[Where can I find the API documentation for the feed?]

[How often does the data in the JSON file refresh?]

[Why is the feed structured by malware family?]

[I am new to threat intelligence.  How can I use the tag, ASN, C2, and hash data in my intel ops?]

[Why are only “top” ASNs and tags included in the feed?]

[Why are the C2 IPs shown twice in two different parts of the JSON?]

[Why is some of the malware infrastructure in the feed not as current as the rest?]

[How do I obtain fuller malware analysis that corresponds with this intelligence feed?]

[I have suggestions that would improve the feed.  Where can I share my suggestions?]


Frequently Asked Questions

# HYAS **Insight Intel Feed**

## How do I get access to the feed?

You can register for the feed on the HYAS website at HYAS.com and we'll send you an email with everything you need to get started.

## I have registered for the feed but I have not received any information to get started. Why not?

HYAS vets new registrations to ensure compliance with ITAR designations and to promote use of the feed by appropriate enterprise, government, and nonprofit organizations. If you do not receive an email confirmation, it may be because we are having trouble verifying your identity. We may not provide initial or ongoing access to the feed if you submitted an email address provided by a free email service or a first and last name that can not be publicly verified.

## My API key is not working or I have forgotten it - what should I do?

If you are having a problem with your API key, you can reset it by replying to the email we sent you that includes your API key and other instructions. Simply reply with the single word "reset" in the response and we will issue you a new API key.

## Where can I find the API documentation for the feed?

API documentation for the intel feed feed lives at https://api.hyas.com/docs/mwi-feed/#/Malware

## How often does the data in the JSON file refresh?

The data refreshes every day at 00:00 UTC.

## Why is the feed structured by malware family?

The intelligence in the feed is grouped by malware family because HYAS typically detonates many different samples of malware belonging to the same family in a single day. We eliminate the duplicates and package the intel for each family together so consumers of the feed get a view of the malware that crosscuts individual attacks, threat actors, and infrastructure involving the malware.

## I am new to threat intelligence. How can I use the tag, ASN, C2, and hash data in my intel ops?

There is much more to this topic than can be reviewed here. Some ways to use the intel in this feed include:

- Use the tags and counts to characterize malware families and observe high-level variability (or lack thereof)
- Use ASN, counts, and countries to identify ASN homogeneity and distribution for particular malware families and how they change over time

- Use C2 intelligence to observe the potentially broad range of IPs involved in command and control for the malware family, and the potential relationships across the different C2 IPs
- Use the hashes for detections and correlation (along with the C2 IPs) and for broader malware analysis sourced through OSINT or other services. HYAS Insight provides the full malware report including malware configuration, targets, and TTPs.

### Why are only “top” ASNs and tags included in the feed?

Top ASNs are included in the feed as a way of simplifying the content while still providing some summary information that better describes the infrastructure in place for the individual malware family. Malware infrastructure may concentrate into one or several ASNs which helps you better understand whether additional investigation into those ASNs is warranted. Each malware detonation is enriched with ASN information and much more in HYAS Insight.

### Why are the C2 IPs shown twice in two different parts of the JSON?

The two separate sets of C2s in the feed are included for convenience. The first set is the aggregation of all C2s for that malware family for the day. It is a simple list of nothing more than the C2 IPs. The second set is the pairing of C2s with the hashes for each detonated malware binary. The first set includes all of the C2 from the second set.

### Why is some of the malware infrastructure in the feed not as current as the rest?

The binaries that HYAS detonates will occasionally include samples first seen in the wild some time ago, but are recent submissions for malware detonation and analysis. This could mean that an older malware is still active and should be of concern, so is included in the feed. Third party tools may indicate that some data is “older” but dismissing such data should be done with caution.

### How do I obtain fuller malware analysis that corresponds with this intelligence feed?

Third party tools may help further enrich HYAS Intelligence. HYAS Insight also includes the full malware analysis for all content available in the HYAS feed, including confidence scores, malware processes, corresponding MITRE ATT&CK Matrix, and PDF reports.

### I have suggestions that would improve the feed. Where can I share my suggestions?

We welcome your suggestions on the feed. Send an email to mwi_feed@hyas.com and we’ll certainly consider your suggestions. Thank you for understanding that we may not be able to respond to all suggestions and inquiries.