Malware Intelligence and Enrichment APIs for Anomali ThreatStream™

User Guide v1.6.x

Introduction

As the volume and complexity of cyber threats increase, contextualizing and prioritizing incidents becomes critical. Enterprises struggle to hire enough malware analysts, and enterprise SOC teams are required to deal with an ever-growing queue of alerts. The industry needs to respond to incidents with tools that are effective and simple.

Anomali ThreatStream aggregates and organizes feeds from multiple trusted partners, providing diverse threat intelligence within their platform. PolySwarm seamlessly integrates via API and allows Anomali's users to obtain file and URL reputation services with a single click, in real-time, from a network of commercial and researcher driven malware detection engines. PolySwarm enriches samples with diverse threat indicators and allows threat hunters and SOC analysts to search for and identify relationships between diverse malware families and threat indicators. PolySwarm also provides a final score derived from crowdsourced opinions (PolyScore™), a single number that reflects the probability that a given file contains malware.

PolySwarm uniquely addresses emergent and 0-day malware by using a network of research-driven engines that compete in real-time to detect malware. These engines are niche, highly specialized, and yield better accuracy rates within their field of expertise. Engines are economically rewarded for early and accurate detection and enterprises benefit from deeper coverage of the malware landscape and 0-day threats.

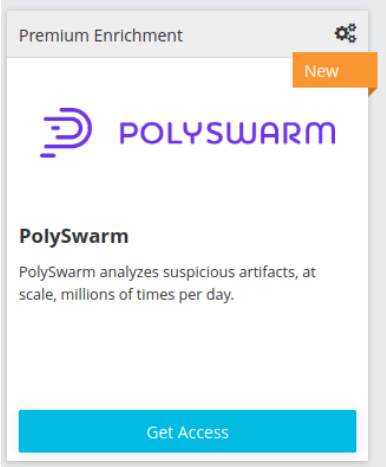
Enrichment Install Prerequisites

1. A PolySwarm API key is required. To obtain an API key, contact your Anomali Sales Engineer/Customer Success Engineer or contact sales@polyswarm.io
2. Have a licensed instance of Anomali.

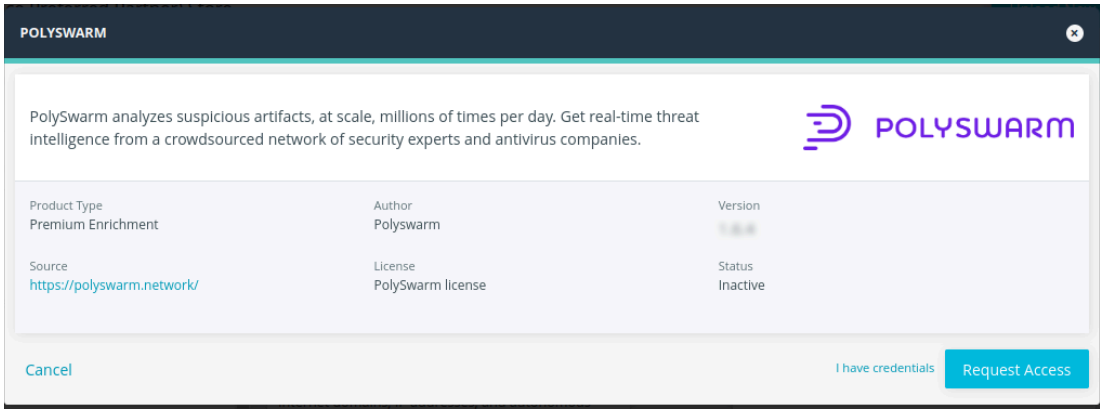
PolySwarm Enrichment

Configuration

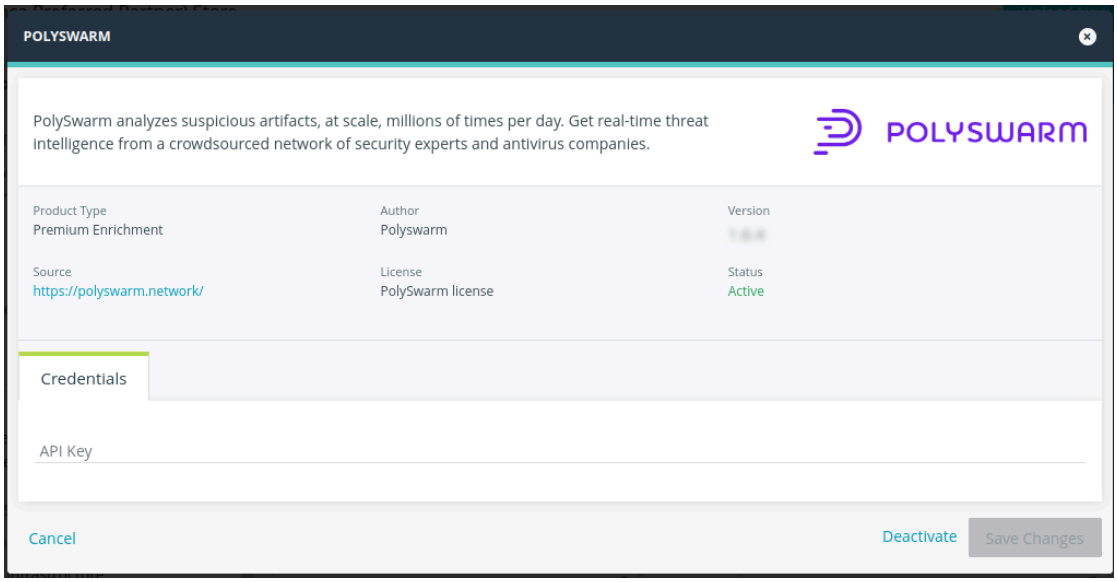
1. Download the enrichment for the APP Store or contact PolySwarm for a guided install
2. On the Polyswarm entry in the APP Store click "Get Access"



3. In the popup, click “I have credentials”



4. Provide the API key gained from Enrichment Install Prerequisites section above



5. Click Save Changes

Enrichment Operation

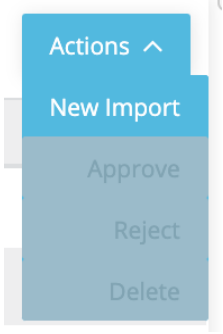
Quick Overview

1. Import your intelligence (SHA256, SHA1 or MD5 digest, domain, ip address)
2. Use PolySwarm's enrichment to view additional details about the hash or malware associated with the domain or ip address.

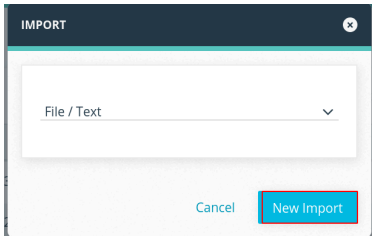
Import Intelligence

1. From the home screen click on **Manage > Import**

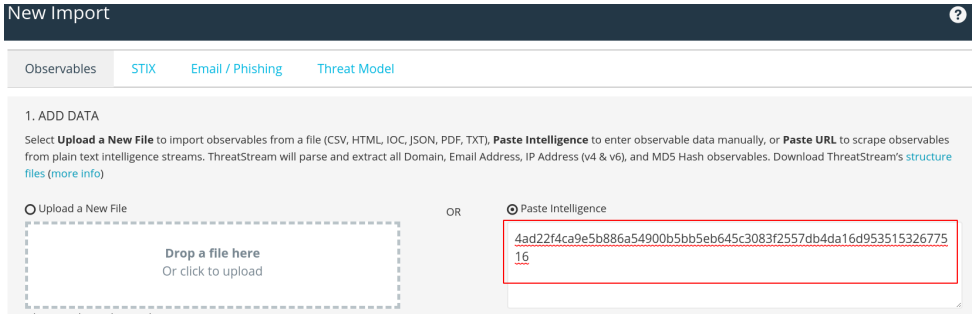
2. From the Imports screen click on **Actions > New Import**

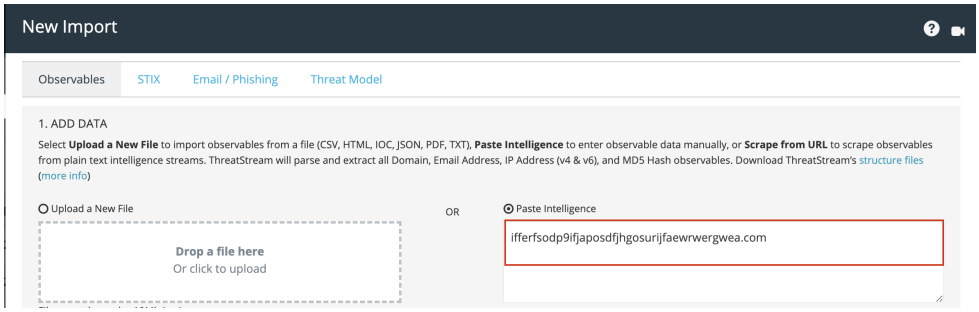


3. Make sure this dialog says **File/Text** then click **New Import**

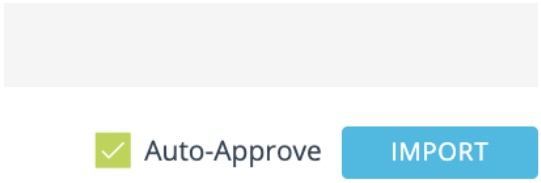


4. Copy your **Hash Value**, **Domain, or IP** into the **Paste Intelligence** section

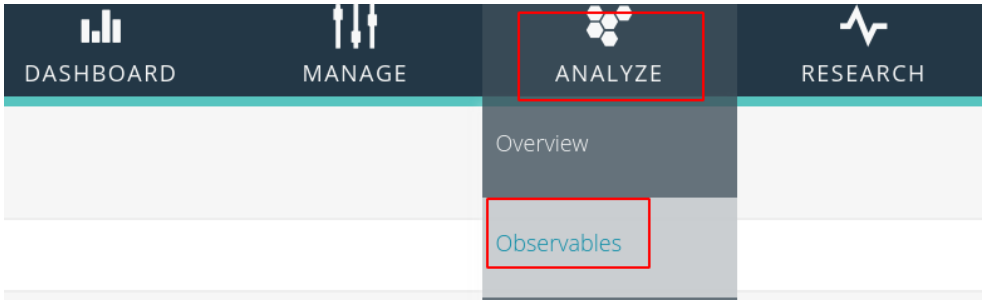




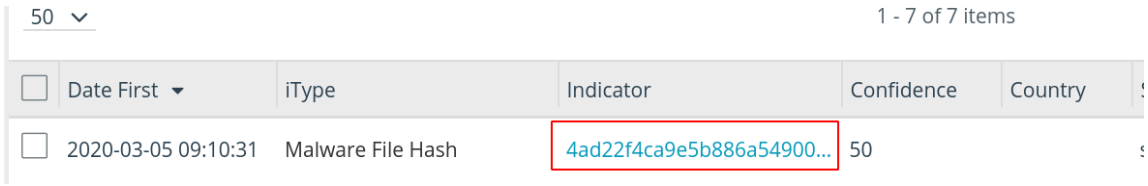
5. At the bottom of the screen click the box to Auto-Approve (if your security policies allow) then click on import.



6. A new Observable should be available to you under the **Analyze Observables** menu at the top of the screen



7. Click on the appropriate Observable to view details. In this case, the hash/domain/ip shown in Step 4



Observable Details - Hash

PolySwarm offers a variety of metadata about this Observable

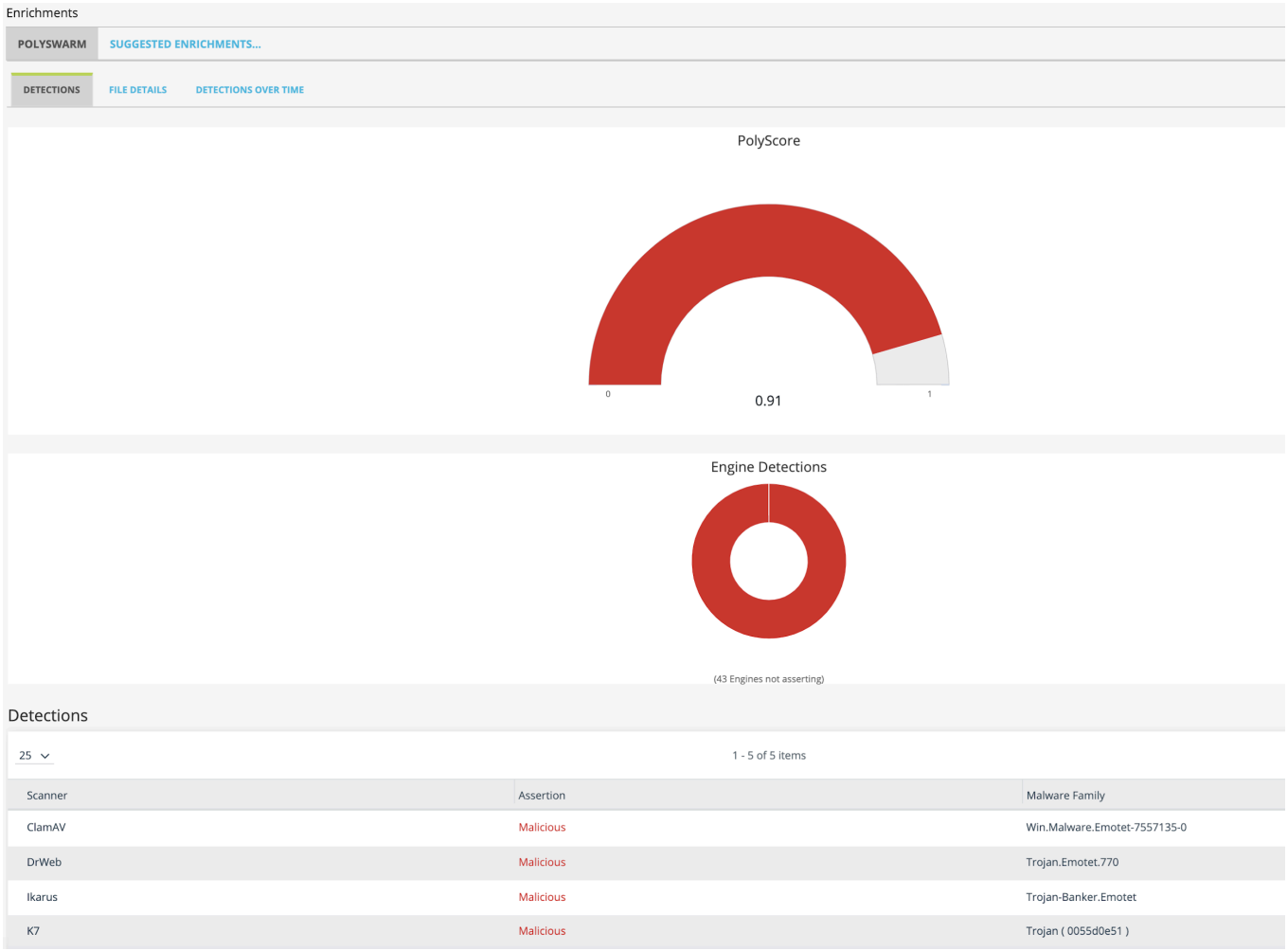
- Malware Detections
- File Details
- Detections Over Time
- Sandbox
- MITRE ATT&CK Framework

Types of hashes supported

- sha256
- md5
- sha1

Malware Detections

The PolyScore represents the likelihood that the artifact is malicious or not. It is a scale between 0 (benign) and 1 (very malicious). The Engine Detections graph is a visual representation of the number of engines that convicted the artifact, the number who found the artifact benign and the number who did not assert. Clicking or hovering over the green or red part of the pie chart will show the number of engines that found the engine benign or malicious. The detections listing is a breakdown of all the engines that responded to the artifact, their assertion (malicious or benign) and the malware family where the scanner assigned the malware (if available). The PolyScore, scanner list and assertions can change over time depending on if the artifact is rescanned or not.



Below the detections chart is a summary of the last scan. Included in this chart is the date of the last scan and a summary of the total assertions count, benign assertions count and malicious assertions count.


Last Scan Summary

25 1 - 4 of 4 items

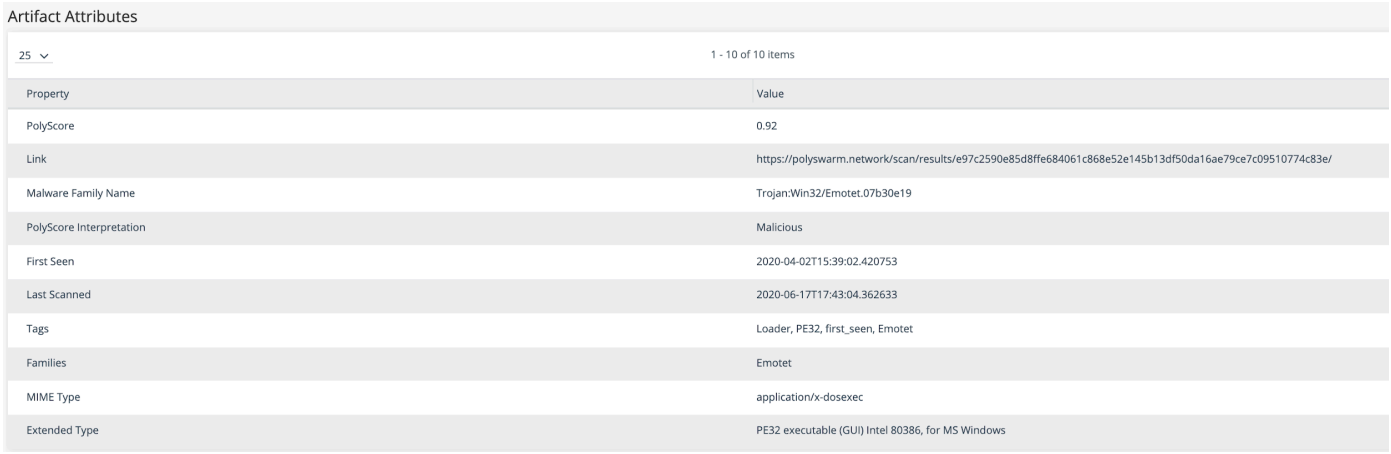
Property	Value
Date	2020-06-17T17:43:04.362633
Total Assertions Count	13
Benign Assertions Count	5
Malicious Assertions Count	8

File Details

Artifact Attributes

Information in this section will give you additional details of the artifact providing additional context about the artifact.

Property	**Possible Values**	**Notes**
PolyScore	0 - 1	Decimal between 0 - 1 that indicates the probability of maliciousness of the artifact taking historical engine performance into account
Link	URL	Permalink to the artifact on polyswarm.network for additional information.
Malware Family Name	String	Malware family name as determined by the longest name provided by an engine
PolyScore Interpretation	Malicious, Suspicious, or Benign	
First Seen	Date and time (UTC)	This is the date and time the file was first seen on the PolySwarm marketplace
Last Scanned	Date and time (UTC)	This is the date and time the file was last scanned on the PolySwarm marketplace
Tags	String	Features and functions of the malware
Families	String	Groups of malware
Countries that Requested a Scan	2 digit county code	Location of IP address that submitted the artifact for scanning
MIME Type		MIMEtype of the file
Extended Type		Extended MIMEtype of the file


Artifact Attributes

25 1 - 10 of 10 items

Property	Value
PolyScore	0.92
Link	https://polyswarm.network/scan/results/e97c2590e85d8ffe684061c868e52e145b13df50da16ae79ce7c09510774c83e/
Malware Family Name	Trojan:Win32/Emotet.07b30e19
PolyScore Interpretation	Malicious
First Seen	2020-04-02T15:39:02.420753
Last Scanned	2020-06-17T17:43:04.362633
Tags	Loader, PE32, first_seen, Emotet
Families	Emotet
MIME Type	application/x-dosexec
Extended Type	PE32 executable (GUI) Intel 80386, for MS Windows

Artifact Hashes

Depending on the artifact type, not all hashes may be shown. Some hashes are not supported on some artifact types.

Property	Possible Values	Notes
authentihash	Any valid hash for the given type	Fuzzy hash value used to find similar files
md5	Any valid hash for the given type	MD5 of artifact
sha1	Any valid hash for the given type	SHA1 of artifact
sha256	Any valid hash for the given type	SHA256 of artifact
sha512	Any valid hash for the given type	SHA512 of artifact
ssdeep	Any valid hash for the given type	Fuzzy hash value used to find similar files
tlsh	Any valid hash for the given type	Fuzzy hash value used to find similar files
imphash	Any valid hash for the given type	Hash of the import functions of the artifact (only visible for PE files)

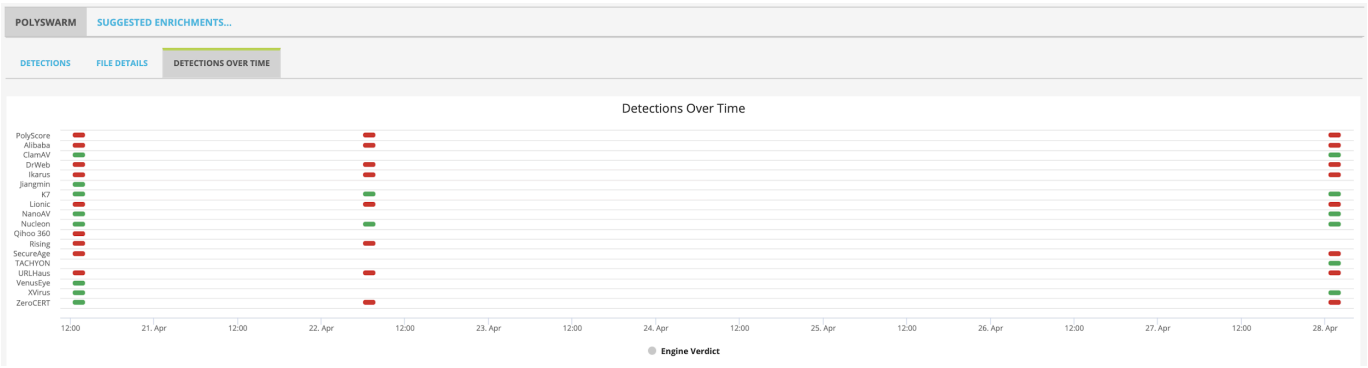
Artifact Hashes

25 1 - 8 of 8 items

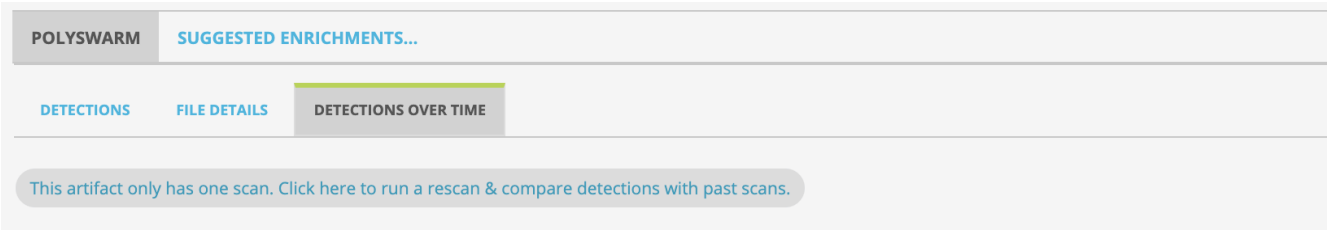
Hash Type	Value
authentihash	6a0f5ca9c50edea038f28a69f46e044acbca157705a37867d74ff3a39f5bb22d
md5	4d216210e347ebe50631cb723e6a5d69
sha1	28e494948444f2d14efe2a59ce9659508eaaa678
sha256	e97c2590e85d8ffe684061c868e52e145b13df50da16ae79ce7c09510774c83e
sha512	ae1620948964957013d9dbdbd7f0f9a6724a4ff3ac263f0590d2afb1af7084377a5b199fdb1295af7625056dfedc755822b5da50bce0184438e88b5fef52ea34
ssdeep	1536:45tJYSOr9tO4MPgKeFU5nJgJ4CLxsn30DVx4Nd29:f/tO4M4KeJSCUkAe
tlsh	cab37c027a3a5c83e29884308c57da7829b1fc936a6056b733e1ff6f1d32542da7521f
imphash	60ea828f72cac35ca99a70349dd4e0d1

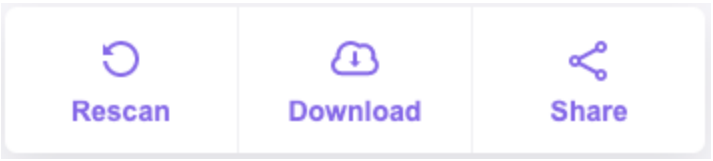
Detections Over Time

This shows trends over time for the PolyScore and engine verdicts on the maliciousness of the artifact. This information is only available in the Anomali integration. Normally only the first and last scan is available in our metadata. PolyScores are normally created on the fly using the latest scoring methodology and engine results when a hash lookup is requested. Historical PolyScores could be based on prior models and applied to the assertions and engine's recent history at the time of scan. PolyScores across models are not comparable. Note: Sometimes the chart may not show the labels of all the engines on the y-axis due to limits in chart sizes. Hovering your mouse over any of the red or green dots will show the engine and their verdict.

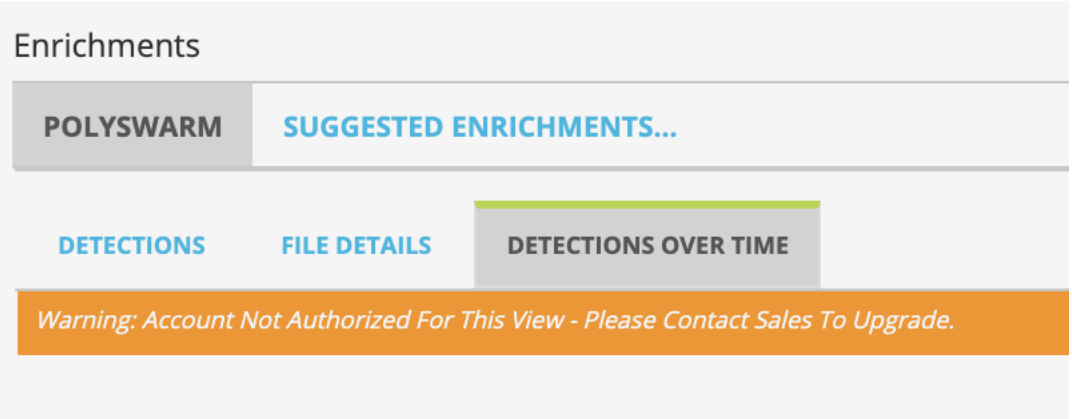


If there has only been a single scan done on the artifact, then you will see the message below along with the same table as the detections tab. If you click on the message, you will be redirected to the polyswarm.network portal where you can click on Rescan to resubmit the artifact to the engines to get an updated scan result. Once the results have been returned, if you refresh the ThreatStream screen, the updated results will be displayed.





If you get the following error message, your API key does not have the correct permissions. Please contact PolySwarm support for assistance (support@polyswarm.io)

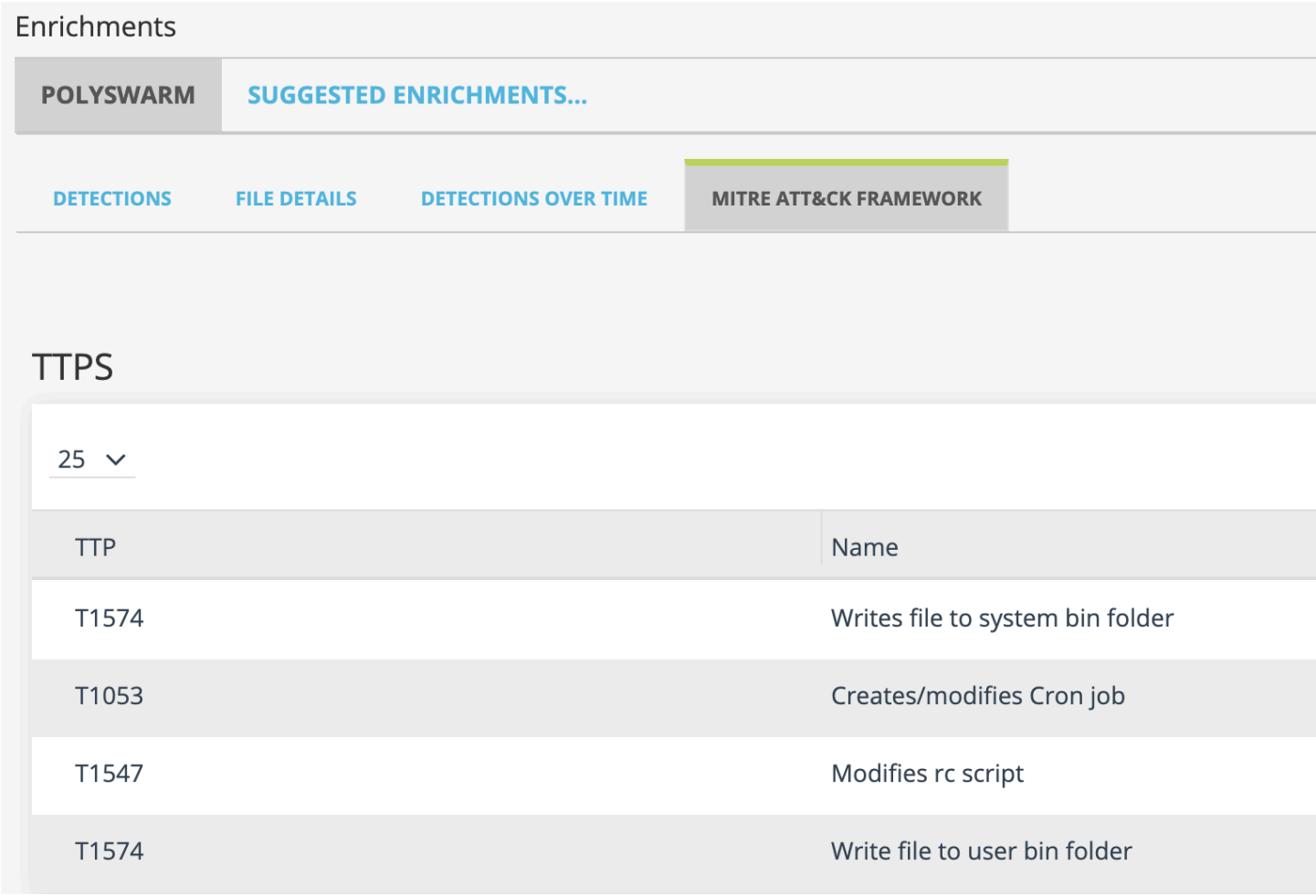


Sandbox

This tab displays the imphash and all ip addresses, urls, and domains that our sandboxes have extracted from the malware. Not all samples have been run through our sandboxes so not all samples will have data on this tab.

MITRE ATT&CK Framework

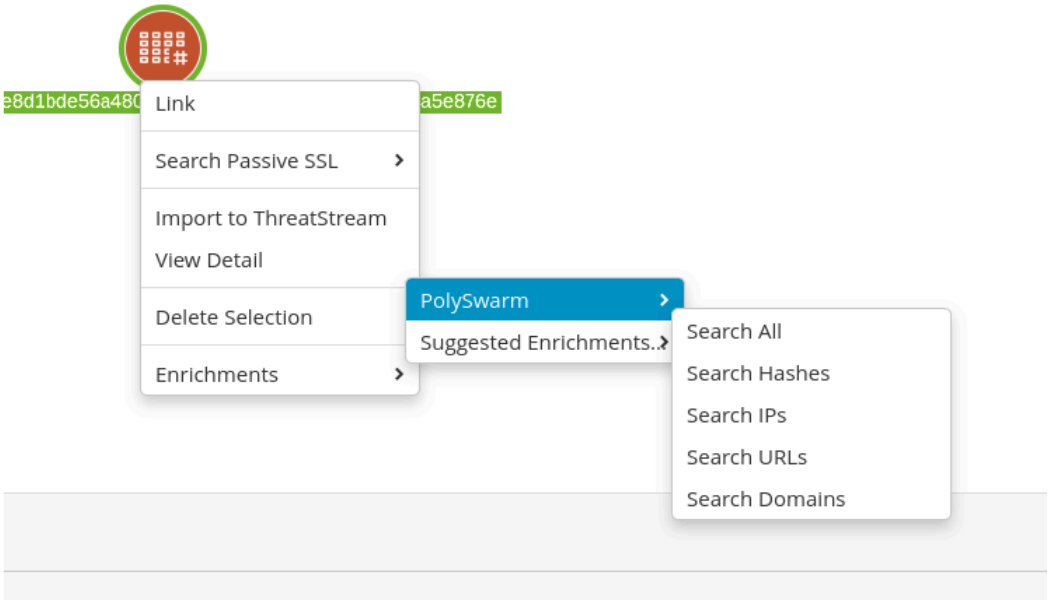
This tab displays the tactics, techniques, and procedures (TTPs) that the malware has displayed when it was run in our sandboxes. Not all samples are run through our sandboxes so not all samples will have data on this tab. More information about the MITRE ATT&CK Framework can be found at https://attack.mitre.org/



Enrichment View - Hash

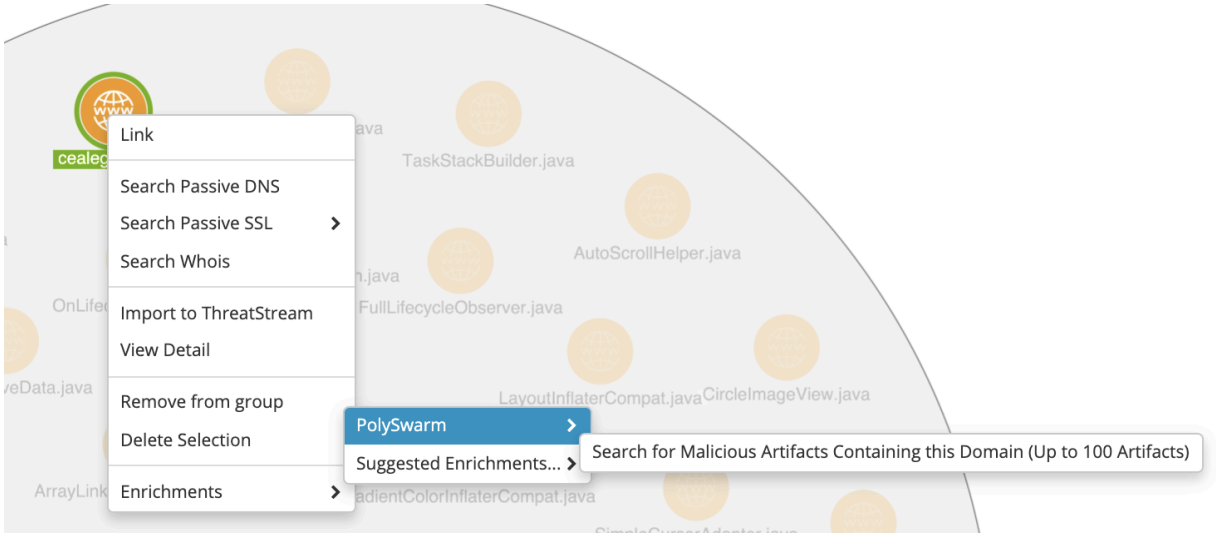
The PolySwarm Enrichment View allows the analyst to pivot to similar file indicators such as associated file names, associated malware and IP/domain information related to the hash of the Observable using PolySwarm's metadata.

- Right clicking the hash will bring up the option to enrich your hash using PolySwarm's metadata.



Enrichment Type	Details
Search Hashes	Creates node that contains a number of other hashes associated to the Observable
Search IPs	List all the IPs discovered during static analysis of the file up to a limit of 50 returned values.
Search URLs	List all the URLs discovered during static analysis of the file up to a limit of 50 returned values.
Search Domains	List all the domain(s) discovered during static analysis of the file up to a limit of 50 returned values.

- If the Observable has associated domains, right clicking on the domain will bring up the option to search for other malware artifacts that contain the same domain (up to 100 artifacts)



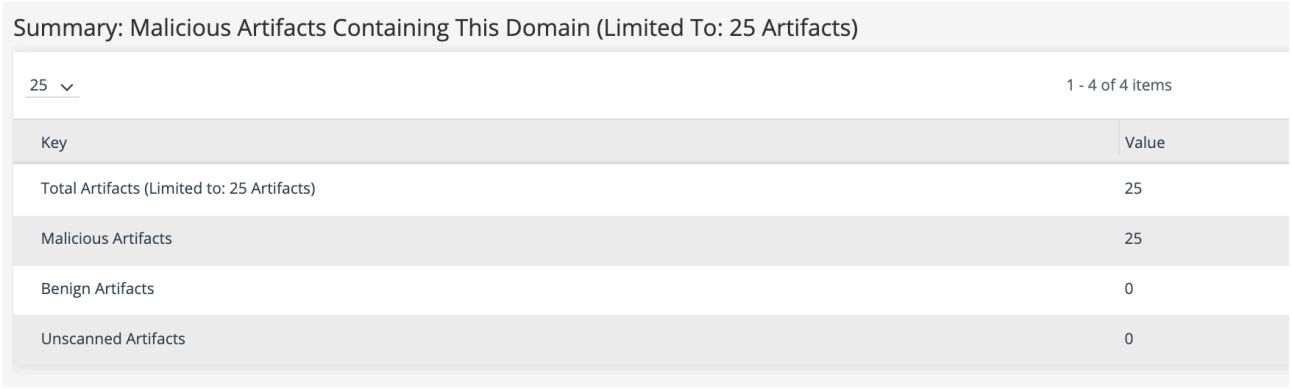
Observable Details - Domain

PolySwarm offers a variety of additional information about this Observable

- Summary of Related Files
- Related Files
- Detections for the Related Files

Summary: Malicious Artifacts Containing This Domain

This chart shows the number of linked artifacts within the PolySwarm marketplace that contain the domain in question and if these samples are malicious or benign. Because some domains may be contained in 1000's of samples, results are limited to 25 artifacts.


Summary: Malicious Artifacts Containing This Domain (Limited To: 25 Artifacts)

25 ⌄ 1 - 4 of 4 items

Key	Value
Total Artifacts (Limited to: 25 Artifacts)	25
Malicious Artifacts	25
Benign Artifacts	0
Unscanned Artifacts	0

Related Artifacts

This chart shows hashes of other artifacts that contain the same observable domain. Additional information about the hash is also shown including if it is malicious or benign, number of engines that detected the sample malicious based on the last scan done on the artifact and the associated PolyScore of the file. Note: The full hash may not be fully shown so you may need to adjust the column sizes to expose the full hash.

Malicious Artifacts Containing this Domain (Limited to: 25 Artifacts)

25 1 - 25 of 25 items

SHA-256	Verdict	Engines Marking Malicious	PolyScore
040303ec6e334c5173248432073f2283ad287af7c6a520ecfd87f45d4a0...	Malicious	5/10	0.79
56d670ad40ec8f23ec2d519a224de87df2cf15bde82bcf05cad4330c8b...	Malicious	7/11	0.79
ed36213c65d2472f3e476cccf29b7ade860a5fcd3f670954a723a827d00...	Malicious	10/14	0.99
2868545ae9aad1872b644951138b4b8edc226e0e95af94bcfe9f579430...	Malicious	11/14	0.99
34d7fb27ad756f8c944fa54686c3270e01022cd015ce86d7bcc568fd412...	Malicious	7/12	0.99
46f211a7d2191bacbff454dc765b6d13f0b676347e73a753369319280f...	Malicious	11/13	0.99
0d30b4886033a4a66544ba786c3f91f86acf3c7d2034aebfd481e7f9c00...	Malicious	13/14	0.99
f8d7aa83fbe2d98fdab9d60e2c620e4eec6e7dcdae210c47e1257eec3d...	Malicious	11/13	0.99
b6f52381d7679e7595424594f4a1e7628bdd1a1d1832e8454399b3504...	Malicious	11/13	0.98
eee40388393b2078022b29479dd3e74f4d5cc8c73ffd7a2cdd7a034782...	Malicious	12/17	0.99
884c4cc639c28e454c009c5c059a8c1f171f394493de29d232e681be97...	Malicious	11/12	0.99
e618779067544936ec65735a2e7216f65af9e7d1e62fb21f76d92b7788...	Suspicious	7/10	0.52
c5c2bf7c330957fa9d107e3a297a51e8807a604930d161f1c60814bd4d...	Malicious	12/14	0.99
683e42142284a59934b7ab15c2e3f2e02a752bde1240bac90198cfb66...	Malicious	9/11	0.99
4c8d13bf9ce95bf59d65e992517b8b372d56c33e2b1eb9eeb91359e57...	Malicious	11/17	0.99
bee1fa90753e36510eb191ca7e73e468045807e5e8320bca7f8fec1f79e...	Malicious	10/13	0.99
db933512f5908900cec144de8928a71692ba16c6b783848302146da95...	Malicious	7/12	0.98
1a6c822ad0073bb758b3548a0a3a99fc716f504070edd0a5c6b9af664f...	Malicious	8/12	0.98

Detections on Related File Listing

This shows details on all of the related files from the above listing with full breakout of all engine assertions and associated malware family (if applicable and provided). There is a similar entry for each of the related files in the related files listing.

Scan Results For Ed36213c65d2472f3e476cccf29b7ade860a5fcd3f670954a723a827d00f5a9d

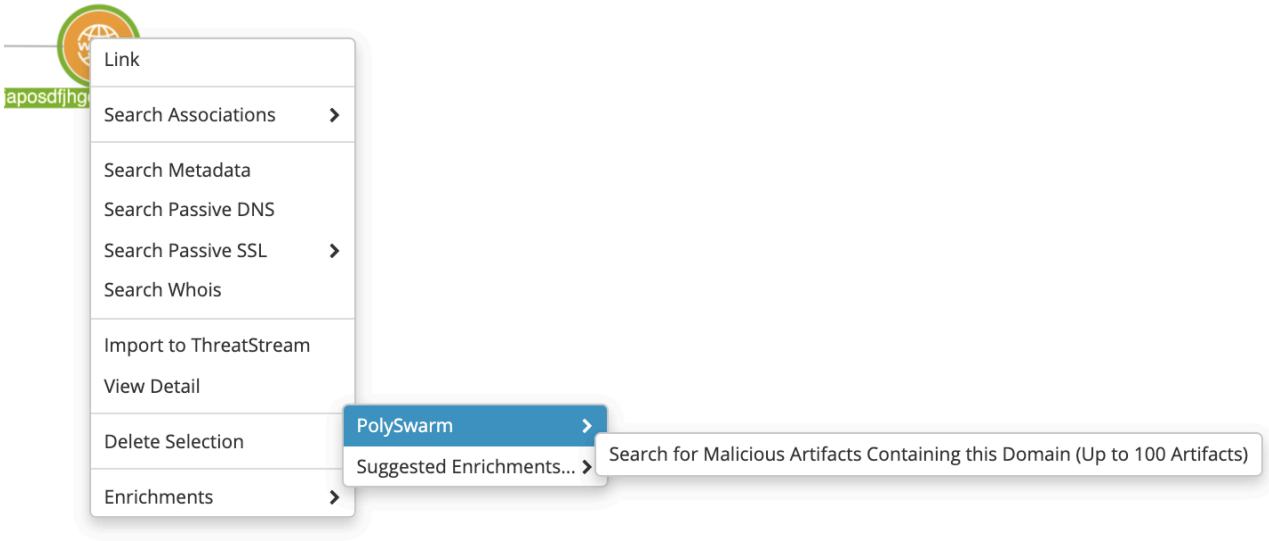
25 1 - 14 of 14 items

Scanner	Assertion	Malware Family
0x29CeEdc17fDFe3E024e6d8BE0B24Ef59B2d52C04	Malicious	win/malicious
Alibaba	Benign	
ClamAV	Malicious	Win.Ransomware.WannaCry-6313787-0
DrWeb	Malicious	Trojan.Encoder.11432
Ikarus	Malicious	Trojan-Ransom.WannaCry
Jiangmin	Malicious	Trojan.Wanna.k
K7	Malicious	Trojan (00557fc41)
Lionic	Benign	
NanoAV	Malicious	Trojan.Win32.Wanna.epxkni
Nucleon	Benign	
Rising	Malicious	Ransom.Wanna!8.E7B2
SecureAge	Malicious	
VenusEye	Malicious	
XVirus	Benign	

Enrichment View - Domain

The PolySwarm Enrichment View allows the analyst from a graphical view to see all associated hashes for the domain in question.

- Right clicking the hash will bring up the option to enrich the domain with any associated hashes that contain this domain. Resulting hashes are in SHA256 format. Total results are limited to 100 artifacts. Depending on your Node Search Limit setting, you may need to rerun this enrichment several times to see all 100 potential results.



- Exploding out the hash node will show all the related hash values. Hovering over a hash will show the other hash values (MD5, SHA1) and latest scan results of the given SHA256 hash. You will need to scroll over to see this additional information.

Enrichment View - IP

The PolySwarm Enrichment View allows the analyst from a graphical view to see all associated hashes for the ip in question.

- Right clicking the hash will bring up the option to enrich the ip with any associated hashes that contain this ip. Resulting hashes are in SHA256 format. Total results are limited to 100 artifacts. Depending on your Node Search Limit setting, you may need to rerun this enrichment several times to see all 100 potential results.