Inbound and Outbound Statistics Response Values

https://campus.barracuda.com/doc/96023079/

The Get Statistics API retrieves your account or domain level inbound and outbound statistics.

The statistics results are reported in the form `action:threat_type:reason`. Refer to the tables below for detailed descriptions of the different actions, threat types, and reasons.

Name	Description
action	The action Email Gateway Defense took with the message.
threat_type	The email threat type Email Gateway Defense protected the message against.
reason	The reason Email Gateway Defense took action with the message.

Table 1. Actions

For more details, see Message Actions Table 2.

Action	Description
allowed	Delivered messages.
blocked	Blocked messages. Messages are blocked due to policies specified on the **Inbound Settings** and **Outbound Settings** pages.
deferred	Deferred messages. Indicates that Email Gateway Defense returned a 4xx response to the sending mail server.
quarantined	Quarantined messages. Messages are quarantined due to policies specified on the **Inbound Settings** and **Outbound Settings** pages.

Table 2. Threat Types

Threat Type	Description
none (none)	A valid message and not classified as a threat type.
data_exfiltration (Data Exfiltration)	Unauthorized transfer of data from a computer or other device. Data exfiltration can be conducted manually via physical access to a computer and as an automated process using malicious programming on the internet or a network.
domain_impersonation (Domain Impersonation)	Often used by hackers as part of a conversation-hijacking attack. Attackers attempt to impersonate a domain by using techniques such as typosquatting, replacing one or more letters in a legitimate email domain with a similar letter or adding a hard-to-notice letter to the legitimate email domain.

malware (Malware)	Email that delivers documents containing malicious software. The malware is either hidden directly in the document itself, or an embedded script downloads it from an external website. Common types of malware include viruses, Trojans, spyware, worms, and ransomware.
phishing (Phishing)	Attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. Cybercriminals research their targets and craft carefully designed messages, often impersonating a trusted colleague, website, or business.
policy (Policy)	Custom inbound and outbound policies specifically applied to a given domain to set security protocols.
scamming (Scamming)	Fraudulent schemes to defraud victims or steal their identity by tricking them into disclosing personal information. Examples of scamming include fake job postings, investment opportunities, inheritance notifications, lottery prizes, and fund transfers.
spam (Spam)	Unsolicited bulk email messages, also known as junk email. Spam comes in various forms. Some spam emails push scams. Others are used to conduct email fraud. Spam also comes in the form of phishing emails that use brand impersonation to trick users into revealing personal information, such as login credentials and credit card details.
url_phishing (Url Phishing)	Email to direct their victims to enter sensitive information such as usernames, passwords, or banking details, on a fake website that looks like a legitimate website. Cybercriminals often use that sensitive information for malicious use.

Table 3. Reasons

Each reason corresponds to a message action in the Message Log. For detailed descriptions of the message actions, see Message Actions Table 1.

Reason	Message Action
_total	Total number of messages in the results that includes all message actions in the specified threat type
account_suspended	Account Suspended
advanced_threat_detection	Advanced Threat Detection (ATD)
anti_fraud	Anti-Fraud
anti_virus	Antivirus
atd_exempt	Advanced Threat Detection (ATD) Exempt
attachment_content	Attachment Content
attachment_filter	Attachment Filter
av_service_unavailable	AV Service Unavailable

barracuda_realtime_system	Barracuda Real-Time System (BRTS)
barracuda_reputation	Barracuda Reputation
body_content	Body Content
bulk_email	Bulk Email
cloudscan_service_unavailable	Cloudscan Service Unavailable
content_protected	Content Protected
content_protected_msdoc	Content Protected MS Document
content_url	Content URL
dkim	DKIM
dmarc	DMARC
emailcat	Email Categorization
from_address	From Address
header_content	Header Content
geoip_policy	GeoIP Policies
image_analysis	Image Analysis
inbound_tls_required	Inbound TLS Required
intent_analysis	Intent Analysis
invalid_recipient	Invalid Recipient
ip_policy	IP Policy
language_policy	Language Policies
malformed	Malformed
message_delivery_interrupted	Message Delivery Interrupted
message_too_large	Message Too Large
no_ptr_record	No PTR Record
office_macros	Office Macros
password_protected_pdf_filtering	Content Protected PDF Filtering
pending_scan	Pending Scan
phishline	Security Awareness Training
possible_mail_loop	Possible Mail Loop
predefined_filter_exception	Predefined Filter Exception
predefined_attachment_content	Predefined Attachment Content
predefined_body_content	Predefined Body Content
predefined_header_content	Predefined Header Content
predefined_recipient_content	Predefined To/CC Address
predefined_sender_content	Predefined From Address
predefined_subject_content	Predefined Subject Content

quarantined_atd_scan_inconclusive	ATD Scan Inclusive
rate_control	Rate Control
realtime_block_list	Realtime Block List
recipient	Recipient
recipient_list	Recipients List
remediated_by_forensics	Remediated by Incident Response
remediated_by_sentinel	Remediated by Impersonation Protection
score	Score
sender_email_address	Sender Email Address
sender_policy	Sender Policies
sender_spoof_protection	Sender Spoof Protection
sent_to_spam_categorization	Sent to Spam Categorization
spf	Sender Policy Framework (SPF)
subject_content	Subject Content
suspicious	Suspicious
system_sender_policy	System Sender Policies
to_address	To/CC Address
tls_required	TLS Required
ui_delivered	UI Delivered

Examples

In the sample response below,

- `allowed:none:_total` indicates the total number of messages that was allowed and did not classify as any of the threat types.
- `allowed:none:none` indicates the number of messages that was allowed and did not classify as any of the threat types.


```
        "allowed:none:_total": {
            "2020-08-01T00:00:00+0000": 154562,
            "2020-08-02T00:00:00+0000": 68261,
            "2020-08-03T00:00:00+0000": 124327,
            "2020-08-04T00:00:00+0000": 236073,
            "2020-08-05T00:00:00+0000": 247927
        },
        "allowed:none:none": {
            "2020-08-01T00:00:00+0000": 154562,
            "2020-08-02T00:00:00+0000": 68261,
```

```
            "2020-08-03T00:00:00+0000": 124327,
            "2020-08-04T00:00:00+0000": 236073,
            "2020-08-05T00:00:00+0000": 247927
        }
```

In the sample response below,

- `blocked:domain_impersonation:_total` indicates the total number of messages that was blocked, classified as a Domain Impersonation threat type, and included all message actions in the results (DKIM, DMARC, No PTR Records, Sender Policy Framework (SPF)).
- `blocked:domain_impersonation:dkim` indicates the number of messages that was blocked and classified as a Domain Impersonation threat type and a DKIM message action.
- `blocked:domain_impersonation:dmarc` indicates the number of messages that was blocked and classified as a Domain Impersonation threat type and a DMARC message action.
- `blocked:domain_impersonation:no_ptr_records` indicates the number of messages that was blocked and classified as a Domain Impersonation threat type and a No PTR Records action.
- `blocked:domain_impersonation:spf` indicates the number of messages that was blocked and classified as a Domain Impersonation threat type and a Sender Policy Framework (SPF) action.

```
        "blocked:domain_impersonation:_total": {
            "2020-08-01T00:00:00+0000": 3185,
            "2020-08-02T00:00:00+0000": 2945,
            "2020-08-03T00:00:00+0000": 2503,
            "2020-08-04T00:00:00+0000": 971,
            "2020-08-05T00:00:00+0000": 3310
        },
        "blocked:domain_impersonation:dkim": {
            "2020-08-01T00:00:00+0000": 2439,
            "2020-08-02T00:00:00+0000": 2219,
            "2020-08-03T00:00:00+0000": 151,
            "2020-08-04T00:00:00+0000": 153,
            "2020-08-05T00:00:00+0000": 2519
        },
        "blocked:domain_impersonation:dmarc": {
            "2020-08-01T00:00:00+0000": 21,
            "2020-08-02T00:00:00+0000": 8,
            "2020-08-03T00:00:00+0000": 25,
            "2020-08-04T00:00:00+0000": 22,
            "2020-08-05T00:00:00+0000": 34
        },
        "blocked:domain_impersonation:no_ptr_records": {
            "2020-08-01T00:00:00+0000": 641,
            "2020-08-02T00:00:00+0000": 568,
            "2020-08-03T00:00:00+0000": 636,
```

```
            "2020-08-04T00:00:00+0000": 699,
            "2020-08-05T00:00:00+0000": 678
        },
        "blocked:domain_impersonation:spf": {
            "2020-08-01T00:00:00+0000": 84,
            "2020-08-02T00:00:00+0000": 150,
            "2020-08-03T00:00:00+0000": 1691,
            "2020-08-04T00:00:00+0000": 97,
            "2020-08-05T00:00:00+0000": 79
        }
```