IMAP Inspector

IMAP Inspector Overview

Type	Inspector (service)
Usage	Inspect
Instance Type	Multiton
Other Inspectors Required	`stream_tcp`
Enabled	`true`

Internet Message Application Protocol (IMAP) enables email clients to retrieve messages from a remote IMAP3 server. An IMAP3 server uses TCP port 143 for insecure sessions or TCP port 993 for IMAP over SSL/TLS.

The `imap` inspector detects IMAP traffic and analyzes IMAP commands and responses.

The `imap` inspector can identify the command, header, and body sections of IMAP messages, and extract and decode multi-purpose internet mail extensions (MIME) attachments. MIME attachments may include multiple attachments and large attachments that span multiple packets.

The `imap` inspector identifies and adds IMAP traffic to the Snort allow list. When enabled, intrusion rules generate events on anomalous IMAP traffic.

IMAP Inspector Parameters

IMAP service configuration

The `binder` inspector defines the IMAP `service` configuration. For more information, see the Binder Inspector Overview.

Example:

```
[
    {
        "when": {
            "service": "imap",
            "role": any
        },
        "use": {
            "type": "imap"
        }
    }
]
```

b_64_decode_depth

Specifies the maximum number of bytes to extract and decode from each Base64 encoded MIME email attachment. You can specify an integer less than 65535, or specify 0 to disable decoding. Specify -1 to place no limit on the number of bytes to decode.

You can enable rule 141:4 to generate events for this parameter, and in an inline deployment, drop offending packets when decoding fails (due to incorrect encoding or corrupted data).

Type: integer

Valid range: `-1` to `65535`

Default value: `-1`

bitenc_decode_depth

Specifies the maximum number of bytes to extract from each non-encoded MIME email attachment. You can specify an integer less than 65535, or specify 0 to disable the extraction of the non-encoded MIME attachment. Specify -1 to place no limit on the number of bytes to extract. These attachment types include 7-bit, 8-bit, binary, and various multipart content types such as plain text, JPEG and PNG images, and MP4 files.

Type: integer

Valid range: `-1` to `65535`

Default value: `-1`

decompress_pdf

Specifies whether to decompress `application/pdf` (PDF) files in MIME attachments.

You can enable rule 141:8 to generate events for this parameter, and in an inline deployment, drop offending packets.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

decompress_swf

Specifies whether to decompress `application/vnd.adobe.flash-movie` (SWF) files in MIME attachments.

You can enable rule 141:8 to generate events for this parameter, and in an inline deployment, drop offending packets.

Type: integer

Valid values: `true`, `false`

Default value: `false`

decompress_vba

Specifies whether to decompress Microsoft Office Visual Basic for Applications macro files in MIME attachments.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

decompress_zip

Specifies whether to decompress `application/zip` (ZIP) files in MIME attachments.

You can enable rule 141:8 to generate events for this parameter, and in an inline deployment, drop offending packets.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

qp_decode_depth

Specifies the maximum number of bytes to extract and decode from each quoted-printable (QP) encoded MIME email attachment. You can specify an integer less than 65535, or specify 0 to disable decoding. Specify -1 to place no limit on the number of bytes to decode.

You can enable rule 141:5 to generate events for this parameter, and in an inline deployment, drop offending packets when decoding fails (due to incorrect encoding or corrupted data).

Type: integer

Valid range: `-1` to `65535`

Default value: `-1`

uu_decode_depth

Specifies the maximum number of bytes to extract and decode from each Unix-to-Unix encoded (uuencoded) MIME email attachment. You can specify an integer less than 65535, or specify 0 to disable decoding. Specify -1 to place no limit on the number of bytes to decode.

You can enable rule 141:7 to generate events for this parameter, and in an inline deployment, drop offending packets when decoding fails (due to incorrect encoding or corrupted data).

Type: integer

Valid range: `-1` to `65535`

Default value: `-1`

IMAP Inspector Rules

Enable the `imap` inspector rules to generate events and, in an inline deployment, drop offending packets.

Table 1: IMAP Inspector Rules

GID:SID	Rule Message
141:1	unknown IMAP3 command
141:2	unknown IMAP3 response
141:4	base64 decoding failed
141:5	quoted-printable decoding failed
141:7	Unix-to-Unix decoding failed
141:8	file decompression failed

IMAP Inspector Intrusion Rule Options

vba_data

Sets the detection cursor to the Microsoft Office Visual Basic for Applications macros buffer.

Syntax: `vba_data;`

Examples: `vba_data;`