POP Inspector

POP Inspector Overview

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

Post Office Protocol version 3 (POP3) enables email clients to retrieve messages from a remote POP3 server. A POP3 server uses TCP port 110 for insecure sessions or TCP port 995 for POP over SSL/TLS.

The `pop` inspector detects POP traffic and analyzes POP commands and responses.

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

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

POP Inspector Parameters

Note Decoding, or extraction when the MIME email attachment does not require decoding, can include multiple attachments and large attachments that span multiple packets.

The highest value is used when the values for the `b_64_decode_depth`, `bitenc_decode_depth`, `qp_decode_depth`, or `uu_decode_depth` parameters are different in:

- the default network analysis policy
- any other custom network analysis policy invoked by network analysis rules in the same access control policy

POP service configuration

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

Example:

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

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 142:4 to generate events for this parameter, and in an inline deployment, drop offending packets when decoding fails.

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 142:8 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 142:8 to generate events for this parameter, and in an inline deployment, drop offending packets.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

decompress_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 142:8 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 142:5 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 142:7 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`

POP Inspector Rules

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

Table 1: POP Inspector Rules

GID:SID	Rule Message
142:1	unknown POP3 command
142:2	unknown POP3 response
142:4	base64 decoding failed
142:5	quoted-printable decoding failed
142:7	Unix-to-Unix decoding failed
142:8	file decompression failed

POP 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;`