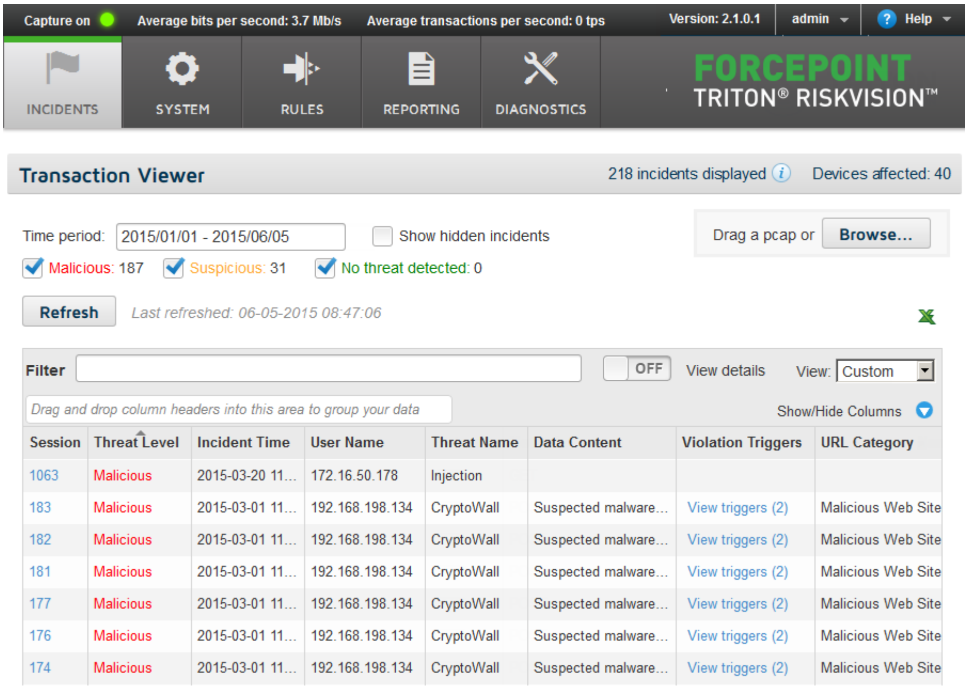
Working with RiskVision Incidents

Incidents | TRITON RiskVision | v2.1 | 02-Jun-2016

When an HTTP or SMTP transaction analyzed by TRITON RiskVision is found to contain malicious, suspicious, data loss, or data theft activity, an **incident** is recorded. The incident record includes information about the transaction, and about why analysis flagged it as an incident.

Use the **Incidents** page in the RiskVision Local Manager to review and investigate incidents in the Transaction Viewer.



Transaction Viewer

218 incidents displayed Devices affected: 40

Time period: 2015/01/01 - 2015/06/05 □ Show hidden incidents

Drag a pcap or Browse...

☑ Malicious: 187 ☑ Suspicious: 31 ☑ No threat detected: 0

Refresh Last refreshed: 06-05-2015 08:47:06

Filter OFF View details View: Custom

Drag and drop column headers into this area to group your data

Show/Hide Columns

Session	Threat Level	Incident Time	User Name	Threat Name	Data Content	Violation Triggers	URL Category
1063	Malicious	2015-03-20 11...	172.16.50.178	Injection			
183	Malicious	2015-03-01 11...	192.168.198.134	CryptoWall	Suspected malware...	View triggers (2)	Malicious Web Site
182	Malicious	2015-03-01 11...	192.168.198.134	CryptoWall	Suspected malware...	View triggers (2)	Malicious Web Site
181	Malicious	2015-03-01 11...	192.168.198.134	CryptoWall	Suspected malware...	View triggers (2)	Malicious Web Site
177	Malicious	2015-03-01 11...	192.168.198.134	CryptoWall	Suspected malware...	View triggers (2)	Malicious Web Site
176	Malicious	2015-03-01 11...	192.168.198.134	CryptoWall	Suspected malware...	View triggers (2)	Malicious Web Site
174	Malicious	2015-03-01 11...	192.168.198.134	CryptoWall	Suspected malware...	View triggers (2)	Malicious Web Site

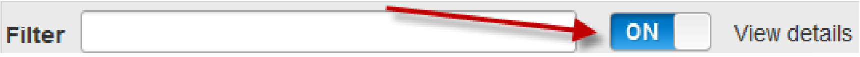
By default, the Transaction Viewer shows:

- All incident records in the database
- All threat levels
- Monitored traffic and incidents from manually submitted pcap files
- Columns most useful to investigating HTTP-based incidents

For information about all of the ways you can customize the Transaction Viewer, see *Customizing the Transaction Viewer*, page 4.

Incident details

More information may be available about individual incidents than can be displayed in the Transaction Viewer table. To see all available details about an incident, switch the **View details** toggle to **ON**, then select a row in the table.



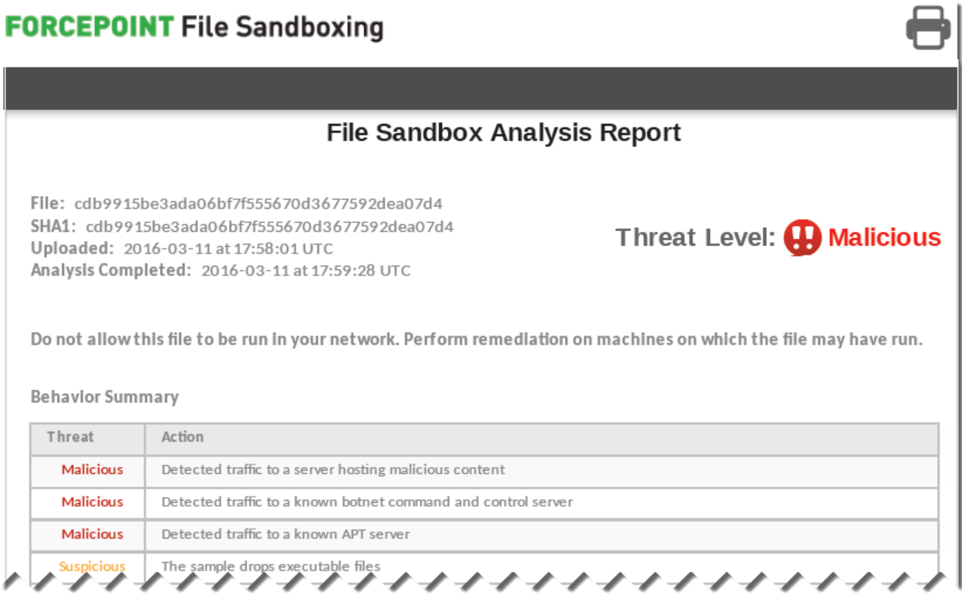
This opens an additional panel at the bottom of the table. See *Understanding RiskVision incident details*, page 12, for more information about the details that may be shown.

Advanced file analysis

If a file is sent for external file analysis, the results of the analysis may include a link to a report. When this occurs, the value in the Threat Level field (Malicious, Suspicious, or No Threat Detected) is underlined, and becomes a link to the report. Click the Threat Level value to open the report in a new browser window.

For Threat Protection Appliance reports, you are prompted to log in to the Controller, then taken to the report page.

File Sandboxing report sample



FORCEPOINT File Sandboxing

File Sandbox Analysis Report

File: cdb9915be3ada06bf7f555670d3677592dea07d4
SHA1: cdb9915be3ada06bf7f555670d3677592dea07d4
Uploaded: 2016-03-11 at 17:58:01 UTC
Analysis Completed: 2016-03-11 at 17:59:28 UTC

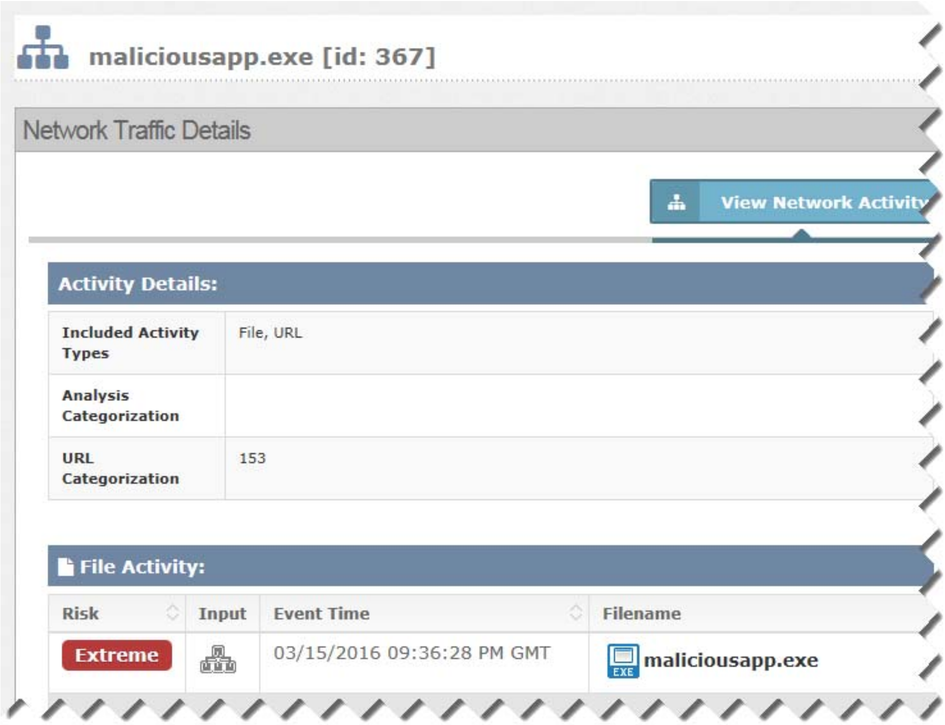
Threat Level: Malicious

Do not allow this file to be run in your network. Perform remediation on machines on which the file may have run.

Behavior Summary

Threat	Action
Malicious	Detected traffic to a server hosting malicious content
Malicious	Detected traffic to a known botnet command and control server
Malicious	Detected traffic to a known APT server
Suspicious	The sample drops executable files

Threat Protection Appliance report sample



maliciousapp.exe [id: 367]

Network Traffic Details

Activity Details:

Included Activity Types	File, URL
Analysis Categorization	
URL Categorization	153

File Activity:

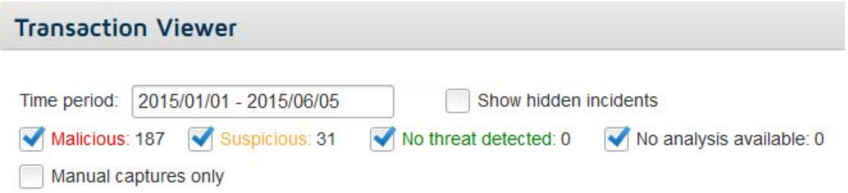
Risk	Input	Event Time	Filename
Extreme		03/15/2016 09:36:28 PM GMT	maliciousapp.exe

Customizing the Transaction Viewer

Incidents | TRITON RiskVision | v2.1 | 02-Jun-2016

You can customize the Transaction Viewer to highlight the details you find most valuable for investigating and remediating security events.

- Use the check boxes near the top of the page to limit the records shown.



Transaction Viewer

Time period: 2015/01/01 - 2015/06/05 □ Show hidden incidents

☑ Malicious: 187 ☑ Suspicious: 31 ☑ No threat detected: 0 ☑ No analysis available: 0

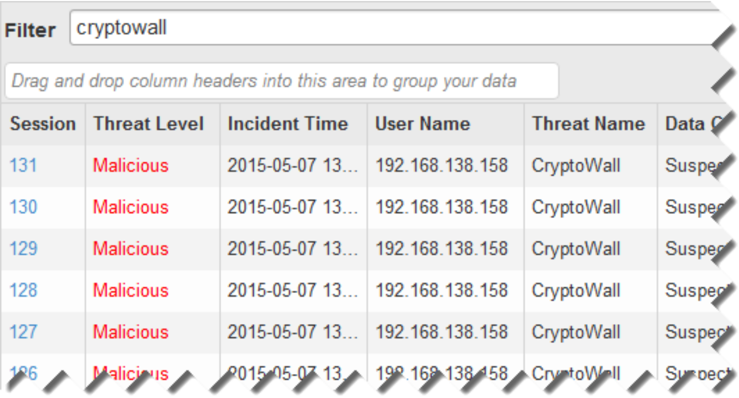
□ Manual captures only

  - Specify the **Time period** to display. The default value reflects the time span between the oldest incident in the database (by incident time) and the current day.

    When you click the field to change the time period, a calendar tool is displayed. Mark the **Specify start and end time** check box below the calendar tool to further narrow the period displayed.

  - Select one or more threat levels to display (malicious, suspicious, no threat detected, and no analysis available).
  - Indicate whether you want to show **Manual captures only**.
  - Specify whether or not to **Show hidden incidents**. Incidents created based on cloud app data that have no other threat or data loss characteristics are hidden by default.

- Enter a string (like a threat name, user name, or IP address) in the **Filter** field to show only incidents that contain that string.



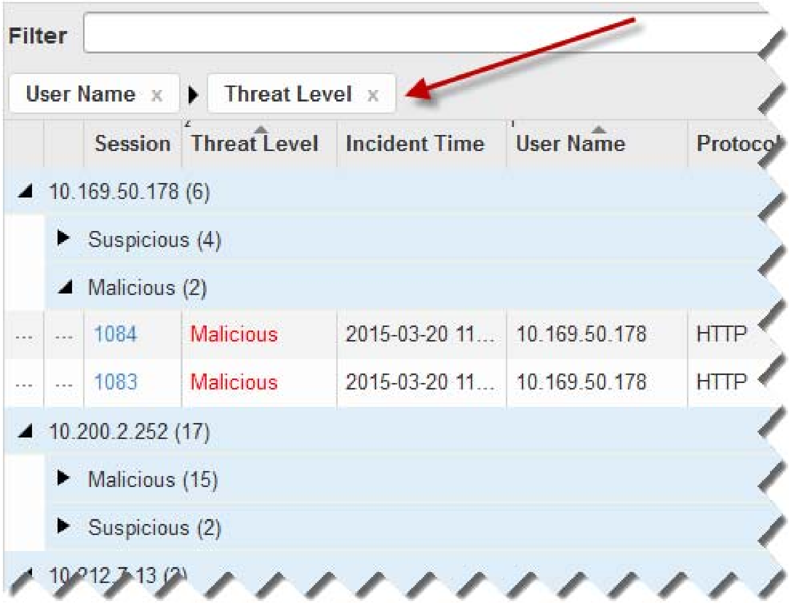
Filter: cryptowall

Drag and drop column headers into this area to group your data

Session	Threat Level	Incident Time	User Name	Threat Name	Data C
131	Malicious	2015-05-07 13...	192.168.138.158	CryptoWall	Suspe
130	Malicious	2015-05-07 13...	192.168.138.158	CryptoWall	Suspe
129	Malicious	2015-05-07 13...	192.168.138.158	CryptoWall	Suspe
128	Malicious	2015-05-07 13...	192.168.138.158	CryptoWall	Suspe
127	Malicious	2015-05-07 13...	192.168.138.158	CryptoWall	Suspe
126	Malicious	2015-05-07 13...	192.168.138.158	CryptoWall	Suspect

- Group the data in the table by one or more fields (for example, source IP and threat name, and shown below). To do this, click on a column header (like **User Name**) and drag it straight up into the sorting row above the table. Repeat for each additional field that you'd like to use to group the data.

The result looks like this, with the “group by” fields appearing at the top of the table, and the data in the table grouped accordingly:



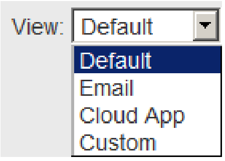
Filter

User Name x ▶ Threat Level x

		Session	Threat Level	Incident Time	User Name	Protoco
◢ 10.169.50.178 (6)						
	▶ Suspicious (4)					
	◢ Malicious (2)					
...	...	1084	Malicious	2015-03-20 11...	10.169.50.178	HTTP
...	...	1083	Malicious	2015-03-20 11...	10.169.50.178	HTTP
◢ 10.200.2.252 (17)						
	▶ Malicious (15)					
	▶ Suspicious (2)					
◢ 10.212.7.13 (2)						

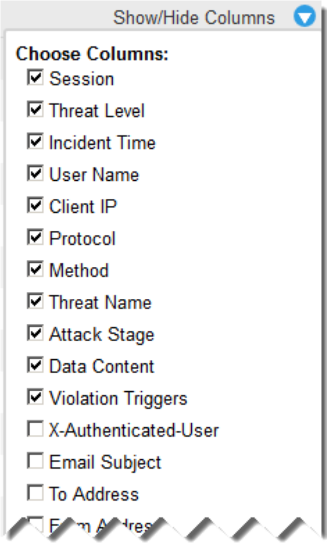
To stop using a particular field to group data, click the “x” next to the field name in the “group by” row.

- Change the columns shown in the table, or reorder the columns:
  - Reorder column headers by dragging them to a new position in the header row.
  - Use the **View** drop-down list to select a predefined set of columns to show in the table. The default view emphasizes threat and data loss information for HTTP transactions.



View: Default

- Use the **Show/Hide Columns** drop-down list to customize which columns appear in the table.



Show/Hide Columns

Choose Columns:

☑ Session
☑ Threat Level
☑ Incident Time
☑ User Name
☑ Client IP
☑ Protocol
☑ Method
☑ Threat Name
☑ Attack Stage
☑ Data Content
☑ Violation Triggers
☐ X-Authenticated-User
☐ Email Subject
☐ To Address
☐ From Address

See *RiskVision Transaction Viewer table columns*, page 6, for more information about the columns that can be displayed in the table.

RiskVision Transaction Viewer table columns

Incidents | TRITON RiskVision | v2.1 | 02-Jun-2016

Use the **Show/Hide Columns** drop-down list to configure the Transaction Viewer table to display any of the following columns.

Note that the columns are shown below in alphabetical order; the order in the Show/Hide Columns list depends on which entry is selected in the **View** list.

Column	Description
Analytic-Assigned Category	The URL category assigned to the incident by the analytic that returned the highest severity level Different analytics may return different URL category results for the same incident.
Attack Stage	Describes which stage of the advanced malware threat kill chain the analyzed file corresponds to See *RiskVision attack stage definitions*, page 10.

Column	Description
Client IP	IP address of the client machine ● If X-Forwarded-For information is sent by an upstream proxy, this is the IP address of the client machine. (In this configuration, the Source IP field shows the proxy IP address.) ● If X-Forwarded-For is not used in your deployment, the Client IP and Source IP fields contain the same IP address.
Cloud App	The name of a cloud app accessed as part of an incident (for example, LiveJournal or Facebook) For more information about investigating cloud app incidents, see Using RiskVision to Investigate Cloud App Use.
Cloud App Risk	The risk level (low, medium, or high) assigned by Cloud App Analysis to the cloud app associated with an incident Refer to the incident details for information about how risk level was determined for a specific cloud app.
Content Classifier	The type of string that Data Analysis matched to find a violation ● For data loss incidents, the Data Content field shows the policy type (such as PCI), and the Content Classifier shows the rule within the policy that was matched (such as Credit Card Numbers). ● For data theft incidents, the Data Content and Content Classifier values often match.
Data Content	The general type of content that Data Analysis found (for example, “PCI” or “Suspected malware communication”)
Destination IP	The IP address of the recipient of an HTTP request
Email Subject	Content of the Subject line of an email message
File Hash	An SHA-1 hash of the file name associated with an incident, used to determine whether a file has been previously analyzed
File Name	The name of the file that was analyzed
File Size	The size, in bytes, of the file analyzed
Forwarded For	The content of the X-Forwarded-For string (if available) in an HTTP header. Used to identify the true source of a proxied transaction. If an upstream proxy inserts X-Forwarded-For data, the Forwarded For and Client IP fields should match. The Source IP field will show the IP address of the proxy.
From Address	Identifies the sender of an email message
Full URL	The entire URL associated with an HTTP transaction
HTTP Return Code	HTTP status code returned in response to a request Examples include 200 (OK), 301 (Moved permanently), 401 (Unauthorized), 404 (Not found), and so on.

Column	Description
Incident Time	Date and time the incident occurred In the case of manually submitted pcap files, this is the timestamp recorded when the pcap was created; not the time that RiskVision analyzed the incident.
Method	HTTP method used in the transaction: GET, PUT, POST, CONNECT, and so on
Number of Categories	The total number of URL categories assigned to an incident during the process of analysis
PCAP Location	Full path to the pcap file associated with an incident in the appliance file system
Plugins	List of analytic plugins used to analyze the incident When file analysis is performed, this field also specifies whether File Sandboxing or Threat Protection was used.
Protocol	HTTP / SMTP
Reason	A string that includes a summary of: ● A numeric internal code for the analytic that identified the malicious software ● The threat name (corresponding to the Threat Name column in the table) ● The attack stage (corresponding to the Attack Stage column in the table). See *RiskVision attack stage definitions*, page 10. ● The channel used to spread the attack (Web or Email) ● An internal alphabetic code for the analytic that identified the malicious software
Session	Unique identifier for the TCP session in which the incident was detected
Severity	The severity estimation returned by Data Analysis based on the type of data and number of violations The possible severity values are high, medium, and low.
Source Host Name	The hostname of the source machine
Source IP	The IP address of the source of a request If there is an upstream proxy, Source IP shows the proxy IP address and Client IP shows the client IP address.
Status	The status of the transaction analysis (for example, pending, in progress, or completed)
Threat Level	Malicious / Suspicious / No Threat Detected A fourth threat level, “File Queued,” may be displayed when an incident is in the process of being analyzed. This indicates that one or more of the plugins contributing to the analysis has not yet returned a result. If the Threat Level is underlined, you can click it to open a file analysis report from File Sandboxing or Threat Protection.

Column	Description
Threat Name	The name of the malware, if known, or a description of the type of malicious activity
Threat Score	A numeric value that combines analytic results to assess the potential severity of an incident
To Address	Identifies the recipient or recipients to whom an email was sent
URL Category Names	The name of each category returned by the URL database and content analysis for the URL associated with the incident
User Agent	The user agent header associated with an HTTP transaction
User Name	The name of the user who initiated an HTTP request This requires integration with a product that provides X-Authenticated-For headers.
Violation Triggers	The strings that caused Data Analysis to return a policy violation When specific triggers are displayed, potentially sensitive information is partially obscured.
X-Authenticated-User	The user name identified by the X-Authenticated-User header field in HTTP transactions passed by an upstream proxy

If you want to see the data for more columns than your monitor comfortably supports, it may be helpful to click the **View details** switch (next to the Filter box) and use the Details pane to review incidents. See *Understanding RiskVision incident details*, page 12, for more information.

RiskVision attack stage definitions

Incidents | TRITON RiskVision | v2.1 | 02-Jun-2016

Most of the attack stages correspond to the Forcepoint Security Labs 7 stages of advanced threats. These are:

Recon: content explicitly used for reconnaissance with malicious intent (threat stage 1)

Lure: content that lures the user and starts the infection chain (threat stage 2)

If more detailed information is known about the incident at this stage, it is classified into one of the other reason codes in this section.

- **Phishing**: a page that attempts to use social engineering for Phishing purposes
- **Fraud**: a page that attempts to use social engineering to defraud the user
- **Black SEO**: a compromised web page that contains links that are used for black hat SEO. Black hat SEO encompasses various methodologies that attempt to raise websites in search engine rankings in violation of search engines' terms of service.
- **Unsolicited Content**: content that is not malicious that was delivered in an unsolicited way (coming through email spam or web spam)
- **Installer Page**: a web page that uses a social engineering trick to install malicious or unwanted software on the user's computer
- **Defacement**: a compromised web page that was defaced and doesn't serve malicious content
- **Hack Tool**: a web page that allows the user to download or use a a tool that can be used for malicious or illegal purposes

Redirection: a URL or host that represents a connection point between the lure and the exploit page or other payload (threat stage 3)

- **Exploit**: malicious content that serves obfuscated or non-obfuscated exploits (threat stage 4)
- **Exploit Kit**: malicious content that is part of an exploit kit (a toolkit that automates vulnerability exploitation) that serves obfuscated or non-obfuscated exploits (threat stage 4)

Dropper File: traffic associated with a malicious or unwanted file that is downloaded to the victim's machine after either a successful exploit attempt or a successful social engineering trick (threat stage 5)

- **Call Home:** traffic originating from malicious software to command and control servers, requesting instructions, updates, and new malware to expand the attack footprint (threat stage 6)
- **Backchannel Traffic**: traffic that originates from a file that is malicious or unwanted (threat stage 6)

Data Theft: content that contains stolen data (threat stage 7)

Some threats don't correspond to a single stage in the kill chain. For threat-related behaviors that go beyond a single stage, there are the following additional attack stage values:

- **Obfuscation**: obfuscated web content that fits different threat stages once the obfuscation is removed.
- **Evasion**: web pages that are used to evade a proxy (goes with the Proxy Avoidance category).
- **Detection Test**: test web pages designed to test that the detection capability of a product deployment (e.g., EICAR files or Forcepoint test portal, etc.)
- **Threat** is used as a generic reason code for malicious content that does not fit a more specific threat type, or has not yet been assigned another reason code.

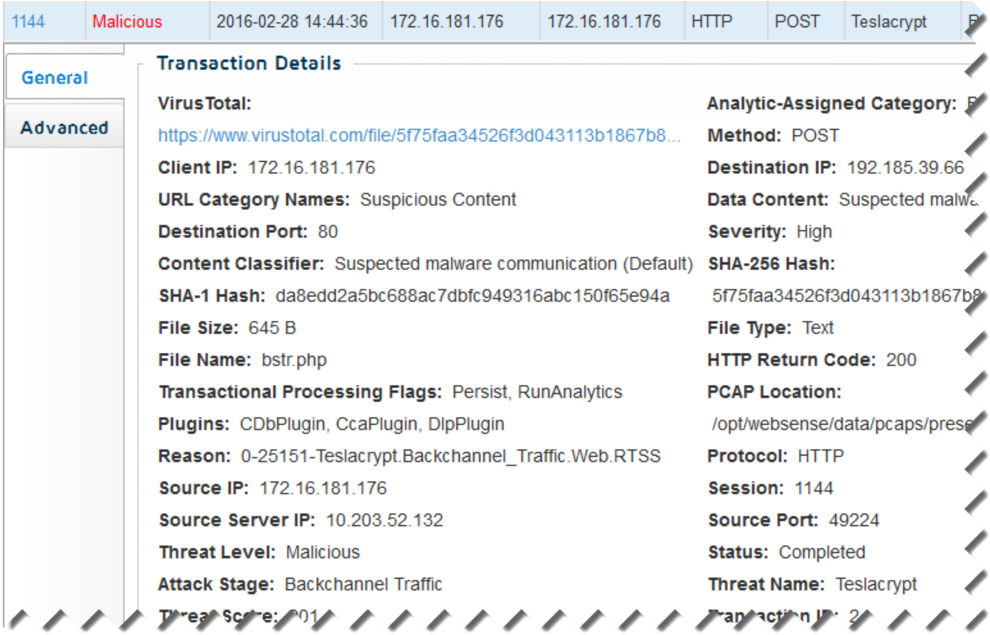
Finally, there are files and behaviors categorized as malicious because of their reputation. For these, the following attack stage values are used:

- **Suspicious Script**: a script with suspicious traits that could be malicious or unwanted.
- **Suspicious Iframe**: an iframe with suspicious traits that could be malicious or unwanted.
- **Risk**: a page with suspicious artifacts that may be malicious or unwanted. Used as a generic reason code for content deemed suspicious based on reputation.

Understanding RiskVision incident details

Incidents | TRITON RiskVision | v2.1 | 02-Jun-2016

To see more details about an incident, enable the **View Details** toggle on the Incidents page, then click on an incident to select it. A panel is added to the bottom of the table, showing any additional details that are available.



1144	Malicious	2016-02-28 14:44:36	172.16.181.176	172.16.181.176	HTTP	POST	Teslacrypt	B

Transaction Details

VirusTotal: https://www.virustotal.com/file/5f75faa34526f3d043113b1867b8...	**Analytic-Assigned Category:** B
	Method: POST
Client IP: 172.16.181.176	**Destination IP:** 192.185.39.66
URL Category Names: Suspicious Content	**Data Content:** Suspected malwa
Destination Port: 80	**Severity:** High
Content Classifier: Suspected malware communication (Default)	**SHA-256 Hash:**
SHA-1 Hash: da8edd2a5bc688ac7dbfc949316abc150f65e94a	5f75faa34526f3d043113b1867b8
File Size: 645 B	**File Type:** Text
File Name: bstr.php	**HTTP Return Code:** 200
Transactional Processing Flags: Persist, RunAnalytics	**PCAP Location:**
Plugins: CDbPlugin, CcaPlugin, DlpPlugin	/opt/websense/data/pcaps/pres
Reason: 0-25151-Teslacrypt.Backchannel_Traffic.Web.RTSS	**Protocol:** HTTP
Source IP: 172.16.181.176	**Session:** 1144
Source Server IP: 10.203.52.132	**Source Port:** 49224
Threat Level: Malicious	**Status:** Completed
Attack Stage: Backchannel Traffic	**Threat Name:** Teslacrypt
Threat Score: 201	**Transaction ID:** 2

For the selected incident, the detail panel shows:

1. Every viewable field in the database that has a value assigned to it. (Fields without a value are hidden.)

   In addition to the columns that can be displayed in the File Analysis table, the General tab of the Details pane may contain the following fields:

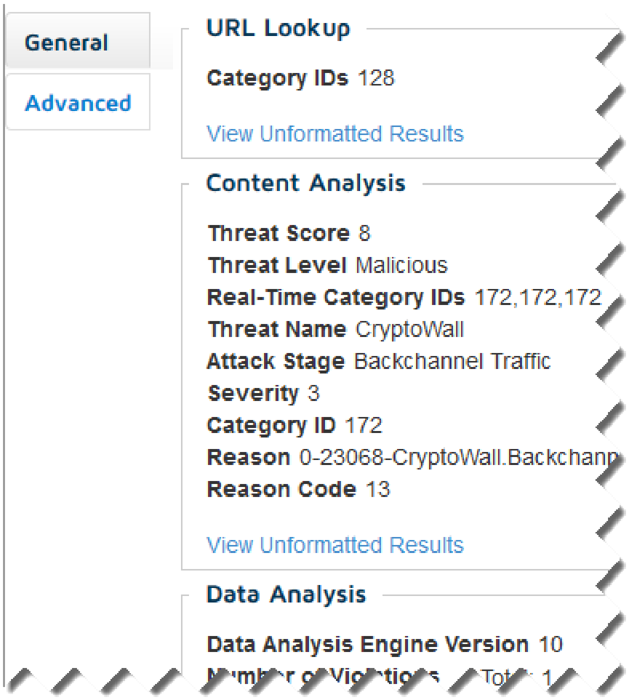
Field	Description
Destination Port	Port on which a request was received
File Type	A description of the type of file associated with the incident, which may correspond with a common file extension (like EXE or JPG)
SHA-1 Hash	The SHA-1 hash of the file associated with the incident (displayed in the table as “File Hash”) Used by the File Sandboxing cloud service
SHA-256 Hash	The SHA-256 hash of the file associated with the incident Used by VirusTotal
Source Port	Port on which a request was sent

Field	Description
Time Report Completed	The time the most recent incident assessment report finished generating
Transaction ID	An internal identifier provided by Transaction Processor
Transactional Processing Flags	Comma-separated list of labels appended to the incident record during analysis For example, if Local Analysis flags an incident for file analysis by File Sandboxing or Threat Protection, the OffBoxScanRequired label is listed in this field.
VirusTotal	A link to VirusTotal that includes the SHA-256 hash of the file associated with the incident Click the link to find out if a VirusTotal report exists for the file.

2. Information about the **Cloud App** (if any), including a summary of the factors contributing to the **App Risk** value shown.

   See Using RiskVision to Investigate Cloud App Use for more information about finding cloud app data and understanding cloud app risk factors.

3. **Advanced** information from each of the analytic tools used to assess the incident.



URL Lookup

Category IDs 128

Content Analysis

Threat Score 8
Threat Level Malicious
Real-Time Category IDs 172,172,172
Threat Name CryptoWall
Attack Stage Backchannel Traffic
Severity 3
Category ID 172
Reason 0-23068-CryptoWall.Backchann
Reason Code 13

Data Analysis

Data Analysis Engine Version 10
Number of Violations Total 1

   Click **View Unformatted Results** in any section of the Advanced tab to see the raw data returned by the selected analytic in a pop-up window.

Position the mouse over any truncated string in the detail panel to see the full string.