



**Hewlett Packard**  
Enterprise

# **HPE Security ArcSight DNS Malware Analytics**

Software Version: 2.4

User's Guide

February 8, 2017

## Alert types

Location: Dashboard > Dashboard page > Alert Types

Alerts are triggered when a certain amount of DNS events occur. The “Alert Types” list describes the type and amount of alerts that were generated as a result of client IPs attempting contact or contacted by malicious domains.

The following are the possible alert types:

Query Long Domains	Clients made numerous queries to domains with very long names, which may be attempting data extraction over DNS
Query NX DGA	Clients made numerous queries to a domain created by a Domain Generation Algorithm (DGA), but no connection was made (attempted fast flux)
Query Resp DGA	Clients made numerous DNS queries to a domain created by a DGA and at least one reply occurred (fast flux contact)
Query Many Blacklists	Clients attempted to connect to numerous blacklisted domains
Query FBIZeusSink	Clients queried domains associated with Zeus malware that has been flagged by the FBI
Query >50% Blacklists	More than 50% of the DNS queries made by clients were to blacklisted domains
Query 1st Blacklist	A possibly infected client made an attempt to connect to a blacklisted domain.

To view the individual alerts of an alert type, click the desired type (see ["Investigating alerts" on page 22](#)).

# Alert information

Location: Alerts > Alerts page

Other Location: Dashboard > Alert Types > alert type selection > Alerts page

The Alerts page displays the alerts that were triggered as the result of infected client IPs.

The "Alerts" table displays the type of alerts that occurred during the specified time range and exactly when they occurred. It also displays the client IPs that were infected. You can sort each piece of information in ascending or descending order by clicking on the arrows in the column headings. You can also drill down on an alert to view all the events that triggered an alert (see ["DNS event information" on page 26](#)).


If you arrive at the Alerts page from the Dashboard page, only the alerts for the selected alert type are listed in the "Alerts" table. If you go directly to the Alerts page, the "Alerts" table displays alerts for all the alert types for the specified time range.

The "Alert Counts" chart provides two scales that show the amount of alerts that were triggered for a specified time range. The first scale uses bars to represent the quantity of alerts while the other uses sparklines. With your mouse in the chart, you can use the mouse wheel to drill down in the chart.

The following information describes an alert from various perspectives. This information also functions as filter criteria for the "Alerts" table (see ["Filtering alerts" on page 24](#)).

Alert Types	Alerts are triggered when a certain amount of suspicious DNS events occur. The "Alert Types" list shows the type and number of alerts that were thrown during the specified time range. An alert type can have a sparkline that represents the DNS event count for that type.  See <a href="#">"Alert types" on page 19</a> .
Top IPs	This list ranks—by the number of alerts, the most infected client IPs for the specified time period.

IP Classes	<p>In this list, you can view the number of suspicious client IPs that belong to each IPv4 class—address range. Classes A through D are supported, with Class D being a multicast address range.</p> <p>A sparkline may be associated with a class, showing the alert count for that class.</p>
Top IP Subnets	<p>The first three IPv4 octets of the alert IP address identifies the network subnet.</p> <p>The “Top IP Subnets” list also shows the number of client IPs—by domain, that were infected. These are ranked from the highest to lowest octet: the third IPv4 octet (ex: 192.168.<b>45</b>.x), the second IPv4 octet (ex: 192.<b>168</b>.x.x), and lastly the first IPv4 octet (ex: <b>192</b>.x.x.x).</p>

To further investigate an alert and its related events, click  for the desired alert in the "Alerts" table (see ["Opening an alert" on page 26](#)).

## DNS event information

Location: Alerts > Alerts table selection > Alert Details page

From the Alerts > Alert Details page, you can learn about the infected client IP and see the DNS events that triggered an alert. DNS Malware Analytics collects all DNS events generated by suspicious client IPs, but lists no more than the first 5,000 of these. These events can be filtered for specific information.

Event information is presented in chart and table forms.

Events Surrounding the Alert	<p>This chart displays the DNS events (represented by sparklines) that occurred prior to the alert. If any DNS events occurred after the alert, these may also be displayed.</p> <p>The "Events Surrounding the Alert" chart uses color-coded sparklines to correspond to the malwares found in the "Malware Breakdown" list.</p> <p>See <a href="#">"Investigating DNS events surrounding the alert" below</a>.</p>
Events Triggering the Alert	<p>In this table, all the DNS events that are responsible for triggering the alert are listed in time order. The table also displays the suspicious domains, the IP address of the domain if it can be resolved, category of each DNS event, and malware used by the suspicious domain.</p> <p>See <a href="#">"Investigating DNS events surrounding the alert" below</a>.</p>

The "Suspicious Client" area provides the address of the infected client IP that produced the DNS events found in the "Events Surrounding the Alert" chart and "All Events Triggering Alert" table. This area also provides the alert type for the predominant threat, the hostname of the infected client, as well as the time of the alert.

You can click the client IP address to open the DNS Finder page and view the domains that the client IP queried (see ["Directly investigating a suspicious client IP" on page 32](#)).

The following information describes DNS events from various perspectives. This information also functions as filter criteria for the "Events Surrounding the Alert" chart and "Events Triggering the Alert" table (see ["Filtering DNS events" on page 29](#)).

Domain Type	This list displays the type and number of domains that the suspicious client IP queried. The possible domain types are blacklisted, graylisted, and DGA domain.
Categories of DNS Events	This list groups by category the DNS events that triggered the alert.
Malware Breakdown	<p>This list displays all the malware types that the infected client used to connect to its controlling domain. A malware can be a known type or it can be comprised of multiple types to create a unique hybrid.</p> <p>This list also provides the malware rate of occurrence. For example, there may be a total of 50 attempts of Conficker-AB, occurring at intervals of 10 for 5 hours trying to "phone home".</p> <p>When the different components of a malware try to use DNS to contact their master domain, this is reflected in the "Malware Breakdown" list using color codes for malware types that match corresponding DNS event in the "Events Surrounding the Alert" chart.</p>
Suspicious Domains	From this list, the domains most responsible for triggering DNS events are listed. For each domain, the total number of DNS events triggered and their rate per hour are provided.