Hewlett Packard
Enterprise

HPE Security ArcSight DNS Malware Analytics

Software Version: 2.4

User's Guide

February 8, 2017

Workflow summary

For an administrator, the workflow summary starts from the DNS Malware Analytics (DMA) Portal. Users (analysts) and devices (DNS Capture Modules) are managed from the portal. This includes adding analysts and setting activation, along with managing analyst information. From the portal, you can also change the name of your organization.

For DNS Capture Modules (DCMs), device management includes updating the content to the blacklist and whitelist and managing and monitoring DCM information.

The workflow summary is based on a Dashboard starting point. There could be alternative starting points in the workflow, such as the Alerts page or DNS Finder page.

The following high-level steps cover the functionality of DMA.

1. Launch HPE - ArcSight DNS Malware Analytics from the Chrome web browser.

   Use the URL that was sent to you in the "Welcome" email (see "Supported browser" on page 9).

Manage users and devices

2. To change the name of your organization, click **Edit** in the Users page (see "Changing your organization name" on page 12).
3. To access HPE - Security ArcSight Enterprise Security Manager (ESM) for alert analysis, click **Generate Alerts Access Token** in the Users page (see "Analyzing alerts in ESM" on page 12).

   This task also involves editing the FlexConnector configuration file with the alerts access token and then setting up a channel in ESM for the DMA alerts.
4. To add an analyst, click **Invite User** in the Users page and then specify the email address of the analyst (see "Adding an analyst" on page 13).

   - DMA issues an email to the new analyst for his or her acceptance.
   - The registration link in this email is active for only 24 hours from time of issue.
   - DMA automatically activates the new analyst.
5. To change analyst information, click ✎ for the desired analyst in the Users page (see "Changing analyst information" on page 14).

   From the Edit User dialog box, you can specify a new analyst email ID and name. You can also activate or deactivate an analyst.
6. To append the blacklist or whitelist with your own content, click the **Whitelist** or **Blacklist** in the Devices page (see "Appending the blacklist or whitelist" on page 15).
7. To assign a name to the DNS Capture Module, click ✎ in the Devices page for the desired DNS Capture Module (see "Naming the DNS Capture Module" on page 16).
8. To control DNS packet flow to the DNS Manager, click the desired control button of the Devices page (see "Monitoring DNS packet flow" on page 17).

   - DMA Portal enables you to stop DNS packet flow to the Device Manager, and restart it again. You can also “reboot” the DNS Capture Module and restart it from a total shutdown.
   - DMA monitors the DNS Capture Module, including the send and receive rates of DNS packets, total number of DNS packets sent and received, and time running for the module.
9. If you need to contact Technical Support, retrieve your database schema name from the Users page and keep it available (see "Database schema information" on page 12).

Specify a time period for analysis

- Specify the period you want to investigate (see "Setting the time range" on page 10.).
  - From the Alerts and DNS Finder pages, you can specify a time range by clicking the begin- and end-time fields.
  - From the Dashboard page, you can view application data for any single day by clicking the time field.

View your network security information

11. From the Dashboard page, view infections on your network.

    - From the "Top Domains Shared by Infected Clients" chart, note the most infecting (suspicious) domains and the client IPs that they may have infected (see "Understanding suspicious domains and querying client IPs" on page 19).

      To learn about all the domains that infected a client IP, click the desired client IP address to open the DNS Finder page (see "Directly investigating a suspicious client IP" on page 32).

      To learn about all the client IPs that a domain infected, click the desired suspicious domain to open the DNS Finder page (see "Directly investigating an infecting domain" on page 31).

    - To learn about a blacklisted domain and all the client IPs infected by this domain, access the "Most Queried Blacklisted Domains" list (see "Understanding the most queried blacklisted domains" on page 20).

      The first five domains are the same ones found in the “Most Infecting Domains and Impacted Client IPs” chart.

    - To learn about the blacklisted domain and all the client IPs infected by this domain, click the desired domain (see "Directly investigating an infecting domain" on page 31).

    - To learn about the type and amount of malware used by the suspicious domains, view the "Top Malware Types" chart (see "Top-offending malware types" on page 20).

    - To open the Alerts page and view individual alerts, click the desired alert type from the Alert Types list.

    - From the "Top Domains Shared by Infected Clients" chart, note the most infecting (suspicious) domains and the client IPs that they may have infected (see "Understanding suspicious domains and querying client IPs" on page 19).

      To learn about all the domains that infected a client IP, click the desired client IP address to open the DNS Finder page (see "Directly investigating a suspicious client IP" on page 32).

      To learn about all the client IPs that a domain infected, click the desired suspicious domain to open the DNS Finder page (see "Directly investigating an infecting domain" on page 31).

    - To learn about a blacklisted domain and all the client IPs infected by this domain, access the "Most Queried Blacklisted Domains" list (see "Understanding the most queried blacklisted domains" on page 20).

      The first five domains are the same ones found in the “Most Infecting Domains and Impacted Client IPs” chart.

    - To learn about the blacklisted domain and all the client IPs infected by this domain, click the desired domain (see "Directly investigating an infecting domain" on page 31).

    - To learn about the type and amount of malware used by the suspicious domains, view the "Top Malware Types" chart (see "Top-offending malware types" on page 20).

- To open the Alerts page and view individual alerts, click the desired alert type from the Alert Types list.

Investigate alerts

12. From the Alerts page, click the desired alert type or types from the "Alert Types" list to see individual alerts (see "Alert information" on page 22).

    - From this page, you can see all the alerts that were triggered as the result of infected client IPs. You can drill down on an alert to view all the events that triggered the alert (see "Investigating a particular alert" on page 26).
    - To investigate alert counts, access the sparkline scale to view the exact time an alert occurred and the bar-chart scale to narrow the range of alert counts (see "Investigating alert counts" on page 23).
    - To export alerts in CVS format, click **Export** (see "Exporting alerts" on page 25).
    - The data that DNS Malware Analytics exports is the time the alert occurred, the type of alert, and the client IP. This is the same data that is in the Alerts table of the Alerts page. DNS events are not exported.

13. To view specific alerts, use alert filter criteria to reduce the Alerts list (see "Filtering alerts" on page 24).

    You can filter alerts based on alert type, most infected client IPs, IP classes, and IP subnets.

Investigate a particular alert

14. To view events and related information for a particular alert, click the desired alert in the Alerts table (see "Investigating a particular alert" on page 26).

    - From the Alerts > Alert Details page, you can learn about the infected client IP and see the events that triggered an alert (see "DNS event information" on page 26).

      DMA collects all events generated by suspicious client IPs, but lists no more the first 5000 of these.
    - To investigate events surrounding the alert, hover over the desired sparkline to learn about the malware used and the exact time of the event, or click on the desired sparkline to learn additional details about the event (see "Investigating DNS events surrounding the alert" on page 27).
    - To view specific events, use the event filter criteria in the left panel to reduce the Alerts list (see "Filtering DNS events" on page 29).

Search for a DNS record

15. To directly investigate an suspicious domain, specify the domain in the **Search** field of the DNS Finder page (see "Directly investigating an infecting domain" on page 31).

- To filter an suspicious domain by a client IP, select the desired client IP bar or bars on the left under “Top Unique Host IP”.
- From the Dashboard, you can discover a suspicious domain (see "Understanding suspicious domains and querying client IPs" on page 19). But if you know the domain that you want to investigate, you can go directly to the DNS Finder page and specify that domain.

16. To directly Investigate an infected client IP, specify the client IP in the **Search** field of the DNS Finder page (see "Directly investigating a suspicious client IP" on page 32).

    - To filter a client IP by a domain, select the desired domain bar or bars on the left under “Top Unique Domains”.
    - From the Dashboard, you can discover infected client IPs (see "Understanding suspicious domains and querying client IPs" on page 19). But if you know the client IP that you want to investigate, you can go directly to the DNS Finder page and specify that client IP.

Monitoring DNS packet flow

About

DNS Malware Analytics (DMA) monitors the send and receive rates of DNS packets, total number of DNS packets sent and received, and time running for the DCM.

Procedure

Location: Devices > Devices page

1. Open the desired DNS Capture Module (DCM).
   - You can have multiple DCMs open at the same time.
   - The status of the DCM can either be running, updating, stopping, stopped or offline.
   - If offline, you cannot control DNS packet flow. See "Troubleshooting the Installation and Setup" in the *DNS Malware Analytics Getting Started Guide*. If you still cannot find your solution, contact Technical Support.
   - The time count is how long the DCM has been running. This number is reset to zero if you force a reconnect or the DCM shuts down.
2. To learn about the DCM, hover over the DCM and then click the more button (▪▪▪).

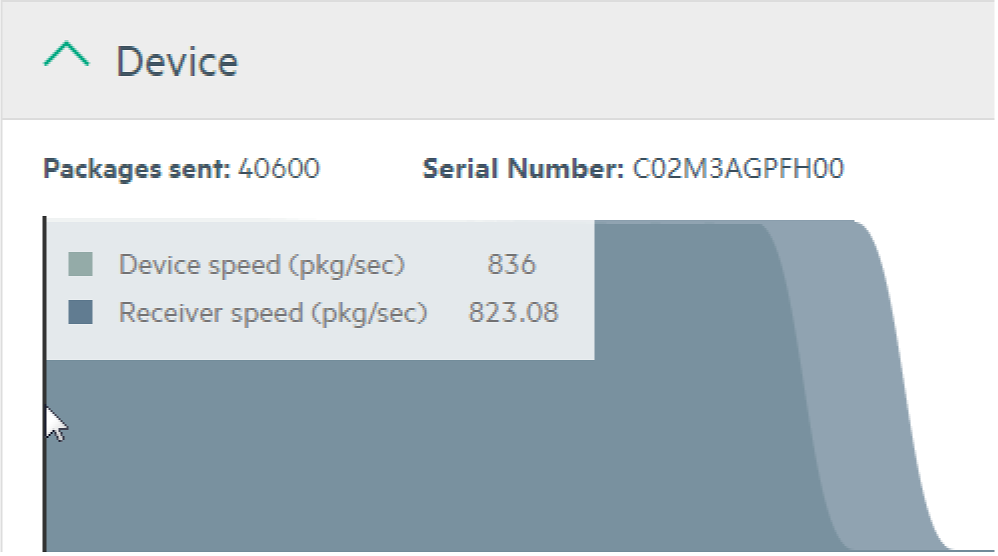
   See "Naming the DNS Capture Module" on the previous page.
3. To control DNS packet flow, click the desired button.

   Note: Only when the DCM is online and connected with the Device Manager are the control buttons functional.

   ⏸ — Pauses DNS packet flow from the DCM, while retaining the communication channel between the DCM and the Analytic Cloud.

   ▷ — Resumes DNS packet flow to the Device Manager.

   ↻ — If the DCM is online and connected, this action will force the DCM to reconnect or "reboot". Also use to restart the DCM from a total shutdown.
4. To learn a rate per second at which the receiver (Analytical Engine) and device (DCM) are processing packets, hover over a desired time segment.



Packages sent: 40600 **Serial Number:** C02M3AGPFH00

🟩	Device speed (pkg/sec)	836
■	Receiver speed (pkg/sec)	823.08

Packages sent — DNS packets collected by the DCM and then stored in the DNS Analytical Cloud. This number is relative to the cycle (time). It does not reflect the total of all cycles. If the DCM is disconnected, either by network problems or because you forced it to disconnect, this number will reset.

Device speed — The speed at which the DCM sends suspicious DNS records to the Analytical Engine.

Receiver speed — The speed at which the Analytical Engine processes DNS records and then writes them to the database.

The graph is updated every second.

Caution: In the rare event that DMA (DCM or Cloud or both) is down, you will not see activity in the graph for at least 60 seconds. HPE engineers monitoring the HPE - ArcSight DNS Malware Analytics Management Center in the cloud will correct this situation in a timely manner.

Filtering alerts

About

You can filter alerts based on alert type, most infected client IPs, IP classes, and IP subnets (see "Alert information" on page 22). Filtering results in more specific information in the "Alerts" table and in the "Alert Counts" chart.

Procedure

Location: Alerts > Alerts page

1. Select the desired filter criteria from the left panel (see "Alert information" on page 22).

    - This selection can be a single criterion or multiple criteria from a single or multiple filter groups.
    - Your filter selection can impact the values of other filter criteria. Whatever filter criteria you select first, determines the available criteria to further narrow your filtering. Subsequent filter selections further reduces the filter criteria values, and can even reduce some to zero.

Example

If you select the single alert type, “Query NX DGA”, the "Top IPs" list will only contain client IPs for which that alert was triggered. The "IP Classes" list will be adjusted to show the number of times a “Query NX DGA” alert occurred in the listed classes. Likewise, the "Top IP Subnets" list will now reflect the number of times a “Query NX DGA” alert occurred in the various subnets.

> **Note:** From the "Alert Counts" chart, you can click the red triangle of the desired sparkline to filter the "Alerts" table to only include the alert or alerts from the selected sparkline (see "Investigating alert counts" on page 23).

2. To filter the contents of the "Alerts" table, specify your criteria in the **Search** field.
3. To clear the filter criteria, click **Reset** for the "Alerts" table.

   If you narrowed the range of alerts in the "Alert Counts" chart, the range selector will be cleared and the chart will include all the sparklines (see "Investigating alert counts" on page 23).

   If you filtered the "Alerts" table based on a sparkline in the "Alert Counts" chart, the table will again include data for the full time range (see "Investigating alert counts" on page 23).

Investigating DNS events surrounding the alert

About

DNS event information is presented in the "Events Surrounding the Alert" chart and the "Events Triggering the Alert" table.

The "Events Surrounding the Alert" chart shows 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.

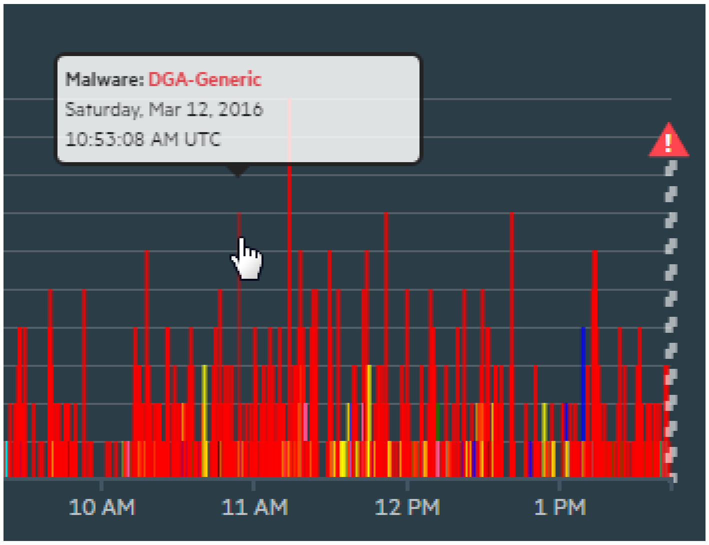
Because a DNS event reflects a type of malware, the "Events Surrounding the Alert" chart uses color-coded sparklines to correspond to the malwares listed in the "Malware Breakdown" list.

In the "Events Triggering the Alert" 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 event, and malware type used by the suspicious domain.

Procedure

Location: Alerts > Alerts table selection > Alert Details page > Events Surrounding the Alert

1. To view the malware or malwares that triggered the event and the exact time an event occurred, hover over the desired sparkline.

   - The height of an event sparkline indicates (for a particular time segment) the frequency in which malware of an infected client IP was attempting to ‘phone home’ to a C&C server at a suspicious domain. The sparkline height can also indicate the frequency in which a C&C server was replying to a malware query.
   - In the above example, the malwares (Conficker-AB, SimdaC, and Virut) associated with the event (pink sparkline) occurred a combination of nine times within 12:50 and 12:55.
   - The alert is represented by an exclamation mark (!) within a red triangle.

2. To view specific DNS event details, click the sparkline for the desired event.

   The "Events Triggering the Alert" table reduces to the DNS event or events of the selected sparkline.

3. To drill down in the chart, position your mouse in the chart and scroll with the mouse wheel.

Location: Alerts > Alerts table selection > Alert Details page > Events Triggering the Alert

The "Events Triggering the Alert" table provides the time a DNS event was generated for the client IP, the URL of a suspicious domain, the IP address of a domain if it can be resolved, the suspicious domain category, and the malware used to infect the client IP.

> **Note:** If the alert type is Query Resp DGA or Query FBIZeusSink, the associated domain will be resolved. If the alert type is Query NX DGA or Query Many Blacklist, the associated domain will not be resolved. For a NX DGA domain, this is indicated by "NXDOMAIN" appearing in the "Resolution" column. For a Query Many Blacklist domain, this is indicated by "N/A" appearing in the "Resolution" column.

The following are the supported suspicious domain categories:

A	Domain that returns a 32-bit IPv4 address.
AAAA	Domain that returns a 128-bit IPv6 address.
Q	Query
CNAME	Domain with a canonical name using an alias name.
SOA	Domain that specifies authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone.
MX	Mail exchange domain whose name maps to a list of message transfer agents for that domain.
NXDOMAIN	For alert type, Query NX DGA, both the "Resolution" and "Category" columns display "NXDOMAIN".

4. To investigate the domain and infected client IP or IPs behind an event, click the desired domain link.

   The DNS Finder page opens (see "Directly investigating an infecting domain" on page 31).