Custom records walkthrough: monitoring activity on suspicious ports

Published: 2016-12-21

The ExtraHop platform can help you gain visibility and real-time access to early attack indicators on your network. One proactive security measure you can take is to monitor ports that you consider vulnerable to trojans and other malware.

For example, because 12345 is an easy-to-remember sequence, this number is often selected when configuring a default port number for a server or a program, making that port value a popular target with attackers.

In this walkthrough, you will write a trigger that commits each transaction over a suspicious port value to a record on an ExtraHop Explore appliance, and then you will create a query to view the collected records.

Prerequisites

- You must have access to an ExtraHop Discover appliance with a user account that has full system privileges.
- Your ExtraHop Discover appliance must be connected to an ExtraHop Explore appliance as described in the Configure an Explore cluster section of the ExtraHop Admin UI Guide.
- Your network must be configured to allow traffic through port 12345.
- Familiarize yourself with the concepts in this walkthrough by reading the Get started with records and Get started with triggers sections in the ExtraHop Web UI Guide.
- Familiarize yourself with the processes of creating triggers by completing the Trigger Walkthrough.

Write the trigger

In the following steps, you will write a trigger that looks for server traffic over port 12345 and then commits a custom record of each transaction to the ExtraHop Explore appliance.

1. Log into a Discover appliance that is connected to an Explore appliance.
2. Click the System Settings icon, and then click **Triggers**.
3. Click **New** to open the Trigger Configuration window.
4. In the Name field, type `Suspicious Port Activity`.
5. In the Events field, select **FLOW_CLASSIFY**.
6. Click the **Editor** tab.
7. Add the following trigger code to the editor:

```
if (Flow.server && Flow.server.port === 12345) {
    commitRecord('Trojan', {
        description: 'Possible NetBus or other trojan',
        protocol:Flow.l7proto
    });
}
```

   To capture all transactions over the port, the trigger invokes the Flow class. The trigger specifies “Trojan” as the record type and adds two properties to the record contents: a description and the protocol of the transaction, if known.
8. Click **Save Changes**.
9. Click the **Assignments** tab, and then click **Assign to All**.

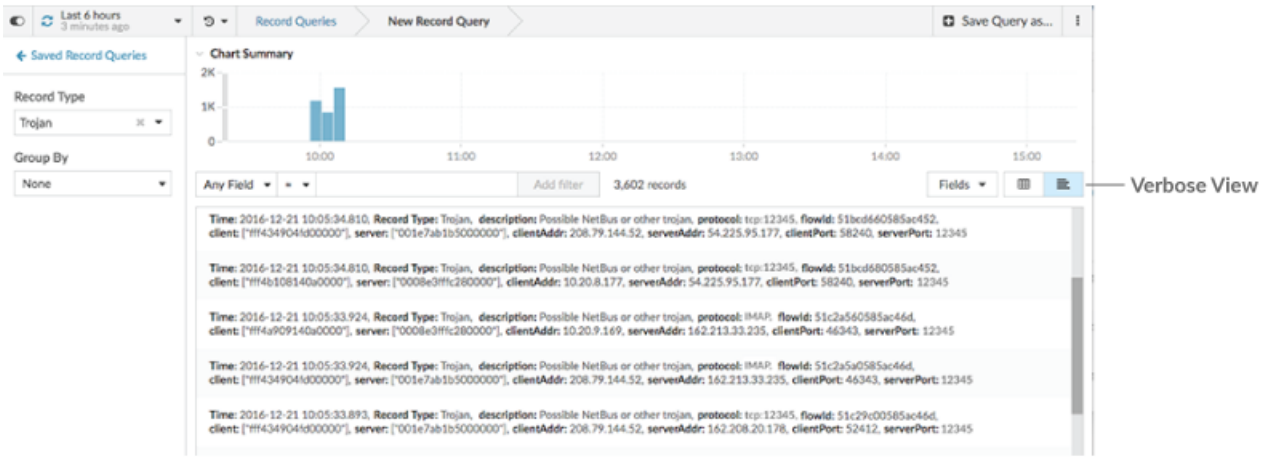
Important: When creating your own triggers, assign triggers only to the specific devices that you need to collect metrics from to minimize the performance impact of your triggers on the ExtraHop system.

10. Click **Save and Close**, and then let the trigger run for at least ten minutes.

Query and view the custom records

In the following steps, you will search for the custom records committed to the Explore appliance and create a saved record query based on the search criteria.

1. From the top-level navigation, click **Records**.
   The query results for all records appear in the content pane
2. From the Record Type drop-down menu, select **Trojan** and then click out of the field.
3. From the Fields drop-down menu, select **Select All**.
4. Click the **Verbose View** icon.
   The content pane displays custom records similar to the following figure:



In addition to the description and protocol specified in the record contents by the trigger, the record includes the following properties that are available from the flow:

- flowID
- client
- clientAddr
- clientPort
- server
- serverAddr
- serverPort

5. Click **Save Query as**.
6. In the Name field, type `Possible Trojans`, and click **Save**.

Check records for malware indicators

If your system is hit by a malware attack or you learn about new malware that is circulating, you can check your records to see if your system has been targeted.

For example, if you learn that a new trojan is often sent through port 12345, you can open the saved Possible Trojans query you created above and check for the following activity:

- Transactions occurring over unexpected protocols. For example, you might expect to see IMAP traffic over port 12345, but not SSH traffic.
- Transactions occurring over unclassified protocols, which are displayed in the query results as tcp:12345. Unclassified protocols are not recognized by the ExtraHop system and might be suspicious.
- Client IP addresses associated with transactions over unexpected or unclassified protocols, and if the IP address originated from an untrusted locale.
- Time stamps of the transactions that you find questionable and that occurred during non-business hours.

Narrowing down suspicious transactions helps you determine if you have a malware problem so that you can get started on a resolution.