ExtraHop exclude_from_doc_site Bundle walkthrough: Detecting ransomware threats in your environment

Published: 2018-10-27

Ransomware is a type of computer virus, which can be downloaded through various means, such as a malicious email or web page. Ransomware encrypts files on a client machine before spreading to file shares that the client is connected to, attempting to encrypt as many files as possible. Ransomware then informs you that the attackers will unencrypt your files only if you pay them a ransom in the form of Bitcoin, an internet currency that is extremely difficult to track.

ExtraHop can help you detect and quarantine ransomware in the early stages to limit the amount of damage done.

In this walkthrough, you will learn how to download, install, and configure the Ransomware Bundle, which is built to identify ransomware attacks in progress. This walkthrough also explains how to configure and interpret the alerts, dashboards, and metrics included in the bundle so you can protect against ransomware threats.

Note: The Ransomware Bundle analyzes only CIFS traffic. The bundle does not currently monitor NFS or iSCSI activity. For help configuring ExtraHop to monitor NFS and iSCSI for ransomware attacks, contact your ExtraHop account representative.

Prerequisites

- Familiarize yourself with the concepts in this walkthrough by reading the Bundles section of the ExtraHop Web UI Guide.
- You must have access to an ExtraHop Discover appliance with a user account that has full write permissions.
- You must be familiar with modifying triggers. For more information, see the Triggers section of the ExtraHop Web UI Guide.

Download the ExtraHop Ransomware Bundle

Before you can upload the Ransomware Bundle to your appliance, you must download the bundle from the ExtraHop website.

1. Go to the ExtraHop Solution Bundles Gallery.
2. In the Search bar, type `Ransomware`.
3. In the table, click **Ransomware Bundle**.
4. If you have not already logged into the ExtraHop website, click **Login** in the right pane and then specify a valid username and password.
5. Click **Download Now**.
6. Save the `.json` file to a location on your local machine.

Upload and apply the Ransomware Bundle to your ExtraHop appliance

After you have downloaded the Ransomware Bundle, you can upload and install the bundle on your appliance.

Note: If you have already installed an earlier version of the Ransomware Bundle, complete the Upgrading the Ransomware Bundle procedure instead and then continue with the next section of this walkthrough.

1. Log into the Web UI of a Discover appliance.
2. Click the System Settings icon in the upper right corner.
3. Click **Bundles**.
4. On the Bundles page, click **Upload**.
5. In the Load Bundle dialog box, click the Choose File button, and then select the Ransomware Bundle file you downloaded from the ExtraHop Solution Bundle Gallery.
6. Click **Upload**.
7. Select the **Apply 7 included assignments checkbox**.

   Note: Selecting this option assigns the Ransomware Bundle to the CIFS Servers Activity Group. The Ransomware Bundle is designed to be assigned only to CIFS Servers, so we recommend that you do not modify this configuration.
8. From the Existing objects drop-down menu, select **Overwrite**.

   Selecting this option will overwrite any objects that have the same name as objects in the bundle.
9. Click **Apply**.
10. In the Bundle Import Status dialog box, click **OK**.
11. In the View Bundle window, click **OK**.

Exclude machines from ransomware monitoring

Most environments have some machines that can be trusted to be free of malicious activity. Excluding these machines from ransomware scanning can improve the performance of the ransomware trigger in the bundle, especially if the machines participate in a lot of CIFS activity. Excluding machines can also help minimize false positives generated by the bundle.

The ransomware trigger has three IP address whitelists that control which machines are excluded from ransomware monitoring. You must configure these lists before you enable the trigger.

Important: The lists are set to a random set of IP addresses by default, so it is important to configure these lists before you enable the trigger; otherwise, the ransomware trigger might miss malicious traffic from those default IP addresses.

IP Whitelists

client_ip_whitelist

Excludes any traffic to or from the specified IP addresses.

client_subnet_whitelist

Excludes any traffic to or from IP addresses in the specified subnets.

conversation_whitelist

Excludes traffic between the specified IP address pairs. For example, `["1.1.1.1", "1.1.1.2"]` exludes traffic from `1.1.1.1` to `1.1.1.2`, but not traffic from `1.1.1.1` to `1.1.1.3`.

As an example, the following steps show you how to modify the `client_ip_whitelist`.

1. Click the System Settings icon.
2. Click **Triggers**.
3. In the table, click **Ransomware CIFS Detection <version>**.
4. Click the **Editor** tab.
5. Scroll down to `var client_ip_whitelist`.

6. Delete the following text:

   ```
   "1.1.1.0", "2.2.2.0"
   ```

7. Replace the text you deleted with an IP address that you do not want to monitor. Enclose the IP address with quotation marks and separate multiple IP addresses with a comma, for example:

   ```
   “172.21.1.245”, “172.21.1.1”
   ```

Configure ransomware alerts

The Ransomware Bundle includes alerts that you can configure to email you when potential ransomware attacks are detected. We recommend that you configure ransomware alerts when you first apply the bundle so you can be alerted when suspicious activity occurs.

1. Click the System Settings icon.
2. Click **Alerts**.
3. Enable each alert and configure the alert to send notifications to your email address.

   Repeat these steps for each of the four ransomware alerts.

   a) Click **Ransomware Type <integer> Detection Event**.
   b) Deselect the **Disable Alert** checkbox.
   c) Click **Notifications**.
   d) In the Additional email addresses field, type your email address.
   e) Click **OK**.

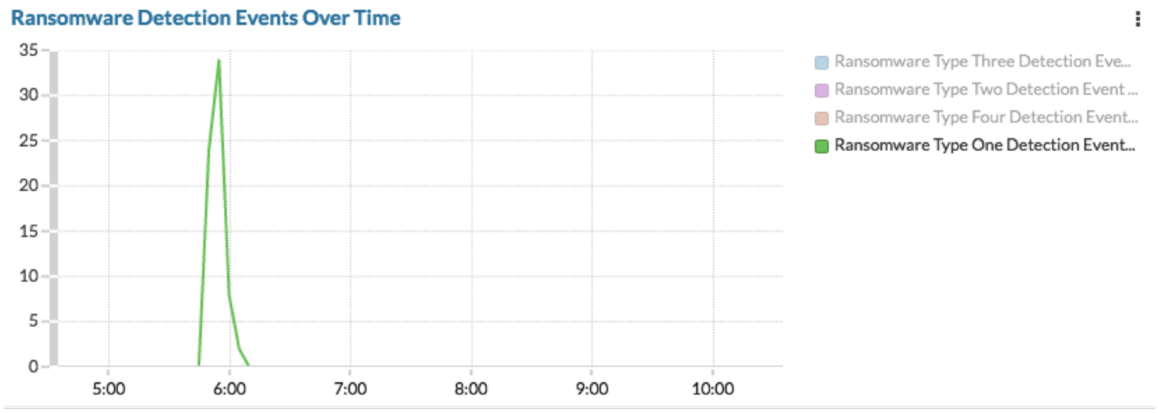
Identify ransomware

This example shows how you can detect ransomware by discovering a malicious file type in your environment.

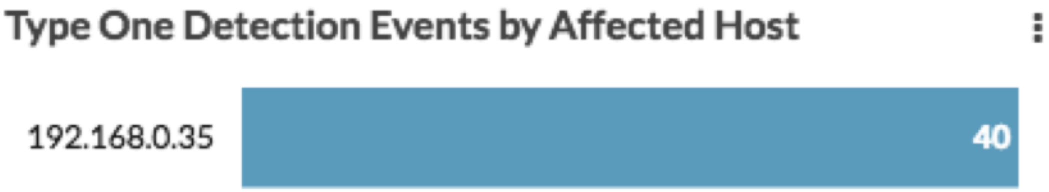
Note: The Ransomware Bundle can detect ransomware in a variety of ways. For information about other ways you can identify ransomware attacks, see the Appendix.

When ransomware is detected, your Discover appliance sends an email to the addresses configured in the ransomware alerts. For example, you might receive an email titled “ExtraHop Alert for Ransomware Type One Detection Event”, which means you should check the Ransomware Detection dashboard on your Discover appliance to investigate further.

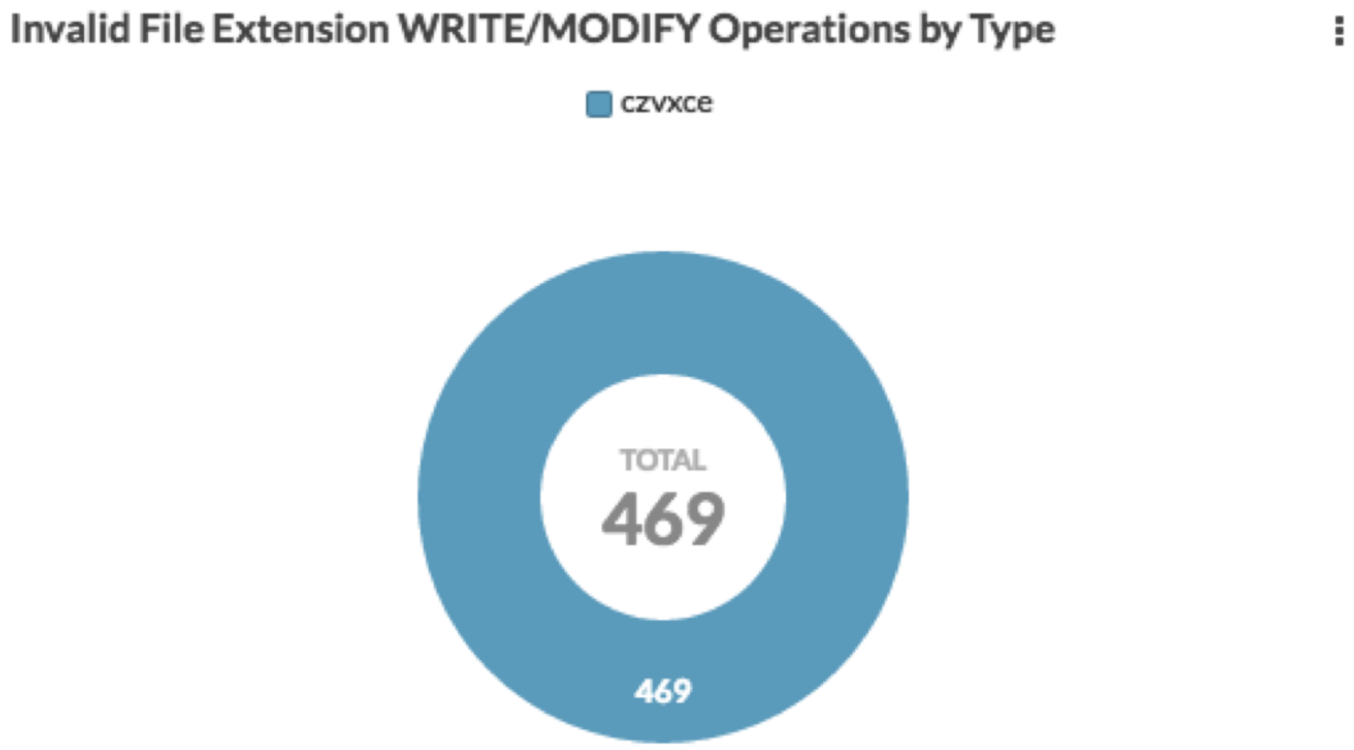
The Ransomware Detection dashboard shows you when and where the suspicious activity was detected. The figure below shows that there were a large number of type one detection events at approximately 5:45. Type one events indicate that a file type known to be used in ransomware attacks was found in your environment.



The Detection Events by Affected Host charts show you which machines are involved in the suspicious activity. The figure below shows that numerous type one detection events occurred on a device with an IP address of 192.168.0.35.



Next, on the Ransomware Supplemental dashboard, the Invalid File Extension WRITE/MODIFY Operations by Type chart shows you which suspicious file types were detected. The following figure shows that 469 write or modify operations occurred for files with the extension .czvxce.



Search engines can offer more information about the suspicious file type. For example, a Google search for “czvxce” will reveal that Coverton ransomware saves encrypted files with the `.czvxce` file extension.

In this example, we now know that a machine with IP address of 192.168.0.35 is under a Coverton ransomware attack and we can take necessary action.

Appendix

Detection types

The Ransomware Bundle detects ransomware by searching your environment for suspicious files. The bundle finds suspicious files by inspecting traffic to and from CIFS servers. When a certain number of suspicious files are found, the Ransomware Bundle logs a detection event. Detection events are categorized by the type of suspicious file detected. In the following sections, we’ll explore which kinds of files cause each type of detection event.

Note: You can fine tune each detection type by modifying the ransomware trigger. For example, you can configure how many suspicious files must be found to trigger a given detection event.

Type one detection

Type one detection searches your environment for file type extensions that are known to be associated with ransomware attacks. The list of malicious file types is maintained in the ransomware trigger under `type_one_blacklist_basic`.

Note: ExtraHop attempts to keep the `type_one_blacklist_basic` list as up-to-date as possible; however, you can update the list with new known ransomware file extensions if you discover any.

Type two detection

Type two detection searches your environment for random file extensions. While some ransomware applications save encrypted files with specific file type extensions, others randomly generate file extensions for encrypted files. The Ransomware Bundle detects these events by maintaining a list of valid file extensions and alerting you if the bundle finds extensions that are not on that list. The list of valid extensions is maintained in the ransomware trigger under `type_two_whitelist_basic`.

Tip: If a file type that is common in your environment is not already included in the list of valid extensions, add the file type to the list to avoid false positives. You can also remove items from the whitelist if you know that the file type does not appear in your environment.

Type three detection

Type three detection searches your environment for potentially malicious file extensions that are not included in the type one blacklist. Although ExtraHop attempts to keep the type one blacklist as up-to-date as possible, new types of ransomware with new extensions are being developed every day.

The difference between how type two detection and type three detection work is subtle. Both detection types alert you when they discover file extensions that are not included in the list of valid file type extensions. However, type two detection focuses on the total number of suspicious extensions, while type three focusses on the total number of files with a suspicious extension.

If there are many different, unknown file types in your environment, it will cause a type two detection event. If there are many files that all share the same suspicious file type, it will cause a type three detection event. The following table demonstrates the difference between type two and type three detection events.

Sample fileset that might cause a type two detection event	Sample fileset that might cause a type three detection event
• `file1.78675` • `file2.44323` • `file3.18921` • `file4.84377` • `file5.15436` • `file6.11353` • `file7.89431` • `file8.09546`	• `file1.iamransomware` • `file2.iamransomware` • `file3.iamransomware` • `file4.iamransomware` • `file5.iamransomware` • `file6.iamransomware` • `file7.iamransomware` • `file8.iamransomware`

Type four detection

Type four detection searches your environment for files commonly found in ransomware attacks. After ransomware finishes encrypting files, ransomware leaves behind a set of instructions that explain how to pay the attackers to recover your data. These instructions are usually included in a file such as `decrypt_instructions.txt` or `help_decrypt.txt`. The Ransomware Bundle includes a list of known ransomware instruction files and alerts you if any of them show up in your environment.

The list of malicious file types is maintained in the ransomware trigger under `type_four_blacklist_advanced`. If one or more of these filenames exists in your environment legitimately, you can exclude those files from type four detection by removing them from the list.

Ransomware dashboard metrics

The Ransomware Bundle includes two dashboards: the Ransomware Detection dashboard and the Ransomware Supplemental dashboard. The Ransomware Detection dashboard shows you when and where ransomware events have occurred in your environment. The Ransomware Supplemental dashboard shows you more detailed information about ransomware threats, such as which suspicious file extensions have been detected.

Ransomware Detection

The Ransomware Detection dashboard shows detection events and which machines are involved in those events.

- Ransomware Detection Events Over Time shows you when each event occurred.
- Type One Detection Events by Affected Host shows you which machines encountered a type one detection event.
- Type Two Detection Events by Affected Host shows you which machines encountered a type two detection event.
- Type Three Detection Events by Affected Host shows you which machines encountered a type three detection event.
- Type Four Detection Events by Affected Host shows you which machines encountered a type four detection event.

Ransomware Supplemental

The Ransomware Supplemental dashboard provides detailed metrics about ransomware attacks to help you further investigate ransomware detection events.

The Invalid vs Valid File Extension WRITE/MODIFY Operations

This widget shows you how many write and modify operations involving invalid file types exist in your environment. Invalid file extensions are defined as any extension that is not included in the list of valid file extensions, which is maintained in the ransomware trigger under `type_two_whitelist_basic`.

Invalid File Extension WRITE/MODIFY Operations by IP Address

This widget shows you which machines are writing or modifying invalid file types and how many files are being written or modified.

Invalid File Extension Write/Modify Operations by Type

These widgets can help you discover whether type two or type three ransomware detection events are valid. The widgets display which invalid file types have been detected in your environment. If you don’t recognize the file type, search for the file type in a search engine (such as Google) to find whether that file type is valid or associated with ransomware attacks. If the file types displayed are expected in your environment, you can add the extensions to the list of valid extensions, which is maintained in the ransomware trigger under `type_two_whitelist_basic`.

Valid File Extension WRITE/MODIFY Operations by Type

This widget shows you which valid file type extensions have been detected in your environment. Valid file extensions are defined as any extension that is currently included in the list of valid file extensions. This widget is less likely to detect ransomware attacks than other ransomware widgets; however, in some cases, the widget might reveal potentially malicious activity. For example, if your environment deals primarily with .doc files, and you suddenly see thousands of `.jpg` files being written or modified, ransomware might be encrypting .doc files as `.jpg` files.

Valid File Extension WRITE/MODIFY Operations by IP Address

This widget shows you which machines are writing or modifying files with valid file types. If you find a suspicious number of operations on a certain file type in the Valid File Extension WRITE/MODIFY Operations by Type widget, this widget will show you which machines are involved in that activity. If you see a large number of writes and modifications coming from a machine that does not normally perform those operations in your environment, you might want to investigate further.