Red Hat Insights 2022

Assessing and Reporting Malware Signatures on RHEL Systems with the Insights for RHEL Malware Service

Know when systems in your RHEL infrastructure are exposed to malware risks

Last Updated: 2022-06-16

Red Hat Insights 2022 Assessing and Reporting Malware Signatures on RHEL Systems with the Insights for RHEL Malware Service

Know when systems in your RHEL infrastructure are exposed to malware risks

Legal Notice

Abstract

Use the Insights for RHEL malware-detection service with IBM X-Force threat intelligence signatures to know when a system in your infrastructure is the victim of a malware attack.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message.

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your feedback on our documentation. To provide feedback, highlight text in a document and add comments.

Prerequisites

- You are logged in to the Red Hat Customer Portal.
- In the Red Hat Customer Portal, the document is in the **Multi-page HTML** viewing format.

Procedure

To provide your feedback, perform the following steps:

1. Click the **Feedback** button in the top-right corner of the document to see existing feedback.

NOTE

The feedback feature is enabled only in the **Multi-page HTML** format.

2. Highlight the section of the document where you want to provide feedback.
3. Click the **Add Feedback** pop-up that appears near the highlighted text.
   A text box appears in the feedback section on the right side of the page.
4. Enter your feedback in the text box and click **Submit**.
   A documentation issue is created.
5. To view the issue, click the issue link in the feedback view.

CHAPTER 1. INSIGHTS FOR RHEL MALWARE-DETECTION SERVICE OVERVIEW

The Insights for Red Hat Enterprise Linux malware-detection service is a monitoring and assessment tool that scans RHEL systems for the presence of malware. The malware-detection service incorporates YARA pattern-matching software and malware-detection signatures. Signatures are provided in partnership with the IBM X-Force threat intelligence team working closely with the Red Hat threat intelligence team.

In the malware-detection service UI, User Access-authorized administrators and viewers can

- See the list of signatures against which their RHEL systems are scanned.
- See aggregate results for all RHEL systems with malware-detection enabled in the Insights client.
- See results for individual systems.
- Know when a system shows evidence of the presence of malware.

These features give security threat assessors and IT incident-response teams valuable information to prepare a response.

The malware-detection service does not recommend resolutions to resolve or remediate malware incidents.

The strategy to take in addressing a malware threat depends on a lot of criteria and considerations specific to each system and organization. Your organization's security incident response team is best qualified to design and implement an effective mitigation and remediation strategy for each circumstance.

1.1. YARA MALWARE SIGNATURES

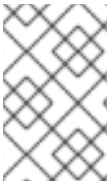
YARA signature detection is the cornerstone of the Insights for RHEL malware-detection service. YARA signatures are descriptions of malware types expressed as patterns. Each description consists of a set of strings and a boolean expression that define a rule. When one or more of the conditions in a signature exist on a scanned RHEL system, YARA records a hit on that system.

1.2. IBM X-FORCE THREAT INTELLIGENCE SIGNATURES

The Insights for RHEL malware-detection service includes predefined signatures developed by the IBM X-Force Threat Intelligence team to expose malware running on RHEL systems. Signatures compiled by the X-Force threat intelligence team are identifiable in the malware-detection service by the *XFTI-* prefix, for example, *XFTI_FritzFrog*.

CHAPTER 2. GET STARTED USING THE INSIGHTS FOR RHEL MALWARE-DETECTION SERVICE

To begin using the malware-detection service, the following actions must be performed. Procedures for each action follow in this chapter.



NOTE

Some procedures require sudo access on the system and others require that the administrator performing the actions be a member of a User Access group with the Malware detection administrator role.

Table 2.1. Procedure and access requirements to set up malware-detection service.

Action	Description	Required privileges
Install YARA and configure the Insights client	Install the YARA application and configure the Insights client to use the malware-detection service	Sudo access
Configure User Access on the Red Hat Hybrid Cloud Console	In Red Hat Hybrid Cloud Console > User Access > Groups, create malware-detection groups, and then add the appropriate roles and members to the groups	Organization Administrator on the Red Hat account
View results	See the results of system scans in the Hybrid Cloud Console	Membership in a User Access group with the Malware detection viewer role

2.1. INSTALLING YARA AND CONFIGURING THE INSIGHTS CLIENT

Perform the following procedure to install YARA and the malware-detection controller on the RHEL system, then run test and full malware-detection scans and report data to the Insights for RHEL application.

Prerequisites

- The system operating system version must be RHEL7 or RHEL8.
- The administrator must have sudo access on the system.
- The system must have the Insights client package installed, and be registered to Insights for RHEL.

Procedure

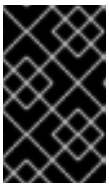
1. Install YARA 4.1 or later.
   Yara RPMs for RHEL7 & RHEL8 are available on EPEL. To install YARA for RHEL8, for example, you would enter the following commands:

   -

```
$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
$ sudo yum install yara
```

Alternatively, you can install yara from the source code using the instructions at this link. Note that the malware-detection controller requires YARA version 4.1.0 or later.

2. If not yet completed, register the system with Insights for RHEL.



IMPORTANT

The Insights client package must be installed on the system and the system registered with Insights for RHEL before the malware-detection service can be used.

a. Install the Insights client RPM.

```
$ sudo yum install insights-client
```

b. Test the connection to Insights for RHEL.

```
$ sudo insights-client --test-connection
```

c. Register the system with Insights for RHEL.

```
$ sudo insights-client --register
```

3. Run the Insights client malware-detection collector.

```
$ sudo insights-client --collector malware-detection
```

The collector takes the following actions for this initial run:

- Creates a malware-detection configuration file in **/etc/insights-client/malware-detection-config.yml**
- Performs a test scan and uploads the results

NOTE

This is a very minimal scan of your system with a simple test rule. The test scan is mainly to help verify that the installation, operation, and uploads are working correctly for the malware-detection service. There will be a couple of matches found but this is intentional and nothing to worry about. Results from the initial test scan will not appear in the malware-detection service UI.

4. Perform a full filesystem scan.

a. Edit **/etc/insights-client/malware-detection-config.yml** and set the **test_scan** option to false.

```
test_scan: false
```

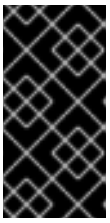
Consider setting the following options to minimize scan time:

- **filesystem_scan_only** - to only scan certain directories on the system
- **filesystem_scan_exclude** - to exclude certain directories from being scanned
- **filesystem_scan_since** - to scan only recently modified files

b. Re-run the client collector:

```
$ sudo insights-client --collector malware-detection
```

5. Optionally, scan processes. This will scan the filesystem first, followed by a scan of all processes. After the filesystem and process scans are complete, view the results at Red Hat Enterprise Linux > Malware detection.



IMPORTANT

By default, scanning processes is disabled. There is an issue with YARA and scanning processes on Linux systems that may cause poor system performance. This problem will be fixed in an upcoming release of YARA, **but until then it is recommended to NOT scan processes**.

a. To enable process scanning, set **scan_processes: true** in **/etc/insights-client/malware-detection-config.yml**.

```
scan_processes: true
```

NOTE

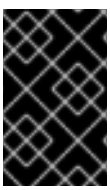
Consider setting these processes related options while you are there:
processes_scan_only - to only scan certain processes on the system
processess_scan_exclude - to exclude certain processes from being scanned
processes_scan_since - to scan only recently started processes

a. Save the changes and run the collector again.

```
$ sudo insights-client --collector malware-detection
```

2.2. CONFIGURE MALWARE-DETECTION GROUPS, ROLES, AND MEMBERS IN USER ACCESS

An Organization Administrator must create malware-detection groups in Red Hat Hybrid Cloud Console > User Access > Groups and add the necessary malware-detection roles and members (registered users on the account).



IMPORTANT

There is no "default-group" role for malware-detection service users. For users to be able to view data or control settings in the malware-detection service, they must be members of one or more User Access groups with one of the following roles:

- **Malware detection viewer**

- **Malware detection administrator**

NOTE

Currently there is no difference in the privileges conferred by those roles, but as new features emerge in the coming months, certain actions will only be available to admin users.

Resources

See the full documentation for configuring User Access on Red Hat Hybrid Cloud Console: *User Access Configuration Guide for Role-based Access Control (RBAC)*.

2.2.1. Creating and configuring malware-detection groups in User Access

The following procedure shows how an Organization Administrator on the account creates a User Access group, and adds the **Malware detection administrator** *role* to the group, then adds *members* who will have administrator privileges in the malware-detection service.

Regardless of the purpose, roles, or members, the following instructions are the same for creating any group in User Access. The Organization Administrator should create one group for administrators and another group for viewers.

IMPORTANT

Currently, there is no difference between the privileges conferred by the Malware detection administrator and viewer roles; however, this will change in a future release.

Prerequisites

You must be logged into your Red Hat Hybrid Cloud Console account as an Organization Administrator.

Procedure

1. Click the **gear icon** in the upper right quadrant of the application window and select **Settings**

2. Navigate to Red Hat Hybrid Cloud Console > User Access > Groups .
3. Click **Create group**.
4. Enter a **group name**, for example, *Malware Administrators*, and a description, then click **Next**.
5. Select the role to add to this group, for example, *Malware detection administrator*. Click the checkbox for that role, then click **Next**.
6. Add members to the group. Search for individual users or filter by username, email, or status. Check the box next to each intended member's name and click **Next**.
7. Review the details to make sure everything is correct. Click **Back** if you need to go back and change something.
8. Click **Submit** to finish creating the group.

2.3. VIEWING MALWARE-DETECTION SCAN RESULTS IN THE RED HAT HYBRID CLOUD CONSOLE

View results of system scans on the Hybrid Cloud Console.

Prerequisites

- YARA and the Insights client are installed and configured on the RHEL system using the procedures described in Chapter 2 of this document.
- You must be logged into the Hybrid Cloud Console.
- You are a member of a Hybrid Cloud Console User Access group with the *Malware detection administrator* or *Malware detection viewer role*.

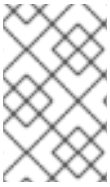
Procedures

1. Navigate to Red Hat Enterprise Linux > Malware detection > Systems .
2. View the dashboard to get a quick synopsis of all of your RHEL systems with malware-detection enabled and reporting results.
3. To see results for a specific system, use the **Filter by name** search box to search for the system by name.

CHAPTER 3. ADDITIONAL MALWARE-DETECTION SERVICE CONCEPTS

3.1. SYSTEM SCAN

At release, Malware detection administrators must initiate the Insights for RHEL malware-detection service collector scan on demand. Alternatively, administrators can run the collector command as a playbook or by using another automation method.



NOTE

The recommended frequency of scanning is up to your security team; however, because the scan can take significant time to run, the Insights for RHEL malware-detection service team recommends running the malware-detection scan weekly.

3.1.1. Initiating a malware-detection scan

Perform the following procedure to run a malware-detection scan. After the scan is complete, data are reported in the Insights for RHEL malware-detection service. The scan time depends on a number of factors, including configuration options, number of running processes, etc.

Prerequisites

Running the Insights client command requires sudo access on the system.

Procedure

1. Run **$ sudo insights-client --collector malware-detection**.
2. View results at Red Hat Enterprise Linux > Malware detection .

3.2. INTERPRETING MALWARE-DETECTION SERVICE RESULTS

In most cases, running a malware-detection scan with YARA will result in no signature matches. This means that YARA did not find any matching strings or boolean expressions when comparing a known set of malware signatures to the files included in the scan. The malware-detection service will send these results to Red Hat Insights and you can see the details of the system scan and lack of matches in the Insights for RHEL malware-detection service UI.

In the case that the malware-detection scan with YARA does detect a match, it will send the results of that match to Red Hat Insights and you can see details of the match in the malware-detection service UI, including the file and date. System scan and signature match history is displayed for the last 14 days so you can detect patterns and provide this information to your security incident response team. For example, if a signature match was found in one scan, but not found in the next scan of the same system, that can indicate the presence of malware that is detectable only when a certain process is running.

3.3. ADDITIONAL CONFIGURATION OPTIONS FOR THE MALWARE-DETECTION COLLECTOR

The **/etc/insights-client/malware-detection-config.yml** file includes several configuration options.

Configuration options

- **filesystem_scan_only**
  This is essentially a whitelist option whereby you specify which files/directories to scan. ONLY the items specified will be scanned. It can be a single item, or a list of items (adhering to yaml syntax for specifying lists of items). If this option is empty, it essentially means scan all files/directories (depending on other options).

- **filesystem_scan_exclude**
  This is essentially a blacklist option whereby you specify which files/directories NOT to scan. A number of directories are already listed meaning they will be excluded by default. These include virtual filesystem directories, eg /proc, /sys, /cgroup; directories that might have external mounted filesystems, eg /mnt and /media; and some other directories recommended to not be scanned, eg /dev and /var/log/insights-client (to prevent false positives). You are free to modify the list to add (or subtract) files/directories.

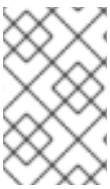
  Note that if the same item is specified both in filesystem_scan_only and filesystem_scan_exclude, eg /home, then filesystem_scan_exclude will 'win'. That is, /home will not be scanned. Another example, it's possible to filesysem_scan_only a parent directory, eg /var and then filesystem_scan_exclude certain directories within that, eg /var/lib and /var/log/insights-client. Then everything in /var except for /var/lib and /var/log/insights-client will be scanned.

- **filesystem_scan_since**
  Only scan files that have been modified 'since', where since can be an integer representing days ago or 'last' meaning since last filesystem scan. For example, filesystem_scan_since: 1 means only scan files that have been created or modified since 1 day ago (within the last day); filesystem_scan_since: 7 means only scan files that have been created/modified since 7 days ago (within the last week); and filesystem_scan_since: last means only scan files that have been created/modified since the last successful filesystem_scan of the malware-client.

- **exclude_network_filesystem_mountpoints and network_filesystem_types**
  Setting **exclude_network_filesystem_mountpoints: true** means that the malware-detection collector will not scan mountpoints of mounted network filesystems. This is the default setting and is to prevent scanning external filesystems, resulting in unnecessary and increased network traffic and slower scanning. The filesystems it considers to be network filesystems are listed in the **network_filesystem_types** option. So any filesystem types that are in that list and that are mounted will be excluded from scanning. These mountpoints are essentially added to the list of excluded directories from the **filesystem_scan_exclude** option. If you set **exclude_network_filesystem_mountpoints: false** you can still exclude mountpoints with the **filesystem_scan_exclude** option.

- **network_filesystem_types**
  Define network filesystem types.

- **scan_processes**



NOTE

Scan_process is disabled by default to prevent an impact on system performance when scanning numerous or large processes. When the status is false, no processes are scanned and the processes_scan options that follow are ignored.

+ Include running processes in the scan.

- **processes_scan_only**
  This is similar to filesystem_scan_only but applies to processes. Processes may be specified as a

single PID, eg 123, or a range of PIDs, eg 1000..2000, or by process name, eg Chrome. For example, the following values: 123, 1000..2000, and Chrome, would mean that PID 123, PIDs from 1000 to 2000 inclusive and PIDs for process names containing the string 'chrome' would ONLY be scanned.

- **processes_scan_exclude**
  This is similar to filesystem_scan_exclude but applies to processes. Like processes_scan_only, processes may be specified as a single PID, a range of PIDs, or by process name. If a process appears in both processes_scan_only and processes_scan_exclude, then processes_scan_exclude will 'win' and the process will be excluded.

- **processes_scan_since**
  This is similar to filesystem_scan_since but applies to processes. Only scan processes that have been started 'since', where since can be an integer representing days ago or 'last' meaning since the last successful processes scan of the malware-client.

Environment variables

All of the options in the **/etc/insights-client/malware-detection-config.yml** file can also be set using environment variables. Using the environment variable overrides the value of the same option in the configuration file. The environment variable has the same name as the configuration file option, but is uppercase. For example, the configuration file option **test_scan** is the environment variable **TEST_SCAN**.

For the **FILESYSTEM_SCAN_ONLY**, **FILESYSTEM_SCAN_EXCLUDE**, **PROCESSES_SCAN_ONLY**, **PROCESSES_SCAN_EXCLUDE**, and **NETWORK_FILESYSTEM_TYPES** environment variables, use a list of comma separated values. For example, to scan only directories **/etc**, **/tmp** and **/var/lib**, use the following environment variable:

```
FILESYSTEM_SCAN_ONLY=/etc,/tmp,/var/lib
```

To specify this on the command line (along with disabling test scan), use the following:

```
$ sudo FILESYSTEM_SCAN_ONLY=/etc,/tmp,/var/lib TEST_SCAN=false insights-client --collector malware-detection
```

Resources

For more information about the Insights client, see *Client Configuration Guide*.