


# CHECK RANSOMWARE EXPOSURE USING SECURITY VALIDATION

Security Validation provides a platform for evaluating your security controls in the face of new **ransomware** (<https://en.wikipedia.org/wiki/Ransomware>). The incident response experience and threat intelligence of Mandiant can provide insight of your security controls' ability to alert or block prevalent ransomware attacks.

To verify and substantiate your security measures against ransomware, you can do the following:

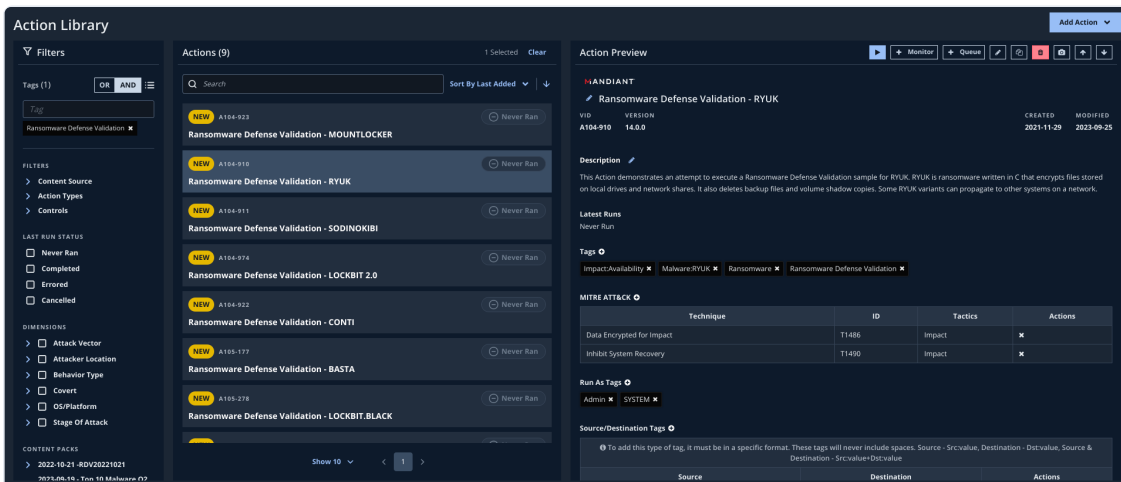
1. **Select and Run Actions from the Action Library** that cover Ransomware Defense Validation (RDV) workflows.
2. **Generate a Ransomware Validation Report.**

 All RDV content is tagged with the `Ransomware Defense Validation` system tag.

## Video Overview


### Run RDV Actions

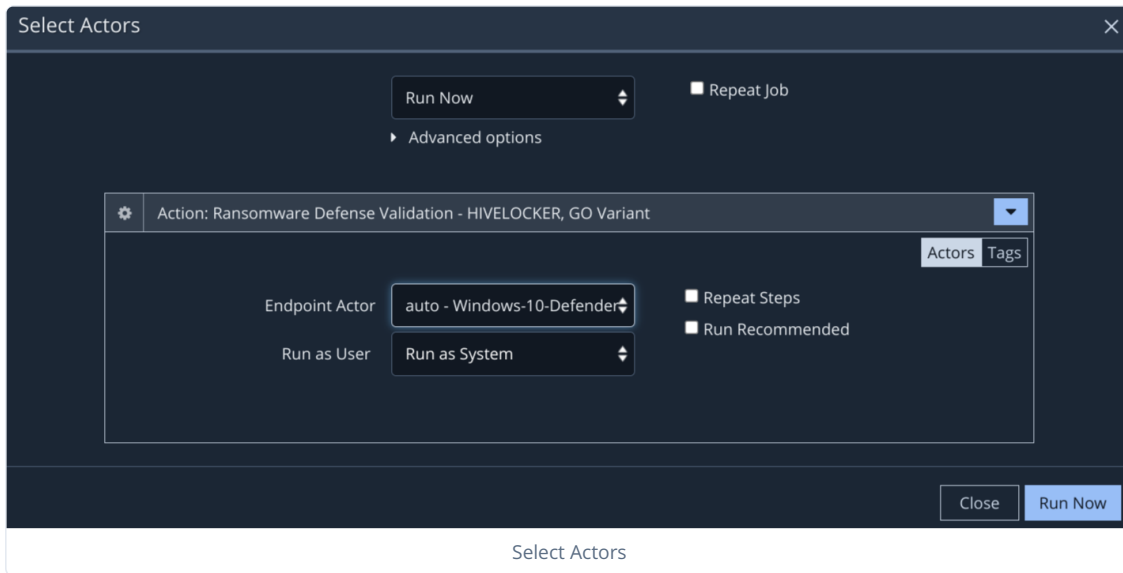
1. Go to **Library > Actions** to open the respective **Actions Library** page.
2. On the **Actions Library** page, add `Ransomware Defense Validation` as a tag to filter on the RDV content.
3. Get a list of ransomware Actions available in the library.



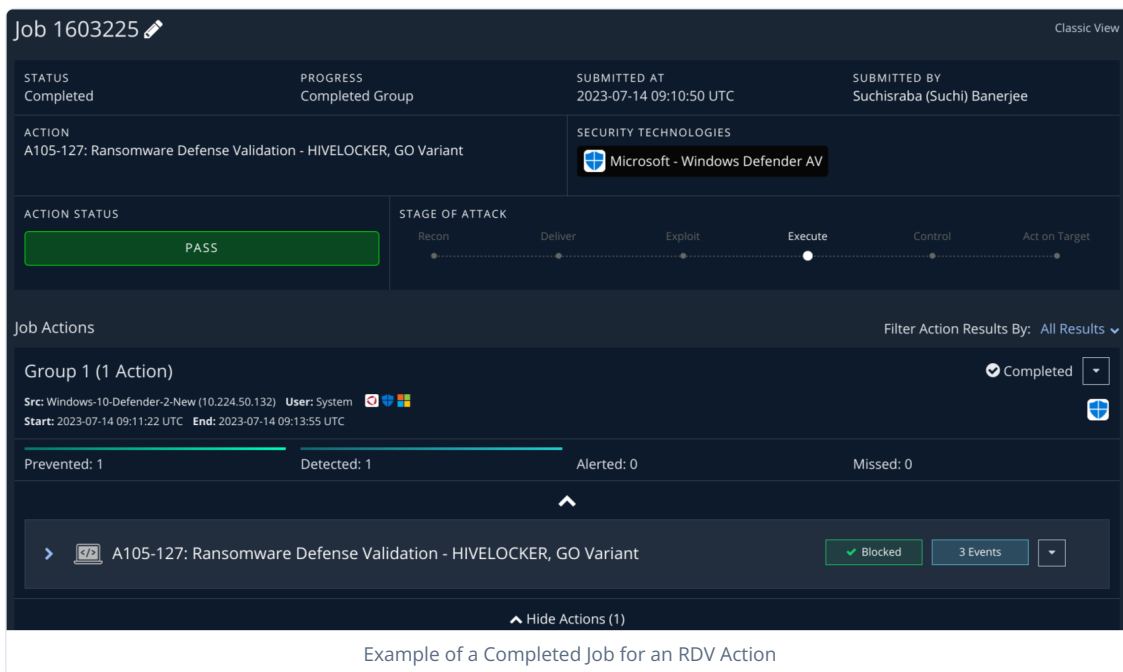
The screenshot shows the Mandiant Action Library interface. On the left, there are filters for tags (currently showing 'Ransomware Defense Validation'), content source, action types, controls, last run status, dimensions, and content packs. The main area displays a list of 9 actions, all tagged with 'Ransomware Defense Validation'. The actions include: MOUNTLOCKER, RYUK, SODINOKIBI, LOCKBIT 2.0, CONTI, BASTA, and LOCKBIT.BLACK. On the right, the 'Action Preview' for 'Ransomware Defense Validation - RYUK' is shown, including its description, latest runs, tags, MITRE ATT&CK techniques, and run as tags.

Action Library with Ransomware Defense Validation-tagged Content

4. Select the Action that you want to run and then click  **Run**.
5. Select **Actors**.
  - o For this example, we'll use a Windows Actor for the **Endpoint Actor**.
  - o If needed for your specific Actor, you can change the **Run as User** entry, but it is not required.



- Click **Run Now** or **Schedule**. When you click Run Now or at the Scheduled time, a Job is created and the Action runs. If you clicked **Run Now**, the Job Results page shows the status and results when the Job completes.



- Repeat the preceding steps if you want to run more ransomware validation Actions.

To learn more about security content and Jobs, refer to [Security Content & Jobs \(https://docs.mandiant.com/home/msv-sc-jobs\)](https://docs.mandiant.com/home/msv-sc-jobs).

### Create a Ransomware Validation Report

After checking your environment for ransomware exposure using the provided Actions, you can use these high-level steps that guide you to the ransomware-specific content widgets that you can add to a report. For more guidance on preparing comprehensive reports, see [Security Validation Reports \(https://docs.mandiant.com/home/msv-reports\)](https://docs.mandiant.com/home/msv-reports).

1. Go to **Analyze > Reports**.
2. Click **Create New Report**.
3. Optional: Update the time range and add rules, then click **Continue**.
4. Add one or both of the Ransomware components (**Ransomware Results** and **Ransomware Summary**), which are listed under the **Layout/Structure** section of the **Panel Library**.

The following screenshot shows an example of the **Ransomware Results** and **Ransomware Summary** content widgets after they're added to a report. Two ransomware families, HIVELOCKER and LOCKBIT 2.0, are selected.

Data Source  
Last 2 weeks (Relative) 
Job Action Results  
4599

Tags

Ransomware Results

Ransomware Defense Validation - HIVELOCKER, GO Variant [View Action Details](#)

Run On	Job Id	Execution Stage Results	Prevented At	Encrypted?
2023-07-14 09:11:22 AM UTC	1603325	<div style="display: flex; justify-content: space-between; align-items: center;"> <div style="text-align: center;">Execute</div> <div style="text-align: center;">Disrupt</div> <div style="text-align: center;">Encrypt</div> <div style="text-align: center;">Ransom</div> </div> <div style="margin-top: 5px; font-size: 0.9em;"> <span style="color: green;">✔</span> Blocked before Execute step.                 </div>	Pre-Execute	No

Ransomware Summary

HIVELOCKER
Control Readiness PASSED

**Description**

HIVELOCKER is a ransomware family that has impacted Windows and Linux operating systems. It was originally written in GoLang, but was rewritten in Rust in early 2022. It can encrypt both logical drives and remote network shares. On execution, the ransomware will parse command-line arguments that specify its behavior, such as processes to terminate and services to stop prior to encryption. HIVELOCKER can skip files based on file size, filename, or file extension specified in a command line argument during the encryption process.

**Actors**

UNC2727 UNC2900

**Aliases**

Hive (Microsoft)

[View More HIVELOCKER Details](#)

---

**Last Run Results - 15 minutes ago**

✔ Blocked before Execute step.

EXECUTE

DISRUPT

ENCRYPT

RANSOM

LOCKBIT 2.0
Control Readiness PASSED

**Description**

Based on [public reporting](#), LOCKBIT first emerged in late 2019. LOCKBIT is a Windows ransomware family capable of encrypting files using an Advanced Encryption Standard (AES)-based multi-threaded encryption algorithm. The key and the infection vector (IV) are then encrypted using the Curve25519 algorithm with an embedded public key and a private key generated at runtime. The malware is capable of maintaining persistence, spreading over the network via group policy objects (GPOs), SMB, and RPC, bypassing UAC, and spamming networked printers with ransom notes. The malware performs a system language check and does not execute on systems using languages common to Commonwealth of Independent States (CIS) countries. To facilitate encryption and prevent data recovery, LOCKBIT deletes Volume Shadow Copies and terminates a list of processes and services. After

[Show More](#)

**Actors**

UNC2758

**Aliases**

Lockbit Red (UNC2758)

[View More LOCKBIT 2.0 Details](#)

---

**Last Run Results - 21 hours ago**

✔ Blocked before Execute step.

EXECUTE

DISRUPT

ENCRYPT

RANSOM

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.