RanSim Product Manual

Updated: 1 month ago
Created: 7 years ago

RanSim Product Manual

RanSim is a tool that simulates ransomware attacks to see how your endpoint protection software might respond in the event of a real ransomware attack. You can use RanSim to see if your endpoint protection software would block ransomware or if it would create false positives. You can also use RanSim to see how specific files would be impacted by ransomware.

Click the links below to learn how to install RanSim, launch RanSim, and view your results. If you prefer video tutorials, you can also watch our RanSim (/hc/en-us/articles/360001529067) video.

> **Note**: For accurate results, your antivirus software must be configured and operating as normal when you use RanSim.

Jump to:

Prerequisites

Installing RanSim

Enabling Controlled Folder Access

Launching RanSim

Ransomware Scenarios

False Positive Scenarios

Analyzing Your RanSim Results

Prerequisites

To install and launch RanSim, you will need to meet the requirements listed below:

- Your computer must use Microsoft Windows 7 or newer.
- Your computer must have at least 2 processor cores, 2 GB of RAM, and 100 MB free HDD space.
- Your computer must be able to connect to the internet.
- Your computer must use a .NET Framework 4.5.2 to launch the tool.

  > **Note**: However, if your computer does not use this framework, the framework will be installed automatically when you install RanSim.

- To run our RIPlacer ransomware scenario, you must enable controlled folder access. For more information, see the Enabling Controlled Folder Access section of this article.

> **Note**: For accurate results, we recommend that you install RanSim on a computer that uses the same programs and security software as your users' computers.

Back to top

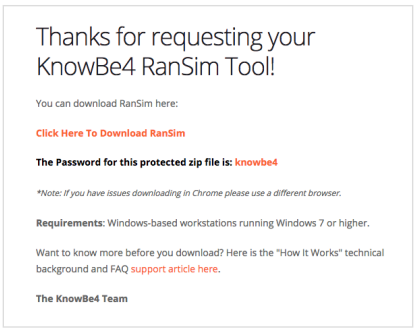
Installing RanSim

Once you've verified that your computer meets the prerequisites in the Prerequisites section above, you are ready to install RanSim.

To install RanSim, follow the steps below:

1. Navigate to knowbe4.com/ransomware-simulator (https://www.knowbe4.com/ransomware-simulator) in your browser.
2. Fill out the fields in the **I want my RanSim download** form.
3. Click **Get RanSim!**.

4. Click the **Click Here To Download RanSim** link. When you click this link, the **ransim.zip** file will download to your computer.



5. Double-click the **ransim.zip** file in your file manager.
6. Then, double-click the **SimulatorSetup.exe** file. When you double-click this file, you will be prompted to enter a password.
7. Enter "knowbe4" in the field to begin installing RanSim on your computer.

Once RanSim has finished installing, an “Installation Successfully Completed” message will display in the **KnowBe4 RanSim Setup** window. To learn how to launch RanSim, see the Launching RanSim section below.

> **Note:** For RanSim to install successfully, the **SimularorSetup.exe**, **Ranstart.exe**, **MainRunner.exe**, and **Collector.exe** files must be able to run. If your antivirus or antimalware product is blocking these files, you'll need to configure the product to allow them. This process will vary depending on the antivirus or antimalware product you are using. If any of these files are quarantined and you did not see a warning prompt to allow the file to run, you will need to restore the file from quarantine and repeat the steps above. For more information, see the Antivirus Software (https://support.knowbe4.com/hc/en-us/articles/360041405954#AV) section of our RanSim Frequently Asked Questions (FAQs) (/hc/en-us/articles/360041405954) article.

Back to top

Enabling Controlled Folder Access

To run the RIPlacer ransomware scenario, Microsoft controlled folder access must be enabled on your computer.

To learn how to enable controlled folder access manually or through Group Policy, click the links below:

- Enable Controlled Folder Access Manually
- Enable Controlled Folder Access Through Group Policy

Enable Controlled Folder Access Manually

To enable controlled folder access manually, follow the steps below:

1. Click the Windows button and enter "Ransomware protection" into the search bar.
2. Turn on the **Controlled folder access** option.
3. Add the following folder paths to the **Protected Folders** section:
    - c:\KB4\Varsim\DataDir\MainTests\8-Files
    - c:\KB4\Varsim\DataDir\MainTests\12-Files
    - c:\KB4\Varsim\DataDir\MainTests\16-Files
4. Navigate back to the **Ransomware protection** screen and click the **Allow an app through Controlled folder access** link.
5. Add the following applications to the allow list:
    - c:\windows\system32\cmd.exe
    - c:\windows\system32\notepad.exe
    - c:\KB4\Varsim\MainRunner.exe

Enable Controlled Folder Access Through Group Policy

To enable controlled folder access through Group Policy, follow the steps below:

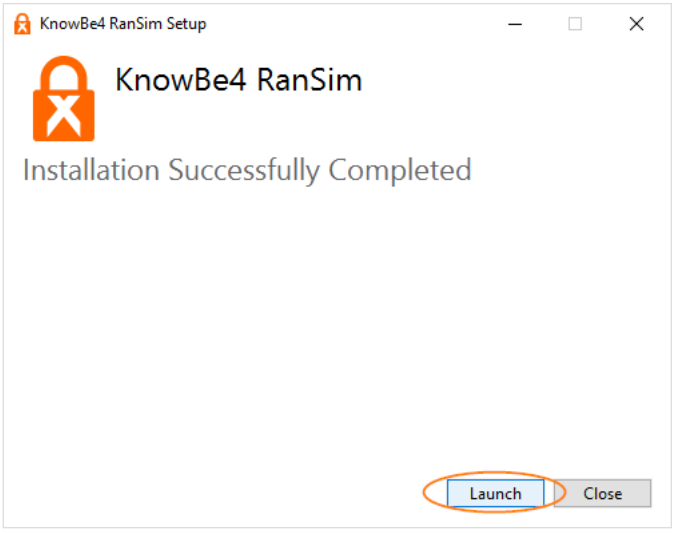
1. Open your **Group Policy Management Console**.
2. Right-click on the **Group Policy Object** you want to configure and click **Edit**.
3. In the **Group Policy Management Editor**, go to **Computer configuration**.
4. Click **Policies**, then click **Administrative templates**.
5. Expand the directory tree to **Windows components** > **Microsoft Defender Antivirus** > **Microsoft Defender Exploit Guard** > **Controlled folder access**.
6. Double-click the **Configure Controlled folder access** setting, then click **Enabled**.
7. Set the **Guard My Folders Feature** setting to **Monitor**.
8. Configure the protected folders and allowed applications. You can find this information in steps 3, 4, and 5 in the Enable Controlled Folder Access Manually subsection above.

Back to top

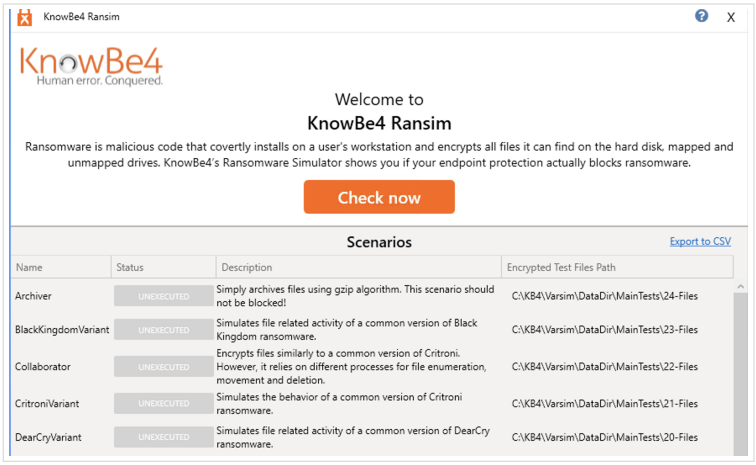
Launching RanSim

To launch RanSim, follow the steps below:

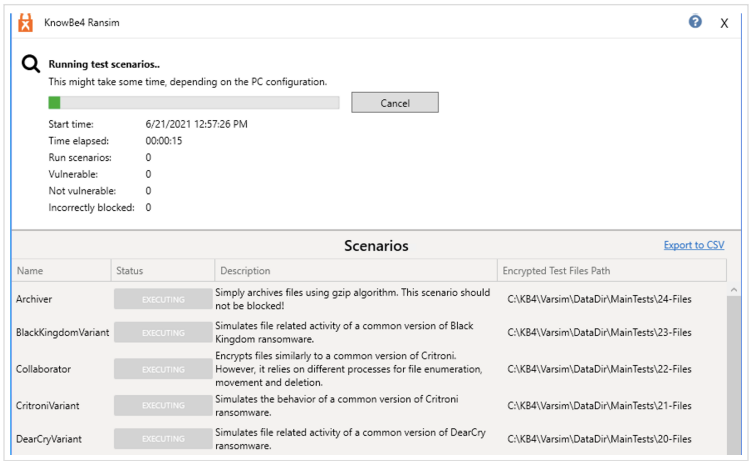
1. In the **KnowBe4 RanSim Setup** window, click **Launch**. Or, double-click the **KnowBe4 Ran Simulator** icon on your computer.



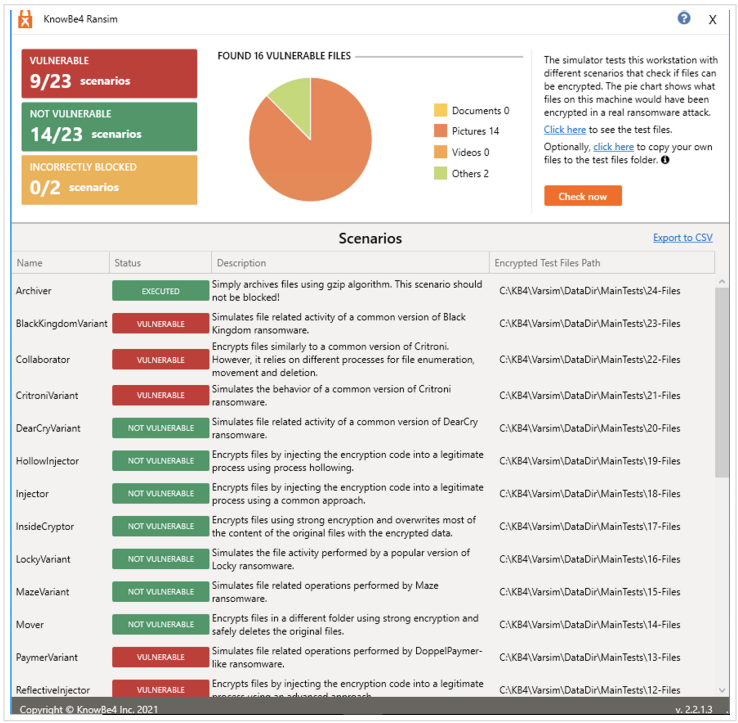
2. In the **Welcome to KnowBe4 Ransim** window, click the **Check now** button. When you click this button, RanSim will start running the ransomware simulations on your computer, including 23 ransomware scenarios and two false positive scenarios. To learn more about these ransomware scenarios and false positive scenarios, see the Ransomware Scenarios and False Positive Scenarios sections below.



You can view the scenarios' progress in the **KnowBe4 Ransim** window.



Once RanSim has run all the scenarios, your results will display. You can view the results for each scenario, including **Vulnerable** scenarios, **Not Vulnerable** scenarios, and **Incorrectly Blocked** scenarios. For more information about viewing and analyzing your results, see the Analyzing Your RanSim Results section below.



> **Tip**: You can click the **Check now** button again to run additional scenarios. After running your first scenarios, you also have the option to add your own test files to the test files folder. Then, RanSim will run tests to see if these files would be vulnerable to ransomware attacks.

Back to top

Ransomware Scenarios

When launched, RanSim will run 23 ransomware scenarios on your computer. To learn more about each scenario, see the table below:

> **Note**: To learn more about the two false positive scenarios that RanSim will run on your computer, see the False Positive Scenarios section below.

Scenarios (A to M) | Scenarios (N to S) | Scenarios (T to Z)

BlackKingdomVariant

This scenario simulates ransomware that appears to be written in Python. This type of ransomware uses code elements that are identical to code shared on development forums. This type of ransomware also uses unused or defunct code.

Example: Black Kingdom or GAmmAWare

Collaborator

This scenario simulates ransomware that uses multiple processes to encrypt files. In this scenario, executable code calls on other processes to enumerate the test files. Then, the original files are encrypted, moved, and deleted.

Example: Currently, there aren't any examples of this scenario. However, your endpoint protection software should be prepared to detect and stop this type of attack.

CritroniVariant

This scenario simulates ransomware that encrypts files using an uncommon attack pattern.

Example: Critroni or CBT

DearCryVariant

This scenario simulates ransomware that encrypts files by copying the files then deleting the original files. The encryption method used in this scenario does not need to contact the attacker's command-and-control server to encrypt files.

Example: DearCry

HollowInjector

This scenario simulates ransomware that uses process hollowing to inject malicious code into a legitimate process.

Example: Jaff or GandCrab

Injector

This scenario simulates ransomware that encrypts files by injecting malicious code into a legitimate process. This type of ransomware injects code by using a common method, such as dynamic link library (DLL) injection.

Example: GandCrab

InsideCryptor

This scenario simulates ransomware that encrypts files and adds the encrypted data to the original file.

Example: PClock

LockyVariant

This scenario simulates a variant of Locky ransomware. This scenario only simulates the method Locky uses to infect files, not its encryption algorithm.

Example: Locky

MazeVariant

This scenario simulates methods used by Maze ransomware.

Example: Maze

Mover

This scenario simulates ransomware that encrypts files and moves the files to a subfolder of the original folder.

Example: Alpha

Back to top

False Positive Scenarios

In addition to 23 ransomware scenarios, RanSim will also run two false positive scenarios on your computer. False positives are files or programs that are incorrectly labeled as malicious and blocked by your endpoint protection software.

RanSim's two false positive scenarios are called the **Archiver** and the **Remover**. If either of these scenarios are blocked by your endpoint protection software, your **Incorrectly Blocked** results in RanSim will increase. For more information about viewing results, see the Analyzing Your RanSim Results section below.

If the false positive scenarios are blocked, your RanSim results may not be an accurate measure of your endpoint protection software's effectiveness.

> **Note**: Unfortunately, we cannot prevent your endpoint protection software from blocking the false positive scenarios.

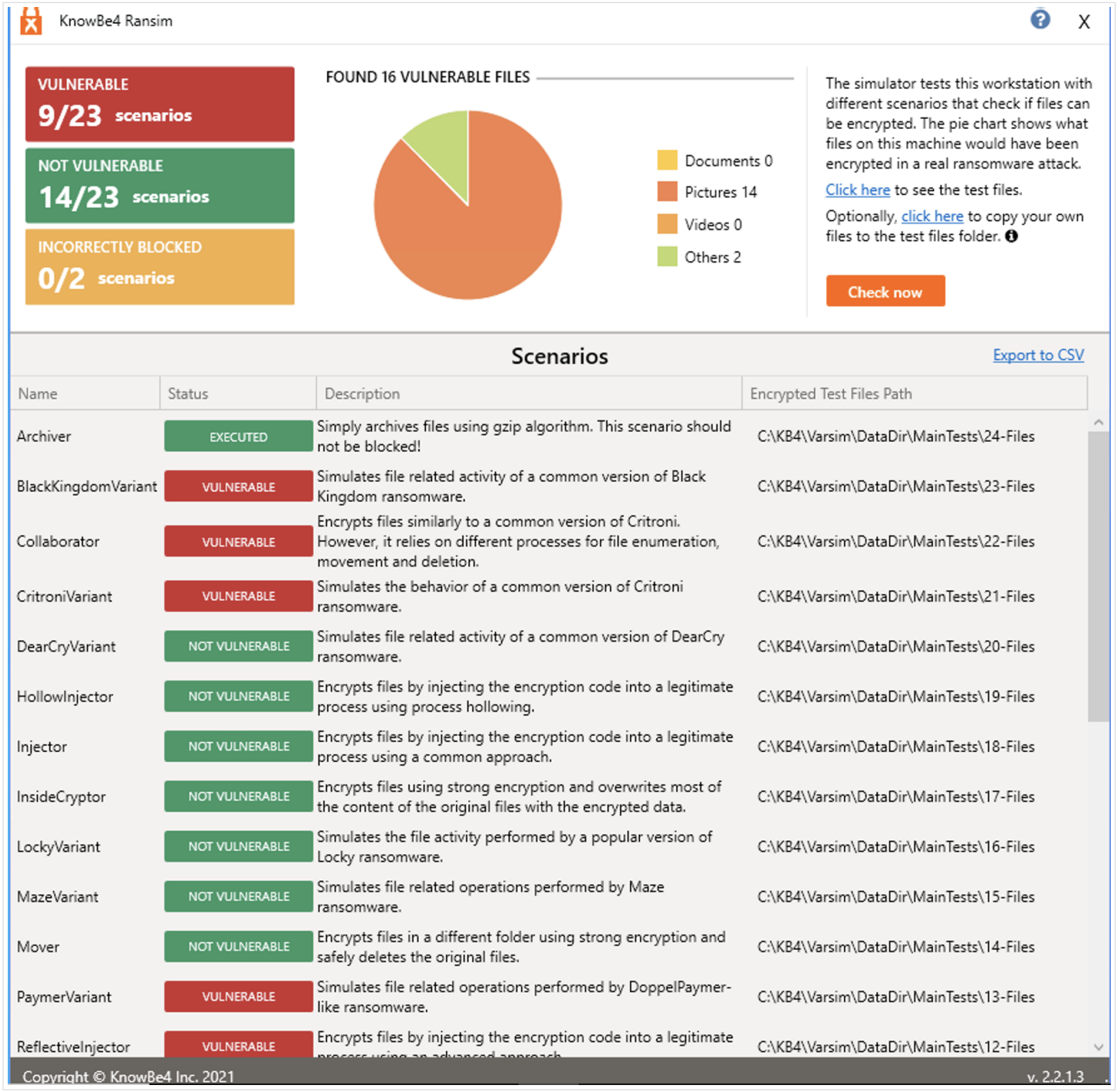
Back to top

Analyzing Your RanSim Results

Once RanSim has finished running all of the ransomware and false positive scenarios, you can view your results in the **KnowBe4 RanSim** window.

In the **Vulnerable**, **Not Vulnerable**, and **Incorrectly Blocked** boxes at the top-left corner of the window, you can view the number of scenarios in each status. Ideally, your results will display as 0/23 **Vulnerable** scenarios, 23/23 **Not Vulnerable** scenarios, and 0/2 **Incorrectly Blocked** scenarios.

In the **KnowBe4 RanSim** window, you can also view a circle graph and table with more information about your results. The circle graph displays information about the type of vulnerable files found, such as documents or pictures. The table displays information about each scenario, including the scenario's name and status, a description of the scenario, and the file path for the encrypted test files.



You can also click the **Export to CSV** link at the top-right corner of the **Scenarios** section to download a CSV file. This CSV file contains information about your RanSim results.

Back to top

✓ (/hc/en-us/signin?return_to=https%3A%2F%2Fsupport.knowbe4.com%2Fhc%2Fen-us%2Farticles%2F229040167-RanSim-Product-Manual)

× (/hc/en-us/signin?return_to=https%3A%2F%2Fsupport.knowbe4.com%2Fhc%2Fen-us%2Farticles%2F229040167-RanSim-Product-Manual)

6 out of 8 found this helpful

Have more questions? Submit a request (/hc/en-us/requests/new)

Comments

Article is closed for comments.

Related articles

Video: RanSim (/hc/en-us/related/click?
data=BAh7CjobZGVzdGluYXRpb25fYXJ0aWNsZV9pZGwrCOtkw9FTADoYcmVmZXJyZXJfYXJ0aWNsZV9pZGkEJ%2BCmDToLbG9jYWxlSSIKZW4tdXMGOgZFVDoIdXJsSSIxL2hjL2VuLXVzL2Fyc
-01cea2d94975b0e363829f79bc17136527af6ed9)

Whitelisting Data and Anti-Spam Filtering Information (/hc/en-us/related/click?
data=BAh7CjobZGVzdGluYXRpb25fYXJ0aWNsZV9pZGkE0mAjDDoYcmVmZXJyZXJfYXJ0aWNsZV9pZGkEJ%2BCmDToLbG9jYWxlSSIKZW4tdXMGOgZFVDoIdXJsSSJXL2hjL2VuLXVzL2FydGljb(
-322166ae8c80f76c6ae21c509501f2c6b2e4e23d)

Phish Alert Button (PAB) Product Manual (/hc/en-us/related/click?
data=BAh7CjobZGVzdGluYXRpb25fYXJ0aWNsZV9pZGkEiJ90DDoYcmVmZXJyZXJfYXJ0aWNsZV9pZGkEJ%2BCmDToLbG9jYWxlSSIKZW4tdXMGOgZFVDoIdXJsSSJHL2hjL2VuLXVzL2FydGljbG
-e9f8922d7f4f18334addad7d50ce39d7afdcfda7)

Weak Password Test (WPT) (/hc/en-us/related/click?
data=BAh7CjobZGVzdGluYXRpb25fYXJ0aWNsZV9pZGwrCFMZ5sYaADoYcmVmZXJyZXJfYXJ0aWNsZV9pZGkEJ%2BCmDToLbG9jYWxlSSIKZW4tdXMGOgZFVDoIdXJsSSI8L2hjL2VuLXVzL2Fyc
-756f7dfeeda179c5f00df5dab720b66a6a52da45)

Breached Password Test (BPT) (/hc/en-us/related/click?
data=BAh7CjobZGVzdGluYXRpb25fYXJ0aWNsZV9pZGwrCDgUw9FTADoYcmVmZXJyZXJfYXJ0aWNsZV9pZGkEJ%2BCmDToLbG9jYWxlSSIKZW4tdXMGOgZFVDoIdXJsSSJAL2hjL2VuLXVzL2Fy
-00919674e74838d832d0cc26bc95d6a2a738d713)