KnowBe4
Human error. Conquered.

KnowBe4 RanSim

How vulnerable is your network against ransomware infections?

Bad guys are constantly coming out with new versions of ransomware strains to evade detection. Is your network effective in blocking ransomware when employees fall for social engineering attacks?

KnowBe4's Ransomware Simulator "RanSim" gives you a quick look at the effectiveness of your existing network protection. RanSim will simulate 5 ransomware infection scenarios and show you if a workstation is vulnerable to infection.

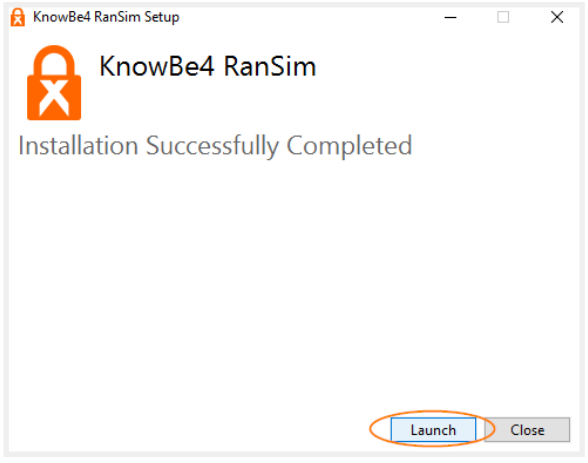
Here's how RanSim works:

- 100% harmless simulation of a real ransomware infection
- Does not use any of your own files
- Tests 5 types of infection scenarios
- Just download the install and run it
- Results in a few minutes!

Three Steps To Getting Started

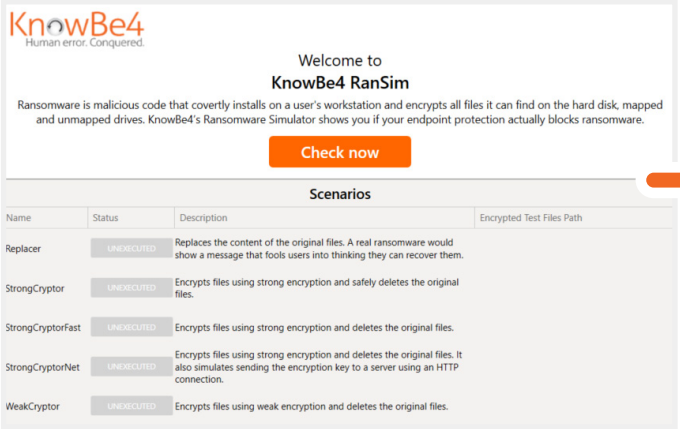
1. Ensure the workstation you are running is Windows 7 or higher, then download and install RanSim.

RanSim Installation/Launch Screen

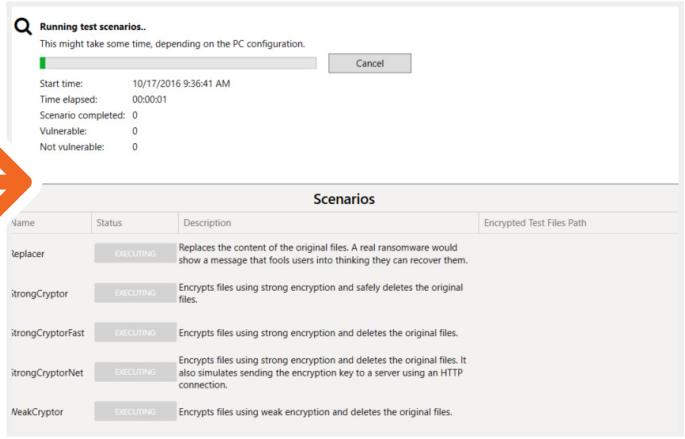


2. Click "Check Now" button. After clicking, RanSim will run five separate scenarios which will simulate different types and methods of ransomware. The name and description of each scenario will be shown on the user interface.

RanSim User Interface

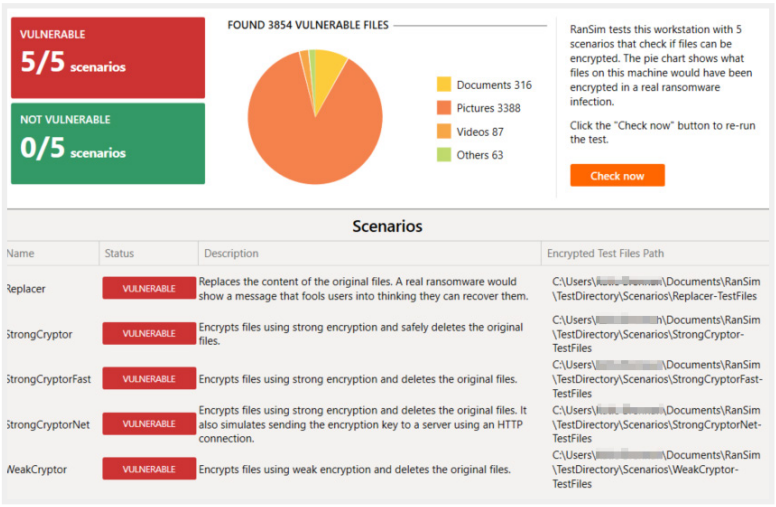


Active RanSim Simulation



3. After the simulations are completed, you'll see results showing if your system is vulnerable or not, based on each of the five scenarios. You'll also see a count of how many files would have been vulnerable if an actual ransomware attack had occurred

Results Screen



If you'd like, you can perform additional checks by simply clicking the "Check Now" button again. For more in-depth information, check out our support article.

NOTE: Created for Windows-based workstations running Windows 7+. RanSim does not alter any existing files on disk. As part of the simulation RanSim does enumerate all files on the local disk(s). For the purposes of encryption, simulated data files are downloaded from the Internet.