

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.

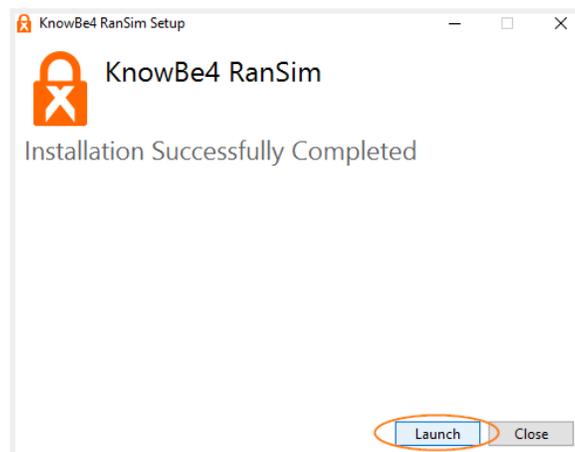
Here's how RanSim works:

- ✓ 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

KnowBe4
Human error. Conquered.

Welcome to
KnowBe4 RanSim

Ransomware is malicious code that covertly installs on a user's workstation and encrypts all files it can find on the hard disk, mapped and unmapped drives. KnowBe4's Ransomware Simulator shows you if your endpoint protection actually blocks ransomware.

Check now

Name	Status	Description	Encrypted Test Files Path
Replacer	UNEXECUTED	Replaces the content of the original files. A real ransomware would show a message that fools users into thinking they can recover them.	
StrongCryptor	UNEXECUTED	Encrypts files using strong encryption and safely deletes the original files.	
StrongCryptorFast	UNEXECUTED	Encrypts files using strong encryption and deletes the original files.	
StrongCryptorNet	UNEXECUTED	Encrypts files using strong encryption and deletes the original files. It also simulates sending the encryption key to a server using an HTTP connection.	
WeakCryptor	UNEXECUTED	Encrypts files using weak encryption and deletes the original files.	

Active RanSim Simulation

Running test scenarios.
This might take some time, depending on the PC configuration.

Start time: 10/17/2016 9:36:41 AM
Time elapsed: 00:00:01
Scenario completed: 0
Vulnerable: 0
Not vulnerable: 0

Scenarios

Name	Status	Description	Encrypted Test Files Path
Replacer	EXECUTING	Replaces the content of the original files. A real ransomware would show a message that fools users into thinking they can recover them.	
StrongCryptor	EXECUTING	Encrypts files using strong encryption and safely deletes the original files.	
StrongCryptorFast	EXECUTING	Encrypts files using strong encryption and deletes the original files.	
StrongCryptorNet	EXECUTING	Encrypts files using strong encryption and deletes the original files. It also simulates sending the encryption key to a server using an HTTP connection.	
WeakCryptor	EXECUTING	Encrypts files using weak encryption and deletes the original files.	

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

VULNERABLE
5/5 scenarios

NOT VULNERABLE
0/5 scenarios

FOUND 3854 VULNERABLE FILES

- Documents 316
- Pictures 3388
- Videos 87
- Others 63

RanSim tests this workstation with 5 scenarios that check if files can be encrypted. The pie chart shows what files on this machine would have been encrypted in a real ransomware infection.

Click the "Check now" button to re-run the test.

Check now

Name	Status	Description	Encrypted Test Files Path
Replacer	VULNERABLE	Replaces the content of the original files. A real ransomware would show a message that fools users into thinking they can recover them.	C:\Users\... \Documents\RanSim \TestDirectory\Scenarios\Replacer-TestFiles
StrongCryptor	VULNERABLE	Encrypts files using strong encryption and safely deletes the original files.	C:\Users\... \Documents\RanSim \TestDirectory\Scenarios\StrongCryptor-TestFiles
StrongCryptorFast	VULNERABLE	Encrypts files using strong encryption and deletes the original files.	C:\Users\... \Documents\RanSim \TestDirectory\Scenarios\StrongCryptorFast-TestFiles
StrongCryptorNet	VULNERABLE	Encrypts files using strong encryption and deletes the original files. It also simulates sending the encryption key to a server using an HTTP connection.	C:\Users\... \Documents\RanSim \TestDirectory\Scenarios\StrongCryptorNet-TestFiles
WeakCryptor	VULNERABLE	Encrypts files using weak encryption and deletes the original files.	C:\Users\... \Documents\RanSim \TestDirectory\Scenarios\WeakCryptor-TestFiles

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.