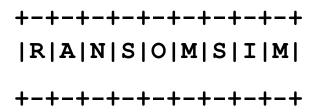
Ransomware Simulator - RANSOMSIM



In order to improve their security posture, many organizations want to test their security products and validate if they can prevent never before-seen ransomware without resorting to running malware.

Built to assist Red/Blue teams test their defenses.

This tool simulates typical ransomware behavior, such as:

- Kill processes (in this version notepad.exe only)
- Deleting Volume Shadow Copies
- Encrypting documents
- Dropping a ransomware note to the chosen folder

USAGE:

ransomsim3.exe [help] [mode] [path] [shadow copy] [password]

Arguments:

help (optional) Show this help message and exit mode Accepts encrypt or decrypt arguments.

path Location of the Folder with files for encryption

shadow copy (optional):

shadows-before - Delete shadows before encryption

shadows-after - Delete shadows after

password (optional) Password to use for encryption/decryption.

Quick Start: ransomsim3.exe encrypt C:\test2

WARNING - If the shadow copy delete option is selected, all shadow copies will be deleted.

WARNING - All files in the folder selected for the encryption will be encrypted.

RANSOMSIM executable hash change

There is an option to change the hash of the file by compiling the source using Autolt compile right click option, or command line compile.

Examples:

Run simulation from cmd: ransomsim3.exe <parameters> Get simulation help - ransomsim3.exe help

Parameters:

- 1. Choose action: (encrypt-Commandline encrypt files, decrypt- command line Decrypt encrypted files)
- 2. Path to the folder to encrypt. Default c:\ransomsimtest
- 3. Shadow copy delete. shadows-before Delete shadows before encryption, shadows-after Delete shadows after encryption.
- 4. Password for encryption. Default Password1
- 5. Encryption algorithm. Default AES (256bit)

Example:

Encrypt all files without shadow copy delete in the c:\ransomsimtest folder with Encryption algorithm AES (256bit) and password Password1.

ransomsim3.exe encrypt

Decrypt all files in the c:\ransomsimtest folder with Encryption algorithm AES (256bit) and password Password1.

ransomsim3.exe decrypt

Change default path to the folder to encrypt.

ransomsim3.exe encrypt c:\test2

Change default path to the folder to decrypt.

ransomsim3.exe decrypt C:\test2

Delete shadow copies and encrypt files.

ransomsim3.exe encrypt C:\test2 shadows-before

Encrypt files and delete shadow copies.

ransomsim3.exe encrypt C:\test2 shadows-after

Delete shadow copies, encrypt files and set custom encryption password.

ransomsim3.exe encrypt C:\test2 shadows-before Password2

Decrypt files with a custom encryption password.

ransomsim3.exe decrypt C:\test2 "" Password2

Encrypt files on the network drive via UNC path.

ransomsim3.exe decrypt \172.21.21.18\test2

Encrypt files on the mapped network drive via mapped drive letter. ransomsim3.exe decrypt Z:\test2

- ** Ransom note deployed to the encrypted folder.
- ** Kill process option added. By default it closes the notepad.exe process if it exists.

WARNING:

This software does not offer any kind of guarantee. Its use is exclusive for educational environments and / or security audits with the corresponding consent of the client. I am not responsible for its misuse or for any possible damage caused by it.