ShieldFS can stop and reverse the effects of extortion code

Italian researchers have developed a custom drop-in driver and system file that can detect signs of ransomwrae infection, stop the malicious activity and even transfer the encrypted file to its original state. .

Named ShieldFS, the new project is the product of 7 researchers from Politecnico di Milano University and is provided with details at the Black Hat USA 2017 security conference.

ShieldFS acts as a COW scanner and encryption operation

According to research reports released this year, ShieldFS has a complex mechanism, designed to detect COW (Copy-On-Write) activities.

COW operation takes place when the application obtains the file, copies, modifies and replaces the original file. Most ransomware variants today rely on the COW mechanism by taking the first file, encrypting its content and replacing it with the original file.

ShieldFS not only detects COW activity but also seeks to use symmetric encryption patterns, commonly used in file encryption.

Once the activity is detected in this form, ShieldFS will check the internal behavior pattern, differentiate normal processes from the infected ransomware.

According to the researchers, ShieldFS is currently equipped with models adapted to 2245 legitimate applications, allowing it to work without causing too many errors that lead to legal blocking.

ShieldFS is used as a file system to recover encrypted files

If ransomware is detected, ShieldFS will tell the operating system to stop the process and use the customized system file to reverse the ransomware behavior.

ShieldFS project is expected to help fight extortion

Technically, this is possible because ShieldFS is packaged as a drop-in driver installed on a virtual system file, designed 'shadowed' on COW operation, to keep a copy of the original file in Short time and allow to restore a certain amount of files.

It can be said that ShieldFS's real-time self-healing system file is like a replacement for Shadow Volume copying, which most variations of ransomware guarantee to be deleted before encrypting the user's file, avoid recovering by specialized data recovery software.

Here's a video of how ShieldFS works. Researchers are still working on this project, saying they intend to officially release in the near future. This is the full report on ShieldFS at Black Hat. *https://www.blackhat.com/docs/us-17/wednesday/us-17-Continella-ShieldFS-The-Last-Word-In-Ransomware-Resilient-Filesystems.pdf*