SSD-Insider++: A firmware-based approach to thwarting ransomware attacks

September 10 2021, by Bob Yirka

Credit: Pixabay/CC0 Public Domain

An international team of researchers is promoting the idea of using firmware to stop ransomware attacks before they can encrypt user data stored on a solid-state drive (SSD). The group presented their ideas back

in 2018 at the IEEE International Conference on Distributed Computing Systems, and more recently spoke to a reporter at The Register describing their ideas.

Ransomware is a type of software that blocks access to user data or an entire computer until a specified amount of money is paid to the entity that unleashes the attack. Over the past year, several high-profile attacks with very large ransom demands have been carried out against well-known entities. Antivirus makers have been hard at work adding features to their products that prevent such attacks, but the group with this new effort suggests a better way to fight ransomware: stopping the software from automatically using code embedded in hardware.

The work involved studying the characteristics of ransomware code and then writing their own code (SSD-Insider++) to recognize it and to stop it before it can encode user data. They then embedded that code in firmware on SDD devices. If SSD-Insider++ recognizes a ransomware attack, all activity to the SSD is stopped, preventing the data from being scrambled and allowing the user to take action to eliminate the threat. The approach comes at a price, of course; the firmware must process every read/write command sent to or from the SSD, which introduces a delay. The researchers claim their firmware adds just 12.8 to 17.3% to average latency delays. They also note that due to features in SSD devices, the software can also reverse any damage that sneaks through the initial stages of an attack.

The researchers tested their firmware using real ransomware and found it able to stop 100% of attacks. They also found that the software was able to repair any damage from attacks in less than 10 seconds. They do acknowledge that their system suffers from one flaw—ransomware coders could reverse-engineer SSD-Insider++ and then use what they learn to alter their own code to prevent it from being discovered. But the researchers note that firmware updates could be delivered to overcome

such changes.

More information: Sungha Baek et al, SSD-assisted Ransomware Detection and Data Recovery Techniques, *IEEE Transactions on Computers* (2020). DOI: 10.1109/TC.2020.3011214

SungHa Baek et al, SSD-Insider: Internal Defense of Solid-State Drive against Ransomware with Perfect Data Recovery, *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)* (2018). DOI: 10.1109/ICDCS.2018.00089