Researchers add 'time-travel' feature to drives to fight ransomware attacks

May 30 2019

Chance Coats presented the findings at the 2019 EuroSysConference. Credit: The Grainger College of Engineering

One of the latest cyber threats involves hackers encrypting user files and then charging "ransom" to get them back. In the paper, "Project Almanac: A Time-Traveling Solid State Drive," University of Illinois students Chance Coats and Xiaohao Wang and Assistant Professor Jian Huang from the Coordinated Science Laboratory look at how they can use the commodity storage devices already in a computer, to save the files without having to pay the ransom.

"The paper explains how we leverage properties of flash-based storage that currently exist in most laptops, desktops, mobiles, and even IoT devices" said Coats, a graduate student in electrical and computer engineering (ECE). "The motivation was a class of malware called ransomware, where hackers will take your files, encrypt them, delete the unencrypted files and then demand money to give the files back."

The flash-based, solid-state drives Coats mentioned are part of the storage system in most computers. When a file is modified on the computer, rather than getting rid of the old file version immediately, the solid-state drive saves the updated version to a new location. Those old versions are the key to thwarting ransomware attacks. If there is an attack, the tool discussed in the paper can be used to revert to a previous version of the file. The tool would also help in the case of a user accidentally deleting one of their own files.

Like any new tool, there is a trade-off.

"When you want to write new data, it has to be saved to a free block, or block that has already been erased," said Coats. "Normally a solid-state drive would delete old versions in an effort to erase blocks in advance, but because our drive is keeping the old versions intentionally, it may have to move the old versions before writing new ones."

Coats described this as a trade-off between retention duration and

storage performance. If the parameters of their new tool are set to maintain data for too long, old and unnecessary versions will be kept and take up space on the storage device. As the device fills with old file versions, the system takes longer to respond to typical storage requests and performance degrades. On the other hand, if the parameters are set to a retention window that is too narrow, users would have a quicker response time, but they may not have all of their backup files saved should a malware attack take place.

To manage this trade-off, Huang and his students built in functionality for the tool to monitor and adjust these parameters dynamically. Despite the dynamic changes to system parameters, their tool guarantees data will be retained for at least three days. This allows users the option to backup their data onto other systems within the guaranteed time-period if they choose to do so.

The idea behind their tool has gained interest at an international level. The paper about this research was published at a top-tier system conference, EuroSys, this past spring. Coats represented the group at the conference.

"Our research group really enjoys building practical computer systems; this is a great practice for our students, they will experience how our research will generate real-world impact," said Huang, an assistant professor of electrical and computer engineering at Illinois. "Moving forward, our group will look at the possibility of retaining user data in a storage device for a much longer time with lower performance overhead, and applying the time-traveling solid-state drive to wider applications such as systems debugging and digital forensics."

More information: Xiaohao Wang et al, Project Almanac, *Proceedings of the Fourteenth EuroSys Conference 2019 CD-ROM on ZZZ - EuroSys '19* (2019). DOI: 10.1145/3302424.3303983

Provided by University of Illinois at Urbana-Champaign

Citation: Researchers add 'time-travel' feature to drives to fight ransomware attacks (2019, May 30) retrieved 26 April 2024 from https://techxplore.com/news/2019-05-time-travel-feature-ransomware.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.