New software stops ransomware attacks

May 13 2020

Credit: CC0 Public Domain

Engineers from SMU's Darwin Deason Institute for Cybersecurity have developed software that detects ransomware attacks before attackers can inflict catastrophic damage.

Ransomware—a type of malware infection that causes important data

files to be locked and prevents users from accessing their important data until the hacker is paid—is crippling cities and businesses all over the world, and the number of ransomware attacks have increased since the start of the coronavirus pandemic. Attackers are also threatening to publicly release sensitive data if ransom isn't paid. The FBI estimates that ransomware victims have paid hackers more than $140 million in the last six-and-a-half years.

Unlike existing methods, such as antivirus software or other intrusion detection systems, SMU's new software works even if the ransomware is new and has not been used before.

SMU's detection method is known as sensor-based ransomware detection because the software doesn't rely on information from past ransomware infections to spot new ones on a computer. In contrast, existing technology needs signatures of past infections to do its job.

"With this software we are capable of detecting what's called zero-day ransomware because it's never been seen by the computer before," said Mitch Thornton, executive director of the Deason Institute and professor of electrical and computer engineering in SMU's Lyle School of Engineering. "Right now, there's little protection for zero-day ransomware, but this new software spots zero-day ransomware more than 95 percent of the time."

The new software also can scan a computer for ransomware much faster than existing software, said Mike Taylor, lead creator of the software and a Ph.D. student at SMU.

"The results of testing this technique indicate that rogue encryption processes can be detected within a very small fraction of the time required to completely lock down all of a user's sensitive data files," Taylor noted. "So the techniquedetects instances of ransomware very

quickly and well before extensive damage occurs to the victim's computer files."

Southern Methodist University (SMU) has filed a patent application for this technique with the U.S. Patent and Trademark Office.

Lyle Engineering students Taylor, a cybersecurity Ph.D. student, and Kaitlin N. Smith, a recent electrical engineering Ph.D. graduate, created the software, along with Thornton.

"Ransomware is malware that enters a victim's computer system and silently encrypts its stored files. It then alerts the user that they must pay a ransom, typically in a non-traceable currency such as bitcoin, in order to receive the key to decrypt their files," Thornton explained. "It also tells the victim that if they do not pay the ransom within a certain time period, the key for decryption will be destroyed and thus, they will lose their data."

SMU's software functions by searching for small, yet distinguishable changes in certain sensors that are found inside computers to detect when unauthorized encryptions are taking place.

When attackers encrypt files, certain circuits inside the computer have specific types of power surges as files are scrambled. Computer sensors that measure temperature, power consumption, voltage levels, and other characteristics can detect these specific types of surges, SMU researchers found.

The SMU software monitors the sensors to look for the characteristic surges. And when a suspicious surge is detected, the software immediately alerts the computer to suspend or terminate the ransomware infection from completing the encryption process.

Use of the computer's own devices to spot ransomware "is completely different than anything else that's out there," Taylor said.

Provided by Southern Methodist University