https://www.dailysentinel.com/news/article_c1130afc-e080-5660-a63b-51849c7f3e08.html

SMU develops anti-ransomware program

From Staff Reports
May 13, 2020

Engineers from Southern Methodist University have developed software that detects ransomware attacks like those earlier this year on Nacogdoches ISD and the City of Garrison before attackers can inflict catastrophic damage.

Ransomware — a type of malware used by hackers to invade computers systems and encrypt files in an effort to extort a ransom to unlock them — is crippling cities and businesses all over the world, and the number of ransomware attacks have increased since the start of the coronavirus pandemic.

Most recently, Texas was hit by attacks that took down the website and case management system for the state’s appellate and high courts.

The attack on the courts' network was discovered by staff Friday morning after beginning overnight, according a statement the Office of Court Administration issued Monday. It says staff limited the damage by disabling part of their network and that the courts will not pay any ransom.

Local trial courts appear to have been unaffected and there is no current evidence that sensitive or personnel information was compromised, according to the statement.

In February, hackers targeted Nacogdoches ISD and locked some files on district computers. The malicious software was also discovered in February on computers in Garrison City Hall but was caught early enough that no damage was done, Mayor Russell Wright said.

Unlike existing methods, such as antivirus software or other intrusion detection systems, the new software developed at the Darwin Deason Institute for Cybersecurity works even if the ransomware is new and has not been used before. The new software does not rely on information from past ransomware attacks to spot new ones on a computer.

“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% 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 technique detects instances of ransomware very quickly and well before extensive damage occurs to the victim’s computer files.”

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.

Cyberattacks have become increasingly more common since 2012, and have begun targeting rural communities in recent years. 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.

The Associated Press, staff writer Josh Edwards and the SUM office of public relations contributed to this report.