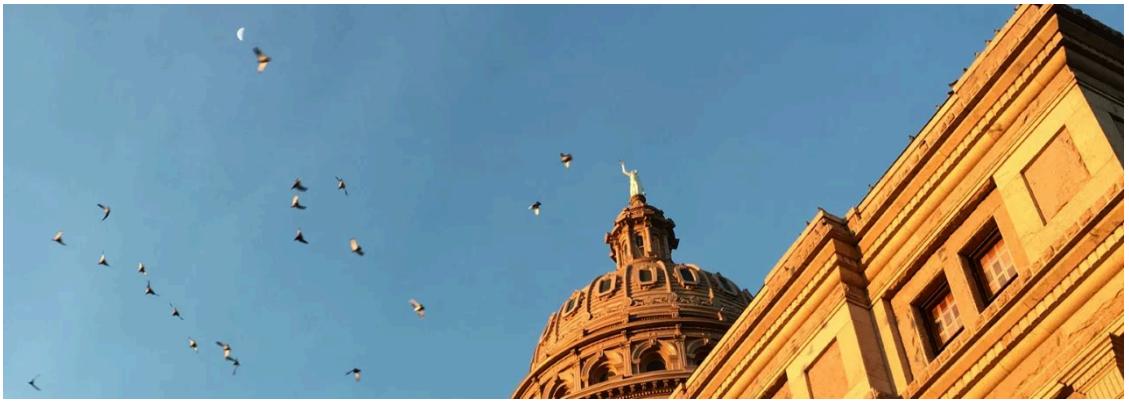
Texas Courts hit by ransomware, network disabled to limit spread

By Sergiu Gatlan

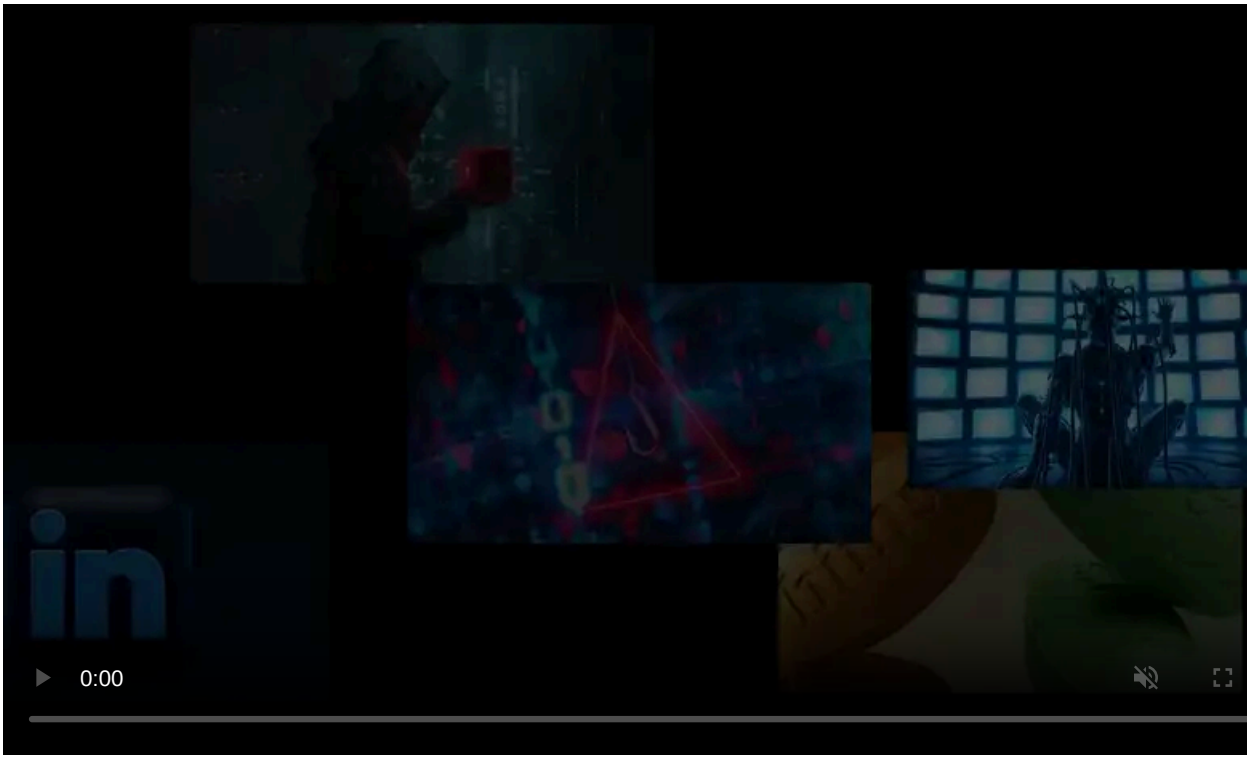
Published: 2020-05-11 · Archived: 2026-04-05 17:03:47 UTC

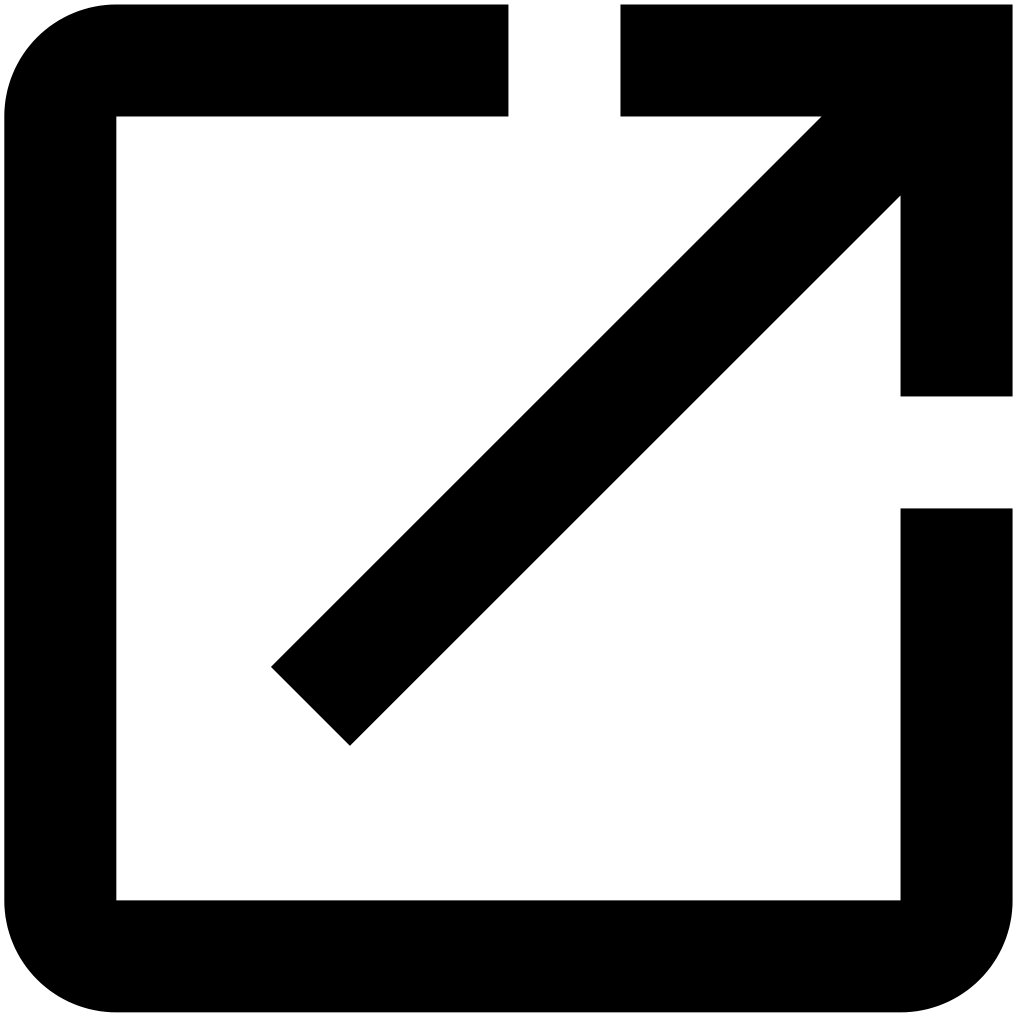


The Texas court system was hit by ransomware on Friday night, May 8th, which led to the branch network including websites and servers being disabled to block the malware from spreading to other systems.

"On Friday, May 8th, the Office of Court Administration (OCA), the information technology (IT) provider for the appellate courts and state judicial agencies within the Texas Judicial Branch, identified a serious security event in the branch network, which was later determined to be a ransomware attack," a statement published today on the site of the Texas Judicial Branch says.

"The attack began during the overnight hours and was first discovered in the early morning hours on Friday. The attack is unrelated to the courts' migration to remote hearings amid the coronavirus pandemic."


0:00



David Slayton, Administrative Director of the Office of Court Administration (OCA), the IT provider for the state judicial agencies and the appellate courts within the Texas Judicial Branch, further explained that the network will remain disabled until the breach is dealt with.

Texas' individual trial court networks were not impacted in the attack and, based on current information, no sensitive data has been compromised.

At this time, there is no indication that any sensitive information, including personal information, was compromised. Additionally, due to the structure of the IT function within the state judiciary, individual trial court networks throughout the state were unaffected by the cyberattack. - David Slayton

Slayton also said that the OCA "was able to catch the ransomware and limit its impact and will not pay any ransom," and that it continues to work on bringing all judicial entities and branch resources affected by the attack back online.

OCA is also collaborating with the Texas Department of Information Resources (DIR) to investigate the ransomware attack, as well as other information security authorities to recover the impacted data.

Texas Judiciary IT systems that have been moved to the cloud during recent years — including eFileTexas (for filing of documents), reSearchTX (for reviewing filed documents), collaboration tools for editing, and sharing documents, and email — haven't been impacted by the attack.

This will allow judicial branch agencies and some of the courts to continue their operations and daily activity unhindered.

"Judicial branch employees supported by OCA have received training in cybersecurity in recent weeks and will continue to receive updated training," Slayton added.

"Due to the ongoing nature of the investigation, remediation, and recovery, OCA will not comment further until additional information is available for public release."

Last year, Texas also faced a coordinated ransomware attack that hit 23 local governments, starting with the morning of August 16.

Those incidents were investigated local Texas authorities such as the DIR, Texas Division of Emergency Management, and Texas Military Department, as well as federal agencies such as the DHS, the FBI – Cyber, and FEMA.

The threat actor behind the attacks supposedly compromised a managed service provider (MSP) used by the Texas administration for technical support to deliver the ransomware payloads.

The attacker eventually asked for a collective ransom of $2.5 million to provide decryptors to all affected Texas entities.
