Over 20 Texas local governments hit in 'coordinated ransomware attack'

By Catalin Cimpanu

Published: 2019-08-18 · Archived: 2026-04-05 23:14:47 UTC

Twenty-three local Texas governments have been infected with ransomware last week in what Texas officials have described as a coordinated attack.

The attack took place on Friday morning, August 16, US time, when several smaller local Texas governments reported problems with accessing their data to the Texas Department of Information Resources (DIR).

DIR officials did not pubish a list of impacted local governments. On Friday, the agency couldn't provide an exact number of impacted entities, but a day later, DIR said the number is 23.

"It appears all entities that were actually or potentially impacted have been identified and notified," DIR said. "Responders are actively working with these entities to bring their systems back online."

The organization has been coordinating recovery efforts together with more than ten other Texas and US government agencies, such as the Texas Division of Emergency Management, the FBI, the DHS, the Texas Department of Public Safety, and others.

"At this time, the evidence gathered indicates the attacks came from one single threat actor," DIR officials said on Saturday.

Sodinokibi ransomware blamed for incident

Initially, *ZDNet* learned from a local source that the ransomware that infected the networks of the 23 local Texas governments encrypted files and then added the .JSE extension at the end.

Reports about a mysterious ransomware using this tactic have been floating around since June 2017, continued throughout 2018, and new activity has been reported as recently as this month.

However, following the publication of an initial version of this artice describing the infection as being caused by a so-called JSE ransomware, *ZDNet* received more information from a more authoritative source that the ransomware responsible for the infections across the 23 local Texas governments was the more well-known Sodinokibi (REvil) ransomware strain.

The .JSE file extensions spotted on some infected systems were most likely the created by the Ostap trojan, as part as one of its self-replication features -- which can be easily confused with ransomware. Ostap is a known trojan that is used to distribute the TrickBot trojan, a malware strain often used nowadays to download and deploy ransomware on infected hosts.

Part of the trend

In recent months, US cities have been a prime target for ransomware gangs, with infections reported all over the US.

In July, the governor of Louisiana declared a state emergency after a similar coordinated ransomware attack hit several school districts.

Article updated on July 19, 4:50 pm, ET, with information from new sources that the incident has been caused by the Sodinokibi (REvil) ransomware.

Related malware and cybercrime coverage:

- AT&T employees took bribes to plant malware on the company's network
- Windows malware strain records users on adult sites
- New Windows malware can also brute-force WordPress websites
- Microsoft: Russian state hackers are using IoT devices to breach enterprise networks
- Chinese cyber spies are stealing money from video game firms on the side
- A cyber-espionage group has been stealing files from the Venezuelan military
- How to avoid .JSE ransomware that hit the Texas government **TechRepublic**

- Malware lingers in SMBs for an average of 800 days before discovery **TechRepublic**
- US mayors resolve not to pay hackers over ransomware attacks **CNET**
