

SUBSCRIBE

SIGN IN

*CAME AND TOOK IT —*

# Ransomware strike takes down 23 Texas local government agencies

Data rustlers hit Texas local agencies in a coordinated ransomware strike.

SEAN GALLAGHER - 8/19/2019, 12:18 PM



[Enlarge](#) / They did.

Early on August 16, a total of 23 local government organizations in Texas were hit by a coordinated ransomware attack. The type of ransomware has not been revealed, and Texas officials asserted that no state networks were compromised in the attack.

A spokesman for the Texas Department of Information Resources (TDIR) told Ars that authorities are not ready to reveal the names of the entities affected, nor other details of the attack. State and federal agencies are in the midst of a response, and TDIR did not have information on whether any of the affected governmental organizations had chosen to pay the ransom.



Join Ars Technica and

## Get Our Best Tech Stories

DELIVERED STRAIGHT TO YOUR INBOX.

SIGN ME UP

Will be used in accordance with our [Privacy Policy](#).

But the TDIR did reveal that the ransomware came from a single source. "At this time, the evidence gathered indicates the attacks came from one single threat actor," a spokesperson said.

"Investigations into the origin of this attack are ongoing; however, response and recovery are the priority at this time."

Response teams from TDIR, the Texas Division of Emergency Management, Texas Military Department, Department of Public Safety, and the Texas A&M University System's Security Operations Center/Critical Incident Response Team (SOC/CIRT) are currently involved in the effort to bring systems back online, as are federal officials from the Department of Homeland Security, the FBI, FEMA, and other agencies.

This has been a particularly brutal year for ransomware thus far. While opportunistic attacks against consumers appear to be down from last year based on data from Malwarebytes, attacks against businesses and governments **are up by 365%**. IBM X-Force incident reporters have noted **a more modest 116% increase** in customer ransomware incidents. In July, the US Conference of Mayors reported that there have been 22 ransomware attacks on city, county, and state governments in the first six months of 2019. Those attacks include some notable incidents, such as the April attack on Albany, New York; RobbinHood ransomware attacks on Greenville, North Carolina and the City of Baltimore; and the Ryuk ransomware attacks **on three Florida municipal governments**. In July, Ryuk hit **Georgia's court system** and then **Georgia's state and capitol police**.

The financial damage has been significant. Baltimore is still in the process of recovering, just sending out its first water bills since May **and facing \$18 million in direct costs and lost revenue**. Elsewhere, two Florida cities paid out a total amounting to about \$1 million worth of cryptocurrency to regain their data.

## Go big or go home

The Texas attacks are the largest coordinated ransomware attacks seen against multiple local governments, but they're not necessarily the first coordinated attacks. Three school districts in northern Louisiana were hit by ransomware in a single incident in July. It's not clear if the districts

shared any network infrastructure. And a **December 2018 attack** struck multiple newspapers owned by Tribune Publishing after Ryuk ransomware spread across Tribune's internal wide-area network.

Texas has also seen a number of isolated ransomware incidents in the past, especially in the form of attacks against its Independent School Districts (ISDs). In February, the **Crosby ISD** near Houston was the victim of a ransomware attack that took the district's entire IT infrastructure down. And back in April 2016, 20 schools in the North East ISD were affected by a ransomware attack that encrypted 2.5 terabytes of data—which was eventually recovered from system backups.

*This story is developing, and Ars will update this article as more details are made available.*

READER COMMENTS 99

SHARE THIS STORY

---

**SEAN GALLAGHER**

Sean is Ars Technica's IT and National Security Editor. A former Navy officer, systems administrator, and network systems integrator with 20 years of IT journalism experience, he lives and works in Baltimore, Maryland.

**EMAIL** [sean.gallagher@arstechnica.com](mailto:sean.gallagher@arstechnica.com) // **TWITTER** [@thepacketrat](https://twitter.com/thepacketrat)



**Customizing Mini  
4WD Racers For  
High Speeds On A  
Small Scale**

WATCH

**Customizing Mini 4WD Racers For High Speed...**

venerable pastime experiencing a new boom in popularity. Randy breaks down the engineering challenges that Mini 4WD drivers need to overcome, and all the tiny gear and tech they use to make it happen. And to help you get started on your own Mini 4WD obsession, Randy unboxes and explains how to assemble a brand new Toyota Gazoo Racing WRT Yaris WRC.



**How Mind Control Saved Oddworld: Abe's Oddysee**



**Nintendo's Corey Olcsvary plays your Super Mario Maker 2 levels**



**Bioware answers unsolved mysteries of the Mass Effect universe**

[+ More videos](#)

[← PREVIOUS STORY](#)

[NEXT STORY →](#)

## Related Stories

Rash of ransomware continues with 13 new victims—most of them schools

Maze ransomware was behind Pensacola “cyber event,” Florida officials say

Georgia courts (mostly) shrug off ransomware attack

Ransomware, “wiper” malware attacks have more than doubled, IBM team says

## Sponsored Stories

Powered by



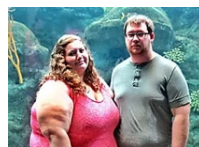
**Read This Before You Renew Amazon Prime Again**  
Wikibuy



**How To Efficiently Empty Your Bowels Every Morning - Top**



**[Photos] She Never Married And Now We Know Why**  
Direct Expose



**[Pics] Couple Makes A Bet: No Eating Out, No Cheat Meals, No**



**Nashville, Tennessee Drivers Are Stunned By This New Rule**



**[Pics] Things You Use Every day That Wouldn't Exist Without NASA**

**Surgeon Explains How**  
Gundry MD

**Alcohol. This Is Them 1 Year After**  
Ice Pop

US Auto Insurance Now

BlitzLift

## Today on Ars

Chrome to start blocking annoying notification requests

*Locke and Key* is finally coming to Netflix with an appropriately spooky trailer

The latest generation of climate models is running hotter—here’s why

Gallery: The amazing costumes, weird controllers, and gaming rarities of MAGFest 2020

Unpatched VPN makes Travelex latest victim of “REvil” ransomware

This tech could mean your phone stops you from getting killed by a car

How Ars tests Wi-Fi gear (and you can, too)

AMD’s third shoe finally drops at CES 2020—7nm Zen 2 mobile CPUs

STORE  
SUBSCRIBE  
ABOUT US  
RSS FEEDS  
VIEW MOBILE SITE

CONTACT US  
STAFF  
ADVERTISE WITH US  
REPRINTS

### NEWSLETTER SIGNUP

Join the Ars Orbital Transmission mailing list to get weekly updates delivered to your inbox.

**SIGN ME UP →**

CNMN Collection  
WIRED Media Group  
© 2020 Condé Nast. All rights reserved. Use of and/or registration on any portion of this site constitutes acceptance of our User Agreement (updated 1/1/20) and Privacy Policy and Cookie Statement (updated 1/1/20) and Ars Technica Addendum (effective 8/21/2018). Ars may earn compensation on sales from links on this site. Read our affiliate link policy.  
Your California Privacy Rights | Settings  
The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast.  
Ad Choices

