Fort Worth officials say leaked data came from Public Information Act request

therecord.media/fort-worth-officials-say-leaked-data-was-public

Jonathan Greig

July 4th, 2023

Officials in the City of Fort Worth, Texas denied being hacked for a second time after the same cybercrime group posted another batch of information allegedly stolen from government networks.

On Saturday, the SiegedSec hacking group said its “final” attack involved 40GB of stolen data from Fort Worth’s Department of Transportation & Public Works. The group shared screenshots of what appeared to be a file transfer service used by the city, which has nearly 1 million residents.

The group leaked the data alongside information stolen from several companies. In its previous attack on the City of Fort Worth and other local governments across the U.S., the hackers claimed that their motive was to punish U.S. states that are banning gender-affirming care.

Several experts have questioned that stated motive, and in subsequent attacks the group targeted states that had not banned the practice.

“This will be the conclusion of SiegedSec's attacks on the U.S,” the group said on Saturday. “Our intention throughout this operation was to make a statement and encourage others to do the same. We have proudly succeeded in our goal. Until next time.”

Fort Worth’s city spokeswoman initially said their IT department was investigating the issue but Fernando Costa, assistant city manager of Fort Worth, later told Recorded Future News that the city’s IT department has determined that the published data “consists of public information posing no risk of identity theft or financial fraud.”

“IT staff validated the source of the data is previously released data in response to a Public Information Act request. The underlying server, database and storage, again, was not compromised,” the city’s IT department said. “All the data posted by the attacking group is public information and not sensitive information that could result in identity theft or financial fraud.”

Last week, the city confirmed that a website with government information was breached and accessed by the same group of hackers.

But they downplayed the severity of that incident in comments to the media, explaining that the data came from a website that city workers use to manage maintenance activities.

“It appears the hackers downloaded file attachments to work orders within the system and those attachments include things like photographs, spreadsheets, invoices for work performed, emails between staff, PDF documents and other related materials for work orders,” the city’s Chief Technology Officer Kevin Gunn said.

None of the information was “sensitive in nature,” Gunn said, adding that overall most of it is data that “would be released through a Public Information Act request.” Gunn said the investigation uncovered that the group stole login information but it is unclear how they managed to accomplish that.

No other systems were accessed and no sensitive data was accessed or released, Gunn reiterated.

SiegedSec never asked the city for a ransom, according to Gunn. When asked by reporters what motivated the group, he referenced their Telegram post, noting that they appeared interested in embarrassing the city and “making a political statement.”

SiegedSec claimed it hacked the governments of Arkansas and Kentucky last year after the state banned abortion following the Supreme Court decision to overturn Roe v. Wade. But state officials later confirmed that the group simply downloaded publicly available record data.

The group leaked documents or defaced the websites of government agencies in Nebraska, South Dakota, Texas, Pennsylvania and South Carolina last week.

- Government
- Cybercrime

Get more insights with the
Recorded Future

Intelligence Cloud.

Learn more.
No previous article

No new articles

Jonathan Greig

Jonathan Greig is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.