# Tulsa warns of data breach after Conti ransomware leaks police citations

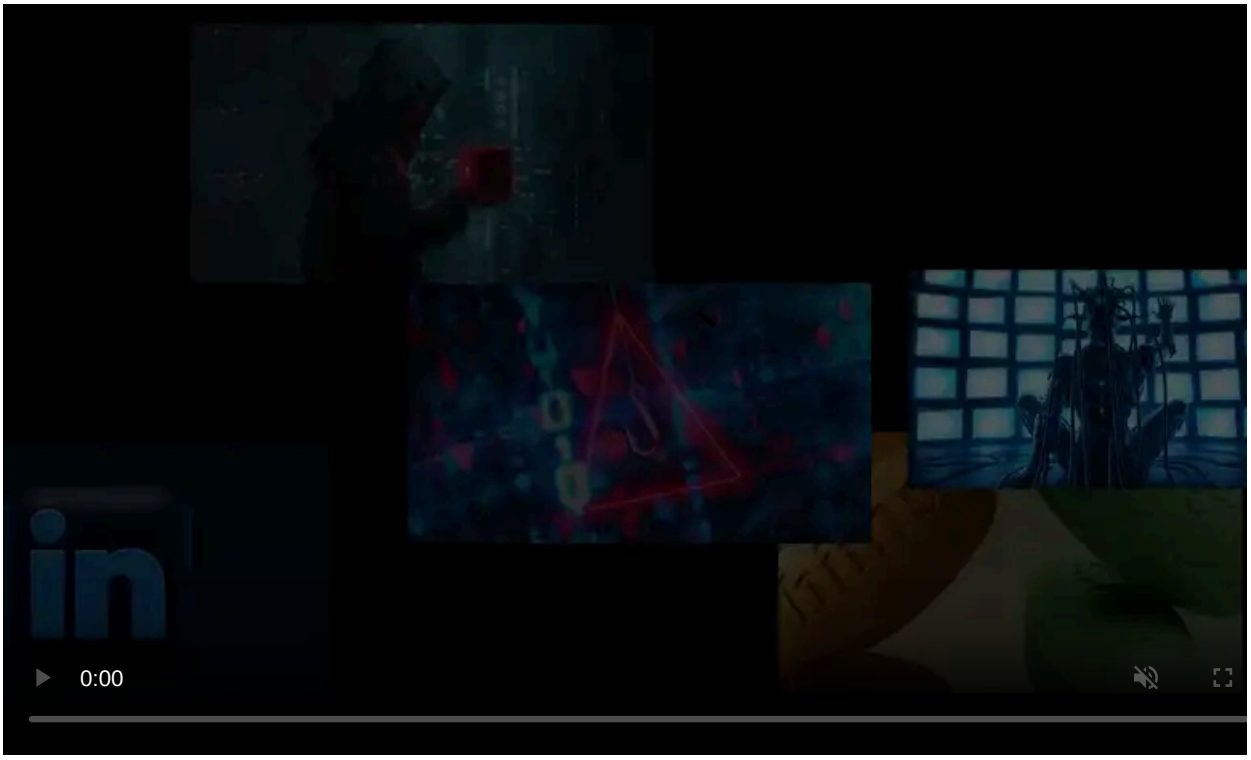
By Lawrence Abrams

Published: 2021-06-23 · Archived: 2026-04-05 17:54:50 UTC

The City of Tulsa, Oklahoma, is warning residents that their personal data may have been exposed after a ransomware gang published police citations online.

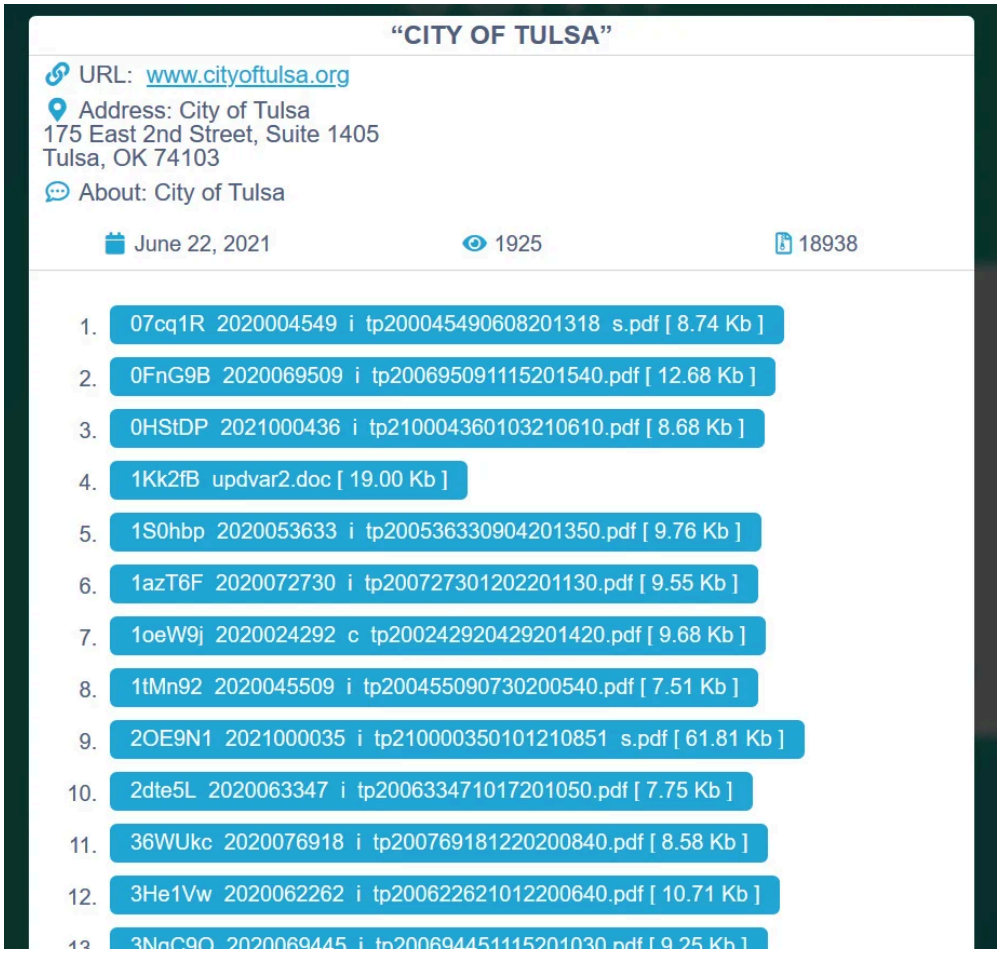
In early May, Tulsa suffered a ransomware attack that led to the City shutting down its network to prevent the spread of the malware.

The attack disrupted Tulsa's online bill payment systems, utility billing, and email, as well as the websites for the City of Tulsa, the Tulsa City Council, Tulsa Police, and the Tulsa 311.


0:00

At the time of the attack, it was unknown what ransomware operation was behind the attack on Tulsa.

However, yesterday the Conti Ransomware gang claimed responsibility and published 18,938 of the City's files, mainly police citations and internal Word docu




**City of Tulsa documents leaked by Conti**

After the leak of data, the City of Tulsa issued a press release warning that personally identifiable information was exposed in the leaked police citations.

"Today, the City of Tulsa was made aware the persons responsible for the May 2021 City of Tulsa ransomware attack shared more than 18,000 City files via the dark web mostly in the form of police citations and internal department files," said the press release.

"Police citations contain some Personal Identifiable Information (PII) such as name, date of birth, address and driver's license number. Police citations do not include social security numbers."

The City is asking "anyone who has filed a police report, received a police citation, made a payment with the City, or interacted with the City in any way where PII was shared" to be extra vigilant against threat actors performing identity theft using the exposed information.

When ransomware gangs publish stolen data, other threat actors download it and use the personal information to conduct their own phishing attacks, scams, and other fraudulent activity.

Due to this, it is vital for those affected to monitor their credit reports and credit card statements for fraud and be on the lookout for suspicious emails or SMS texts claiming to be from the City.

---