Hacked software provider acknowledges ransomware attack

September 25 2020, by Jake Bleiberg

The sign for Tyler Technologies is seen outside the company's offices, Thursday, Sept. 24, 2020, in Plano, Texas. The major U.S. provider of software services to state and local governments, including the online publishing of election results, has told customers that an unknown intruder broke into its phone and IT systems. Plano, Texas-based Tyler Technologies told customers in an email that it discovered the breach and contacted law enforcement and enlisted outside cybersecurity help. (AP Photo/LM Otero)

A major U.S. provider of software services to state and local governments acknowledged Friday that it was hit by a ransomware attack two days after telling clients an unknown intruder had compromised its phone and information technology systems.

Tyler Technologies said in a statement that it confirmed the intruder used ransomware but did not provide further details on its response, citing an ongoing investigation. A spokesperson for the Dallas-area company did not directly answer a question about whether it paid to have its systems unlocked.

Ransomware purveyors are increasingly breaking into company and government networks and siphoning out valuable data before scrambling them and demanding payouts. They threaten to make the stolen data public if the victim doesn't pay up.

Tyler, which is a publicly traded S&P 500 company, informed clients across the country Wednesday about the data breach, but said the impact appeared limited and that there was no reason to believe its customers were affected. The company said it brought in outside information technology experts and informed law enforcement.

The FBI has declined to comment on the breach.

Tyler provides software services to local and state governments across the country for everything from jail and court management systems to payroll, human resources, tax and bill collection, and land records.

Some governments also use one of its platforms to post election data online, although that use appears limited and Tyler has said data for that software is hosted on Amazon Web Services, not the network that was hacked.

Cybersecurity experts say voter registration databases are particularly sensitive. Voting could be seriously disrupted if voter records were altered or deleted.

Malware attacks are often not detected for months, and experts warn that gives hackers plenty of time to hop on to connected networks and surreptitiously prepare disruptive attacks.

Dan Wallach, a Rice University computer scientist, said the attack on Tyler gets the hackers "adjacent to sensitive election materials."

"The idea is that you first establish a beachhead, then spread out laterally and dig in," Wallach told The Associated Press.

The hack follows other ransomware attacks on parts of the Texas courts system and the state Transportation Department. More than 20 local governments in the state were hit by similar hacks in 2019.

Brett Callow, an analyst with the cybersecurity firm Emsisoft, previously said Tyler may have been hit with the same ransomware that struck the Texas Department of Transportation, based on an encrypted file uploaded to the Google-owned malware identification service VirusTotal in June that included "tylertech" in the file name.