# Government software provider Tyler Technologies hit by ransomware

bleepingcomputer.com/news/security/government-software-provider-tyler-technologies-hit-by-ransomware/

Lawrence Abrams

By
Lawrence Abrams

- September 23, 2020
- 08:03 PM
- 0

Leading government technology services provider Tyler Technologies has suffered a ransomware attack that has disrupted its operations.

Tyler Technologies is one of the largest U.S. software development and technology services companies dedicated to the public sector.

With a forecasted $1.2 billion in revenue for 2020 and 5,500 employees, Tyler Technologies provides technical services for local governments in many states in the USA.

Starting earlier today, Tyler Technologies' website began to display a maintenance message, and their Twitter account tweeted that they were having technical difficulties.


In an email seen by BleepingComputer, Tyler Technologies CIO Matt Bieri emailed clients stating that they are investigating a cyberattack and have notified law enforcement.

"I am writing to make you aware of a security incident involving unauthorized access to our internal phone and information technology systems by an unknown third party. We are treating this matter with the highest priority and working with independent IT experts to conduct a thorough investigation and response."

"Early this morning, we became aware that an unauthorized intruder had disrupted access to some of our internal systems. Upon discovery and out of an abundance of caution, we shut down points of access to external systems and immediately began investigating and remediating the problem. We have since engaged outside IT security and forensics experts to conduct a detailed review and help us securely restore affected equipment. We are implementing enhanced monitoring systems, and we have notified law enforcement," Bieri stated in an email to clients.

Bieri also stated that current investigations indicate that the attack was limited to Tyler Technologies' local network.

In posts to the Municipal Information Systems Association of California (MISAC) forum shared with BleepingComputer, local government employees were told that Tyler Technologies suffered a ransomware attack affecting their phone ticketing system and support systems.

"We were told this morning from one of the support techs that they got hit with ransomware early this morning on their corporate networks. Don't have any other details at this point other than support is down until they access their systems," one local municipality employee posted to the MISAC forum.

Another MISAC user stated that they heard the attack was limited to Tyler Technologies' internal network and did not affect clients.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731 or on Wire at @lawrenceabrams-bc.

## Tyler technologies hit by RansomExx ransomware

Cybersecurity sources familiar with the attack told BleepingComputer that Tyler Technologies suffered an attack by the RansomExx ransomware.

RansomExx is a rebranded version of the Defray777 ransomware and has seen increased activity since June when they attacked the Texas Department of Transportation (TxDOT), Konica Minolta, and most recently IPG Photonics.

While BleepingComputer has not obtained the ransom note, we found an encrypted file uploaded to VirusTotal today related to this attack.

This encrypted file has an extension of '.tylertech911-f1e1a2ac,' which includes Tyler Technologies' name and is the same format used in other RansomExx attacks.

RansomExx does not have a ransomware data leak site, but that does not mean they do not steal unencrypted files before deploying their ransomware.

BleepingComputer has contacted Tyler Technologies with further questions but has not received a response.

*Thx to Fate112 for the tip!*

### Related Articles:

Luxury fashion house Zegna confirms August ransomware attack

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

Practice your development skills with lifetime access to DevDojo

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

- Developer
- Public Sector
- RansomEXX
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence

Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

## You may also like: