Tyler Technologies paid ransomware gang for decryption key

bleepingcomputer.com/news/security/tyler-technologies-paid-ransomware-gang-for-decryption-key

By
Lawrence Abrams

- October 10, 2020
- 10:05 AM
- 0

Tyler Technologies has paid a ransom for a decryption key to recover files encrypted in a recent ransomware attack.

Tyler Technologies states that they are the largest software company in North America devoted to the public sector, with over $1.2 billion in revenue for 2020 and 5,500 employees.

On September 23rd, Tyler Technologies suffered a cyberattack by the RansomExx ransomware operators, who were also behind recent attacks on Konica Minolta and IPG Photonics.
In response to the attack, Tyler Technologies immediately disconnected portions of their network to contain the ransomware's spread and limit their clients' exposure.

"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," Tyler Technologies CIO Matt Bieri emailed clients.

The attack caused significant disruption to Tyler Technologies operations, it was contained locally and did not spread to their clients.

Sources in the public sector have told BleepingComputer that the ransomware attack severely impacted Tyler Technologies and that the company expected it would take thirty days to recover operations fully.

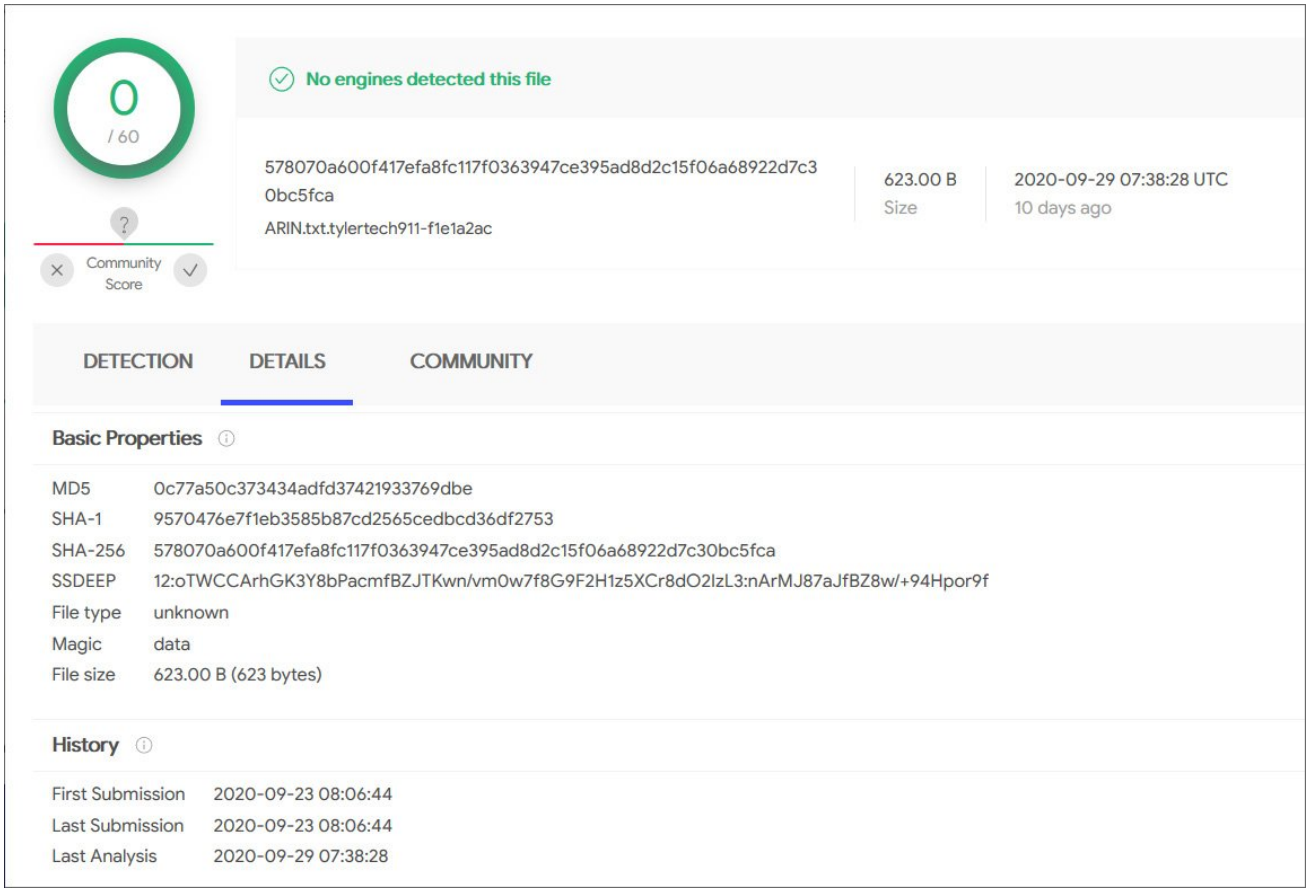
Paid ransom to obtain a decryptor

A source told BleepingComputer that Tyler Technologies paid the RansomExx ransom demand to recover encrypted data.

It is not known, though, how much was paid to receive a decryption key.

When the ransomware encrypted Tyler Technologies' files, they appended an extension similar to '.tylertech911-f1e1a2ac.'

To prove that the decryptor was valid, BleepingComputer was able to decrypt encrypted files [1, 2] uploaded to VirusTotal at the time of the ransomware attack.



Encrypted Tyler Technologies file on VirusTotal

When decrypted, the Arin.txt file contained a list of IP ranges used by the company.

RansomExx is also known to steal data before encrypting devices on a network. The ransomware operators then threaten to release this stolen data unless a victim paid the ransom.

As many school districts, court systems, and local and statement governments in the United States are Tyler Technologies customers, the risks of the public leaking of sensitive information and source code is concerning.

This concern may have been a driving factor in the decision to pay the ransom.

When asked about the decryptor, Tyler Technologies did not dispute the ransom payment, but told BleepingComputer that they could not disclose any further information at this time.

"Given the sensitivities around the incident and our investigation of it, and our active cooperation with law enforcement, we are not at liberty to disclose additional details at this time."

Related Articles:

The Week in Ransomware - September 25th 2020 - A Modern-Day Gold Rush

Tyler Technologies warns clients to change remote support passwords

Ransomware gangs add DDoS attacks to their extortion arsenal

ThunderX ransomware silenced with release of a free decryptor

Government software provider Tyler Technologies hit by ransomware

Lawrence Abrams

Lawrence Abrams is the creator and owner of BleepingComputer.com. Lawrence's area of expertise includes 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

You may also like: