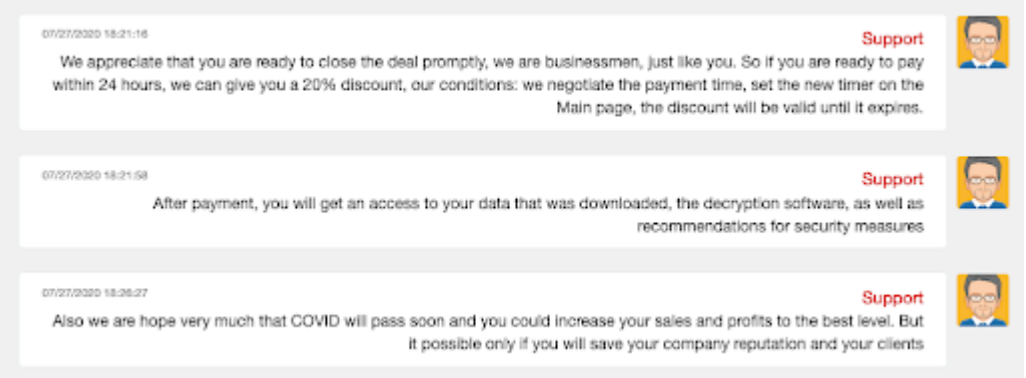
Ragnar Locker Targets CWT in Ransomware Attack

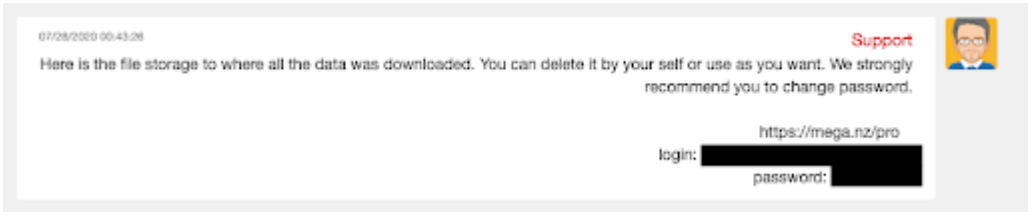
By Orlaith Traynor

Published: 2020-07-31 · Archived: 2026-04-06 03:22:54 UTC

Ragnar Locker strikes again. CWT, formerly Carlson Wagonlit Travel and fifth largest travel management firm, confirmed a cyber attack, which it said occurred the weekend of July 26-27, 2020. According to Threatpost, CWT stated, “We can confirm that after temporarily shutting down our systems as a precautionary measure, our systems are back online and the incident has now ceased.” Ragnar Locker initiated the ransomware attack and may have stolen 2 terabytes of data, allegedly including thousands of global executives credentials. This is particularly worrisome given CWT provides travel services to as much as 33% of the Fortune 500. The ransomware criminals then demanded a $10 million dollar ransom in exchange for a commitment not to publicly release the stolen data. To demonstrate the seriousness of their threat, Ragnar Locker showed CWT a password-protected press release on a hidden part of their website. It appears CWT negotiated down the ransom amount, citing a recent downturn in their business resulting from the COVID-19 crisis. Ragnar Locker committed not to publish the stolen information, and even shared tips to avoid future hacks, after a final payment of $4.5 million dollars was paid in



bitcoin (414). Subsequent to the payment, Ragnar Locker held up their end of the bargain, providing credentials to access a MEGA Cloud drive where CWT's stolen data was held and removing the press announcement from their private website. Ragnar Locker even shared tips to avoid future hacks including information that no antivirus can avoid such an infection, but better internal policies may.



CybelAngel investigated this ransomware incident after an independent security analyst uncovered a malware sample citing CWT as a victim of the Ragnar cryptolocker and exposed this ransomware exploit on Twitter to his 23,000 followers. According to exchanges we were able to read between CWT and Ragnar, credentials to access the stolen data on a MEGA Cloud drive were shared to the victim. CybelAngel cannot confirm whether the documents were deleted in time or if a third party was able to retrieve them beforehand. We continue monitoring the situation and scanning for sensitive data from this incident which may be exposed on the internet. CybelAngel detects data leaks across the internet far beyond the Surface and Deep/Dark Web to include connected storage, cloud apps, open databases, et al. Only with the proprietary combination of machine learning and expert cyber analysis, can CybelAngel detect data leaks quickly enough to avert catastrophic data breaches.

Source: https://cybelangel.com/blog/ragnar-locker-targets-cwt/