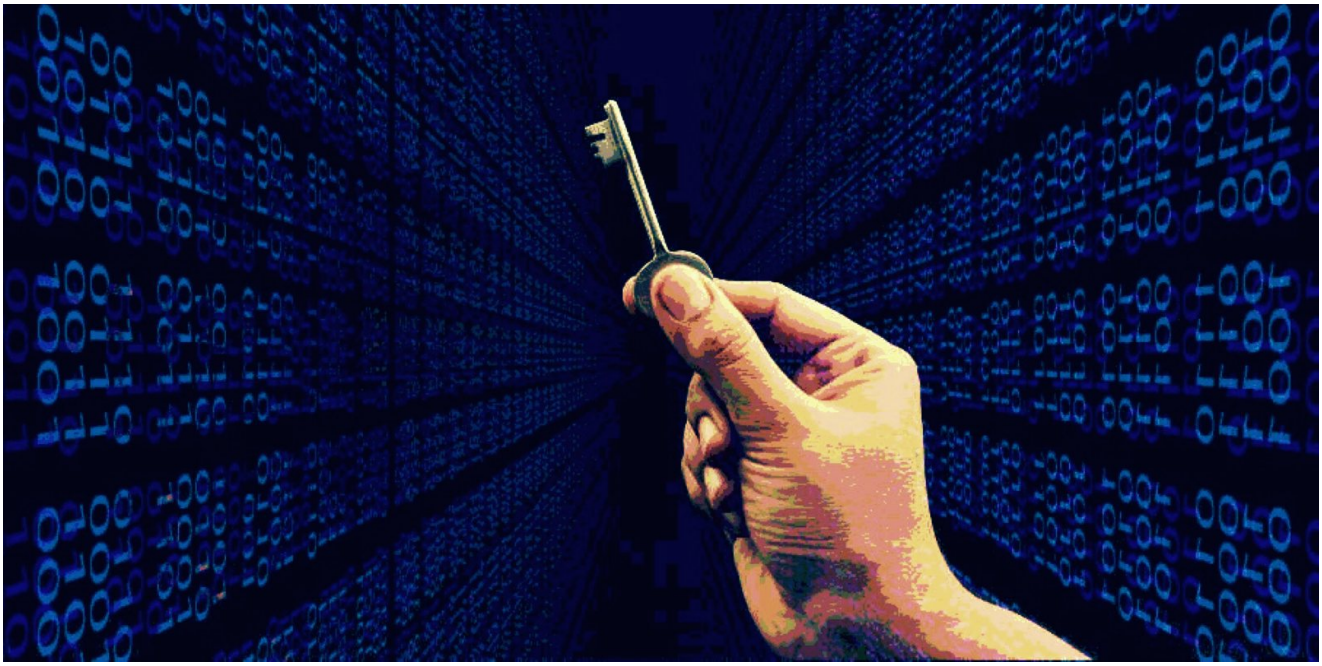
AstraLocker ransomware shuts down and releases decryptors

bleepingcomputer.com/news/security/astralocker-ransomware-shuts-down-and-releases-decryptors/

Sergiu Gatlan

By
Sergiu Gatlan

- July 4, 2022
- 02:15 PM
- 1

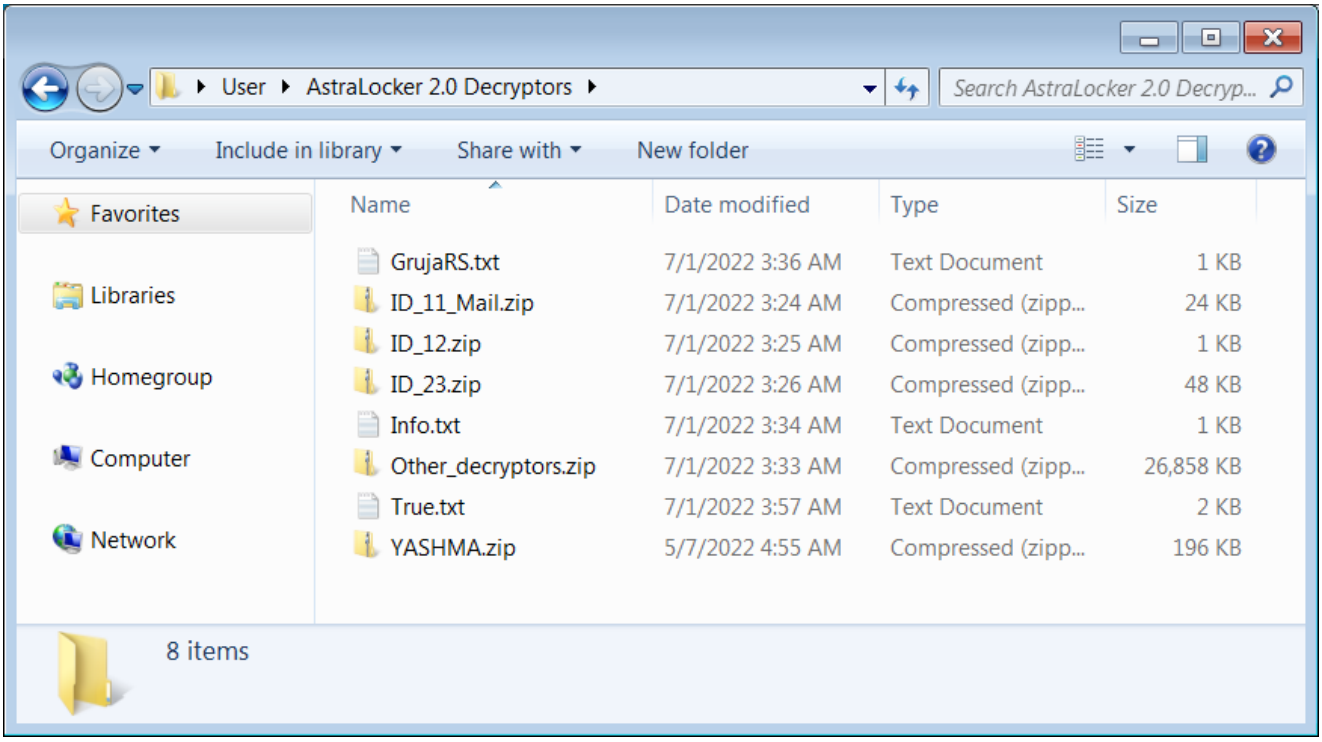


The threat actor behind the lesser-known AstraLocker ransomware told BleepingComputer they're shutting down the operation and plan to switch to cryptojacking.

The ransomware's developer submitted a ZIP archive with AstraLocker decryptors to the VirusTotal malware analysis platform.

BleepingComputer downloaded the archive and confirmed that the decryptors are legitimate and working after testing one of them against files encrypted in a recent AstroLocker campaign.

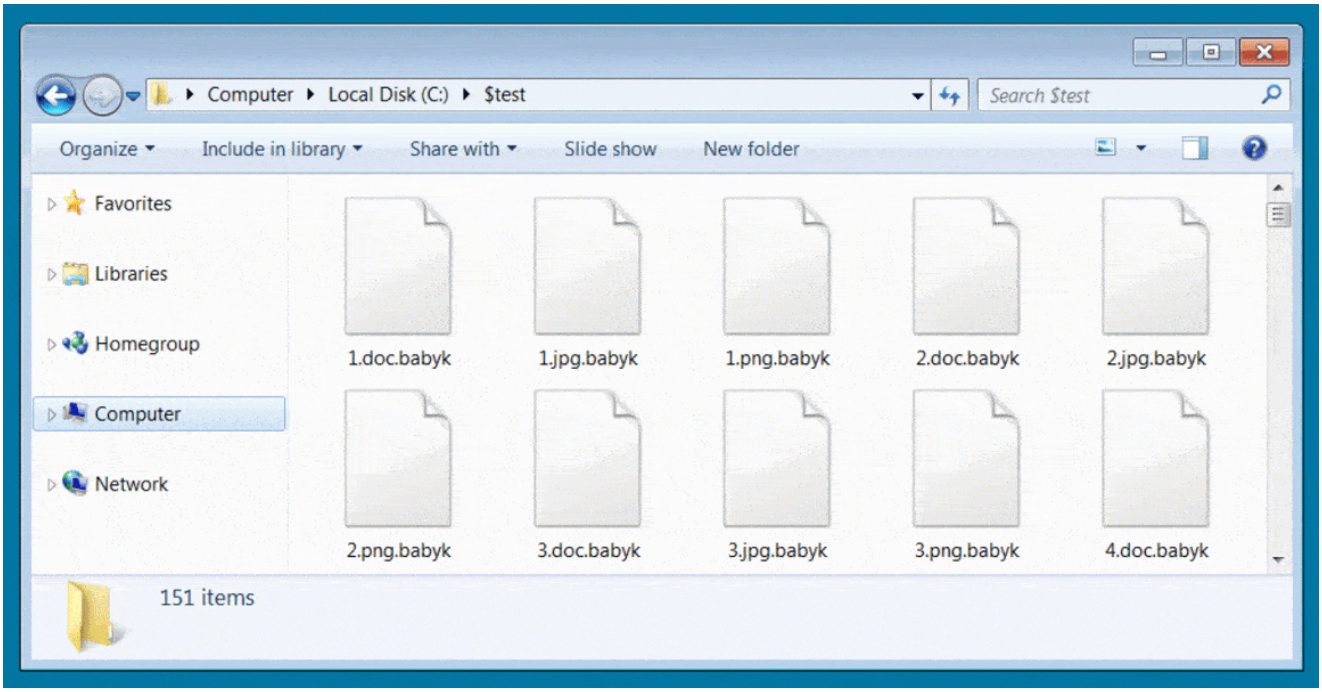
While we only tested one decryptor that successfully decrypted files locked in one campaign, other decryptors in the archive are likely designed to decrypt files encrypted in previous campaigns.



AstraLocker decryptors (BleepingComputer)

"It was fun, and fun things always end sometime. I'm closing the operation, decryptors are in zip files, clean. I will come back," AstraLocker's developer said. "I'm done with ransomware for now. I'm going in cryptojaking lol."

While the developer did not reveal the reason behind the AstraLocker shutdown, it's likely due to the sudden publicity brought by recent reports that would land the operation in law enforcement's crosshairs.



AstraLocker decryption demo (BleepingComputer)

A universal decryptor for AstraLocker ransomware is currently in the works, to be released in the future by Emsisoft, a software company known for helping ransomware victims with data decryption.

While it doesn't happen as often as we'd like, other ransomware groups have released decryption keys and decryptors to BleepingComputer and security researchers as a gesture of goodwill when shutting down or releasing new versions.

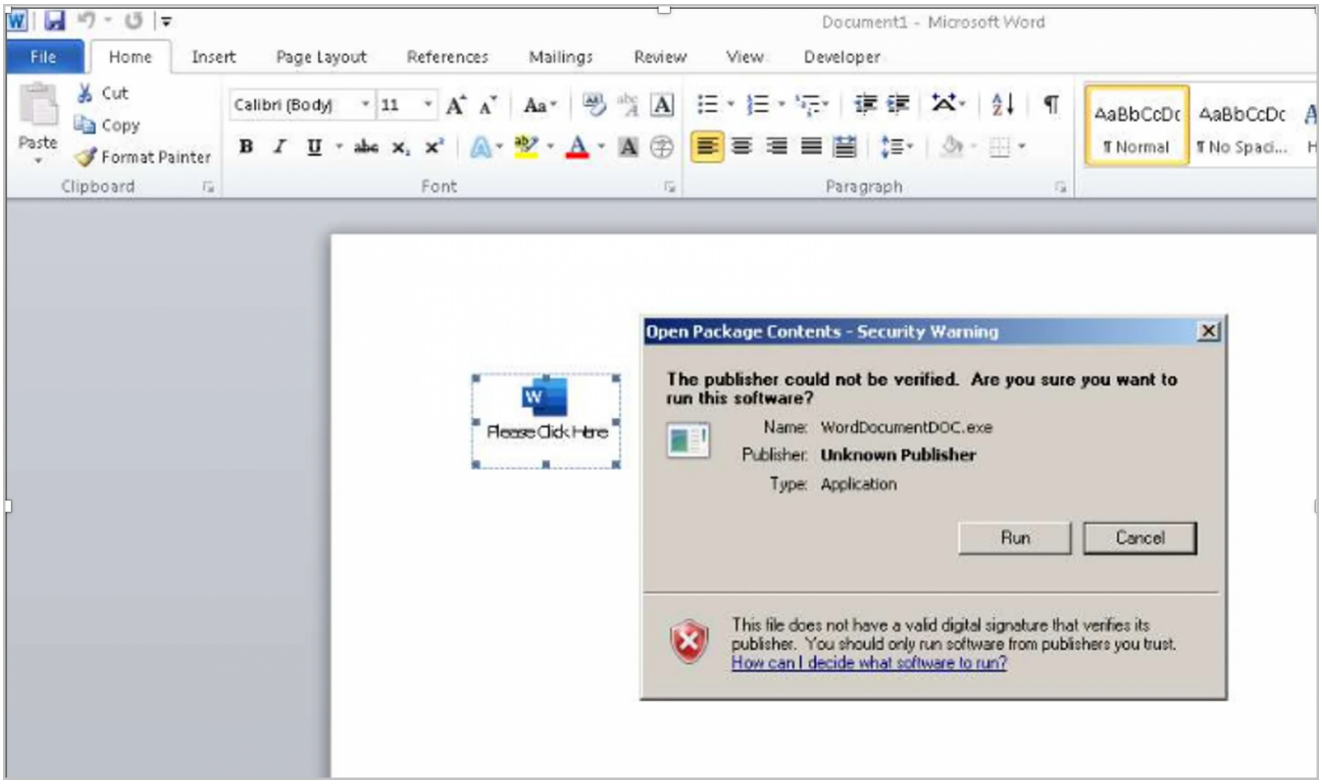
The list of decryption tools released in the past includes Avaddon, Ragnarok, SynAck, TeslaCrypt, Crysis, AES-NI, Shade, FilesLocker, Ziggy, and FonixLocker.

AstraLocker ransomware background

As threat intelligence firm ReversingLabs recently revealed, AstraLocker used a somewhat unorthodox method of encrypting its victims' devices compared to other ransomware strains.

Instead of first compromising the device (either by hacking it or buying access from other threat actors), AstraLocker's operator would directly deploy the payloads from email attachments using malicious Microsoft Word documents.

The lures used in AstroLocker attacks are documents hiding an OLE object with the ransomware payload that will get deployed after the target clicks Run in the warning dialog displayed when opening the document.



AstraLocker ransom note (ReversingLabs)

Before encrypting files on the now-compromised device, the ransomware will check if it's running in a virtual machine, kill processes and stop backup and AV services that would hinder the encryption process.

Based on ReversingLabs' analysis, AstraLocker is based on the leaked Babuk Locker (Babyk) ransomware source code, a buggy but still dangerous strain that exited the space in September 2021.

Additionally, one of the Monero wallet addresses in AstraLocker's ransom note was also linked to the operators of Chaos ransomware.

Related Articles:

No More Ransom helps millions of ransomware victims in 6 years

Free decryptor released for AstraLocker, Yashma ransomware victims

AstraLocker 2.0 infects users directly from Word attachments

BlackByte ransomware gang is back with new extortion tactics

Hackers attack UK water supplier but extort wrong company