

Avaddon ransomware shuts down and releases decryption keys

By Lawrence Abrams

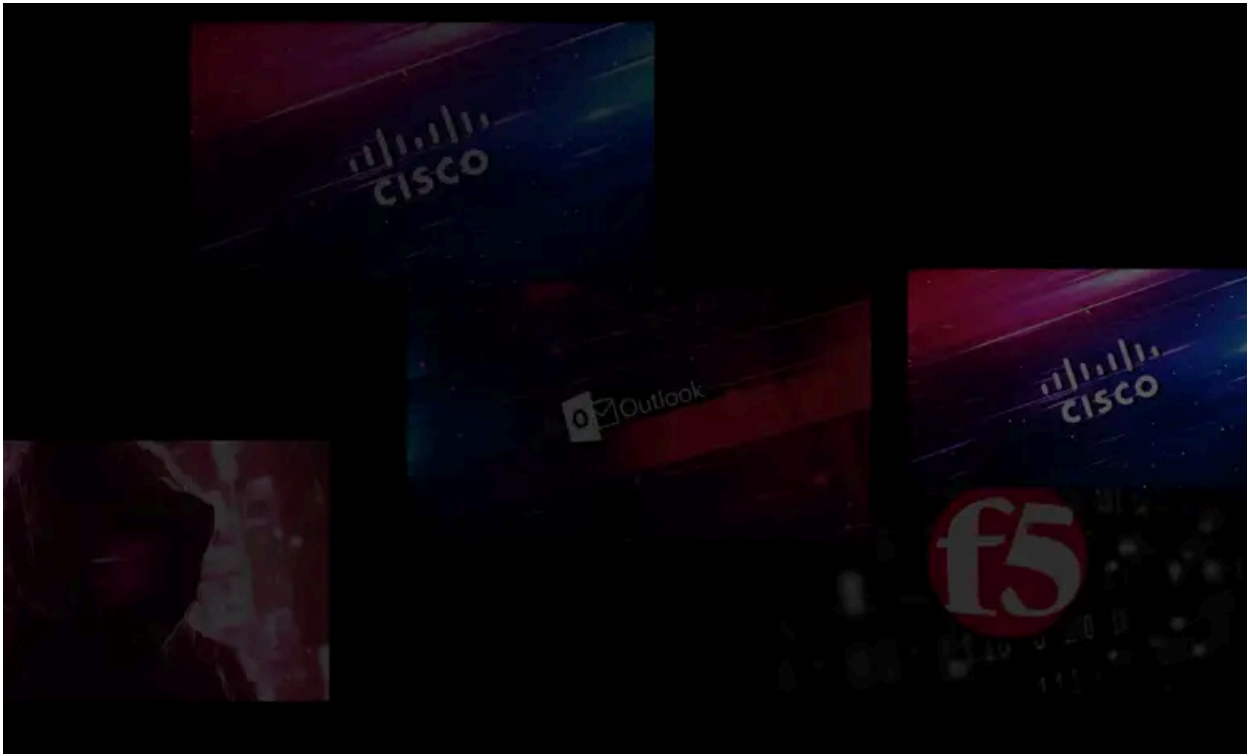
Published: 2021-06-11 · Archived: 2026-04-02 12:28:19 UTC



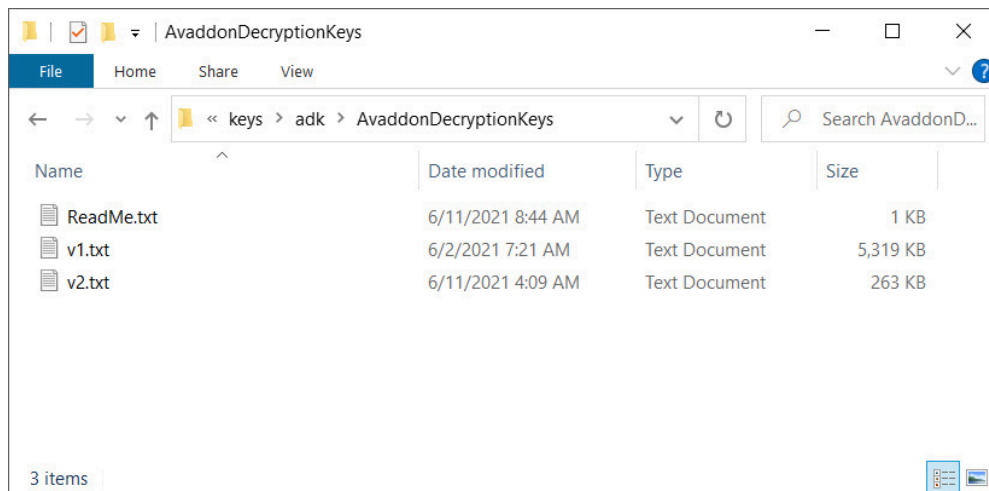
The Avaddon ransomware gang has shut down operation and released the decryption keys for their victims to [BleepingComputer.com](https://www.bleepingcomputer.com).

This morning, BleepingComputer received an anonymous tip pretending to be from the FBI that contained a password and a link to a password-protected ZIP file.

This file claimed to be the "Decryption Keys Ransomware Avaddon," and contained the three files shown below.



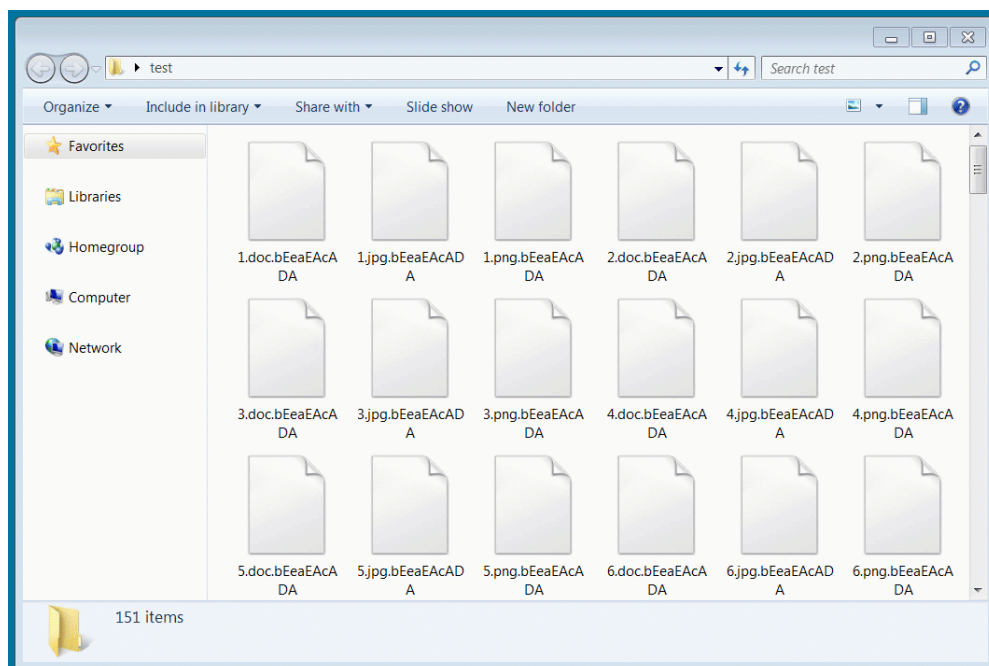
Visit Advertiser website [GO TO PAGE](#)



Avaddon decryption keys shared with BleepingComputer

After sharing the files with [Fabian Wosar](#) of Emsisoft and [Michael Gillespie](#) of Coveware, they confirmed that the keys are legitimate.

Using a test decryptor shared with BleepingComputer by [Emsisoft](#), I decrypted a virtual machine encrypted today with a recent sample of Avaddon.



Decrypting Avaddon encrypted files with released keys

In total, the threat actors sent us 2,934 decryption keys, where each key corresponds to a specific victim.

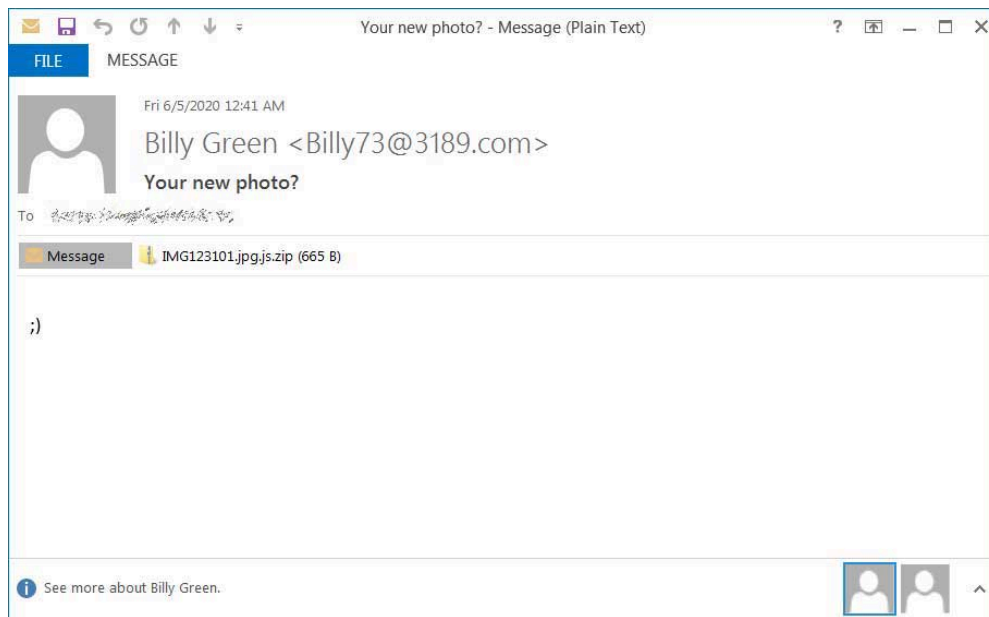
Emsisoft has [released a free decryptor](#) that all victims can use to recover their files for free.

While it doesn't happen often enough, ransomware groups have previously released decryption keys to BleepingComputer and other researchers as a gesture of goodwill when they shut down or release a new version.

In the past, decryption keys have been released for [TeslaCrypt](#), [Crysis](#), [AES-NI](#), [Shade](#), [FilesLocker](#), [Ziggy](#), and [FonixLocker](#).

Avaddon shuts down ransomware operation

Avaddon [launched its operation in June 2020](#) through a phishing campaign that contained a winking smiley, shown below.



Avaddon phishing email

Over time, Avaddon has grown into one of the larger ransomware operations, with the FBI and Australian [law enforcement recently releasing advisories](#) related to the group.

At this time, all of Avaddon's Tor sites are inaccessible, indicating that the ransomware operation has likely shut down.

Furthermore, ransomware negotiation firms and incident responders saw a mad rush by Avaddon over the past few days to finalize ransom payments from existing unpaid victims.

Coveware CEO [Bill Siegel](#) has told BleepingComputer that Avaddon's average ransom demand was around \$600k.

However, over the past few days, Avaddon has been pressuring victims to pay and accepting the last counteroffer without any push back, which Siegel states is abnormal.

It is not clear why Avaddon shut down, but it was likely caused by the increased pressure and scrutiny by law enforcement and governments worldwide after recent attacks against critical infrastructure.

"The recent actions by law enforcement have made some threat actors nervous: this is the result. One down, and let's hope some others go down too," Emsisoft threat analyst Brett Callow told BleepingComputer.

With the recent attacks against [Colonial Pipeline](#) and [JBS](#), ransomware has become a priority of the US government.

As most of the larger ransomware operations are believed to be operated within Russia or other CIS countries, President Biden will be discussing these recent ransomware attacks with Russian President Vladimir Putin at the June 16 Geneva summit.

Update 6/11/21: Added link to free Avaddon decryptor.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/>