Free decryptor released for TrickBot gang's Diavol ransomware

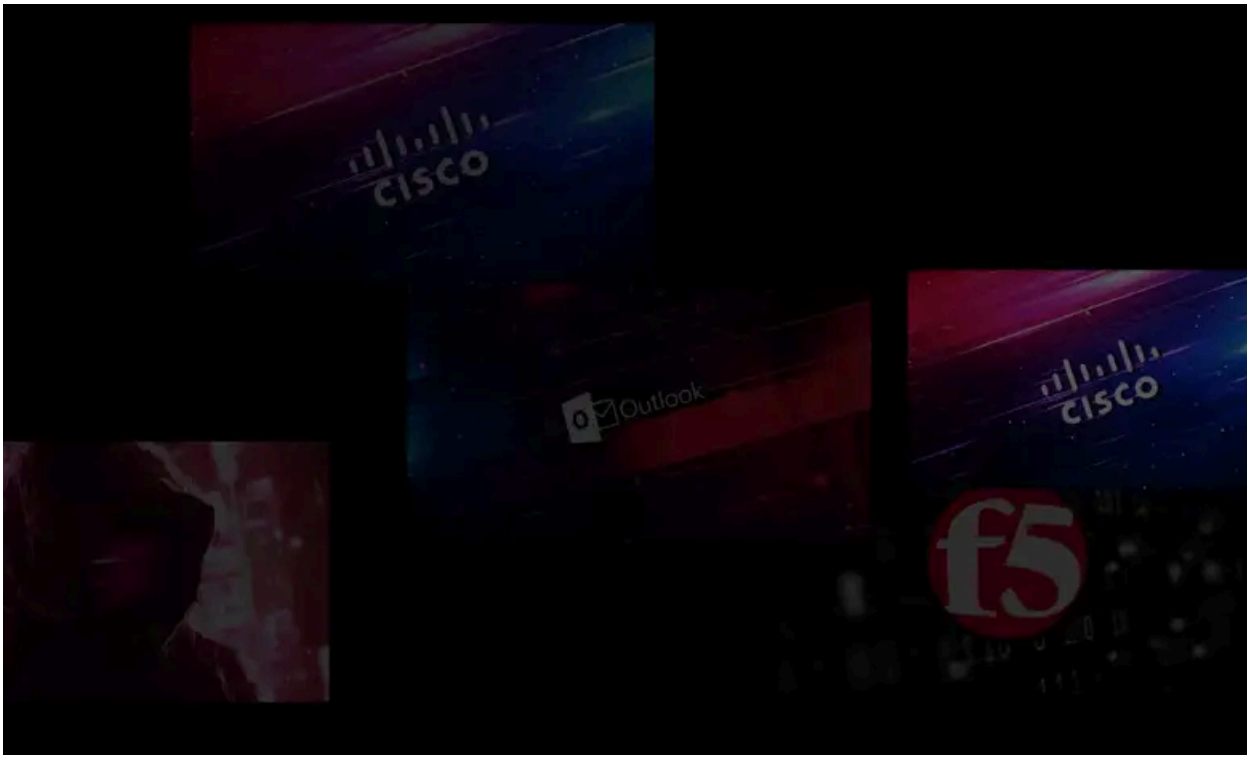
By Sergiu Gatlan

Published: 2022-03-18 · Archived: 2026-04-02 12:40:48 UTC

Cybersecurity firm Emsisoft has released a free decryption tool to help Diavol ransomware victims recover their files without paying a ransom.

Diavol ransomware victims can download the free tool from Emsisoft's servers to decrypt their data using detailed instructions available in this usage guide [PDF].

"The decryptor requires access to a file pair consisting of one encrypted file and the original, unencrypted version of the encrypted file to reconstruct the encryption keys needed to decrypt the rest of your data," Emsisoft explains.


cisco
Outlook
cisco
f5

"By default, the decryptor will pre-populate the locations to decrypt with the currently connected drives and network drives."

This Diavol ransomware decryption tool will keep the files encrypted in the attack as a failsafe if the decrypted files are not identical to the original documents.

Additionally, it comes with an "Allow partial decryption of large files," needed to partially recover some files larger than the pair of files provided for reconstructing the encryption keys. This is required because the decryptor might fail to recover such files due to technical limitations.

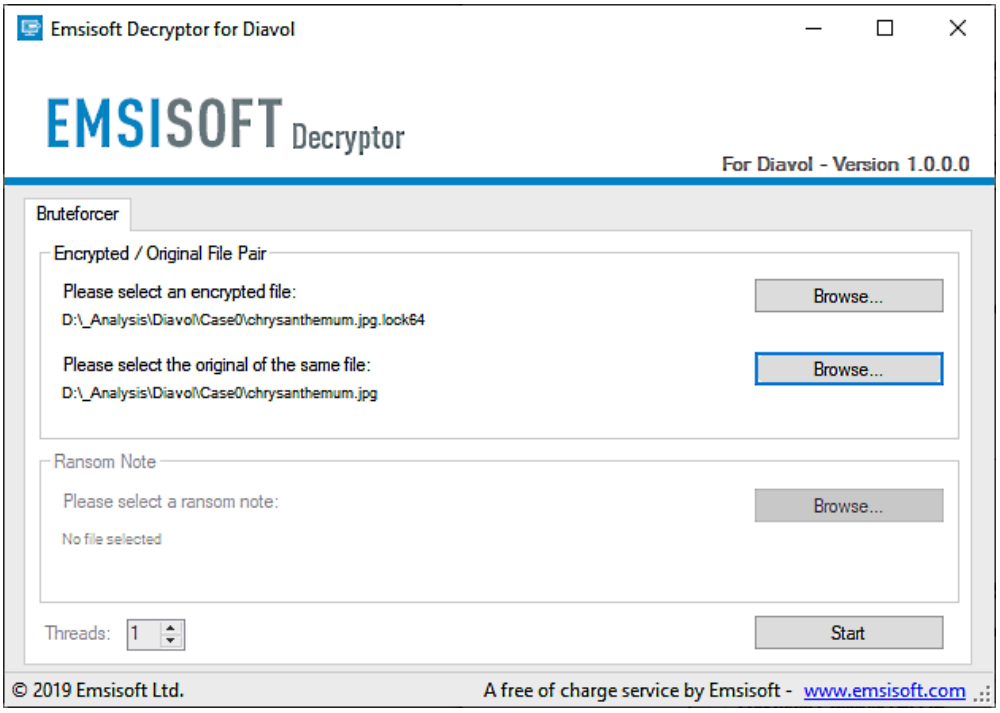


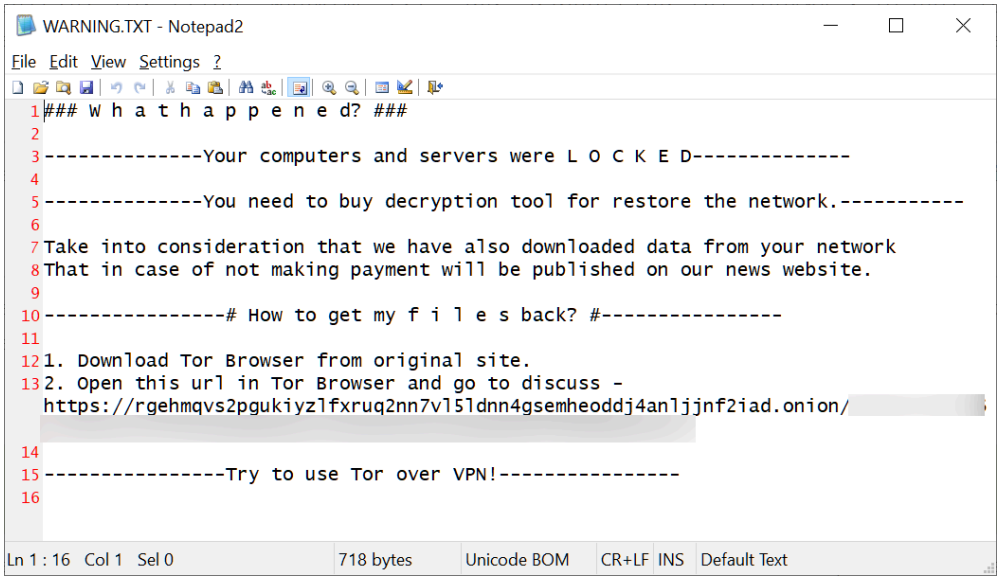
Image: Emsisoft

Unlike other ransomware families that use symmetric algorithms to speed up the encryption process significantly, Diavol's encryption procedure employs user-mode Asynchronous Procedure Calls (APCs) with an asymmetric encryption algorithm.

Diavol also comes with no obfuscation as it doesn't use packing or anti-disassembly tricks, but it still hinders analysis efforts by storing its main routines within bitmap images.

Before the encryption process is done, Diavol will change encrypted Windows devices' backgrounds to a black wallpaper with an "All your files are encrypted! For more information see README-FOR-DECRYPT.txt" message.

Notably, while the Diavol ransomware originally created ransom notes named README_FOR_DECRYPT.txt, as the FBI pointed out, BleepingComputer has seen a switch in November to ransom notes named Warning.txt.



Diavol ransom note (BleepingComputer)

FortiGuard Labs security researchers first tied this ransomware strain to the TrickBot gang (aka Wizard Spider) after spotting it deployed on different systems together with Conti ransomware payloads in an attack blocked by the company's EDR solution in early June 2021.

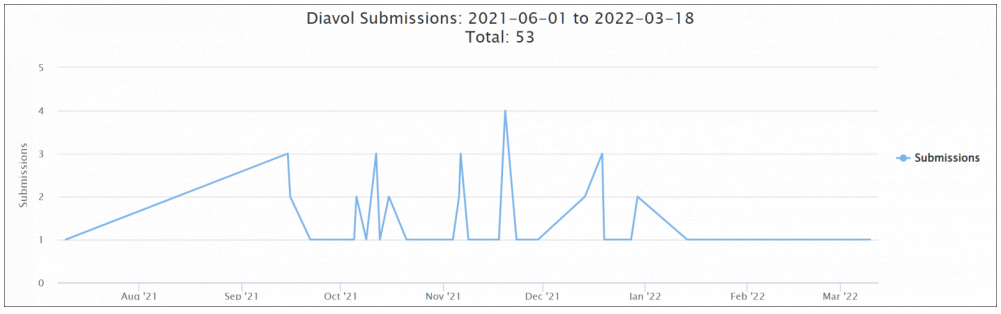
Following their report and likely after the arrest of Alla Witte, who was involved in ransomware development for the malware gang, the FBI also formally linked it to the TrickBot cybercrime gang.

This Russian-based financially motivated cybercrime group operates the Trickbot botnet used to drop second-stage malware on compromised systems and networks.

The FBI first learned of the ransomware strain in October 2021, and, since then, it has seen ransom demands between $10,000 and $500,000, with lower payments accepted following ransom negotiations.

These ransoms are in stark contrast to the massive ransoms demanded by other ransomware gangs linked to TrickBot, including Conti and Ryuk. They have historically requested multi-million dollar payments for decryptors and not leaking stolen data online.

Although active since at least June 2021, Diavol ransomware has never been very active and has only a few dozen submissions on the ID-Ransomware service.



Diavol ransomware activity (BleepingComputer/ID-Ransomware)

Source: https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-trickbot-gangs-diavol-ransomware/