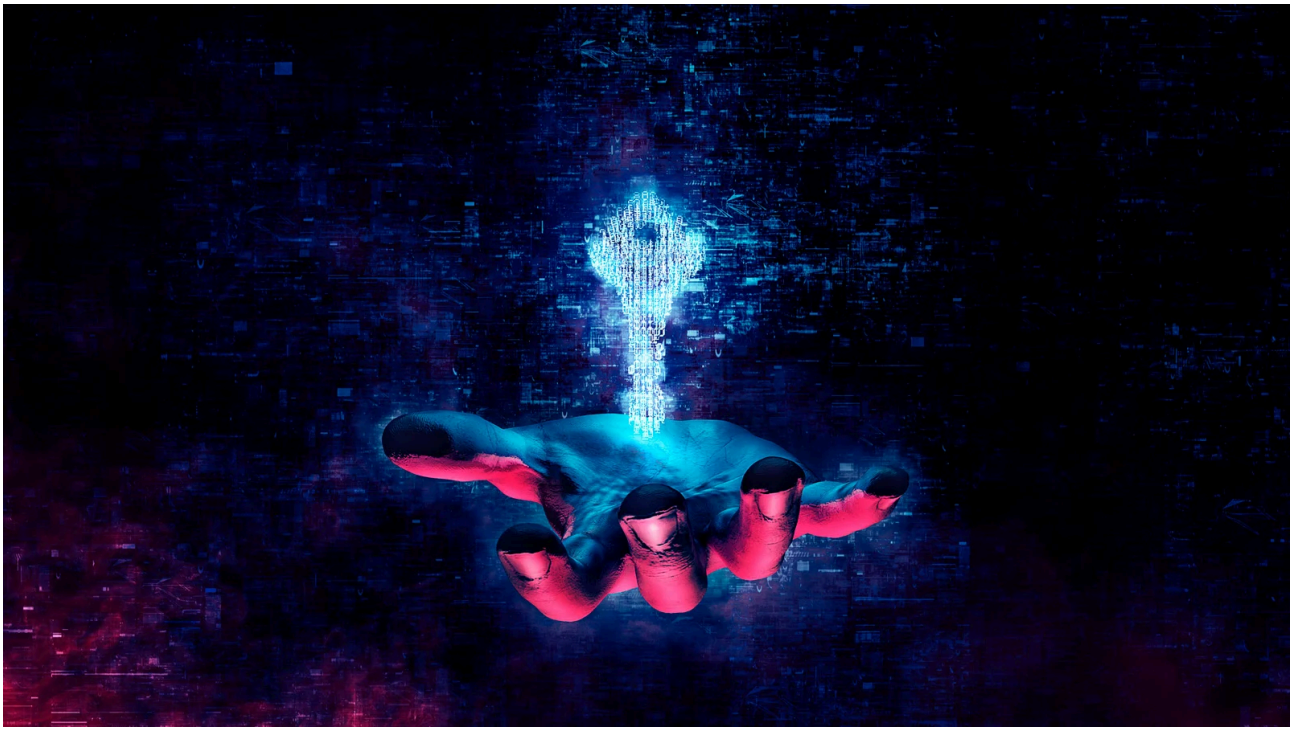
Bitdefender releases free MegaCortex ransomware decryptor

By Bill Toulas

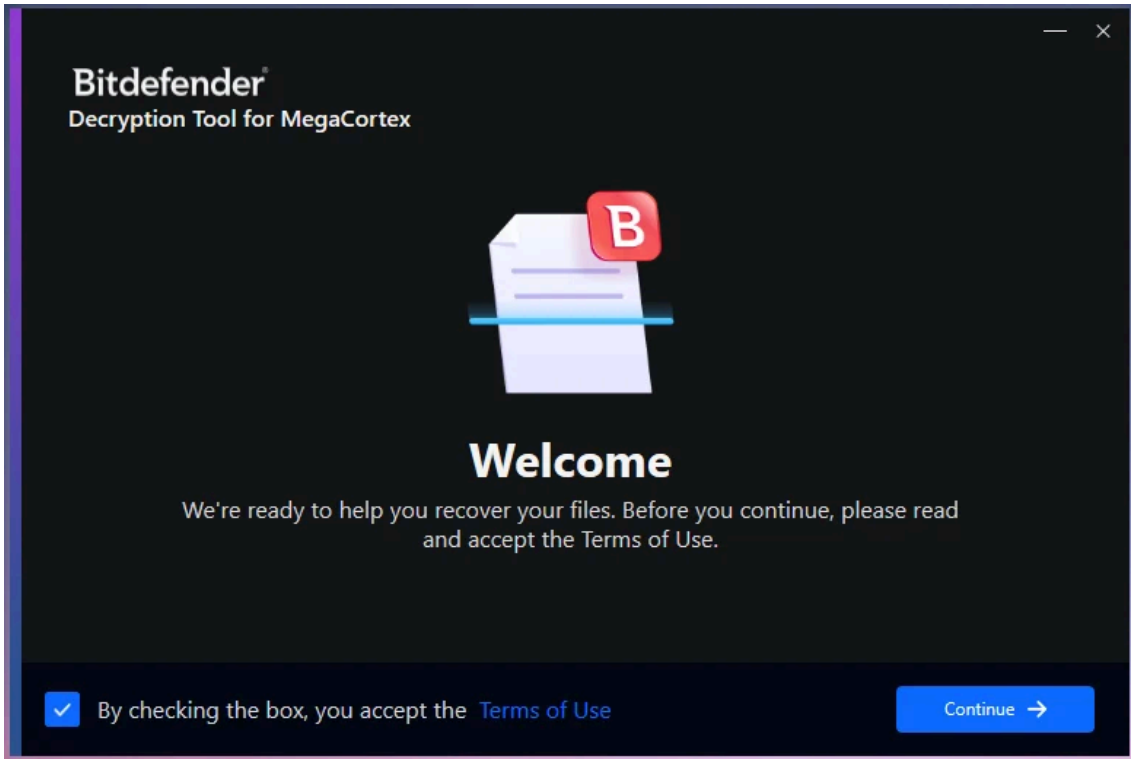
Published: 2023-01-05 · Archived: 2026-04-10 02:49:43 UTC



Antivirus company Bitdefender has released a decryptor for the MegaCortex ransomware family, making it possible for victims of the once notorious gang to restore their data for free.

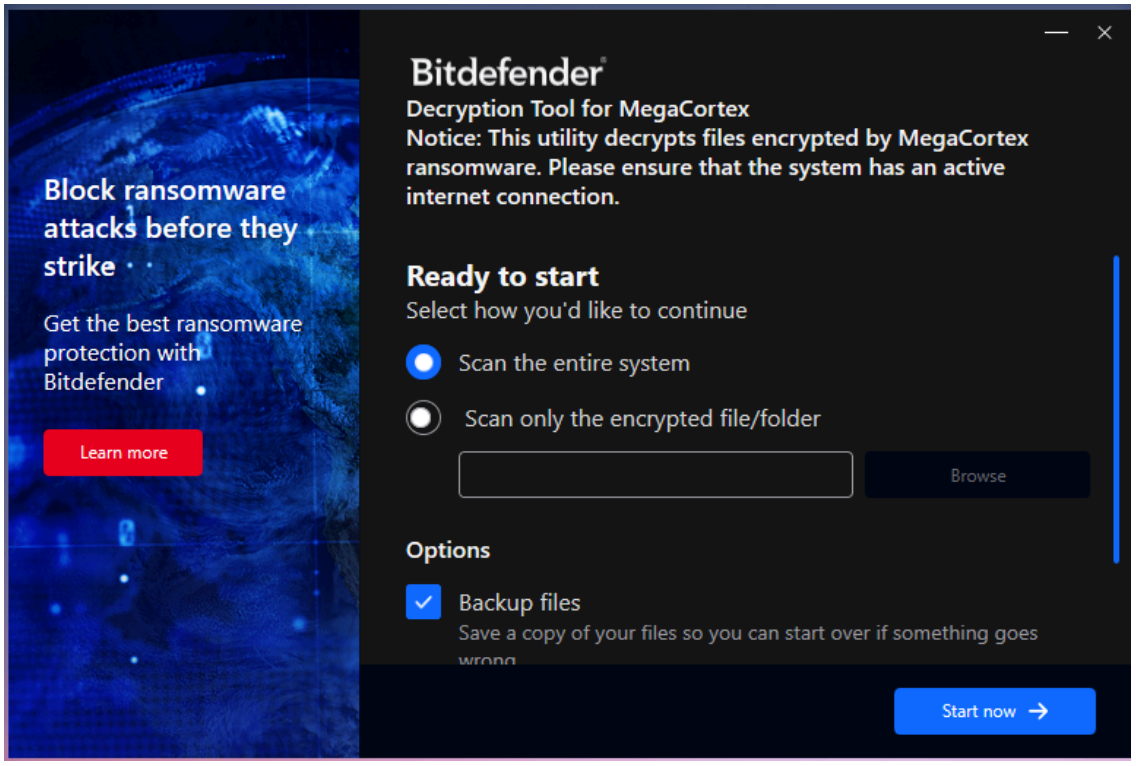
The creation of the decryptor was the combined work of Bitdefender analysts and experts from Europol, the NoMoreRansom Project, and the Zürich Public Prosecutor's Office and Cantonal Police.

Using the decryptor is pretty straightforward, as it's a standalone executable that doesn't require installation and offers to locate encrypted files on the system automatically.



Decryptor's welcome screen *(BleepingComputer)*

Moreover, the decryptor can back up the encrypted files for safety in case something goes wrong in the decryption process that could corrupt the files beyond recovery.



Decryptor's options *(BleepingComputer)*

Also, for those who attempted to decrypt their files previously with mixed success, the new decryptor offers an advanced setting to replace them with clean files.

You may download the tool from this page and read the user manual for more details on using Bitdefender's MegaCortex decryptor.

MegaCortex's rise and fall

The MegaCortex ransomware was first discovered by Sophos researchers in May 2019, who observed it targeting corporate networks and found along with QBot, Emotet, and Cobalt Strike.

Samples captured in July 2019 revealed that MegaCortex operators were launching more targeted attacks, adjusting the ransom demands according to the victim size and using particularly threatening language.

In November 2019, MegaCortex operators started engaging in double extortion tactics, threatening the victims with the publication of their data if they didn't meet their demands.

By the end of that month, the Dutch National Cyber Security Centre placed MegaCortex among the most active ransomware operations in the cybercrime underground.

In December 2019, the FBI warned organizations about the threat of MegaCortex, describing the intrusion methods used by the threat group and providing defense tips and mitigation recommendations.

Throughout 2020, the activity of MegaCortex waned, and there weren't many victims affected by this particular strain.

In October 2021, Europol announced the arrest of 12 individuals responsible for 1,800 ransomware attacks in 71 countries, many of which deployed the MegaCortex and LockerGoga strains.

This arrest ultimately led to the release of a free LockerGoga ransomware decryptor by BitDefender in September after the authorities discovered private keys used in attacks.

"This analysis revealed numerous private keys from ransomware attacks. These keys enable damaged companies and institutions to restore data previously encrypted with the "LockerGoga" or "MegaCortex" malware," stated a coordinated announcement by the Zürich Public Prosecutor's Office.

While BitDefender has not stated how they obtained the private keys for today's MegaCortex decryptor, it was likely created with master keys found by the Zurich authorities.

Source: https://www.bleepingcomputer.com/news/security/bitdefender-releases-free-megacortex-ransomware-decryptor/