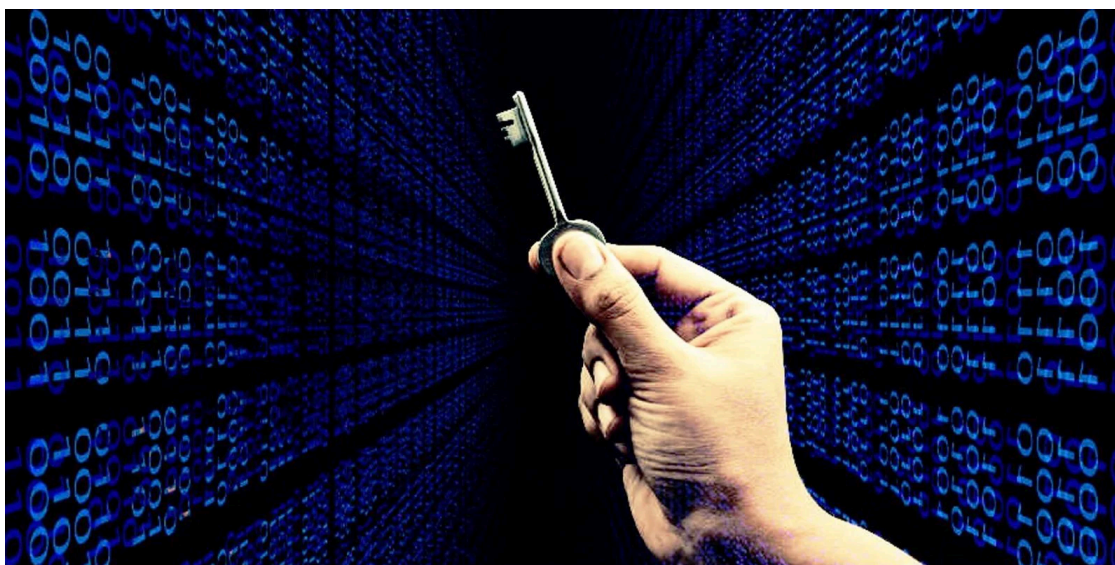


## Bitdefender releases free decryptor for LockerGoga ransomware

By Bill Toulas

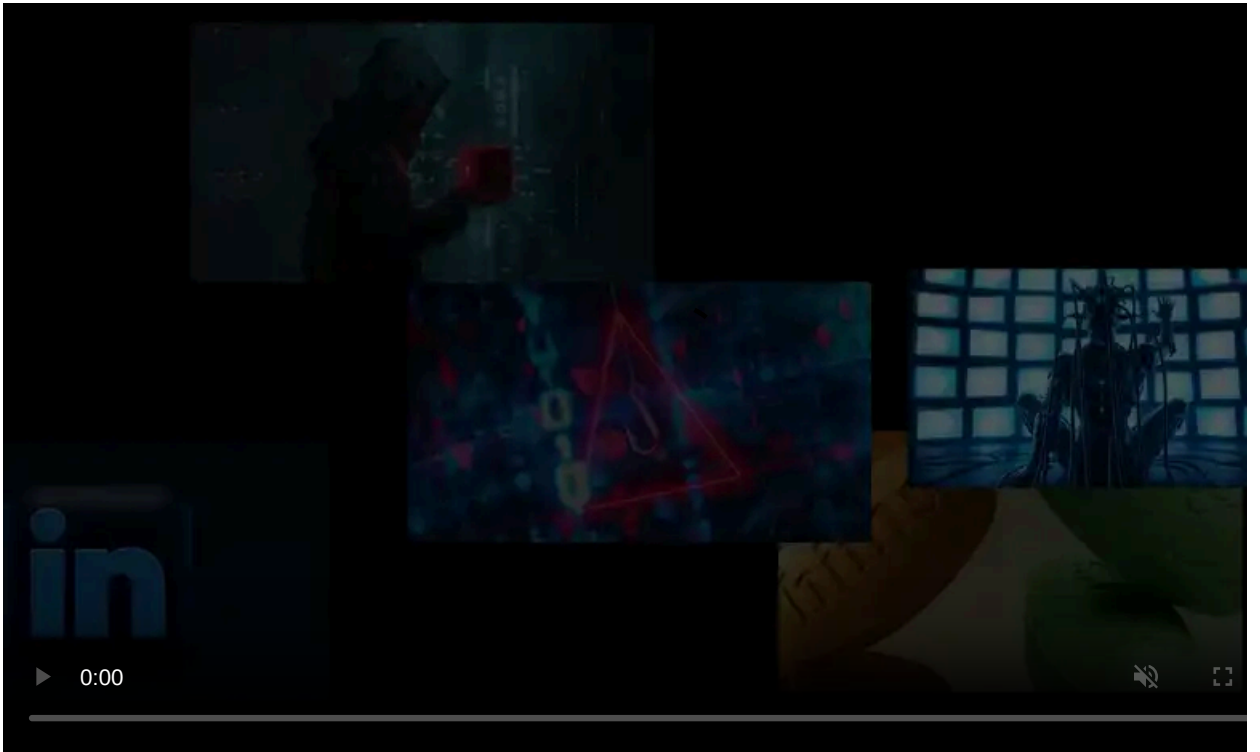
Published: 2022-09-16 · Archived: 2026-04-05 17:23:32 UTC



Romanian cybersecurity firm Bitdefender has released a free decryptor to help LockerGoga ransomware victims recover their files without paying a ransom.

The free tool is available for download from [Bitdefender's servers](#) and allows you to recover encrypted files using instructions in this usage guide [\[PDF\]](#).

Bitdefender says the decryptor was developed in cooperation with law enforcement agencies, including Europol, the NoMoreRansom Project, the Zürich Public Prosecutor's Office, and the Zürich Cantonal Police.



Visit Advertiser website [GO TO PAGE](#)

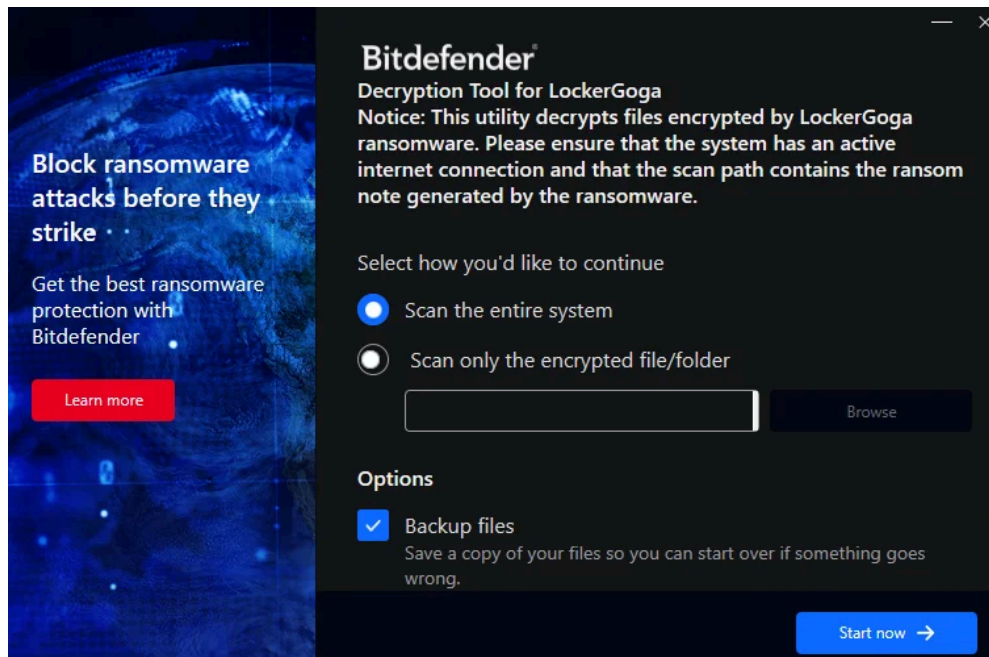
For a working decryptor to be created, researchers usually need to identify a flaw in the cryptography used by the ransomware encryptor.

However, in this case, the LockerGoga operators were [arrested in October 2021](#), which may have allowed law enforcement to access the master private keys used to decrypt victims' encryption keys.

## How to decrypt your files

Files encrypted by LockerGoga will have the ".locked" filename extension and cannot be opened with regular software.

Bitdefender's tool offers to scan your entire filesystem or a single folder, locate any encrypted files, and perform the decryption automatically.



**Bitdefender's LockerGoga decryptor**

For this to work, the computer needs to be connected to the internet, and the ransom notes generated by the ransomware during the encryption need to be in the original paths.

Bitdefender says the decryptor can operate either on a single machine or on entire networks encrypted by LockerGoga.

Note that the decryption process can be interrupted or not always work as expected, and you might end up with corrupted files. For this reason, the decryptor has the "backup files" option ticked by default, and users are recommended to leave that setting enabled.

## Who was LockerGoga

The LockerGoga ransomware operation launched in January 2019, hitting high-profile targets such as the French engineering firm [Altran Technologies](#) and the Norwegian aluminum giant [Norsk Hydro](#).

Together with Ryuk and MegaCortex, LockerGoga was involved in ransomware attacks against at least [1,800 organizations](#) worldwide.

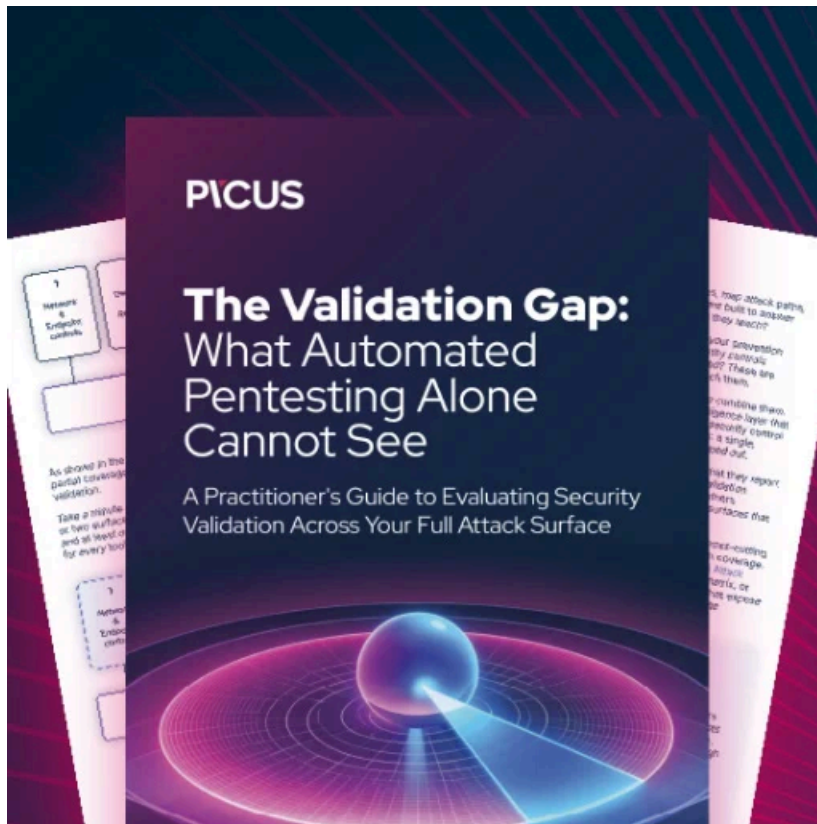
In October 2021, [twelve individuals were arrested](#) in an international law enforcement operation for deploying various ransomware strains, including LockerGoga.

"Its operator, who has been detained since October 2021 pending trial, is part of a larger cybercrime ring that used LockerGoga and MegaCortex ransomware to infect more than 1,800 persons and institutions in 71 countries to cause an

estimated damage of \$US 104 million," Bitdefender explains in the decryptor announcement.

Since the operator's arrest, threat actors have ceased using the LockerGoga ransomware, and the ransomware's source code was never released.

Therefore, this decryptor will mostly be for past victims who refused to pay the ransom and have been waiting to recover their files for free.



### **[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/bitdefender-releases-free-decryptor-for-lockergoga-ransomware/>