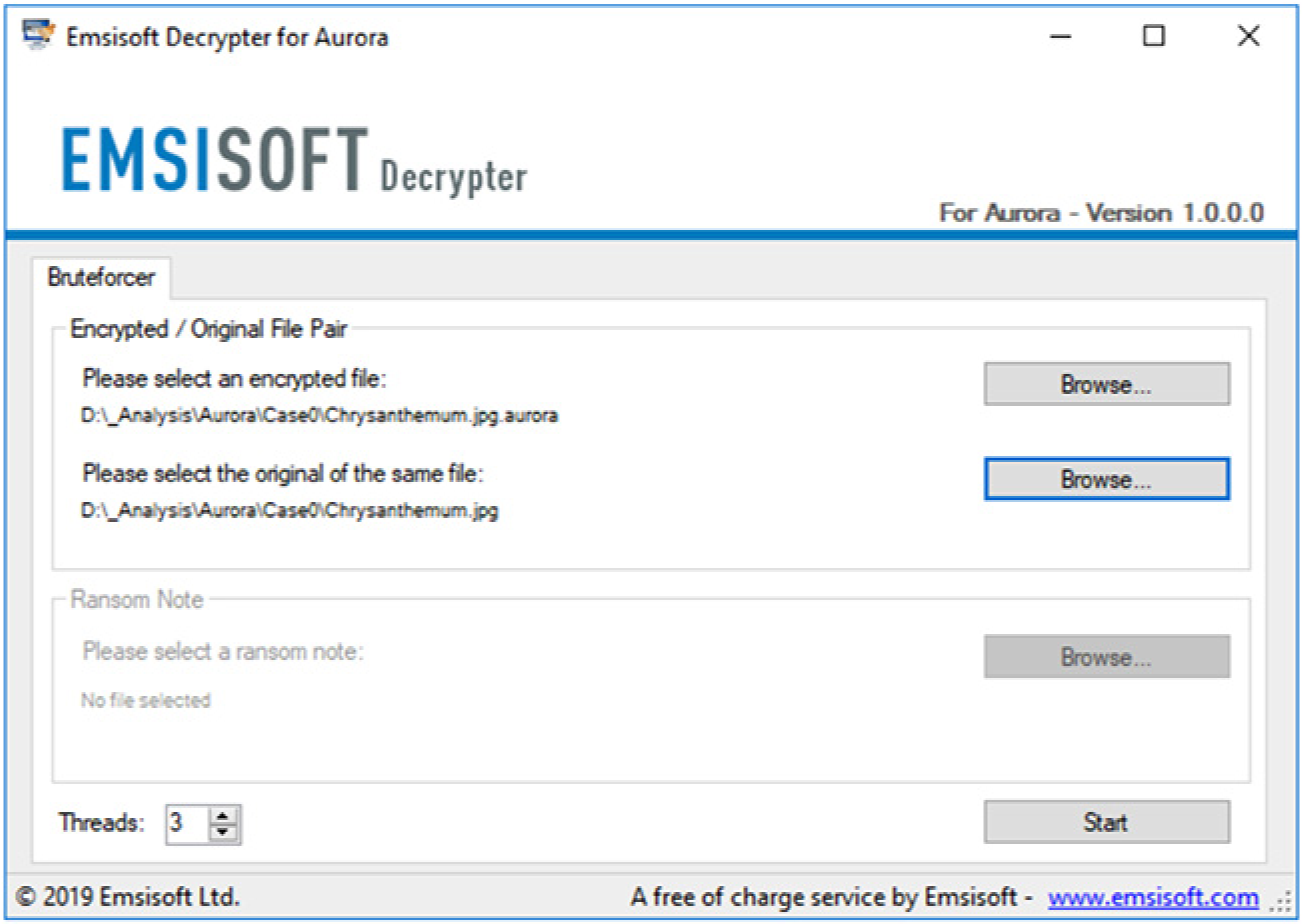
A LockerGoga primer and decrypters for Mira and Aurora ransomwares

helpnetsecurity.com/2019/04/02/aurora-decrypter-mira-decrypter/

April 2, 2019

There’s some good news for victims of the Mira and Aurora ransomwares: free decrypters have been made available.



New decrypters

F-Secure has released a decrypter for victims of the **Mira ransomware**. (You'll known you've been hit if the encrypted files sport the *.mira* extension.)

"Most often, decryption can be very challenging because of missing keys that are needed for decryption. However, in the case of Mira ransomware, it appends all information required to decrypt an encrypted file into the encrypted file itself," the company explained.

The tool can be found here, and instructions on how to use it here.

Before running the tool, users need to remove the ransomware from the computer, lest it encrypt the decrypted files again.

"It is important to run the tool on the specific computer where the files were originally encrypted. This is because the recovery key for each files are calculated from the computer where the files got encrypted," the company added.

Emsisoft has released a decrypter for victims of the **Aurora ransomware**, aka Zorro, Desu, or AnimusLocker. (You'll known you've been hit if the encrypted files sport the *.Aurora*, *.aurora*, *.animus*, *.ONI*, *.Nano*, *.desu* or *.cryptoid* extension.)

By the by, Michael Gillespie, security researcher and the creator of ID Ransomware, the online tool that ransomware victims can use to identify the specific malware they've been hit with, has also released a decrypter for the Aurora ransomware earlier this year.

About LockerGoga

Unlike Mira and Aurora, the LockerGoga ransomware seems to have been flinged at specific, high-profile targets.

The name became widely known after the recent Norsk Hydro attack. The company did not name the ransomware that hit them, but the Norwegian National Security Authority confirmed it is LockerGoga.

The Center for Internet Security has released a primer containing the most current information about the ransomware and known indicators of compromise.

"LockerGoga reportedly targets other sectors, although a disproportionate amount of victims reside in the industrial/manufacturing sector," the organization pointed out. Known recent victims include French engineering consulting firm Altran and U.S. chemical companies Hexion and MPM Holdings (Momentive).

At this time, the initial intrusion vector is unknown, they say, but it seems that the ransomware is unable to spread itself to other computers on the network.

They also pointed out that, in some cases, the victims won't even be able to tell they've been targeted with this specific malware.

"Cisco's Talos group observed that some LockerGoga variants forcibly log victims off their devices. They are then unable to log back onto the device, which also means they may not see the ransom note. Furthermore, in some cases the network interface on each system was disabled and the local user account passwords were changed. This can cause confusion on the victim's end as to their issue's root cause," they noted.

"If this is an intentional feature, then it is possible that the CTAs have both financial and destructive motivations."

Their advice for organizations is to make regular backups of their important files and make sure that they are able to recover from them.