27.07.2020, 08:00 CEST

PRESS RELEASE – UNDER EMBARGO

No More Ransom: how 4 million victims of ransomware have fought back against hackers

While the world is in the grip of a coronavirus outbreak, another virus is quietly wreaking havoc. Although this virus has been around for years, its cases have been rising alarmingly in the past few months and has brought critical activities such as hospitals and governments to a standstill. This virus is ransomware, but a free scheme called No More Ransom is helping victims fight back without paying the hackers.

Celebrating its fourth anniversary this month, the No More Ransom decryption tool repository has registered since its launch over 4.2 million visitors from 188 countries and has stopped an estimated $ 632 million in ransom demands from ending up in criminals' pockets.

Powered by the contributions of its 163 partners, the portal has added 28 tools in the past year and can now decrypt 140 different types of ransomware infections. The portal is available in 36 languages.

You can consult all the key figures in our dedicated infographic: No More Ransom

How No More Ransom works

No More Ransom is the first public-private partnership of its kind helping victims of ransomware recover their encrypted data without having to pay the ransom amount to cybercriminals.

To do this, simply go to the website nomoreransom.org and follow the Crypto Sheriff steps to help identify the ransomware strain affecting the device. If a solution is available, a link will be provided to download for free the decryption tool.

Prevention remains the best cure

No More Ransom goes a long way to help people impacted by ransomware, but there are still many types of ransomware out there without a fix. Fortunately, there are some preventative steps you can take to protect yourself from ransomware:

- Always keep a copy of your most important files somewhere else: in the cloud, on another drive offline, on a memory stick, or on another computer.
- Use reliable and up-to-date anti-virus software.
- Do not download programs from suspicious sources.
- Do not open attachments in e-mails from unknown senders, even if they look important and credible.
- And if you are a victim, do not pay the ransom!

Do you have an innovative solution for ransomware families not covered yet in the portal to help victims recover their files without giving into the demands of the criminals? Then we want to hear from you.