NO MORE RANSOM – DO YOU NEED HELP UNLOCKING YOUR DIGITAL LIFE?

Public awareness and prevention

Would like to learn more? Download the No More Ransom flyer and visit www.nomoreransom.org .

Ransomware is a type of malware that locks the victims' computer or encrypts their data, demanding them to pay a ransom in order to regain control over the affected device or files. It's a top threat for EU citizens and one of the top priorities for law enforcement.

No More Ransom (NMR) is an initiative by Europol's European Cybercrime Centre, the National High Tech Crime Unit of the Netherlands' police and McAfee to help victims of ransomware retrieve their encrypted data without having to pay to the criminals. NMR showcases the value of public-private cooperation in disrupting criminal businesses with ransomware connections. Victims should no longer be forced to either pay a ransom or lose their files. By restoring access to their infected systems free of charge, we provide users with a third choice they did not have before.

Launched in July 2016, the free resources have assisted more than 6 million people, growing up to over 170 supporting partners from law enforcement, private sector and academia. The resources are available in 37 different languages, and it counts with more than 120 tools capable of decrypting over 150 different types of ransomware.

HOW DOES IT WORK?

1. The victim uploads two encrypted files and the ransomware note to the NMR Crypto Sheriff.
2. The Crypto Sheriff matches the information against a list of available decryption tools.
3. If there is a positive hit, the link to the tools is provided. The victim only needs to follow the instructions to unlock their files.
4. If no tool is available at the moment, the victim is advised to continue checking in the future, as new tools are added on a regular basis.

HOW TO AVOID BECOMING INFECTED BY RANSOMWARE?

Ransomware attacks often start with:

- Phishing
- Vulnerable software
- Publicly available personal information
- Public Wi-Fi networks

Visitors can also find information on what ransomware is, how it works and, most importantly, how to protect themselves. Awareness is key as there are no decryption tools for all existing types of malware available to this day.

- Regularly back up data stored on your computer. Keep at least one copy offline.
- Do not click on links in unexpected or suspicious emails.
- Browse and download only official versions of software and always from trusted websites.
- Use robust security products to protect your system from all threats, including ransomware.
- Ensure that your security software and operating system are up-to-date.
- Be wary while browsing the internet and do not click on suspicious links, pop-ups or dialogue boxes.
- Do not use high privilege accounts (accounts with administrator rights) for daily business.

INFECTED… WHAT TO DO NEXT?

- Always visit www.nomoreransom.org to check whether you have been infected with one of the ransomware variants for which there are decryption tools available free of charge.
- Don't pay the ransom. You will be financing criminals and encouraging them to continue their illegal activities.
- Report it to your national police. The more information you provide, the more effectively law enforcement can disrupt the criminal enterprise.

CRIME AREAS: Cybercrime
TARGET GROUPS: General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
ENTITIES: European Cybercrime Center (EC3)