No More Ransom: new partners, new decryption tools, new languages to better fight ransomware

The global fight against ransomware continues tirelessly as the No More Ransom (NMR) project welcomes more than 30 new partners from both the public and private sectors. With more partners joining the fight, more decryption tools become available, offering new possibilities to victims of ransomware.

No More Ransom was launched in July 2016 by the Dutch National Police, Europol, Intel Security and Kaspersky Lab, introducing a new level of cooperation between law enforcement and the private sector to fight ransomware together. On www.nomoreransom.org users can find information on what ransomware is and how to protect themselves and, equally important, victims can find tools to help them decrypt their blocked devices for free.

In order to better assist victims from all over the world, the online portal is now available not only in English, but also in Dutch, French, Italian, Portuguese and Russian. Translations into yet more languages are currently ongoing, and their implementation will follow very soon.

Today, Bitdefender, Check Point, Emsisoft and Trend Micro have become new associated partners to the project. As a consequence, 32 new decryption tools have been added to nomoreransom.org. So far, eight free-of-charge tools have been available to victims, and nearly 6000 people were able to successfully decrypt their devices without having to pay criminals to do so.

New supporting partners are: AnubisNetworks, AON, Armor, Association for Preventing and Countering Frauds (APCF), BH Consulting, CECyF (Centre Expert contre la Cybercriminalité Français), Cyberlaws.NET, Cylance Inc., DATTO, Inc., ESET, FS- ISAC (Financial Services – Information Sharing & Analysis Center), G DATA Software AG, Heimdal Security, S21Sec, Smartfense, SWITCH, Ukrainian Interbank Payment Systems Member Association (EMA), CERT-EU (Computer Emergency Response Team for the EU institutions, agencies and bodies), IRISS CERT (Irish Reporting and Information Security Service), CIRCL.LU (Computer Incident Response Center Luxembourg) and SI-CERT (Slovenian Computer Emergency Response Team).
In addition, we welcome eu-LISA (the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice), as well as the Austrian, Croatian, Danish, Finnish, Maltese, Romanian, Singaporean and Slovenian police as supporting partners, making a total of 22 countries involved.

Both the private sector and law enforcement are stepping up efforts to fight these cybercriminals who are using ransomware to deprive their victims of large amounts of money. However, awareness remains key to preventing ransomware from being successful. Some simple protection measures can prevent a lot of harm: always have a back-up system in place so a ransomware infection can’t destroy your personal data forever; use robust antivirus software to protect your system from ransomware; keep all the software on your computer up to date and literally trust no-one, as any account can be compromised.

More prevention tips and information are available on www.nomoreransom.org.