

'No More Ransom' Grows: Thousands of Users Get Hacked Data Without Paying



The 'No More Ransom' campaign, jointly set up by Intel Security, Kaspersky Lab, Europol and the Dutch National police in the summer has expanded with 34 additional decryptors added to its roster of anti-hacking tools.

See Also: [No More Ransom](#)

The No More Ransom site provides a guide to what ransomware is, how it works and, most importantly, how to ensure protection of data. The goal is to help victims of ransomware retrieve their encrypted data without having to pay the criminals once it has been locked by criminals.

The website has proven very successful with more than 6,000 users enabled in the decryption of their files using No More Ransom tools. They have done this without having to pay ransom demanded by hackers.

Security companies Emsisoft, Check Point, Trend Micro and Bitdefender have joined the project as associate partners, contributing to the development of decryption keys and tools.

Also on board the project as supporting partners are: ESET, Heimdal Security, Computer Emergency Response Team for the EU institutions, agencies and bodies, Irish Reporting and Information Security Service, and the Computer Incident Response Centre Luxembourg.

Ransomware attacks on healthcare facilities are increasing with reports of incidents hitting the headlines on a regular basis. "The increase has been evident over the past three to five years," a Europol spokesperson told HealthManagement.org. "There are two things you can do immediately to protect your organisation from cyber hacking. Firstly, exercise digital hygiene amongst staff. This means staff need to be educated to not open emails from unknown sources for example. The second is to keep your anti-virus up to date. It's amazing how organisations fail to implement these two basic measures and how much disruption this can cause."

Announcing the new partnerships, Europol said that both the private sector and law enforcement were stepping up efforts to fight cybercriminals who are using ransomware to deprive their victims of large amounts of money "However, awareness remains key to preventing ransomware from being successful."

Source: [HealthcareITNews](#)

Image Credit: Nomoreransom.org

Published on : Tue, 20 Dec 2016