HealthManagement
Promoting Management and Leadership

Recover Data with No Ransom: New Initiative

The Dutch National Police, Europol, Intel Security and Kaspersky Lab have joined forces to launch the initiative No More Ransom (www.nomoreransom.org). The move represents new non-commercial cooperation between law enforcement and the private sector in the fight against ransomware.

No More Ransom is a new online portal that aims to inform the public about ransomware risks and to help victims recover their data without paying a ransom to the cybercriminals.

Ransomware is malware that locks a victims' computer or encrypts their data, demanding them to pay a ransom in order to regain control over the affected device or files.

“Ransomware is a top threat for EU law enforcement: almost two-thirds of EU Member States are conducting investigations into this form of malware attack. While the target is often individual users' devices, corporate and even government networks are affected as well,” an official announcement said. “The number of victims is growing at an alarming rate: according to Kaspersky Lab, the number of users attacked by crypto-ransomware rose by 5.5 times, from 131 000 in 2014-2015 to 718 000 in 2015-2016.”

See Also: Improve Cybersecurity: Fire CEOs?

The site provides a guide on what ransomware is, how it works and, most importantly, how to protect themselves. The project provides users with tools that may help them recover their data once it has been locked by criminals. In its initial stage, the portal contains four decryption tools for different types of malware, the latest developed in June 2016.

In response to Shade ransomware which has infected devices in Russia, Ukraine, Germany, Austria and Kazakhstan as well as France, Czech Republic, Italy, and the U.S. the public-private partnership created a special tool which victims can download from the No More Ransom portal to retrieve their data without paying the criminals. The tool contains more than 160, 000 keys.

The initiative advises victims not to pay ransom as there is no guarantee they will get the decryption key they need in return.

"This initiative shows the value of public-private cooperation in taking serious action in the fight against cybercrime," said Raj Samani, EMEA CTO for Intel Security. "This collaboration goes beyond intelligence sharing, consumer education, and takedowns to actually help repair the damage inflicted upon victims.”

Healthcare is particularly vulnerable to ransomware attacks with several high-profile cases hitting the headlines this year.

Source: Europol HealthcareITNews
Image Credit: Interpol

Published on : Tue, 2 Aug 2016