NO MORE RANSOM: LAW ENFORCEMENT AND IT SECURITY COMPANIES JOIN FORCES TO FIGHT RANSOMWARE

25 Jul 2016

Press Release

A new tool containing 160.000+ keys will help victims to retrieve their data

Today, the Dutch National Police, Europol, Intel Security and Kaspersky Lab join forces to launch an initiative called No More Ransom, a new step in the cooperation between law enforcement and the private sector to fight ransomware together. No More Ransom(www.nomoreransom.org) is a new online portal aimed at informing the public about the dangers of ransomware and helping victims to recover their data without having to pay ransom to the cybercriminals.

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. 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. 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.

NOMORERANSOM.ORG

The aim of the online portal www.nomoreransom.org is to provide a helpful online resource for victims of ransomware. Users can 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. If you are infected, the chances are high that the data will be lost forever. Exercising a conscious internet use following a set of simple cyber security tips can help avoid the infection in the first place.

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 for the Shade variant.

Shade is a ransomware-type Trojan that emerged in late 2014. The malware is spread via malicious websites and infected email attachments. After getting into the user's system, Shade encrypts files

stored on the machine and creates a .txt file containing the ransom note and instructions from cybercriminals on what to do to get user's personal files back. Shade use strong decryption algorithm for each encrypted file, with two random 256-bit AES keys generated: one is used to encrypt the file's contents, while the other is used to encrypt the file name.

Since 2014, Kaspersky Lab and Intel Security prevented more than 27 000 attempts to attack users with Shade Trojan. Most of the infections occurred in Russia, Ukraine, Germany, Austria and Kazakhstan. Shade activity was also registered in France, Czech Republic, Italy, and the US.

By working closely together and sharing information between different parties, the Shade command and control server used by criminals to store keys for decryption was seized, and the keys were shared with Kaspersky Lab and Intel Security. That helped to create 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.

PUBLIC – PRIVATE COOPERATION

The project has been envisioned as a non-commercial initiative aimed at bringing public and private institutions under the same umbrella. Due to the changing nature of ransomware, with cybercriminals developing new variants on a regular basis, this portal is open to new partners' cooperation.

Wilbert Paulissen, Director of the National Criminal Investigation Division of National Police of the Netherlands: "We, the Dutch police, cannot fight against cybercrime and ransomware in particular, alone. This is a joint responsibility of the police, the justice department, Europol, and ICT companies, and requires a joint effort. This is why I am very happy about the police's collaboration with Intel Security and Kaspersky Lab. Together we will do everything in our power to disturb criminals' money making schemes and return files to their rightful owners without the latter having to pay loads of money."

"The biggest problem with crypto-ransomware today is that when users have precious data locked down, they readily pay criminals to get it back. That boosts the underground economy, and we are facing an increase in the number of new players and the number of attacks as a result. We can only change the situation if we coordinate our efforts to fight against ransomware. The appearance of decryption tools is just the first step on this road. We expect this project to be extended, and soon there will be many more companies and law enforcement agencies from other countries and regions fighting ransomware together", says Jornt van der Wiel, Security Researcher at Global Research and Analysis Team, Kaspersky Lab.

"This initiative shows the value of public-private cooperation in taking serious action in the fight against cybercrime," says 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. By restoring access to their systems, we empower users by showing them they can take action and avoid rewarding criminals with a ransom payment."

Wil van Gemert, Europol Deputy Director Operations, finally: "For a few years now ransomware has become a dominant concern for EU law enforcement. It is a problem affecting citizens and business alike, computers and mobile devices, with criminals developing more sophisticated techniques to cause the highest impact on the victim's data. Initiatives like the No More Ransom project shows that linking expertise and joining forces is the way to go in the successful fight against cybercrime. We expect to help many people to recover control over their files, while raising awareness and educating the population on how to maintain their devices clean from malware."

ALWAYS REPORT

Reporting ransomware to law enforcement is very important to help authorities get an overall clearer picture and thereby a greater capacity to mitigate the threat. The No More Ransom website offers to the victims the possibility to report a crime, directly connecting with Europol's overview of national reporting mechanisms.

If you have somehow become a victim of ransomware, we advise you not to pay the ransom. By making the payment you will be supporting the cybercriminals' business. Plus, there is no guarantee that paying the fine will give you back the access to the encrypted data.

Tips & advice to prevent ransomware from infecting your electronic devices

CRIME AREAS Cybercrime
TARGET GROUPS General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
COUNTRIES Austria • Czech Republic • France • Germany • Italy • Netherlands • Russia • Ukraine • United States of America
ENTITIES European Cybercrime Center (EC3)

Source URL: https://www.europol.europa.eu/newsroom/news/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-to-fight-ransomware