BioSpectrum
the business of Bio & Health Sciences
ASIA EDITION

Kaspersky updates decryption tool to fight ransomware pair

30 September 2019 | News

Kaspersky has updated its RakhniDecryptor tool to allow users whose files were encrypted by Yatron and FortuneCrypt ransomware to retrieve their data without paying a ransom

Ransomware is a dangerous threat to healthcare consumers and businesses, with new types of malware being developed rapidly by cybercriminals every day, in order to victimize users. Once locked out of files, corporations and healthcare users are at the mercy of empowered cybercriminals who demand substantial amounts of money to regain access to their information.

Yatron and FortuneCrypt are typical examples of this kind of malware. Yatron is the part of a so-called ransomware-as-a-service affiliate program and its developers were reported to be planning to use the infamous EternalBlue and DoublePulsar exploits (malicious programs that use vulnerabilities in legal software to distribute other malicious software) as a propagation tool for the malware. While encrypting the victims' files, this ransomware changes their extension to '.Yatron'. Kaspersky has developed a tool that is capable of recognizing such files and bringing them back to a normal state.

The other variant of ransomware – FortuneCrypt – is unusual as it is written with a BlitzMax compiler based on publicly available information and is a programming framework developed specifically for those involved in the first steps of video games development. Both ransomware variants contain issues in how they deal with the victims' files, and this allowed Kaspersky researchers to find ways of undoing the damage this malware caused.

"It would be too bold to say that both of these malicious programs can be regarded as significant developments in the ransomware threat landscape as they were not distributed too widely. However, this doesn't mean that the cybersecurity community shouldn't pay attention to less successful strings of ransomware. The goal of a coordinated effort which our industry currently takes against ransomware is not only to help victims retrieve their files, but also to make the business of ransomware itself as troublesome and costly for scammers as possible. The more families we defeat, the harder it is for cybercriminals to profit from their activity. The new decryption tools we've released are contributions to this goal and certainly won't be the last", said Orkhan Mamedov, a security expert at Kaspersky.

For those users who become victims of a ransomware attack and are left locked out of their files or devices, Kaspersky recommends taking the following steps:

1. Do not pay the ransom if a device has been locked. Paying extortionate ransoms only encourages cybercriminals to continue their attacks
2. Contact your local law enforcement agency and report the attack
3. Try to find out the name of the ransomware Trojan. This information can help cybersecurity experts decrypt the threat and retain access to your files
4. Back-up your files so they can be recovered should an attack happen
5. Keep your cybersecurity solution up-to-date by always installing the latest software patches

Both the Yatron and FortuneCrypt decryptors have been added to the Kaspersky RakhniDecryptor tool. They can be downloaded from the No More Ransom website – a project launched by the Dutch National Police, Europol, McAfee and Kaspersky in 2016. The project involves cybersecurity experts and law enforcement agencies working together to share solutions and stop the scourge of ransomware.