EUROPOL

PAY NO MORE: UNIVERSAL GANDCRAB DECRYPTION TOOL RELEASED FOR FREE ON NO MORE RANSOM

25 Oct 2018

Press Release

New tool made available to all in latest victory of law enforcement in the battle against ransomware

As of today, victims of the GandCrab ransomware can recover their files without giving into the demands of the criminals thanks to a new decryption tool released for free on www.nomoreransom.org ⬀ .

This data recovery kit was developed by the Romanian Police in collaboration with its counterparts from Bulgaria, France, Hungary, Italy, Poland, the Netherlands, United Kingdom and United States, together with the security company Bitdefender and Europol. It is the most comprehensive decryption tool available to date for this particular ransomware family: it works for all but two existing versions of the malware (v.1,4 and 5), regardless of the victim's geographical location. This tool is released a week after the criminal group behind GandCrab made public decryption keys allowing only a limited pool of victims located in Syria to recover their files.

GANDCRAB IN A NUTSHELL

GandCrab is one of the most aggressive malware attacks in recent months, infecting nearly half a million victims since it was first detected in January 2018.

Once GandCrab takes over a victim's computer and encrypts its files, it demands a ransom ranging from USD 300 to 6 000. The ransom must be paid through virtual currencies known to make online transactions less traceable, such as DASH and Bitcoin.

Back in February, a first decryption tool was made available on No More Ransom ☑ by the Romanian Police, with the support of the internet security company Bitdefender and Europol. A second version of the GandCrab ransomware was subsequently released by the criminals, this time with an improved coding which included comments to provoke law enforcement, security companies and No More Ransom. A third version followed a day later.

Now in its fifth version, this file-locking malware continues to be updated at an aggressive pace. Its developers are constantly releasing new versions of it, with new, more sophisticated samples being made available to bypass cybersecurity vendors' countermeasures.

UNDERGROUND ALLIANCES

The rapid spread of GandCrab has been helped along by a ransomware-as-a-service scheme, which offers on the dark web to wannabee criminals with little to no technical expertise a toolkit for launching quick and easy malware attacks, in exchange for a 30% cut from each ransom payment.

In order to further maximise the profits, the GandCrab developers are also partnering up with other services in the cybercrime supply chain, enabling different criminal groups to practice their core competencies while working together to earn more illicit profits than they would be able to gather working individually.

HOW TO STAY SAFE IN THE FUTURE

Victims who have fallen to this ransomware should visit www.nomoreransom.org ☑ where this new decryption tool is available for free.

The best cure against ransomware remains diligent prevention. Users are strongly advised to:

- Always keep a copy of their most important files somewhere else: in the cloud, on another drive, on a memory stick, or on another computer.
- Use reliable and up-to-date anti-virus software.
- Not download programs from suspicious sources
- Not open attachments in e-mails from unknown senders, even if they look important and credible

> ❯ And if you are a victim, don't pay the ransom!

Find more information and prevention tips on www.nomoreransom.org ↗

CRIME AREAS   Cybercrime
TARGET GROUPS General Public • Law Enforcement • Academia • Professor • Students • Researcher •
Press/Journalists • Other
COUNTRIES   Bulgaria • France • Hungary • Italy • Netherlands • Poland • Romania • United Kingdom •
United States of America
SUPPORT &   Operational coordination • Operational support • Information exchange • Forensics • Analysis •
SERVICES   Intelligence

Source URL: https://www.europol.europa.eu/newsroom/news/pay-no-more-universal-gandcrab-decryption-tool-released-for-free-no-more-ransom