JUST RELEASED: FOURTH DECRYPTION TOOL NEUTRALISES LATEST VERSION OF GANDCRAB RANSOMWARE

17 Jun 2019

Press Release

A strong team of international law enforcement and private sector partners unveils new tool

On 17 June, a new decryption tool for the latest version of the most prolific ransomware family GandCrab has been released free of charge on www.nomoreransom.org. This tool allows victims of ransomware to regain access to their information encrypted by hackers, without having to pay demanded ransoms. The tool is released in partnership with law enforcement agencies from Austria (Bundeskriminalambt – BMI), Belgium (Federal Computer Crime Unit), Bulgaria (General Directorate Combating Organized Crime - Cybercrime Department), France (Police Judiciaire de Paris – Befti), Germany (LKA Baden-Württemberg), the Netherlands (High Tech Crime Unit), Romania (DIICOT), the United Kingdom (NCA and Metropolitan Police), the United States (FBI) and Europol and its Joint Cybercrime Action Taskforce (J-CAT), together with the private partner Bitdefender.

The decryption tool counters versions 1 and 4 and versions 5 to 5.2, which are the latest to be used by cybercriminals. Previous decryptors for the GandCrab ransomware have helped more than 30 000 victims recover their data and save roughly $50 million in unpaid ransoms. Most importantly, the joint efforts have weakened the operators' position on the market and have led to the demise and shutdown of the operation by law enforcement. This shutdown was a global law enforcement effort supported by Bitdefender and McAfee.

Launched in January 2018, GandCrab quickly became the go-to tool for hackers for affiliate-based ransomware, holding 50% share of all the ransomware market by mid-2018. Set as a ransomware-as-a-service licensing model, distributors could buy the ransomware on dark web markets and spread it among their victims. In exchange, they would pay 40% of their profit to the GandCrab developers and keep 60% for themselves. The GandCrab operators recently claimed that they have extorted more than $2 billion from victims. It is likely that they subjected over 1.5 million victims all over the world to this ransomware.

BETTER SAFE THAN SORRY

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 emails from unknown senders, even if they look important and credible;
- don't pay the ransom if you are a ransomware victim!

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	Austria • Belgium • Bulgaria • France • Germany • Netherlands • Romania • United Kingdom • United States of America
ENTITIES	Joint Cybercrime Action Taskforce (J-CAT)
SUPPORT & SERVICES	Operational support • Information exchange

---

Source URL: https://www.europol.europa.eu/newsroom/news/just-released-fourth-decryption-tool-neutralises-latest-version-of-gandcrab-ransomware