New GandCrab v5.1 Decryptor Available Now

labs.bitdefender.com/2019/02/new-gandcrab-v5-1-decryptor-available-now/

Bogdan BOTEZATU

February 19, 2019

Bitdefender
Free ransomware decryption tools for business and home users
DOWNLOAD NOW

Today we’re happy to announce that our collaboration with the Romanian Police, Europol and other law enforcement agencies has yielded another new decryptor for all GandCrab ransomware versions released since October 2018.

If you need to decrypt versions 1, 4 and up through 5.1, then download and run our brand new tool:

Download the GandCrab decryptor

Bitdefender Labs on the Case

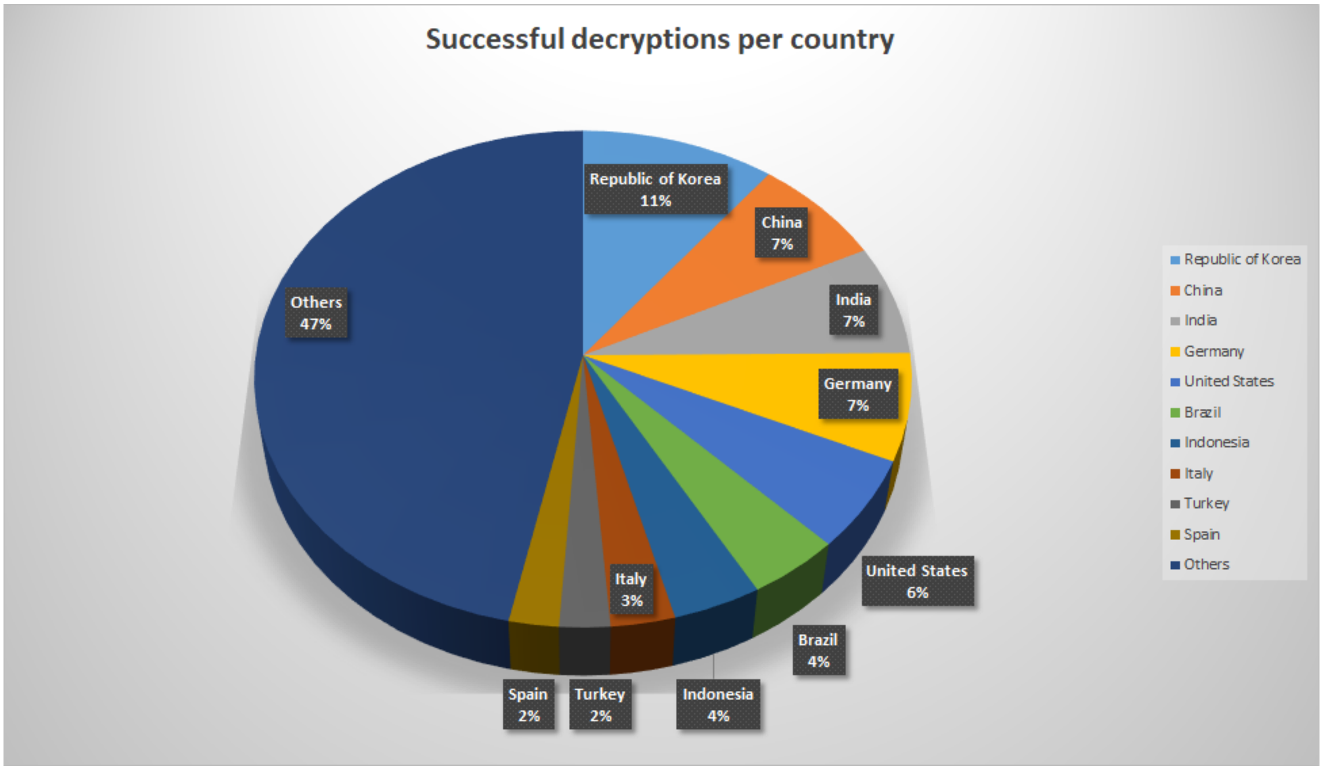
When GandCrab started spiking on the threat map in January 2018, Bitdefender released the first free decryptor to help victims take their digital lives back. More than 2,000 home users, companies and non-profits used it to retrieve their lost data and avoid paying millions in ransom.

Ten months later, we released another decryptor to expand support to GandCrab versions 1, 4 and 5 up to 5.0.3. Ever since, we been contacted by and keeping in touch with thousands of victims seeking help.

While this is the third time we have defeated GandCrab encryption in the past year, our celebration will be short-lived. We’ll be back to work tomorrow, as GandCrab operators will no doubt change tactics and techniques.

GandCrab in Numbers

GandCrab has inflicted hundreds of millions of dollars in losses globally since its emergence, and is now one of the most prevalent families of ransomware on the market. Since our first decryptor, in aggregate we have already helped nearly 10,000 victims save more than $5 million dollars in decryption fees nearly 20,000 victims save a minimum of $18 million US dollars by the end of February: .



GandCrab on the Attack

Last year, some GandCrab affiliates began attacking organizations via exposed Remote Desktop Protocol instances, or by directly logging in with stolen domain credentials. After authenticating on a compromised PC, attackers manually run the ransomware and instruct it to spread across the entire network. Once the network is infected, the attackers wipe their traces clean and contact the victim with a decryption offer.

Recently, GandCrab operators have also started delivering ransomware to companies via vulnerabilities in remote IT support software used by managed service providers to manage customer workstations. To learn more about what MSPs need to do in order to stay safe from ransomware, watch our webinar:

GandCrab is targeting MSPs. Are you sure you're protected?

GandCrab is targeting MSPs. Are you sure you're protected? | Bitdefender Webinar | MSP

Learn what GandCrab attacks look like and how you can limit potential damage to your business. Best security practices to protect your business and clients offered by Bitdefender.

Bitdefender Antivirus

This persistence is why prevention is crucial. If you have a security solution, make sure it is up-to-date and has layered defenses against ransomware. The better it is at detection, the lower your chances of infection. Also make sure you are running the latest version of your OS and third-party software.

If you don’t have a security solution, get one now. It helps a lot, and it’s way less expensive than a $600 ransom payment.

Last but not least, *stop whatever you are doing and make and verify an external backup of your important data*. Should disaster strike, you will have a copy to restore from.

Otherwise, Bitdefender and partner law enforcement agencies advise victims to reject the demands of ransomware operators. Instead, back up the encrypted information and notify the police immediately. And follow us here for updates.

TAGS

anti-malware research free tools

AUTHOR

Bogdan BOTEZATU

Information security professional. Living my second childhood at @Bitdefender as director of threat research.

View all posts