


Killswitch File Now Available for GandCrab v4.1.2 Ransomware

 sensortechforum.com/killswitch-file-now-available-gandcrab-v4-1-2-ransomware/

Ventsislav Krastev

July 19, 2018



The South Korean company [Ahnlab](#) has developed a Killswitch for the latest version of the virus, calling itself v4.1.2, causing the ransomware to stop functioning.

Ahnlab has reportedly analyzed the internal version 4.1.2 of GandCrab ransomware, which is part of the **4.1 version**, using the **.KRAB file extension** after file encryption. Researchers have then designed an app, that works as a defensive measure and can be dropped on users' computers before they become infected with **GandCrab 4.1.2**. For the defense tactic to work, you will need to get the file, which has a string in it's name and has the .lock file extension. Such .lock files are essential to GandCrab's way of operation and here are the steps in which they are created:

Step 1: GandCrab 4.1.2 infects your computer and encrypts your files.

Step 2: The virus creates a .lock file with a mutex, for which the virus scans for comparing the file to the .lock files of other infected computers.

Step 3: If the .lock file already belongs to GandCrab's infected computers' list, the virus shuts down and doesn't encrypt anything to prevent double encryption and infection to take place.

Researchers have cleverly devised such a .lock file, which acts as a killswitch and the whole app can be downloaded from the following link (also available on asec.ahnlab.com/1145):

[Download](#)

[GandCrab Killswitch](#)

IMPORTANT NOTICE! Your antivirus may detect the killswitch as a virus, but it is also available on Anhlab's research site above and we believe that the file can be trusted, because it is not an actual GandCrab but merely a method used to prevent the actual threat so be advised to disable your antivirus and anti-malware software before downloading the file.

After downloading the file, victims should save it either in the **%Application Data% directory for older Windows Versions** or in the **%ProgramData% directory for Windows 7 and newer versions** of the operating system. This prevents your computer from certain file encryption, even if **GandCrab v4.1.2** has already infected the machine.



New Updates in GandCrab v4.1.2<

GandCrab is the type of ransomware that has been spreading and infecting computers since [January, 2018](#). The virus has undergone major changes since then, using fake Dental Records and other fake .exe files to infect user PC's. The malware which preyed on users who had SMBv1 enabled on their machine has been updated in a 4.1 version, which has evolved in it's current 4.1.2 internal variant. The latest version of **GandCrab** is using more and more methods to spread, like the newer EternalBlue exploits used in the [WannaCry outbreak](#), that happened back in 2017. But in the same time, this newer version of the virus has also stopped using some older exploits, like SMB to infect computers, suggesting newer

operating systems to be targeted. One thing has remained certain – GandCrab still uses the same methods to spread and they are not likely to be automatic, since the virus uses spam e-mails with malicious attachments of all types and may also upload the infection files on suspicious and low reputation sites. It is strongly advisable to apply proper anti-malware protection and also make sure to learn how to safely store your important files in order to protect yourself from malware infections, like **GandCrab** (see related articles below):

Related: [Protect Yourself from Getting Infected by Malicious E-mails](#)

Related: [Safely Store Your Important Files and Protect Them from Malware](#)



Ventsislav Krastev

Ventsislav is a cybersecurity expert at SensorsTechForum since 2015. He has been researching, covering, helping victims with the latest malware infections plus testing and reviewing software and the newest tech developments. Having graduated Marketing as well, Ventsislav also has passion for learning new shifts and innovations in cybersecurity that become game changers. After studying Value Chain Management, Network Administration and Computer Administration of System Applications, he found his true calling within the cybersecurity industry and is a strong believer in the education of every user towards online safety and security.

[More Posts - Website](#)

Follow Me:



[Previous post](#)

[Next post](#)