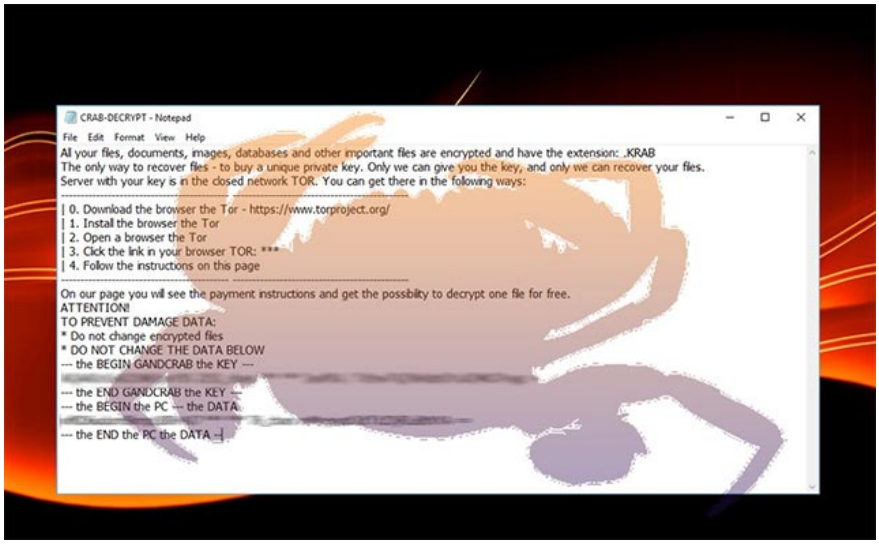
The official GandCrab 5.2 decoder was released, ending a bad nightmare called GandCrab Ransomeware

The Bitdefender security team has recently actively collaborated with law enforcement agencies around the world, successfully releasing the latest version of the decoder for GandCrab extortion code that has blown the wind. worldwide during the past 1 year.

The Bitdefender security team has recently actively collaborated with law enforcement agencies around the world, successfully releasing the latest version of the decoder for GandCrab extortion code that has blown the wind. worldwide during the past 1 year. With GandCrab 5.2, these malicious victims can easily decrypt files encrypted by versions 1, 4 and 5 to 5.2.

In official announcements issued by both Bitdefender and Europol, a decoder for GandCrab Ransomware has been released to provide victims of this extortion code with a specific decoding tool for encrypted files. turned up by the latest version of GandCrab.

1. Shade ransomware, the nightmare of 5 years ago is showing signs of returning



Notice of GandCrab's ransom

Organizations involved in the development and distribution of the decoder GandCrab 5.2 include:

"This tool was released in cooperation with law enforcement agencies from Austria (Bundeskriminalambt - BMI), Belgium (Federal Computer Crime Unit - FCCU), Bulgaria (Bulgarian Cybercrime Unit - BCU), France (Police Judge de Paris - Befti), Germany (LKA Baden - Wurttemberg),), Netherlands (Department of High-tech Crime Prevention - HTCU), Romania (DIICOT), United Kingdom (NCA and Metropolitan Police), United States (FBI and Europol, together with private partners: Bitdefender International Security Team ".

Similar to previous releases of the GandCrab Ransomware decoder built by Bitdefender, this tool is not freely available because of the occurrence of vulnerabilities in the encryption algorithm. Instead, the security team will work with law enforcement agencies from many countries to get access to GandCrab's command and control servers (C2 Server) to download solutions. necessary decryption key, thereby using them to decrypt victim files.

Instructions on how to use GandCrab decoder can be found at the end of this article. If you need any help, please leave a comment in this article or ask questions on the GandCrab Support and Help forum of Bleeping Computer network security.

1. [Infographic] 7 effective ways to protect businesses from Ransomware

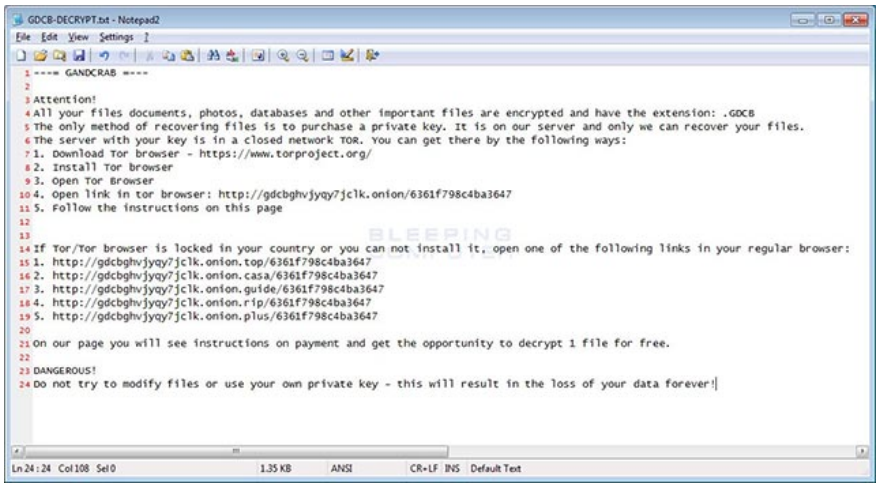
GandCrab Ransomware

1. The rise and fall of GandCrab blackmail
2. How to decode encrypted GandCrab file

The rise and fall of GandCrab blackmail

Most tech sites, big security teams around the world, have been closely monitoring GandCrab since it was first released on January 28, 2018. At that time, This malicious code has only just begun to be distributed through Ransomware-as-an-Affiliate system on underground hacker forums like Exploit.in.

At the first release, GandCrab Ransomware was distributed through the RIG exploit. When it spreads to the victim's system, it will immediately encrypt the entire file system being stored on the computer and connect the .GDCB extension to the name of each file.



The original notice of GandCrab's ransom

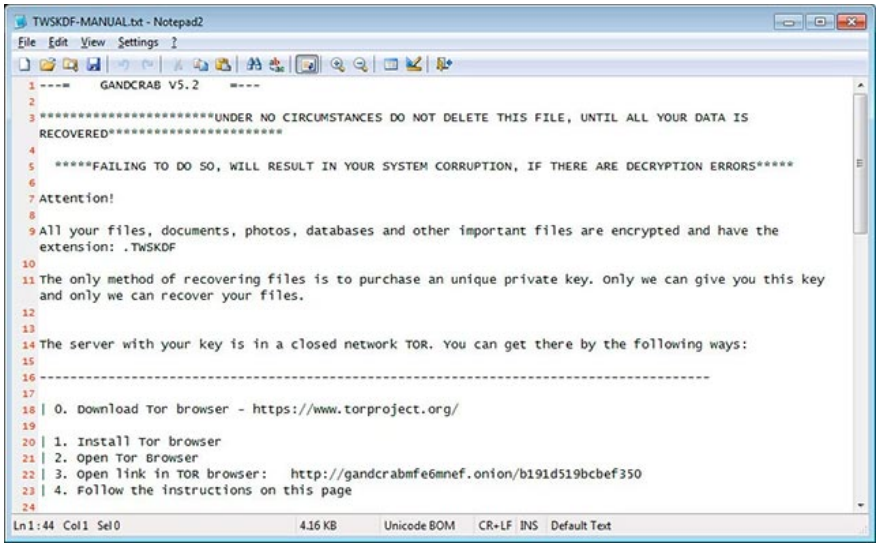
Hackers who develop malicious code - the one behind GandCrab - have already had ridicule and even challenged network security researchers and security organizations who are closely monitoring every activity. their movements.

As mentioned in the first release of ransomware GandCrab, malicious developers decided to use their domain names for their Command & Control (C2 server) servers based on organizations and websites. supposedly doing the research or the most concerned about this ransomware as a 'challenge', including:

1. bleepingcomputer.bit
2. nomoreransom.bit
3. esetnod32.bit
4. emsisoft.bit
5. gandcrab.bit

Since then, two factions: Security experts and the people behind GandCrab have been involved in "retaliatory" behavior. During this period, security researchers temporarily lagged behind the rampant spread of GandCrab on a global scale. They silently watched the group of GandCrab release many new versions of malicious code until the final version of 5.2 was released a few months ago.

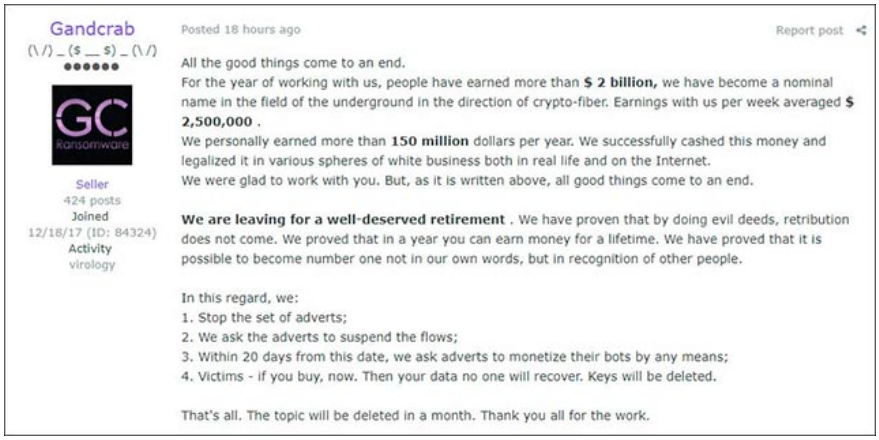
1. New ransomware detection not only encrypts files but also helps 'clean up' the system



Ransom note GandCrab 5.2

In the next phase, security teams around the world began to launch heavy counter-attacks. A large number of GandCrab C2 servers have been successfully hacked, along with network security experts actively launching special decoders for this extortion code.

After nearly a year and a half of 'winding up', until the beginning of June, the people behind GandCrab ransomware claimed that the malware stopped working and at the same time urged the malicious 'branches' of I stopped the distribution of malicious code. They claimed to have pocketed more than $ 2 billion through GandCrab, and $ 150 million of them were cashed and successfully "laundered" through investing in business projects and entities. France.



GandCrab shutdown notice

Declaration of attackers With the latest decoder just released, the life cycle of GandCrab Ransomware has officially ended and now the victim of this malicious code can completely retrieve files of They are free.

1. GandCrab blackmail extinguished after earning $ 2.5 billion worldwide

How to decrypt the file is encrypted by GandCrab

If your system is infected with GandCrab Ransomware v1, v4 and versions 5-5.2, it is currently possible to retrieve all encrypted files without paying ransom using the solver. The code is updated by Bitdefender.

First, download the BDGandCrabDecryptTool.exe file from this link.

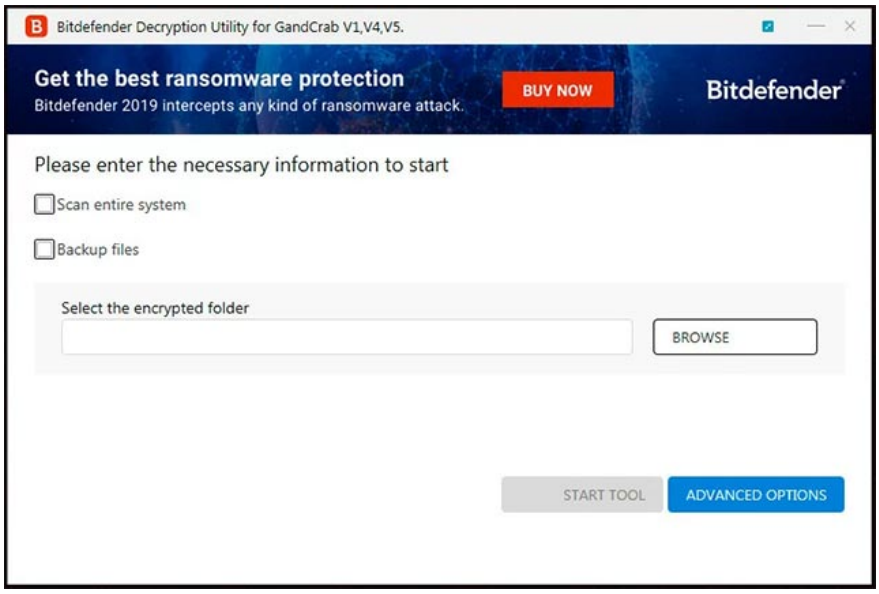
The latest GandCrab decoding tool

After the download process is complete, double-click the downloaded program and will receive a license agreement, click accept with the given terms.

Next, the decoder will start to be launched and show a message that your system needs to be connected to the Internet to continue the necessary steps. The reason for this requirement is that the decoder will need to reconnect to the Bitdefender servers to check your decryption key and download it to the computer.

Internet connection required

The screen will now display the option to decode GandCrab as shown in the example below. At this point, you can choose to decrypt all encrypted files on the system or manually decrypt (decrypt only specific directories).



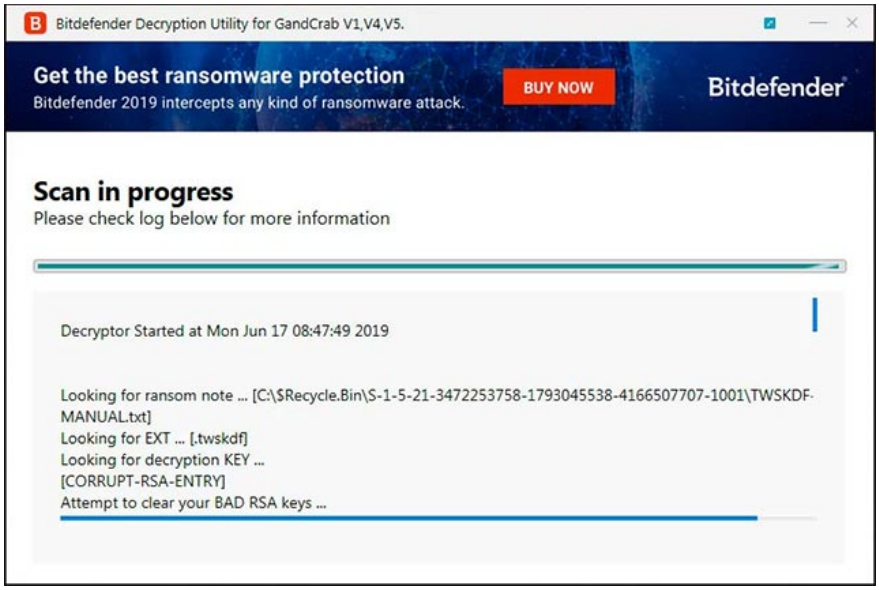
Select the decoding option for Bitdefender GandCrab tool

Researchers recommend that you try to manually decode a specific directory first to make sure the decoder works correctly and that no serious problems occur.

After you have selected the decoding option you want, to start the process, you need to click the **Start Tool** button **.**

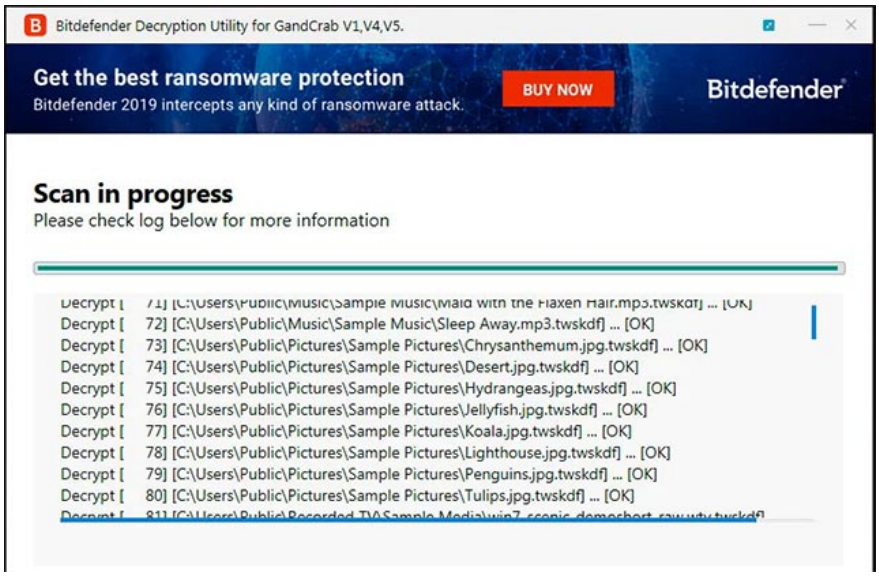
When the decoding process starts taking place, the decoder will search for a ransom note to collect certain information. This information will then be uploaded to Bitdefender's server.

1. Cr1ptT0r Ransomware spreads on D-Link NAS devices, targeting embedded systems



Get the decryption key from the Bitdefender server

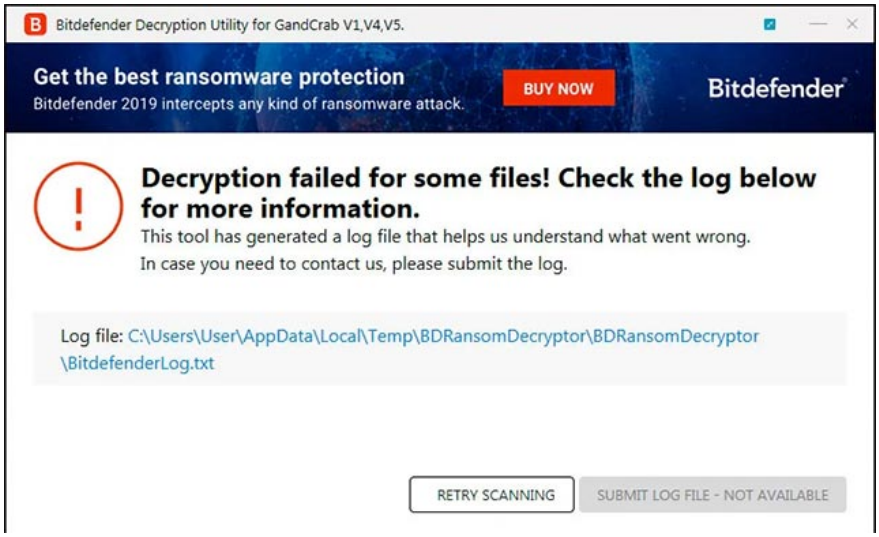
When a decryption key is retrieved and downloaded, the decoder will begin decrypting the files on your system.



The process of decoding the encrypted file GandCrab

When the decoding process is complete, the decoder will send a message to you, and will issue warnings in case any problems occur.

If a problem occurs, you can click the log file link to automatically open the log file named% Temp% BDRansomDecryptorBDRansomDecryptorBitdefenderLog.txt. This file will contain a summary of information about the decrypted files as well as the case of errors, unable to successfully decrypt.



The decoding process is complete

For example, in researchers' tests at Bleeping Computer, Bitdefender's decoder was able to successfully decode almost all of the files in the system, except for those 10 problems. Thankfully, these are only application-specific files, meaning they can be recreated by reinstalling the application.

If you have trouble working with this decoder, please leave a question at the GandCrab Support and Help forum, specifically in this topic.

Although it has caused countless troubles all over the world and the people behind it have not been brought to light yet, yet anyway, GandCrab, or any other ransomware that stops working is still something to celebrate.