Good riddance, GandCrab! We’re still fixing the mess you left behind.

labs.bitdefender.com/2019/06/good-riddance-gandcrab-were-still-fixing-the-mess-you-left-behind

Bogdan BOTEZATU

June 17, 2019

On January 28th 2018, our analysts on watch saw a small blip pop up on the Bitdefender Threat Map. It was one of millions of blips we see daily here at Bitdefender, but that blip marked the birth of a new family of ransomware that would cause great pain to innocent victims around the world. The same blip would show up at least 50,000 more times in the following month and several more million times in the next year. It came to be known as "GandCrab."

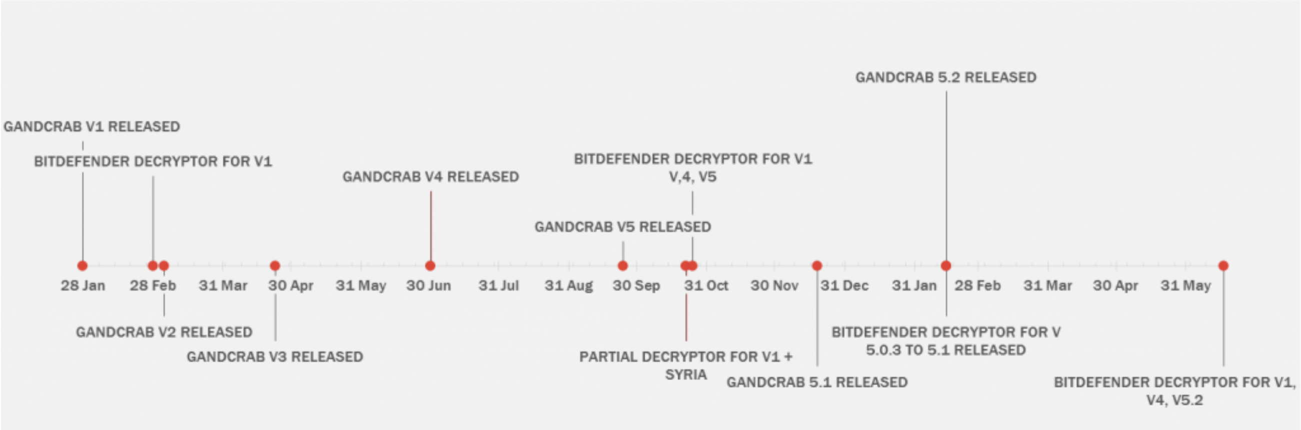
Download the GandCrab decryptor

This family of ransomware, likely operated out of the former Soviet space, grabbed more than 50 percent of the ransomware market share by August 2018. Access to GandCrab ransomware was sold on underground markets to affiliates, who were responsible for infecting victims and extorting money from them. In exchange, the affiliates gave 40% of their profit to the original GandCrab developers. This fostered a diverse distribution system. Some affiliates would spam out their payloads, while others would infect victims through, for instance, exploit kits or remote access to enterprise computers.

At Bitdefender, we've carefully counted these blips and spared no effort in bringing relief to the unlucky ones who crossed paths with the GandCrab team. In collaboration with partner law enforcement agencies including Europol, Romanian Police, DIICOT, FBI, NCA and

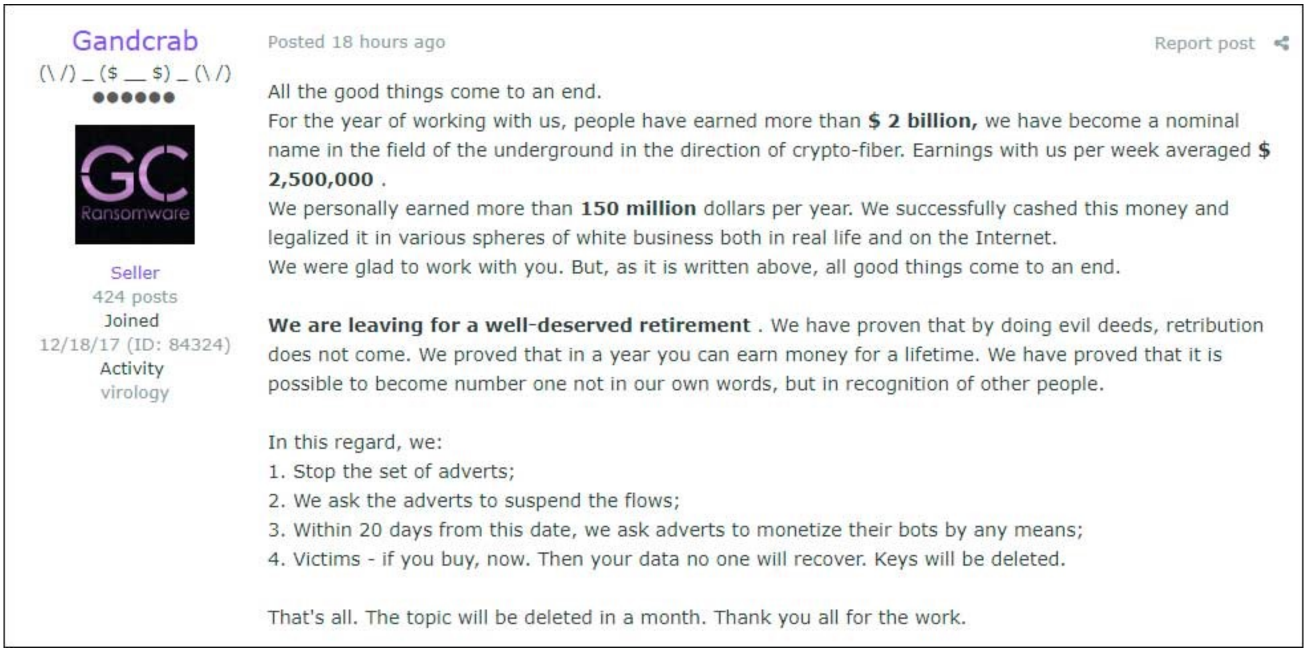
Metropolitan Police, as well as Police Offices in France, Bulgaria, we have managed to offer several decryptors to help GandCrab victims get their data back for free.

These tools totaled more than 30,000 successful decryptions and have saved victims roughly $US 50 MILLION in unpaid ransom. Most importantly, it helped us weaken the ransomware operators by cutting off their monetization mechanisms and establishing a positive mindset among new victims, who would rather wait for a new decryptor than give in to hackers' ransom demands.



In more than a year of operation, we estimate GandCrab has claimed more than 1.5 million victims around the world, both home users and corporations. GandCrab operators and affiliates boldly claimed on private underground forums recently that the team behind the malware has extorted more than $2 billion from victims.

While the number is clearly exaggerated, the GandCrab operation was prolific enough to score enough revenue to allow its masters to retire. According to the same claim, the GandCrab team has stopped affiliates from accessing new versions of the malware and has urged them to prepare for an imminent shutdown. The shutdown will be followed by deletion of all keys, leaving the victims unable to retrieve the ransomed data even if they do pay ransom.



All the good things come to an end.
For the year of working with us, people have earned more than **$ 2 billion,** we have become a nominal name in the field of the underground in the direction of crypto-fiber. Earnings with us per week averaged **$ 2,500,000** .
We personally earned more than **150 million** dollars per year. We successfully cashed this money and legalized it in various spheres of white business both in real life and on the Internet.
We were glad to work with you. But, as it is written above, all good things come to an end.

We are leaving for a well-deserved retirement . We have proven that by doing evil deeds, retribution does not come. We proved that in a year you can earn money for a lifetime. We have proved that it is possible to become number one not in our own words, but in recognition of other people.

In this regard, we:
1. Stop the set of adverts;
2. We ask the adverts to suspend the flows;
3. Within 20 days from this date, we ask adverts to monetize their bots by any means;
4. Victims - if you buy, now. Then your data no one will recover. Keys will be deleted.

That's all. The topic will be deleted in a month. Thank you all for the work.

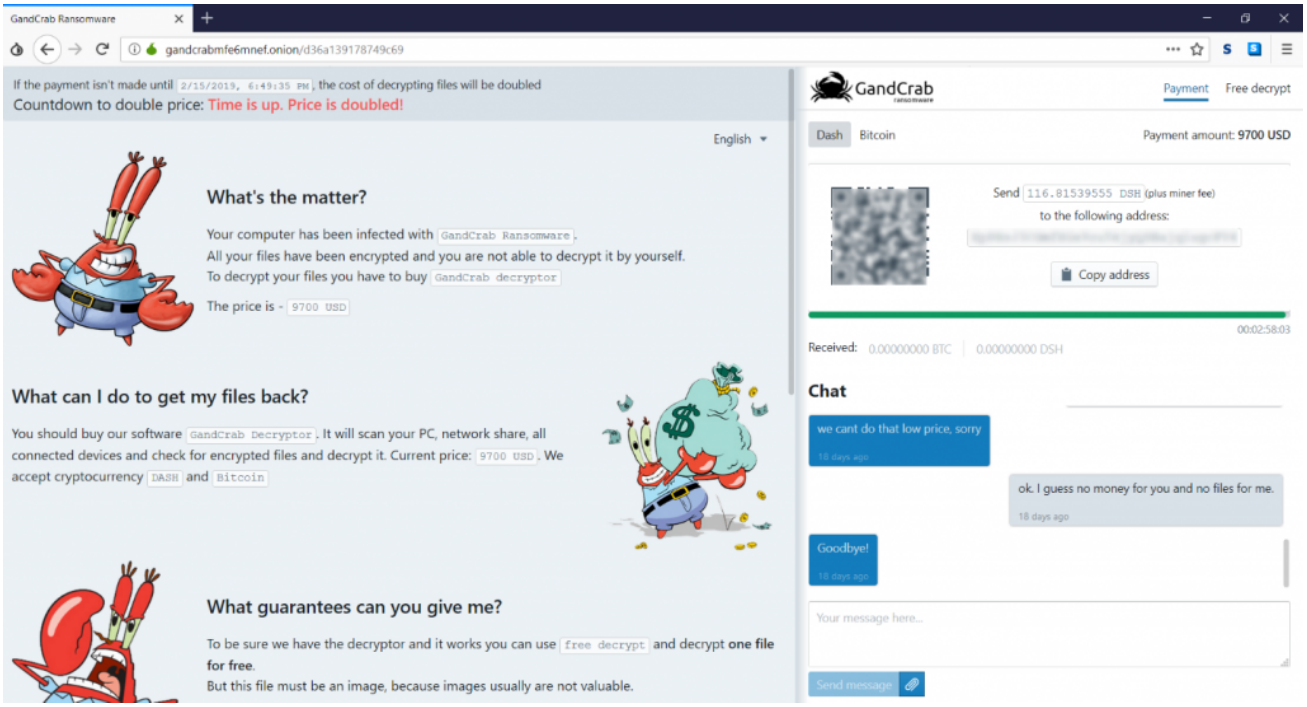
GandCrab shutdown announcement – photo courtesy to bleepingcomputer.com
Fortunately, we have released an update to the tool that neutralizes the latest versions of GandCrab, including version 5.2. The tool is available immediately and can be downloaded for free below or from the No More Ransom Project.

Facts and figures about GandCrab

From its inception in January of 2018, GandCrab quickly became hackers’ go-to tool for affiliate-based ransomware. Likely based in the former Soviet space, its operators and affiliates target victims all around the world, with the exception of Russian-speaking countries and several others where market economics make it impossible for victims to pay up (such as Syria). In less than a year, GandCrab became the world’s widest-spread ransomware, accounting for half of all ransomware infections.

A key advantage of GandCrab over other ransomware families is its ransomware-as-a-service licensing model, where distributors purchase and spread the malware and split the decryption fees with the original developer. Affiliates keep 60%, while the rest goes to the developers. This segregation of duties allow developers to improve on the code and add new features (such as antivirus circumvention techniques) and let the distributors focus on delivery and exploitation of victims.

The GandCrab business also brings new features, such as a chat service for victims to contact the affiliates to negotiate discounts, extend the payment deadline or ask for help exchanging fiat money into digital currency.



If the payment isn't made until 2/15/2019, 6:49:35 PM, the cost of decrypting files will be doubled
Countdown to double price: Time is up. Price is doubled!

What's the matter?

Your computer has been infected with GandCrab Ransomware.
All your files have been encrypted and you are not able to decrypt it by yourself.
To decrypt your files you have to buy GandCrab decryptor

The price is - 9700 USD

What can I do to get my files back?

You should buy our software GandCrab Decryptor. It will scan your PC, network share, all connected devices and check for encrypted files and decrypt it. Current price: 9700 USD. We accept cryptocurrency DASH and Bitcoin

What guarantees can you give me?

To be sure we have the decryptor and it works you can use free decrypt and decrypt **one file for free.**
But this file must be an image, because images usually are not valuable.

Payment amount: **9700 USD**

Send 116.81539555 DSH (plus miner fee)
to the following address:
[redacted]

00:02:58:03

Received: 0.00000000 BTC | 0.00000000 DSH

Chat

we cant do that low price, sorry
18 days ago

ok. I guess no money for you and no files for me.
18 days ago

Goodbye!
18 days ago

Your message here...

In addition to bridging communications with the victim, the chat also has a “secret” area that gives shady data recovery companies a discount on behalf of victims to mask a ransom payment as a “data recovery fee” for customers.

Not all victims are treated equally: GandCrab prioritizes ransomed information and sets individual pricing by type of victim. An average computer costs from $600 and $2,000 to decrypt, and a server decryption costs $10,000 and more. While helping victims with decryption, we’ve seen ransom notes asking for as much as $700,000, which is quite a price for one wrong click.

The three decryptors released in collaboration with partner law enforcement agencies – and particularly the GandCrab decryptor for version 5.1 – compelled GandCrab affiliates shrink their business to avoid unnecessary costs. For instance, in February 2019, after the release of the decryptor for version 5.1, affiliates kept pushing decryptable versions of the malware for more than a week, allowing fresh victims to decrypt their data for free. As of March 2019, GandCrab’s market share has shrunk back to 30 percent, with almost one in three infections tied to the group.

How to stay safe

Ransomware decryption is a delicate matter, as the malware writers use the same technology that helps people protect their banking transactions, communications and online interactions. Encryption is easy, but decryption without a key is nearly impossible. Every month, Bitdefender sees 12 new strains of ransomware, which means cyber-criminals push out a total of more than 140 new families a year. Out of these, almost 10 percent are decryptable by leveraging loopholes in the attackers’ code or through partnerships with law enforcement organizations.

When dealing with ransomware, prevention is key. Once your system gets encrypted, chances of decryption are thin, despite the industry's efforts to bring your data back. Here are some tips to help you prevent ransomware attacks and minimize the amount of money that flows to cyber-crime operators:

1. Run a security solution. If you have a security solution installed, make sure that you are using the full range of technologies to fend off a ransomware attack. Behavioral-based detection, heuristics based on machine learning and ransomware remediation are key technologies to detect and block ransomware attacks. If you don't have one installed, Bitdefender offers a highly effective security solution for free.
2. Make frequent backups on offline media. Backups are an extremely effective solution against loss of data if disaster strikes. Get a portable hard-drive and religiously back important data up as you create it. DO NOT keep the drive connected for longer than needed for backup purposes, as most ransomware encrypts information on connected removable drives and network shares.
3. If all else fails, do not pay the ransom. Ransom payments allow the attackers to thrive, and let them develop more aggressive strains of malware. If your system becomes infected, back the affected data up and immediately notify the Police. While they might not be able to immediately help you out with decryption, they will log the incident and start working with partner private cybersecurity companies on a solution.

Ready to take your data back? Download the tool below.

Download the GandCrab decryptor

TAGS

anti-malware research   free tools

AUTHOR

Bogdan BOTEZATU

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