

# GandCrab Ransomware Shutting Down After Claiming to Earn \$2 Billion

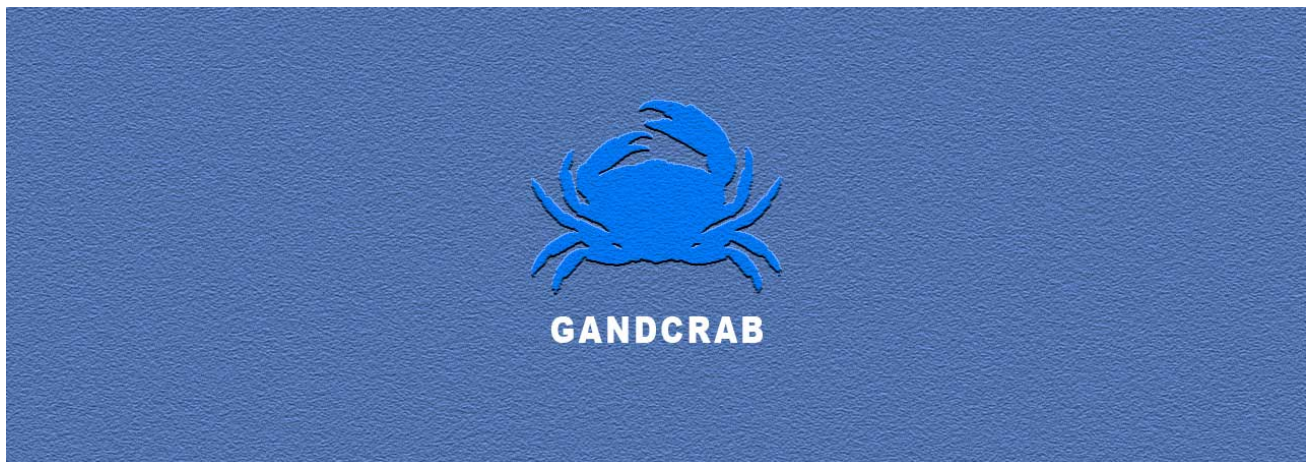
[bleepingcomputer.com/news/security/gandcrab-ransomware-shutting-down-after-claiming-to-earn-25-billion/](https://bleepingcomputer.com/news/security/gandcrab-ransomware-shutting-down-after-claiming-to-earn-25-billion/)

Lawrence Abrams

By

[Lawrence Abrams](#)

- June 1, 2019
- 11:56 AM
- 2



After almost a year and a half, the operators behind the GandCrab Ransomware are shutting down their operation and affiliates are being told to stop distributing the ransomware.

Filling the gaps left behind by the shutdown of large scale ransomware operations such as TeslaCrypt, CryptoWall, and Spora, GandCrab exploded into the ransomware world on January 28th, 2018, when they started marketing their services on underground criminal sites.


Since then, they had become one of the dominant, if not the most dominant, actors in ransomware operations, with their operations only starting to slow down over the past few months.

According to security researchers [Damian](#) and [David Montenegro](#) who have been following the exploits of GandCrab on the underground hacking and malware forum Exploit.in, the GandCrab operators have posted that they are shutting down their operation.

In images provided to BleepingComputer by Damian, we can see the operators stating that they have generated more than \$2 billion in ransom payments, with average weekly payments of \$2.5 million dollars. They go on to say they have personally earned \$150 million, which they have cashed out and invested in legal business entities.

**Gandcrab** Posted 18 hours ago Report post

(\ /) \_ (\$ \_ \$) \_ (\ /)  
●●●●●●



**Seller**  
424 posts  
Joined  
12/18/17 (ID: 84324)  
Activity  
virology

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 Ransomware

With this announcement GandCrab has said they have stopped promoting the ransomware, asked the affiliates to stop distributing the ransomware within 20 days, and asked their topic to be deleted at the end of the month.


  
●●●●●●



**Moderator**  
1339 posts  
Joined  
01/09/16 (ID: 66450)  
Activity  
other / other

Posted 17 hours ago

**Moderator warning:**



Top closed from the flood.  
PS Put the keys in public and everyone will be happy.

**I DO NOT CONSULT, DO NOT GET ON QUESTIONS!**  
**I DO NOT WORK, NOT BY THE TOPICS!**  
Guys, let's live together @ Leopold  
Jabber Contact in profile, only on Maud issues.

### Moderator closing the topic

They have also told victims to pay for needed decryption now as their keys will be deleted at the end of the month. This is could be a last money grab and we hope that the GandCrab devs will follow other large ransomware operations and release the keys when shutting

down.

BleepingComputer has reached out to the developers and asked them to do so.

Historically, BleepingComputer has seen large-scale ransomware operations fill the void left when another ransomware shuts down. It would not be surprising to see another operation spring up in the near future, especially when as noted by GandCrab:

"We have proven that by doing evil deeds, retribution does not come."

## Lofty claims of earnings

---

While the operators behind GandCrab most likely made many millions of dollars, the claims of \$2 billion in ransom payments are very likely to be untrue.

These lofty claims are not surprising, as the developers of GrandCrab have always been jokesters and have engaged security researchers in ways most malware developers do not.

Using taunts, jokes, and references to organizations and researchers in their code, it was obvious that the GandCrab developers were monitoring us as much as we were monitoring them and got a big kick out of it.

For example, in their first release of the ransomware, GandCrab decided to use domain names for their Command & Control servers that are based on organizations and sites known for ransomware research. For example, you can bleepingcomputer, nomoreransom, eset, and emsisoft listed below in their initial C2 servers.

```
bleepingcomputer.bit  
nomoreransom.bit  
esetnod32.bit  
emsisoft.bit  
gandcrab.bit
```

They also frequently dropped hellos to researchers who analyzed their ransomware.

| Hello, [#GandCrab](#) :) [pic.twitter.com/ICHixxolkI](https://pic.twitter.com/ICHixxolkI)

| — Marcelo Rivero (@MarceloRivero) [April 17, 2018](#)

It was not all fun and games, though, for the GandCrab operators also had a vindictive streak. After AhnLab released a vaccine app for GandCrab, the ransomware developers contacted BleepingComputer to tell us that they were releasing a zero-day for the AhnLab v3 Lite antivirus.

```

[05:21:11] <> Hello, Catalin. I am GandCrab. Ping me when online
[05:21:57] <> I want to release ahnlab 0day denial of service exploit.
[05:22:23] <>
http://filestorage.biz/download.php?file:
Archive password is GandCrab

Target: AhnLab V3 Lite
Type: Denial of service
Author: GandCrab

*Abstract*

Ahnlab V3 Lite Denial of service. Possibly can trigger full write-what-where condition with privelege escalation.

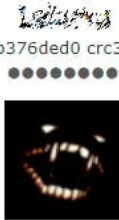
Tested on Win7 x86, Win7 x64, Win 10 x64

[05:24:15] <> It is an answer for kill-switch. Their killswitch has became useless in only few hours. My exploit
will be an reputation hole for ahnlab for years
[05:28:37] <> just as verification look inside support message. I also set unusual bot price and expiration time.
http://gandcrab2pie73et.onion/ /support

```

### Caption

Their antics and success didn't go unnoticed by other members of Exploit.in who wished them farewell or were saddened to see them leave.



**b376ded0 crc32**  
●●●●●●●●

User  
1229 posts  
Joined  
12/14/17 (ID: 84236)  
Activity  
other

Posted 18 hours ago

Everything has a beginning, and everything will have an end, so I'm glad - here the end is definitely a good, happy end.

I am glad that I was a part of it all, but not big, but a part. Even sad somehow, but we will not talk about the bad 😊 The guys have a good rest this summer, they worked a lot and now they can afford to rest on the crabs, the main thing is not to boil in the sun ❤️

For the crab, a separate place appeared in my heart during these months.

---

Do not make transactions without confirmation in PM

btc adress for donation 1MrXzUx8ffTi3WcEnMkBU95xrK5vqusTXV

To resolutely and universally  
It became young-green  
And red.

**donaldtrump1**  
megabyte  
●●●



User  
83 posts  
Joined  
01/22/17 (ID: 75933)  
Activity  
other

Posted 18 hours ago

i think i will cry :( :)

While the GandCrab antics have been amusing at times, they ultimately inflicted a lot of pain and suffering on many people who lost their data, work, and potentially even businesses. Their shutdown of operations is a good thing.

## Related Articles:

---

[Windows 11 KB5014019 breaks Trend Micro ransomware protection](#)

[Industrial Spy data extortion market gets into the ransomware game](#)

[New 'Cheers' Linux ransomware targets VMware ESXi servers](#)

[SpiceJet airline passengers stranded after ransomware attack](#)

[US Senate: Govt's ransomware fight hindered by limited reporting](#)

- [GandCrab](#)
- [Ransomware](#)

[Lawrence Abrams](#)

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- [Previous Article](#)
- [Next Article](#)

## Comments

---



[Mr.Tom](#) - 2 years ago

- 
- 

Oh those crazy clownsters.. <honk> <honk>



• [guidecca](#) - 2 years ago

- 
- 

Karma has a way of catching up to people and I think these guys will get more bad karma than they can handle.

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

**You may also like:**

---