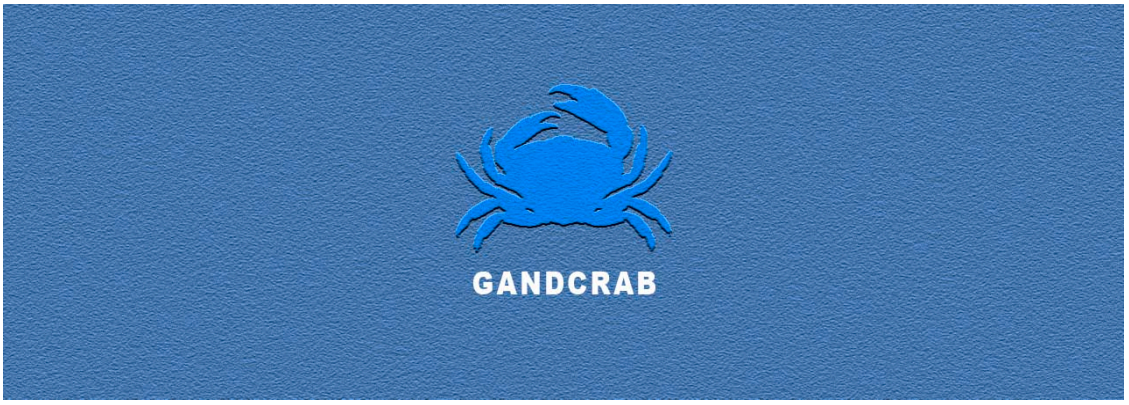
GandCrab Ransomware Shutting Down After Claiming to Earn $2 Billion

By Lawrence Abrams

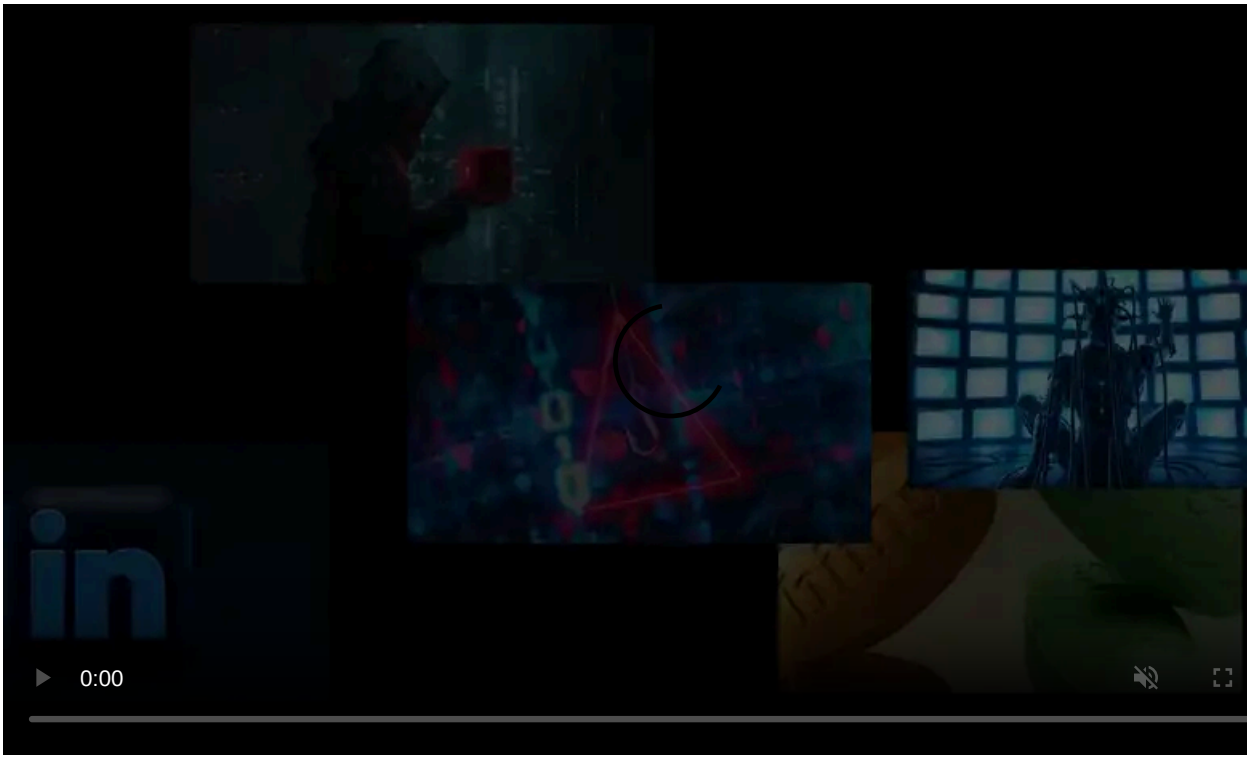
Published: 2019-06-01 · Archived: 2026-04-05 17:15:54 UTC

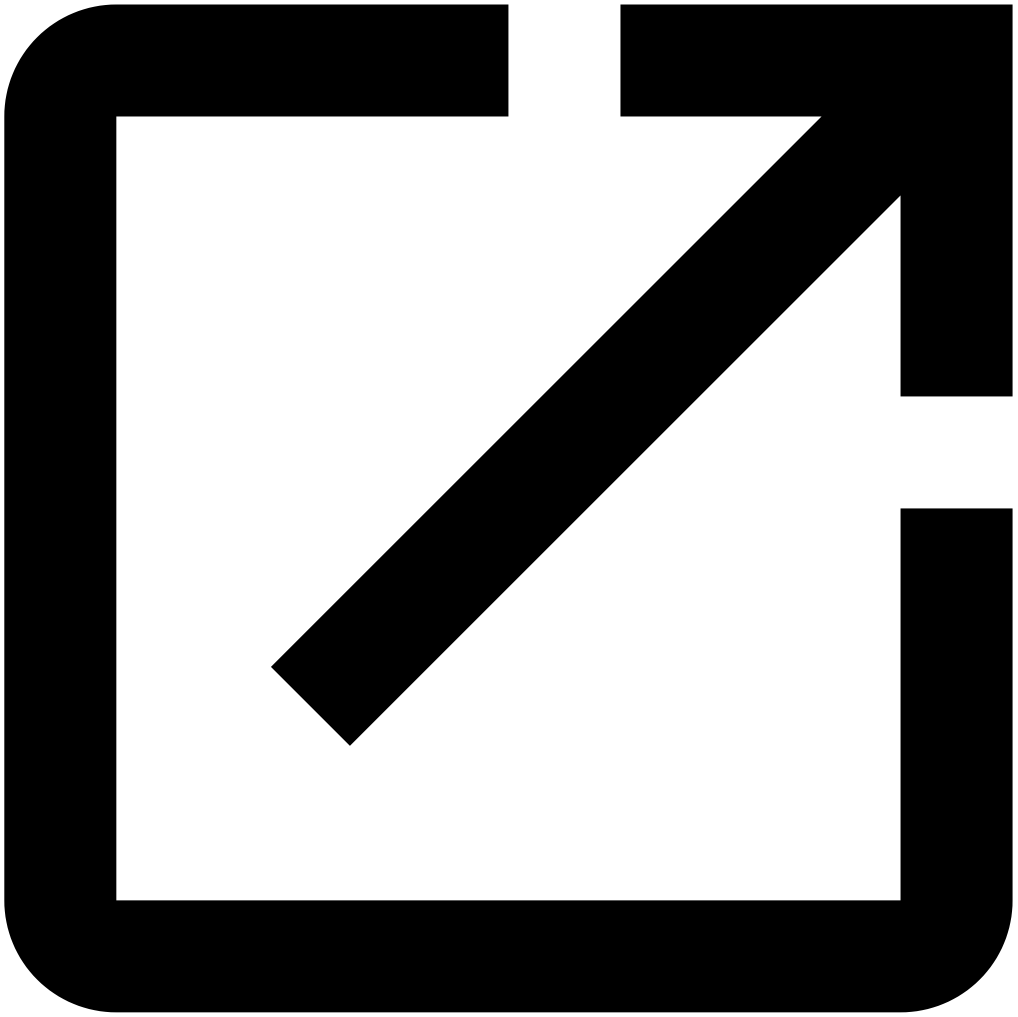


After almost a year and a half, the operators behind the GandCrab Ransomware are shutting down their operation and affiliates are being told to stop distributing the ransomware.

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.

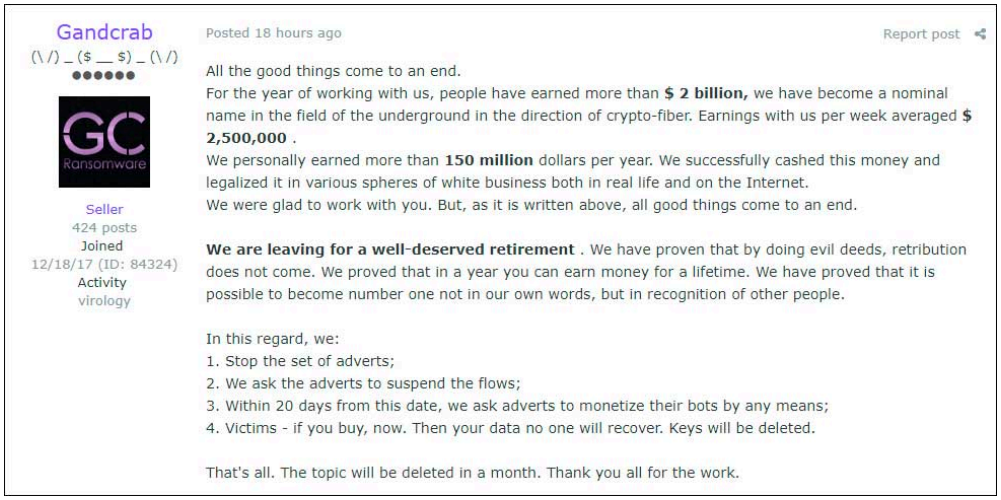
Since then, they had become one of the dominant, if not the most dominant, actors in ransomware operations, with their operations only starting to slow down over the past few months.


0:00



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 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 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.

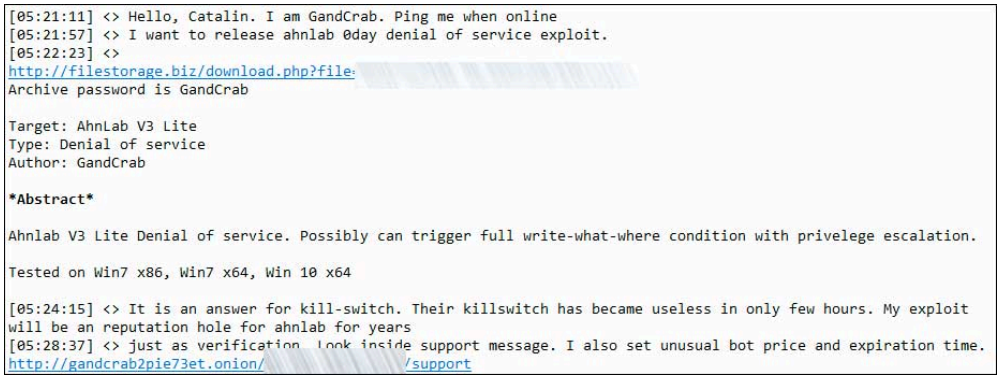
Using taunts, jokes, and references to organizations and researchers in their code, it was obvious that the GandCrab developers were monitoring us as much as we were monitoring them and got a big kick out of it.

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
```

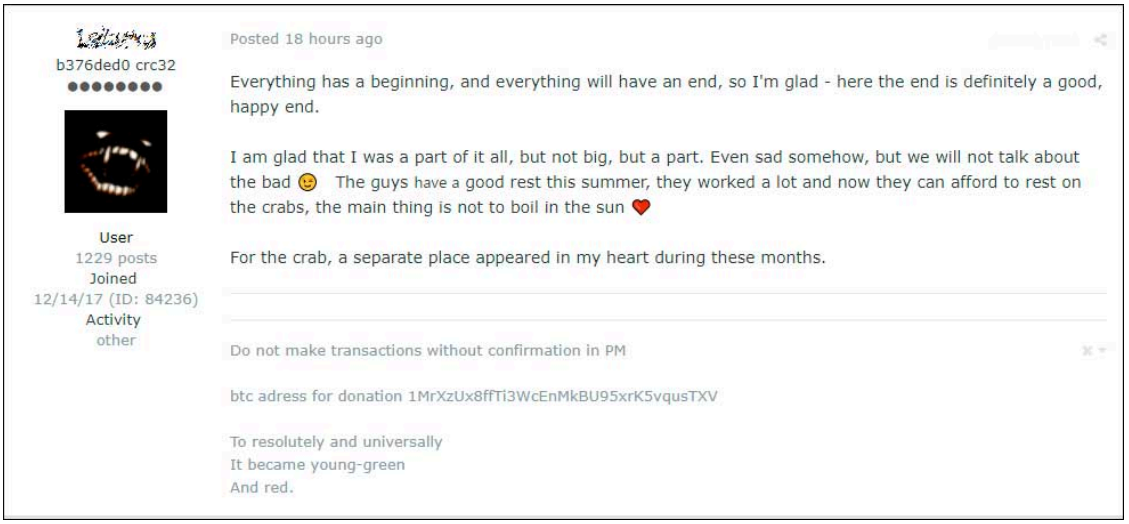
They also frequently dropped hellos to researchers who analyzed their ransomware.

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.

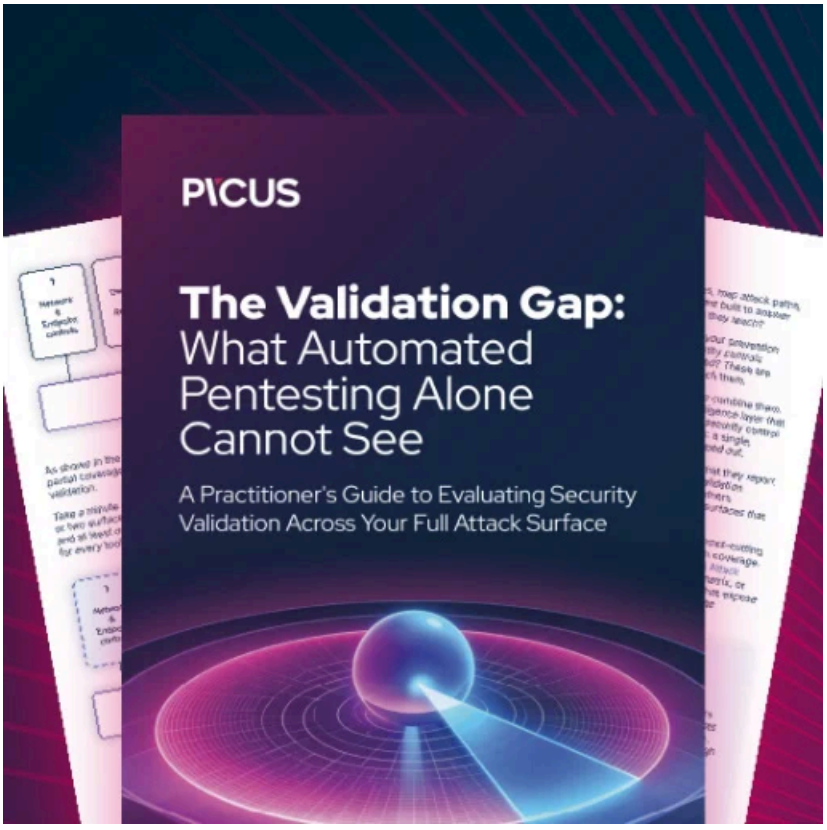


Caption

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.



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.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
