GandCrab ransomware operator arrested in Belarus

By Ionut Ilascu

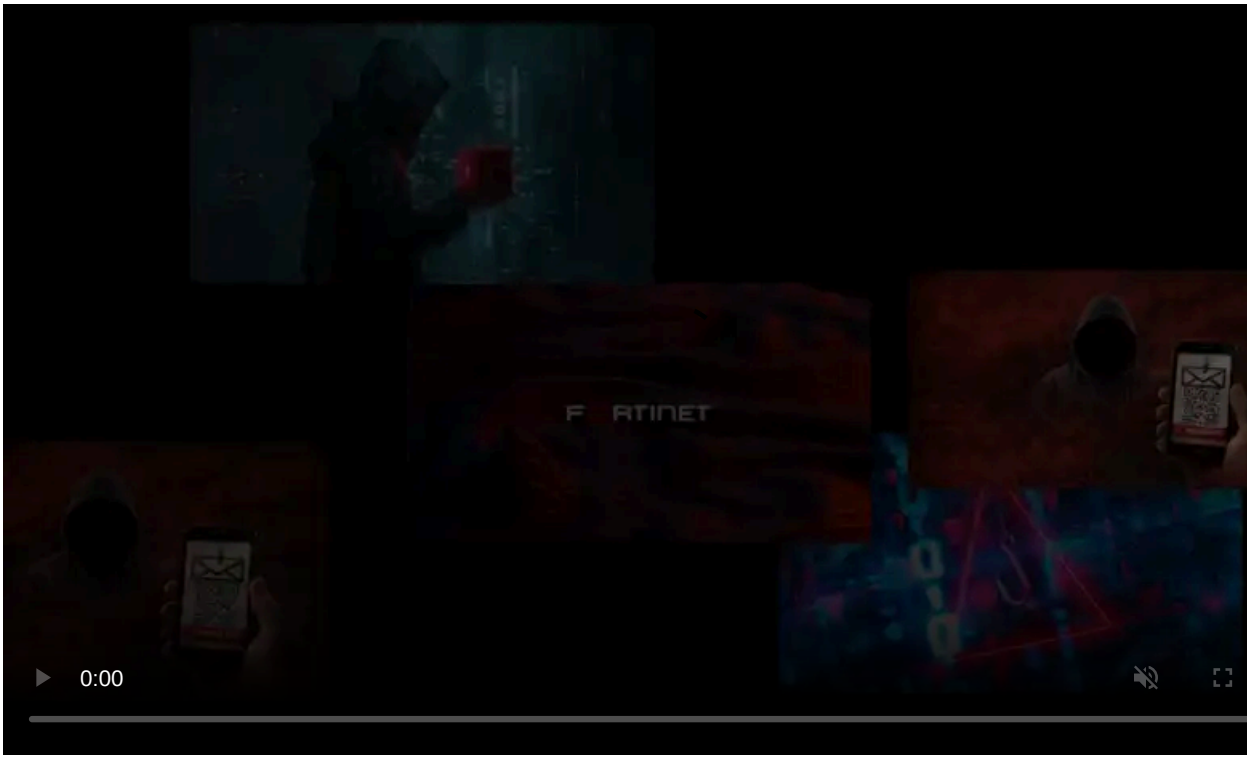
Published: 2020-07-31 · Archived: 2026-04-05 21:03:33 UTC

An affiliate of the GandCrab ransomware-as-a-business (RaaS) has been arrested, according to an official release. Authorities were able to identify the individual in cooperation with law enforcement in Romania and the U.K.

The cybercriminal's identity has not been published but Office "K" of the Ministry of Internal Affairs in Belarus says that he is a 31-years old living in Gomel, a city in southeastern Belarus.

Encrypted computers in nearly 100 countries

The arrested GandCrab member was an affiliate, or 'Advert', for the organization and was responsible for distributing the ransomware to victims.


F RTINET
0:00

"It was established that a 31-year-old resident of Gomel who had no previous convictions infected more than a thousand computers. For decrypting each of them, he demanded an amount equivalent to 1.2 thousand US dollars. Access to the admin panel for managing the ransomware botnet was carried out via the darknet, which allowed the attacker to remain anonymous for a long time," said Vladimir Zaitsev, Deputy Head of the High-Tech Crimes Department of the Ministry of Internal Affairs.

"Part of the profit was transferred to the administrators (operators) of the server he leased. The victims of the hacker were users from almost a hundred countries, and the largest number of victims were in India, the USA, Ukraine, Great Britain, Germany, France, Italy and Russia," Zaitsev added.

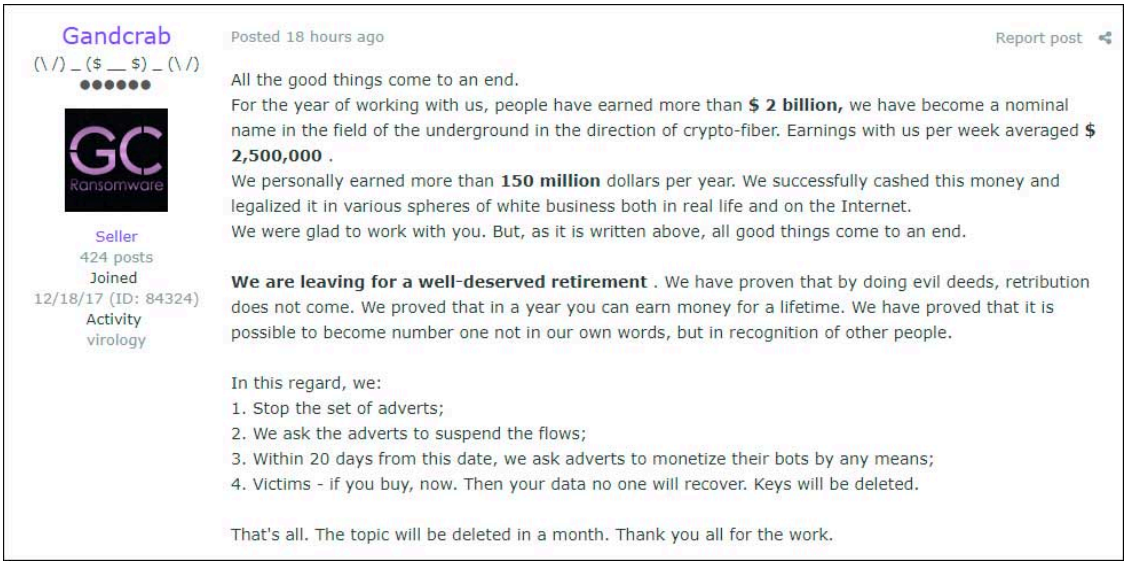
It is unclear how much money the criminal made from this operation but he shared part of the paid ransoms with GandCrab administrator(s) who kept a server hidden in the darknet, allowing affiliates to remain hidden.

As part of their role of infecting victims, GandCrab affiliates would earn 60% for the first three ransom payments they are responsible for. After the third payment, their revenue share would jump to 70%.

This means if the arrested affiliate was demanding $1,200 as a ransom payment, they would earn $840 per victim and the GandCrab developers would earn $360.

Larger affiliates who demanded millions of dollars would stand to make far greater amounts of payments.

GandCrab shut down their operation on June 1st, 2019, after claiming to have generated more than $2 billion in ransom payments and personally earning $150 million.



Gandcrab
(\ /) _ ($ __ $) _ (\ /)

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

Posted 18 hours ago — Report post

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.

After GandCrab was shutdown, the FBI released the master decryption keys for the ransomware and BitDefender released a decryptor that allowed victims to recover their files for free.

It is not known how law enforcement obtained these keys, but it could have been through a seizure of one of the Tor payment servers.

After GrandCrab shut down, another ransomware variant called REvil, or Sodinokibi, was created to fill the void left behind.

It has been reported that there are code similarities and ties between the operators/affiliates of REvil ransomware and GandCrab.
