GandCrab ransomware operation says it's shutting down

By Written by Catalin Cimpanu, ContributorContributor June 1, 2019 at 2:22 a.m. PT

See als

-

The creators of the GandCrab ransomware announced yesterday they were shutting down their Ransomware-as-a-Service (RaaS) operation, *ZDNet* has learned.

The GandCrab RaaS is an online portal where crooks sign up and pay to get access to custom builds of the GandCrab ransomware, which they later distribute via email spam, exploit kits, or other means.

When an infected user pays a ransom demand, the original GandCrab author earns a small commission, while the rest of the money goes to the crook who distributed the ransomware.

Retirement plans

Yesterday night, a source in the malware community has told ZDNet that the GandCrab RaaS operator formally announced plans to shut down their service within a month.

The announcement was made in an official thread on a well-known hacking forum, where the GandCrab RaaS has advertised its service since January 2018, when it formally launched.

In the forum message, the GandCrab authors bragged about the ransomware having earned over $2 billion in ransom payments, with the operators making roughly $2.5 million per week and $150 million per year. *It goes without saying that these numbers should be taken with a grain of salt.*

"We successfully cashed this money and legalized it in various spheres of white business both in real life and on the Internet," the GandCrab crew bragged.

"We are leaving for a well-deserved retirement," they said. "We have proved that by doing evil deeds, retribution does not come."


GandCrab forum ad

Our source tells *ZDNet* that this was the last step in a process that started earlier this week when the GandCrab crew announced RaaS customers via private emails about plans to shut down the service.

Renters of the GandCrab ransomware were told to wind down operations and cash out within the next month.

Plans to delete decryption keys

The forum thread also leaves an ominous message for GandCrab victims, as the GandCrab RaaS operators said they were planning to delete all decryption keys, making file recovery for infected victims impossible.

Some of the security researchers we approached have told ZDNet this could be a ploy to make victims panic and pay the ransom demand. However, they shifted their views when they learned that GandCrab RaaS customers were also told to wind down operations.

In the past, when ransomware operations have shut down, they usually tended to release all victim decryption keys for free so that users could recover their data. Something like this happened for victims of ransomware families such as TeslaCrypt, XData, Crysis, and FilesLocker.

Even the GandCrab crew showed some compassion in the past by releasing free decryption keys for all users infected in war-torn Syria.

GandCrab was on the decline

A chart shared with *ZDNet* by Michael Gillespie -- the creator of ID-Ransomware, a service that lets ransomware victims identify the type of ransomware that has infected their systems -- shows a steady decline in GandCrab activity this month.


GandCrab IDR stats
Image: Michael Gillespie

The chart shows that GandCrab was losing customers even before the shutdown announcement.

Security

-
-
-
-

Over the past year, the GandCrab ransomware family has been one of the most active ransomware threats around. It was one of the few ransomware strains that were being mass-distributed via email spam and exploit kits, but

also as part of targeted attacks against high-profile organizations (a tactic known as big-game hunting) at the same time.

The ransomware has seen frequent updates and is currently at version 5.2, at the time of today's shutdown.

Cyber-security firm Bitdefender released GandCrab decryptors on three occasions over the past year. These are apps that allow victims to recover encrypted files without paying the ransom. The last one was released in February this year and could decrypt GandCrab versions up to version 5.1 (with the exemption of v2 and v3).

The GandCrab author also had a spat with South Korean security vendor AhnLab last summer after the security firm released a vaccine for the GandCrab ransomware. As retaliation, they included a zero-day for the AhnLab antivirus in the GandCrab code.

Recently, Sophos Labs has observed criminal groups scanning the internet for open MySQL databases running on Windows systems, which they tried to infect with GandCrab. Probably the most high-profile attack that GandCrab was behind is a series of infections at customers of remote IT support firms in the month of February.

If the GandCrab crew follows through on their plans and actually shuts down, their legacy remains as one of a ransomware strain that has dominated the ransomware landscape in the second half of 2018 and the first half of 2019, when it was, by far, the most active strain on the market.

Cybercrime and malware, 2019 predictions

Related malware and cybercrime coverage:

- Emotet is dominating the malicious threat landscape in 2019
- CEO who sold encrypted phones to criminal gangs gets nine years in prison
- New HiddenWasp malware found targeting Linux systems
- Hackers are scanning for MySQL servers to deploy GandCrab ransomware
- I2P network proposed as the next hiding spot for criminal operations
- Company behind LeakedSource pleads guilty in Canada
- The dark web is smaller, and may be less dangerous, than we think **TechRepublic**
- Game of Thrones has the most malware of any pirated TV show **CNET**
