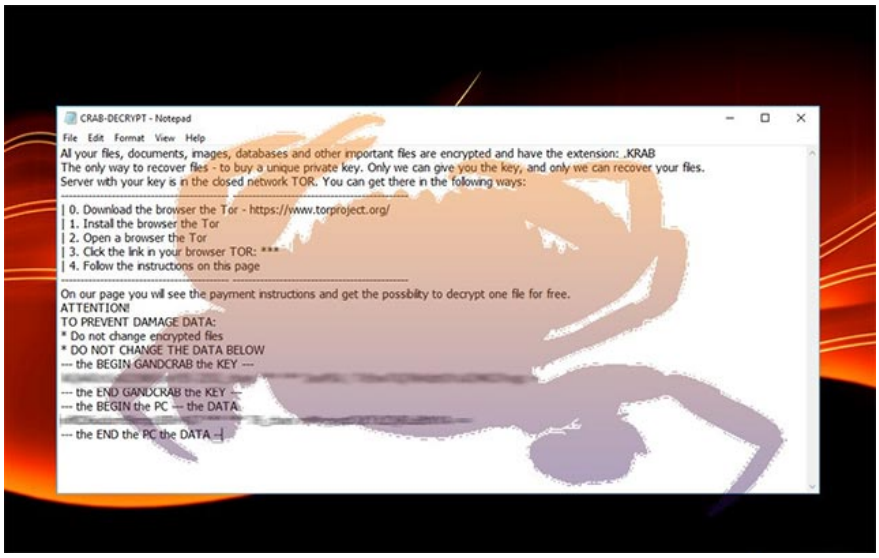
GandCrab blackmail extinguished after earning $ 2.5 billion worldwide

After nearly a year and a half of 'storming', the people behind GandCrab ransomware claimed that the malware stopped working and at the same time urged their malicious 'branches' to stop distributing this extortion code. .

GandCrab is a blackmail (ransomware) distributed through the RIG vulnerability exploit toolkit. When infected, the files in the computer are encrypted into a * .GDCB or * .CRAB file. The malicious code will then generate a required CRAB-DECRYPT.txt file and instruct the user to pay the ransom from $ 400-1,000 by DASH electronic payment to decrypt the data.

After nearly a year and a half of 'storming', the people behind GandCrab ransomware claimed that the malware stopped working and at the same time urged their malicious 'branches' to stop distributing this extortion code. .



1. Warning: Detecting a campaign to spread malicious code GandCrab 5.2 into Vietnam via fake email of the Ministry of Public Security

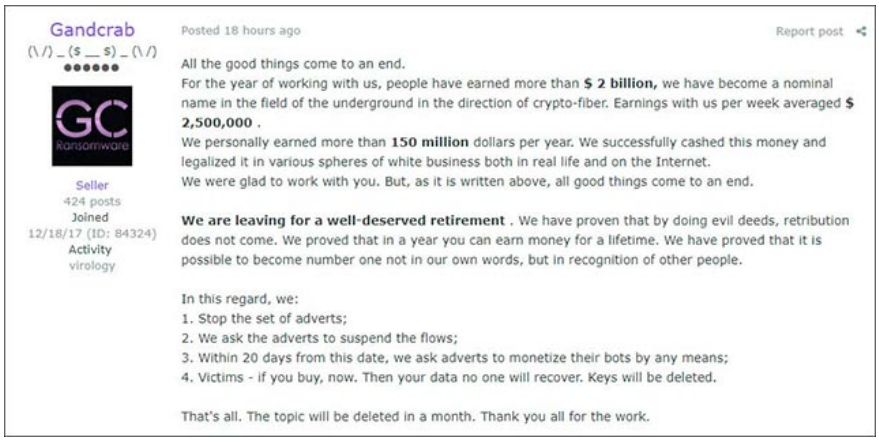
Appearing as an option to fill significant gaps in the world of extortion blackmail code left behind after large-scale ransomware operations like TeslaCrypt, CryptoWall and Spora shut down, GandCrab has 'sent greetings'. 'to the internet world on January 28, 2018, and soon developed booming soon after the attackers began to promote their services on underground, black web sites.

Since then, GandCrab has become one of the dominant names, causing obsession for all networked computer systems worldwide. It is not unusual to assume that GandCrab is the most dominant name, in the overall ransomware activities over the past 1 year. The operation of extortion malware only began to show signs of

cooling in the past few months when the attackers had pocketed a decent amount of money.

According to a recent finding by two experienced security researchers Damian and David Montenegro - who have followed GandCrab exploits since the malware invites to appear, on the hack and malicious software forum. Exploit.in, GandCrab hackers have posted content that says they are gradually ceasing GandCrab completely in the near future.

According to the contents of the screenshot provided by Damian for the BleepingComputer technology site, it can be seen that the guys behind GandCrab said they earned a total of more than $ 2 billion from the malicious code through the accounts. Paying the victim's ransom, in which GandCrab, on average, helps these guys pocket about $ 2.5 million a week. More specifically, $ 150 million of which has been cashed and successfully "washed" through investing in legitimate business projects.



1. Hacker attacks a US city demanding $ 100,000 ransom with Bitcoin

Also in this announcement, the authors of GandCrab said they had stopped promoting the ransomware, asking branches to stop distributing malicious code GandCrab within 20 days and requesting to remove all related topics at the end of the month. this.

Besides, attackers also do not forget to give the 'final' warning to the victims who are still hesitant to pay the ransom that they will have to pay for the necessary data decryption right now. because the decryption keys for their data will be deleted at the end of the month, meaning that the victim's encrypted data will be forever 'gone into the past'. This may be the final claim and hope that GandCrab developers will follow other major

ransomware activities and release decryption keys before officially stopping.

Historically, the field of network security has seen many cases of large-scale ransomware activities appearing to replace, the remaining space when a large ransomware has just stopped working. Therefore, it is not surprising to see another ransom attack 'sprouting' in the near future after GandCrab disappears, especially when the guys behind this malicious code have also launched The words 'note' are as follows:

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

(Interpretation: We have pointed out the fact that please rest assured to do the things you want, including bad behavior, violating the law, because cause and effect are not real. ')

Yes, if this is a nice retreat of GandCrab, after causing huge losses of up to $ 2.5 billion worldwide, they have the right to gloat with the above judgment!

1. Discovery of Trojan scattering steals virtual money through YouTube

Huge amount of money was pocketed

It is true that the people behind GandCrab may have made a lot of money after this mission, but there is no guarantee that they can get that much money. The $ 2.5 figure will of course need to be verified.

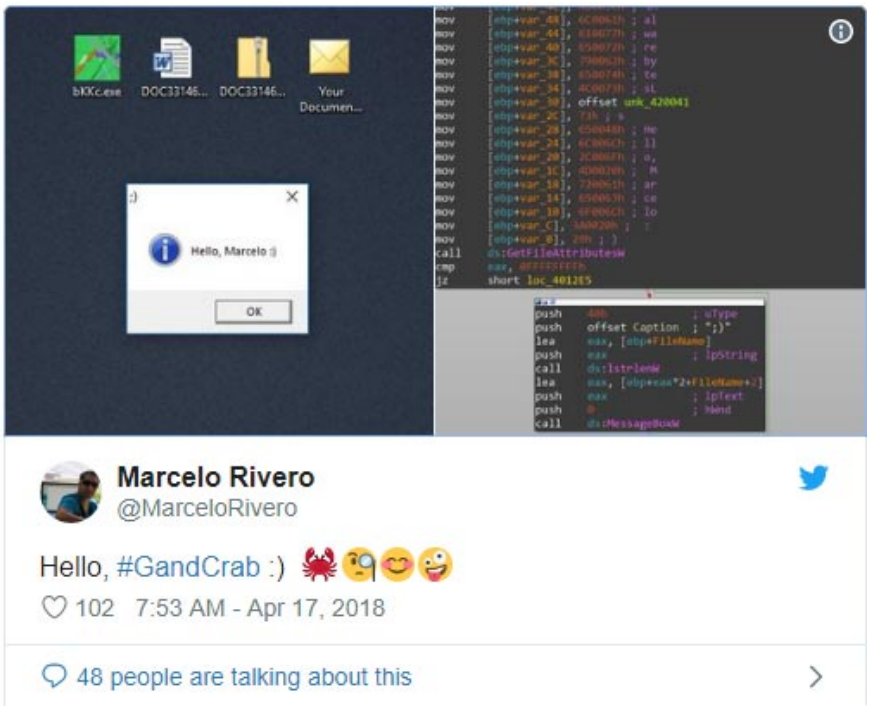
The claims of this "strong" part are absolutely not surprising because GrandCrab developers have always been jokes, and that has drawn the attention of many security researchers. worldwide in the way that most malware developers have not or do not.

By using mockery, jokes and references to organizations and many of their well-known security researchers in the malicious code, it is clear that the people behind GandCrab have followed the experts on security. The secret is as much as the way experts pay attention to them, and this has contributed to 'inspiring' the attacker.

For example, in the first release of ransomware GandCrab, malicious developers decided to use domain names for their Command & Control (C2 server) servers based on organizations and websites that were supposedly is studying or most concerned about this ransomware as a 'challenge', including:

1. bleepingcomputer.bit
2. nomoreransom.bit
3. esetnod32.bit
4. emsisoft.bit
5. gandcrab.bit

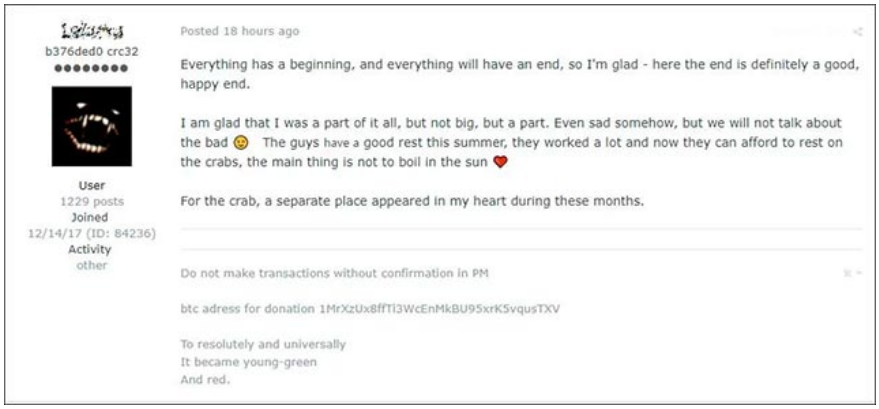
In addition, they regularly send 'cordial greetings' to security researchers who have been closely monitoring their ransomware.



1. [Infographic] 7 effective ways to protect businesses from Ransomware

But this is absolutely not a fun game of 'hide and seek'. The people behind GandCrab also had some retaliation against security teams. After AhnLab released 'vaccine application' for GandCrab, the attackers immediately contacted BleepingComputer to disclose information that they had released a zero-day targeting AhnLab v3 antivirus program. Lite - a real response 'has weight'.

However, the antics and even the success of GandCrab were not noticed by other members of Exploit.in, with many conflicting emotions about the event that the malicious code stopped working.



1. The cybersecurity tools that every business should know

Although GandCrab jokes can be amusing in some situations, the loss, trouble and even the suffering it inflicts on victims - these malicious people take data and work. work and may be a lifelong business. After all, GandCrab, or any other ransomware, stops working is a good thing for humanity.