NOT SO CRAB MENTALITY
“A TRUE RAAS STORY”

CHRISTOPHER C. ELISAN
About Me

- Senior Malware Researcher @FlashpointIntel
- Past Adventures
  - RSA
  - Damballa
  - F-Secure
  - Trend Micro
- @Tophs
Author Of...

MALWARE, ROOTKITS & BOTNETS
Christopher C. Elisan

Advanced Malware Analysis
Christopher Elisan

Lab Setup and Top Tier Tools for Analysis & Reporting
Co-Author Of...
SAM is back

I'm high on life.
Ben has a new gig...

I need cash for Valentine’s…
Saw this work from home gig…
Wanna get in on the action?

What is it?
Recruitment

Отписался в ПМ.

Уточните пару моментов:

Партнёрам отдавать на Вашу сторону 60 - 40%.

Чистота скан-и рантайм будет поддерживаться? (для меня это большой вопрос.)

Наконец-то люди стали переводить на безопасную крипту

Сообщение отредактировал 29.01.2018, 18:27

**TERMS OF SERVICE AND RULES OF THE PARTNERSHIP PROGRAM:**

1. We work 60%-40% with major partners able to increase their percentage up to 70%.
2. Carry out installations through hacks and spam, or else through quality, usable traffic from traffic market** (we aren't interested in a world mix or India).
3. We reserve right to refuse service to anyone for any reason.
4. Free support between PayPal and Admins || Victims and PayPal (ticket)
5. We do not provide exploit kits or other methods of delivering downloads

*traffic exchange will be considered after a detailed conversation

1. Do not upload the .exe file to unverified antivirus scanners (which will send the sample to antivirus labs)
2. Do not make any attempts to operate the ransomware in countries in the Commonwealth of Independent States
3. Do not post the .onion address of the control panel anywhere
4. Do not transfer the account to a third party

If any of these rules are violated, the account will be deleted without any further payments made.

Attention! We are recruiting a limited number of participants and will stop taking on new partners until new free spots become available.

Please send your application via private message with a description of your sources and quantity of load/traffic per 24 hours.

Respectfully, GandCrab team
Bad Idea...

THAT’S NOT LEGIT.. THAT’S RAAS!!!
**Ransomware-as-a-Service**

- Makes cybercrime accessible to the masses
- Malware authors create the ransomware and make it available to download and use for free, for an upfront fee, or for partnership
- Programming skill is not needed to be successful

Image Source: Trend Micro
Three months later...

I NEED CASH FOR SUMMER VACAY...
SAW THIS WORK FROM HOME GIG...
WANNA GET IN ON THE ACTION? 
WHAT IS IT?
[I have] ransomware. I am responsible for making the malware evade anti-virus software, you will be responsible for spreading it. (Looking for a highly-skilled partner to cooperate with).

The name of the ransomware is [GandCrab].
[For more in-depth information,] please see the reporting from below.

https://www[.]hackeye.net/securitytechnology/netsec/12140.aspx
https://www[.]hackeye[.]net/threatintelligence/12530.aspx
http://www[.]freebuf[.]com/column/162254.html

Searching for high-skilled [malware] spreaders.
[Profits will be split] 60 percent/40 percent
[If there are high profits then the split] will be raised to 70 percent/30 percent

You do not have to worry about malware coding, evading anti-virus systems and so on. All you need to do is spread the malware.
Bad Idea... again...

WHERE ARE YOU GETTING THESE POSTINGS?
SHOW ME!!!
DDW Forum

CHECK OUT THIS FORUM
Backend
### Bots

<table>
<thead>
<tr>
<th>Country</th>
<th>IP</th>
<th>Bot</th>
<th>Sub</th>
<th>Trial</th>
<th>Encrypted?</th>
<th>Visits</th>
<th>Amount</th>
<th>Payoff</th>
<th>RegDate</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN</td>
<td>256c655358a65a3c84</td>
<td>100</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$100.00</td>
<td>No</td>
<td>1 day ago</td>
</tr>
<tr>
<td>CN</td>
<td>9808d837a4a88f1e</td>
<td>100</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$100.00</td>
<td>No</td>
<td>1 day ago</td>
</tr>
<tr>
<td>CN</td>
<td>67c6b5108d3a3d17</td>
<td>100</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$200.00</td>
<td>No</td>
<td>1 day ago</td>
</tr>
<tr>
<td>CN</td>
<td>ab95a8e4e6a773f6</td>
<td>100</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$100.00</td>
<td>No</td>
<td>2 days ago</td>
</tr>
<tr>
<td>CN</td>
<td>99d8b051208f3cfa</td>
<td>100</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$100.00</td>
<td>No</td>
<td>2 days ago</td>
</tr>
<tr>
<td>HK</td>
<td>5e192b4c35c0b5e</td>
<td>100</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$100.00</td>
<td>No</td>
<td>2 days ago</td>
</tr>
<tr>
<td>HK</td>
<td>6217b9a9a757a93</td>
<td>100</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$100.00</td>
<td>No</td>
<td>2 days ago</td>
</tr>
<tr>
<td>IN</td>
<td>ea279414a29088b1</td>
<td>100</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$100.00</td>
<td>No</td>
<td>2 days ago</td>
</tr>
<tr>
<td>PL</td>
<td>1895a8494d444</td>
<td>100</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$100.00</td>
<td>No</td>
<td>2 days ago</td>
</tr>
<tr>
<td>CN</td>
<td>65a219d7c24532d</td>
<td>100</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$100.00</td>
<td>No</td>
<td>2 days ago</td>
</tr>
<tr>
<td>IN</td>
<td>2a1c506f54a96</td>
<td>100</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$100.00</td>
<td>No</td>
<td>2 days ago</td>
</tr>
<tr>
<td>CN</td>
<td>60d0407d0935c31</td>
<td>100</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$100.00</td>
<td>No</td>
<td>2 days ago</td>
</tr>
<tr>
<td>IT</td>
<td>e1110a68e67847e</td>
<td>100</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$100.00</td>
<td>No</td>
<td>2 days ago</td>
</tr>
<tr>
<td>IT</td>
<td>31110a30e65e34a</td>
<td>100</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$100.00</td>
<td>No</td>
<td>2 days ago</td>
</tr>
<tr>
<td>CN</td>
<td>38d94a80500bb3</td>
<td>200</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$200.00</td>
<td>No</td>
<td>2 days ago</td>
</tr>
<tr>
<td>CN</td>
<td>68097383c7b3a214</td>
<td>200</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$200.00</td>
<td>No</td>
<td>2 days ago</td>
</tr>
<tr>
<td>CN</td>
<td>b5a677e64633e3d5</td>
<td>200</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$200.00</td>
<td>No</td>
<td>2 days ago</td>
</tr>
<tr>
<td>CN</td>
<td>17a86a6786f19b0</td>
<td>150</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
<td>$50.00</td>
<td>No</td>
<td>3 days ago</td>
</tr>
</tbody>
</table>
SAM vs GandCrab
GandCrab Behavior

- Determines system information, usually to detect if the system is virtualized
- Attempts to resolve many APIs, a known technique to avoid static detection
- Connects to ipv4bot.whatismyipaddress.com to determine victim’s IP address
- Executes nslookup to determine address of C2
- Looks for documents. Photos, databases and other important files to encrypt
- Encrypts files and changes extension to .CRAB
- Folder where encrypted files are located contains CRAB-DECRYPT.TXT

Image Source: Bleeping Computer
import random
import string

def random_string_generator(size=10, chars=string.ascii_lowercase + string.digits):
    return ''.join(random.choice(chars) for _ in range(size))

C:\USERS\%CURRENT_USER%\APPDATA\ROAMING\MICROSOFT
GandCrab Persistency Technique

Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
Value_Name = gdinrxwldth,
Data = "C:\Users\2XC7u663GxWc\AppData\Roaming\Microsoft\agnlxz.exe"
Size = 229 KB
Type = REG_SZ
The Ransom Note

We are sorry, but your files have been encrypted!

To decrypt your files, you have to pay a ransom of 490 USD.

Files decryptor’s price is 490 USD.

Payment will be due within 24 hours. If not, the cost of decrypting files will be doubled.

Time left to double price:

01 days 23h:59m:09s

What is ransomware and how can I protect against it?

Ransomware is a type of malware that encrypts your files and demands payment in exchange for restoring access.

What can I do to get my files back?

You can use a ransomware decryptor or try to remove the ransomware from your system.

What guarantees can you give me?

We cannot guarantee the success of the ransomware decryptor.

What are they asking for payment in?

They are asking for payment in Bitcoin.

How can I pay for the decryptor?

You can pay for the decryptor using Bitcoin.
Expired Ransom Note

We are sorry, but your files have been encrypted!

Don't worry, we can help you retrieve all of your files!

Files decryptor's price is 888 USD

Amount was doubled!

Time left to double price:

00 days 00h:00m:00s

What file matter?
Your computer has been infected with GandCrab Ransomware. Your files have been encrypted and you can decrypt it by paying.
In the meanwhile, you can prepare for decryption and install anti-virus software, but once paid, you will only satisfy the ransom payment.

What can I do to get my files back?
You need to buy GandCrab Decryptor. This software will help you decrypt all your encrypted files and reverse GandCrab on your PC.
Current price: 888 USD. As payment, you need cryptocurrency, such as Bitcoin.

What guarantees can you give to me?
Your paid anti-virus software and decryptor files for free.

What is cryptocurrency and how can I purchase GandCrab Decryptor?
You can read more about it here. Some guarantees are given.
Payment Method
24/7 Support
Try Before You Buy
There is a solution...
GandCrab and other Ransomware Decryption Tools

HTTPS://WWW.NOMORERANSOM.ORG/EN/DECRYPTION-TOOLS.HTML

NO MORE RANSOM!
As for Ben...