FLASHPOINT

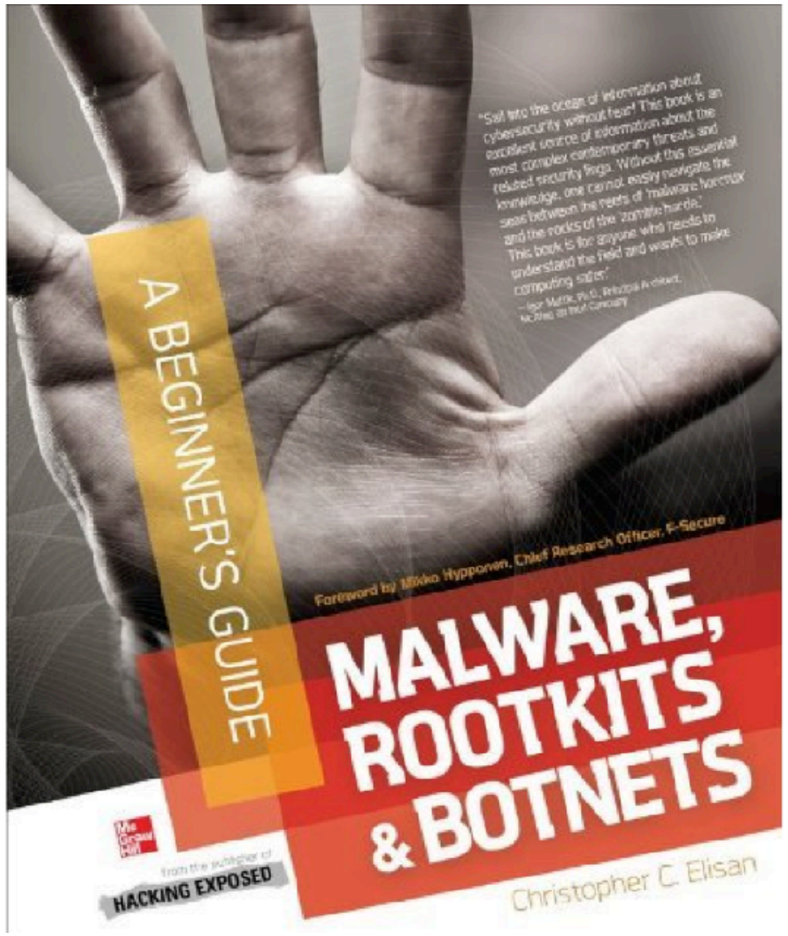
NOT SO CRAB MENTALITY
"A TRUE RAAS STORY"

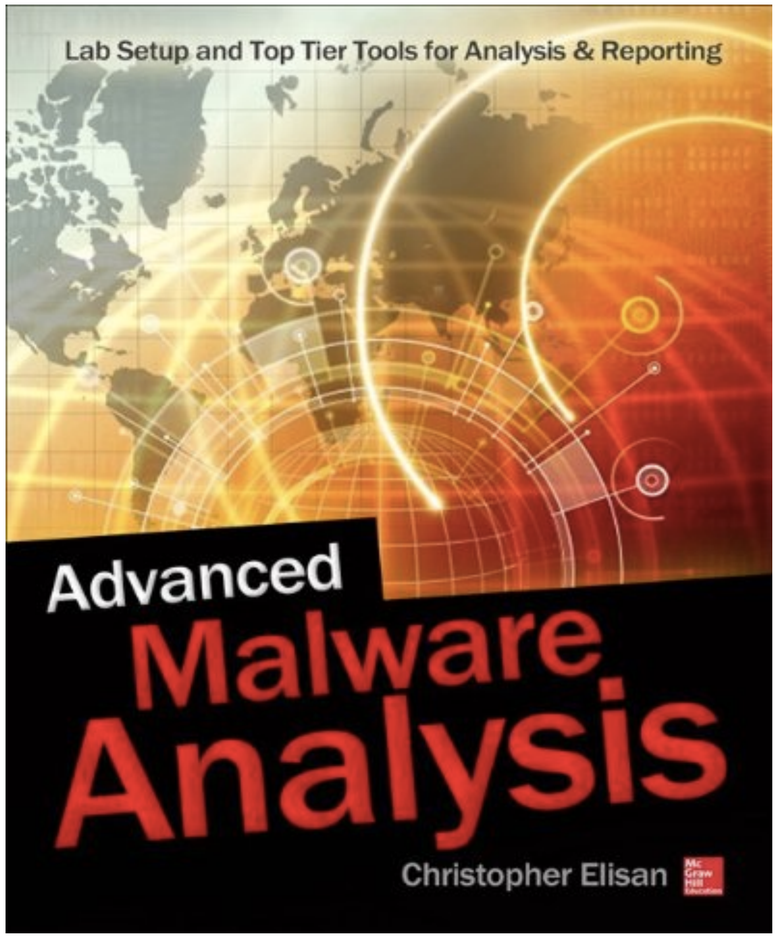
CHRISTOPHER C. ELISAN

About Me

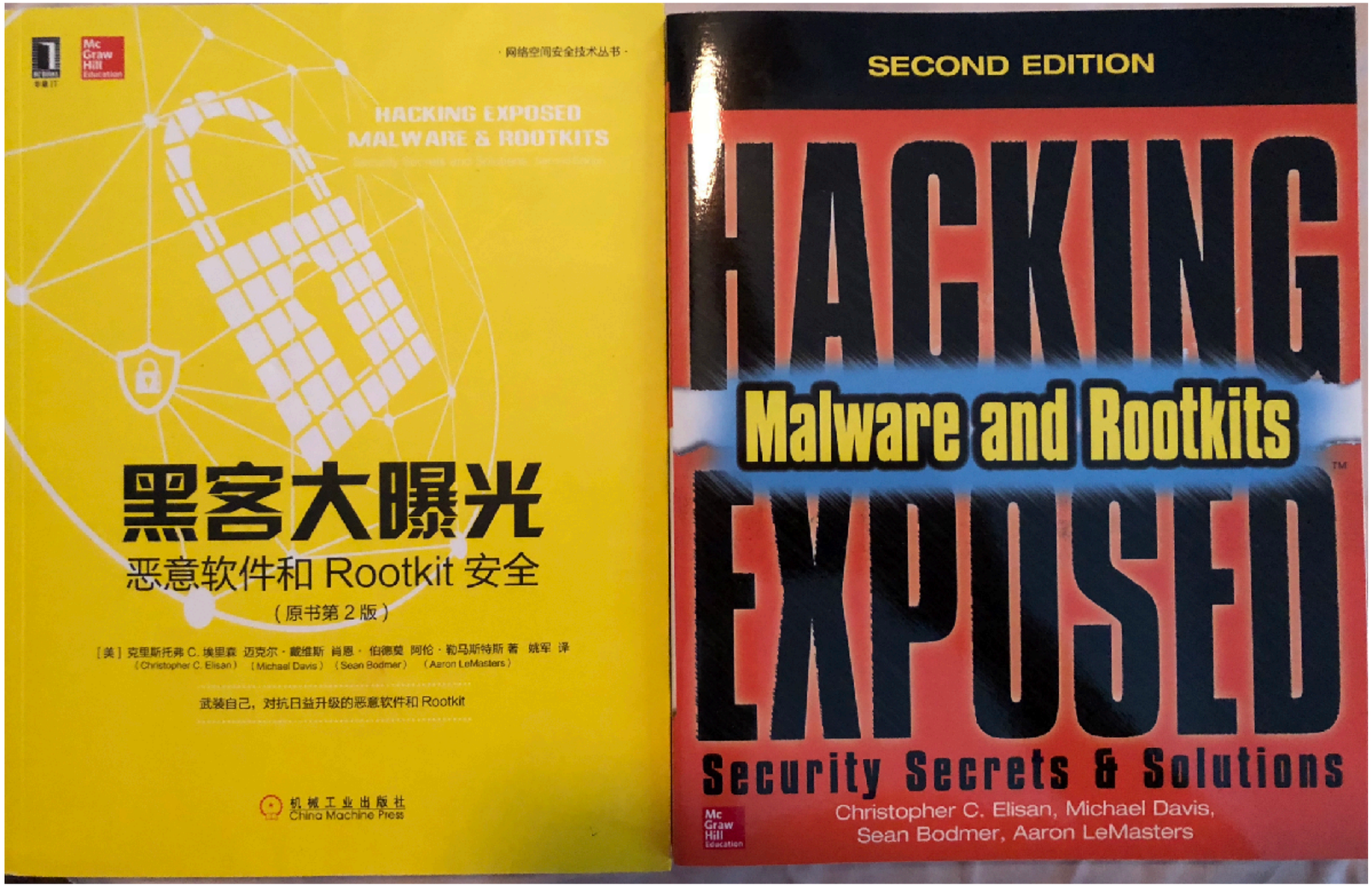
- Senior Malware Researcher @FlashpointIntel
- Past Adventures
  - RSA
  - Damballa
  - F-Secure
  - Trend Micro
- @Tophs

Author Of...


A BEGINNER'S GUIDE
Foreword by Mikko Hypponen, Chief Research Officer, F-Secure
MALWARE, ROOTKITS & BOTNETS
Christopher C. Elisan
HACKING EXPOSED


Lab Setup and Top Tier Tools for Analysis & Reporting
Advanced
Malware Analysis
Christopher Elisan

Co-Author Of...

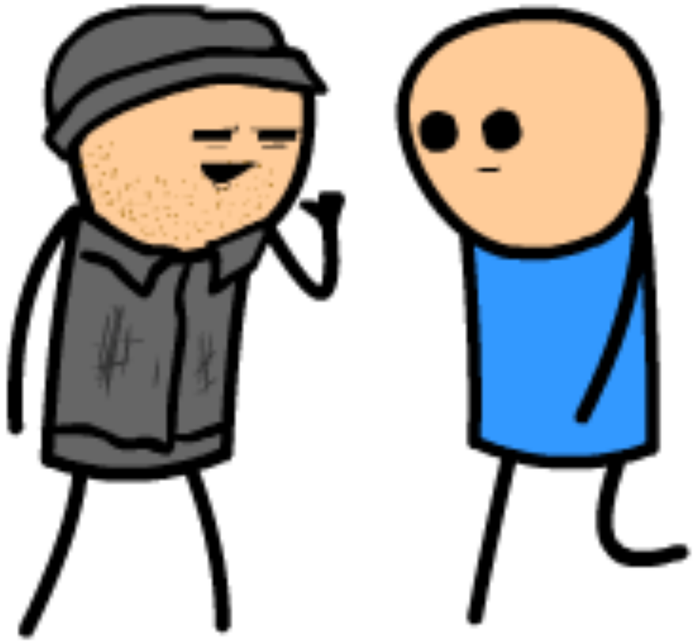

· 网络空间安全技术丛书 ·
HACKING EXPOSED
MALWARE & ROOTKITS
黑客大曝光
恶意软件和 Rootkit 安全
（原书第 2 版）
[美] 克里斯托弗 C. 埃里森 迈克尔·戴维斯 肖恩·伯德莫 阿伦·勒马斯特斯 著 姚军 译
（Christopher C. Elisan） （Michael Davis） （Sean Bodmer） （Aaron LeMasters）
武装自己，对抗日益升级的恶意软件和 Rootkit
机械工业出版社
China Machine Press
SECOND EDITION
HACKING
Malware and Rootkits
EXPOSED
Security Secrets & Solutions
Christopher C. Elisan, Michael Davis,
Sean Bodmer, Aaron LeMasters

SAM is back

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

on January 29, 2018 13:19 UTC

Отписался в ПМ.

Уточните пару моментов:

Цитата
4. Бесплатная поддержка между ПП и Админами || **Жертвами и ПП (тикет)**

Т.е. переговоры с жертвой нужно будет вести самостоятельно?

Цитата
крупным партнёрам есть возможность увеличения процента в Вашу сторону до 70%;

о каких суммах идет речь?

Чистота скан- и рантайм будет поддерживаться? (для меня это больной вопрос)
Цитата
оплата Вашего % выкупа на Ваш кошелек **Dash**

Наконец-то люди стали переходить 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 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 anti-virus 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 loads/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

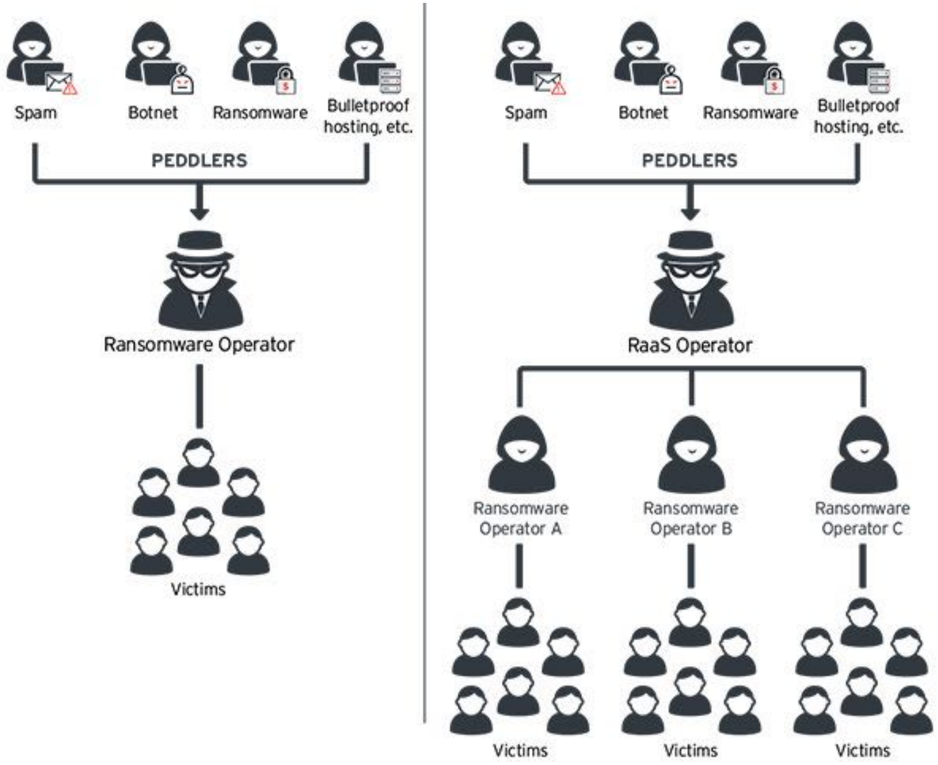
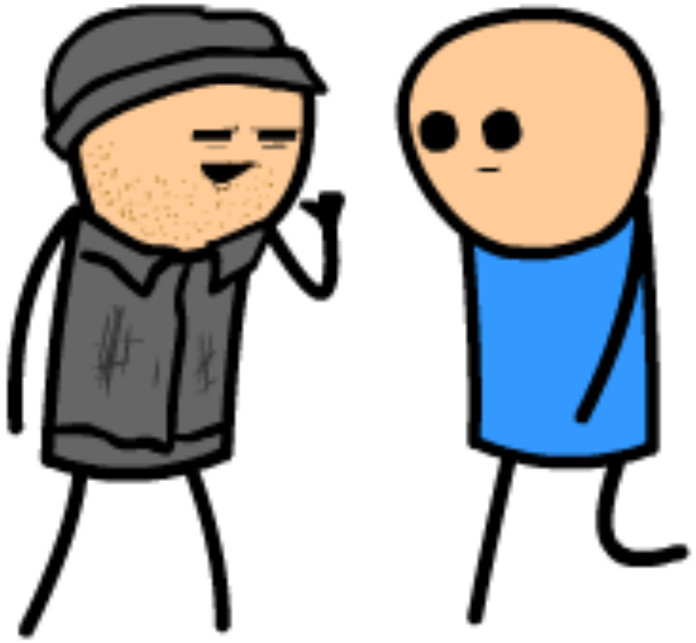


Image Source: Trend Micro

Three months later…

I NEED CASH FOR SUMMER VACAY…
SAW THIS WORK FROM HOME GIG…
WANNA GET IN ON THE ACTION?

WHAT IS IT?



Recruitment

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

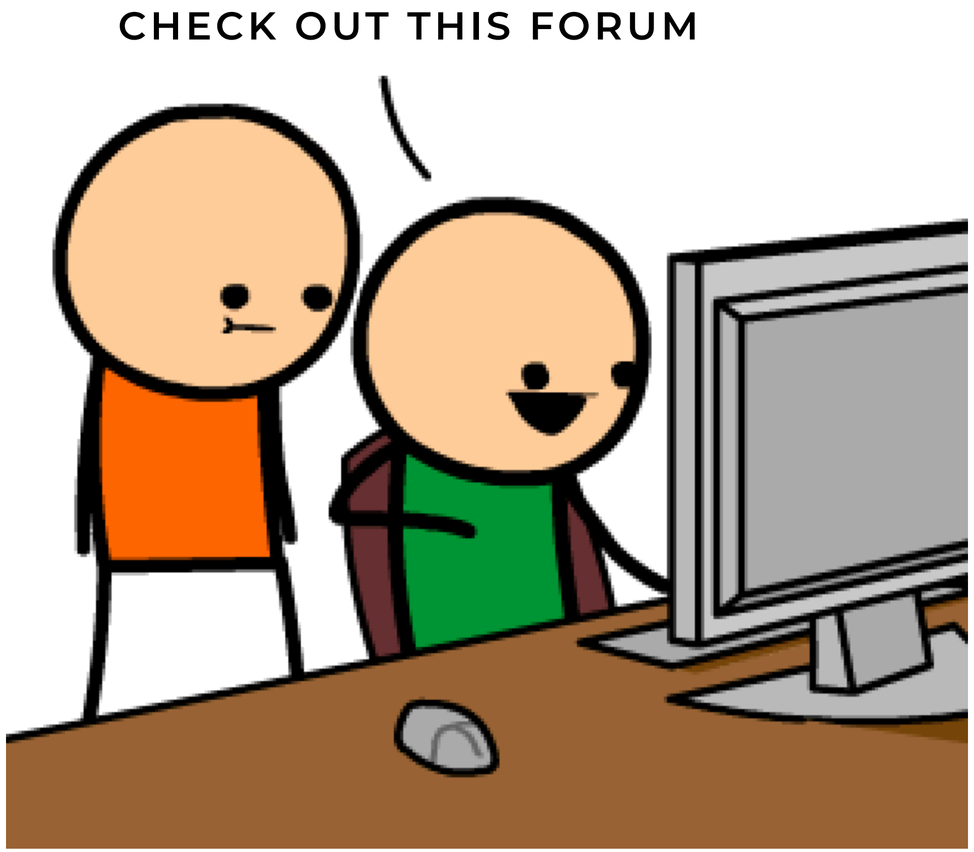
Searching for high-skilled [malware] spreaders.
[Profits will be split] 60 percent/40 percent
[If there are high profits then the split] will be raised to 70 percent/30 percent

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.

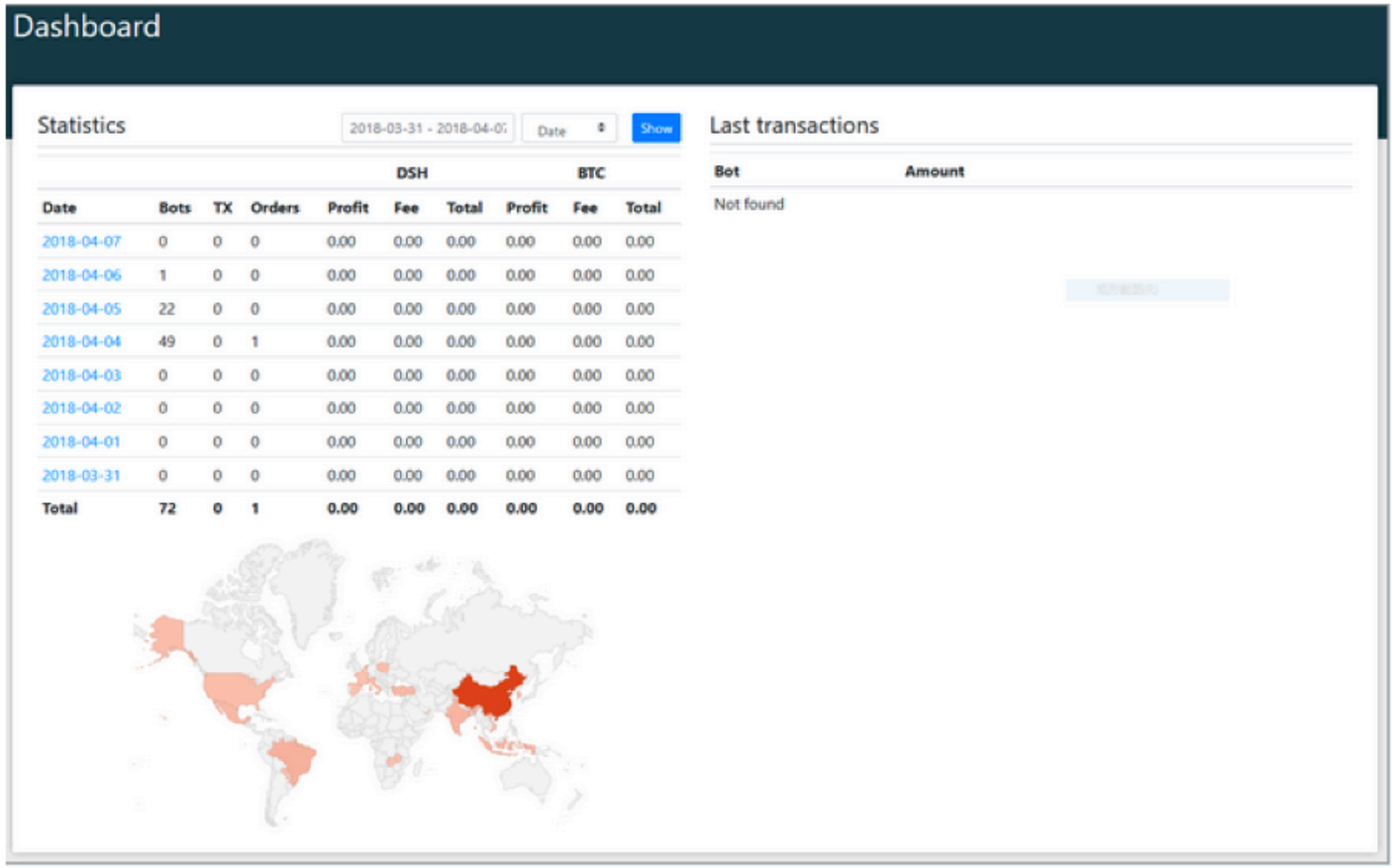
Bad Idea… again…

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

DDW Forum

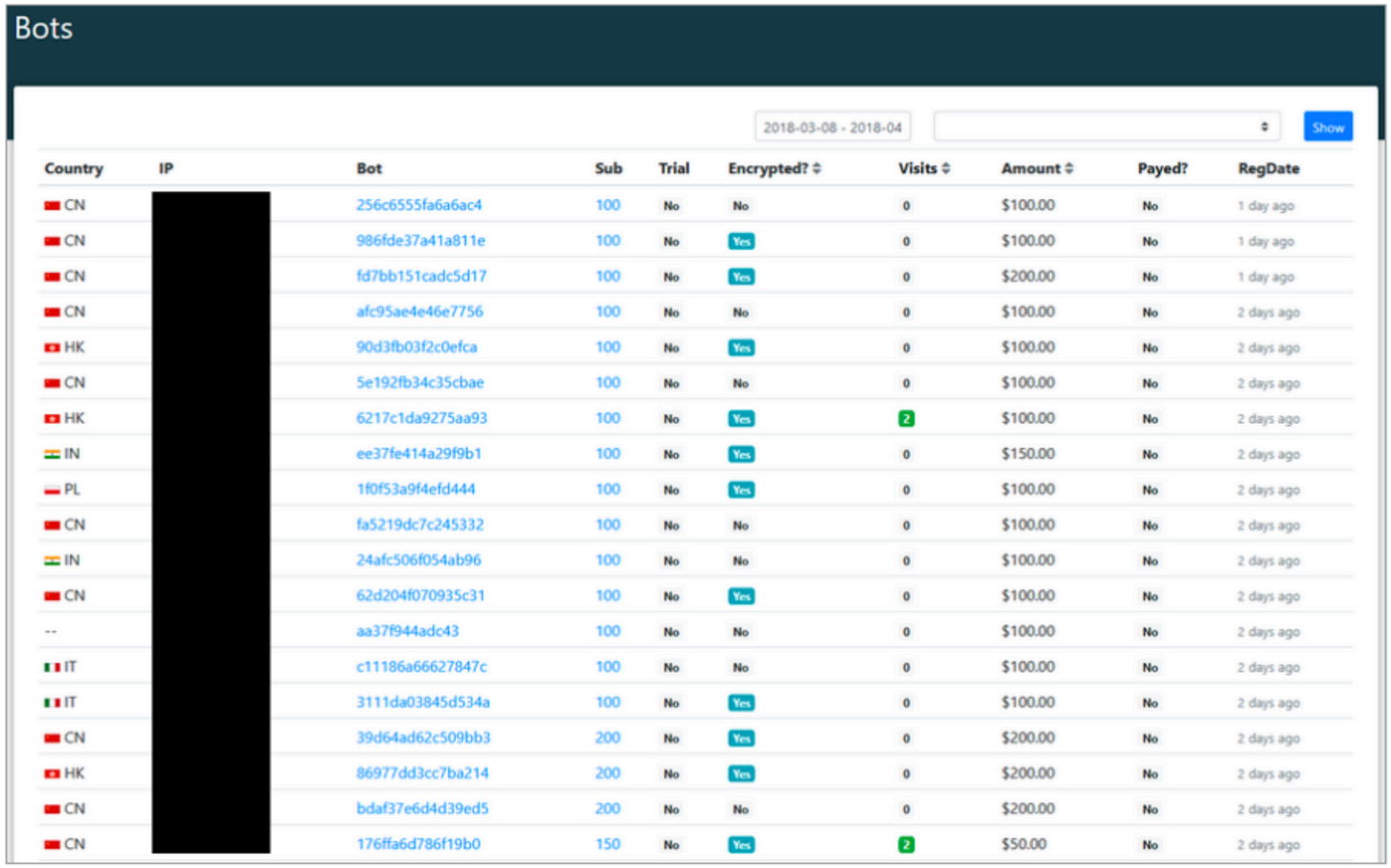


Backend



				DSH			BTC		
Date	Bots	TX	Orders	Profit	Fee	Total	Profit	Fee	Total
2018-04-07	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00
2018-04-06	1	0	0	0.00	0.00	0.00	0.00	0.00	0.00
2018-04-05	22	0	0	0.00	0.00	0.00	0.00	0.00	0.00
2018-04-04	49	0	1	0.00	0.00	0.00	0.00	0.00	0.00
2018-04-03	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00
2018-04-02	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00
2018-04-01	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00
2018-03-31	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00
Total	**72**	**0**	**1**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**

Backend

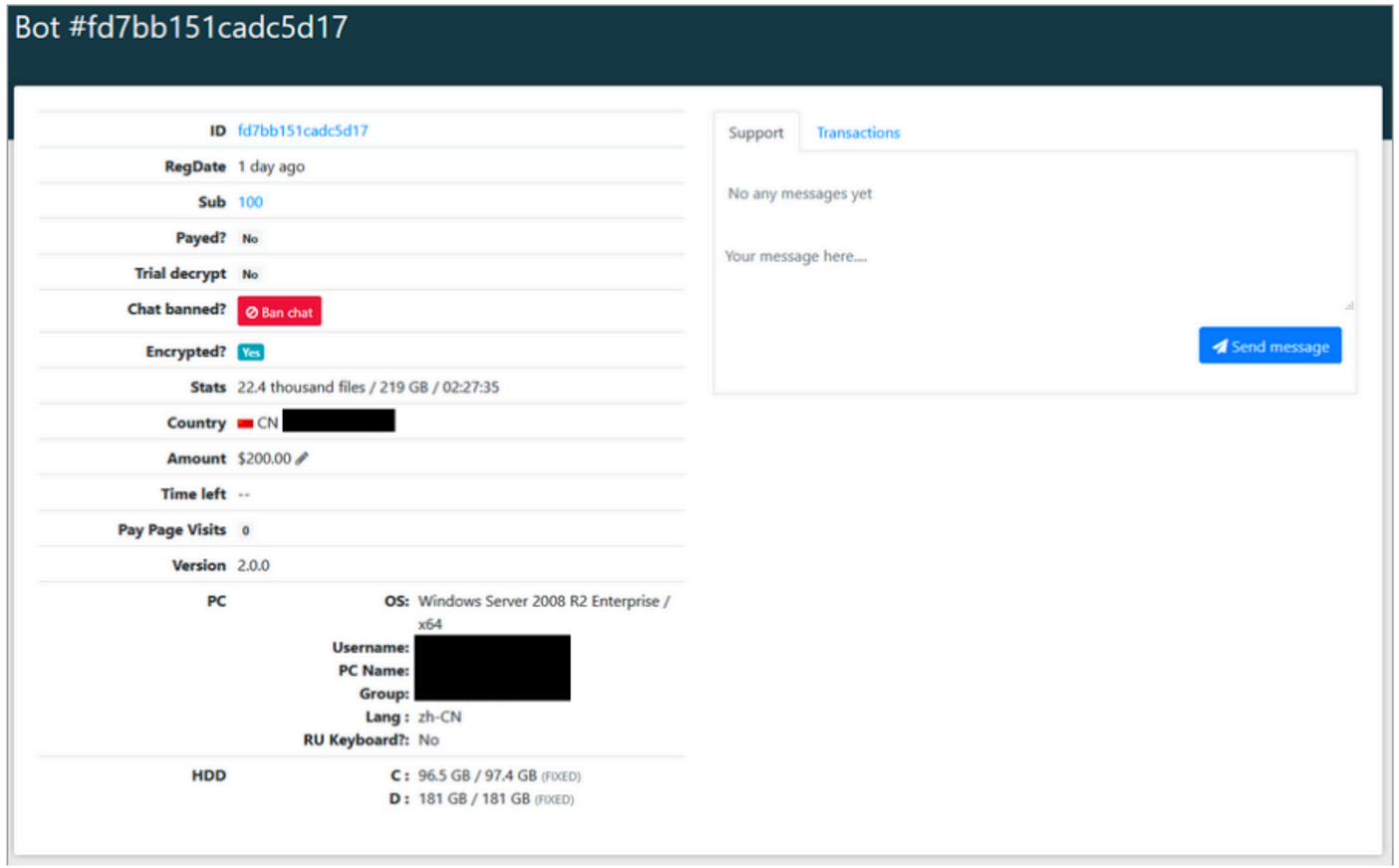


Bots

2018-03-08 - 2018-04 | Show

Country	IP	Bot	Sub	Trial	Encrypted?	Visits	Amount	Payed?	RegDate
CN	[redacted]	256c6555fa6a6ac4	100	No	No	0	$100.00	No	1 day ago
CN		986fde37a41a811e	100	No	Yes	0	$100.00	No	1 day ago
CN		fd7bb151cadc5d17	100	No	Yes	0	$200.00	No	1 day ago
CN		afc95ae4e46e7756	100	No	No	0	$100.00	No	2 days ago
HK		90d3fb03f2c0efca	100	No	Yes	0	$100.00	No	2 days ago
CN		5e192fb34c35cbae	100	No	No	0	$100.00	No	2 days ago
HK		6217c1da9275aa93	100	No	Yes	2	$100.00	No	2 days ago
IN		ee37fe414a29f9b1	100	No	Yes	0	$150.00	No	2 days ago
PL		1f0f53a9f4efd444	100	No	Yes	0	$100.00	No	2 days ago
CN		fa5219dc7c245332	100	No	No	0	$100.00	No	2 days ago
IN		24afc506f054ab96	100	No	No	0	$100.00	No	2 days ago
CN		62d204f070935c31	100	No	Yes	0	$100.00	No	2 days ago
--		aa37f944adc43	100	No	No	0	$100.00	No	2 days ago
IT		c11186a66627847c	100	No	No	0	$100.00	No	2 days ago
IT		3111da03845d534a	100	No	Yes	0	$100.00	No	2 days ago
CN		39d64ad62c509bb3	200	No	Yes	0	$200.00	No	2 days ago
HK		86977dd3cc7ba214	200	No	Yes	0	$200.00	No	2 days ago
CN		bdaf37e6d4d39ed5	200	No	No	0	$200.00	No	2 days ago
CN		176ffa6d786f19b0	150	No	Yes	2	$50.00	No	2 days ago

Backend


Bot #fd7bb151cadc5d17
ID fd7bb151cadc5d17
RegDate 1 day ago
Sub 100
Payed? No
Trial decrypt No
Chat banned? Ban chat
Encrypted? Yes
Stats 22.4 thousand files / 219 GB / 02:27:35
Country CN [redacted]
Amount $200.00
Time left --
Pay Page Visits 0
Version 2.0.0
PC
OS: Windows Server 2008 R2 Enterprise / x64
Username: [redacted]
PC Name:
Group:
Lang : zh-CN
RU Keyboard?: No
HDD
C : 96.5 GB / 97.4 GB (FIXED)
D : 181 GB / 181 GB (FIXED)
Support
Transactions
No any messages yet
Your message here....
Send message

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

GandCrab Dropped File

C:\USERS\%CURRENT_USER%\APPDATA\ROAMING\MICROSOFT

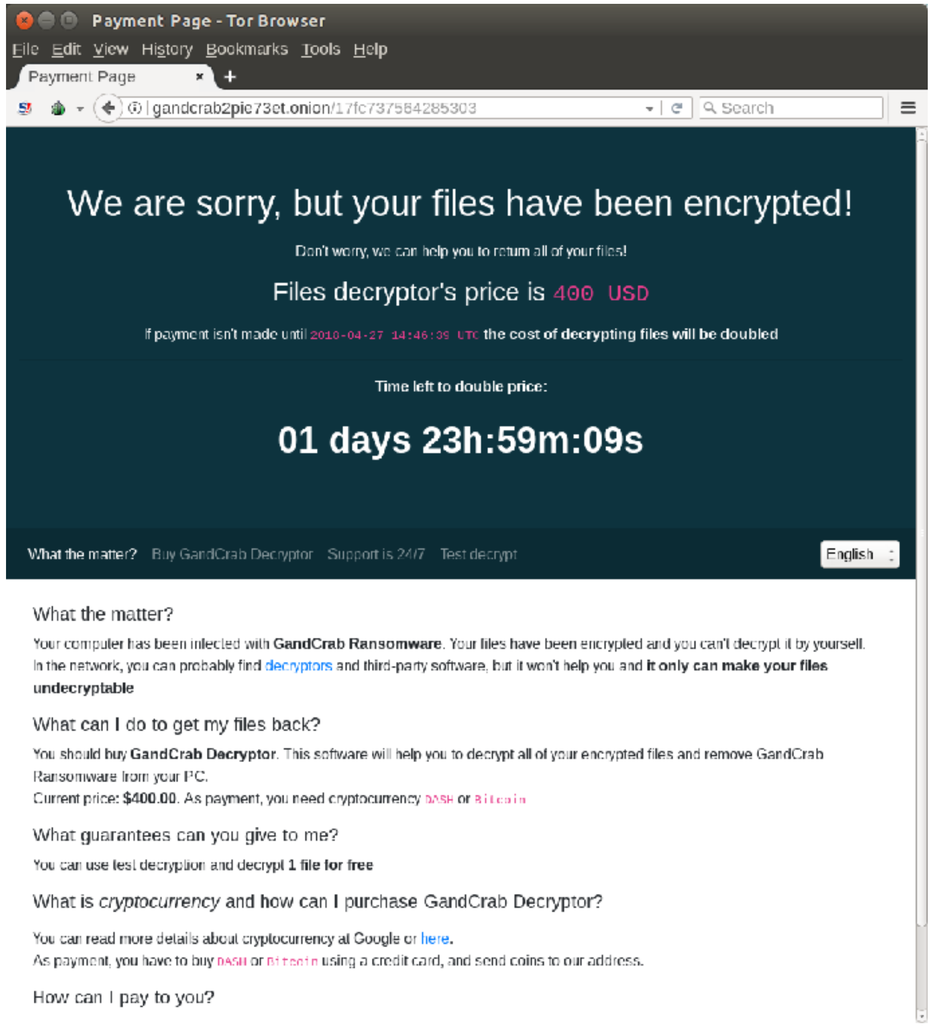
```python
import random
import string

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

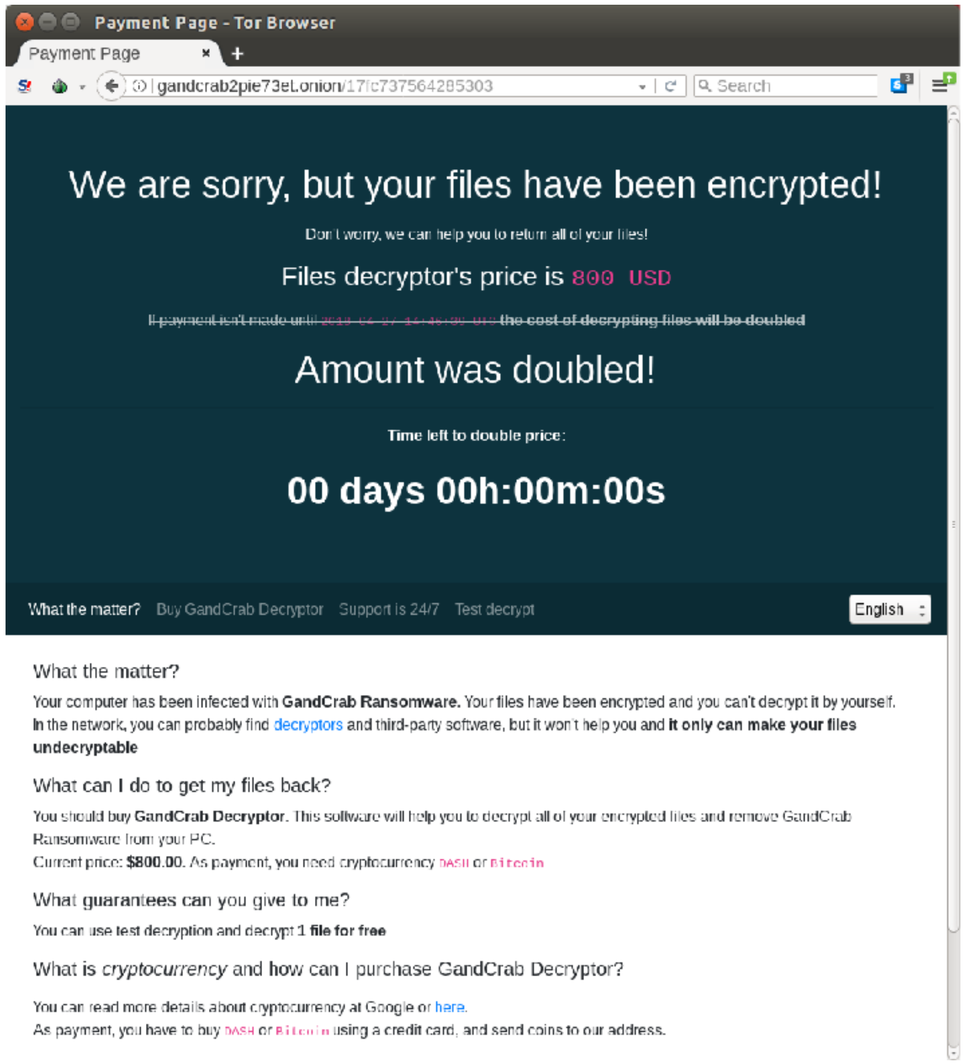
GandCrab Persistency Technique

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

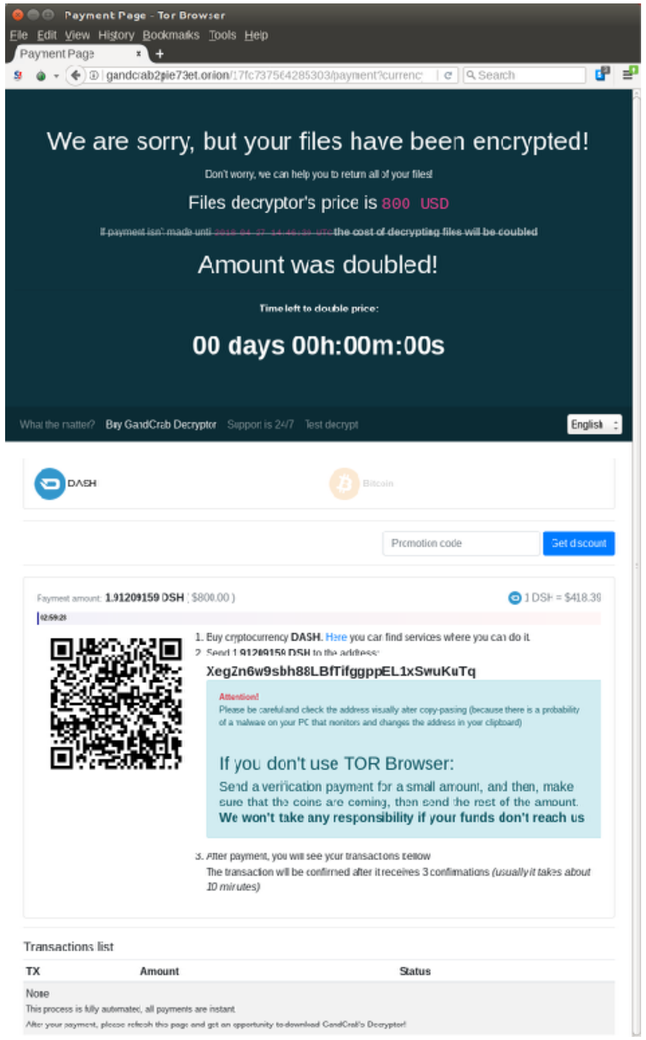
The Ransom Note

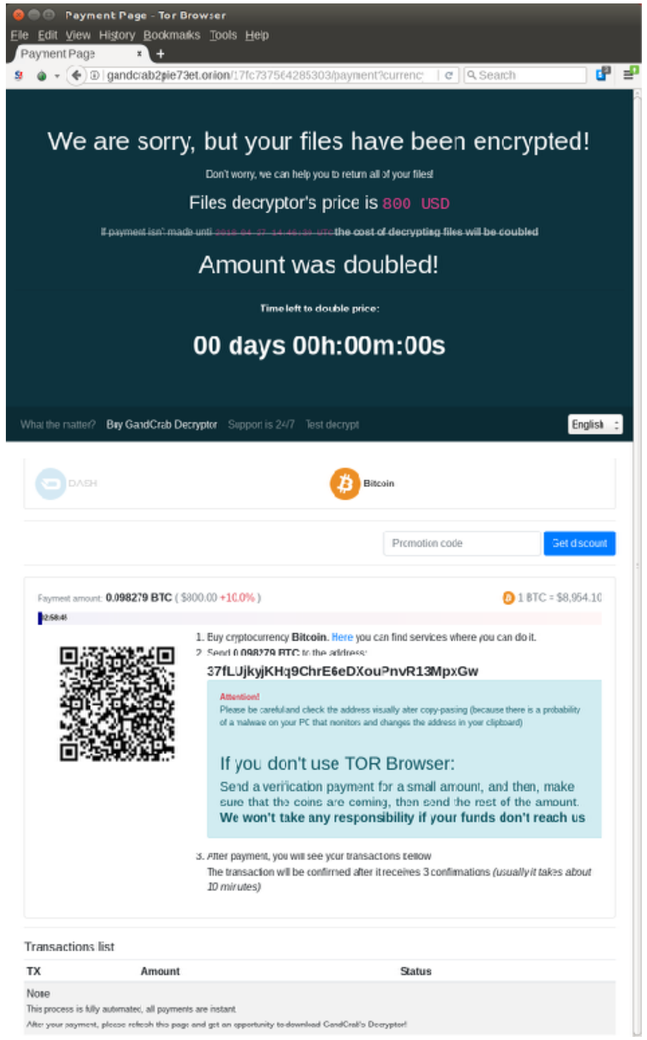


Expired Ransom Note

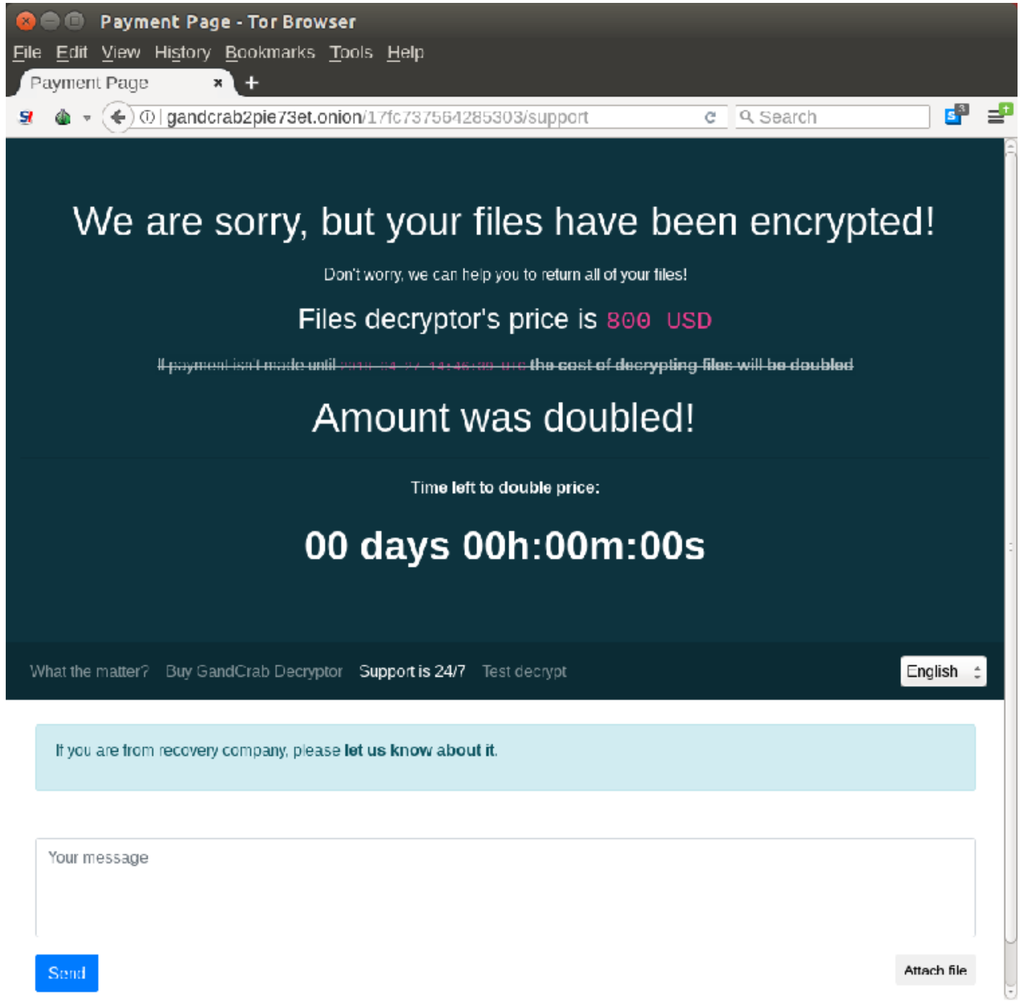


Payment Method

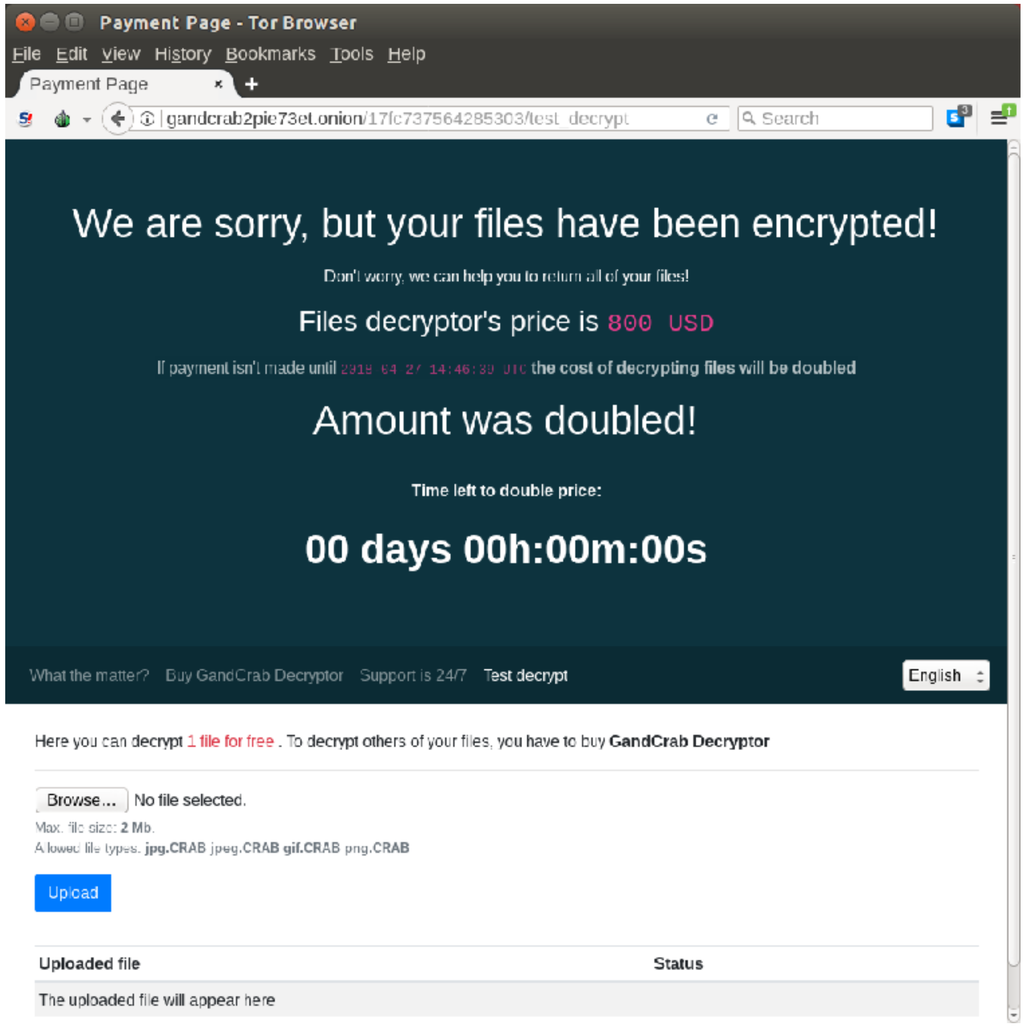




24/7 Support


Payment Page - Tor Browser
File Edit View History Bookmarks Tools Help
Payment Page
gandcrab2pie73et.onion/17fc737554285303/support
Search
We are sorry, but your files have been encrypted!
Don't worry, we can help you to return all of your files!
Files decryptor's price is 800 USD
If payment isn't made until the cost of decrypting files will be doubled
Amount was doubled!
Time left to double price:
00 days 00h:00m:00s
What the matter? Buy GandCrab Decryptor Support is 24/7 Test decrypt
English
If you are from recovery company, please let us know about it.
Your message
Send
Attach file

Try Before You Buy



There is a solution...

GandCrab and other Ransomware Decryption Tools

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

As for Ben...