



NOT SO CRAB MENTALITY  
"A TRUE RAAS STORY"

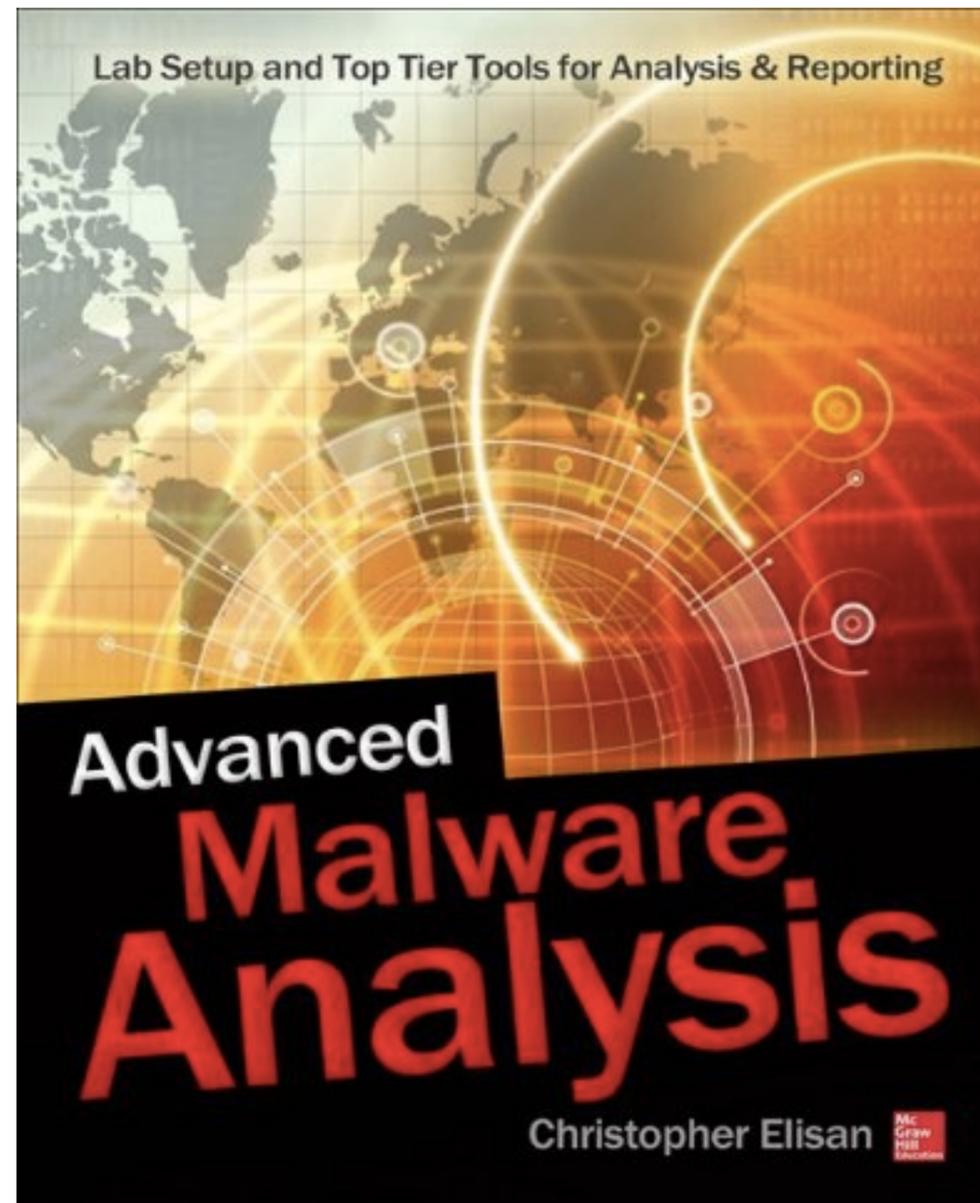
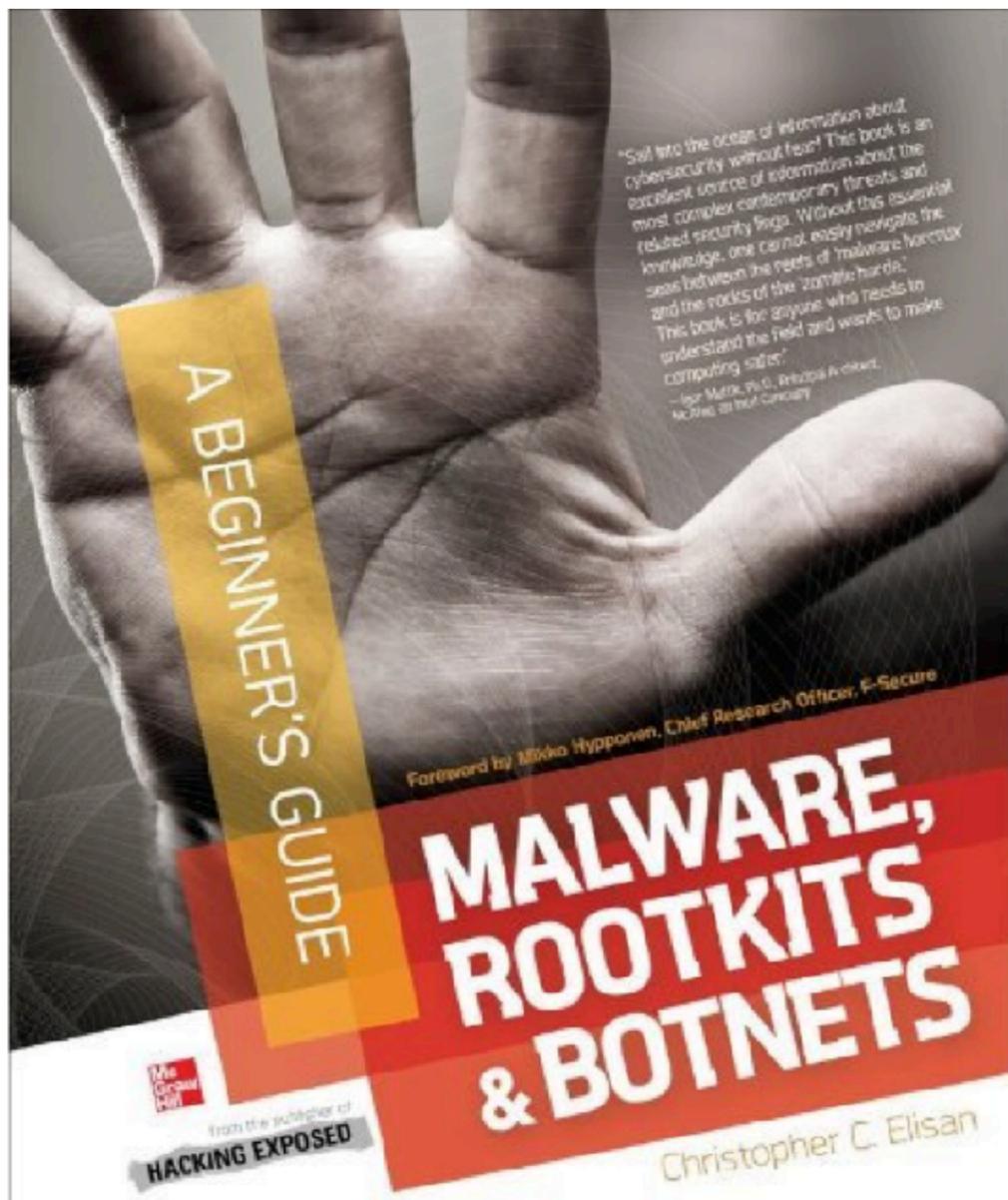
CHRISTOPHER C. ELISAN

# About Me

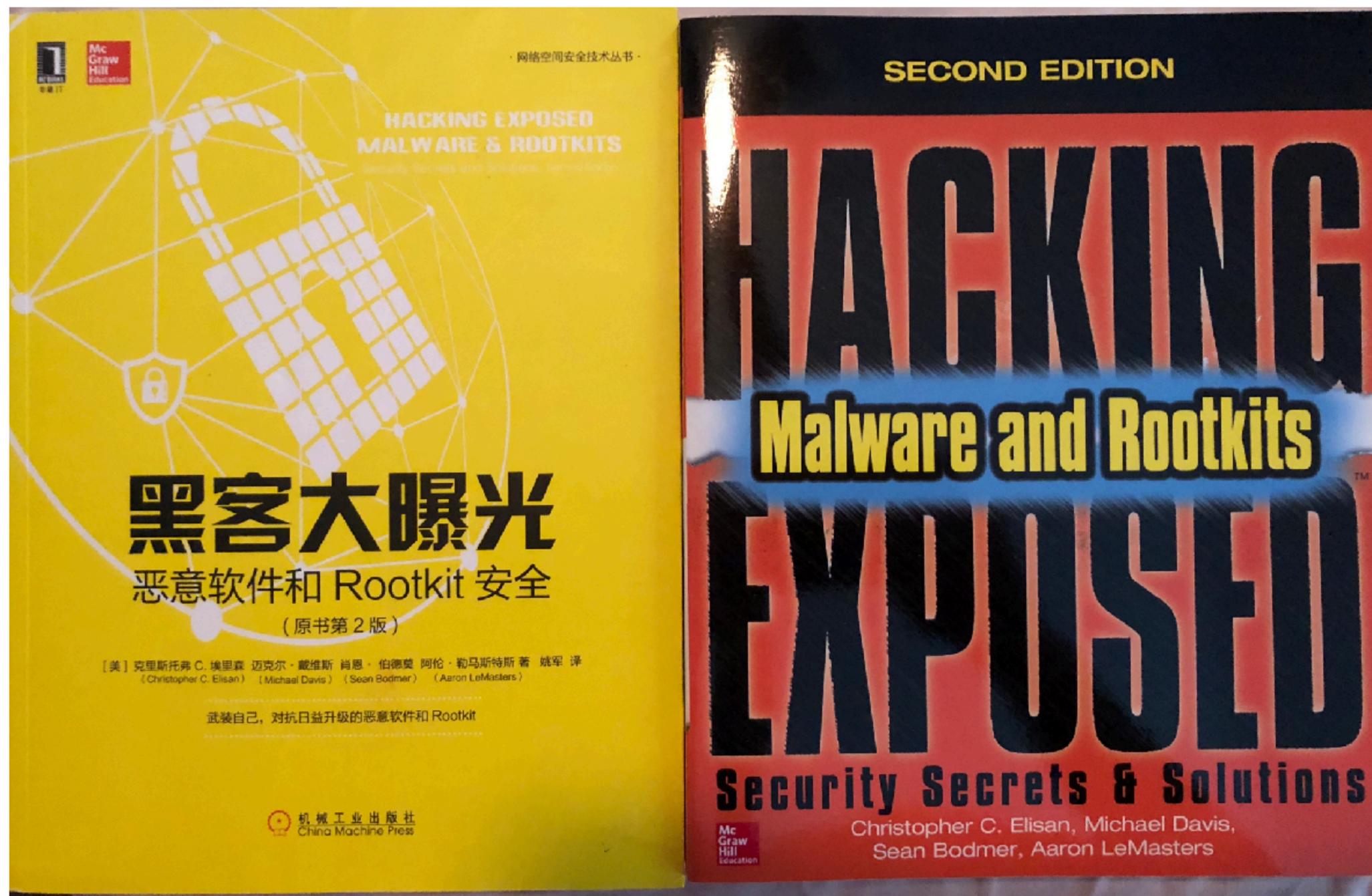
- Senior Malware Researcher @FlashpointIntel
- Past Adventures
  - RSA
  - Damballa
  - F-Secure
  - Trend Micro
- @Tophs



# Author Of...

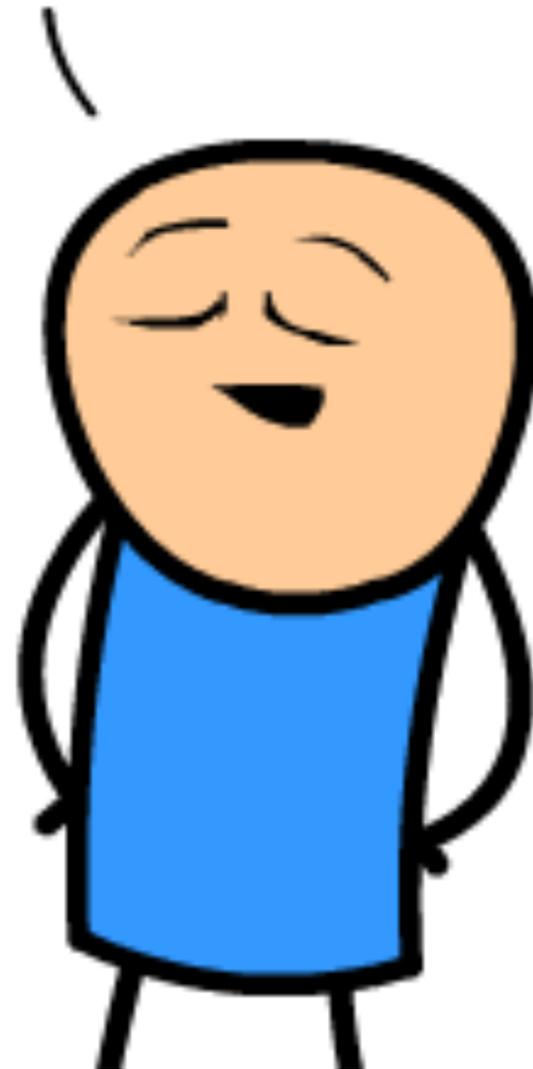


# Co-Author Of...



# SAM is back

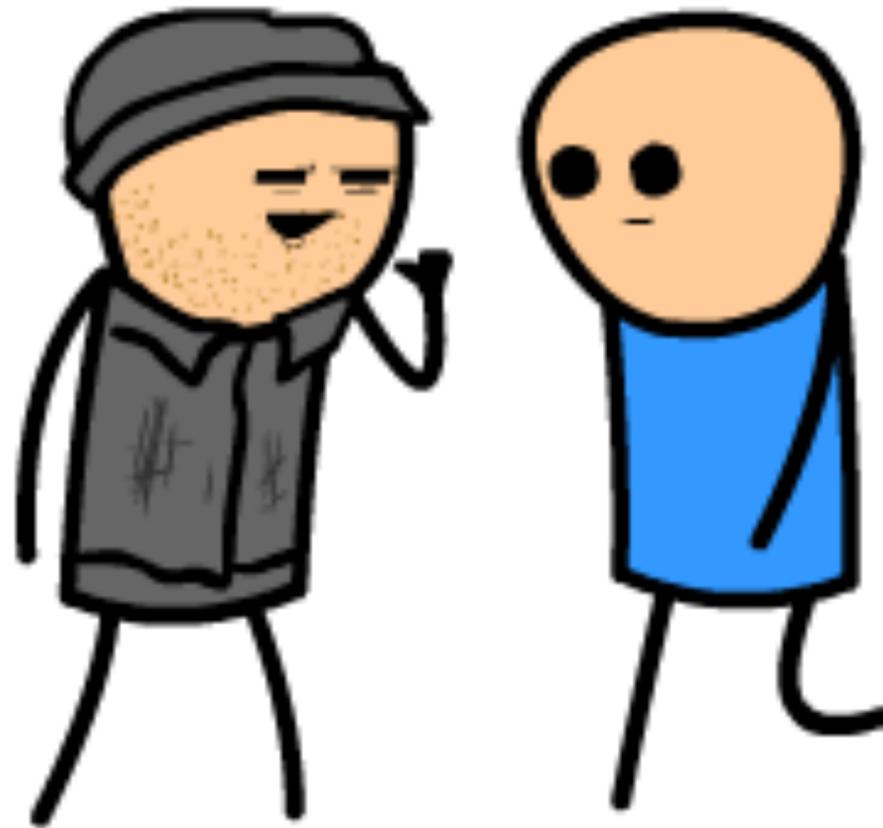
I'M HIGH ON LIFE.



# 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

★ 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 большой вопрос )

Цитата

оплата Вашего % выкупа на Ваш кошелек **Dash**

Наконец-то люди стали переходить на безопасную крипто

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 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.*

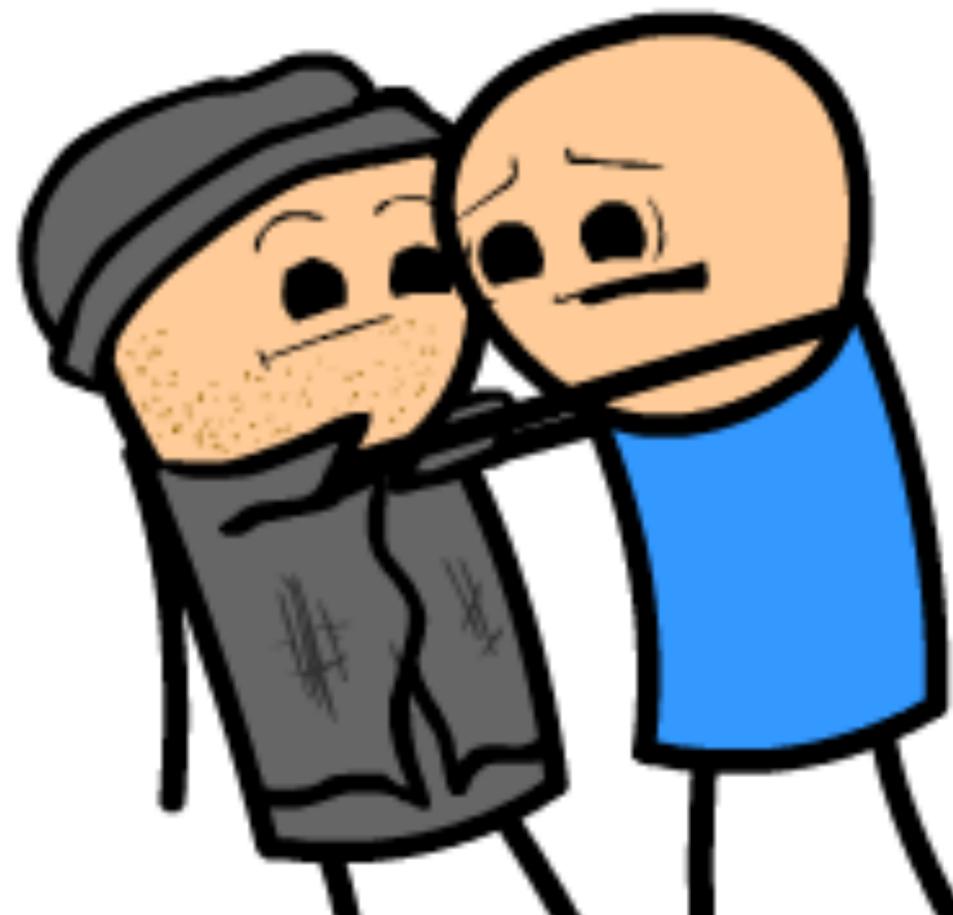
*Attention! We are recruiting a limited number of participants and will stop taking on new partners until new free spots become available.*

*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

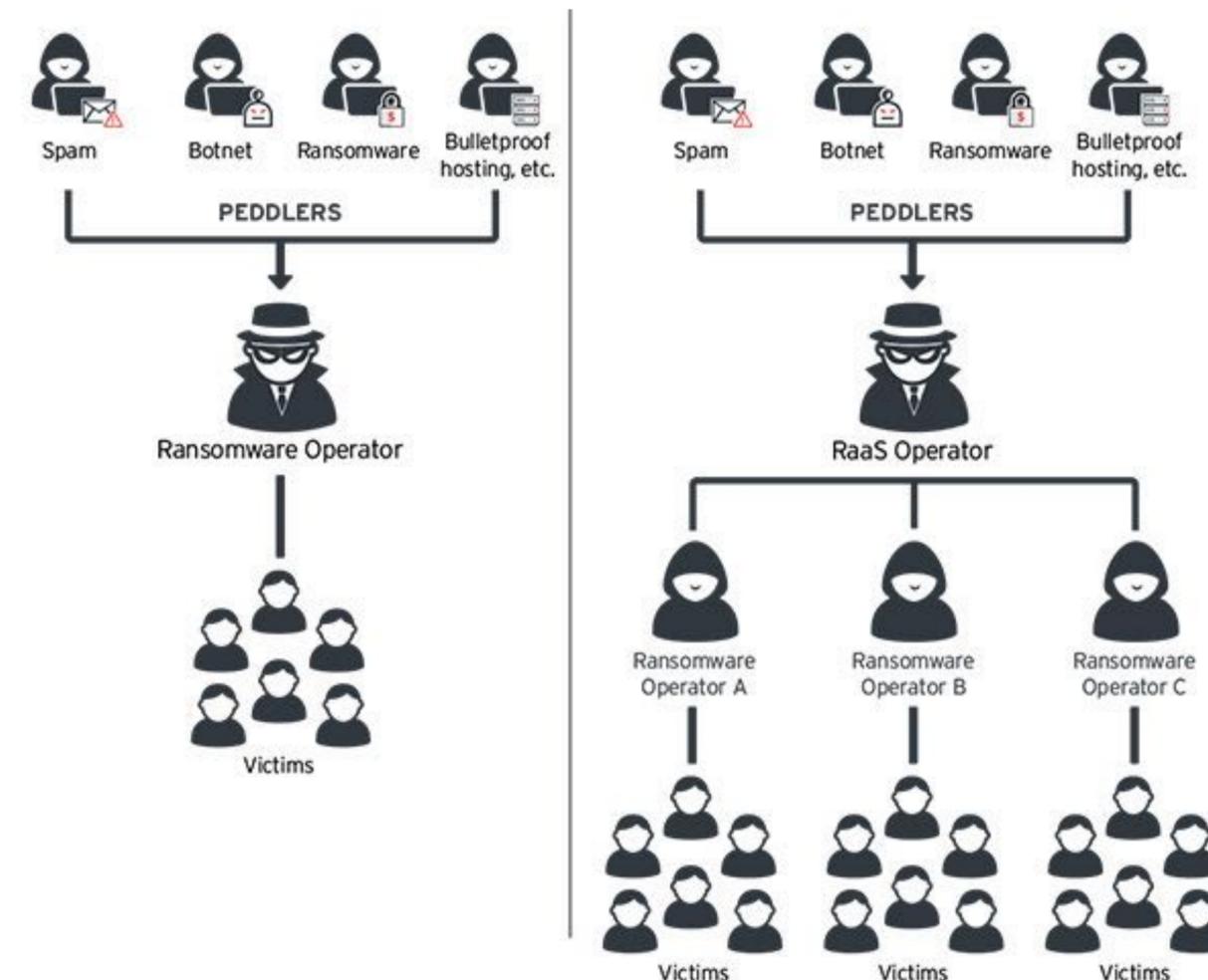
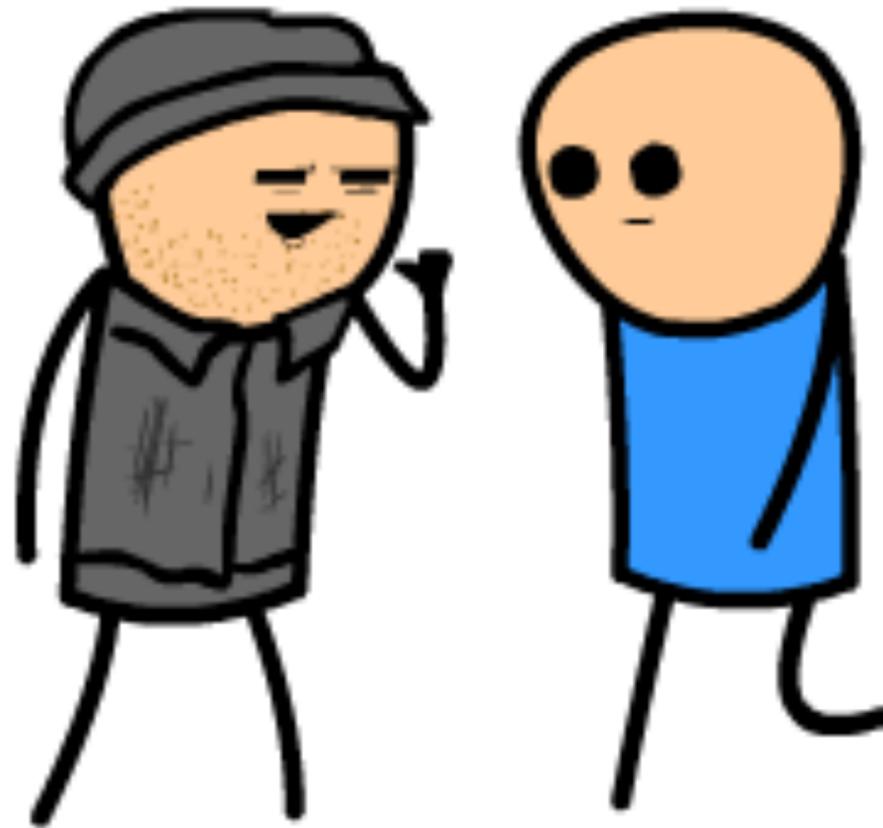


Image Source: Trend Micro

## 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/securitytetchnology/netsec/12140.aspx)*

*[https://www\[.\]hackeye\[.\]net/threatintelligence/12530.aspx](https://www[.]hackeye[.]net/threatintelligence/12530.aspx)*

*[http://www\[.\]freebuf\[.\]com/column/162254.html](http://www[.]freebuf[.]com/column/162254.html)*

*Searching for high-skilled [malware] spreaders.*

*[Profits will be split] 60 percent/40 percent*

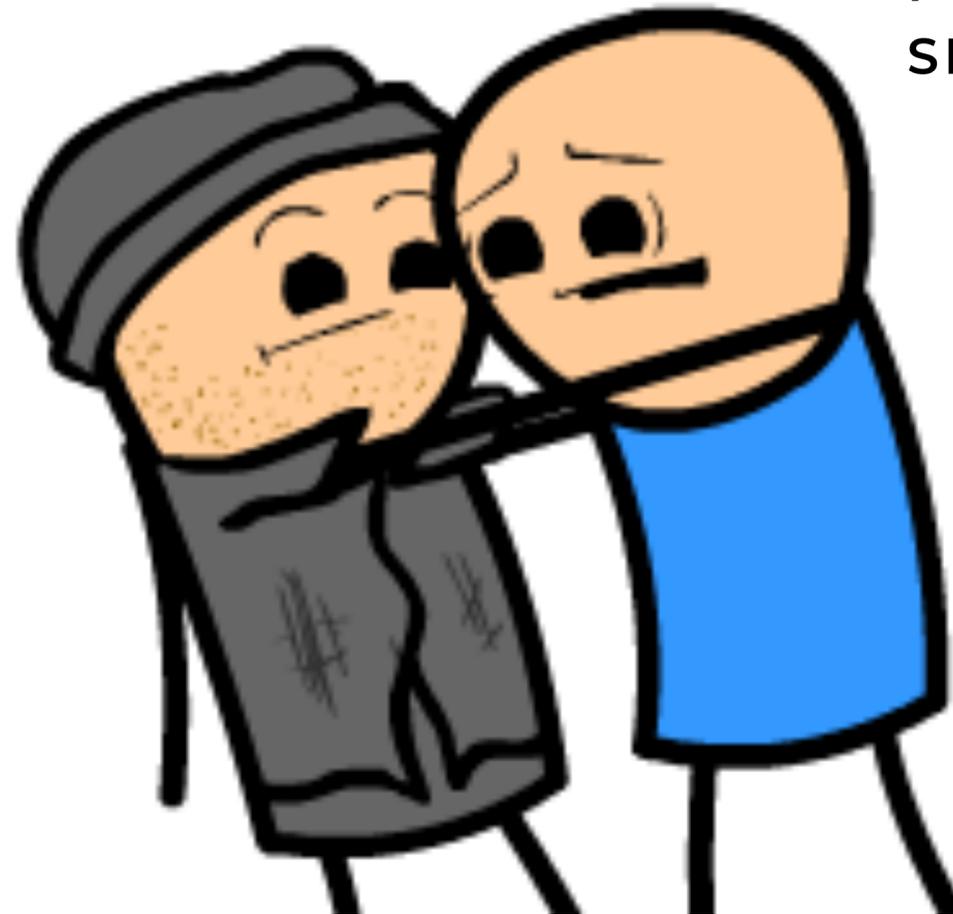
*[If there are high profits then the split] will be raised to 70 percent/30 percent*

*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



### Dashboard

#### Statistics

2018-03-31 - 2018-04-01

Date	Bots	TX	Orders	DSH			BTC		
				Profit	Fee	Total	Profit	Fee	Total
<a href="#">2018-04-07</a>	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00
<a href="#">2018-04-06</a>	1	0	0	0.00	0.00	0.00	0.00	0.00	0.00
<a href="#">2018-04-05</a>	22	0	0	0.00	0.00	0.00	0.00	0.00	0.00
<a href="#">2018-04-04</a>	49	0	1	0.00	0.00	0.00	0.00	0.00	0.00
<a href="#">2018-04-03</a>	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00
<a href="#">2018-04-02</a>	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00
<a href="#">2018-04-01</a>	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00
<a href="#">2018-03-31</a>	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00
<b>Total</b>	<b>72</b>	<b>0</b>	<b>1</b>	<b>0.00</b>	<b>0.00</b>	<b>0.00</b>	<b>0.00</b>	<b>0.00</b>	<b>0.00</b>



#### Last transactions

Bot	Amount
Not found	

### Bots

2018-03-08 - 2018-04

Country	IP	Bot	Sub	Trial	Encrypted?	Visits	Amount	Payed?	RegDate
CN	[REDACTED]	256c6555fa6a6ac4	100	No	No	0	\$100.00	No	1 day ago
CN	[REDACTED]	986fde37a41a811e	100	No	Yes	0	\$100.00	No	1 day ago
CN	[REDACTED]	fd7bb151cadc5d17	100	No	Yes	0	\$200.00	No	1 day ago
CN	[REDACTED]	afc95ae4e46e7756	100	No	No	0	\$100.00	No	2 days ago
HK	[REDACTED]	90d3fb03f2c0efca	100	No	Yes	0	\$100.00	No	2 days ago
CN	[REDACTED]	5e192fb34c35cbae	100	No	No	0	\$100.00	No	2 days ago
HK	[REDACTED]	6217c1da9275aa93	100	No	Yes	2	\$100.00	No	2 days ago
IN	[REDACTED]	ee37fe414a29f9b1	100	No	Yes	0	\$150.00	No	2 days ago
PL	[REDACTED]	1f0f53a9f4efd444	100	No	Yes	0	\$100.00	No	2 days ago
CN	[REDACTED]	fa5219dc7c245332	100	No	No	0	\$100.00	No	2 days ago
IN	[REDACTED]	24afc506f054ab96	100	No	No	0	\$100.00	No	2 days ago
CN	[REDACTED]	62d204f070935c31	100	No	Yes	0	\$100.00	No	2 days ago
--	[REDACTED]	aa37f944adc43	100	No	No	0	\$100.00	No	2 days ago
IT	[REDACTED]	c11186a66627847c	100	No	No	0	\$100.00	No	2 days ago
IT	[REDACTED]	3111da03845d534a	100	No	Yes	0	\$100.00	No	2 days ago
CN	[REDACTED]	39d64ad62c509bb3	200	No	Yes	0	\$200.00	No	2 days ago
HK	[REDACTED]	86977dd3cc7ba214	200	No	Yes	0	\$200.00	No	2 days ago
CN	[REDACTED]	bda37e6d4d39ed5	200	No	No	0	\$200.00	No	2 days ago
CN	[REDACTED]	176ffa6d786f19b0	150	No	Yes	2	\$50.00	No	2 days ago

Bot #fd7bb151cad5d17

ID	fd7bb151cad5d17
RegDate	1 day ago
Sub	100
Payed?	No
Trial decrypt	No
Chat banned?	<a href="#">Ban chat</a>
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: [REDACTED]
	Group: [REDACTED]
	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](http://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

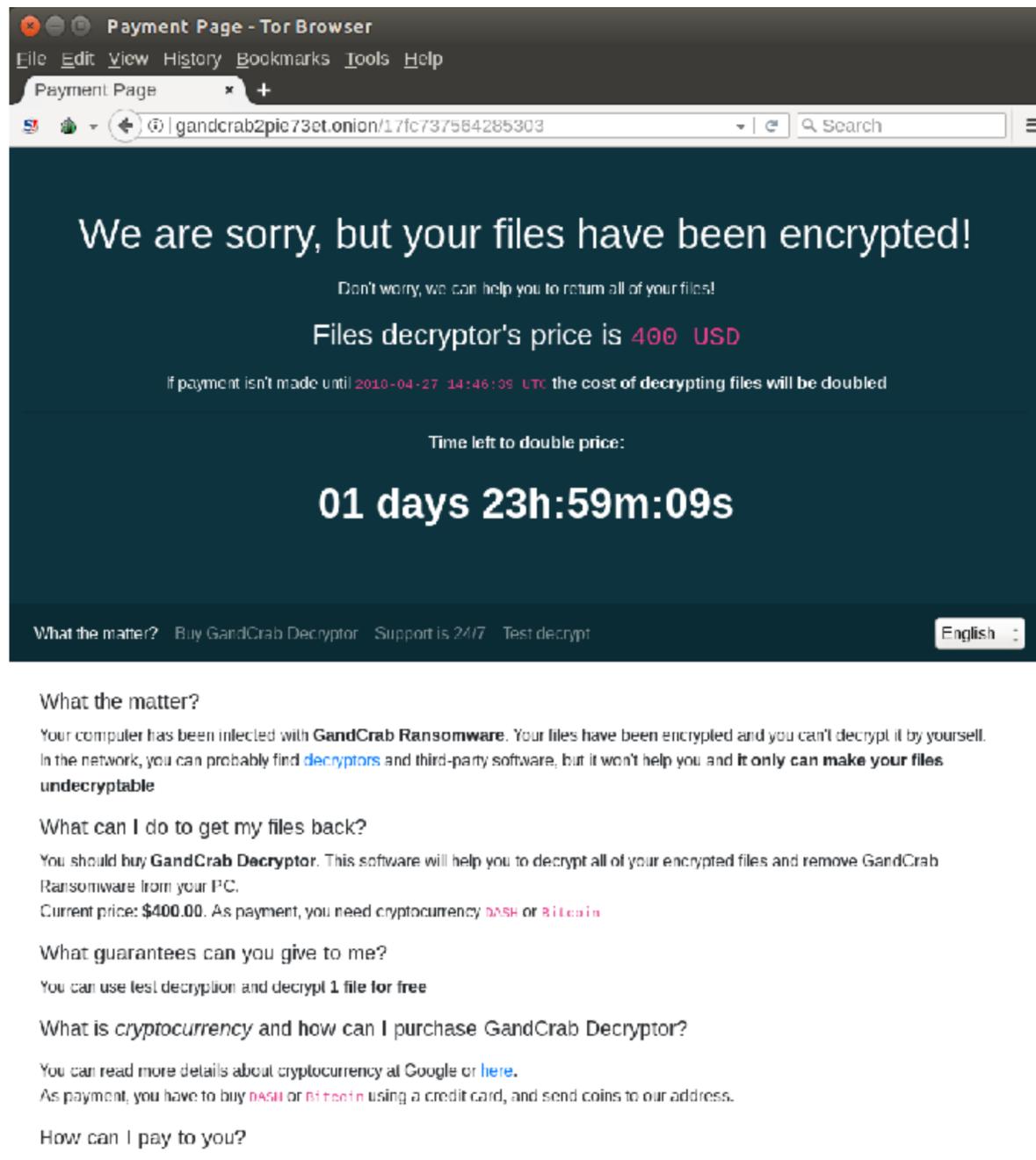
```
import random
import string

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 = gdirxwidth,  
Data = "C:\Users\2XC7u663GxWc\AppData\Roaming\Microsoft\agnlxz.exe"  
Size = 229 KB  
Type = REG_SZ
```

# The Ransom Note



Payment Page - Tor Browser

File Edit View History Bookmarks Tools Help

Payment Page

gandcrab2pic73et.onion/17fc737584285303

## 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 **400 USD**

If payment isn't made until **2010-04-27 14:46:39 UTC** the cost of decrypting files will be doubled

Time left to double price:

# 01 days 23h:59m:09s

What the matter? Buy GandCrab Decryptor Support is 24/7 Test decrypt English

### What the matter?

Your computer has been infected with **GandCrab Ransomware**. Your files have been encrypted and you can't decrypt it by yourself. In the network, you can probably find [decryptors](#) and third-party software, but it won't help you and **it only can make your files undecryptable**

### What can I do to get my files back?

You should buy **GandCrab Decryptor**. This software will help you to decrypt all of your encrypted files and remove GandCrab Ransomware from your PC.  
Current price: **\$400.00**. As payment, you need cryptocurrency **DASH** or **Bitcoin**

### What guarantees can you give to me?

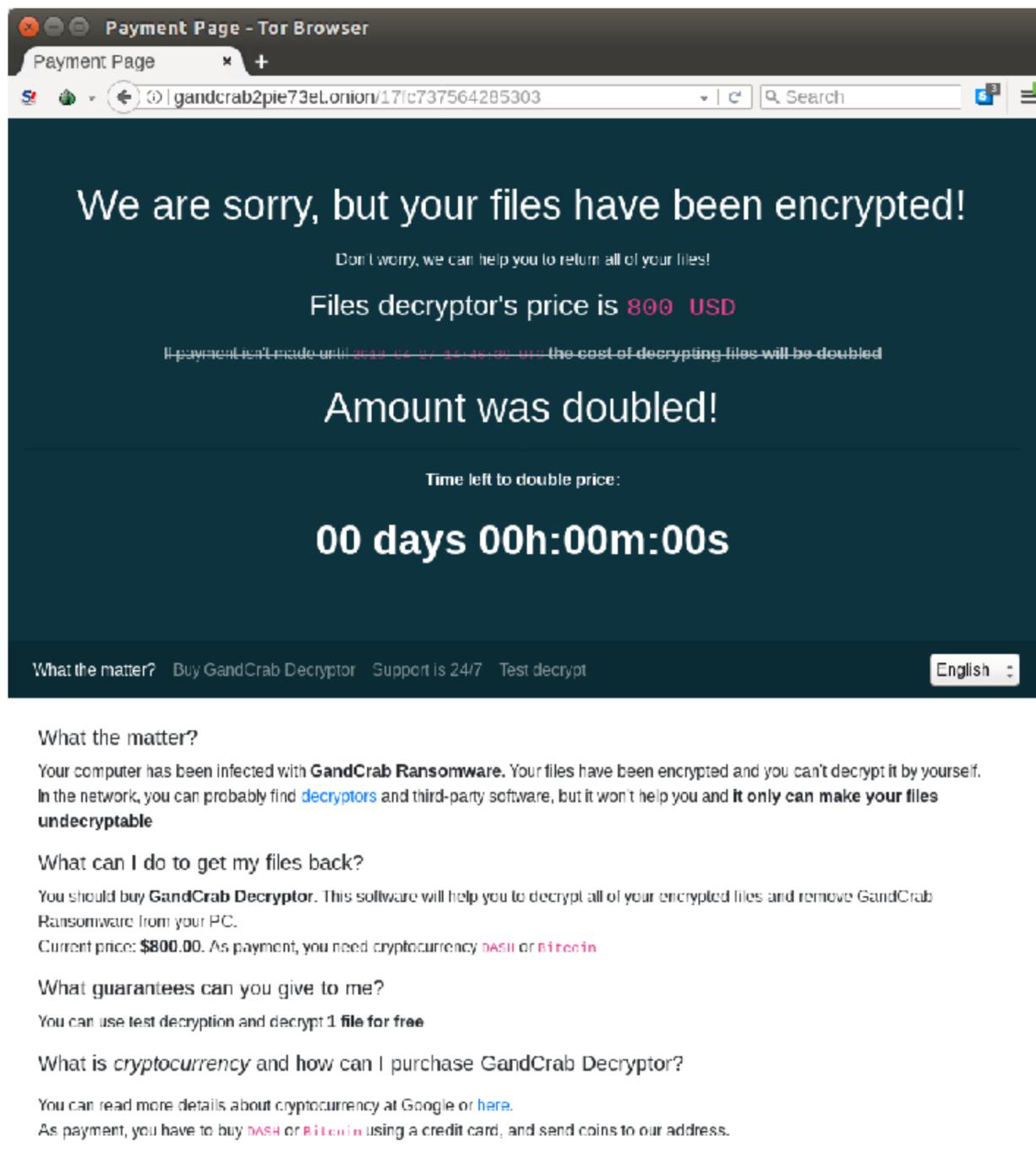
You can use test decryption and decrypt **1 file for free**

### What is *cryptocurrency* and how can I purchase GandCrab Decryptor?

You can read more details about cryptocurrency at Google or [here](#).  
As payment, you have to buy **DASH** or **Bitcoin** using a credit card, and send coins to our address.

### How can I pay to you?

# Expired Ransom Note



Payment Page - Tor Browser

Payment Page

gandcrab2pie73eLoniorn/17fc737564285303

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 **2019-04-27 14:48:00 UTC** 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

**What the matter?**  
Your computer has been infected with **GandCrab Ransomware**. Your files have been encrypted and you can't decrypt it by yourself. In the network, you can probably find [decryptors](#) and third-party software, but it won't help you and **it only can make your files undecryptable**

**What can I do to get my files back?**  
You should buy **GandCrab Decryptor**. This software will help you to decrypt all of your encrypted files and remove GandCrab Ransomware from your PC.  
Current price: **\$800.00**. As payment, you need cryptocurrency **DASH** or **Bitcoin**

**What guarantees can you give to me?**  
You can use **test decryption** and decrypt **1 file for free**

**What is *cryptocurrency* and how can I purchase GandCrab Decryptor?**  
You can read more details about cryptocurrency at Google or [here](#).  
As payment, you have to buy **DASH** or **Bitcoin** using a credit card, and send coins to our address.

# Payment Method

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 2018-04-27 14:45:00 UTC 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

DASH Bitcoin

Promotion code Get discount

Payment amount: 1.91209159 DSH (\$800.00) 1 DSH = \$418.39

QR code

1. Buy cryptocurrency DASH. Here you can find services where you can do it.  
2. Send 1.91209159 DSH to the address:  
**XegZn6w9sbh88LBFifggppEL1xSwuKuTq**

**Attention!**  
Please be careful and check the address visually after copy-pasting (because there is a probability of a malware on your PC that monitors and changes the address in your clipboard)

**If you don't use TOR Browser:**  
Send a verification payment for a small amount, and then, make sure that the coins are coming, then send the rest of the amount.  
**We won't take any responsibility if your funds don't reach us**

3. After payment, you will see your transactions below  
The transaction will be confirmed after it receives 3 confirmations (usually it takes about 10 minutes)

Transactions list

TX	Amount	Status
None		

Note  
This process is fully automated, all payments are instant.  
After your payment, please refresh this page and get an opportunity to download GandCrab's Decryptor!

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 2018-04-27 14:45:00 UTC 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

DASH Bitcoin

Promotion code Get discount

Payment amount: 0.098279 BTC (\$800.00 +10.0%) 1 BTC = \$8,954.10

QR code

1. Buy cryptocurrency Bitcoin. Here you can find services where you can do it.  
2. Send 0.098279 BTC to the address:  
**37fLJkyjKHq9ChrE6eDXouPnvR13MpxGw**

**Attention!**  
Please be careful and check the address visually after copy-pasting (because there is a probability of a malware on your PC that monitors and changes the address in your clipboard)

**If you don't use TOR Browser:**  
Send a verification payment for a small amount, and then, make sure that the coins are coming, then send the rest of the amount.  
**We won't take any responsibility if your funds don't reach us**

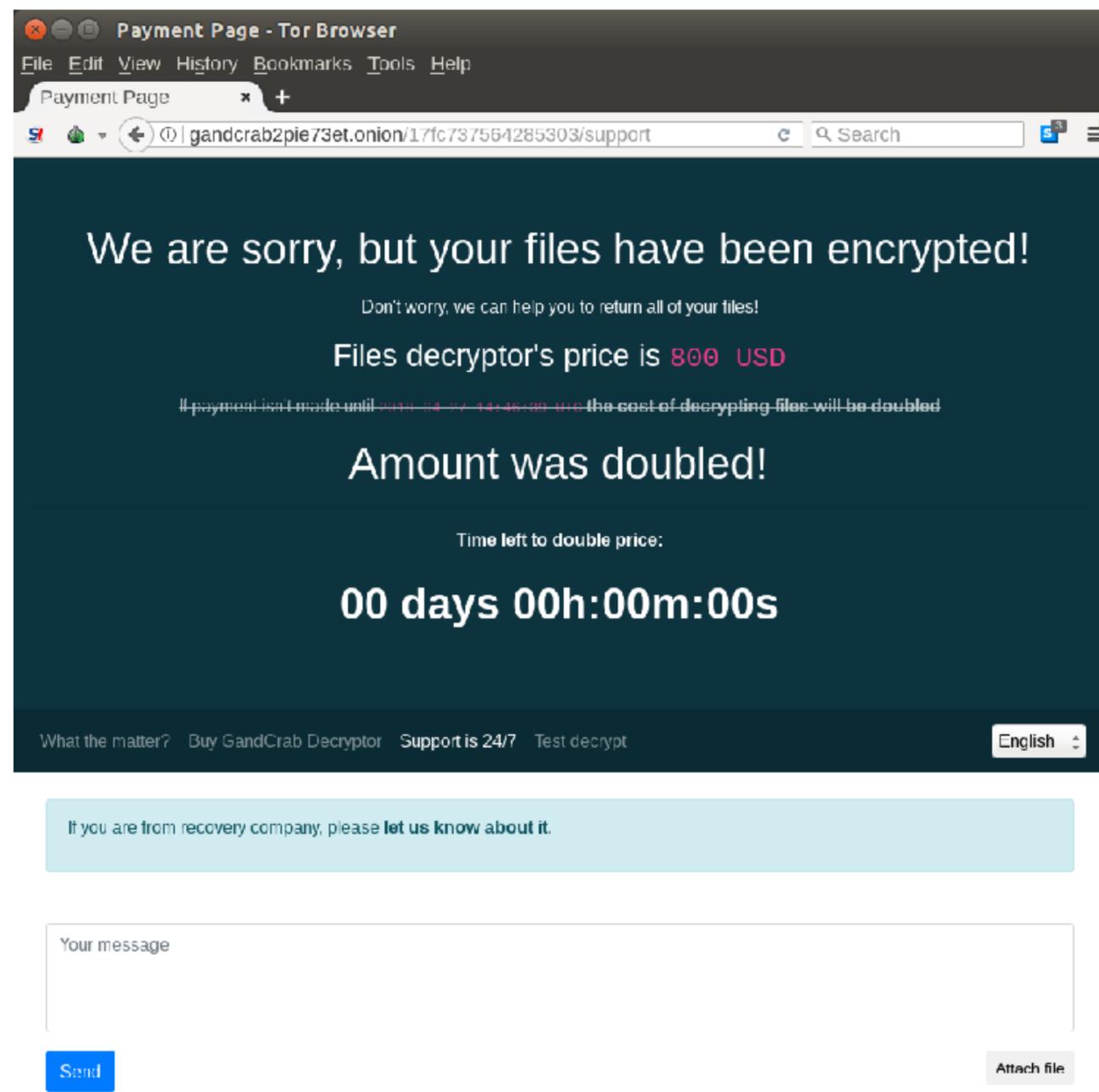
3. After payment, you will see your transactions below  
The transaction will be confirmed after it receives 3 confirmations (usually it takes about 10 minutes)

Transactions list

TX	Amount	Status
None		

Note  
This process is fully automated, all payments are instant.  
After your payment, please refresh this page and get an opportunity to download GandCrab's Decryptor!

# 24/7 Support



The screenshot shows a web browser window titled "Payment Page - Tor Browser". The address bar displays the URL "gandcrab2pie73et.onion/17fc737554285303/support". The main content of the page is on a dark green background and reads:

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 2020-04-07 14:36:00, the cost of decrypting files will be doubled~~

**Amount was doubled!**

Time left to double price:

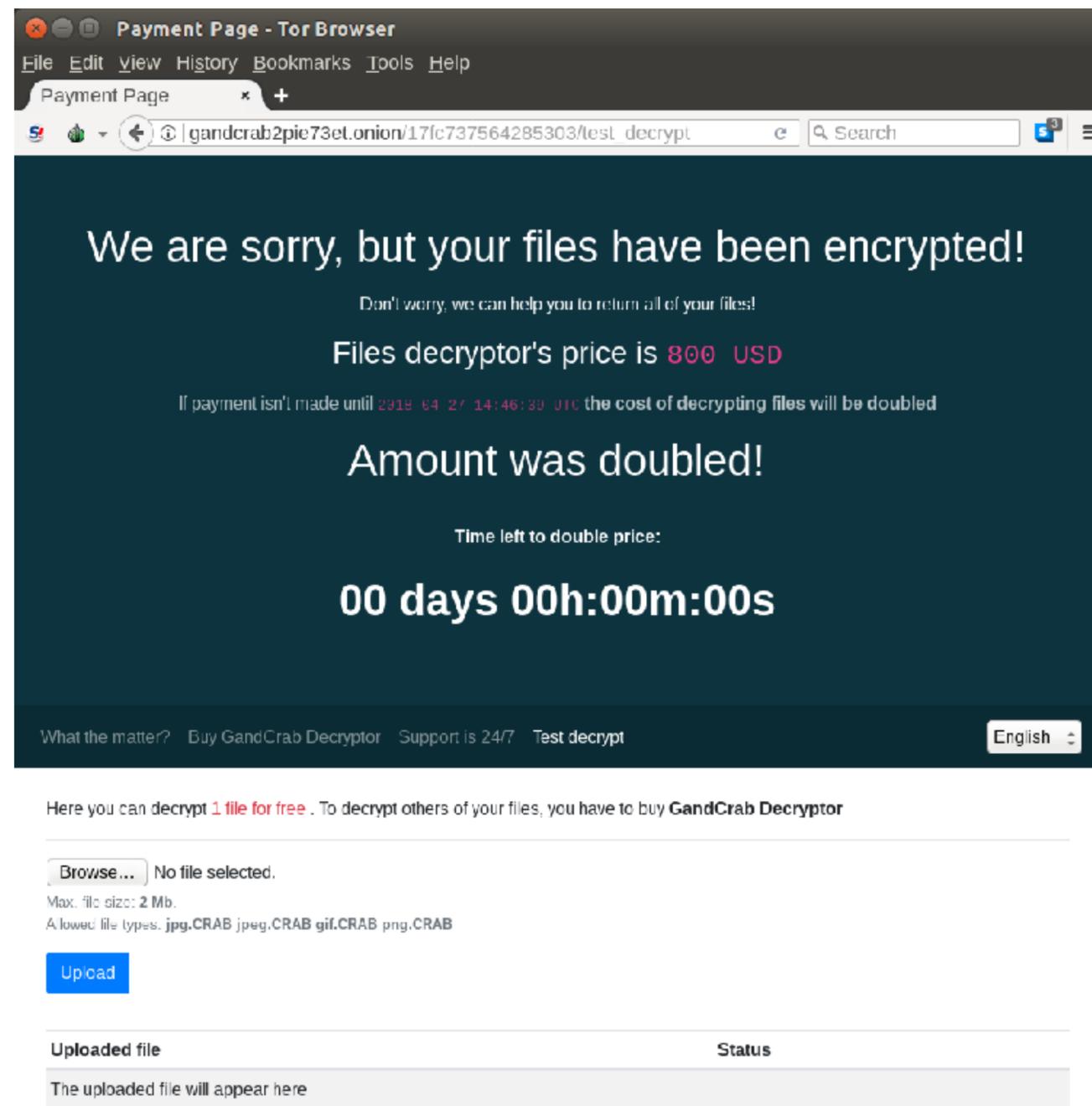
**00 days 00h:00m:00s**

At the bottom of the page, there are links for "What the matter?", "Buy GandCrab Decryptor", "Support is 24/7", and "Test decrypt". A language dropdown menu is set to "English".

Below the main content, there is a light blue box with the text: "If you are from recovery company, please **let us know about it.**"

Below that is a text input field labeled "Your message". At the bottom left of the input area is a blue "Send" button, and at the bottom right is a grey "Attach file" button.

# Try Before You Buy



The screenshot shows a web browser window titled "Payment Page - Tor Browser". The address bar contains the URL "gandcrab2pie73et.onion/17fc737564285303/test\_decrypt". The page content is as follows:

**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 2019-04-27 14:46:30 UTC the cost of decrypting files will be doubled  
**Amount was doubled!**  
Time left to double price:  
**00 days 00h:00m:00s**

At the bottom of the dark green message box, there are links: "What the matter?", "Buy GandCrab Decryptor", "Support is 24/7", "Test decrypt", and a language dropdown menu set to "English".

Below the message box, the text reads: "Here you can decrypt 1 file for free . To decrypt others of your files, you have to buy GandCrab Decryptor".

There is a file upload section with a "Browse..." button and the text "No file selected." Below this, it specifies "Max. file size: 2 Mb." and "Allowed file types: .jpg.CRAB .jpeg.CRAB .gif.CRAB .png.CRAB". A blue "Upload" button is present.

At the bottom, there is a table with two columns: "Uploaded file" and "Status". The table is currently empty, with the text "The uploaded file will appear here" in the first row.

There is a solution...



# GandCrab and other Ransomware Decryption Tools

[HTTPS://WWW.NOMORERANSOM.ORG/EN/DECRYPTION-TOOLS.HTML](https://www.nomoreransom.org/en/decryption-tools.html)

**NO MORE RANSOM!**

As for Ben...

