Boost your cyber criminal activities with cryptocurrencies?

or the tough life of the attackers.

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy -
TLP:WHITE

April 13, 2016

What’s CIRCL?

CIRCL
Computer Incident
Response Center
Luxembourg

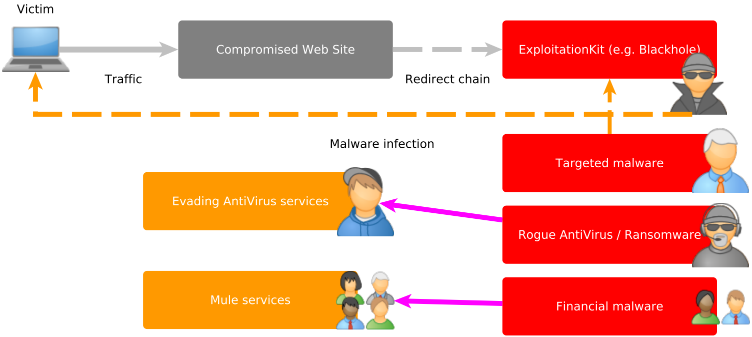
- The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents.
- CIRCL is the CERT for the **private sector**, communes and non-governmental entities in Luxembourg.
- CIRCL supports organizations located/incorporated in Luxembourg in case of incident or proactively by providing an advanced sharing platform (MISP).

Ransomware from locker to crypto

Attackers experimented many potential techniques to extort money from computer users like

- **Locking** access to computer;
- **Leaking** personal information to the public;
- **Losing** critical information and data;
- Using **fear** of police, law enforcement or hierarchies;
- or **destructing** physical equipments.

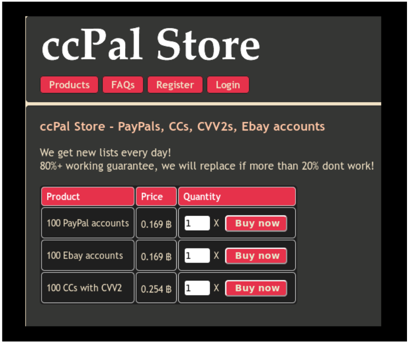
Cybercriminal ecosystem - an overview



- Cash-out is a key element for attackers to get the money out and drop the risks on the mules.
- Bitcoin plays a role in the overall ecosystem but it's not a silver bullet solution for the attacker.

The use of bitcoin by cyber criminals

- The early use of bitcoin was an alternative process to the vetting (e.g. access to private forums).
- Buying CC or stolen accounts.



ccPal Store - PayPals, CCs, CVV2s, Ebay accounts

We get new lists every day!
80%+ working guarantee, we will replace if more than 20% dont work!

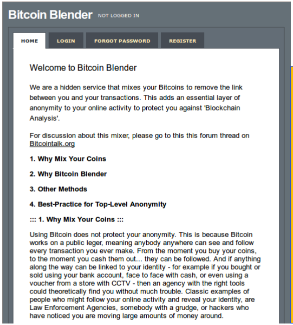
Product	Price	Quantity
100 PayPal accounts	0.169 Ƀ	1 X Buy now
100 Ebay accounts	0.169 Ƀ	1 X Buy now
100 CCs with CVV2	0.254 Ƀ	1 X Buy now

Crypto-ransomware and bitcoin

- When ransom-lockers are used, computers are fully locked and unusable (e.g. attacker use paysafe cards, ucash, ...).
- Crypto-ransomware encrypt the data (and the system remains usable). Allowing the victim to get access to a bitcoin provider.
- Bitcoin helps the attacker to have an alternative scheme of payment but...
  - **Attackers are users of bitcoin and they do mistakes**.
  - Victims might find difficult to use bitcoin.
  - Attackers still need to cash out.

Bitcoin privacy

- Bitcoin is not anonymous and **everyone**[1] **can track the transactions**.
- Attackers have to use mixer(s) to hide their traces or limit the ability to traceback.



Welcome to Bitcoin Blender

We are a hidden service that mixes your Bitcoins to remove the link between you and your transactions. This adds an essential layer of anonymity to your online activity to protect you against 'Blockchain Analysis'.

For discussion about this mixer, please go to this this forum thread on Bitcointalk.org

1. Why Mix Your Coins

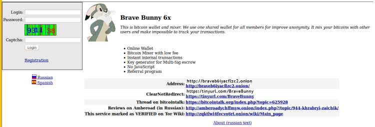
2. Why Bitcoin Blender

3. Other Methods

4. Best-Practice for Top-Level Anonymity

::: 1. Why Mix Your Coins :::

Using Bitcoin does not protect your anonymity. This is because Bitcoin works on a public leger, meaning anybody anywhere can see and follow every transaction you ever make. From the moment you buy your coins, to the moment you cash them out... they can be followed. And if anything along the way can be linked to your identity - for example if you bought or sold using your bank account, face to face with cash, or even using a voucher from a store with CCTV - then an agency with the right tools could theoretically find you without much trouble. Classic examples of people who might follow your online activity and reveal your identity, are Law Enforcement Agencies, somebody with a grudge, or hackers who have noticed you are moving large amounts of money around.



Brave Bunny 6x

This is bitcoin wallet and mixer. We use one shared wallet for all members for improve anonymity. It mix your bitcoins with other users and make impossible to track your transactions.

- Online Wallet
- Bitcoin Mixer with low fee
- Instant internal transactions
- Key generator for Multi-Sig escrow
- No JavaScript
- Referral program

Address:	http://braveb6iyacflzc2.onion http://braveb6iyacflzc2.onion/
ClearNetRedirect:	https://tinyurl.com/BraveBunny https://tinyurl.com/BraveBunny
Thread on bitcointalk:	https://bitcointalk.org/index.php?topic=625928
Reviews on Amberoad (in Russian):	http://amberoadychffmyw.onion/index.php?/topic/944-khrabryi-zaichik/
This service marked as VERIFIED on Tor Wiki:	http://zqktlwi4fecvo6ri.onion/wiki/Main_page

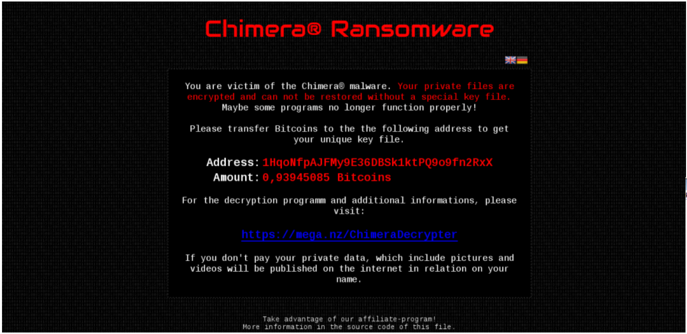
About (russian text)

[1] Including law enforcement, security researcher

The risks of using mixer(s)

- Mixer(s) can be operated by anyone having a small assets of coins (or claiming to have some).
- A random fee is taken by the mixer service.
- Attackers need to find reliable mixing and laundering service(s).
- Such service can be fake or a decoy. Various copy-cats exist on Tor or I2P.
- Mixing is just a part of the problem. How do you cash out?

Attracting your victim to become a mule



Chimera® Ransomware

You are victim of the Chimera® malware. Your private files are encrypted and can not be restored without a special key file. Maybe some programs no longer function properly!

Please transfer Bitcoins to the the following address to get your unique key file.

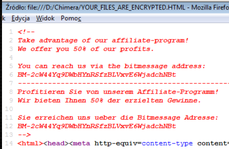
Address: 1HqoNfpAJFMy9E36DBSk1ktPQ9o9fn2RxX
Amount: 0,93945085 Bitcoins

For the decryption programm and additional informations, please visit:

https://mega.nz/ChimeraDecrypter

If you don't pay your private data, which include pictures and videos will be published on the internet in relation on your name.

Take advantage of our affiliate-program!
More information in the source code of this file.



Źródło: file:///D:/Chimera/YOUR_FILES_ARE_ENCRYPTED.HTML - Mozilla Firefo

```
<!--
Take advantage of our affiliate-program!
We offer you 50% of our profits.

You can reach us via the bitmessage address:
BM-2cW44Yq9DWbHYnRSfzBLVxvE6WjadchNBt
-----------------------------------------------
Profitieren Sie von unserem Affiliate-Programm!
Wir bieten Ihnen 50% der erzielten Gewinne.

Sie erreichen uns ueber die Bitmessage Adresse:
BM-2cW44Yq9DWbHYnRSfzBLVxvE6WjadchNBt
-->
<html><head><meta http-equiv=content-type content=
```

Conclusion

- Defense mechanisms can only be built by **knowing and understanding the attackers**.
- Installing more software or hardware is just increasing the **attack surface**.
- **Sharing** and improving your existing infrastructure (including reducing the software installed) is key to improve your security posture.
- **Logging and monitoring** are often underestimated or hidden (or even rationalized) behind meaningless dashboard.

Q&A - Contact

- info@circl.lu
- `https://www.circl.lu/`
- OpenPGP fingerprint: 3B12 DCC2 82FA 2931 2F5B 709A 09E2 CD49 44E6 CBCD
- Twitter: @adulau - @circl_lu