BTCWALL

btcwall.io

The secure storage project for bitcoins and their owners information.

Our goal – to protect Your savings!

Whitepaper 0.2 Beta-version can be upgraded.

CONTETNTS

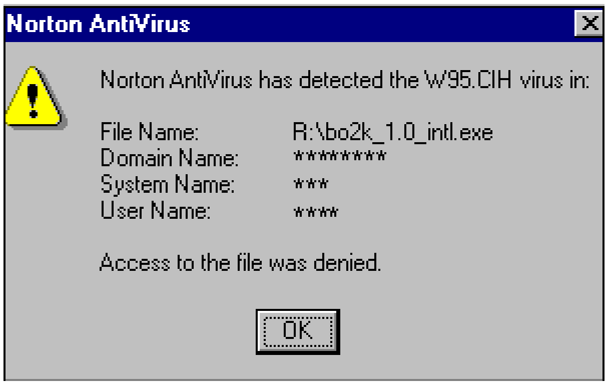
Introduction

Our company is focusing on the creation of an anonymous secure bitcoins storage system. The main advantage of the system is reliable data storage and ease of use. The system solves the problem of full anonymity of the wallet owner.

To confirm the relevance of the product, our experts conducted a study on how cybercrime will develop in 2017-2018 and why the crypto currency holders will primarily be at the center of its attention. The results of the study are represented below.

Ransomware history

20 or more years ago malicious software mostly did not bring any profit, it was made on a lark.



Norton AntiVirus has detected the W95.CIH virus in:

File Name: R:\bo2k_1.0_intl.exe
Domain Name: *********
System Name: ***
User Name: ****

Access to the file was denied.

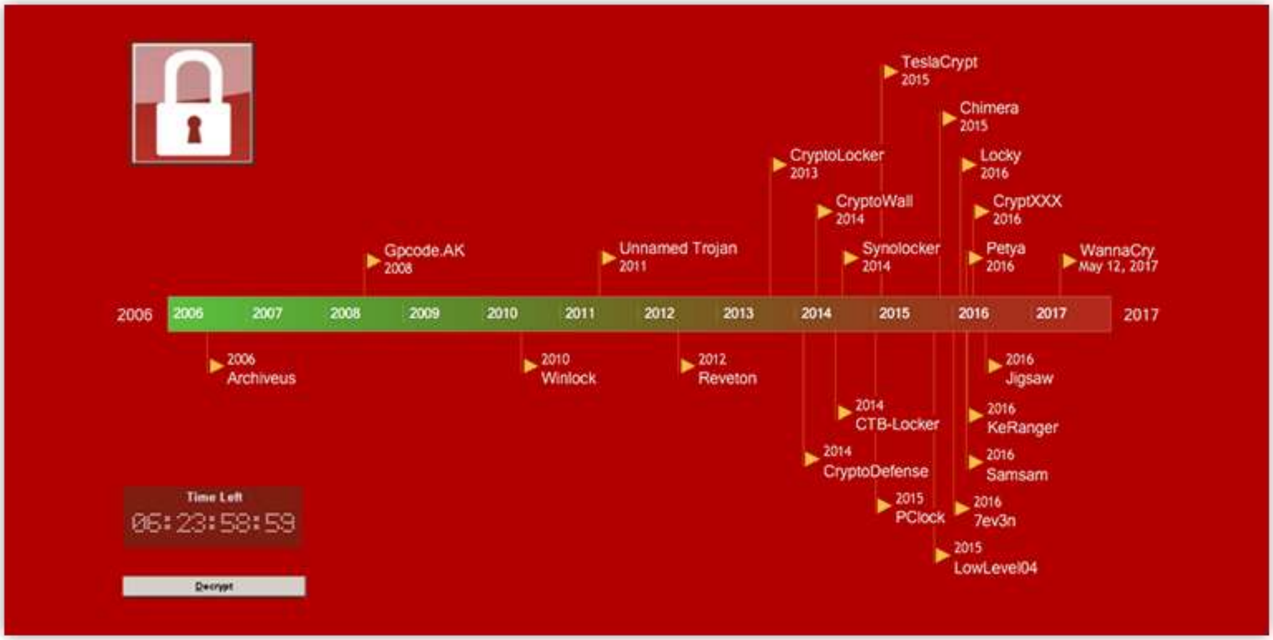
1999 CIH virus, destroyed all data on disks, free-of-charge.

With the advent of commerce and credit cards, carders and the first botnets stealing and intercepting data appeared on the Internet. Botnets and credit cards theft flourished while making a profit. Over time, the botnets were actively stricken, and new means of protection were implemented, as a result of which botnets support became unprofitable for their owners. In particular, this was due to:

- After setting up the botnet, it immediately gets into the trackers of network attacks, after which it will not last long;
- bulletproof hosting service costs at least 400$ monthly
- botnets working through p2p and TOR do not solve the problem, antiviruses have become much smarter.
- For a botnet operating it is necessary to crypt it and update it for all users every few hours - it costs about $ 40 at a time and can reach up to $ 5,000 per month, and does not ensure unconditional success.
- If earlier it was possible to buy traffic, send it to a thread and get a very large amount of infected machines as a result, now it is almost impossible. In this way you can infect only abandoned, not updated systems, which are fat lot of use.
- Traffic has also become more difficult to get because of the huge number of bots and competition, today it's just impossible to buy ready-to-use high-quality loadings.
- There are problems with withdrawal of funds

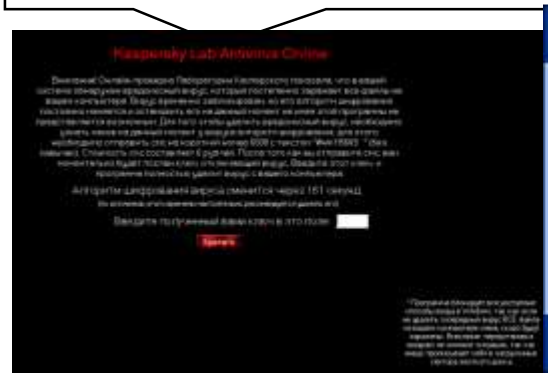
The problems described above led to the fact that almost all cybercriminals switched from botnets and theft to simple extortion for restoring access to computers.

Ransomware history:



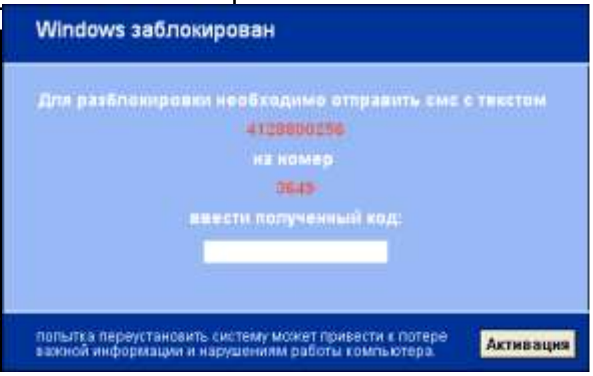
The first programs, extorting money for restoring access, were extremely wretched and primitive. Getting into the user's computer, through browsers vulnerabilities, they blocked the monitor and demanded a ransom. No files were encrypted, the lock was easy to remove. In the case of payment, as a rule, they also did not disappear.

2009-2012 evolution of primitive ransomware, files were not encrypted, money was accepted through SMS or gift card.



Kaspersky Lab Antivirus Online

[illegible]



Windows заблокирован

Для разблокировки необходимо отправить смс с текстом

4128800256

на номер

3649

ввести полученный код:

попытка переустановить систему может привести к потере важной информации и нарушениям работы компьютера.

Attention! Kaspersky Lab online check has shown that your system has detected a malicious virus that gradually infects all files on your computer. The virus is temporarily blocked, but its encryption algorithm is constantly changing and stopping it at the moment without having this program is not possible In order to remove a malicious virus , It is necessary to find out what the encryption algorithm is at the moment, for this you need to send a text message to the short number 6008 with the text * # win1l5669 * (without quotes) The cost of the SMS is 6 rubles Once you have sent a text message, you will be sent instantly disables the virus key Enter the key, and the program will remove the virus completely from your computer.

The virus encryption algorithm will change after 161 seconds.

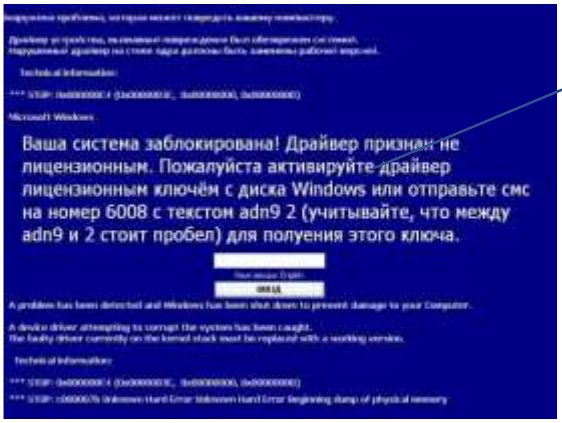
(After this time it is highly recommended to delete it

Enter the received key to this field:

Delete

The malware blocks all other input methods in Windows, because if you do not remove malicious viruses, all files on your computer will soon become infected. Warning: reinstalling Windows will not solve the situation. Since the virus registers itself in the boot sectors of the hard disk

For unlocking send SMS with the text 4128800256 to the number 3649. Enter the received code:



Microsoft Windows

Ваша система заблокирована! Драйвер признан не лицензионным. Пожалуйста активируйте драйвер лицензионным ключём с диска Windows или отправьте смс на номер 6008 с текстом adn9 2 (учитывайте, что между adn9 и 2 стоит пробел) для получения этого ключа.

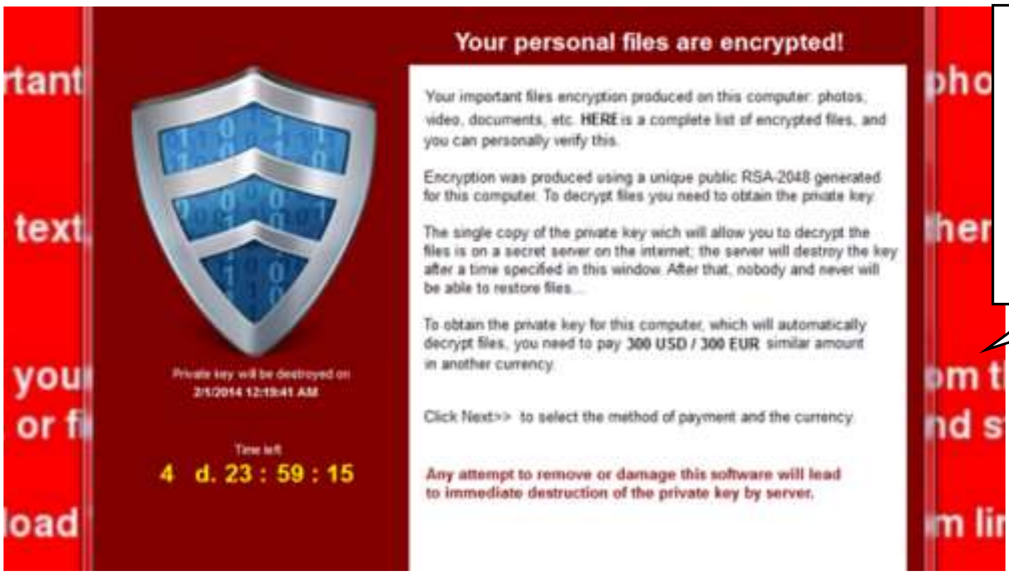
A problem has been detected and Windows has been shut down to prevent damage to your Computer.

A device driver attempting to corrupt the system has been caught. The faulty driver currently on the kernel stack must be replaced with a working version.

Technical information:

Your system is locked! The driver is recognized as uncertified. Please activate the driver with a license key from the Windows disk or send an SMS to the number 6008 with the text adn9 2 (note that there is a space between adn9 and 2) to get this key.

This method could be used to easily infect millions of users by simply buying traffic or ready loadings. Despite the fact that bitcoin appeared in 2009, cybercriminals did not hurry to implement this new way of accepting money, but continued to use the usual methods in the form of gift cards and codes.



Your personal files are encrypted!

Your important files encryption produced on this computer: photos, video, documents, etc. **HERE** is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key wich will allow you to decrypt the files is on a secret server on the internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** similar amount in another currency.

Click Next>> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to immediate destruction of the private key by server.

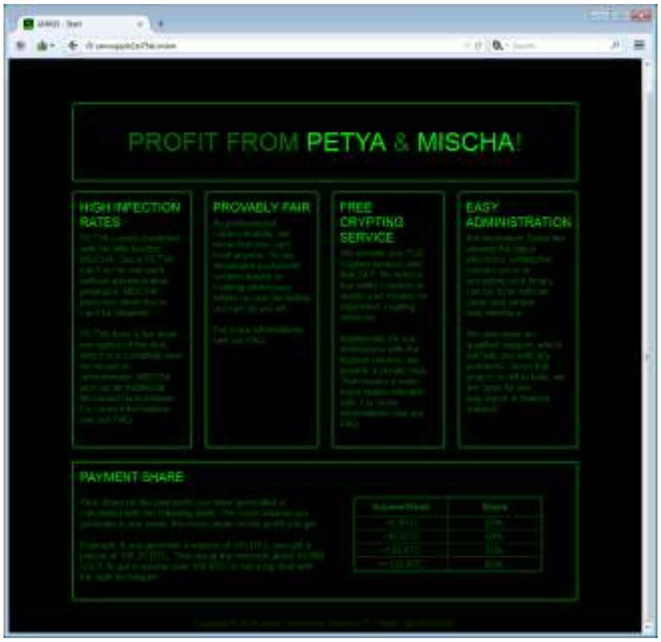
Private key will be destroyed on
2/1/2014 12:19:41 AM

Time left
4 d. 23 : 59 : 15

2013 one of the first known viruses encrypting data without recovery possibility.

Cybercriminals needed more than 5 years to switch to bitcoins and appreciate it! Extortionists, encrypting files and requiring ransom in bitcoins, began to actively develop since 2013. At the moment, they completely replaced primitive screen lockers, resulting in almost complete disappearance of botnets and other malicious programs.

To date, to make a profit, it's enough just to deliver the extortion program to the user. Anonymity (with proper use) and the convenience of bitcoins allowed to demand any amount of ransom almost with impunity. Extortionists developed, affiliate programs appeared, and in order to earn millions it was enough just to succeed with delivery the finished product to the user.



PROFIT FROM PETYA & MISCHA!

HIGH INFECTION RATES

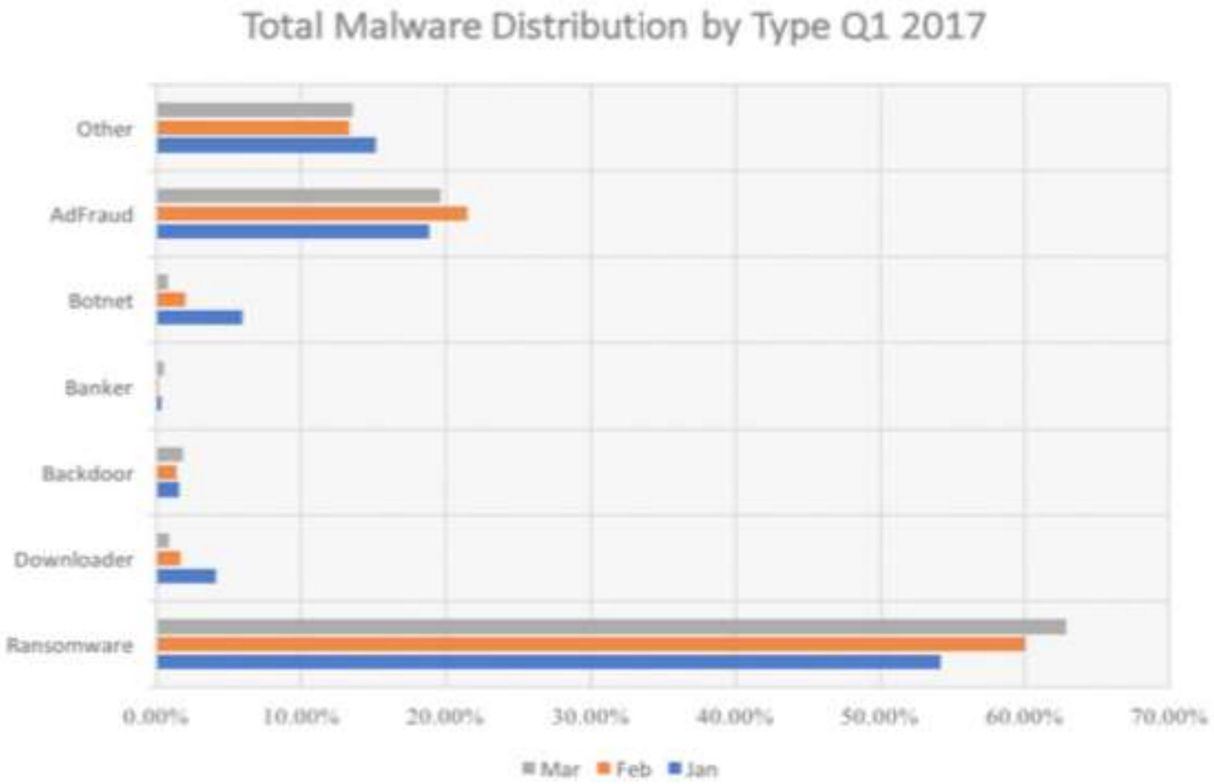
PROVABLY FAIR

FREE CRYPTING SERVICE

EASY ADMINISTRATION

PAYMENT SHARE

2016, one of the first partnership programs for extortion, today revenues have fallen so much that almost all the programs closed down.



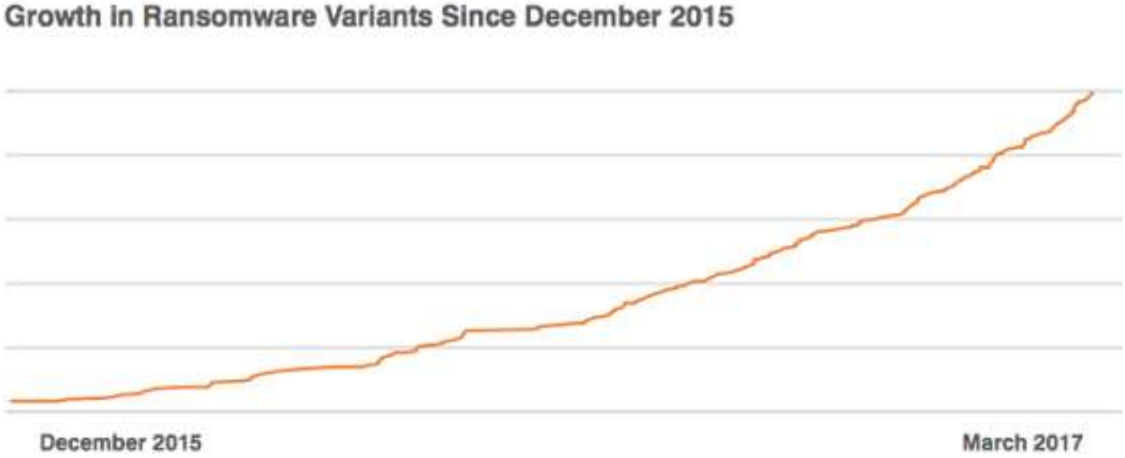
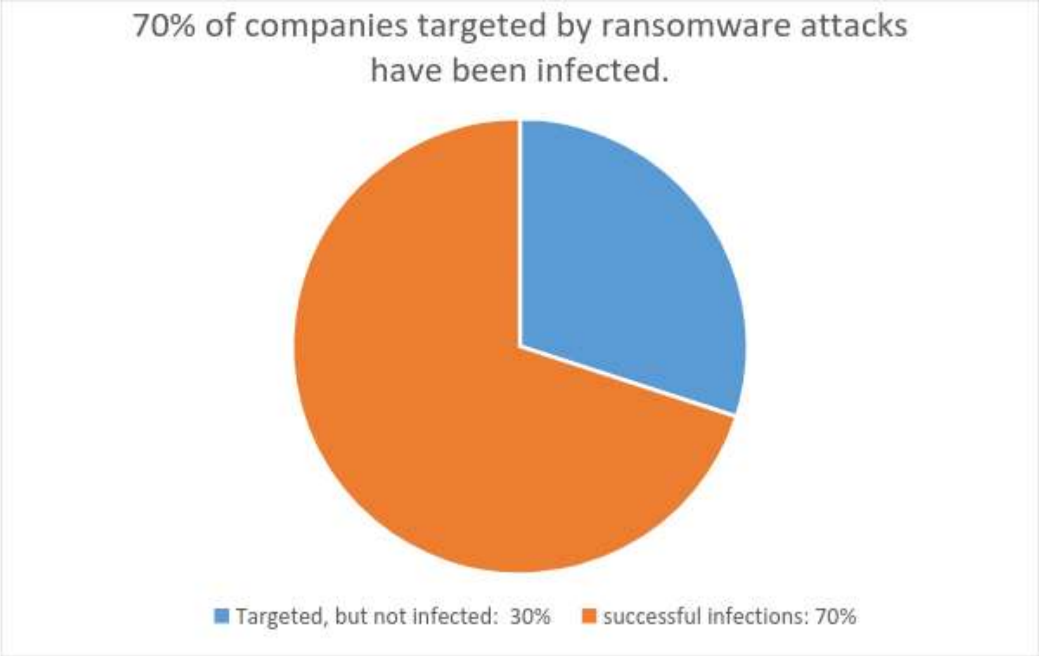
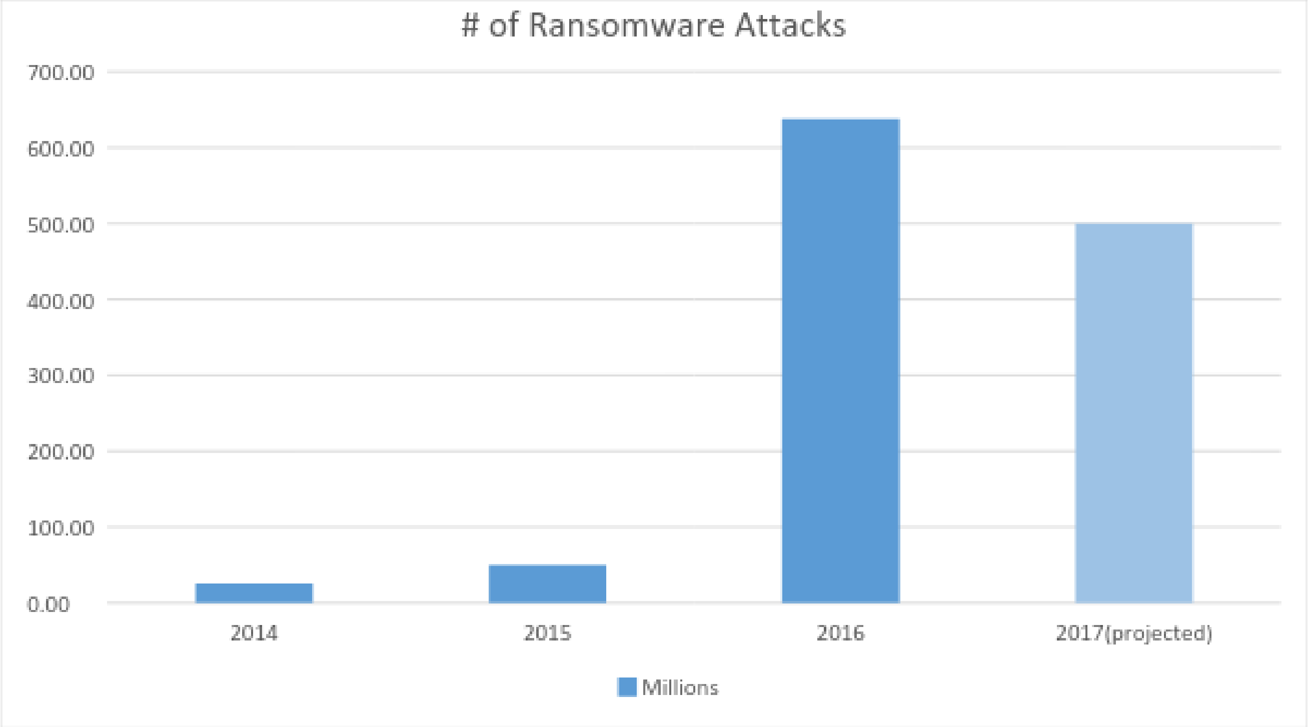
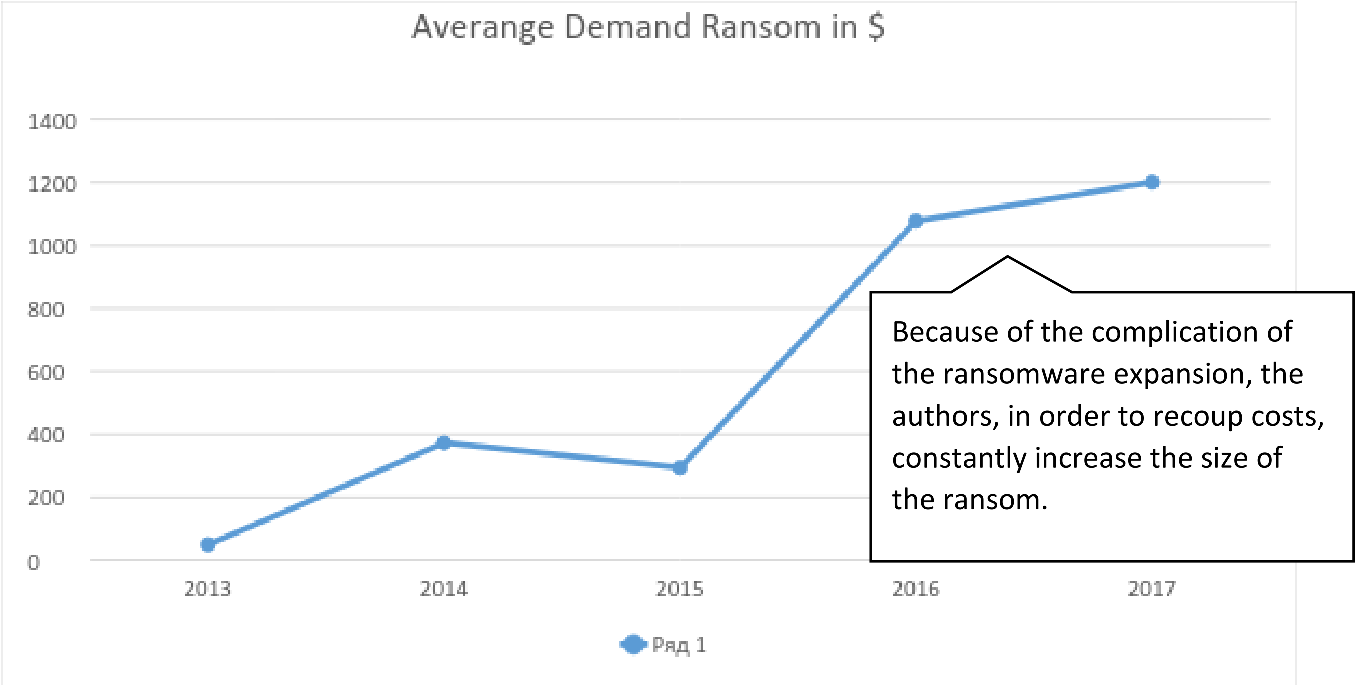


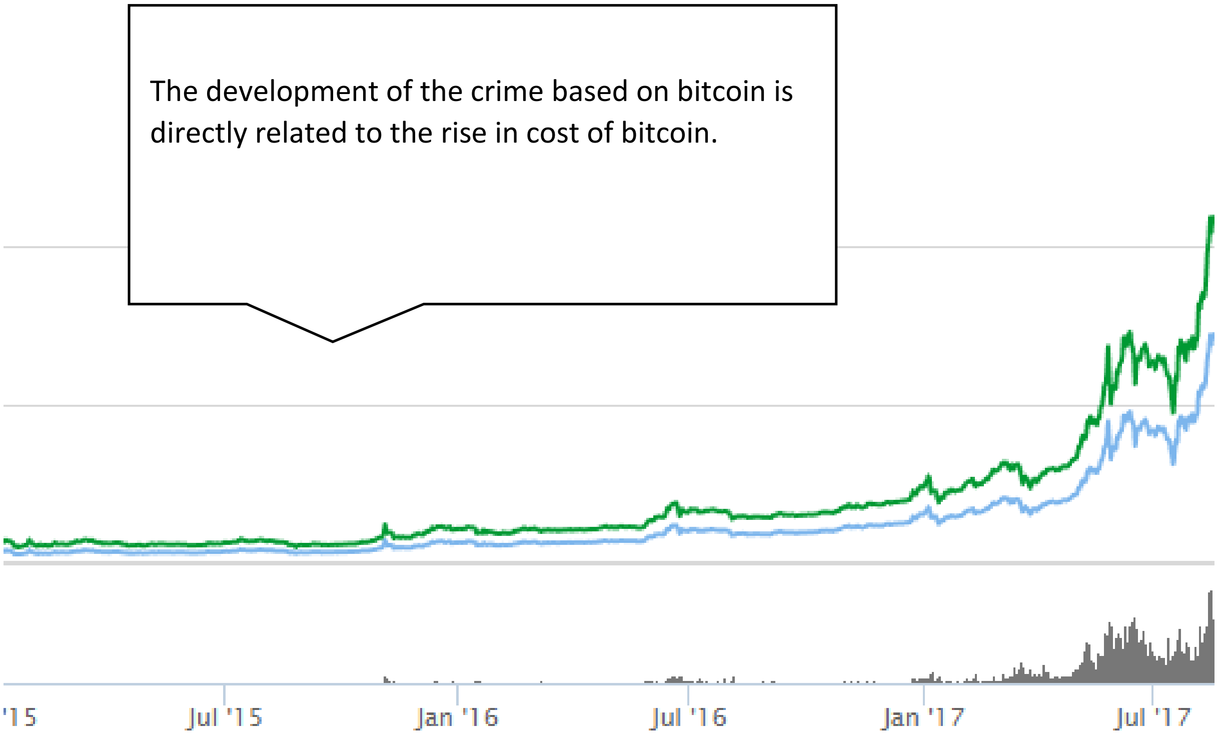
Figure 6: Indexed growth in total number of observed ransomware strains, December 2015-March 2017


70% of companies targeted by ransomware attacks have been infected.
Targeted, but not infected: 30%
successful infections: 70%


# of Ransomware Attacks
700.00
600.00
500.00
400.00
300.00
200.00
100.00
0.00
2014
2015
2016
2017(projected)
Millions

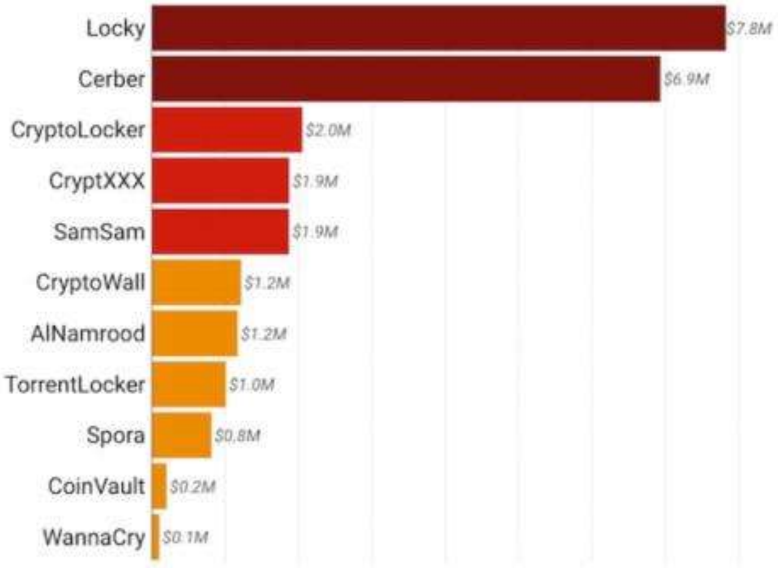


Because of the complication of the ransomware expansion, the authors, in order to recoup costs, constantly increase the size of the ransom.

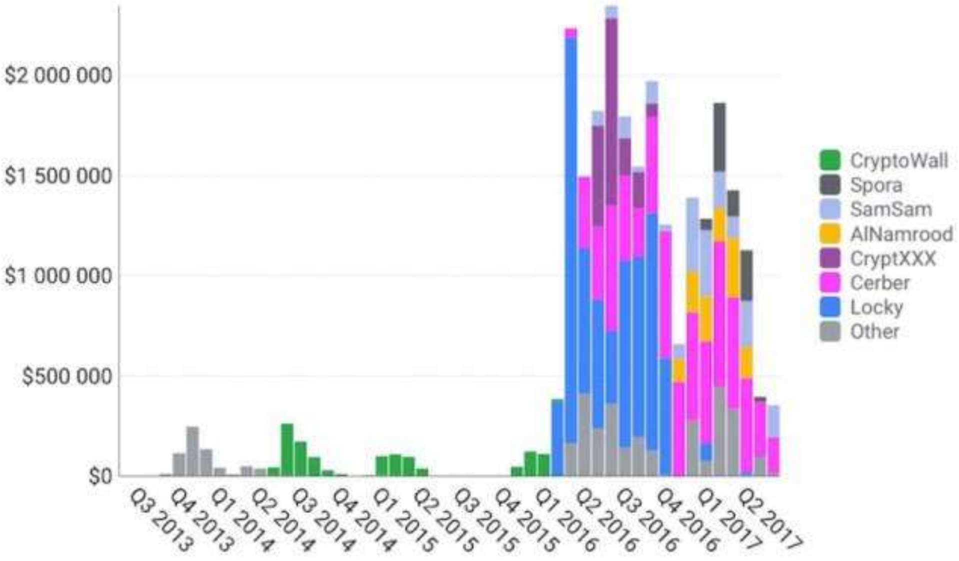


The development of the crime based on bitcoin is directly related to the rise in cost of bitcoin.

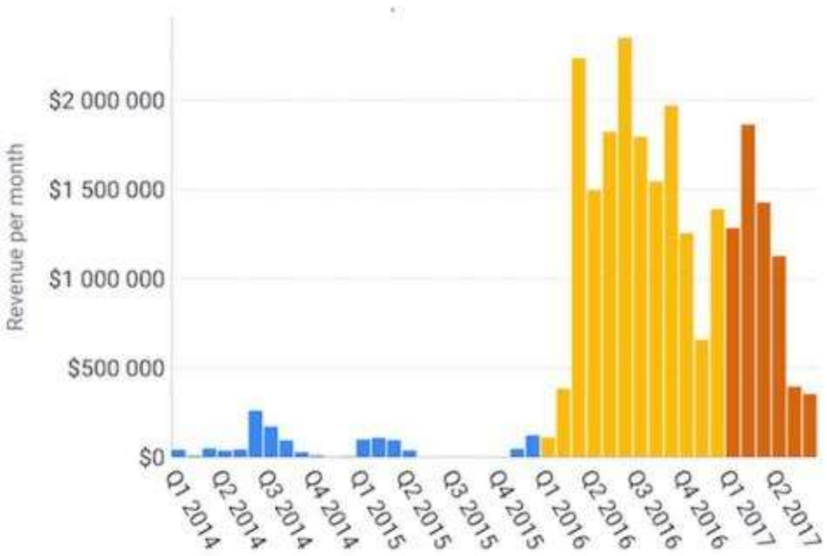
Despite the growth graphs of extortion, including an increase in the cost of ransom, the incomes of extortionists are rapidly falling. This is an alarming signal about the growth of new types of crimes, primarily in the field of theft of the crypto currency.



The ecosystem is dominated by a few kingpins



A fast changing market



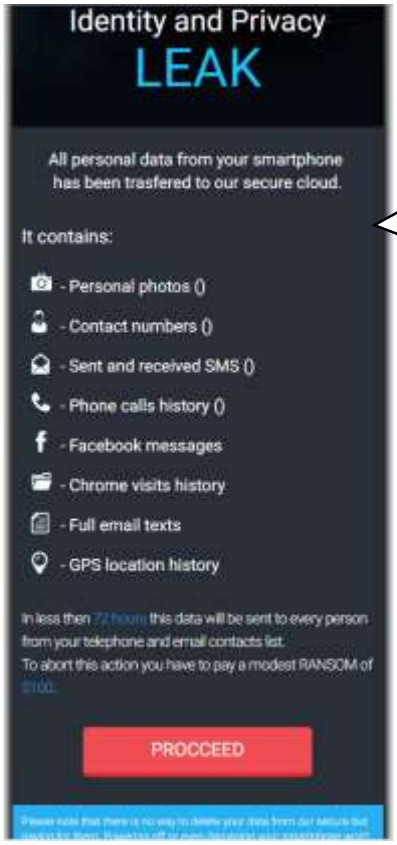
In 2016 ransomware became a multi-million $ business

At the same time, extortion for the recovery of data encrypted by the virus is on the decline. The method brings to its owners progressively smaller income. In 2017, the owners of the WannaCry virus obtained ransom only $ 60,000 (without taking into account the increase in the cost of bitcoin) with damage of more than a billion dollars, and the notPetia virus income was only $ 7,000. As the result of this, all well-known partner programs closed down: Petia RAAS, Cerber RAAS and many others.

It's even harder to get loadings. The first protection programs against unauthorized file changes began to appear only at the end of 2016. Now such protection is added to the usual antivirus content, and in new versions of Windows 10 such protection will be imbedded by default into the system core.

What is the future of ransomware

Data encrypting ransomware do already change tactics. There has appeared a first ransomware that sends user personal files to all contacts in his social network in case of non-payment of ransom.



Identity and Privacy
LEAK

All personal data from your smartphone has been trasfered to our secure cloud.

It contains:

- - Personal photos ()
- - Contact numbers ()
- - Sent and received SMS ()
- - Phone calls history ()
- - Facebook messages
- - Chrome visits history
- - Full email texts
- - GPS location history

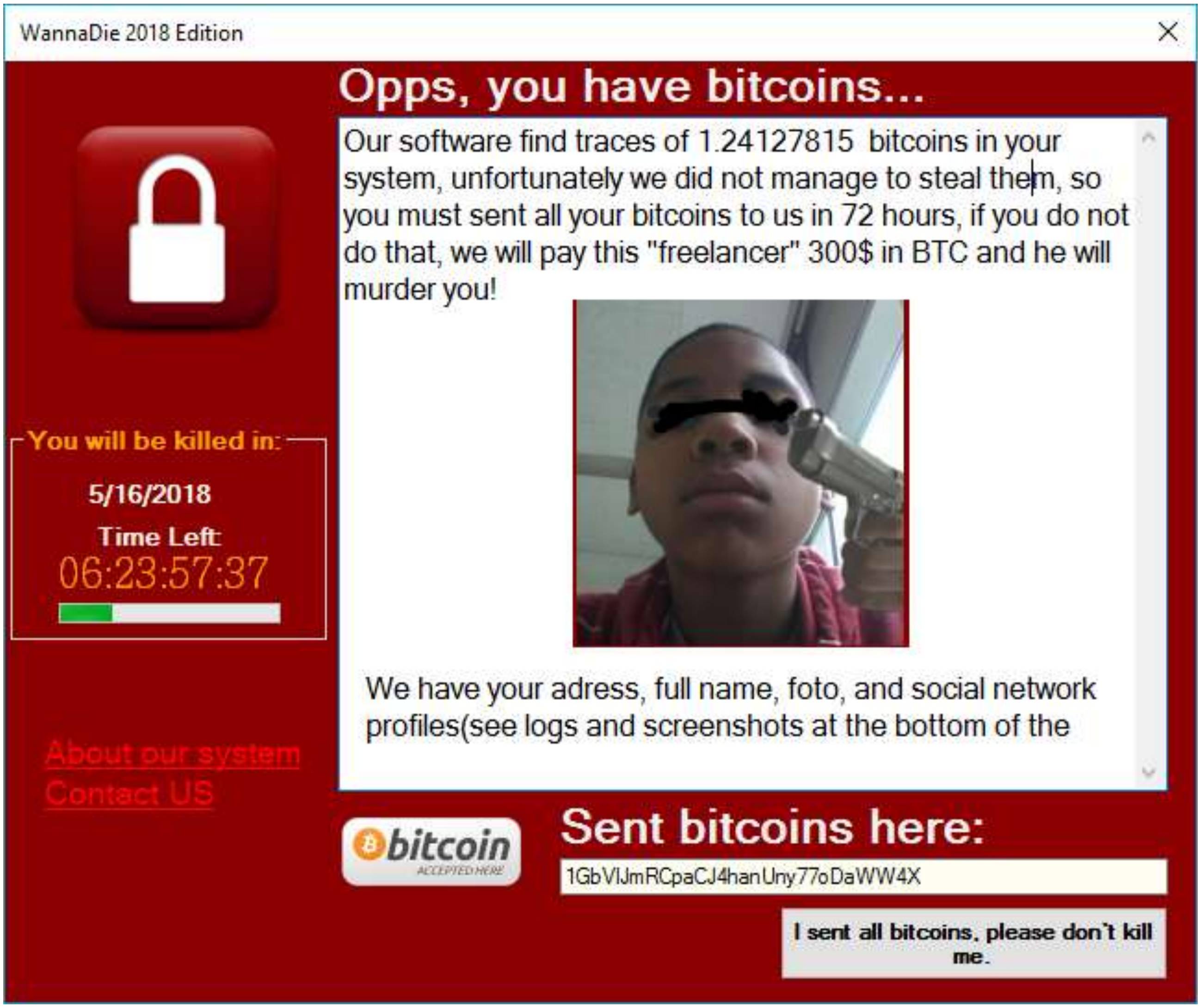
In less then 72 hours this data will be sent to every person from your telephone and email contacts list.
To abort this action you have to pay a modest RANSOM of $100.

Please note that there is no way to delete your data from our secure but [illegible]

2017, Evolution of ransomware, now programs threaten the spread of personal data in the event of non-payment.

The near future of crime and extortion:

Our specialists have developed a concept for the future of a new class of ransomware (#murderware) which will be dangerous and against which our project BTCWALL will protect you.



WannaDie 2018 Edition

Opps, you have bitcoins...

Our software find traces of 1.24127815 bitcoins in your system, unfortunately we did not manage to steal them, so you must sent all your bitcoins to us in 72 hours, if you do not do that, we will pay this "freelancer" 300$ in BTC and he will murder you!

We have your adress, full name, foto, and social network profiles(see logs and screenshots at the bottom of the

You will be killed in:

5/16/2018

Time Left:

06:23:57:37

About our system

Contact US

Sent bitcoins here:

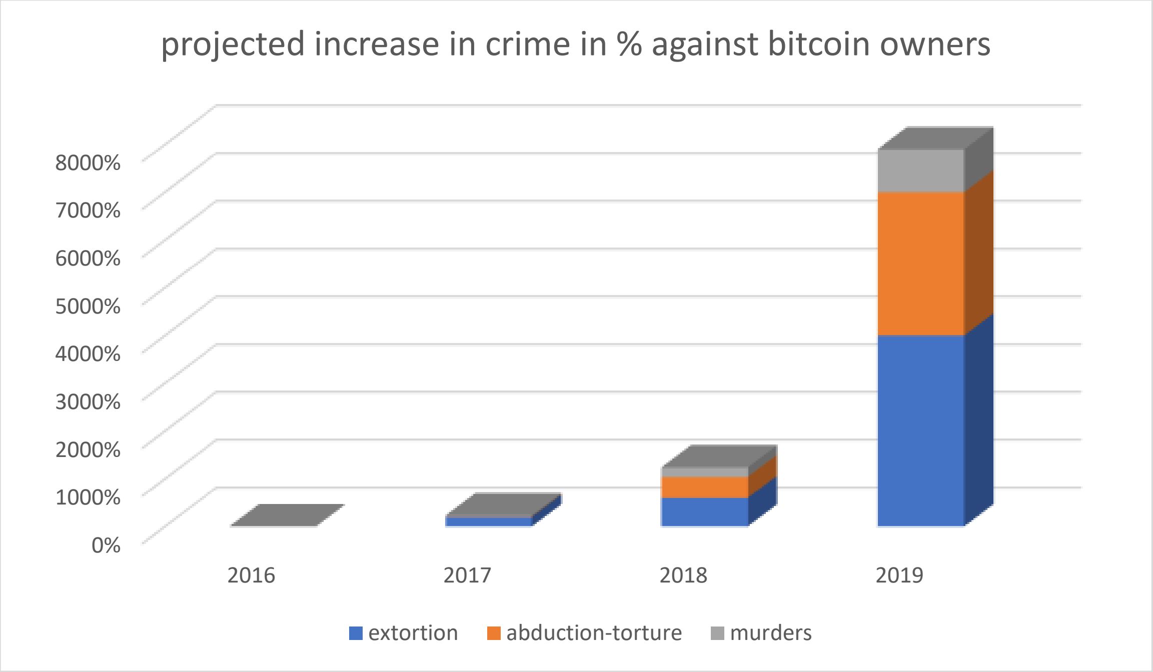
1GbVlJmRCpaCJ4hanUny77oDaWW4X

I sent all bitcoins, please don't kill me.

Our forecast for 2017-2020:

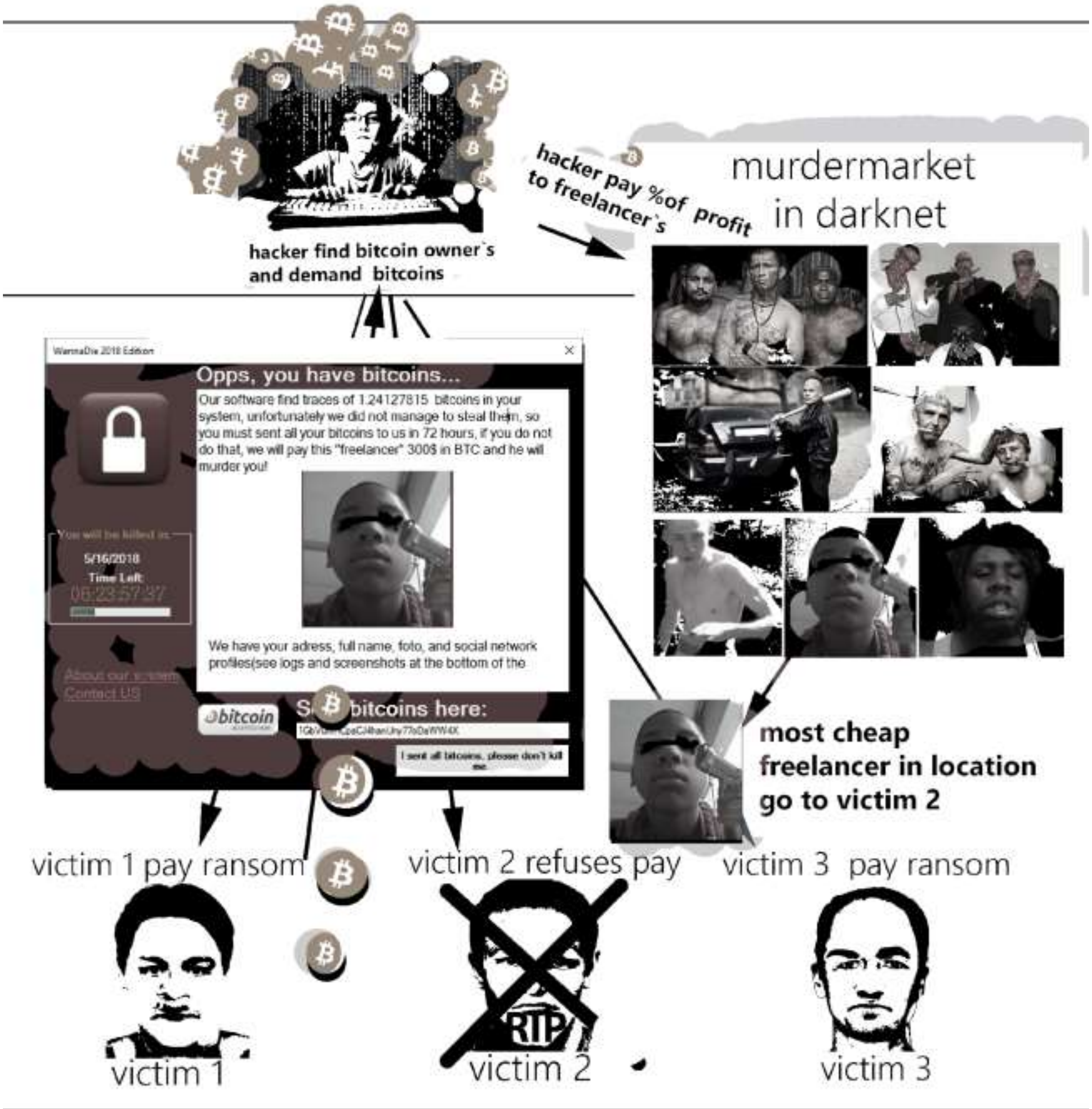
- 2017 - Malicious software is reoriented to steal bitcoins and crypto currency.
- 2017-2018 - Viruses that not only steal bitcoins, but also:
    - Search for traces of their use, in logs, deleted files, in browser history, bookmarks, as well as in just installed wallets of crypto-currency in the system and their residual files.
    - demand to transfer part or all of the bitcoins to the specified address, and in case of refusal scare with police or gungsters depending on the country of residence. Display the victim's address received automatically from the found logs or by ip address, if possible automatic photo from webcams.
    - Distribute (sell) on the Internet (primarily in darknet) to interested persons information about the owner of the crypto currency.
- 2018-2020 sites rises in the darknet, similar to the sites for selling drugs, specialized in selling information about the owners of bitcoins. The buyers of such information are low-level criminals, extortionists and murderers, people who are ready to raise money by any possible means.

Our forecast for the number of crimes against the owners of bitcoins:



The operational scheme of murder programs (#murderware) at its peak of development, according to our forecasts, will look something like this:

Specialists of btcwall.io
developing protection against a new type of crime,
this is concept how future ransomware may work:



Opps, you have bitcoins...

Our software find traces of 1.24127815 bitcoins in your system, unfortunately we did not manage to steal them, so you must sent all your bitcoins to us in 72 hours, if you do not do that, we will pay this "freelancer" 300$ in BTC and he will murder you!

We have your adress, full name, foto, and social network profiles(see logs and screenshots at the bottom of the

S[illegible] bitcoins here:

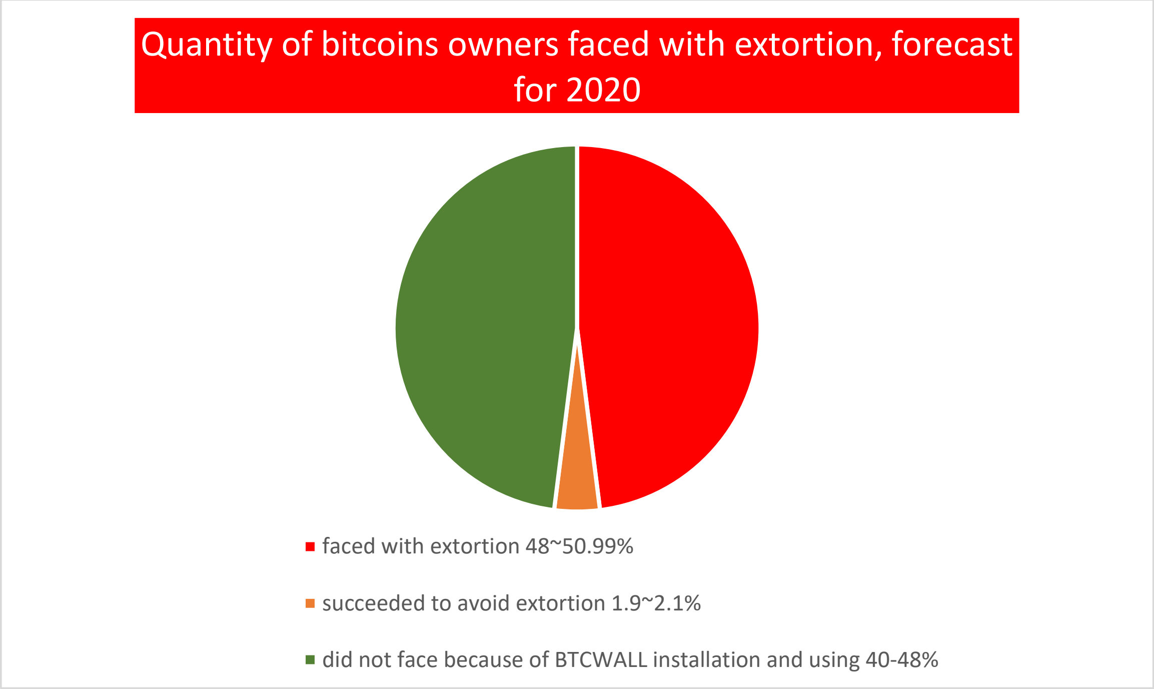
1GbV[illegible]CpaCJ4hanUny77oDaWW4X

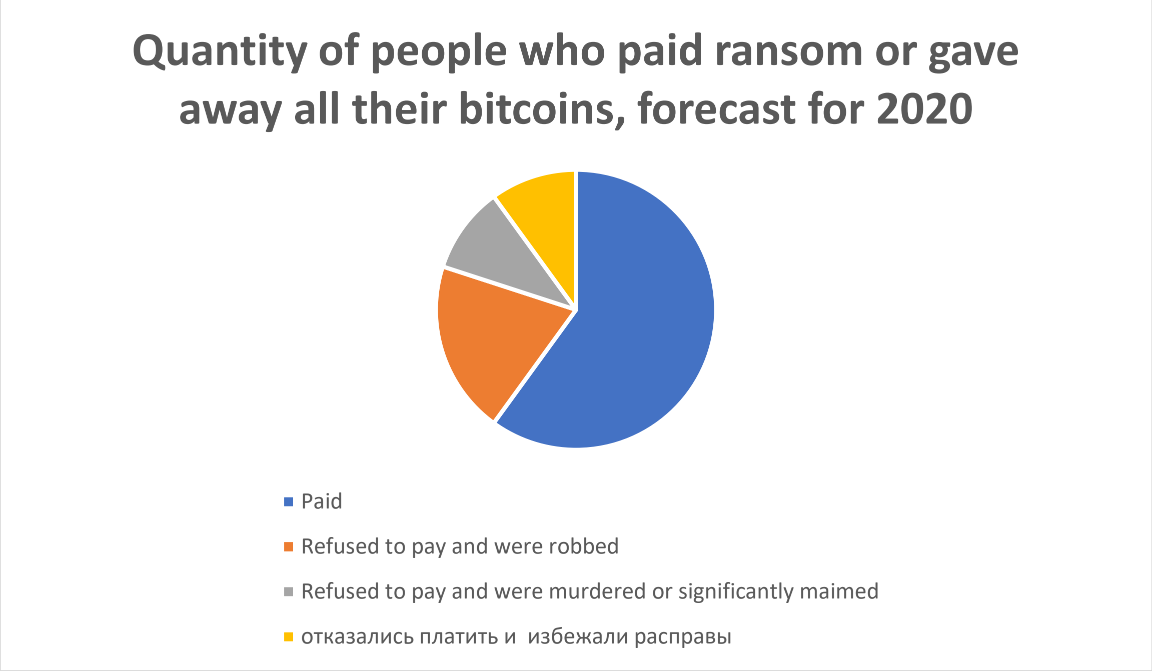
BTCWALL is bitcoin-wallet, which is not only protect bitcoins, but also their owners.

Why bitcoins owners become victims of extortion??

- Bitcoins can not be tracked when used correctly.
- The owners of bitcoins are, as a rule, the least protected people from torture, kidnapping and murder. Miners, ICO investors, Investors, Traders, and ordinary people postponing bitcoins for the future will be the first to fall for the influence of crime.
- In most countries, after theft-extortion of their bitcoins, they can not even apply to police, and in some they can even receive prison terms for the possession and use of bitcoins.
- At the moment, the owners of bitcoins are very easy to track.
- A malicious program that searches for traces of using bitcoins in computers is much more difficult for antiviruses to track than any other malicious software.

Why will criminals threat with the dissemination of information about the owner and with reprisal for the purpose of bitcoins extortion? Because the programs of extortionists, encrypting files, even in their best days brought a maximum of 1-2% of payment from all successful attacks. Violence threat can result up to 90% of payments from extortion, in the case if victims will consider threats real. The reality of cybercriminal threats can be provided by organizing a couple of real cases. At the same time, novelty and uniqueness will allow to quickly and widely disseminate information through the media.





Quantity of people who paid ransom or gave away all their bitcoins, forecast for 2020

How will criminals track bitcoins owners?

Bitcoins owners, in addition to the newly created malicious programs, from which BTCWALL will protect, will be searched for by old, long-proven methods. If you have ever registered on any site or service associated with bitcoins, you are already in special bases called "bitcoin grinder". People who get into them, are to be hacked first of all. Almost all known sites are usually cracked. Verify this by going to https://haveibeenpwned.com/ and entering your details. Such sites contain databases that are available to anyone. Real figures of hacking are unknown and can reach up to 99% of all sites and services with all users in them. Attackers have access not only to your passwords, but also to personal data. Having received them, all means of fraud and hacking are in use. Owners of large balances in the near future will get into bitcoin grinders for offline "processing". The bases will be supplemented by the exact place of residence of account holders. Protection against such attacks can only be realized by creating special additional services for using crypto currency and protecting owners. This is what we will be doing in the process of creating the ICO.

How bitcoins are being stolen nowadays

Here is a small example of how your bitcoins are stolen today and what will our wallet secure from:

If you get into bitcoin grinder (a database of bitcoins owners with emails, phones and passwords, if you have registered on any site related to crypto-currency, then be sure - you and your passwords are already there), all your passwords ever entered on the sites + the most simple passwords are selected at a speed of 100,000 per minute, and this is only on one computer by one intruder. Thousands of hackers and millions of bots will use this database every day on all sites where your bitcoins or useful information can be stored. The license for such software costs about $ 5-12, but there are also hacked free versions. Advanced cybercriminals prefer to use their own botnets consisting of millions of computers.

In case when it is known that you have more than $ 10 in bitcoins, you are hacked even more actively. If password attack didn't succeed or you have phone authorization, criminals will hack your phone, gaining access to all your accounts. In some services and countries they can hack a phone for free, simply by contacting technical support and asking for a redirect. If this does not work out, then criminals just reissue the phone to other user. They usually do this for free through their accomplices from the operator company. If this is not possible, then you can buy this service on the black market. Recovery of any phone number costs $ 150 -200 $.

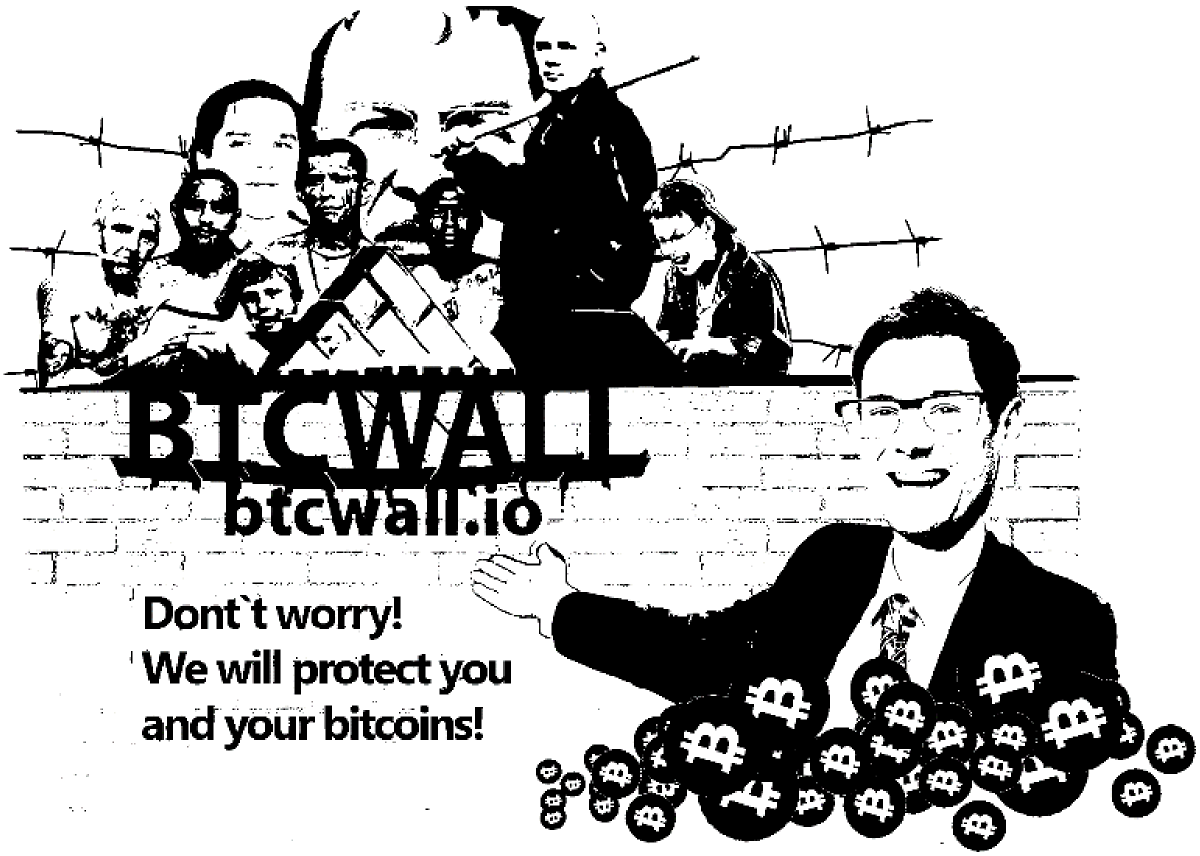
If there are signs that you have a significant amount, then they will try to hack your computer. They will send you a trojan, for example, through your friends. Criminals will hack them first, and then they will send you with the help of social engineering, and this is only if you no longer have vulnerabilities in the system. It is very likely that you already have some malicious software. Malicious software can completely transfer the control of your computer, record all your actions, substitute addresses for sending bitcoins in the clipboard, replace any visible and entered information and, naturally, steal bitcoins, passwords and all files that can be useful to attackers. Tracking cybercriminal is almost impossible, since all hacking occurs as a rule from already infected computers.

Any file that you can download from the Internet can be infected with anything and be invisible by any antivirus software. It can even be the antivirus itself from the official site. Cybercriminal hacks websites thousands in a day, stealing all the information there and infecting everything. Often this is done in fully automatic mode. Also not only sites can be hacked, but your router too, provider, or domain site.

Even if you did not download anything, your computer, router, Wi-Fi network, and any device in your home can be and will be hacked. Criminals have not yet found all the vulnerabilities in our PCs, and if they have, they do not use them in large numbers in order that they not to be corrected. But if you have bitcoins, the will exactly use everything they can. The more new software, hardware, and patches are issued, the more potentially new vulnerabilities appear. If you now connect a computer with an un-upgraded system or a weak password, it will be guaranteed to be hacked within 2-15 minutes. During this time, all information will be stolen, a crypto currency miner will be installed, and the files will be encrypted by a WannaCry ransomware. This is today's reality.

These are just some elementary ways that every beginning hacker of school age knows. Therefore, be sure to know and understand the following: if you store bitcoins in any online service, you will lose them very soon with a probability of 99.9%. If you store bitcoins on a computer connected to the Internet, you too will lose everything. The only solution is to use BTCWALL or correctly made cold storage that is not convenient without the use of BTCWALL and is too difficult for many people.

We also need to understand that if criminals will not succeed to steal bitcoins from you remotely, they can come to you today to force you to give bitcoins. Only our storage system can protect bitcoins and their owners from this - BTCWALL.



BTCWALL

Our wallet is a protective complex of programs and services for maximum protection of bitcoins, not only from theft, but also to hide traces of using bitcoins in systems. Depending on the size of the collected funds, we will add new functions to it and connect new services.

The existing means of protecting bitcoins and limitations

Online wallets, as well as wallets that store or accept private codes can not be considered even theoretically to store bitcoins from theft. If your system on which the bitcoins are located is connected to the Internet or to a network where the devices have Internet access, then you are guaranteed to lose all means.

Today it is safe to store bitcoins only when using cold storage or on systems not connected to the network. Wallets that support cold storage are inconvenient to use, difficult to master and do not have sufficient functionality.

None of the wallets except BTCWALL has protection from "fools" who still decide to launch a wallet on a computer connected to the Internet or generate a new wallet on it even with subsequent removal.

No wallet or antivirus, except for BTCWALL, has the functionality of secure file deletion. In order to completely remove the file, you have to erase it and overwrite the empty space at least 35 times, otherwise the data can and will be restored.

No wallet or antivirus except BTCWALL has special protection against data spoofing in the clipboard.

There is not any commercial solution for storage and protection of bitcoins, no one is responsible for lost bitcoins or vulnerabilities in software.

None of the wallet or service has the ability to urgently secretly call the police while physical contact with criminals who attempt to steal the bitcoins from the owner by robbery and torture.

All known wallets, except for BTCWALL, do not assume any built-in protection against malware, and antiviruses are completely useless towards new threats. They are more likely to harm than to benefit. Antivirus can detect only the already known program that has infected dozens of computers and got into anti-virus databases, while malicious code can be infected or slightly changed and the virus will again be invisible for all antiviruses. Even now there are viruses that are able to rewrite their own code.

None of the wallets, except for ours, is trying to hide the traces of the presence and use of bitcoins. When criminals appear who will actively monitor crypto currency users, torture and extort money from them, it will take at least several years to implement the protection that is already in our BTCWALL wallet.

How does BTCWALL work and what is that?

The storage system of bitcoins is a super-secure wallet that provides the greatest possible protection and anonymity.

(In the description below, we list what already existing features in our test version of the wallet, which we made for ourselves. After fundraising, we will completely rewrite the code and significantly improve the functionality and add new features.)

The capabilities of the developed BTCWALL storage system

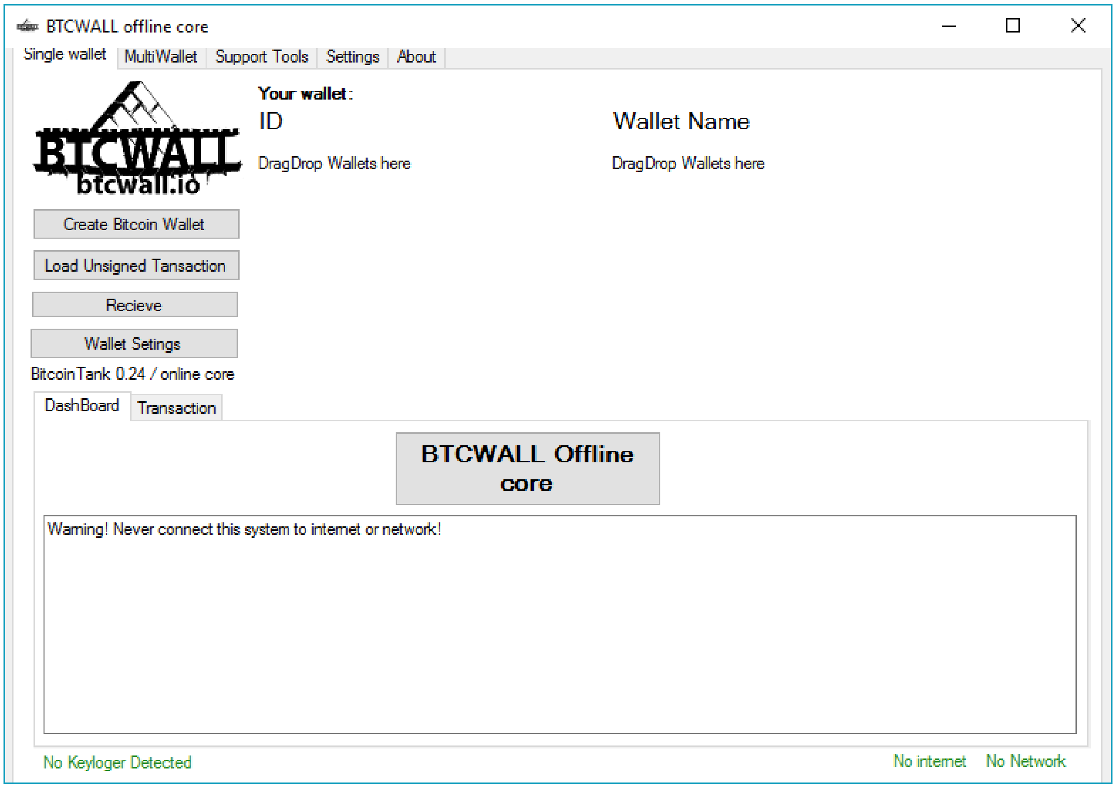
- The generation of new private keys, as well as access to them are possible only on a system completely disconnected from the Internet.
- The wallet has a very simple interface and protection from the foolproofing, even the child can now safely store the bitcoins and hide their use.
- The wallet is divided into 2 separate programs: one for reliable cold storage of private keys and transactions signing; via the second you can watch the balance of the wallet, create offline transactions for signing in the first program.

- The wallet supports unlimited generation of both wallets and addresses to them
- The purse is launched in a portable mode, in order not to leave traces of its presence, for simplicity and ease of use. It can safely remove itself.
- By default, the wallets are stored in a hidden format using stenography and additional protection, the wallets are masked by randomly generated images or in any user specified file.
- In one file you can save both one wallet with all addresses and transaction history, and unlimited number of wallets.
- Using a unique wallet storage format allows you to add additional protection.
- The wallet has the built-in specialized protection against malicious programs aimed at stealing bitcoins, for example, by using a spoofed address in the clipboard, it also has built-in protection against any keyloggers.
- The wallet hides its presence in the system for the security of the bitcoins, the wallets are masked as ordinary files, the wallet never automatically downloads the last used wallets in order not to give out the location of the position.
- The wallet automatically deletes logs of using bitcoins in the system, and also safely deletes files without the possibility of recovery.
- Using a unique format for wallets storage allows you to add additional protection, in case of robbery, torture and extortion, by entering the code symbol for the password, bitcoins can be automatically transferred to a secure address, and the wallet itself will operate in a fake transaction mode.
- The purse will have built-in premium services such as a hidden call to the police and private security company when trying to physically extort the bitcoins from the wallet owner and fix their actions on the microphone or webcam. Premium subscription allows you to order a personal bodyguard in the event of an important negotiation or sale of bitcoins.
- The wallet will have a built-in bitcoin mixer, you will not be able to track transactions and balance of your wallet for criminals.
- The wallet will have a built-in anonymous distributed exchange, working on the blockchain, you can completely anonymously and reliably exchange bitcoins directly from your wallet.
- The wallet can work either with a full blockchain base or remote on anonymous servers in the TOR, the wallet has a built-in TOR client with a separate thread and protection against disconnection, the leakage of the real IP address is excluded. All wallet contacts with additional developer services are also carried out through the TOR, but in a separate thread.
- The wallet supports simultaneous work with an unlimited number of wallets, can generate millions of wallets at a time, and also check their balance and allow to work comfortably with them. In this case, you can save all wallets in one file, hidden and protected with stenography and additional protection.
- In the future the wallet will support other crypto-currencies, as well as new functions according to the wishes of users.
- The wallet constantly informs the owner about new threats and fraudulent schemes used by criminals, which are processed online by our experts.
- The authors of the wallet are interested in protecting people, since the wallet will be profitable because of licenses sales and premium subscriptions. The authors will constantly improve the protection and security by adding new features.

The in-depth performance review of BTCWALL

Our wallet consists of 2 separate programs.

1. Offline part of the wallet intended to generate private keys, store wallets and sign transactions, can only be used on the device completely disconnected from the Internet. The program constantly checks the ability to connect to the Internet and, if found, displays a warning and will not allow you to create private keys and sign transactions. It will also block all network packets. By default, the wallet supports stenography and all private keys are stored secretly as randomly generated files, and it is possible to select any file in which private keys will be hidden using stenography. To use hidden wallets in files, you just need to select this file in the program.

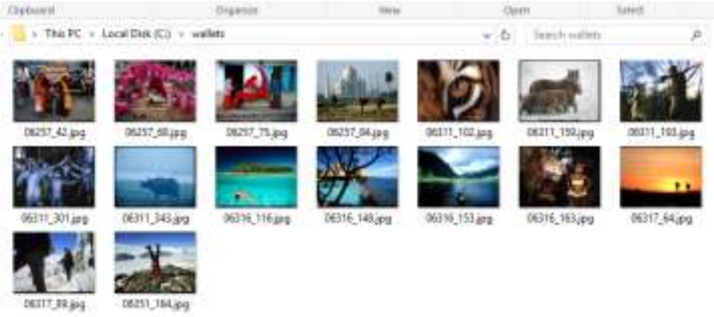


Waming! Never connect this system to intemet or network!

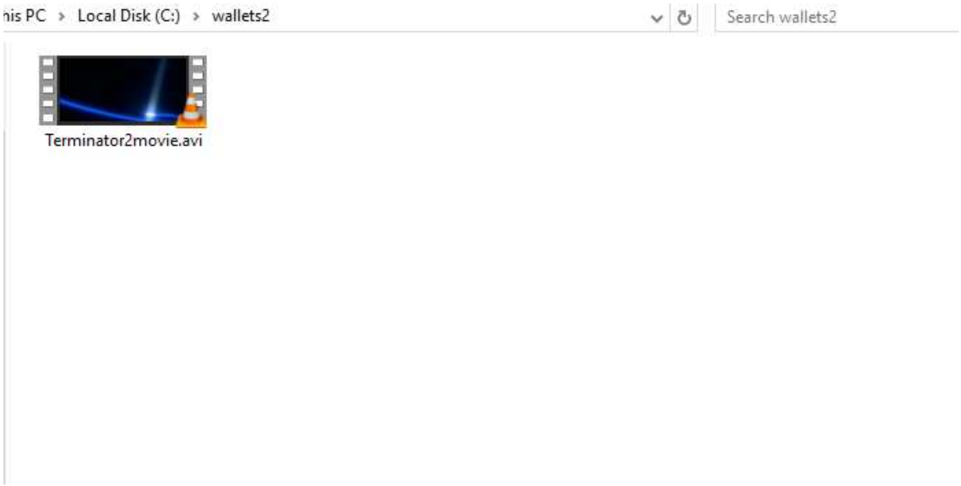
No Keyloger Detected

No intemet No Network

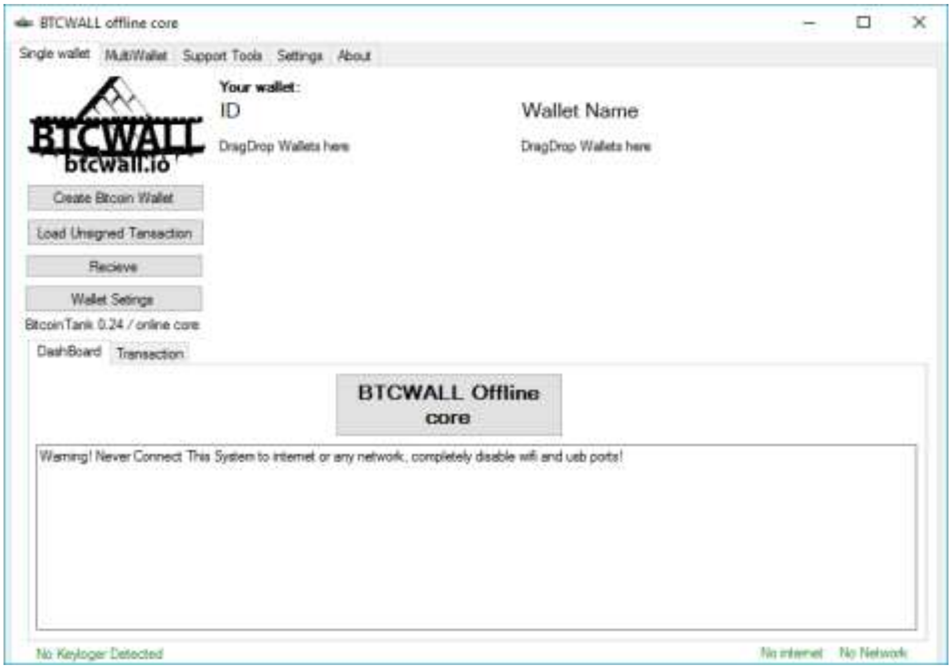
Wallets created in BTCWALL are shown below:



You can put each wallet in a separate file or record an unlimited number of addresses and wallets into any file of your choice. For example, you can generate immediately and write 10 000 wallets in one file, while the file remains working and private keys are hidden and encrypted. Even if the attackers or the police guess which files store wallets, they still will not be able to recognize the type of data encrypted in them. Encryption is carried out both for the data itself and the wallets inside them using the most reliable cryptographic algorithms.



The offline part of the wallet can create simultaneously an unlimited number of wallets and addresses and save them both in separate files or in one file. The online part also supports multiple numbers of wallets and addresses.



Your wallet:

ID

DragDrop Wallets here

Wallet Name

DragDrop Wallets here

BitcoinTank 0.24 / online core

Warning! Never Connect This System to internet or any network, completely disable wifi and usb ports!

No Keyloger Detected

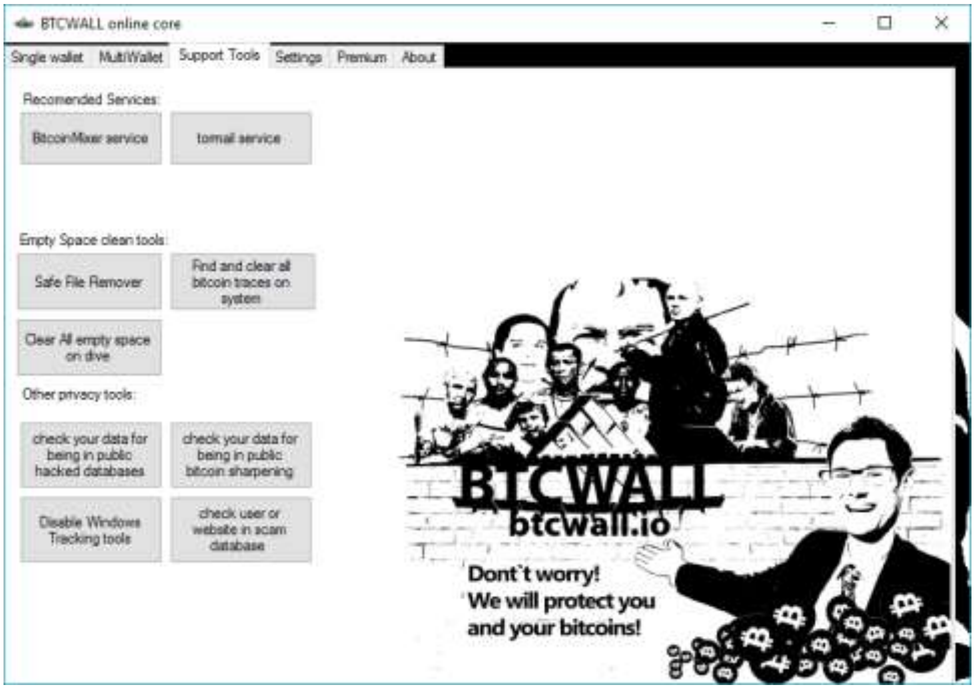
No internet No Network

2. The online part of the wallet is used to create transactions and check the balance of wallets. To send transactions, the computer must be connected to the Internet. Private keys are not stored and are not created in this program and the computer. This part is used to check the wallets balance and send bitcoins. This part uses the protection that other wallets do not have. Despite the fact that private keys are not stored, money can still be stolen by changing the wallet address to a similar one where funds will be sent to, so the program has a multi-level protection against such attacks. The wallet constantly checks and tests the clipboard and then detects malware that try to spoof the address and reports it. In addition, the wallet has a built-in antivirus that detects basic attacks.

For anonymity, the wallet uses a built-in TOR, which runs in a separate thread for each transaction and when changing wallets, has built-in connection checking and wallet network access without a secure connection. The online part of the wallet also supports stenography. The wallets storing the private keys in the online part are not supported and a warning is displayed that you can not store private keys on a computer connected to the network.

Online and offline parts support the built-in file killer intended for clearing both all free disk space and individual files. If you have ever stored private keys on a computer that is currently connected to the network or will be connected in the future, your money will be stolen. The deleted data can be recovered and in order to completely delete the file from the disk it is necessary to overwrite it more than 35 times. However, even this can not help, because the data is stored in RAM, which does not disappear after a reboot, since operating systems write and store the contents of RAM in paging files. The wallet has built-in simple tools that can delete all the files and clean up everything where you can store data about the use of crypto currency. After the signed transaction is sent, it can be safely removed from the computer by the wallet. To use the wallet it is very desirable to download the full base of the blockchain, but if there is no such option, the wallet supports the electrum's servers.

The online and offline parts of the wallet work in a portable mode and do not require installation, which allows you to quickly install, transfer and delete them without traces of using. At startup, wallets are not downloaded automatically in order not to display their location, the generated wallets are not stored in one place by default, all wallets with private keys are masked as common files or inside any specified file.



Additional useful features that the wallet will have:

Transfer of transactions for signing between offline and online modules

In order to make a transaction, you need to create it in the online version of the wallet and transfer it to the offline core in order to sign it with a private key. We develop a reliable, secure and convenient way to transfer transactions to the offline wallet core for signing and transferring back to make payments. We did not solve the problem completely, and we have to use USB or other storage device for transmission, which is not entirely safe. In the case of ICO success, we will certainly solve this and other problems.

Additional protection for BTCWALL wallet

In addition to passive protection of stored bitcoins and concealment of traces of using crypto currency on the computer, the wallet will have active protection by several methods.

Since by default the hidden wallets created with stenography by the BTCWALL wallet can be opened and decrypted only with BTCWALL, it becomes possible to implement additional protection.

When you open a wallet in the offline or online BTCWALL core, you can put an additional password and install additional protection. If an incorrect or specially set password is entered, a fake wallet with a fake balance optionally opens..

If the attackers tho found out that you have bitcoins and you were kidnapped or you became a victim of extortion at home, the wallet has additional protection: by entering a definite password, all transactions transmitted in this session will become fake (Double Spending Transactions), which can deceive kidnappers and save your life. Also, we are developing the protecting feature that, in case of danger, will transfer all the bitcoins to a special protected wallet, which criminals will not be able to access.

ICO structure and revenues

Developers of the BTCWALL wallet collect funds for the launch of the BTCWALL wallet, the development of appropriate technologies and the launch of services complementing the product. For this purpose, investment BTCWALL Tokens (BTCW), which are smart contracts based on Ethereum (see Appendix 1), are issued by BTCWALL developers. Developers of BTCWALL will ensure the storage and disposition of collected funds as required.

The token name: BTCW token is a share BTCWALL smart contract. BTCWALL token grants substantial interest in the sale of the commercial version of the BTCWALL wallet. All issued tokens in total figure the share of 40% profit.

Tokens will be distributed in proportion to the amount contributed by investors during the ICO.

Manner of payment: According to the Articles of association, at the end of each financial year, 40% of the distributed profits of BTCWALL or BTCWALL developers are transferred to a specialized Ethereum (ETH) wallet, after which ETH is distributed to the holders of BTCWALL tokens in accordance with the terms of the smart contract (i.e., in accordance with the tokens share of their total number).

The tokens number: 80,000,000 (eighty million) tokens, the destruction of the unsold balance will be carried out upon completion.

Start-up currency rate:
The cost of one token is set at 1 US dollar per token.

The tokens distribution:

- Among users: 90%;
-

- Among founders: 7%;
- «Bounty»-campaign: 3%.

Bonuses

Pre-ICO: +70% of bonus tokens

- 1st day: +50% of bonus tokens;
- 2-7 days: +40% of bonus tokens;
- 2nd week: +25% of bonus tokens;
- 3d week: +20% of bonus tokens;
- 4th week: +10% of bonus tokens;
- 5th week: +0% of bonus tokens.

«Bounty»-campaign:

- «Facebook»-campaign: 10% of cumulative remuneration;
- «Twitter»-campaign: 10% of cumulative remuneration;
- Bitcointalk-signatures campaign: 15% of cumulative remuneration;
- BTCWALL support in network discussions – 10% of cumulative remuneration;
- Translations into other languages on Bitcointalk: 15% of cumulative remuneration;
- Special support: 40% of cumulative remuneration.

Remuneration for the "bounty"-campaign is carried out after the completion of the main placement, following the results of which all tokens sold are taken for 90% of their total number. The remaining 7% is then distributed among the founders and as rewards as described above.

Projected revenue.

The number of BTCWALL users is planned at 40% -70% from 12 million of all bitcoin owners and the figure will grow.

The revenue distributed between the owners of the tokens is planned to be received from the sale of the advertisement of the checked services in our protected wallet. This is the first solution for protection of bitcoins and their owners using unique technologies, the cost of one license can reach up to $ 500 for commercial use, it will be purchased by people who need maximum security and easy to protect their savings, it is very little money for them. The planned income for the next 2 years is planned at $ 500 000 000 from the sale of licenses. And at least 20 000 000 $ from advertising or referral programs from services, exchangers, exchanges, ICO displayed in our wallet.

When we reach the necessary fees, we will open our own anonymous exchange of crypto-currencies working on smart contracts of our own tokens. In case of its opening, we pledge to redeem all BTCW tokens for at least $ 2.0 or exchange them for tokens to be used in the exchange.

Income from patents: in case someone decides to compete with us they will have to pay fees for using our protection technologies for which we will issue patents. In this case, the account can go for tens of millions of dollars, but incomes are difficult to forecast in this area, since competitors may not appear and some of the patents may be rejected.

In case of the required amount (see the roadmap) on the ICO, we will open a Private Security Enterprise with leading experts in this field to protect the owners of crypto currency. The company will also supply and install security systems and vehicles. Expected additional income will be $ 200 000 000 per year.

Revenues from own exchange: when we collect the necessary amount (see the roadmap) we will create our own automated anonymous exchange for bitcoins based on the blockchain and smart contracts that will use our BTCWALL tokens for work. The commission charged for each transaction will be up to 0.05%, with a daily turnover of $ 50 000 000 the income will be $ 2 500 000 per day or $ 900 000 000 per year, but with rising popularity of using crypto currency this amount will increase tenfold.

Floatation:

At the first opportunity, we will take public all our tokens on the exchange, their rate should grow with our profit, as all of their owners will be charged interest of all our profits from the BTCWALL wallet and all services associated with it, including our own Exchange which we are going to open if the project succeeds.

Thus, the profitability from the purchase of our BTCW tokens can range from hundreds to thousands of percent per year.

Additional features of BTCWALL tokens:

Tokens will be used to pay for a commercial version of the wallet, as well as premium subscriptions. Our security company will also use BTCW tokens as its domestic currency.

Our BTCWALL wallet will support in the future, in addition to other crypto currencies and bitcoin, also BTCWALL tokens.

Expenses

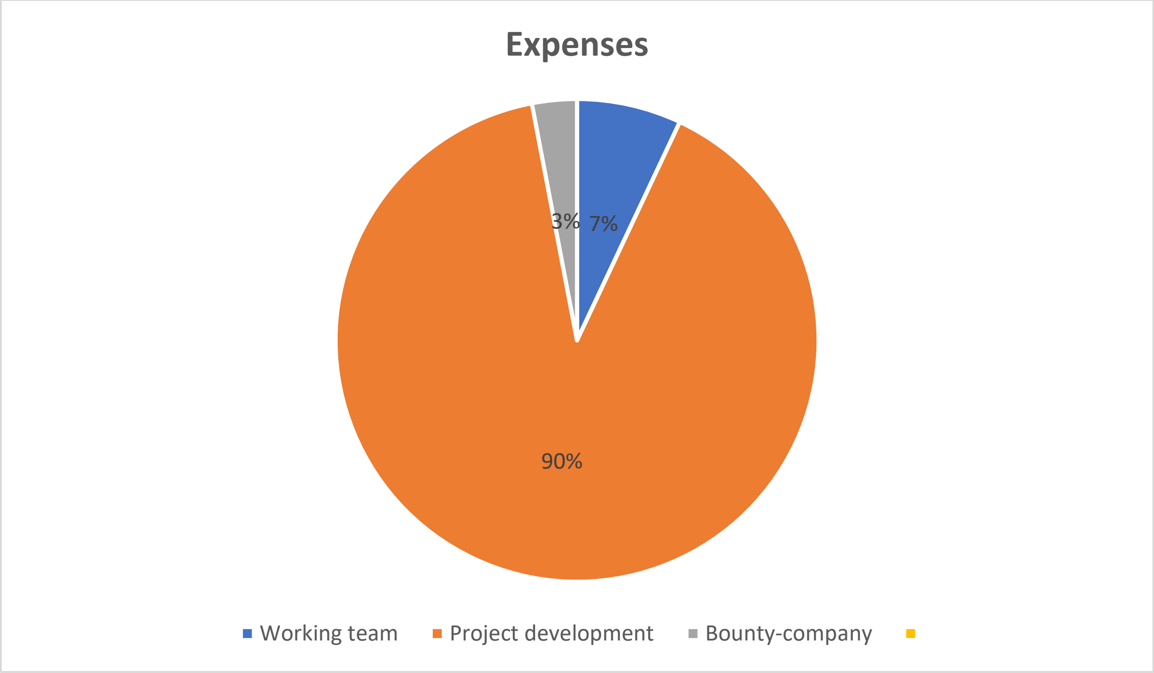
All money, collected during the campaign, will be spent as follows:

7% Will go to our team for the work done and the subsequent work.

3% Bounty-company.

All other funds will go to the project development.

Despite the fact that we already have the working code of the program with almost all the declared functions, we need to completely rewrite it and conduct beta testing, since at the moment part of the code is made up of open source codes. We plan to make the most reliable and secure from threats, which will appear just tomorrow. This will allow us to sell a commercial version of the wallet to companies, as well as advertising useful services in it.



BTCWALL roadmap

The creation of BTCWALL includes many different aspects, including development, testing, technology, patenting algorithms in all possible countries.

Below you can get acquainted with the step-by-step plan, which covers the main levels of our activity based on ICO results. Each level of the ICO is conceived as the basis for the next one, and will be implemented taking into account the response of users to new functions and the amount of collected funds for the ICO.

The main, although not the only, articles for spending funds received at the ICO will be the development of code, the development of systems, a thorough security audit, the purchase of equipment, office openings, recruitment and marketing.

The launch of pre-sale BTCW tokens is scheduled for September 2017

The launch of the ICO is scheduled for September 30, 2017

Depending on the funds collected, we start to work and add the appropriate functions and services.

Roadmap:

Fees 2 000 000 $, all work is planned to be done until 2017.12

- We issue a BTCWALL wallet with all declared basic functions.
- Attracting people to the problem of crypto currency user safety for raising the rate of the BTCW token and increasing the BTCWALL wallet users number
- Submission of patents in all relevant countries for the purpose of monopolizing the market of security software that protects the user.
- We create a commercial version of BTCWALL for companies and commercial use. (Free of charge for common users)
- Also, advertising of reliable mixers of exchangers and exchanges is added into the wallet to increase the income of BTCW owners

The expected income in this case will be $ 270 000 000 per year from the sale of the license ($ 250 000 000) and from advertising in the free version wallet ($ 20,000,000). The total expected return is 13 500% for one year, 40% of the funds will be added to the owners of BTCWALL tokens.

Fees 5 000 000 $, all work is planned to be done until 2018.05

- Adding premium subscription for wealthy customers and personal protection.
- Creation of a response center for crimes against BTCWALL premium service owners.
- Adding support for other currencies according to users reviews
- Adding many new features according to users reviews.
- Floatation of the token onto all possible crypto-currency exchanges

- Adding support for the BTCW token in the wallet, for the transfer and payment of premium services.
- Adding a built-in anonymous mixer for crypto currency in the BTCWALL wallet

The additional expected return in this case will be $ 400 000 000, which is in summary $ 670 000 000 per year, which is 13 400% for the first year.

Fees 20 000 000, all works are planned to be done until 2018.10

- Creation of an anonymous distributed exchange for crypto currency using BTCW tokens.
- Adding the built-in support for the exchange into the BTCWALL wallet

The additional expected return in this case will be $ 900 000 000, which is $ 1 570 000 000 per year, which is 7 850%.

In case of shortage of money for a minimum of $ 2 000 000, the money will be spent on PR for the purpose of organizing the additional crowdfunding, so that investors can be assured of the fulfillment of our promises.

FAQ

Why would users install your wallet and pay for it?

For today there are no alternatives to our solution, our wallet is the first commercial wallet providing maximum protection. People who will look for the most secure wallet in 99% will choose us. For ordinary users, the wallet will be free. For commercial use it will be necessary to purchase a license. Wallet will support premium service for particularly well-off customers.

Is it possible to export private keys?

It is possible, if there is such a need, the wallet can generate 10 000 wallets and private keys in 1 minute, can also work and check the balance conveniently from many wallets at once, create and sign transactions.

How do you guarantee the reliability of your wallet and your promises?

In order to guarantee security, you need to invest in development and security auditing as much as writing code. That is why most of the funds we receive will be spent on testing the security of both leading experts and third parties for a reward in case of successful hacking.

In the case if tho my bitcoins are stolen from my wallet, do you bear responsibility for this??

We guarantee that the probability of loss of funds when using our wallet will be several times lower than using any other wallets and services. Every situation about loss of bitcoins will be carefully investigated by our specialists and an appropriate update will be made to protect the program. If the theft was due to our fault because of the vulnerabilities committed by our programmers and you have a premium subscription, then we pledge to return you all the funds. To prevent this from happening, we will constantly hold contests for hacking our code and pay hackers compensation from specially allocated funds for security testing.

Will you have a phone support line for customers?

Of course we will have a phone support line. For this purpose, a center for operational analysis and response to incoming signals and threats is created. In addition to the telephone line there will be an online chat with a specialist. This is provided for the case you want to turn in additional information or your computer has been stolen.

I have subjected to bitcoins theft twice in an online service and a wallet. Can you advise how to avoid it further?

For this purpose our project BTCWALL is created, the wallet is made so as to provide the safety and simplify the use as much as possible. The wallet itself gives you advice, and blocks incorrect actions such as Internet connection on the computer where private keys will be stored.

What if my computer is infected and swarming with viruses that are not detected by any antivirus?

Your computer can swarm with viruses and hackers, they can not do anything with your funds because private keys can be created and stored on systems completely disconnected from the network. Offline client constantly checks the connection to the Internet and blocks all network packets and displays a warning.

WEBSITE: http://www.btcwall.io

WHITE PAPER: http://btcwall.io/whitepaperENG.pdf, http://btcwall.io/whitepaperRUS.pdf.

TWITTER: https://twitter.com/btcwall

TELEGRAM: https://t.me/joinchat/E1xbSAtny4NewcUF1waTwg

SLACK:
https://join.slack.com/t/btcwall/shared_invite/MjI5NzY4MTMyNTI4LTE1MDM0NzE3NDUtODMzYzVmZDhlZg

YOUTUBE: https://www.youtube.com/channel/UCybHHD6mPD_lt-JLP66YvOw