

Tracking One Year of Malicious Tor Exit Relay Activities (Part II)

 nusenu.medium.com/tracking-one-year-of-malicious-tor-exit-relay-activities-part-ii-85c80875c5df

nusenu

May 8, 2021



[nusenu](#)

May 8, 2021

.

19 min read

>25% of the Tor network's exit capacity has been attacking Tor users

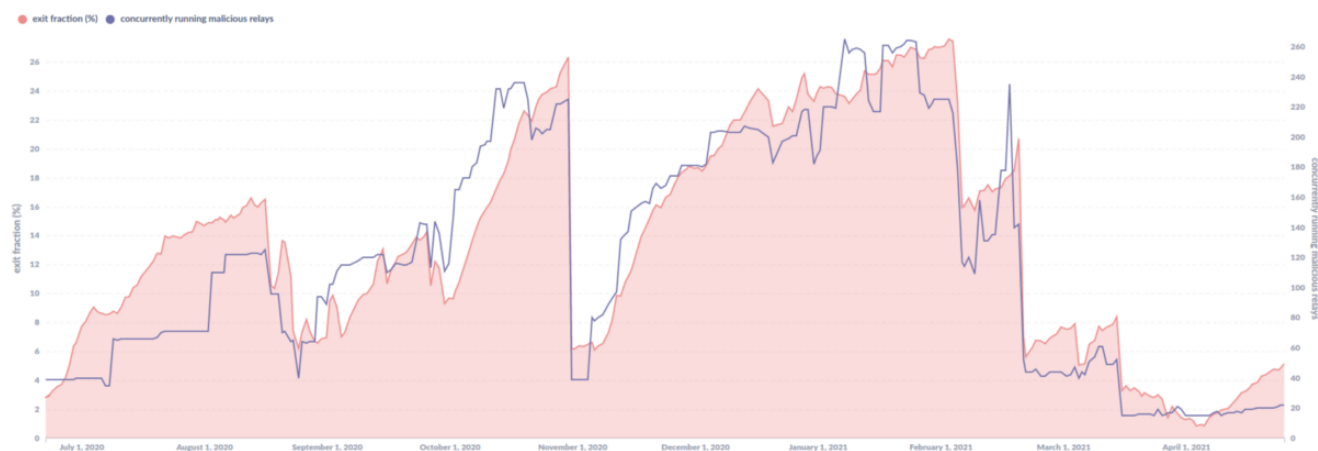


Figure 1: Malicious Tor exit fraction (measured in % of the entire available Tor network exit capacity) over time by this particular malicious entity between July 2020 and April 2021. Peak value: The attacker did manage approx. 27.5% of the Tor networks exit capacity on 2021-02-02. Graph by (raw data source:)

In August 2020 I reported about "[How Malicious Tor Relays are Exploiting Users in 2020 \(Part I\)](#)". Back then I made the hypothesis that the entity behind these malicious tor relays is not going to stop its activities anytime soon. Unfortunately this turned out to be true. In this follow-up post, I will give you an update, share what additional information we learned about the attacker since August 2020 and to what extend they were and still are active on the tor network.

After publishing the previous blog post it took only a few days until two sets of relay groups that were on my radar at the time (Figure 8 in [Part I](#)) got confirmed performing the same kind of attacks against Tor users as previously observed:



Figure 2: 2020-08-16: ContactInfo “exitrelays@protonmail.com” tor relays get caught doing MITM attacks. They got removed from the tor network on 2020-08-17. Source:

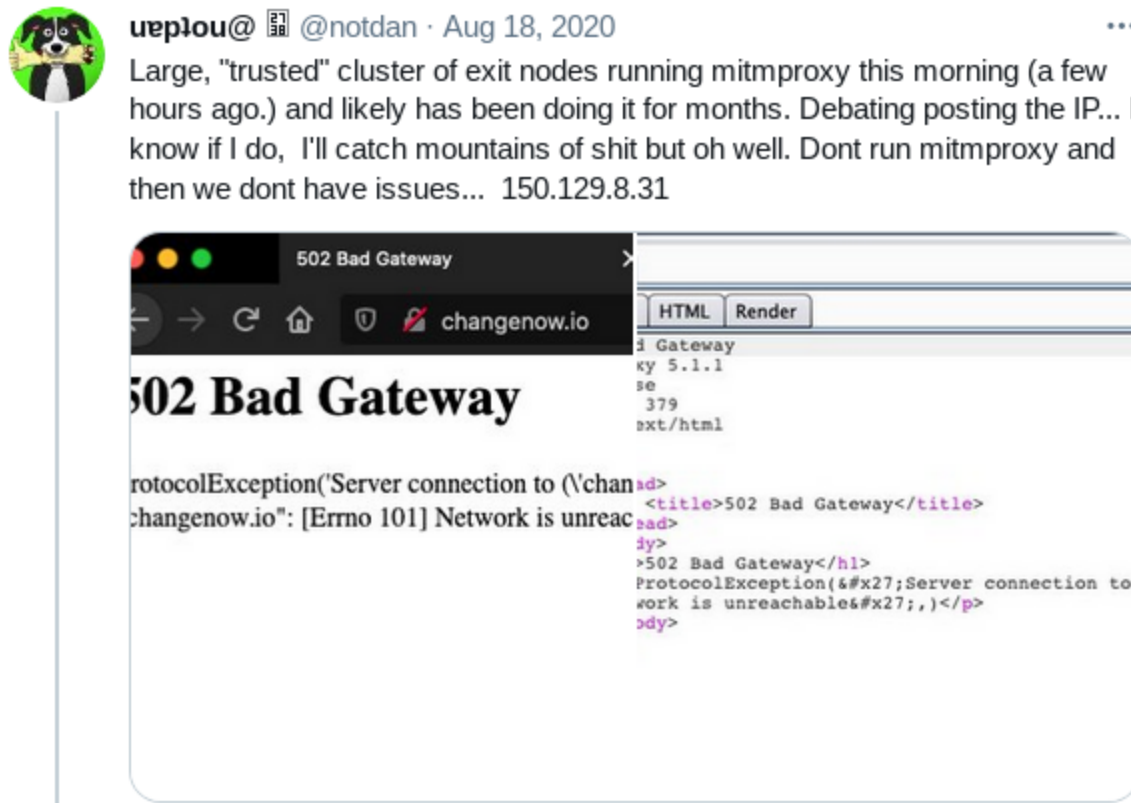


Figure 3: 2020-08-18: ContactInfo “kleinendorstwiebe AT gmail DOT com” tor relays are confirmed as malicious. They got removed on 2020-08-19. Source:

New negative records

The graph in Figure 1 starts where the first graph in the [previous blog post](#) ends and shows the fraction of known malicious exit capacity linked to this specific actor between July 2020 and April 2021. You can see the repeating pattern of new malicious relays getting added to the tor network and gaining significant traction before dropping sharply, when they got removed.

In terms of scale of the attacker's exit fraction, they managed to break their own record from May 2020 (>23% malicious exit fraction) twice:

- on 2020-10-30 the malicious entity operated more than 26% of the tor network's exit relay capacity
- and on 2021-02-02 they managed more than 27% of tor's exit relay capacity. This is the largest malicious tor exit fraction I've ever observed by a single actor.

Since there likely are additional malicious exit relays by this actor — which I did not manage to uncover I expect their actual fraction to be slightly higher (+1-3%) than the fractions stated above.

The attacker managed such a large fraction, that the total fraction managed by somewhat known tor relay community members — that made up about 73% before this attacker started its operations over a year ago — dropped to below 50% at the end of 2020 before it started to recover again after 2021-02-05.

Figure 4 shows the malicious exit fraction split by relay [ContactInfo](#). The attack strategy to hide large amounts of malicious tor exit relays by faking multiple distinct ContactInfos continued (as previously reported).

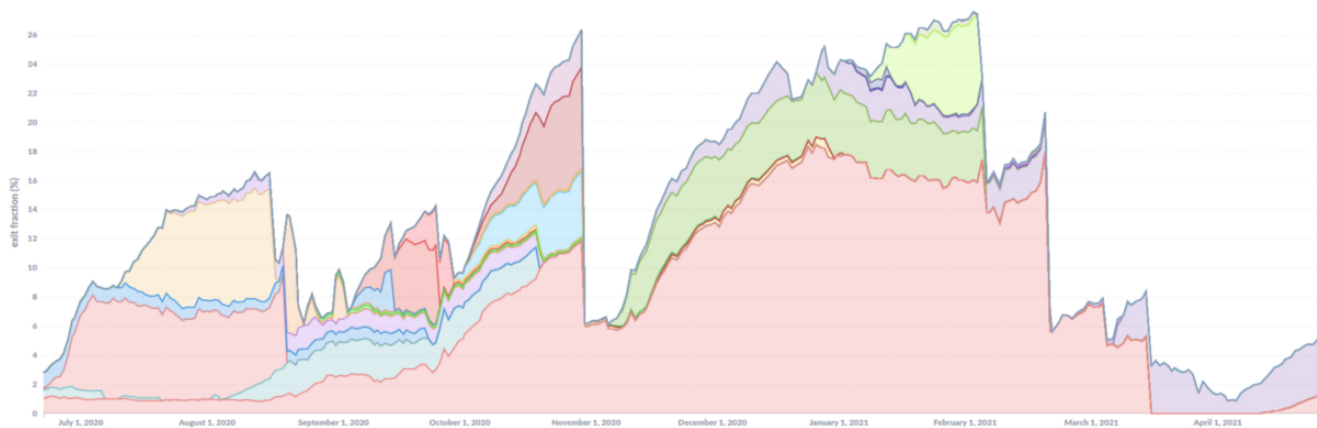


Figure 4: Confirmed malicious Tor exit capacity (measured in % of the entire available Tor exit capacity) between 2020-06-21 and 2020-11-01 by ContactInfo (stacked). Only actual malicious relays are included (for example not all relays using ContactInfo CypherpunkLabs were malicious. Graph by (raw data source:)

New malicious trends

But also new attack trends and have been observed:

This actor is increasingly adding malicious tor relays without any ContactInfo (this is the largest fraction, shown in red in Figure 4). Once a malicious tor exit relay is detected, all other relays using the same ContactInfo are easily found and removed, this is not an issue for them if they do not have a ContactInfo at all. Figure 5 shows the overall tor exit fraction that had no ContactInfo set (blue) and what part of it was malicious (red). We can obviously not rule out that even more of them are malicious and we failed to detect them. The vast majority of exit capacity without ContactInfo was malicious between October 2020 and March 2021.

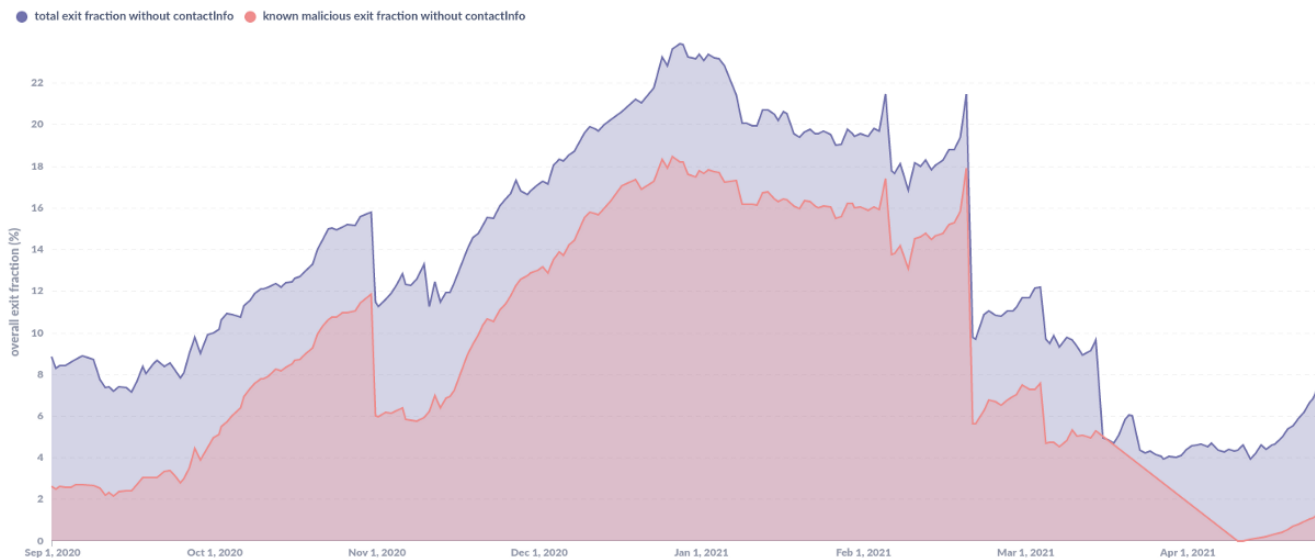


Figure 5: What fraction of exit relays not having any relay ContactInfo was malicious? (You can ignore the straight red line above “Apr 1, 2021”, that is just a interpolation) Graph by (raw data source:)

The “[Expectations for Relay Operators](#)” document (draft) says:

Be sure to set your ContactInfo to a working address [...]

Roger Dingledine (one of the founders of the Tor Project) also has a [clear opinion](#) on this topic:

Make clear that being a relay operator requires transparency about the relay operator, not secrecy

The tor client has no configuration option to say “do not use exits without ContactInfo”. I wrote a short [proof-of-concept python script](#) (not reviewed, not signed) that demonstrates such a feature by excluding exit relays without ContactInfo in the exit position via the “[ExcludeExitNodes](#)” option, but it is not meant to be used by the average user and we aim for more robust protections than a simple “has ContactInfo? y/n” test (it still can be one of multiple factors). To allow everyone to easily see what exit fraction is currently contributed by exit relays without ContactInfo I added a new [graph](#) to [OrNetStats](#) which gets updated on a daily basis.

This is not directly visible because the list of contacts was too large to include in Figure 4, but the malicious actor also started to impersonate other operators to hide malicious relays by using their ContactInfos. In one case they used ' ContactInfo. (Side note: To avoid false positives Figure 4 was generated by identifying malicious relays by fingerprint and not by searching for the ContactInfos used by CypherPunkLabs.)

Reaction time matters

In August and September 2020 malicious relays got reported and removed continuously (see the Appendix II for examples). In October 2020 the malicious exit fraction reached a new record (>26% malicious exit fraction). What was different in October 2020? Like the previously identified groups, also the groups appearing at the end of September and the beginning of October 2020 got detected by OrNetRadar (a relay group detector):

They got reported to the Tor Project on 2020-10-04, unfortunately there was no reaction and so these malicious relay groups gained significant exit fraction over time before they got probably discovered again and removed at the end of October 2020:

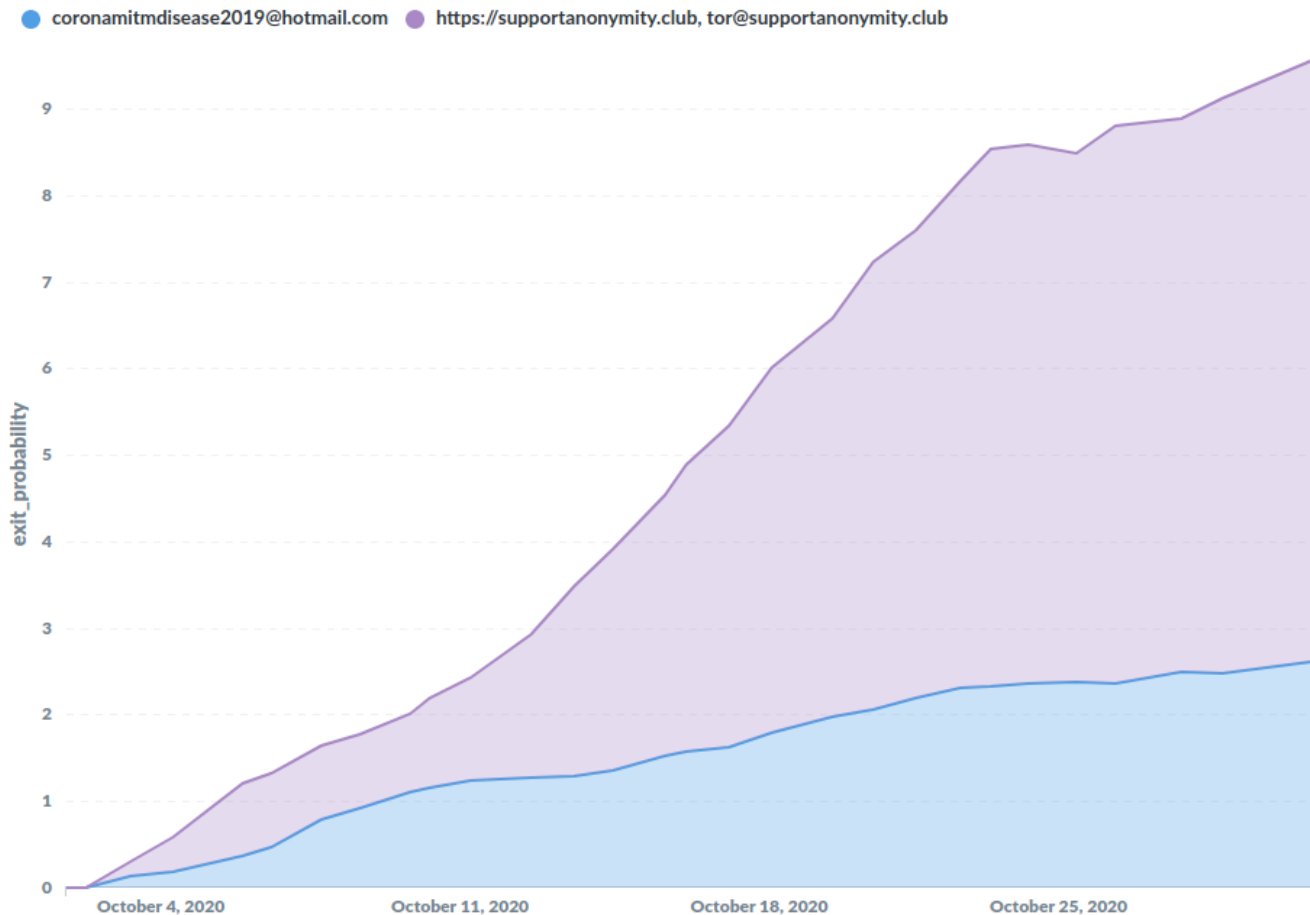


Figure 6: Malicious exits using ContactInfo “supportanonymity.club” and “coronamitmdisease2019@hotmail.com” got reported when their exit fraction was at 0.57%. Graph by (raw data source:)

Another example: The following graph shows the exit fraction of a set of malicious relays (identified by their relay fingerprint), that got reported in August 2020 and was found again on the tor network with over 1% exit fraction in April 2021.

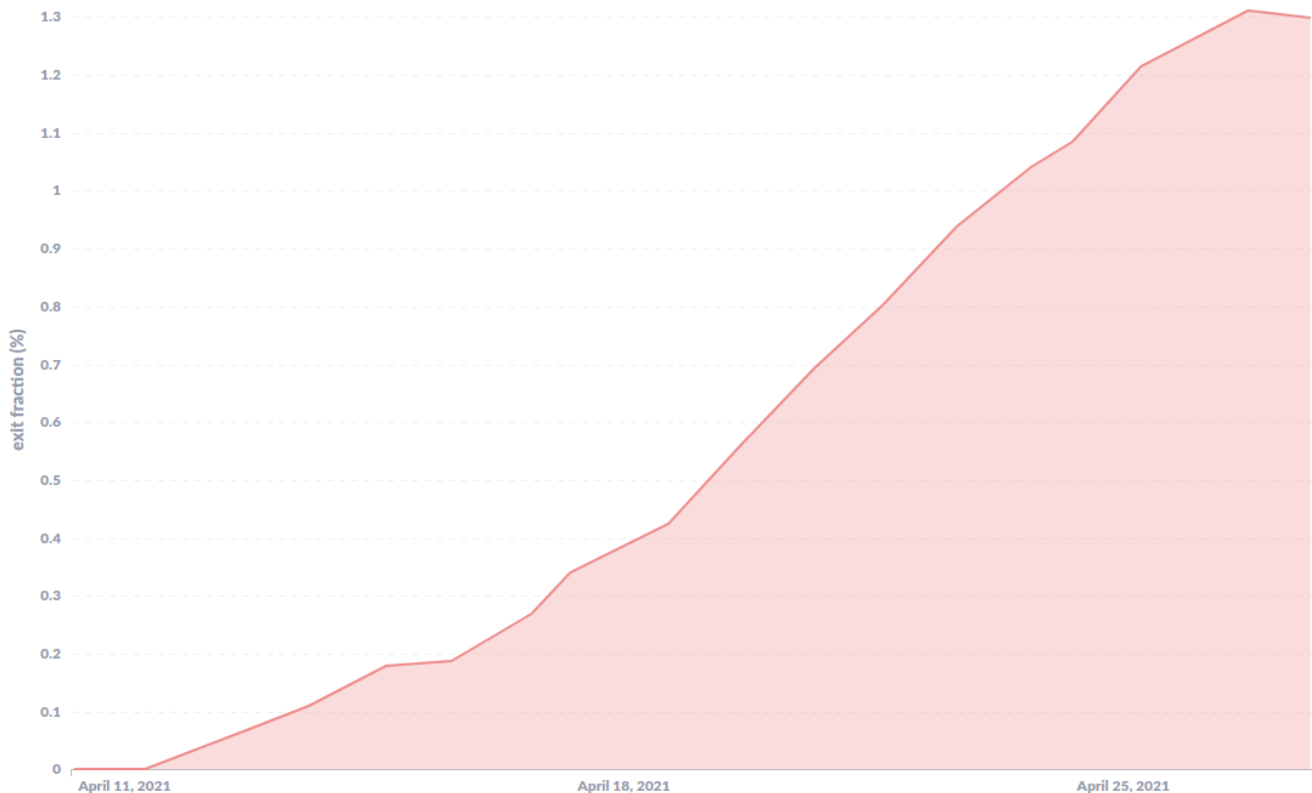


Figure 7: Malicious Tor exit relays reported on 2020-08-20 and found on the tor network again in April 2021 (removed on 2021-04-27). Graph by (raw data source:)

New adversarial tactics

In September, on 2020-09-03 “Андрей Гвоздев <andrejgvozdev55@gmail.com>” reported CypherpunkLabs relays, an undeclared relay group (but not necessarily run with malicious intends), to bad-relays at lists.torproject.org.

At the time I answered:

thanks for your email. We have them on our radar and they promised to improve things after our first contact but in fact they didn't. We will follow up on them.

<https://lists.torproject.org/pipermail/tor-relays/2020-August/018878.html>

Even though I contacted CypherpunkLabs multiple times the situation with their relay configuration had not improved at the time. Such MyFamily misconfigurations make impersonation attacks easier for attackers.

About three weeks later, on 2020-09-26, the malicious entity started to take advantage of CypherpunkLabs' relay misconfiguration. New malicious exit relays using CypherPunkLabs' ContactInfo appeared. Is this related to the email from 2020-09-03? A coincidence? At the time I did not realize what just happened, but the events that followed until the end of 2020 made it clear.

Unexpected Luck with WHOIS data

On 2020-10-31 Roger Dingledine sent an [email to the tor-relays mailing list](#) mentioning that tor directory authorities removed a long list of malicious exit relays for performing the known attacks (mitmproxy, sslstrip) against tor users. Side note: Since CypherPunkLabs did not properly declare their relay group it was not possible to tell their relays apart from the attacker's relays (they even used the same hosting company for the malicious relays). So all of them, those actually run by CypherpunkLabs and those run by the attacker, got removed altogether:



Source:

At the bottom of the [long list of malicious tor exit relays](#) published by Roger Dingledine, we can see the following set of malicious exit relay identifiers (fingerprints):

Group #7:

other4E6C7297F16523A236EE1A2EE23AF54ABEF1549055D490E9E440DD4458F16ABCDD79F48396D55EA97

Unlike most of the other relays they were **not** located at one of the usual hosters (OVH, Leasweb, Frantech). These relays did run on the following IP addresses: 185.32.222.167–185.32.222.170 (if you would like to verify that: [archive](#)) located in Switzerland at the internet service provider Datasource AG ([AS51395](#)). Let's have a look at what WHOIS information is available for these IP addresses:

Responsible organisation: [Datasource AG](#)
 Abuse contact info: andrejgvozdev55@gmail.com

```

inetnum:      185.32.222.166 - 185.32.222.173
netname:      TorExitServer
country:      CH
admin-c:      AG25099-RIPE
abuse-c:      AG25099-RIPE
tech-c:       AG25099-RIPE
status:       ASSIGNED PA
mnt-by:       MNT-DA327-RIPE
mnt-by:       MNT-DA327
created:      2020-09-15T06:51:50Z
last-modified: 2020-09-15T07:02:48Z
source:       RIPE
  
```

Login to update  [RIPEstat](#) 

Figure 8: WHOIS records contain the email address “” as abuse contact for the small IP block used by malicious exit relays. Source: RIPE Database ()

Due to the size (just a few IP addresses) and it’s status (“ASSIGNED PA”) the assignment, this is likely an end user assignment (instead of the hoster’s contact info). Of particular interest is the abuse-contact, since it shows the email address that contacted the bad-relays team on 2020–09–03 and reported the CypherpunkLabs relays which then became a impersonation attack victims after they got reported.

The RIPE database can also be used to find other IP blocks that use the same abuse-contact (inverse lookup). Using that search method we found one additional IP block also hosting tor exit relays but unlike the other exit relays these relays were not removed at the time (October 2020):

Responsible organisation: [Datasource AG](#)
 Abuse contact info: andrejgvozdev55@gmail.com

```

inetnum:      91.192.103.4 - 91.192.103.111
netname:      TorExit
country:      CH
abuse-c:      AG25099-RIPE
admin-c:      AG25099-RIPE
tech-c:       AG25099-RIPE
status:       ASSIGNED PA
mnt-by:       MNT-DA327-RIPE
mnt-by:       MNT-DA327
created:      2020-11-04T08:21:58Z
last-modified: 2020-11-04T08:21:58Z
source:       RIPE
  
```


Login to update  [RIPEstat](#) 

Figure 9: Inverse RIPE DB lookup for abuse handle finds an additional IP block also containing malicious exit relays. Source: RIPE database (2021–01–04).

On 2020–12–31 a new tor exit relay using a confirmed malicious ContactInfo (“fbirelays@protonmail.com” — see [Part I](#)) joined the tor network. The IP address of that relay (91.192.103.35) happened to be located in this IP address block. That means that we have multiple independent paths that link the email address andrejgvozdev55@gmail.com to the attacker:

- tested the bad-relays team by reporting the CypherPunkLabs relays to see if they get removed for improper MyFamily configuration. This information is crucial for them because an attacker can not establish a mutual MyFamily configuration with the victim they impersonate. A few weeks later malicious relays appeared using the CypherPunkLabs ContactInfo (CypherPunkLabs was not the only relay group they reported..).
- shows up as abuse-contact in WHOIS for two small IP blocks that contain malicious tor exit relays.
- One of these exit relays in these IP blocks used a confirmed malicious ContactInfo previously identified (“”).

It is unclear why they would reuse confirmed malicious ContactInfos and link their new exit relays to known malicious activities, since one would expect that known malicious ContactInfos are on an alert and removal list, but since they removed the known malicious ContactInfo from the relay configuration on 2021-01-16 while keeping the relay running, my guess is that they reused tor configuration files and unintentionally used a confirmed malicious ContactInfo. Such presumably unintentional disclosure happened multiple times.

The RIPE database abuse-contact records for these IP blocks leads to an address in Moscow, Russia:

```

role:          Andrey Gvozdev
address:       Zvenigorodskoe shosse, d13, kv12
address:       123022 Moscow
e-mail:        andrejgvozdev55@gmail.com
abuse-mailbox: andrejgvozdev55@gmail.com
nic-hdl:       AG25099-RIPE
mnt-by:        MNT-DA327-RIPE
mnt-by:        MNT-DA327
created:       2020-09-15T06:54:36Z
last-modified: 2020-11-04T14:24:01Z
source:        RIPE

```

RIPE Database Software Version 1.99

The abuse-contact information for the IP addresses used by malicious tor exit relays.
Source: RIPE database ()

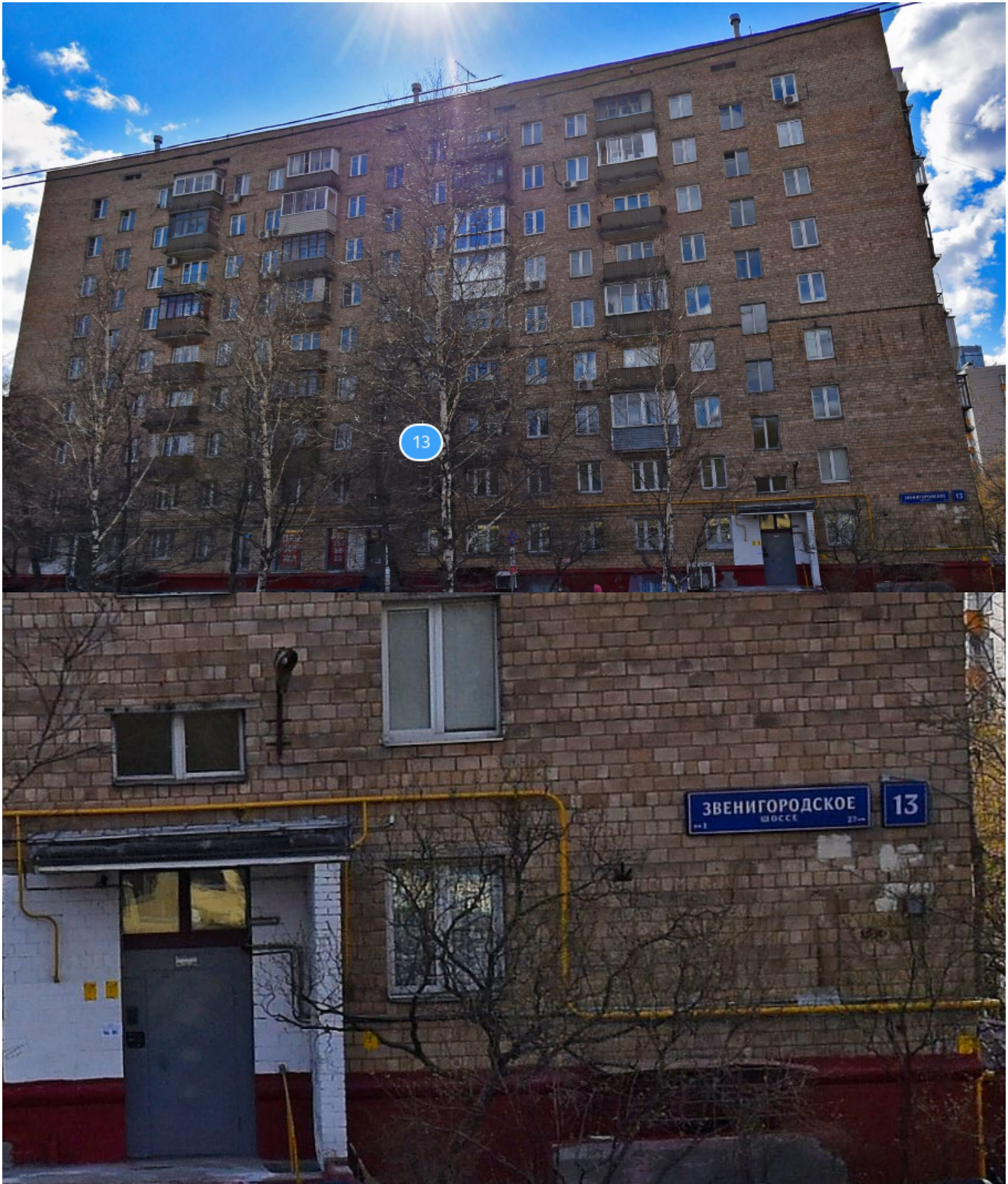
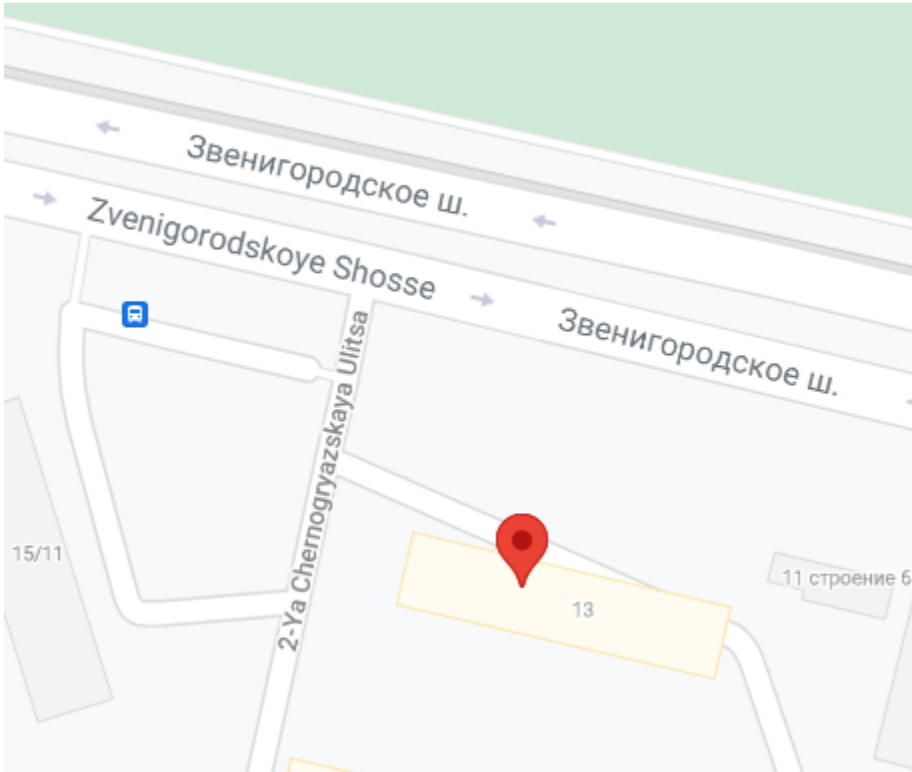


Figure 10/11: The abuse-contact address of the IP range hosting malicious tor exit relays (185.32.222.166–185.32.222.173) is allegedly located at this building in Moscow according to RIPE database records. Image Source: yandex.com



Apartment **Apartments Zvenigorodskoe Shosse**

13-023 👍👍👍

📍 Звенигородское шоссе 13, Presnensky, 123022 Moscow, Russia –

[Excellent location - show map](#)



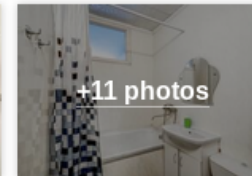
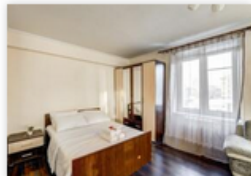
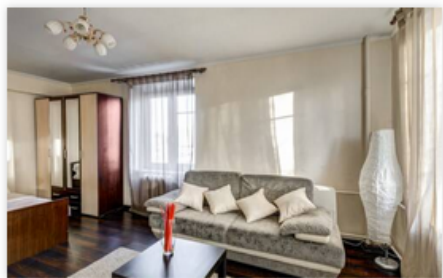
Reserve your apartment stay

We Price Match



Exceptional 9.6
3 reviews

Excellent location! 10



+11 photos

Figure 12/13: The alleged abuse-contact address used by the malicious exit relay operator can also be found on booking.com. According to the building has 108 apartments and 9 floors. That makes 12 apartments per floor, so apart. 12 (“kv12”) could theoretically be on the

ground floor. Image Source: Google Maps / (,) (Zvenigorodsko(y)e shosse 13 / Звенигородское шоссе 13)

An email address in the RIPE database is not necessarily there with the consent of the actual email address owner even though addresses are validated to some extent by the RIPE NCC. There was still the possibility that the actual attacker fraudulently provided the address “andrejgvozdev55@gmail.com” as abuse-contact without actually having access to it (impersonation), but we can rule that out since the hosting company confirmed that the RIPE database records are correct and the email address is verified. There is also a second reason why using someone else’s email address as abuse-contact for a tor exit IP block will not remain unnoticed for very long: That email address will get actual abuse emails delivered to it. So we are confident that the owner of the email address andrejgvozdev55@gmail.com is actually running these malicious exit relays. After confronting them they did not respond (not too surprising).

To what extent the physical address is authentic is unknown at this point. It would obviously not make much sense for an attacker to use their actual address when ordering servers, but at the same time they used a single email address when ordering servers for malicious relays and reporting non-malicious relays to the Tor Project. And it is not clear whether they knew that their email address and (alleged) physical address ends up in public RIPE database records.

WHOIS information is rarely ever useful for malicious tor relay investigations, but in this particular case we were lucky and found useful information and were even able to find more malicious exit relays using RIPE database inverse-lookups.

>1 000 new exit relays in early May 2021

The tor network usually consists of less than 1 500 tor exit relays. In early May 2021 over 1 000 new unnamed tor exit relays without ContactInfo joined the tor network within less than 24 hours (1, 2, 3, 4). Although that sounds like an impressive number of exit relays, such massive relay groups impose little risk for tor users because they basically get removed right away before gaining any meaningful traction. When I noticed them I thought they are trolling because no one can assume such a large Sybil stays on the network for long, until I got email from them. Someone responded off-list to a short note I wrote to the tor-relays mailing list about this event. Apparently they were not amused by the removal of these exit relays (I do not claim any credit for their removal). It is likely that this is the same entity previously observed, because their limited vocabulary is consistent with earlier emails I got from “andrejgvozdev55@gmail.com”.

Countermeasures

My previous blog posts about malicious tor relay activities ([1](#), [2](#)) featured a section about proposals the Tor Project could implement to reduce the risks for Tor Browser users. That did not turn out to be fruitful. So after several attempts to convince them to improve the situation I'm going to take an another approach: Digital self-defense for tor users. This is a work in progress and my plan is to write about it in more detail in a future blog post but this section might provides some overview.

In addition to tor user protections I also tackle tor relay operator impersonation attacks via a non-spoofable ContactInfo — which (exit) relay operators are encouraged to implement and many (exit) relay operators adopted it already. Being able to confirm if a relay is actually operated by the entity it is claimed to be operated in an automated manner is a corner stone for addressing operator impersonation attacks and malicious relays in general.

Why did it take me several years before even considering the self-defense approach?

- The scale of the detected attacks has never been as large as in 2021.
- Non-central options should only be considered after trying (and failing) to achieve protections at the tor directory authority level because they will never reach all users.
- Tor client configuration changes should generally be avoided to avoid splitting the anonymity set and only be used as an option of last resort (or as a method to vote with your feed as a tor user).
- Non-default tor client configurations make network wide load balancing harder.
- It requires more effort.

Nonetheless we are in a dilemma between knowingly using malicious tor exit relays vs. excluding them via the tor client configuration at the price of having a non-default configuration. This is additionally complicated by the fact that the exact nature of the attacks are not entirely known. We know about mitmproxy, sslstrip, bitcoin address rewrites and download modification attacks but it is not possible to rule out other types of attacks. Imagine an attacker runs 27% of the tor network's exit capacity and a firefox exploit affecting Tor Browser gets published before all users got their (auto)updates.

HTTPS-Only Browser Mode

The HTTPS-Only mode (which might land in Tor Browser based on Firefox 91 ESR) would be a strong protection, but there are still some uncertainties with that as well as a Tor Browser developer points out [on a tor mailing list](#):

When Tor Browser migrates to Firefox 91esr we will look at enabling https-only mode for everyone, but there remains a significant concern that there are many sites that do not support HTTPS (especially more region specific sites) and the question of what messaging Tor Browser should use in that case.

Solving the fake ContactInfo impersonation attacks

Problem: ContactInfo is an unverified arbitrarily spoofable string and malicious actors take advantage of that by using other peoples ContactInfos to hide their malicious relays — especially if their MyFamily configuration is not properly setup. This even goes as far as using names of (former) tor community people that do not even run exit relays.

Solution: Non-spoofable ContactInfos. The [ContactInfo Information Sharing Specification](#) (version 2) provides a [non-spoofable ContactInfo “url”](#) field that can be protected against impersonation attacks. The specification ties a relay to a domain and makes use of the [IANA](#) registered [“tor-relay” well-known URI](#) to place the list of relay fingerprints operated by an entity at a well defined location on the operator domain (or via DNS TXT records). An attacker claiming to be another trusted operator (for example [“emeraldionion.org”](#)) can be detected because the attacker can not place his relay fingerprints at the [defined location](#). This effectively protects the provided “url” field. Even operators that do not own a domain have used Github pages and similar services to protect their relay’s ContactInfo in this way. This non-spoofable ContactInfo field is also the foundation for graphs showing trusted/untrusted exit fraction over time.

Over 20% of the tor network’s exit capacity is already protecting their ContactInfo “url” field using this method. Please consider [using a non-spoofable ContactInfo](#) if you are a tor relay operator to help prevent these attacks. As a nice side effect you get an aggregated graph for your group of relays on OrNetStats ([example](#)). Generating the ContactInfo string has become rather easy with the availability of <https://torcontactinfogenerator.netlify.app/> contributed by [Eran Sandler](#) (only “url”, “proof” and “ciissversion” fields are needed for a non-spoofable ContactInfo).

Note: Also malicious operators can and will setup these fields, but the key point is, that they can not impersonate other relay operators.

Visualizing known and unknown exit fraction

Visualizations provide a good overview on what is going on on the tor network with regards to changes related to who controls what exit fraction for example. I use the following graph to get an idea on what is going on before proceeding with more specific investigations. It shows the aggregated exit probability from operators I classify as “somewhat known/non-malicious”.



Figure 14: Likely non-malicious exit fraction over time graph allows to draw indirect conclusions about (large scale) malicious activities. Graph by (raw data source:)
 The graph spans over more than one year and can indirectly show malicious relay activities (indicated by a significantly decreasing exit fraction) or outages at known operators. This can be seen without having to know anything about the attackers in specific but it requires constant manual investigations because it has a significant problem: It uses untrusted input data (ContactInfo) that malicious entities are taking advantage of by using other peoples ContactInfo.

This is where the non-spoofable ContactInfo “url” field comes in. With the increasing adoption of the non-spoofable ContactInfo field we can visualize what fraction of the network is “known” without depending on arbitrarily spoofable input data. Instead we simply use domain names from the non-spoofable ContactInfo url field and specify “I know emerald onion.org, hviv.nl, ...”. Figure 15 shows all current non-spoofable domains by exit operators. This is a snapshot of the daily updated [graph I’m adding to OrNetStats](#) with the release of this blog post. On OrNetStats you can interactively select whether a operator should be include or not by clicking on an operator domain. It is up to the user to decide which operator they consider trusted.

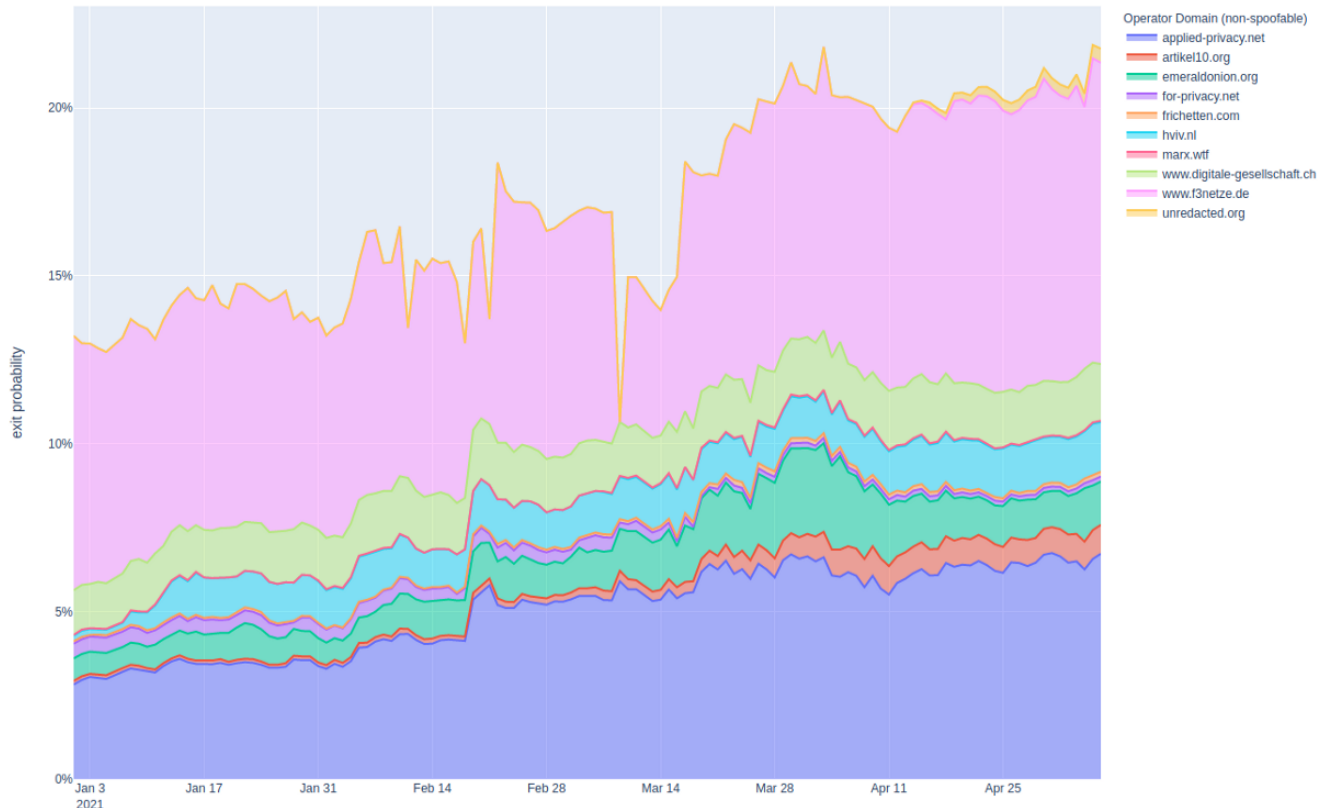


Figure 15: Contributed exit fraction by (non-spoofable) operator domain. Graph by This graph is similar to what Roger Dingledine wrote in [this Tor Project gitlab issue](#), but instead of tagging each relay individually we leave the task to (verifiable) link a relay to an operator to the operator running it and then do the tagging (known vs. unknown) on the operator level instead of at the relay level, this should scale well and does not require any actions if an operator adds a new relay to the network.

The aggregated exit fraction in Figure 14 is significantly larger than in Figure 15 where we use non-spoofable input data, but we have just started and more operators are about to adopt the non-spoofable ContactInfo to make this even more useful. I envision a future where a tor user can choose his preferred risk level between “I want to use known exits only” and “I’m fine with some higher risk, I want more diversity, allocate up to 20% of unknown tor exit relays”. Beware that this comes at the price of splitting the anonymity set. On the long run all Tor Browser traffic should be authenticated and encrypted which will make running malicious exit relays less profitable for malicious entities.

Summary

- The entity attacking tor users, originally disclosed in , is actively exploiting tor users since over a year and expanded the scale of their attacks to a new record level (>27% of the tor network’s exit capacity has been under their control on 2021–02–02).
- The average exit fraction this entity controlled was above 14% throughout the past 12 months (measured between 2020–04–24 and 2021–04–26).

- The malicious actor actively reported non-malicious but poorly configured relays to the Tor Project's bad-relays mailing list to find viable victims to use for operator impersonation attacks.
- Most of the malicious tor exit capacity did not have any relay ContactInfo. Throughout the last 6 months the majority of tor exit capacity without ContactInfo was malicious.
- The attacker primarily uses servers at the hoster OVH.
- In early May 2021 the attacker attempted to add over 1 000 exit relays to the tor network.
- The attacker (or one of them) likely uses the Russian language interface of gmail.com.
- As of 2021-05-08 I estimate their exit fraction between 4-6% of the tor network's exit capacity.
- A new field for tor relays has been specified and has been adopted by over 20% of the network's exit capacity so far.
- OrNetStats has been extended to include two new graphs: exit fraction and graphs showing

key take away for tor relay operators:

Want to help with tor network safety? on your tor relays.

Additional Background / Disclosure

After publishing [Part I in August 2020](#) I got email from the Tor Project in which they shared their concerns about me "leaking" information from the private bad-relays mailing list without their consent. While I agree that it is reasonable to expect some level of confidentiality after being invited to a non-public mailing list I questioned that my blog post did any damage to the goals of the bad-relays team. I have unsubscribed from the bad-relays mailing list as of 2021-01-01. It did not feel like being on that list allowed me to help reduce the risk for tor users and relevant discussions happen also elsewhere. Regardless of that I'll continue to work towards a safer tor network.

I have informed them about the upcoming publication of information related to "andrejgvozdev55@gmail.com" before this blog post went public:

fyi: I'll soon publish information about this email address and its links to malicious relay operations.

It will include information I learned through this list via my interactions with that gmail address (timestamps and content).

They had no objections.

Want to support this type of research?

I'm looking for a new maltego license (the previously donated license I got after publishing my previous blog post expired).

Appendix (bonus material)

Fake profiles for fake relays: relaystor.xyz

On 2021-02-13 and 2021-02-16 close to 100 relays joined the network. All of them had the domain <https://relaystor.xyz> in their ContactInfo field. They are not so relevant from an exit fraction point of view because they were not on the tor network for long but I still found them interesting because they made some effort to build some fake profiles:

- (rudimentary) website
- twitter profiles (created 2012 and 2014)
- telegram channel
- BTC donation address

Here is a screenshot of their "about" page:

We are two IT specialists who are passionate about Internet surveillance and censorship:

Albinus - has been working as a system administrator for 8 years. It was his idea to launch TOR relays, responsible for relay maintenance and security.

Arthur - senior C++ developer. Helps to maintain relays, responsible for financial expenses.

Feel free to contact us if you have an idea how to improve our relays or if you want to help us. Any help is appreciated.

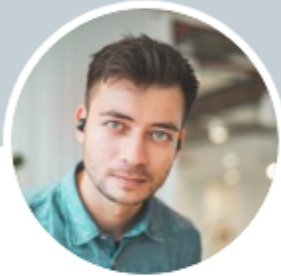
Follow us on twitter: [Albinus](#), [Arthur](#).

Our telegram channel: t.me/relaystorxyz

Go back

Source: (archived version:)

The twitter links point to these profiles:



Follow

Arthur Tyler
@temporaca86

C++ developer

📍 USA 🗓️ Born March 15, 1986 📅 Joined September 2012

87 Following 26 Followers

Tweets

Tweets & replies

Media

Likes



Arthur Tyler @temporaca86 · Feb 25

...

Hey, guys, check out our new project: relaystor.xyz. Thanks a lot to my friend Albinus for his help.



Source:



Albinus Marín Fernandez
@n64alys184

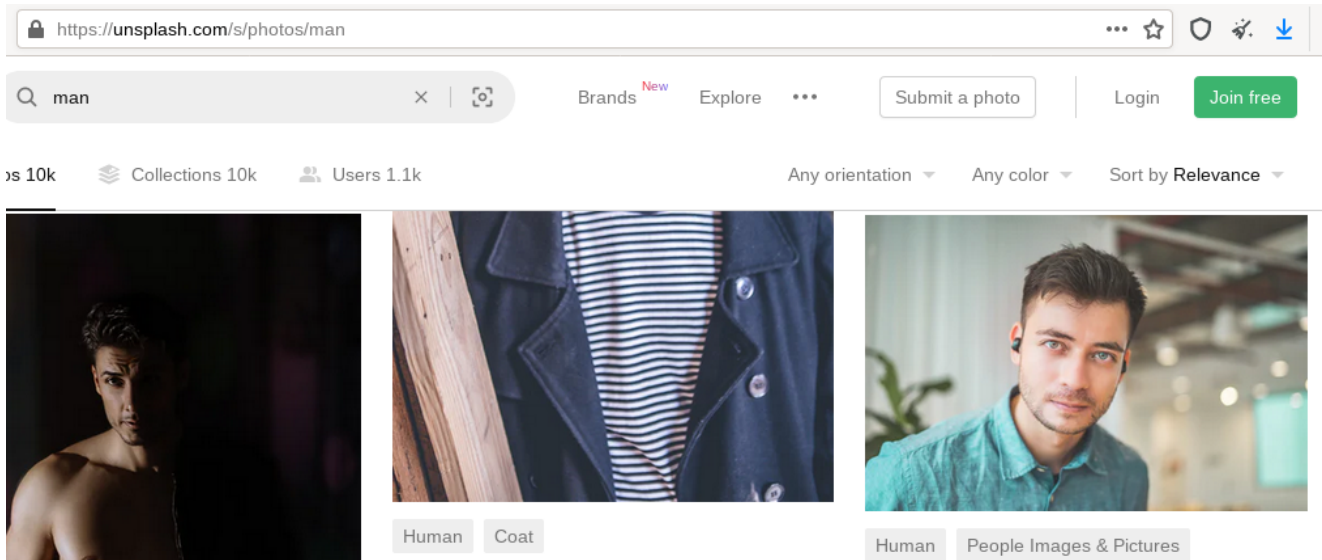
Spain Born May 17, 1983 Joined July 2014

439 Following 28 Followers

Follow

Source:

The profile pictures can be found on a stock image website (unsplash) using image reverse search:



https://unsplash.com/s/photos/man

man

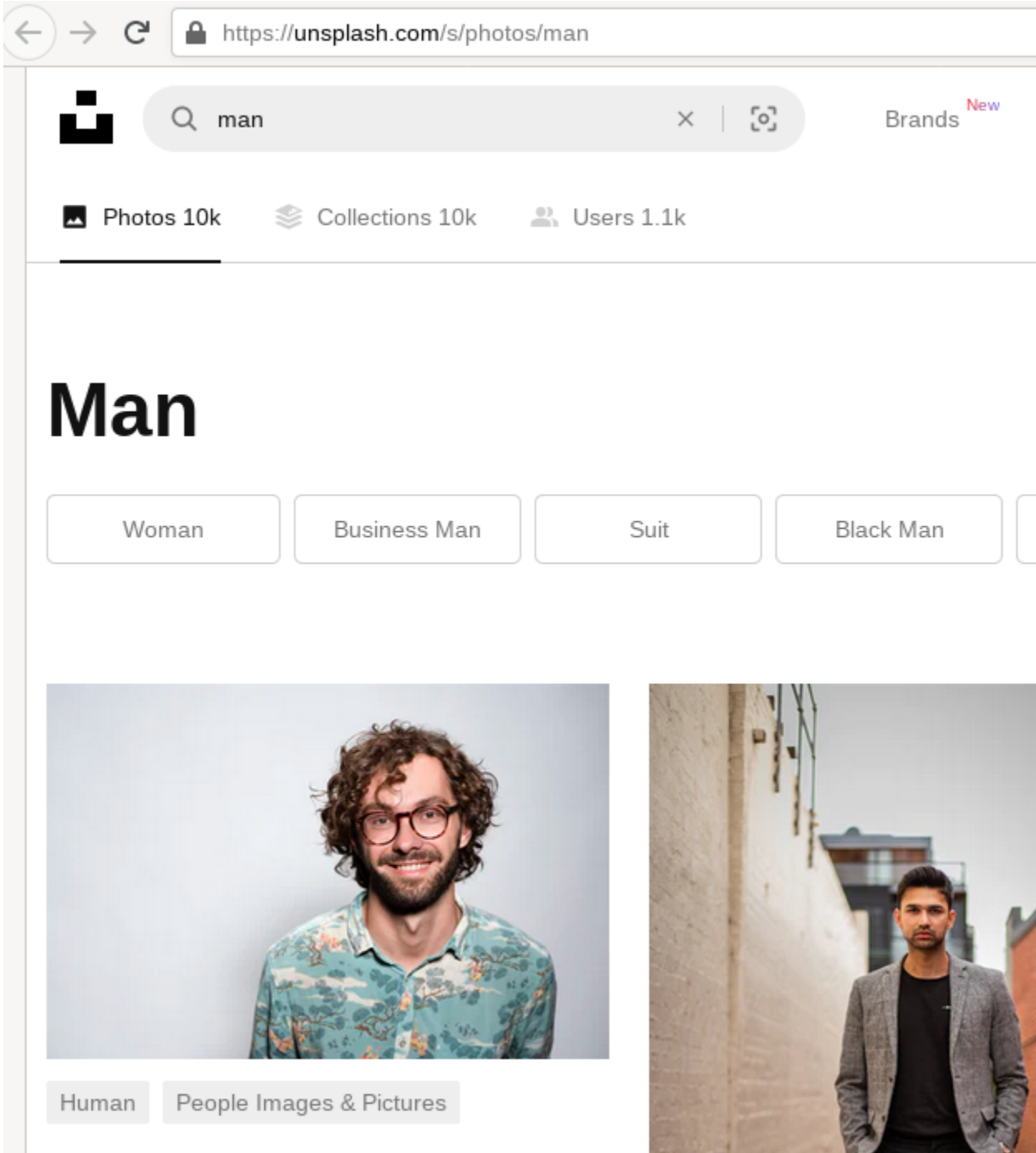
Brands ^{New} Explore ... Submit a photo Login Join free

10k Collections 10k Users 1.1k Any orientation Any color Sort by Relevance

Human Coat

Human People Images & Pictures

Source:



Source:

The website also has a donation page pointing to a bitcoin address, which could be interesting from a 'follow-the-money' perspective, but there are unfortunately no transactions with this address:

Send BTC here: `bc1qcatkzga54sz3eyzwlr4hzmtd37rgpenqp62yz`

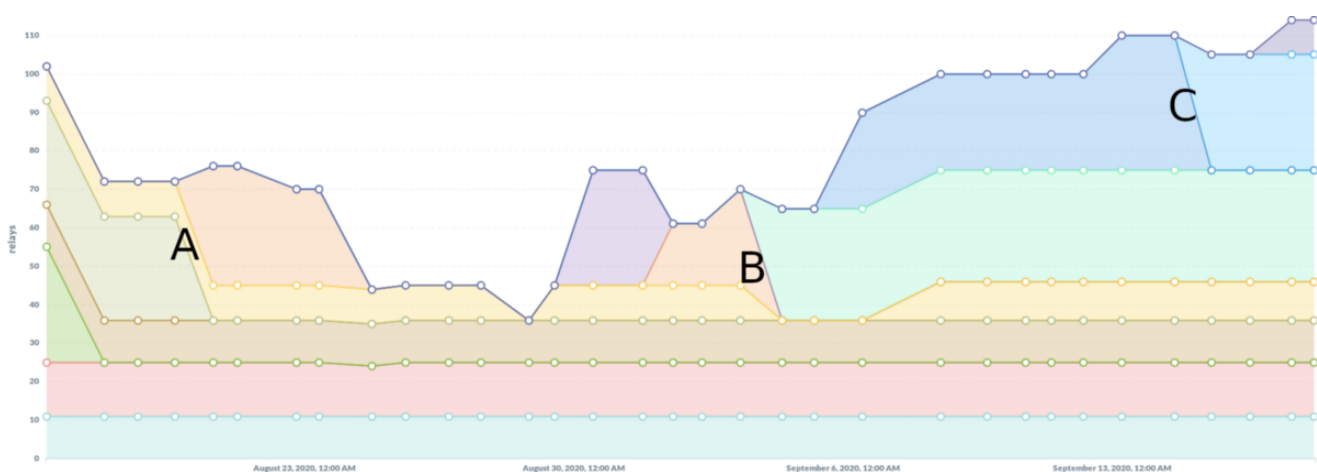
[Go back](#)

Donation bitcoin address shown on the rudimentary relaystor.xyz website. This address has 0 transactions: (source:)

Timeline for events related to andrejgvozdev55@gmail.com (not comprehensive)

- 2020–09–03 Андрей Гвоздев reports the undeclared relay group of CypherPunkLabs to the bad-relays mailing list. (10 days before that I did send about this — which might gave them this idea in the first place)
- 2020–09–03 I responded by letting them know that the CypherPunkLabs relay group is on our radar and that we were in contact with them.
- 2020–09–07 first malicious exit at SOFTplus Entwicklungen GmbH gets added (185.32.222.167) — no ContactInfo given. The abuse contact (RIPE database) later points to
- 2020–09–15 first RIPE DB entries related to are created
- 2020–09–21 's on the tor-relays mailing list
- 2020–09–26 impersonation: first malicious exit relays using CypherPunkLabs as contact appear (relay fingerprint:
1EC0CCAFA8ABD5470B062AF470EAC97DD069C655)
- 2020–10–31 a large fraction of by tor directory authorities
- 2020–11–06–2020–12–16: more tor exit relays get added in the two identified IP blocks located in (Datasource AG) and at other known hosters (, more ,)
- 2020–12–31 a new relay using a previously confirmed and known malicious ContactInfo (“” — see) appears on one of the known IP block in AS51395 (91.192.103.35) with abuse contact pointing to “”
- 2021–01–16 ContactInfo (“”) and nickname is removed from that relay (using this known malicious ContactInfo was probably unintentional)
- 2021–01–18 I reached out to using a random email address, but they didn't want to disclose which tor relays they run.
- 2021–02–04 malicious tor exit relays removal event: at (,)
- 2021–02–18 malicious tor exit relays removal event at multiple hosters (Amarutu Tech., OVH, Frantech, ...)
- 2021–02–22: get added again ()
- 2021–03–04 malicious tor exit relays removal event at OVH
- 2021–03–14 malicious tor exit relays removal event: this is the last seen date for many malicious tor exit relays at AS51395, Datasource AG and a few other ASes (Amarutu Tech, Liteserver Holding, ...).
- 2021–04–08 23 new tor exit relays using contactInfo “andrejgvozdev55(at)gmail(dot)com [tor-relay.co]” join the tor network
- 2021–04–10 previously identified malicious exit relays (reported to the Tor Project in August 2020) join the Tor network again. (removed on 2021–04–27)
- 2021–04–12: Last seen date for the relays using contactInfo “andrejgvozdev55(at)gmail(dot)com [tor-relay.co]”;

Appendix II



Timeseries graph showing the new malicious groups getting added immediately after a removal event, which makes them linkable. Graph by (raw data source:)

- : malicious exit group with contact “kleinendorstwiebe AT gmail DOT com” gets kicked→”cockcockcockcock(at)cock(dot)li” relays become exit relays (previously non-exits)
- : malicious exit group with contact “cockcockcockcock(at)cock(dot)li” gets kicked → “exit_abuse@posteo.net” relays
- : exit group with contact “BlackHatsMatter@protonmail.com” gets kicked→”hgonxhe51@gmail.com” relays

Appendix III

Emails from andrejgvozdev55@gmail.com on public Tor Project mailing lists:

[tor-relays] SSH

Hello I'm running a TOR relay, every time I SSH to my server I see a message that there were thousands of failed login...

lists.torproject.org

<https://lists.torproject.org/pipermail/tor-relays/2021-March/019420.html>

[tor-relays] ISP

Edit description

lists.torproject.org

[tor-relays] Relay Configurator

Next message (by thread): [tor-relays] Relay Configurator

lists.torproject.org

<https://lists.torproject.org/pipermail/tor-relays/2021-April/019552.html>