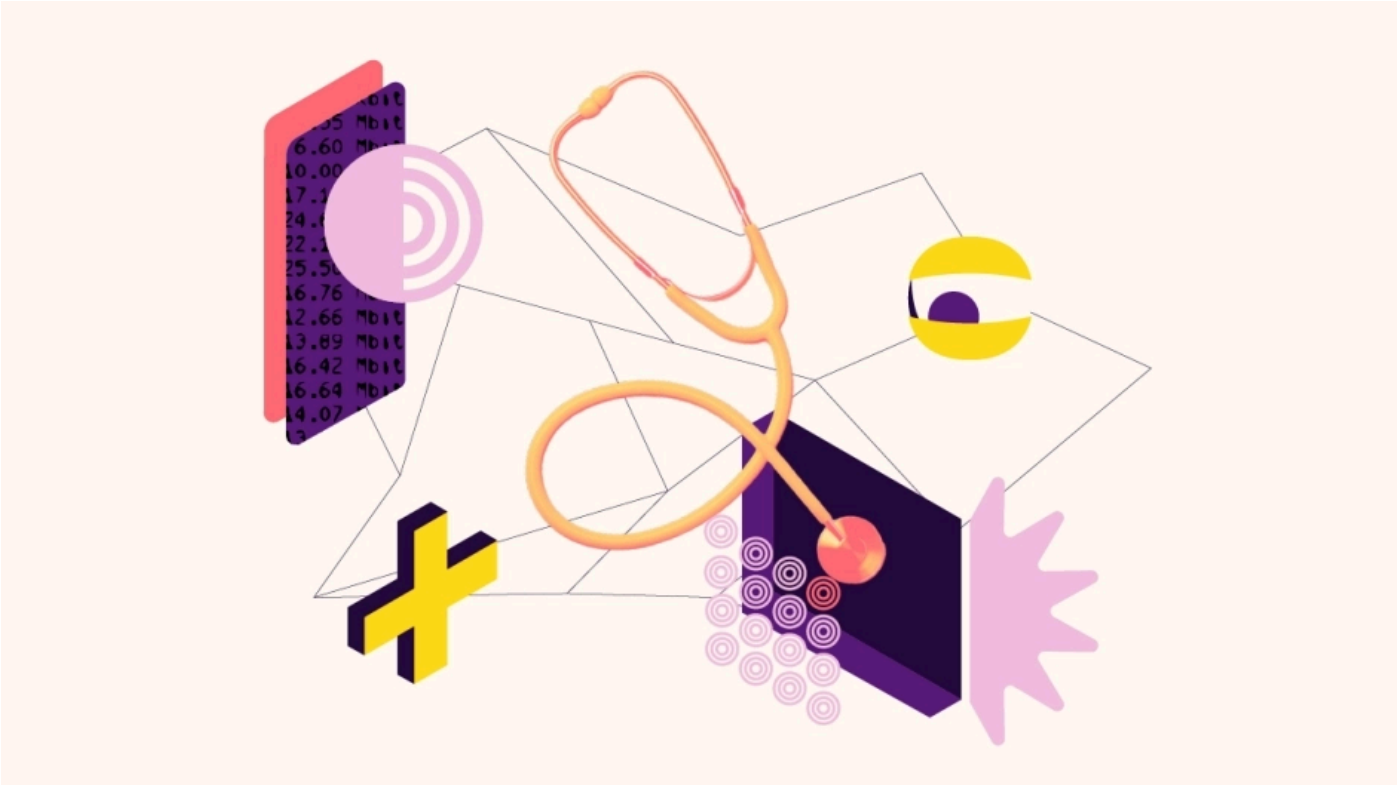
Is Tor still safe to use?

by isabela and pavel | September 18, 2024



+++ Update October 10th, 2024 +++

In response to the claims made in Deutsche Welle's (DW) reporting, which suggests that v3 Onion Services were impacted by this attack, we cannot confirm whether the affected service had Vanguard protections enabled. Given the time frame of the attack, it is likely the affected service lacked Vanguard protections, which made Onion Services more vulnerable to relatively easy guard discovery attacks although the exact method remains unclear.

We are continuing to investigate this issue and will provide updates as more information becomes available.

We are writing this blog post in response to an investigative news story looking into the de-anonymization of an Onion Service used by a Tor user using an old version of the long-retired application Ricochet by way of a targeted law-enforcement attack. Like many of you, we are still left with more questions than answers--but one thing is clear: Tor users can continue to use Tor Browser to access the web securely and anonymously. And the Tor Network is healthy.

Please note, that for the great majority of users worldwide that need to protect their privacy while browsing the Internet, Tor is still the best solution for them. We encourage all Tor users and relay operators to always keep software versions up to date.

From the limited information The Tor Project has, we believe that one user of the long-retired application Ricochet was fully de-anonymized through a guard discovery attack. This was possible, at the time, because the user was using a version of the software that neither had Vanguards-lite, nor the vanguards addon, which were introduced to protect users from this type of attack. This protection exists in Ricochet-Refresh, a maintained fork of the long-retired project Ricochet, since version 3.0.12 released in June of 2022.

Vanguards-lite, released in Tor 0.4.7, protects against the possibility of combining an adversary-induced circuit creation with circuit-based covert channel to obtain a malicious middle relay confirmed to be next to the user's Guard. Once the Guard is obtained, netflow connection times can be used to find the user of interest. In this case, the netflow attack could proceed quickly, because the attacker was able to determine when the user was online and offline due to their Onion Service descriptor being available, combined with the low number of users on the discovered Guard.

Responsible Disclosure

In contrast to the CCC, Chaos Computer Club, who was provided access to the documents related to the case and was able to analyze and validate the reporter's assumptions, we were only provided a vague outline and asked broad clarifying questions that left us with uncertainty of the facts, and questions of our own. While we appreciate the journalist contacting us, this same access was not given to the Tor Project.

Given the potential risk to our users, we decided to go public. We requested that anyone with additional information about the case share it with us. This would allow us to conduct our own analysis and determine the best course of action to protect our users.

To be clear, The Tor Project did not intend to ask for the sources of the story, but sought to understand what evidence existed for a de-anonymization attack to accurately respond to the investigating reporter's questions and assess our disclosure responsibilities. And we continue to have an interest in obtaining more information about how Onion Services users were de-anonymized. If we had access to the same documents as CCC, it would be possible to produce a report with more clarity regarding the actual state of the Tor network and how it affects the great majority of its users.

We need more details about this case. In the absence of facts, it is hard for us to issue any official guidance or responsible disclosures to the Tor community, relay operators, and users.

We are calling for more information from you.

If you have any information that can help us learn more about this alleged attack, please email security@torproject.org.

If you want to encrypt your mail, you can get the OpenPGP public key for this address from keys.openpgp.org. Fingerprint: 835B 4E04 F6F7 4211 04C4 751A 3EF9 EF99 6604 DE41

Your assistance will help all of us take the necessary steps and precautions to keep Onion Services safe for the millions of users that rely on the protections Tor provides.

A healthy network

It is important to note that Onion Services are only accessible from within the Tor network, which is why the discussion of exit nodes is irrelevant in this case. But we would like to share that the number of exit nodes has significantly increased over the past two years, with over 2,000 now available. To the best of our knowledge, the attacks happened between 2019-2021.

While it is fair to question the concentration of these nodes in certain countries or operations, this has very little to do with the described attack from what we learned in the articles published so far. The attacks occurred on an old version of the long-retired application

Ricochet that lacked new features The Tor Project has released since to mitigate against the kind of 'timing' analysis described in the articles. The most current versions of Ricochet-Refresh have such protections in place.

Another important thing to mention is the longevity of the user connection for such 'timing' analysis to be successful. A Tor Browser user that does not maintain its connection for a long time, is less vulnerable to such analyses.

After the period of the attacks described to us, 2019-2021, our Network Health team has flagged thousands of bad relays which the Directory Authorities then voted to remove. Those included many that would come from a single operator or tried to enter the network in large scales. The Network Health team has implemented processes to identify possible large groups of relays that are suspected to be managed by single operators and bad actors and not allow them to join the network.

The Tor Project knows that diversity of relays is a pressing issue for the Tor community and we are having many conversations with our community and relay operators about this subject to understand how we can address common pain points together.

Over the last year alone, we've launched a number of new initiatives such as the EFF's Tor University Challenge and the introduction of the Tor's network health API at DEF CON 32 earlier this year. Tor's bandwidth has actually increased substantially in recent years, as shown in this link: https://metrics.torproject.org/bandwidth.html?start=2013-06-20&end=2024-09-18. This means the Tor network is faster than it has ever been. And we continue to conduct outreach campaigns and efforts to grow the network.

You can help

We encourage those who can to volunteer and contribute bandwidth and relays to grow and diversify the Tor network. By ensuring hardware, software, and geographic diversity of the Tor network, we can continue to significantly minimize the potential for abuse and surveillance on the Tor network--and make guard attacks even harder to execute. As far as the Tor community is concerned, the best way to ensure network health, protect users and relay operators is keeping Tor software up to date and following the guidance that we publish on the Tor Project's official channels.

It is important to remember that Tor is one of the few alternatives that provide a vision and actionable model for a decentralized Internet that make this sort of attack impractical for those who seek to surveil a large portion of internet users. Yet, as of today, Tor is still bound by the limitations of an internet ecosystem that is predominantly owned and governed by only a handful of large corporations.

We will continue to update this blog post as more information becomes available.

network applications community

Comments

We encourage respectful, on-topic comments. Comments that violate our Code of Conduct will be deleted. Off-topic comments may be deleted at the discretion of the moderators. Please do not comment as a way to receive support or to report bugs on a post unrelated to a release. If you are looking for support, please see our FAQ, user support forum or ways to get in touch with us.

Kontynuuj dyskusję 17 odpowiedzi

atari September 2024

here is a lot of discussion about this post: Is Tor still safe to use? | Hacker News

jbash September 2024

> From the limited information The Tor Project has, we believe that one user of the long-retired application Ricochet was fully de-anonymized through a guard discovery attack.

What is this information that you have, and why does it make you believe that?

1 odpowiedź

boldsuck ▶ jbash September 2024

This is stated in the investigations by Panorama and STRG_F.
Panorama
ARD

It also says: the investigations against the “Boystown” administrator have begun because he was looking for boys to abuse via the “Ricochet” chat service.

1 odpowiedź

jbash ▶ boldsuck September 2024

It doesn’t say anything that I noticed about it being a guard discovery attack. In fact it seems to indicate that it was just plain end to end correlation. I mean, yeah, that discovers your guard, but not in a way that vanguards are going to do anything about.

It’s true that, if I remember right, a lot of really suspicious nodes popped up on the network around that time, and maybe it was guard discovery by stimulating traffic. But it’s also true that, if you’re Germany, I’m not sure you *need* to run any nodes.

The network as a whole is worryingly easy to watch. And when you don’t really know what’s going on, it’s not necessarily the best idea to tell people to go ahead and do whatever because “it was just old software”.

Anyway, did ricochet embed its own Tor at all? Vanguards are a Tor feature, not a client feature, are they not?

… although another thing to do might be to add, and actually use, a self destruct for old versions of both classic Tor and Arti. Including the embeddable versions.

2 odpowiedzi

boldsuck September 2024

>  jbash:
>
> It doesn’t say anything that I noticed about it being a guard discovery attack.

This was mentioned several times in the reports. Among other things, the two Ricochet entry servers.

>  jbash:
>
> Vanguards are a Tor feature, not a client feature, are they not?

??
Tor can be configured as anything: client Socks5Proxy, router, HiddenService client & server, …

Vanguards-lite is both client & server (HiddenService) feature full-vanguards add one also.
https://lists.torproject.org/pipermail/tor-relays/2024-September/021862.html

At the time of this investigation, v2 HiddenService was current and vanguards lite did not yet exist.

1 odpowiedź

jbash ▶ boldsuck September 2024

> This was mentioned several times in the reports. Among other things, the two Ricochet entry servers.

OK, “guard discovery attack” is ambiguous.

As I understand it, the “guard discovery attack” that vanguards is trying to deal with is one where you run a bunch of intermediate nodes, provoke a hidden service to set up a bunch of circuits, and hope that you detect one or more of those circuits being built through your node. You do this because you can’t see much, if any, traffic that doesn’t go to nodes you control.

Another way to discover guards (and other things) is just to watch the whole network, without necessarily operating any nodes, and observe the traffic from the hidden service *to its guard*. That still discovers the guard, but vanguards has no effect on it.

What I’m saying is that the German government probably approximates a global passive adversary well enough to have success with the second attack, and that I don’t see anything in the story that tells me which method they actually used.

The fact that there were a bunch of bogus nodes around then is perhaps relevant, but not dispositive.

> `Vanguards are a Tor feature, not a client feature, are they not?`
>
> Tor can be configured as anything: client Socks5Proxy, router, HiddenService client & server, …

What I'm asking is why Ricochet, as a client of Tor, has any effect on whether vanguards are used or not. In the *original* architecture, the Tor program would be a separate entity that would be updated independent of Ricochet. Therefore Ricochet would be irrelevant to the choice to use or not use vanguards, heavy or light. So talking about how old Ricochet was would be basically irrelevant to anything.

If the Tor code was *bundled* in Ricochet (as now seems to be common but also seems like a bad idea from a security point of view), then presumably you'd have old versions of both.

I never used Ricochet and don't know how it worked.

… but there's still nothing that proves that it would matter either way.

1 odpowiedź

A **abc** September 2024

> jbash:
>
> If the Tor code was *bundled* in Ricochet (as now seems to be common but also seems like a bad idea from a security point of view), then presumably you'd have old versions of both.
>
> I never used Ricochet and don't know how it worked.

If you read about Ricochet then you'd know the answers. It's probably still on GitHub.

I tried Ricochet a long time ago but 1) it was already defunct 2) I knew my family would not like it 3) there was no (easy) way to track/log conversations 4) other stuff too.

Yes, the Ricochet app bundled the tor binary.

M **MustBeMe** September 2024

Great blog post! It's weird how the documents access were only available to the CCC.

A **abc** September 2024

> isabela & pavel:
>
> Another important thing to mention is the longevity of the user connection for such 'timing' analysis to be successful. A Tor Browser user that does not maintain its connection for a long time, is less vulnerable to such analyses

> for a long time, is less vulnerable to such analyses.

This is a key lesson, I think, but it still leaves me with questions.

For example “connection” is vague. Does that mean a connection to the Tor network? Or does that mean a connection to a site (whether onion or not)? Both?

If I run without JavaScript (which is as often as possible) I’m fairly certain no continuous connections to a site are going to happen. (Barring a page with meta refresh in the head.)

When I leave for lunch and Tor Browser is left running, there is a continuous connection to the Tor network. Should I choose “Work Offline” each time I go away from my computer? I’d rather do that than quit TB altogether. (I use both regular browsing windows and Private windows, the latter keeps the history from becoming cluttered.)

In writing this I think I figured out the answer 😉 but will post it anyway so hopefully others can benefit. 🙂

M **mulloch94** September 2024

Pleased to see Tor make an announcement on this. I must say, this whole thing kind of reeks of German law enforcement overplaying the situation in an attempt to spread panic. Unless this story has been updated, I’m still confused as to where the exit nodes play any role in the actual deanonymization of a single Ricochet user. Simply put, they don’t. I was reading this from a 3rd party source (In German, which I don’t speak or read) however, so perhaps I didn’t have all the facts. But now after this PSA I think I’m even more convinced. I don’t see how one user using an outdated project not even being maintained anymore bears any weight to the claim law enforcement is using exit nodes to deanonymize people.

1 odpowiedź

A **abc** September 2024

> M mulloch94:
>
> …I’m still confused as to [whether] exit nodes play[ed] any role… [?]

No.

There is no such thing as an exit node to reach an onion site.

1 odpowiedź

M **mulloch94** ▶ abc September 2024

I meant where when I said where. I’m aware there’s no exit nodes used to reach onion sites. There was, however, a German report that said law enforcement seized a number of exit relays and were deanonymizing people with that information. But that wasn’t mentioned here by Tor’s announcement nor was it mentioned anywhere else. Also, given the nature of the network

Tor's announcement nor was it mentioned anywhere else. Also given the nature of the network itself, and what limited information exit relays can know about Tor users, to me this suggests the German authorities are probably blowing smoke. Unless more information drops I have no reason to believe them.

1 odpowiedź

MadeInDex September 2024

Will you implement timing delays & cover traffic? Or is that unnecessary?

boldsuck September 2024

> jbash:
>
> It doesn't say anything that I noticed about it being a guard discovery attack.

Panorama

> So ermittelte das BKA zweimal Tor-Knoten, mit denen sich vom damaligen "Boystown"-Administrator Andreas G. betriebene Plattformen ins Tor-Netzwerk verbanden. Dabei handelte es sich zum Beispiel um einen Chat, in dem sich führende Mitglieder verschiedener pädokrimineller Foren austauschten. **Zweimal gelang es überdies, sogenannte "Eintrittsserver"** vom Chatdienst "Ricochet" zu identifizieren, den G. nutzte - es war der Durchbruch für das BKA. Zur finalen Identifikation verpflichtete das Amtsgericht Frankfurt am Main schließlich den Provider Telefónica, unter allen o2-Kundinnen und -Kunden herauszufinden, wer von ihnen sich zu einem der identifizierten Tor-Knoten verband.

> jbash:
>
> It's true that, if I remember right, a lot of really suspicious nodes popped up on the network around that time,

KAX19 - Their discovery and blocking in the Tor network was reported at the time.
But this was also mentioned in the investigative reports. Do you only read the headlines? If you are really interested in the topic you should read the journalistic articles linked to it. And the corresponding thread in the relay mailing list.

> jbash:
>
> The network as a whole is worryingly easy to watch.

- It finally takes a year and a half until they identify the node (Guard) that Admin uses to connect to the Tor network.
- The timing analysis included complete surveillance of the mobile operator Telefónica

(o2). We have four mobile phone networks in Germany. Telefónica Group o2 has almost 43 million mobile phone customers.

I don't think that's easy. And in order to get such extensive provider monitoring approved, serious criminal acts would have to have taken place.

These things do not apply to normal users who spend a few hours a day researching anonymously on the Internet.

> jbash:
>
> Vanguards are a Tor feature, not a client feature, are they not?

Vanguards-lite has been auto enabled in the client for years.
Isabela has already written that.

1 odpowiedź

boldsuck September 2024

> mulloch94:
>
> There was, however, a German report that said law enforcement seized a number of exit relays and were deanonymizing people with that information.

I don't know that Tor exit servers have been seized in recent years. (But many exit operators have had their houses searched.) And even if there were seized servers, there are no logs.[1] A Tor relay is a router (like the internet backbone router) that routes encrypted connections and no relay knows the complete connection.

[1]The cops only have many work to do but don't get any information. I know that the cybercrime departments in Germany are completely overloaded. They told me that themselves and I saw the mountains of confiscated IT equipment. When I worked there as an electrical engineer.

jbash ▶ boldsuck October 2024

> Zweimal gelang es überdies, sogenannte "Eintrittsserver"

We've already been over that. There are different ways to discover guards, and not all of them are "guard discovery attacks" in the sense that was bein used *here*.

> Their discovery and blocking in the Tor network was reported at the time.

… and yet nobody knows for sure who was operating them or whether they were related to this. Yes, I did read it, and it gave me no new or convincing information.

> I don’t think that’s easy.

It’s easy once you have the infrastructure set up and the aprovals in place.

> And in order to get such extensive provider monitoring approved, serious criminal acts would have to have taken place.

The whole point of something like Tor is that you want to protect people even when some government *does* think “serious criminal acts” have taken place. What is and is not a “criminal act” is a matter of politics and can vary from place to place.

If it can’t protect against a government that considers something a priority, then it’s not serving its most important purpose.

Whether a “normal user” (whatever that means) can hide from some advertising tracker is a distinctly secondary concern, especially because if that’s all you care about, you don’t need anything as heavy as Tor to begin with.

It’s true that the German government is unusually well positioned to attack the network, and that other governments may have more trouble. It’s nonetheless a problem that the network’s guarantees can be breached.

> Vanguards-lite has been auto enabled in the client for years.

The “client” here is the application *using* tor. The *SOCKS* client. I wouldn’t call the tor program itself a client of tor.

1 odpowiedź

boldsuck October 2024

> jbash:
>
> > Vanguards-lite has been auto enabled in the client for years.
> >
> > The “client” here is the application *using* tor. The *SOCKS* client. I wouldn’t call the tor program itself a client of tor.

It doesn’t matter if your app uses the SocksPort or the ControlPort. The app (such as TorBrowser or Ricochet-Refresh) uses Tor in client mode and **Vanguards-lite is active**.

I hope you run some relays to improve the situation for people in oppressive systems.
Then a second Operation Liberty Lane for the United States, Brazil, Germany, and the United Kingdom will no longer be as easy as it was in 2019-2021.

Kontynuuj dyskusję

Upcoming Events

June 23, 2026 – June 24, 2025
DW Global Media Forum (GMF) 2026

Recent Updates

Sunsetting Tor 0.4.8 – Please update to 0.4.9 by September

by ahf | June 23, 2026

We want to sunset Tor 0.4.8. Please update before September.

New Release: Tails 7.9

by tails | June 18, 2026

Tails 7.9 is now available.

New Release: Tor Browser 15.0.16

by boklm | June 17, 2026

Tor Browser 15.0.16 is now available from the Tor Browser download page and also from our distribution directory.

Download Tor Browser

SUBSCRIBE TO OUR NEWSLETTER

Get monthly updates and opportunities from the Tor Project:

Sign up