# Who is Running Hundreds of Malicious Tor Relays? | Darknetlive

Archived: 2026-04-05 14:20:01 UTC

A threat actor is running hundreds of malicious Tor relays as part of what researchers suspect is an attempt to deanonymize Tor users.

Nusenu, a Tor relay operator, first identified “KAX17” as a sophisticated threat actor in 2019. At the time, Nusenu had identified a “long-running suspicious relay group” that was active since 2017, if not earlier. “At their peak, they reached >10% of the Tor network’s guard capacity,” Nusenu wrote in 2019.

In nusenu’s most recent blog post about KAX17, they provided the following summary of the actor’s behavior:

- active since at least 2017
- sophistication: non-amateur level and persistent
- uses large amounts of servers across many (>50) autonomous systems (including non-cheap cloud hosters like Microsoft)
- operated relay types: mainly non-exits relays (entry guards and middle relays) and to a lesser extend tor exit relays
- (known) concurrently running relays peak: >900 relays
- (known) advertised bandwidth capacity peak: 155 Gbit/s
- (known) probability to use KAX17 as first hop (guard) peak: 16%
- (known) probability to use KAX17 as second hop (middle) peak: 35%
- motivation: unknown; plausible: Sybil attack; a collection of tor client and/or onion service IP addresses; deanonymization of tor users and/or onion services

In October 2020, nusenu reported KAX17’s exit relays to the Tor Project which resulted in their removal from the network. Before the removal of the actor’s exit relays, a Tor user had up to a 16% chance of connecting to one of KAX17’s guard relays, up to a 35% chance of using KAX17’s middle relays, and up to a 5% chance of using one of the actor’s exit relays. The worst-case scenario on 2020, 09, 08, nusenu wrote, KAX17 could de-anonymize tor users with the following probabilities:

- first hop probability (guard) : 10.34%
- second hop probability (middle): 24.33%
- last hop probability (exit): 4.6%’

Guard, middle and exit probability between 2019–01–01 and the removal event on 2021–11–08 | nusenu

The day after the Tor Project had removed the exit relays reported by nusenu, a new "large no-name exit relay group" appeared. Nusenu has not attributed the new group to KAX17 yet but also does not believe KAX17 "halted their exit operations completely."

While investigating this threat actor's relays, nusenu discovered an email address that had initially appeared in the ContactInfo descriptor field of KAX17's relays. The actor later removed the email address. When looking into the email address, nusenu found it on the tor-relays mailing list.

"Interestingly it became almost exclusively involved on the mailing list when policy proposals with regards to malicious relays were discussed or when large malicious relay groups got removed. They apparently disliked the proposals to make their activities less effective."

(Nusenu noted that any relay operator could have used the particular email address for their relay's ContactInfo. However, the email address appeared on KAX17's relays long before appearing on the tor-relays mailing list.)

Nusenu outlines some potential solutions in their blog post. It is worth reading if tor's weaknesses are of interest to you: Is "KAX17" performing de-anonymization Attacks against Tor Users?

Cimpanu, reporting for The Record, asked nusenu about the chances of KAX17 being part of a research project. Nusenu provided the following response:

- Academic research is usually limited in time. KAX17 has been active since 2017.
- Researchers do not get involved in weakening anti-bad-relays policies on the Tor mailing list.
- Researchers do not fight against their removal and do not replace removed relays with new relays.
- Research-based relays usually run within 1-2 autonomous systems, not >50 ASes.
- Research relays usually run <100 relays, not >500.
- Research relays usually do have a relay ContactInfo.
- The Tor Project is quite well connected to the research community.

via The Record “A mysterious threat actor is running hundreds of malicious Tor relays”

It is hard to imagine this being part of a research project. Then again, Carnegie Mellon researchers conducted a traffic confirmation attack and a Sybil attack as part of some form of research. The FBI discovered this research and used it to arrest at least two people, one of whom is likely known to readers of this site: Brian Farrell, aka DoctorClu, who was involved in the administration of Silk Road 2.0.

KAX17 certainly seems like a state-backed actor.

---

Source: https://darknetlive.com/post/who-is-responsible-for-running-hundreds-of-malicious-tor-relays/