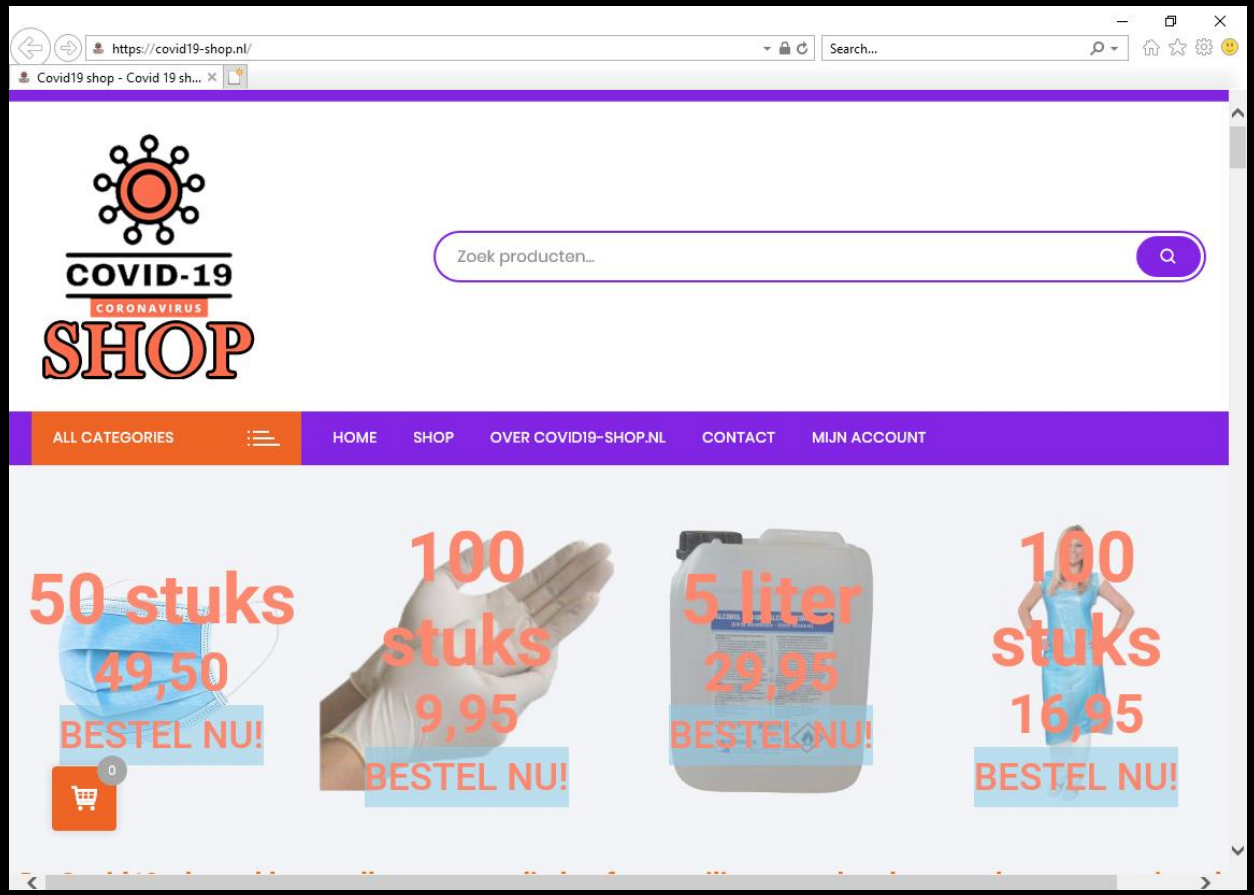
Helping hands: Measuring the impact of a large threat intelligence sharing community

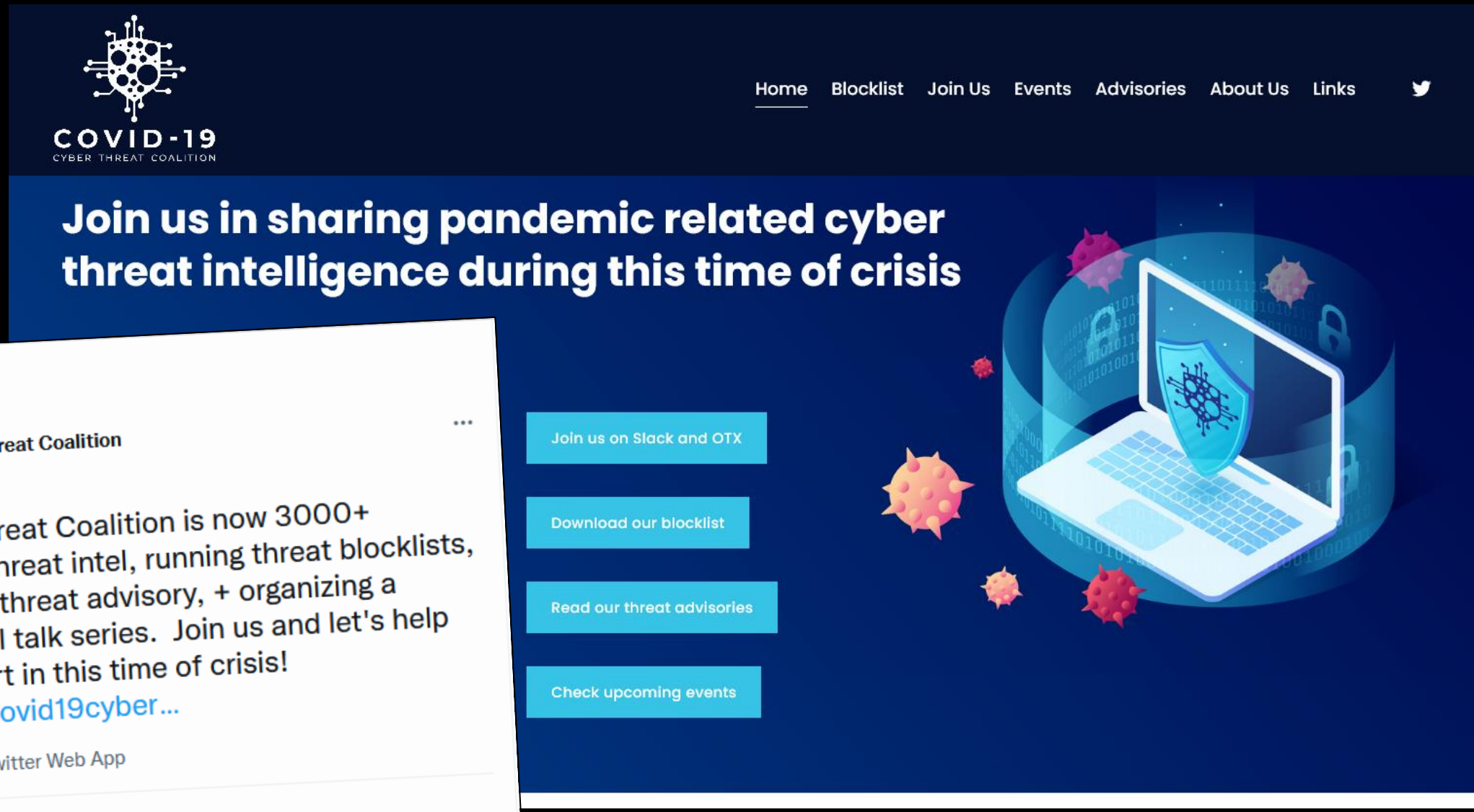
Xander Bouwman*, Victor Le Pochat, Pawel Foremski,
Tom Van Goethem, Carlos H. Gañán, Giovane C. M. Moura,
Samaneh Tajalizadehkhoob, Wouter Joosen, Michel van Eeten

In February 2020, the WHO coined the ‘coronavirus’ name.

Per day, over 5,000 domain names related to ‘coronavirus’ or ‘COVID’ were registered at its peak in March.



covid19-shop[.]nl on 2020-05-28



cyberthreatcoalition.org

Our Mission

As our global community strains under the weight of the coronavirus pandemic, cyber criminals are taking advantage, attacking our most critical institutions and playing on our fears and anxieties in campaigns of extortion and fraud. We want to help preventing that.

The COVID-19 Cyber Threat Coalition (CTC) is a global volunteer community focused on stopping these actors. We're united in our feeling that extraordinary times call for bridging traditional boundaries to operate with unity and purpose.

Collaboration

We pledge to break down traditional barriers to intelligence sharing in this time of extraordinary crisis. Cybercrime crosses organizational and national boundaries, and so must we, now more than in the past. By bringing together a broad, inclusive group of thousands and making extraordinary efforts to work together, we make patterns, outliers and trends in threats visible that would otherwise have been missed.

Professionalism

We pledge to produce a professional-quality threat feed that the broad IT security public can rely upon. Volunteerism doesn't mean a loss of professionalism or capability. Just as global militaries work to erect well-run hospitals out of converted hotels, our mission is to operate the largest professional-quality threat lab in the history of cybersecurity out of donated cloud infrastructure and with rapidly assembled teams of diverse, cross-geography, cross-industry threat researchers.

Public good

We pledge to privilege the public good over our own and our institutions' self-interest. We're professionals and professional organizations with careers and revenue to manage, but when the world is on fire, public good trumps self-interest. It follows that we don't endorse or promote commercial products, and have no tolerance for self-promotion or jockeying for position within our ranks.

cyberthreatcoalition.org/about-us/our-mission

"We pledge to break down traditional barriers to intelligence sharing in this time of extraordinary crisis."

"We pledge to **produce a professional-quality threat feed** that the broad IT security public can rely upon."

"(…) our mission is to **operate the largest professional-quality threat lab in the history of cybersecurity**"

Did the CTC community succeed?
We asked:

1. How did the COVID-19 Cyber Threat Coalition community work?

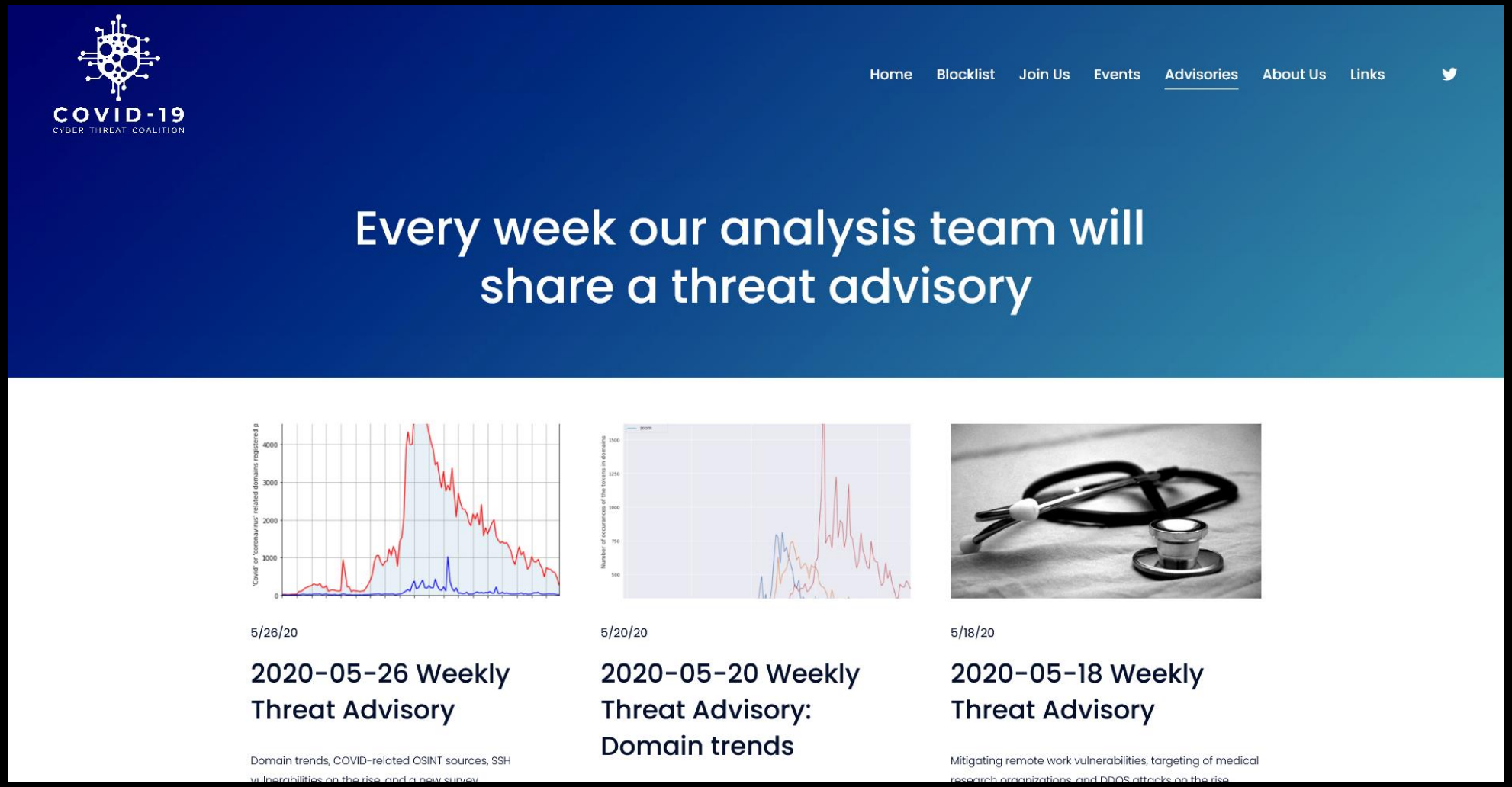
2. Does making threat data freely available improve the ability of defenders to act?

3. Does collaboration at scale lead to better coverage?

A ‘natural experiment’ to investigate long-standing questions on threat information sharing.

Our motivation: **How do we make the best use of good will?**

1 How did the CTC community work?



cyberthreatcoalition.org (available via Internet Archive)

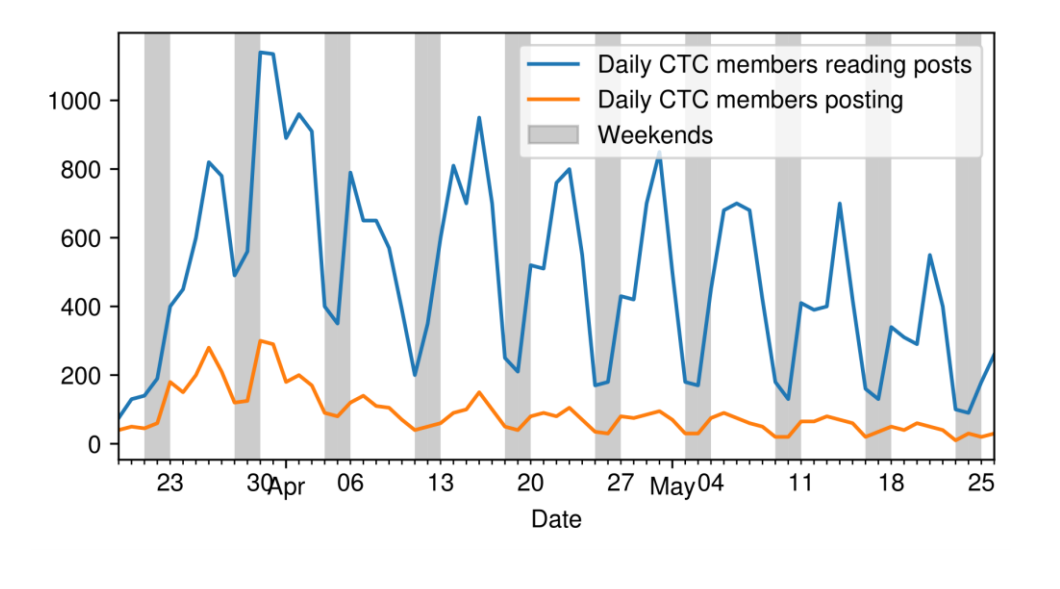


Figure 1: Member activity on the CTC Slack workspace.

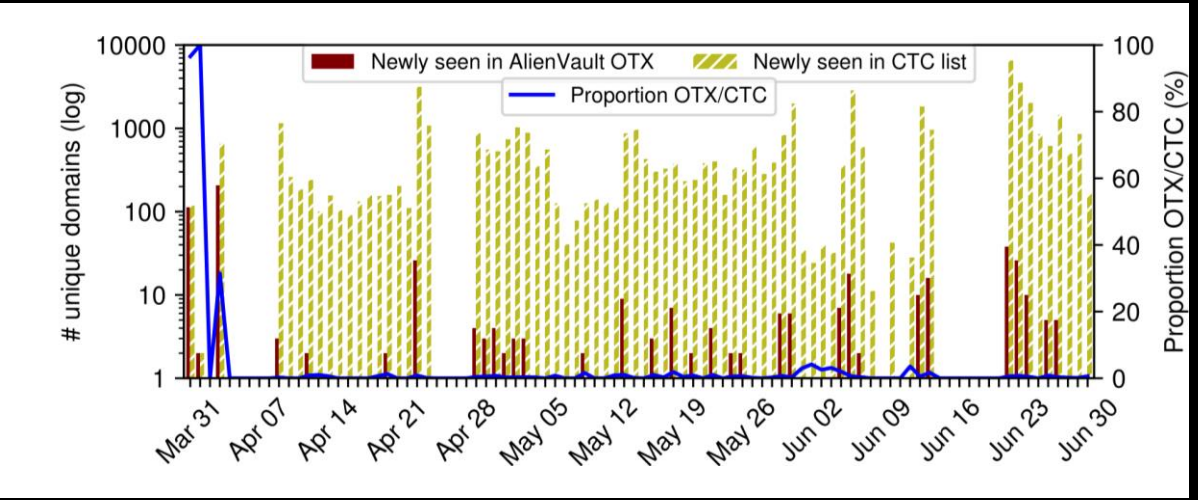


Figure 2: Counts of unique domains newly seen in the CTC AlienVault OTX group and on the CTC blocklist (log scale), and the proportion of AlienVault OTX domains that were propagated to the CTC blocklist.

2 Does making threat data freely available improve the ability of defenders to act?

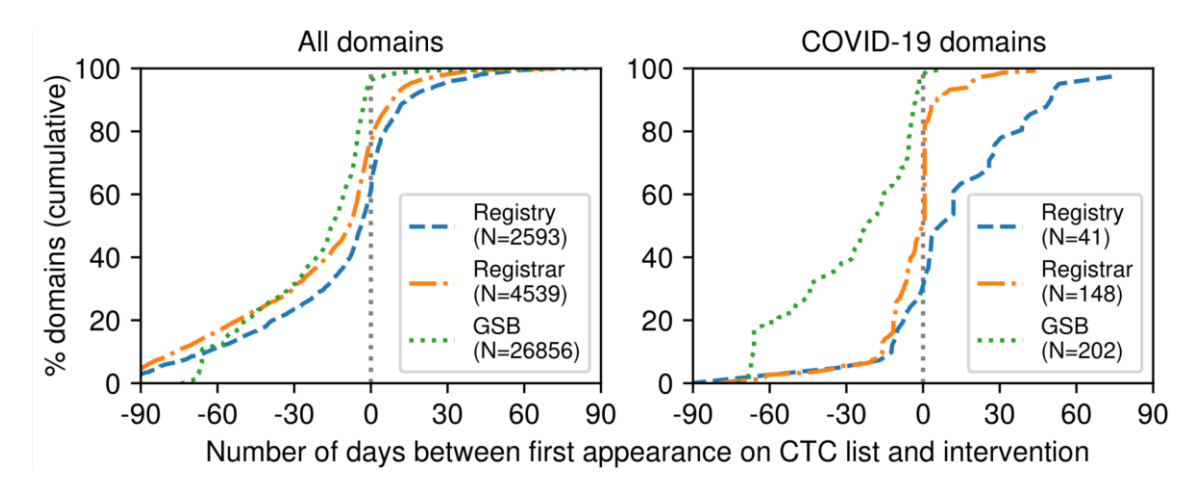


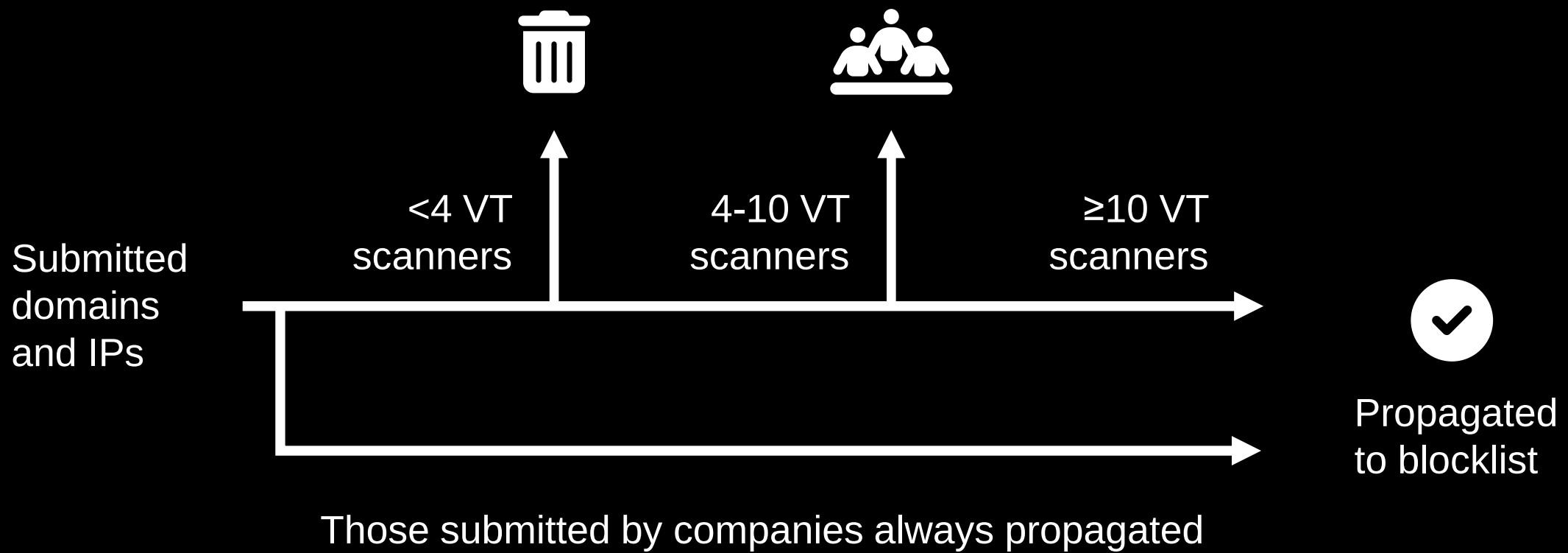
Figure 11: Delay between the first appearance of a domain on the CTC blocklist and interventions by registries, registrars and Google Safe Browsing (GSB).

CTC blocklist overall	58.4% of domains already acted on
Domains with one of 370 COVID-related keywords in 15 languages	25.1% of domains already acted on

Quad9 inclusion

3 Does collaboration at scale lead to better coverage?

Community admins wanted to “provide reasonable assurance that what we re-share with the public are examples of truly malicious artifacts”.



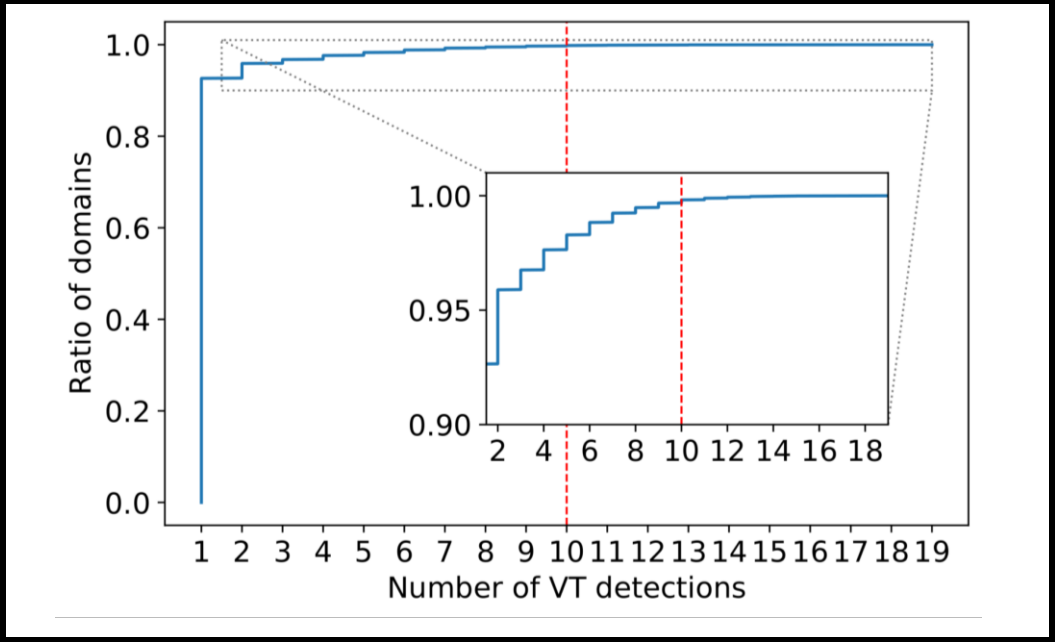


Figure 10: Proportion of COVID-19 keyword domains detected by a given number of VirusTotal domain scanners.

Domains with one of 370 COVID-related keywords in 15 languages

2.6% of blocklist

Domains containing just the keyword ‘whatsapp’

2.8% of blocklist

4 Conclusion and lessons we draw for future communities

Conclusion

Yes, volunteers **can** aggregate timely information over existing infrastructures, but we argue that this community's coverage of threats could have been better, had it capitalized on its many volunteers.

Lessons learned

1 Scaling up the community does not automatically lead to better pooling of threat information.

2 Existing threat intelligence and abuse mitigation structures are actually quite resilient and able to adapt to ‘new’ types of threats.

3 Openness of the community requires a scalable quality assurance process for the contributed indicators.

Helping hands: Measuring the impact of a large threat intelligence sharing community

Xander Bouwman*, Victor Le Pochat, Pawel Foremski,
Tom Van Goethem, Carlos H. Gañán, Giovane C. M. Moura,
Samaneh Tajalizadehkhoob, Wouter Joosen, Michel van Eeten

x.b.bouwman@tudelft.nl

@xbouwman