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.
Join us in sharing pandemic related cyber threat intelligence during this time of crisis.
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?
How did the CTC community work?
Every week our analysis team will share a threat advisory

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.
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
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”.

Submitted domains and IPs

- <4 VT scanners
- 4-10 VT scanners
- ≥10 VT scanners

Those submitted by companies always propagated

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

Domains containing just the keyword ‘whatsapp’

2.6% of blocklist

2.8% of blocklist

Figure 10: Proportion of COVID-19 keyword domains detected by a given number of VirusTotal domain scanners.
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.
Scaling up the community does not automatically lead to better pooling of threat information.

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

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