

Thesis
B.Sc.

Thesis
M.Sc.

IDP

Blocklists: Who is blocked?

Motivation

Blocklists are often used in research to label malicious hosts and to train models to identify similar malicious targets. A quick web search reveals that a multitude of blocklists exist.

Often, their entries differ massively. Some differ in respect to the actual targets but focus on the same threat. Others differ in the types of targets, e.g.:

- malicious ASes
- Spammers
- C&C Server

Efficient blocklists are a valuable product that is often monetized, thus information is limited. Therefore, an analysis of blocklists requires a detailed analysis of listed targets.

The goal of this thesis is to extend a blocklist analysis infrastructure. The current infrastructure is able to regularly download blocklists and manage entries. Furthermore, initial TLS scans are integrated. Possibilities to extend the infrastructure are the addition of further lists, the deployment of further scans, e.g., traceroutes, and the combination of data sources. Furthermore, the churn of blocklists and differences between lists should be analyzed in more detail.

Caution!

Almost all allocations change over time. Please check regularly to ensure you have the latest version of the DROP lists. They should not be imported into your networks filters and forgotten about. If you do not keep this type of filter data up to date, over time you will eventually encounter problems reaching areas of the Internet if allocations listed in an old version of these lists get reassigned to new networks. Before applying any filters or blocks to your network always carefully consider the ramifications of such filters.

<https://www.spamhaus.org/drop/>

Your Task

- Extend a blocklist analysis infrastructure
- Setup additional Scans besides TLS in close collaboration with us
- Analyse blocklisted targets in more detail based on different points of view

Requirements

- Basic programming knowledge in Python or Go
- Familiarity with GIYF-Based work approaches

Contact

Johannes Zirngibl zirngibl@net.in.tum.de
Patrick Sattler sattler@net.in.tum.de
Markus Sosnowski sosnowski@net.in.tum.de

<https://net.in.tum.de/members/zirngibl/>

