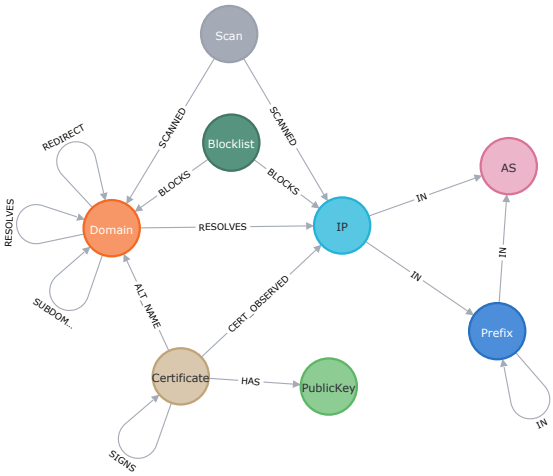
Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Thesis B.Sc. | Thesis M.Sc. | IDP, Guided Research

Propagating (Dis-)Trust accross servers in a TLS Graph

Motivation



The Internet undergoes an increasing adoption of the TLS to encrypt and authenticate traffic. This applies to malware as well. Essential for the authentication of servers is the interaction of the DNS and the x509 certificate infrastructure. With active scans it is is possible to cryptographically verify whether a server on a specific IP address has the proper certificate for a requested domain name. This creates a relation among TLS servers that can be used to propagate (mis-)trust among these servers. Previous work has established a pipeline that scans and parses the data into the TLS Graph (see the schema in the figure) which combines information from the DNS, TLS, BGP, and downloaded blocklist. Manual inspection shows the graph can reveal previously hidden relations among malware servers. For example, a certificate obtained from a blocked IP address is seen elsewhere but only one of these addresses is captured by the blocklist. However, the Internet is complex and these relations are not as clearly defined as one would hope. For example, what happens if an IP address seems to be shared by unrelated organisations? This can be caused by cloud providers or CDNs. In these cases we do not want to label them falsly as malicious if it is used both by benign actors and cyber criminals. Hence, weighting the different connections is challenging.
Graph algorithms can be used to automatically find related nodes of known malicious actors that are potentially malicious as well. Results can be validated using external sources like https://virus-total.com.

Your Task

- Research on suitable graph algorithms and possibilities to validate the results
- Implement and evaluate selected approaches

Technologies

- Python 3, networkx, scikit-learn
- Algorithms from shallow learning (e.g., LPA) or custom message passing
- Neo4j for manual inspection and visualization

Contact

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