Technische Universität München, Department of Informatics

Chair for Network Architectures and Services

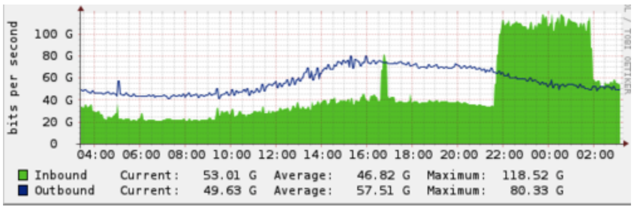
Prof. Dr.-Ing. Georg Carle

Thesis M.Sc.

IDP, Guided Research

Leveraging extended flow data for botnet detection

Motivation



```
🟩 Inbound   Current:  53.01 G  Average:  46.82 G  Maximum:  118.52 G
🟦 Outbound  Current:  49.63 G  Average:  57.51 G  Maximum:   80.33 G
```

Botnets are a major threat to the security of the Internet. The C&C servers send commands to the bots which then execute these commands and perform e.g. Distributed Denial-of-Service (DDoS) attacks, spam campaigns or scan for vulnerable hosts. In order to eliminate the threats posed by botnets it is necessary to detect C&C servers and infected hosts as participants in those botnets. Research shows [1, 3] that it is generally possible to automatically perform this detection in the network. In this thesis you will extend the flow monitoring toolkit Vermont [2] by adding new IPFIX information elements which are useful for botnet detection.

Your Task

- Identify flow information which can help in identifying botnet traffic
- Implement these new flow information elements into Vermont
- Evaluate the suitability of your approach on botnet and benign traffic

Requirements

- Knowledge in low-level programming, ideally C++
- Understanding of the concept of flow data (IPFIX)
- Willingness and motivation to experiment and learn new concepts autonomously (GIYF-based work approach)

Bibliography

[1] Leyla Bilge, Davide Balzarotti, William Robertson, Engin Kirda, and Christopher Kruegel. Disclosure: detecting botnet command and control servers through large-scale netflow analysis. In *Proceedings of the 28th Annual Computer Security Applications Conference*, pages 129–138. ACM, 2012.

[2] TUM I8. Vermont GitHub. https://github.com/tumi8/vermont.

[3] Matija Stevanovic and Jesper Melgaard Pedersen. An efficient flow-based botnet detection using supervised machine learning. In *Computing, Networking and Communications (ICNC), 2014 International Conference on*, pages 797–801. IEEE, 2014.

Contact

Oliver Gasser	gasser@net.in.tum.de
Johannes Naab	naab@net.in.tum.de

http://go.tum.de/306574