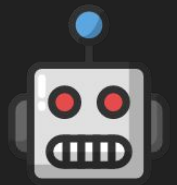


# VisiBot

## Automated detection of IoT Botnets using heuristic techniques

Author: Daniel Arthur (2086380A)
Supervisor: Dr. Angelos K. Marnerides

Level 4 Individual Project, University of Glasgow

# 1. Introduction

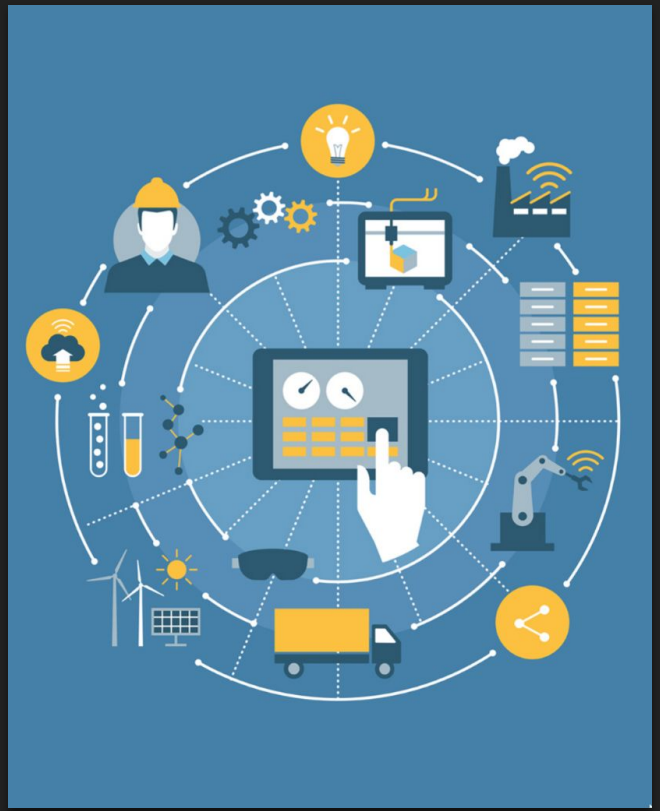
The **2016 Mirai Botnet** Attack [1]

- Targeted DynDNS
- 1.2Tbps attack strength
- Comprised entirely of IoT devices

What is the **The Internet of Things (IoT)**?

"The interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data." - Oxford Lexico [2]

https://velocityglobal.com/blog/industry-news-how-the-internet-of-things-will-impact-global-business/



# 1.1 The Problem

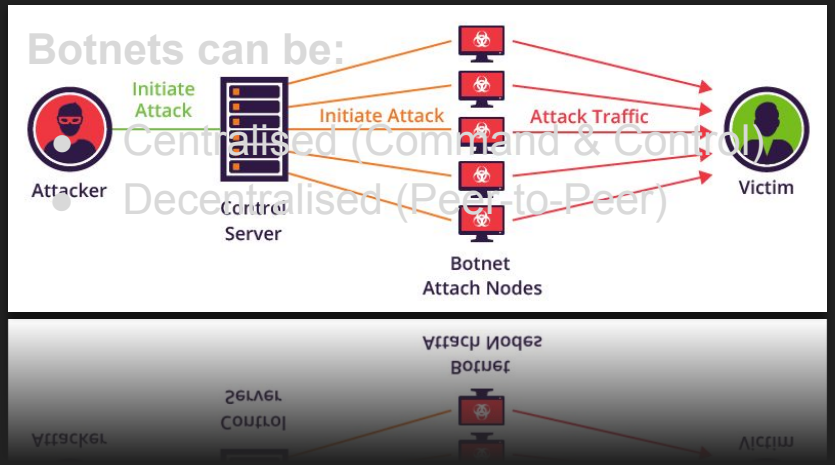
**Definition of Botnet:**

“A network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam.” - Oxford Lexico [3]

**Botnets are often used for:**

- Distributed Denial of Service (DDoS)
- Monetary gain (DDoS for hire)
- Mass spamming, Crypto-mining, Data theft

https://www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack/



# 1.2 The Solution

**Current Implementations:**

- Often highly theoretical (Difficult to automate/deploy)
- May become outdated as botnets evolve
- Exclusively targets specific botnets / communication protocols

**VisiBot -** Aims and Objectives**:**

- **Automated** botnet detection for scalability, modularity, and distribution
- **Heuristic**-based botnet identification
- **Centralised** and **Peer-to-Peer** botnet detection
- Real-time geographic **visualisation**

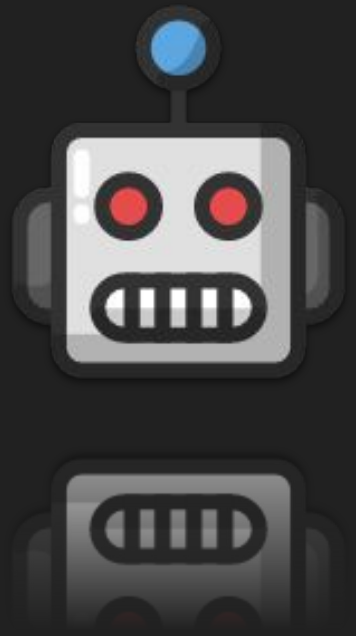
# 2. Background

- Preemptive botnet detection
  - Moon et al. (2012) [4]
- IoT Honeypot Systems
  - Pa Pa et al. (2016) and Antonakakis et al. (2017) [5, 6]
- Static & Dynamic Analysis of Centralised IoT Botnets
  - Bastos et al. (2019) and Ceron et al. (2019) [7, 8]
- DNS-based IoT Botnet Detection
  - Dwyer et al. (2019) [9]
- Peer-to-Peer IoT Botnet Detection
  - Herwig et al. (2019) [10]

# 3. Design Overview

## VisiBot Processing System

- Message Broker Design Pattern
  - **Automation** and **parallelism** through worker-based task queue
- Honeypot Packet Processing
  - **Malware extraction** and **Packet Classification**
- IoT Malware Sandbox Analysis
  - Static, Dynamic, and Network analysis
- C2 and P2P Identification
  - Through four simple **heuristics**



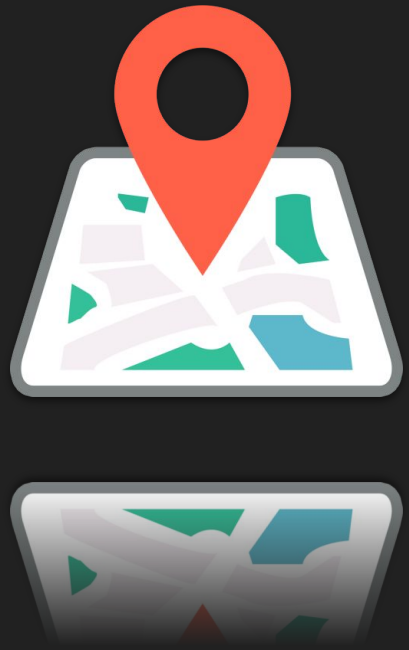
# 3.1 Design Overview: Heuristic Analysis

Malware Analysis Heuristics:

1. Infected host performs P2P DNS Query during network analysis
2. infected host performs data transaction with foreign IP address
3. Interaction between infected host and hard-coded IP address
4. Interaction between infected host and blacklisted C2 Server

# 3.2 Design Overview: Web Application

- MVC Design Pattern
  - Model, View, Controller
- Interactive Visualisation
  - Map-based User Interface
- Geographic Clustering
  - Groups markers based on distance
- Network Visualisation
  - Shows IP address interactions as a graph



# 4. Implementation

- Docker, Celery, and Redis
  - Containerised applications and deployment
  - Scalable Celery workers which consume tasks from Redis broker
- Bad Packets Honeypot Service
  - Accessible via REST API
- LiSa Sandbox Analysis
  - Automated linux malware analysis

- Additional services
  - Sources**: MaxMind GeoIP2**, **VirusTotal**, **IPWHOIS**, and **IPInfo.io**
  - Blacklists**: Spamhaus, Barracuda, Abuse.ch, Spamrats** and **DNSBL**

# 4.1 LiSa Sandbox

- Created by Daniel Uhříček [11]
- Docker + Celery + RabbitMQ
- Supports x86_64, i386, arm, mips, and aarch64
- QEMU emulation
  - Static analysis: Radare2
  - Dynamic analysis: SystemTap
- VirusTotal Integration
- REST API

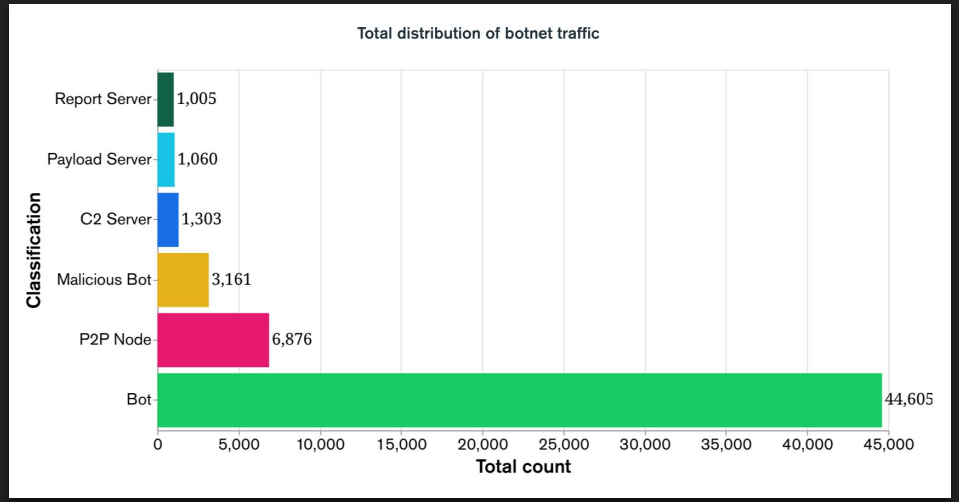
# 4.2 VisiBot Web Application

- Frontend: NuxtJS
- Backend: ExpressJS
- Database: MongoDB
- Interactive Map: LeafletJS
- User Interface: BootstrapVue

# 5.1 Results - Data Collection

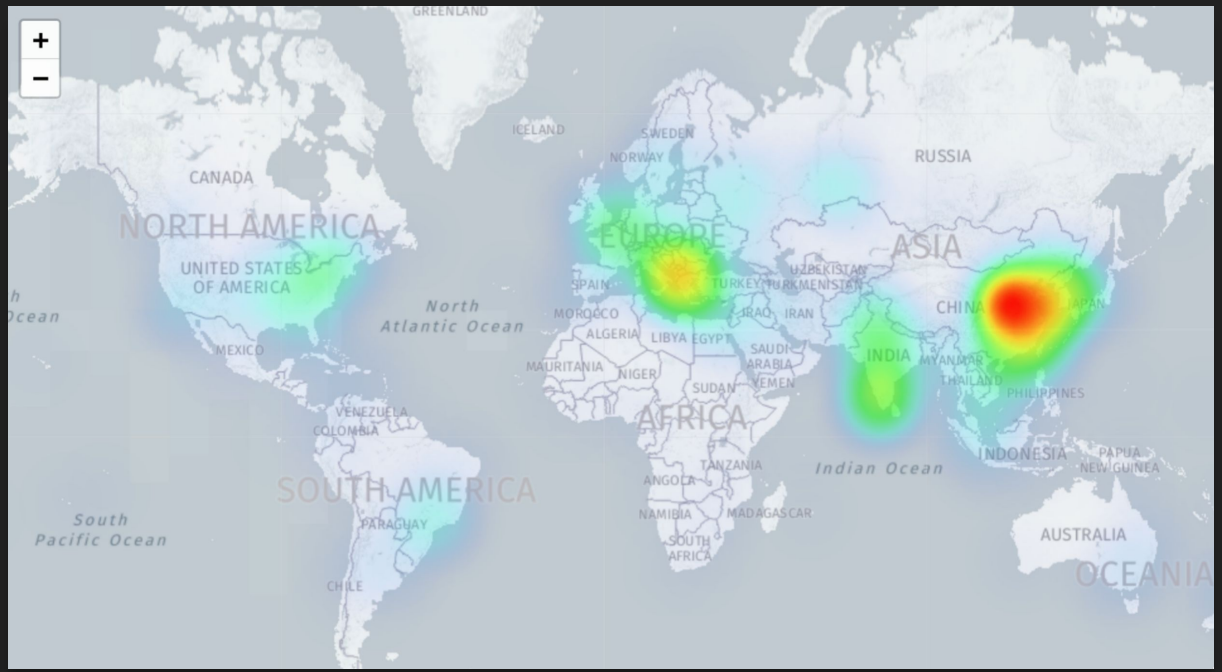
Over a 35-day data collection period:

- 58,010 Unique IP Addresses
- 82,050 Botnet Events
- 4,000 Autonomous Systems
- 1,654 Malware Samples

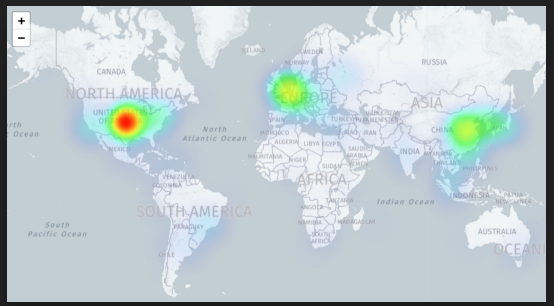


# 5.2 Results - Geographic Density

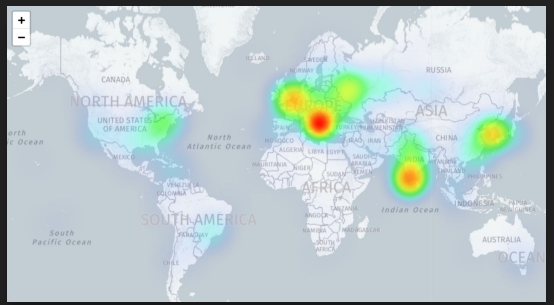
Overall Traffic Density




C2 Traffic Density



P2P Traffic Density



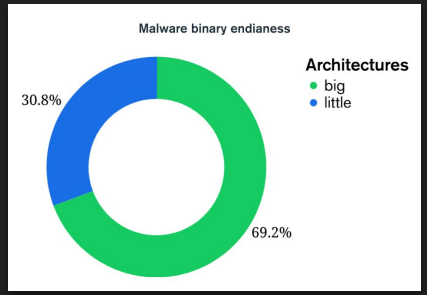
# 5.3 Results - Malware Analysis

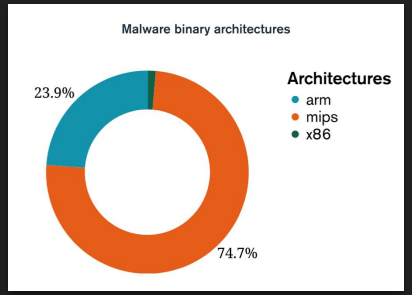
Primarily **Mozi.a** and **Mozi.m** binaries

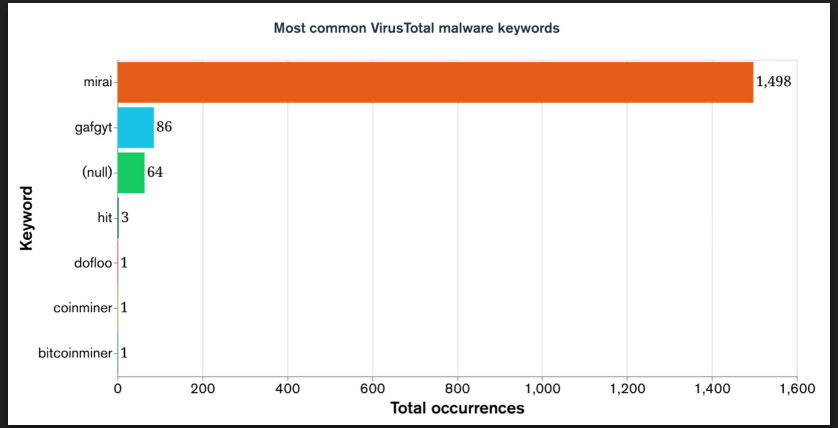
- Peer-to-Peer Mirai Botnet Variant

Other sample types:

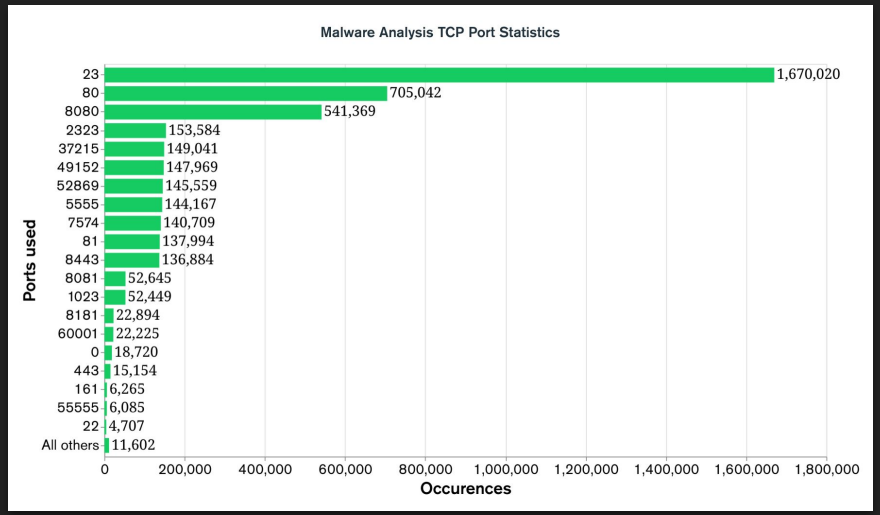
- Bashlite aka gafgyt
- Coin miners
- Unknown variants

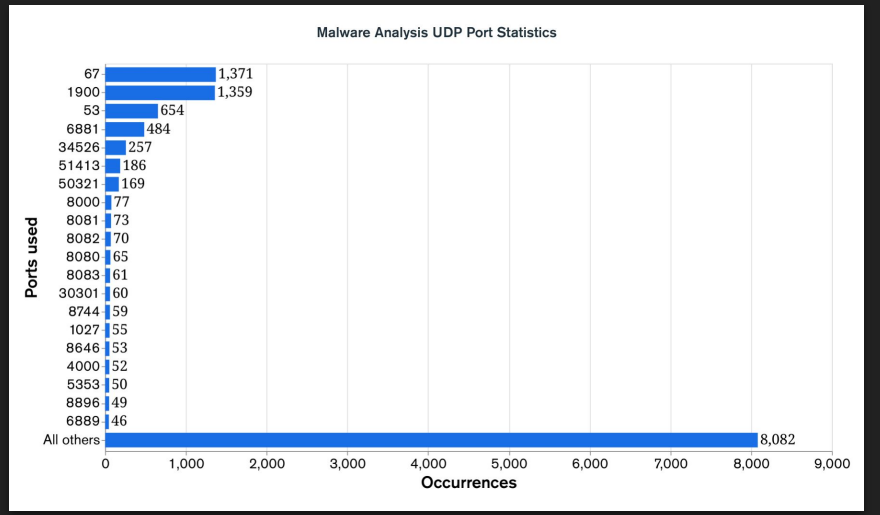


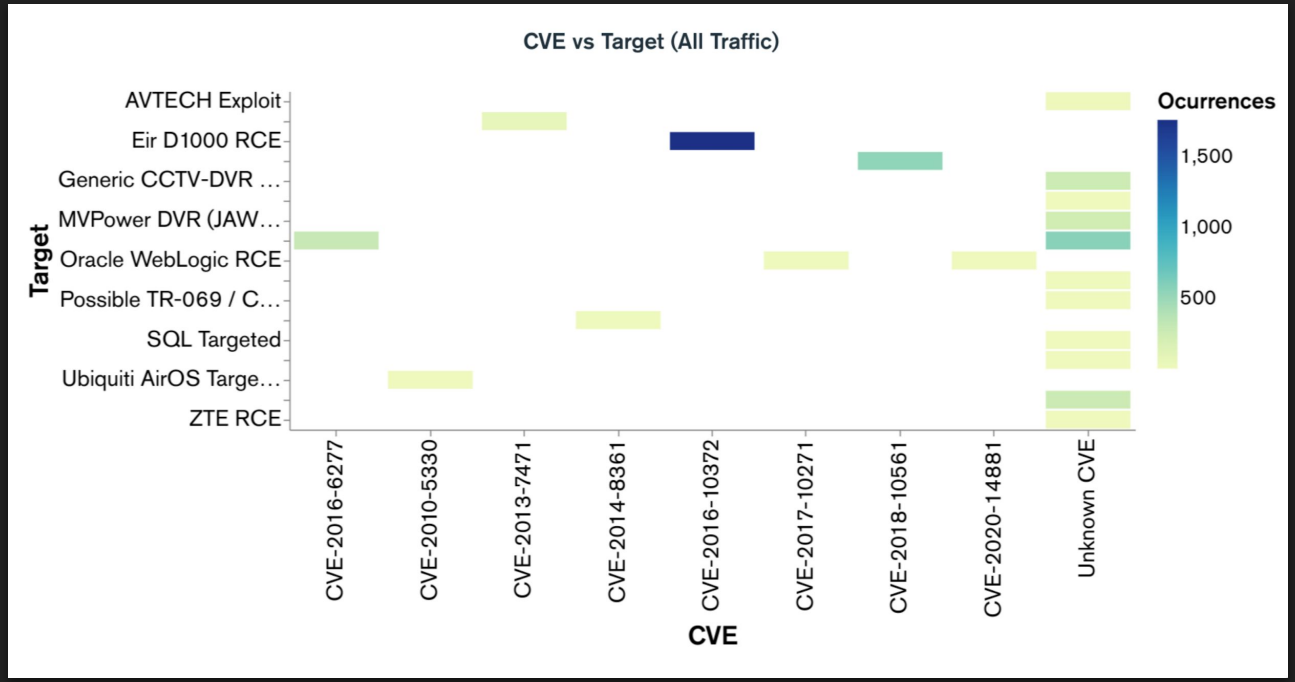
# 5.4 Results - Port Statistics (TCP vs UDP)



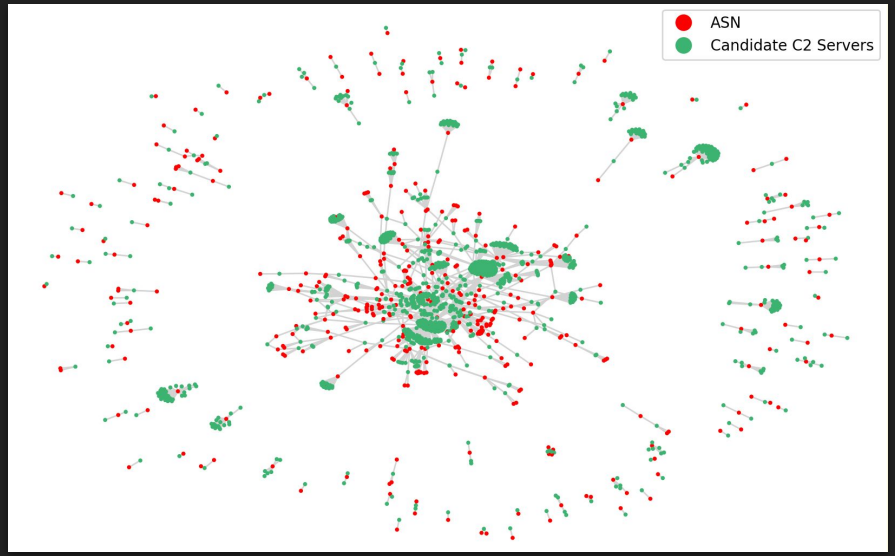

- Mostly randomly accessed ports via UDP protocol
- Telnet Port Scanning Activity: TCP Ports 23 and 2323
- Common Vulnerability Exploits (Ports 49152, 8080, 7574, etc.)

# 5.5 Results - Common Vulnerability Exploits (CVE)

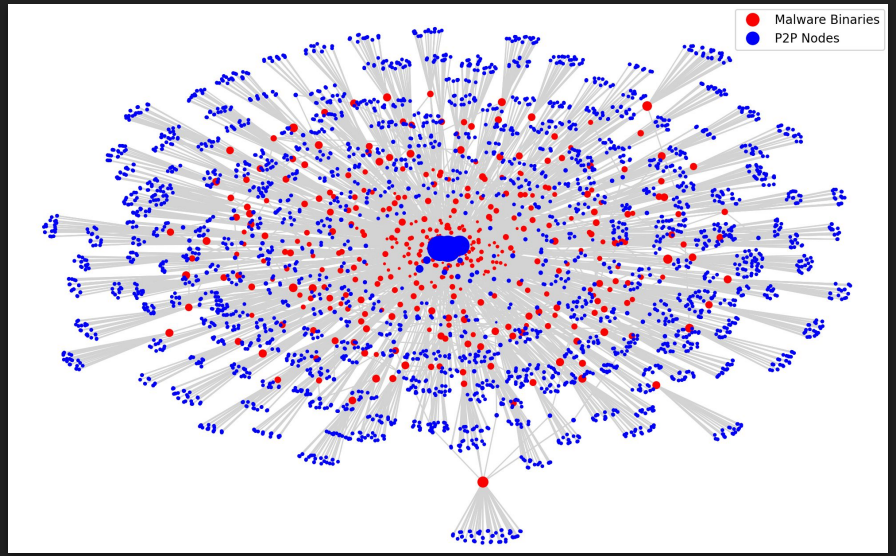


# 5.6 Results - Interaction Visualisations

NetworkX **K-Components approximation algorithm** [11]




Historical Interactions between candidate C2s and Autonomous Systems (AS).




Network interactions between analysed malware samples and Identified Peer-to-Peer nodes.

# 6. Evaluation and Conclusion

Benefits:

- Simple yet effective heuristics
- Extendable, Scalable and distributable
- Real-time visualisation of botnets and ASN activity
- Identification of centralised and Peer-to-Peer IoT botnets

Issues:

- Malware unpacking
- Candidate validation
- Sample extraction limitations

# 7. Future Work

- Stream-based Honeypot collection
- Improved malware sample unpacking
- Supplementary heuristics using captured packet information (PCAP)
- Candidate C2 and P2P validation procedures

Thank you!

# 8.1 References


1. Mark Maunder. Dyndns is currently being ddos'd – may affect your site, 2016. URL https://www.wordfence.com/blog/2016/10/dyndns-currently-ddosd-may-affect-site/. [Accessed March 24, 2021]
2. Lexico. Definition of Internet of Things, 2021. URL https://www.lexico.com/definition/internet_of_things. [Accessed April 8, 2021]
3. Lexico. Definition of botnet, 2021. URL https://www.lexico.com/definition/botnet. [Accessed April 8, 2021]
4. Young Hoon. Moon, Eunjin. Kim, Suh Mahn. Hur, and Huy Kang. Kim. Detection of botnets before activation: an enhanced honeypot system for intentional infection and behavioral observation of malware. Next Generation Communication and Network Security, 5: 1094–1101, 2012. doi: 10.1002/sec.431. URL https://doi.org/10.1002/sec.431.
5. Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, and Christian Rossow. Iotpot: A novel honey for revealing current iot threats. Journal of Information Processing, 24:522–533, 2016. doi: 10.2197/ipsjjip.24.522. URL https://dx.doi.org/10.2197/ipsjjip.24.522.
6. Artur Marzano, David Alexander, Osvaldo Fonseca, Elverton C Fazzion, Klaus Steding Jessen, Marcio Jose Chaves, Italo Cunha, Dorgival Olavo Guedes, and Wagner Meira Jr. Understanding the mirai botnet. 2018 IEEE Symposium on Computers and Communications (ISCC), pages 1093–1100, 2018. doi: 10.1109/ISCC.2018.8538636. URL https://doi.org/ 10.1109/ISCC.2018.8538636
7. Gabriel Bastos, Artur Marzano, Osvaldo Fonseca, Elverton Fazzion, Cristine Hoepers, Klaus Steding-Jessen, Chaves Marcelo H.P.C, Italo Cunha, Dorgival Guedes, and Wagner Meira. Identifying and characterizing bashlite and mirai c&c servers. 2019 IEEE Symposium on Computers and Communications (ISCC), pages 1–6, 2019. doi: 10.1109/ISCC47284.2019.8969728. URL https://doi.org/10.1109/ISCC47284.2019.8969728
8. João Marcelo Ceron, Klaus Steding-Jessen, Cristine Hoepers, Lisandro Zambenedetti Granville, and Cíntia Borges Margi. Improving iot botnet investigation using an adaptive network layer. Sensors 2019, 19, 727, 2019. doi: 10.3390/s19030727. URL https://doi.org/10.3390/s19030727.

# 8.2 References


9. Owen P Dwyer, Angelos K Marnerides, Vasileios Giotsas, and Troy Mursch. Profiling iot-based botnet traffic using dns. 2019 IEEE Global Communications Conference (GLOBECOM), 2019. doi: 10.1109/GLOBECOM38437.2019.9014300. URL https://doi.org/10.1109/GLOBECOM38437.2019.9014300.
10. Stephen Herwig, Katura Harvey, George Hughey, Richard Roberts, and Dave Levin. Measurement and analysis of hajime, a peer-to-peer iot botnet. Network and Distributed Systems Security (NDSS) Symposium 2019, 2019. doi: 10.14722/ndss.2019.23488. URL https://dx.doi.org/10.14722/ndss.2019.23488.
11. NetworkX Developers and contributors. Networkx K-Components approximation algorithm. https://networkx.org/documentation/stable//reference/algorithms/generated/networkx.algorithms.approximation.kcomponents.k_components.html, 2014–2020. [Accessed March 24, 2021].