Fraunhofer FKIE

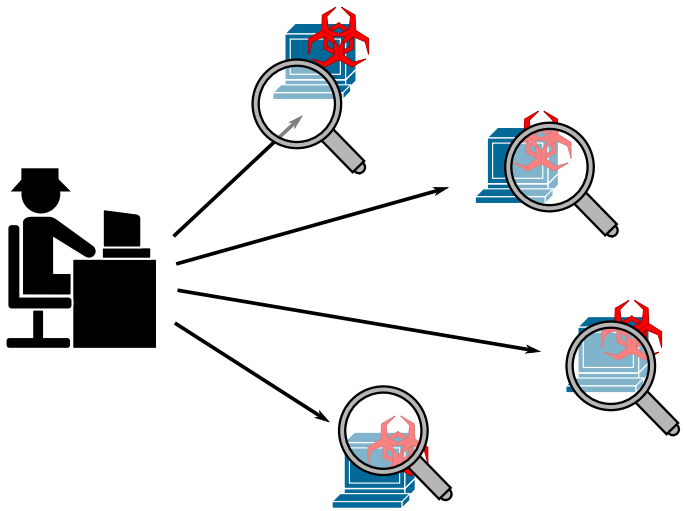
Botnet detection using general-purpose security sensors

Till Elsner

elsner@cs.uni-bonn.de

Fraunhofer FKIE

Botnets



- Network of remotely controllable computers.
- Controlled using (automatically spreading) malware.
- Used to run attacks or steal data from infected computers.

Detection/Monitoring

Detection of malware or unusual host behaviour.
Recognition of known botnet patterns.
Detection of C&C channel.
Reverse engineering.
Enumeration of P2P botnets using active tracking.

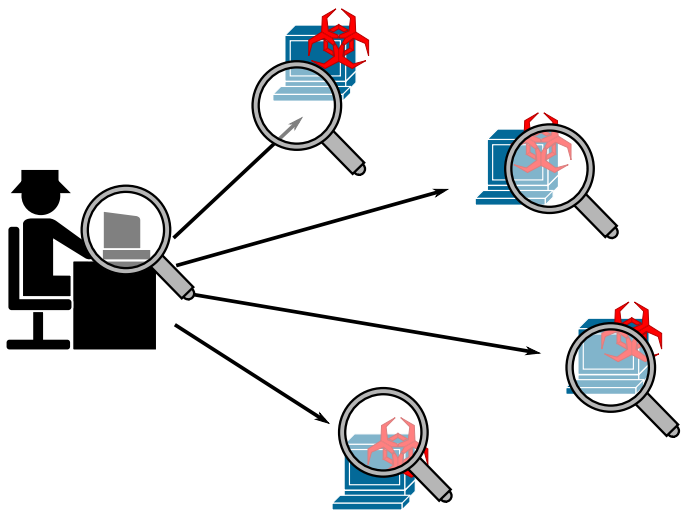
What it's all about

Goal: Distributed botnet detection

- local views provide only limited picture
- insight into private/corporate networks
- behaviour of bots in different locations

Naive Approach

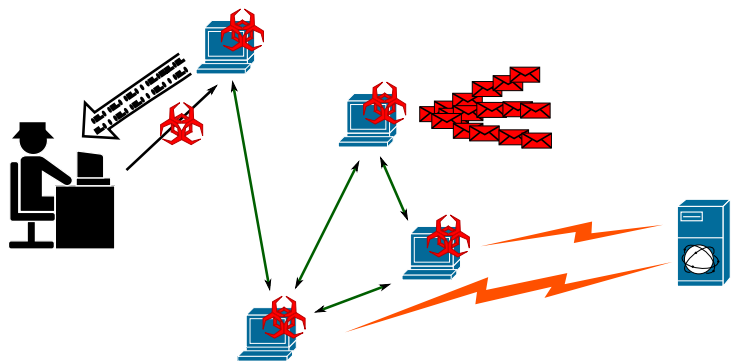
Specific botnet detection sensors are applied at all view points.



Disadvantages:

- Roll-out costs
- Adjustment of every sensor for new botnets
- Difficult inside private/corporate networks

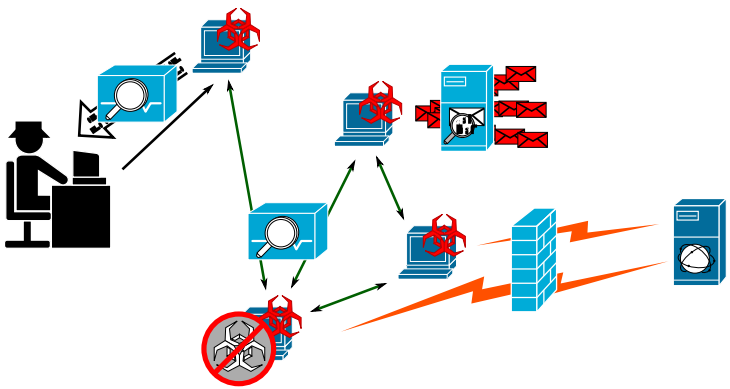
Botnet Structure



A botnet is a
complex network structure

- spanning over administrative and geographical borders
- featuring characteristic attributes such as a C&C infrastructure, epidemic malware infection, coordinated actions etc.

Focus on Characteristic Features

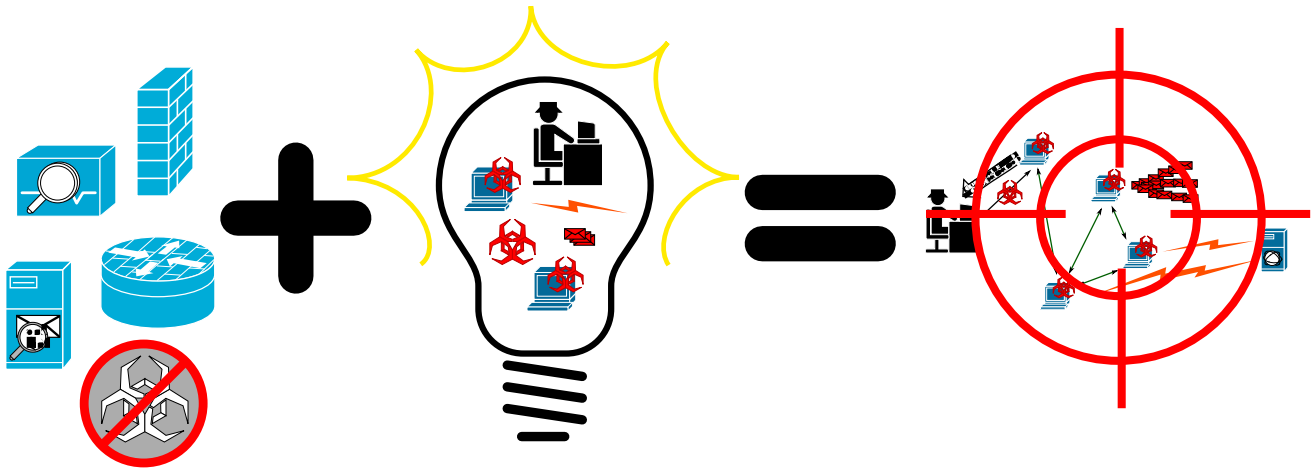


Existing sensors:

- AV detects malware
- IDS detects port scans, break-in attemps
- Firewall detects attacks
- Spam filter detects email campaingn
- ...

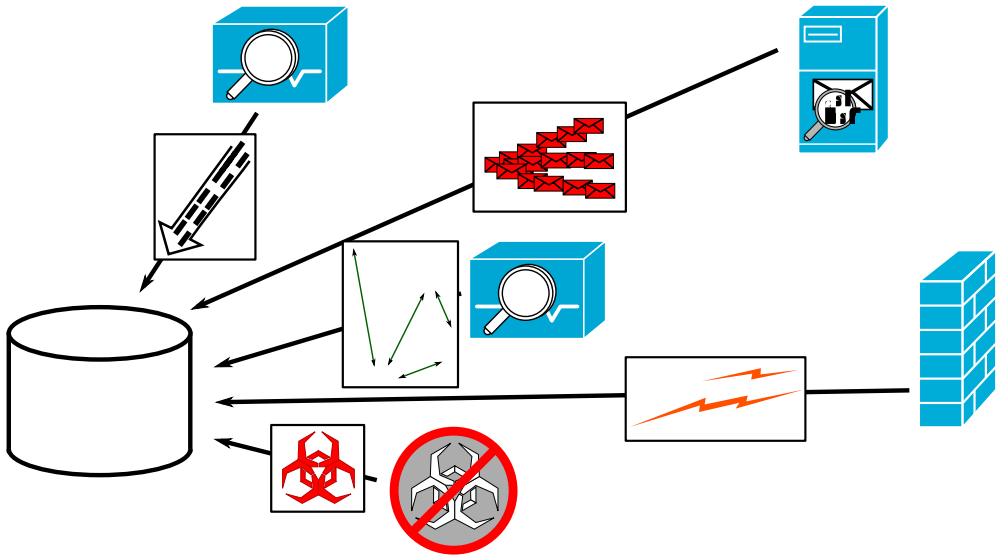
Not botnet-aware!

Our Approach



Fraunhofer FKIE

Accumulation of Security Events



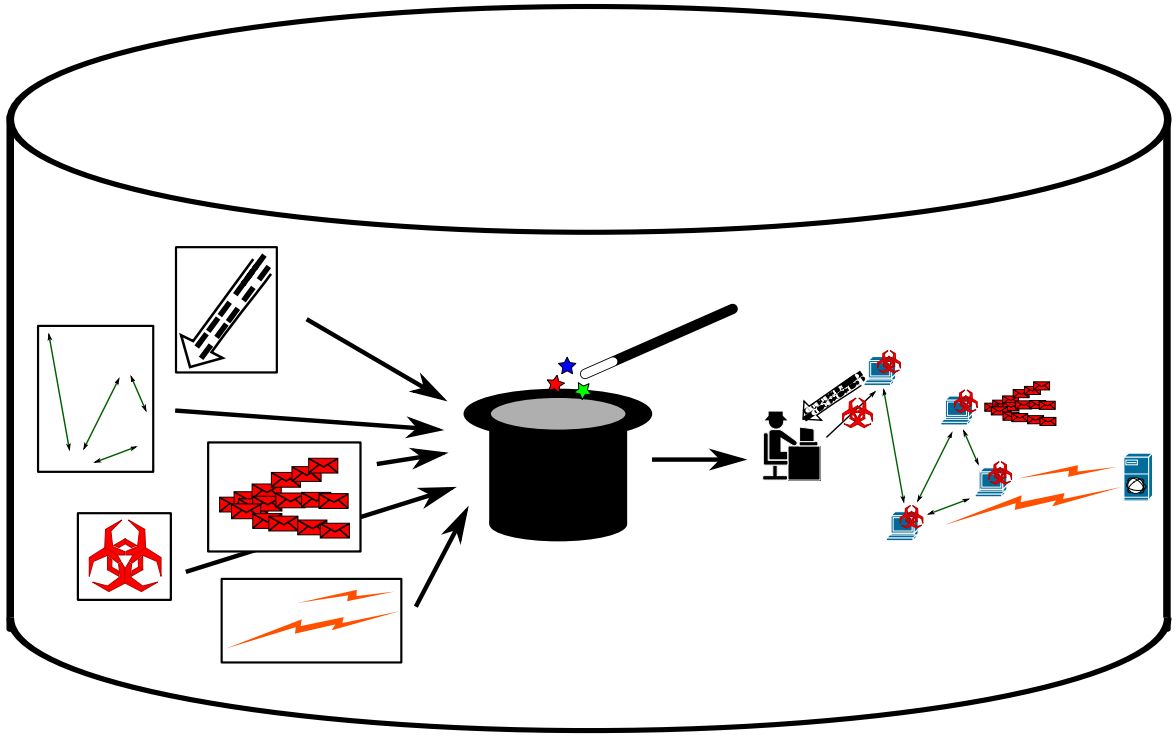
- Single events are just security violations.
- A combination of events may indicate botnet activity.

Requirements

A botnet detection system based on existing sensors must

- integrate into existing network infrastructures
- provide sufficient protection of sensitive data
  - Privacy
  - Confidentiality

Information Fusion



Fraunhofer FKIE

Botnet Detection

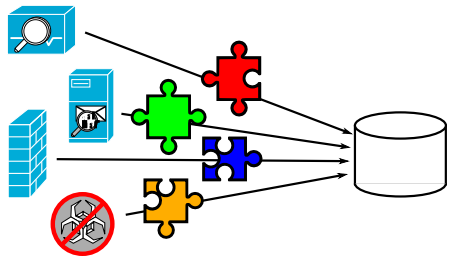
Analysis:

- Recognition of known patterns
- Time-based correlation
- Behaviour-based correlation

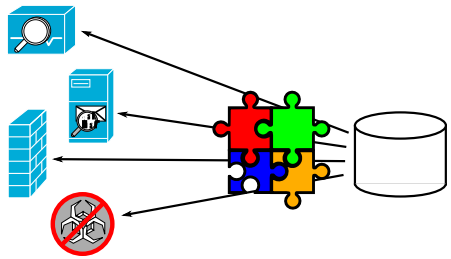
Expected result:

- Identification of clusters of events sharing certain characteristics.
- Classification of clusters as “botnets” with certain likelihood.
- Iterative correlation to increase
  - likelihood of correct classification
  - amount/grade of detail of characteristics

Information Exchange



- Sensor data is provided for central analysis.

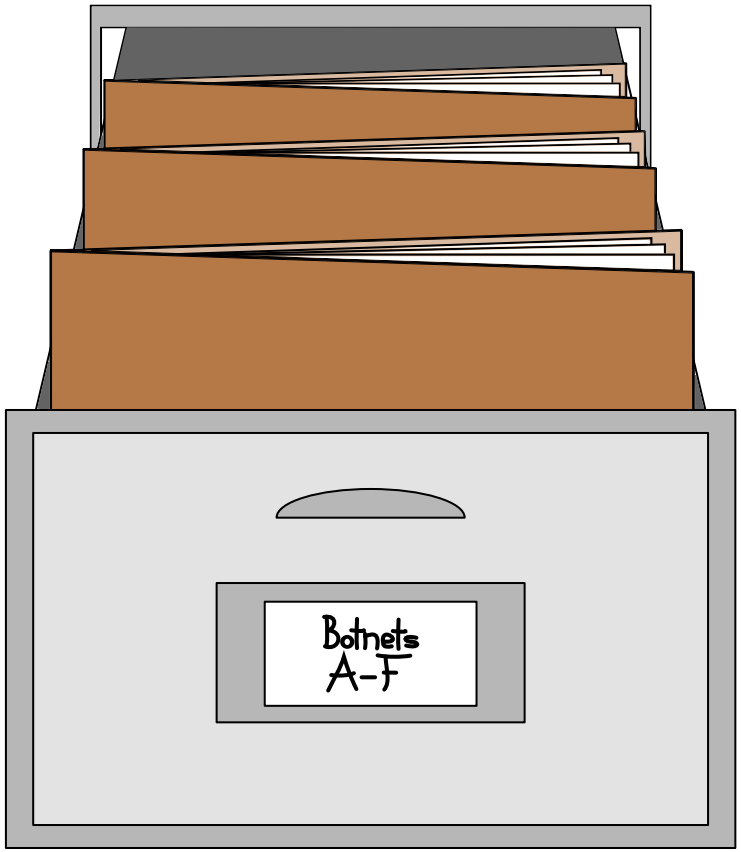


- Results from central analysis are fed back to sensors.

Information Exchange – Example

Sensor	**Anomaly**	**Correlated by**	**Information gain**
Spam filter	spam emails	similar pattern	sender addresses
Mail AV	malware	sender addresses	malware used by botnet
Host AV	malware	botnet malware	more suspicious addresses
IDS	port scans, break-in attempts	suspicious addresses	bot attack vectors
DNS	(queries)	suspicious addresses	domains used by botnet

Knowledge Base



- “Botnet catalog”
- Register
  of suspicious activities
- Access to
  botnet-related events
- Knowledge base
  for botnet research

Fraunhofer FKIE

Advantages

+ Existing sensors: Large database
+ Central analysis logic: Quick and flexible adjustments
+ Information exchange: Threat information flow between different (kinds of) security devices
+ Multi-facet monitoring: Robust against stealth techniques
+ Generic features: Detection of unknown botnets

Thank you for your attention!

Questions?