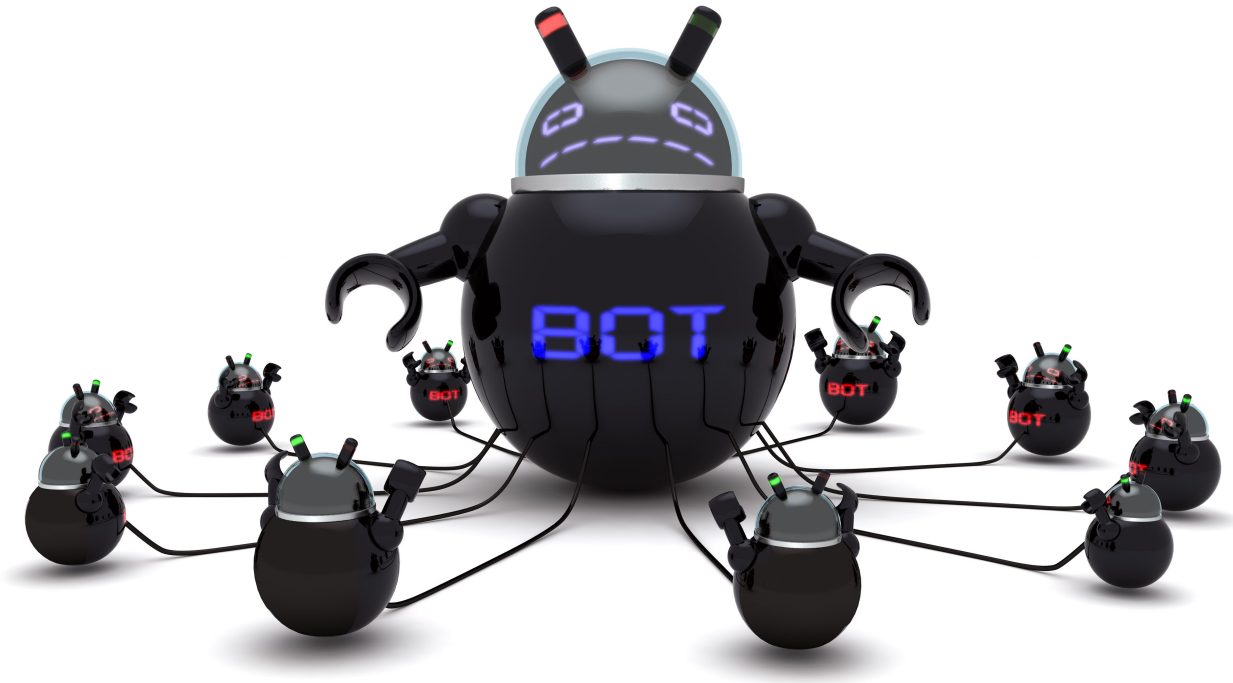
BotWatcher

Transparent and Generic Botnet Tracking

Thomas Barabosch, Adrian Dombeck, Khaled Yakdan, Elmar Gerhards-Padilla
firstname.lastname@fkie.fraunhofer.de
RAID 2015, Kyoto, Japan

Fraunhofer FKIE

Botnets



source: http://core0.staticworld.net/images/article/2013/04/botnet-100034898-orig.jpg

Motivation

- Complexity of botnets is increasing
  - Comprises several MW stages/MW families/malicious actions
- Understanding the botnet ***life-cycle*** is important for further investigations and countermeasures

Related Work

- Botnet Tracking
  - [Caballero2011], [Rossow2011], [Rossow2012], [Rossow2013]
- Botnet Infiltration and Takeover
  - [Kanich2008], [Stone-Gross2009], [Rossow2013]
- Sandboxes
  - Time-based evasion

However, current solutions do not support life-cycle investigations

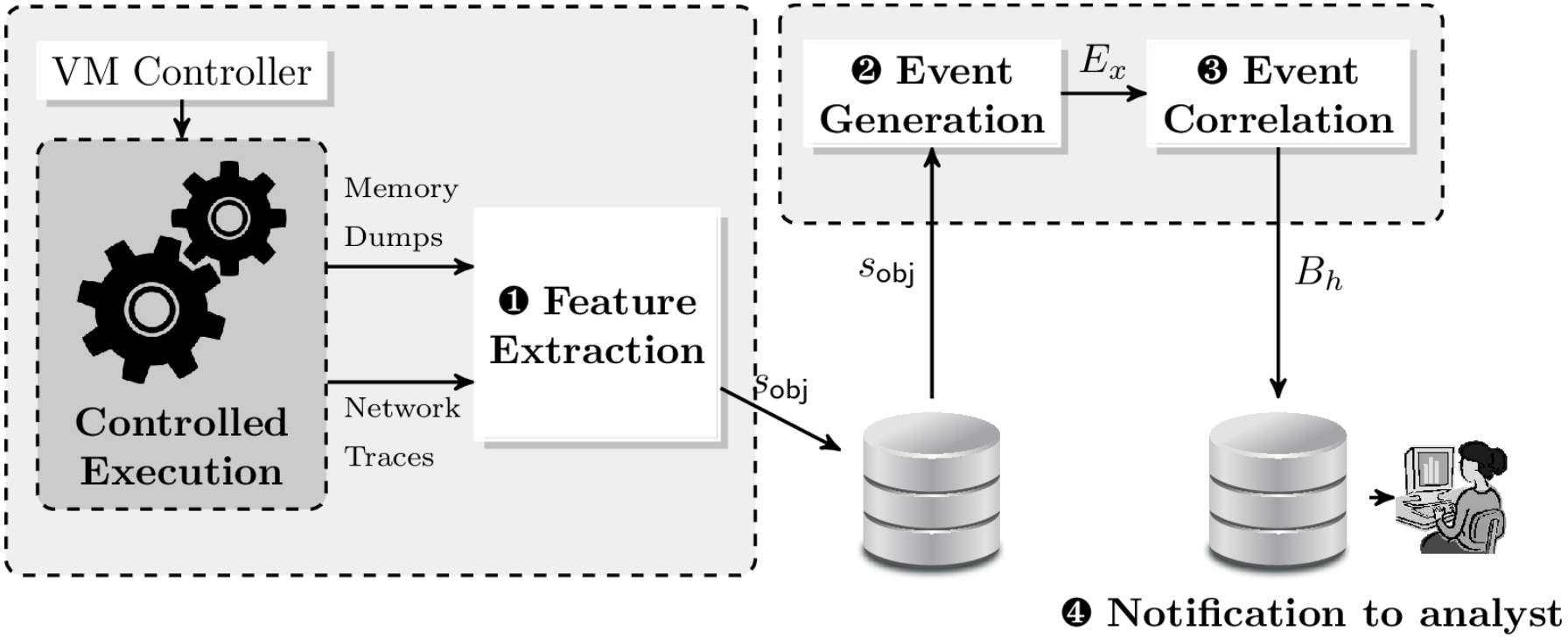
- Lack of ***Genericity*** (no assumptions about malware)
- Lack of ***Transparency*** (hard to detect analysis environment)

Contributions

1. Transparent and generic botnet tracking
2. Inference Rules for reconstructing malicious behavior
3. Evaluation of prototype on Windows and OS X

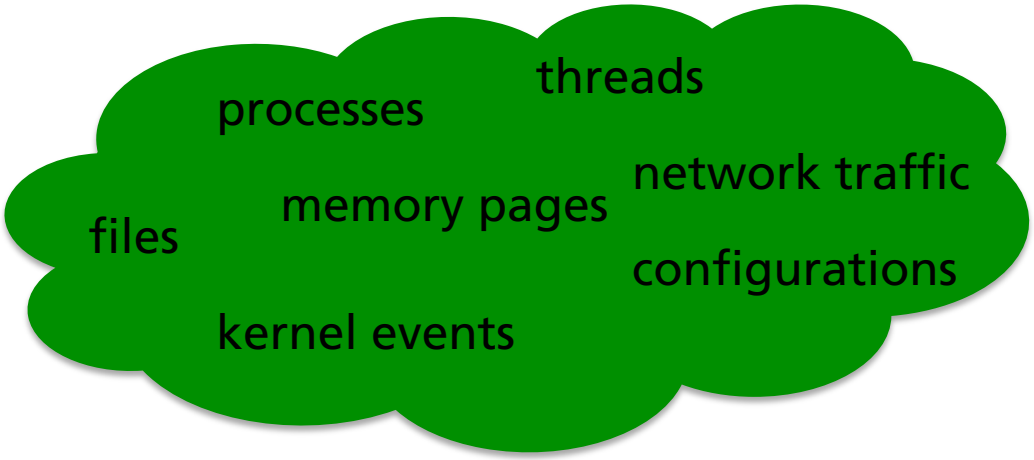
BOTWATCHER

General Overview



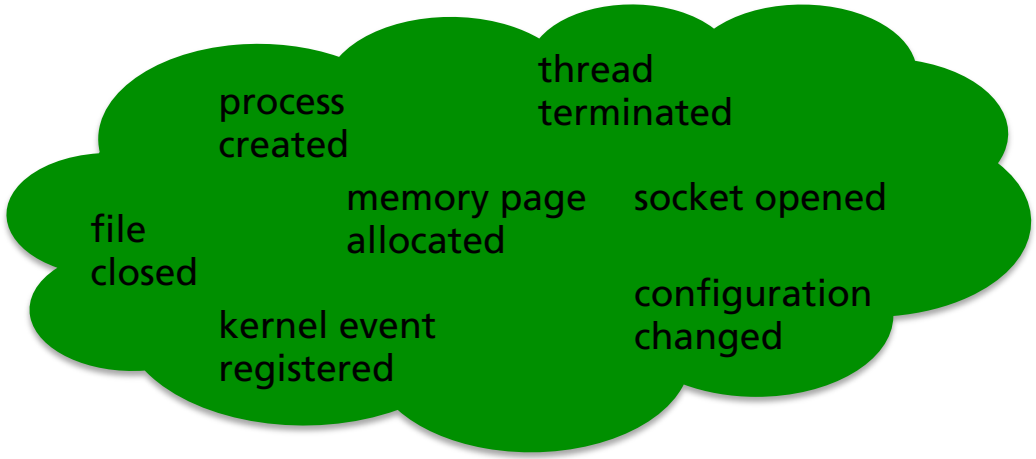
Phase I: Execution Feature Extraction

- Extraction of system state S from outside
- S(t) is described by a set of execution features present at t
- Host-based (memory)
  - Program execution and interaction with OS result in a lot of changes in memory
  - Monitoring allows reconstruction of series of actions that caused changes
- Network-based



Phase II: Execution Event Generation

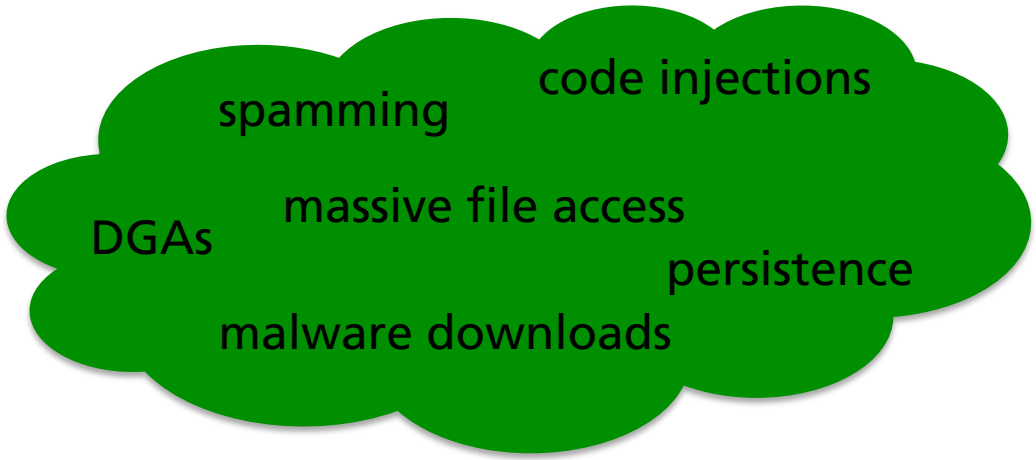
- Comparison of S(t-1) and S(t) for detecting state transitions, i.e. determination of execution events



Phase III: Event Correlation

- Inferring high-level (malicious) behavior from low-level execution events
- Inference rules

$$\frac{P_1 \quad P_2 \quad \ldots \quad P_n}{C}$$



Phase III: Event Correlation

$$\frac{\textsc{Download}[pp_{id}, ts_1] \quad \mathcal{P}\,[p_{id}, pp_{id}, \tau_{\mathbf{create}}, ts_2] \quad ts_2 \geq ts_1}{\textsc{MalwareDownload}\,[p_{id}, ts_2]}$$

$$\frac{\mathcal{N}\,[s, p_{id}, \tau_{\mathbf{start}}, -, ts_1] \quad [s, p_{id}, \tau_{\mathbf{stop}}, -, ts_2] \quad ts_2 \geq ts_1}{\textsc{Download}\,[p_{id}, ts_2]}$$

EVALUATION

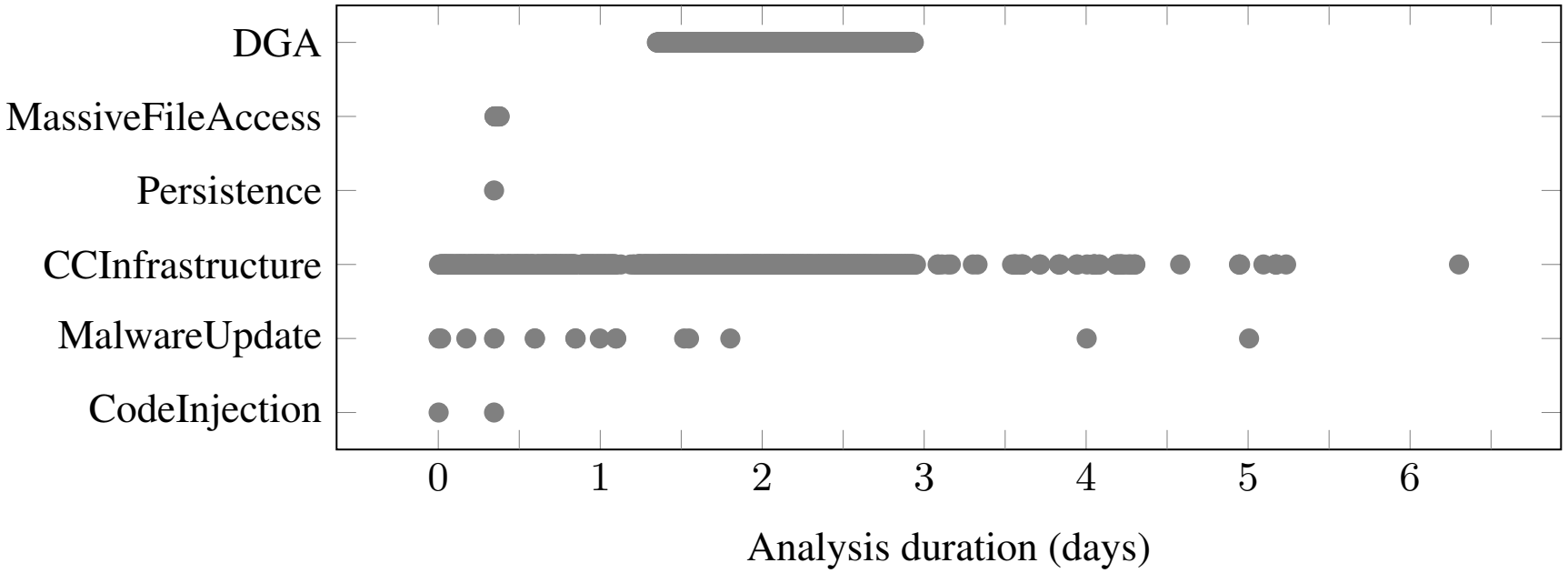
Case Studies

- Prototype
  - VirtualBox, Volatility and Bro
- Microsoft Windows XP and 8 32 bits 
  - **Upatre**, **Emotet**, Gamarue, Necurs
- Mac OS X Mavericks 64 bits 
  - VidInstaller
- Duration up to one week

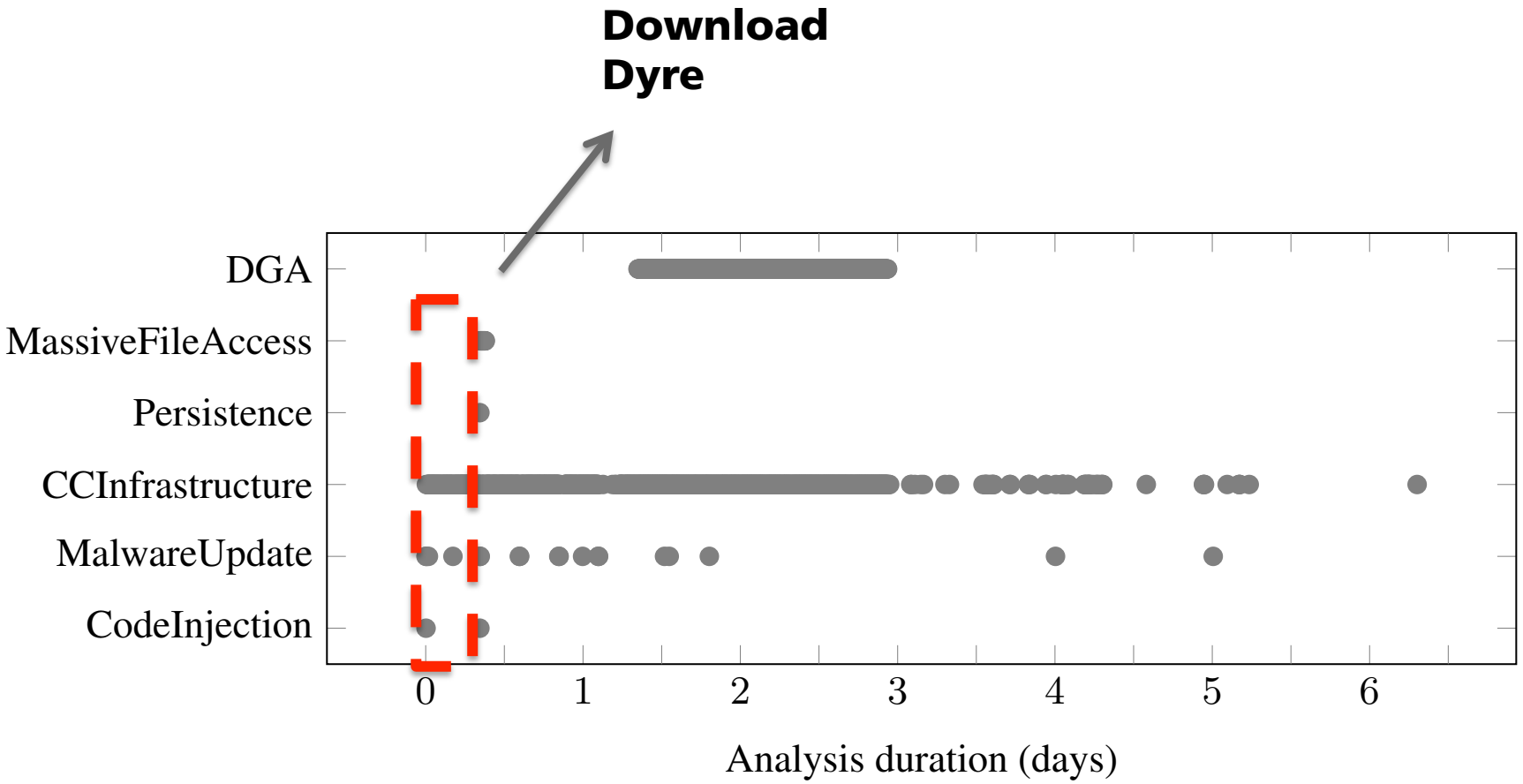
Case Study Upatre: Introduction

- Very small dropper
  - Entrypoint to complexer botnet infrastructures
  - In this case: Kegotip, Pushdo and Dyre
- Tracking period: 2015-01-15 – 2015-01-22

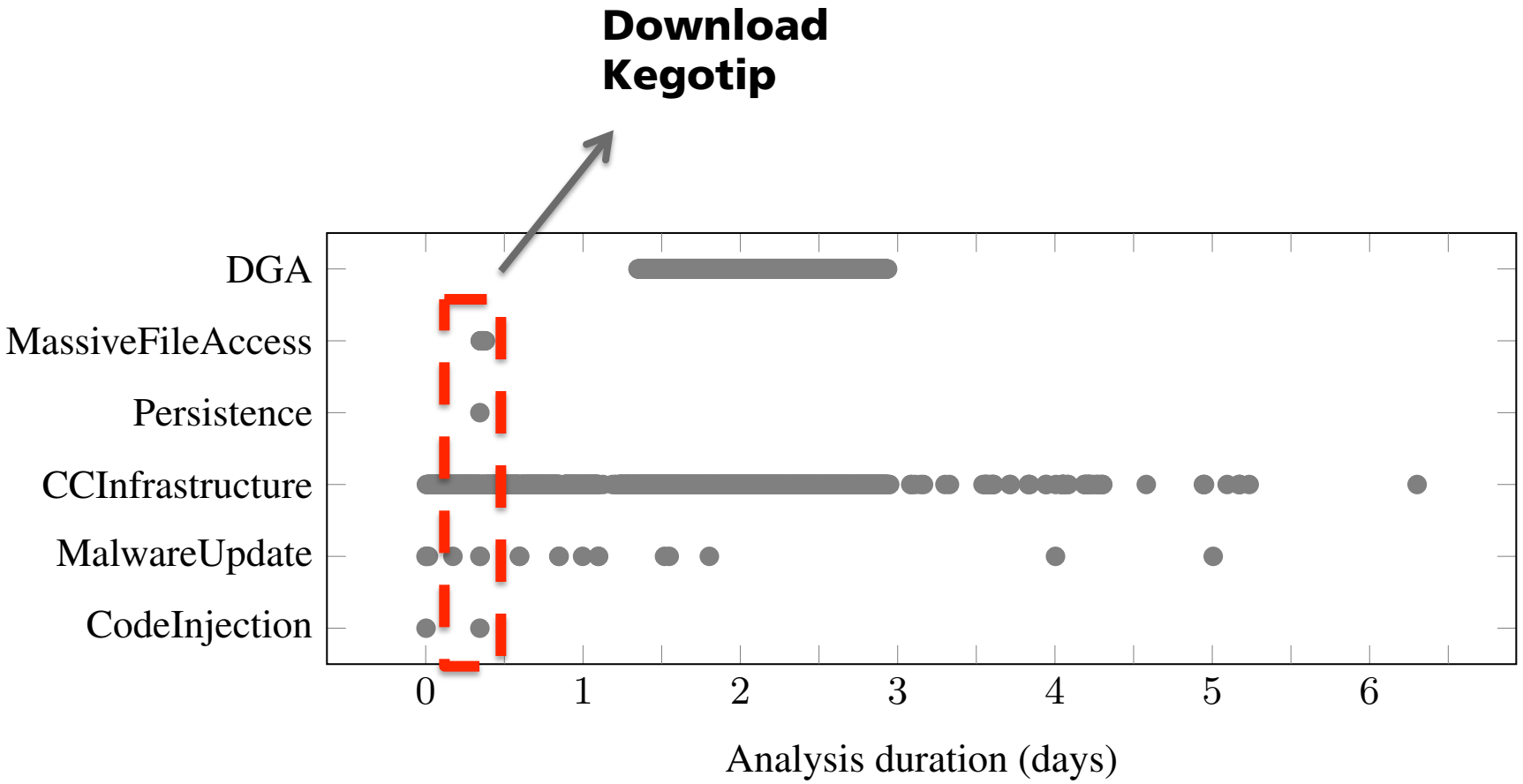
Case Study Upatre: Results



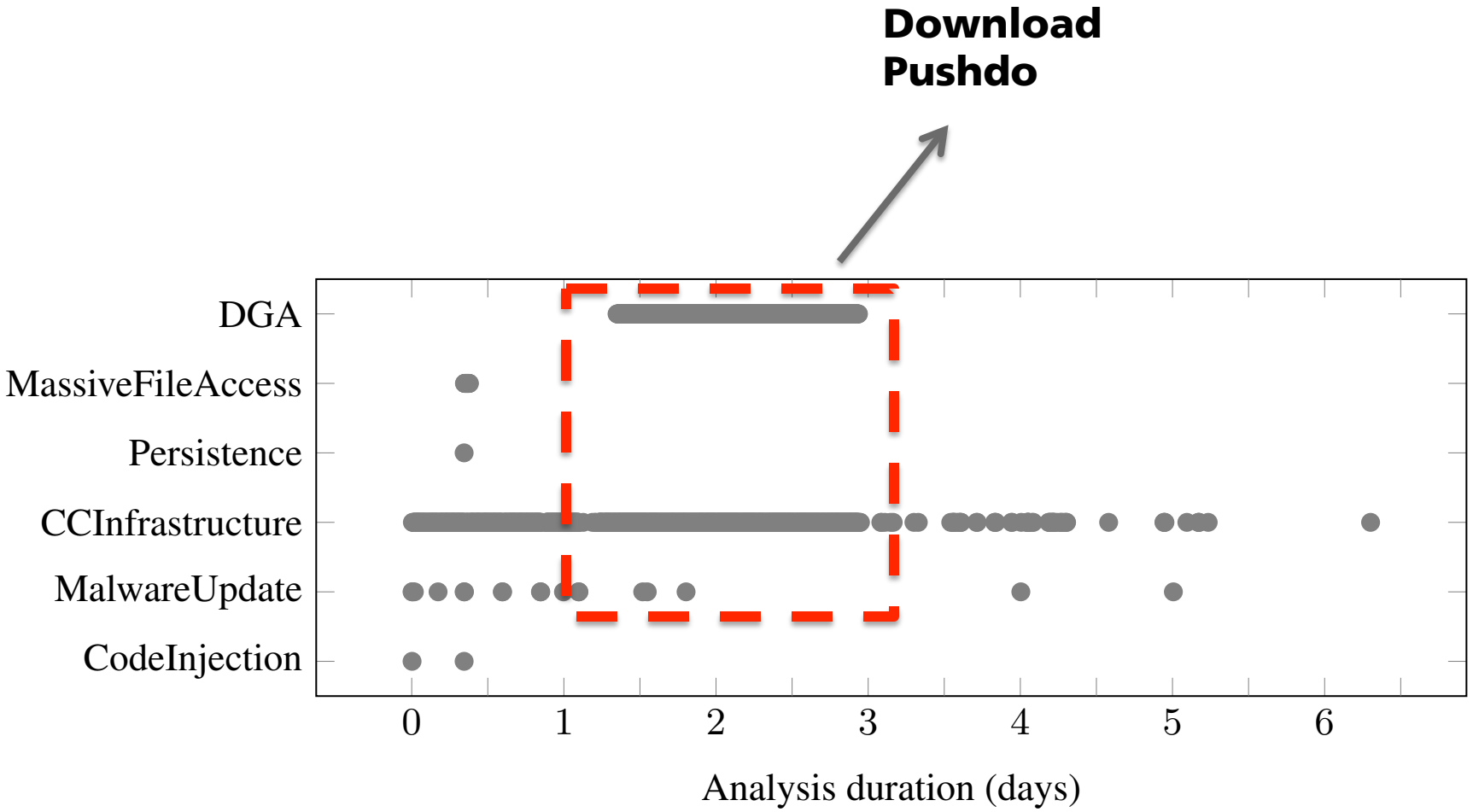
Case Study Upatre: Results



Case Study Upatre: Results

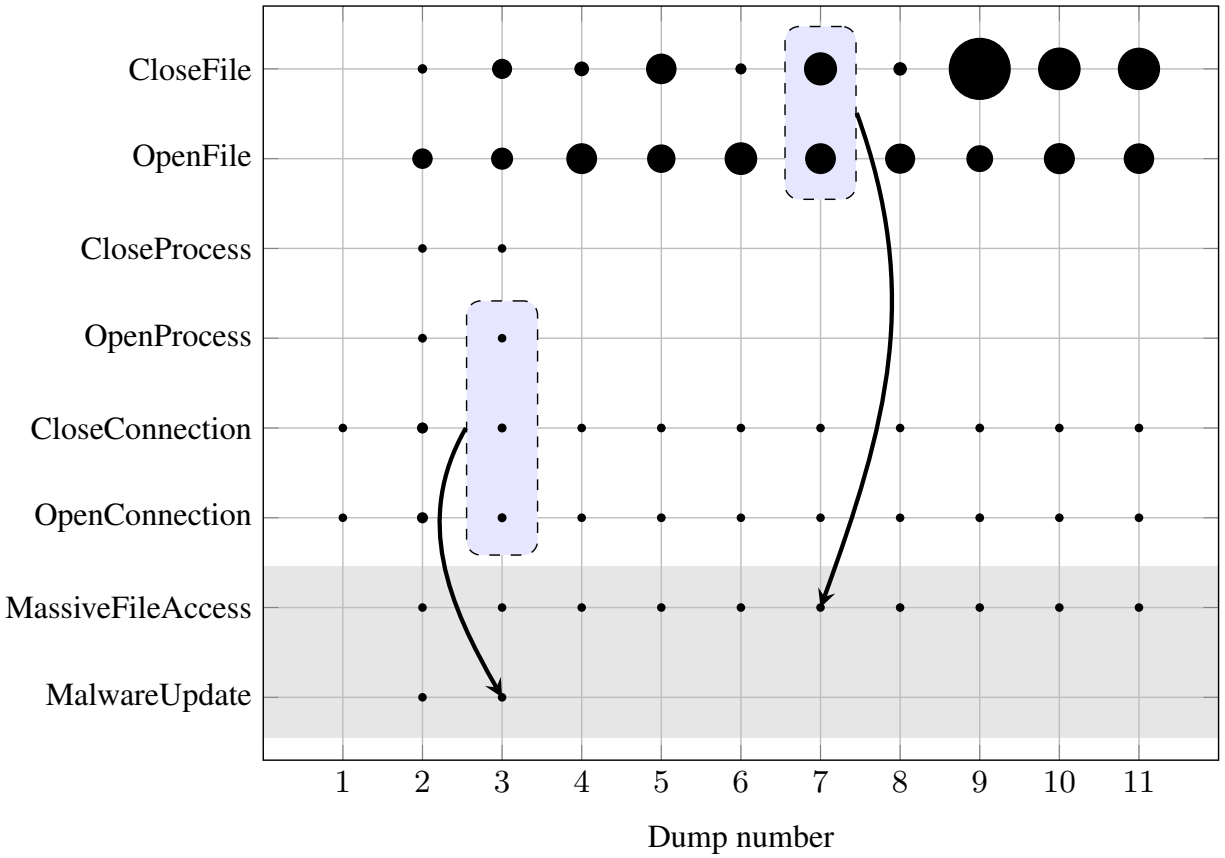


Case Study Upatre: Results



Fraunhofer FKIE

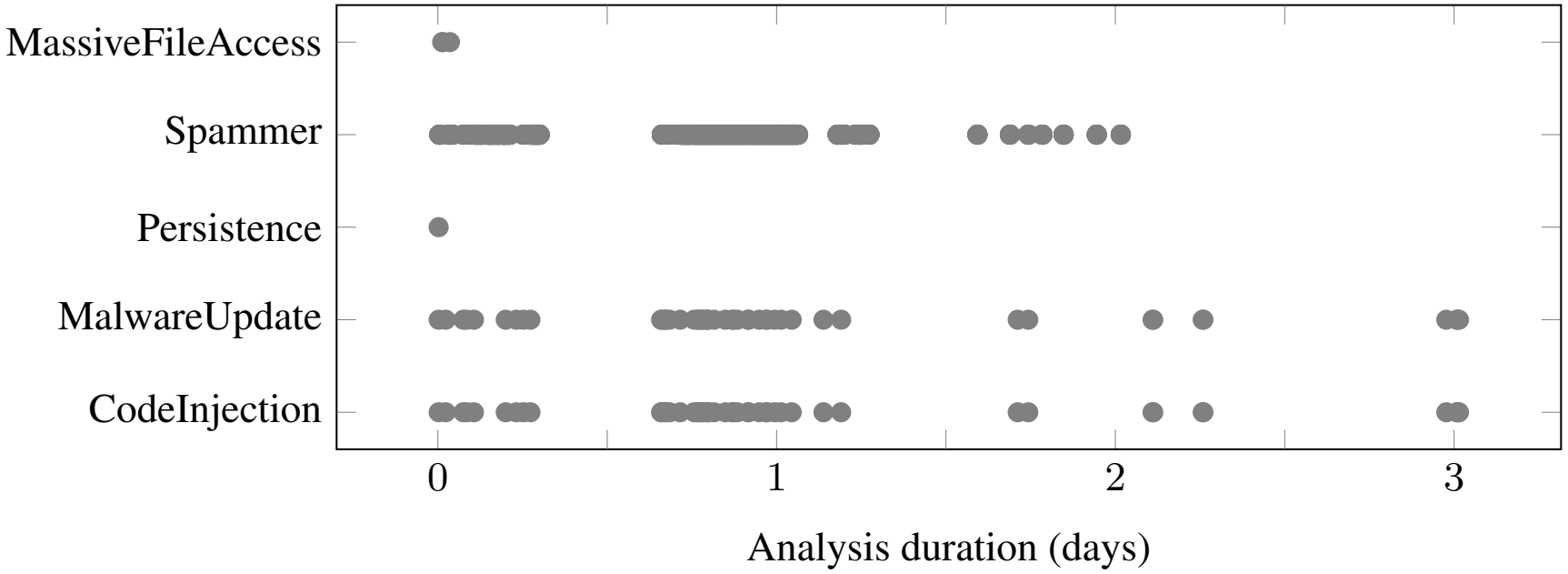
Case Study Upatre: Results (Kegotip Download)



Case Study Emotet: Introduction

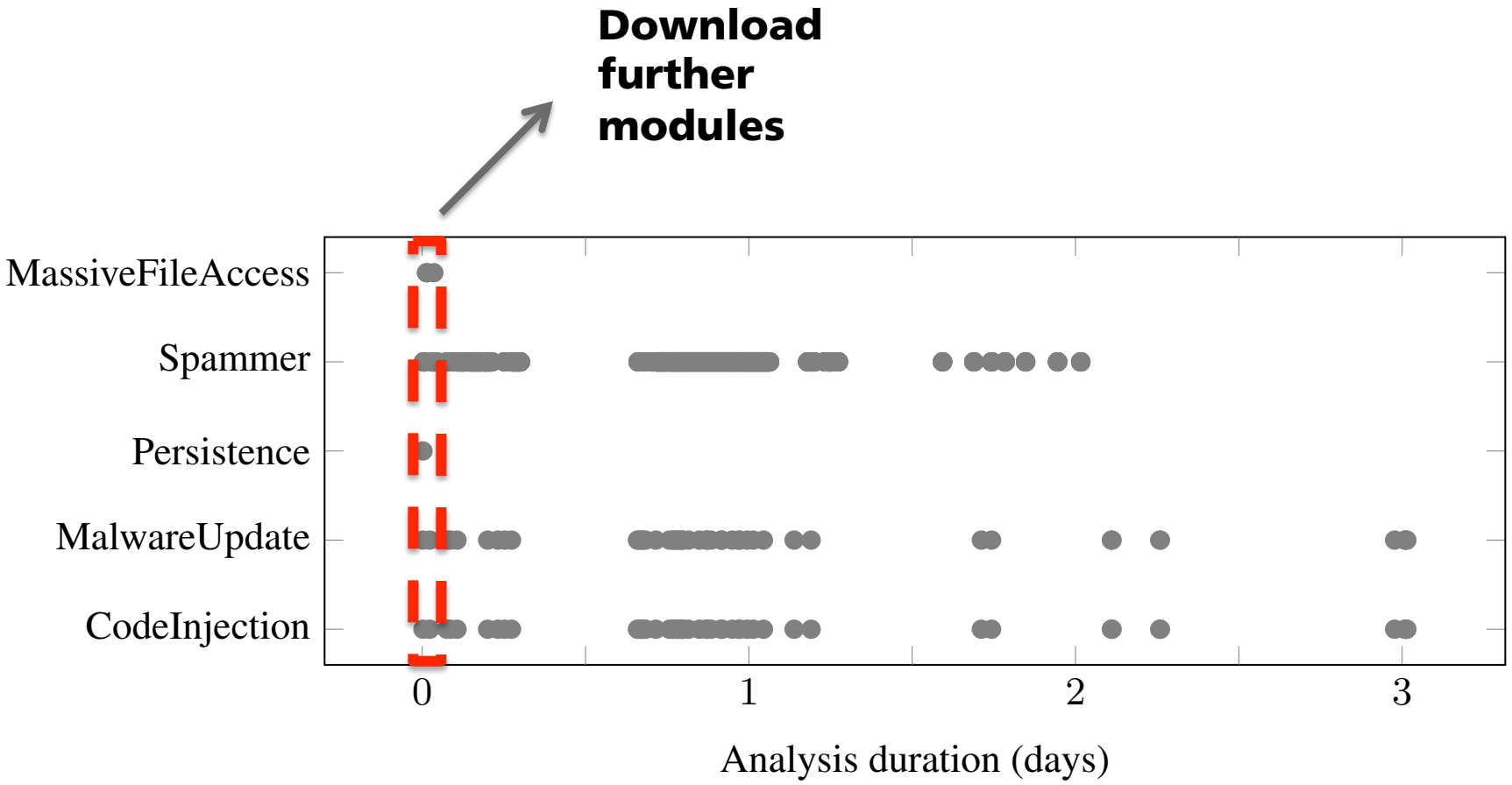
- Modular botnet
  - Feodo, Geodo, Cridex, Dridex, …
- Several modules
  - Dropper, spammer, grabber, …
- Tracking period: 2015-05-19 – 2015-05-22

Case Study Emotet: Results

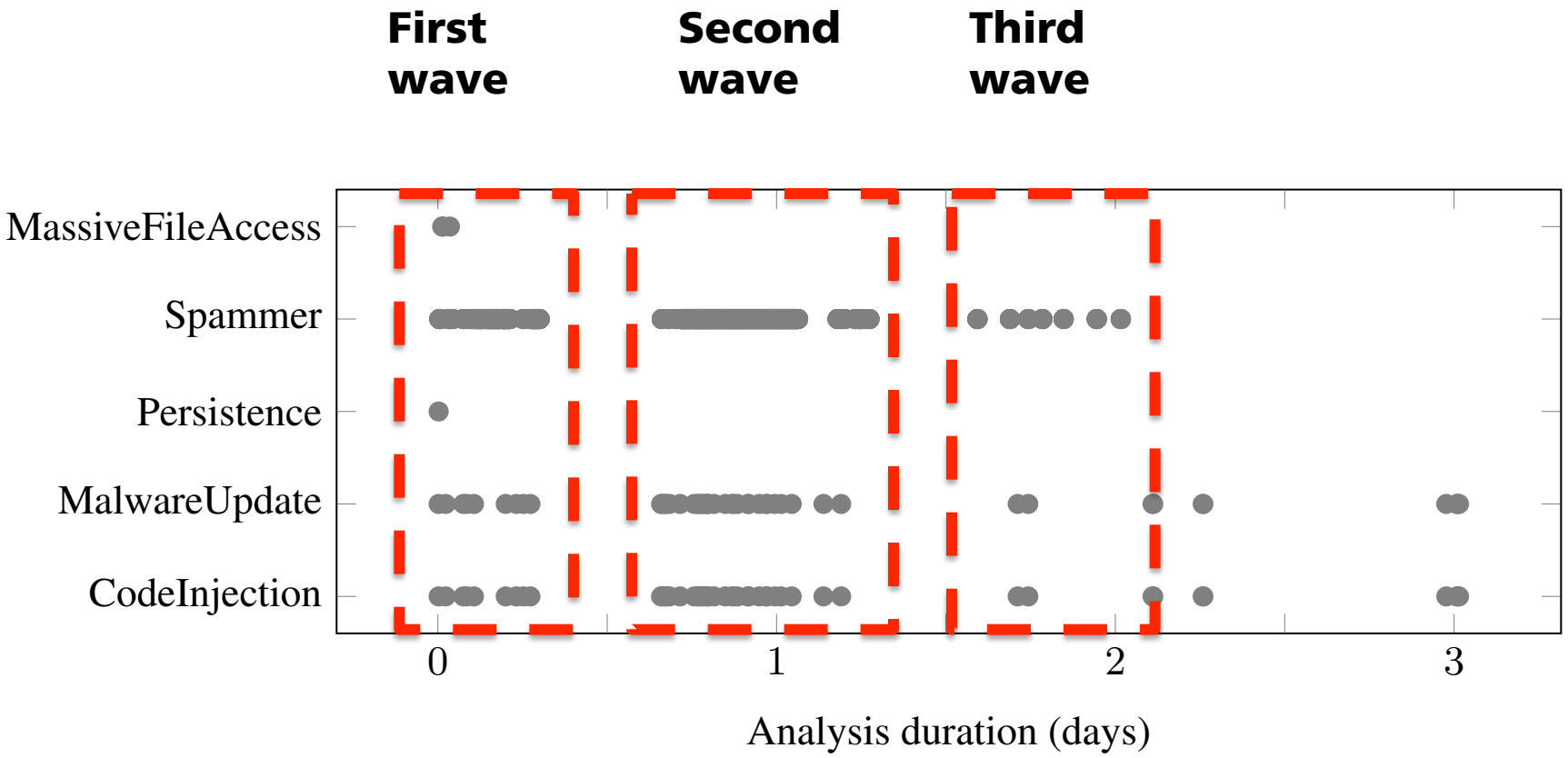


Fraunhofer FKIE

Case Study Emotet: Results



Case Study Emotet: Results



Discussion of Evaluation

- Threw light on several botnets
  - Detected several malicious actions
  - Intercepted MW updates and new MW downloads
  - Witnesses phases of botnet activity
- Gives malware analyst further pointers
- Circumvented time-based evasion techniques
  - Client-side and server-side

Limitations

- Memory dump frequency
  - Evaluate thoroughly intervals between two dumps
- Analysis environment detection
  - Possible solution: make it run on bare-metal

CONCLUSION & FUTURE WORK

Conclusion & Future Work

- Transparent and generic botnet tracking
  - Outside view of analysis system
  - Inference rules reconstructing malicious behavior
  - Platform-independent
- Future work
  - Perform long-term analysis
  - Extend inference rule set
  - Improve behavior attribution for multiple malwares on the machine

JAPAN IN BONN/GERMANY …

source: https://drscdn.500px.org/photo/66124681/m%3D2048/56532151378f51a812301477e2c86a0b