Malware Incident Response in IoT

Presented by
Ahmed Lekssays

Supervised by
Prof. Elena Ferrari and Prof. Barbara Carminati

Motivation

- Kaspersky detected more than **2 billion attacks** targeting more than **100k users** around the world in the first quarter of 2021[1].
- **37% of organizations** worldwide were hit by a ransomware attack in 2021[2].
- There were **236 million ransomware attacks** in the first half of 2022[3].
- IoT malware were used in large Distributed Denial of Service attacks that stopped giant companies' services for hours[4].
- IoT devices worldwide are projected to reach **30.9 billion units by 2025**[5].

[1] https://securelist.com/it-threat-evolution-q1-2021-non-mobile-statistics/102425/

[2] https://www.statista.com/statistics/1246438/ransomware-attacks-by-country/

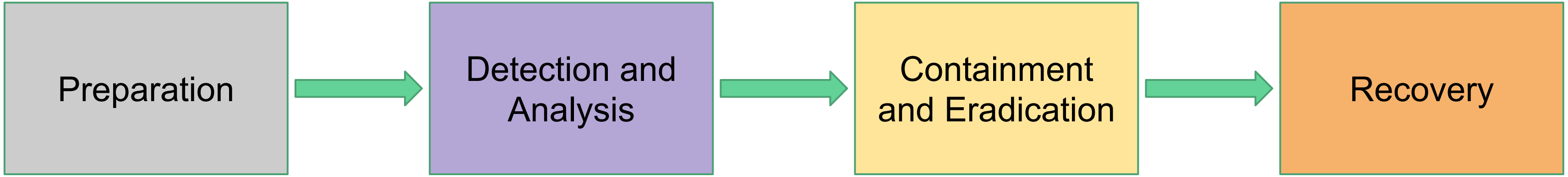
[3] https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

[4] https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

[5] https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

Our Research

- NIST has introduced a set of **guidelines (NIST SP 800-83)** to follow in case of malware attacks incidents.
- NIST SP 800-83 has four steps:
  - **Preparation** is about preparing employees to handle malware attacks by training them and raising awareness about such attacks.
  - **Detection and Analysis** is about detecting the malware through its behavior and analyzing its weaknesses.
  - **Containment and Eradication** is about isolating the malware to limit the spread and use the weaknesses to eradicate it.
  - **Recovery** is about helping devices recover to normal operation (e.g., recovering the data).



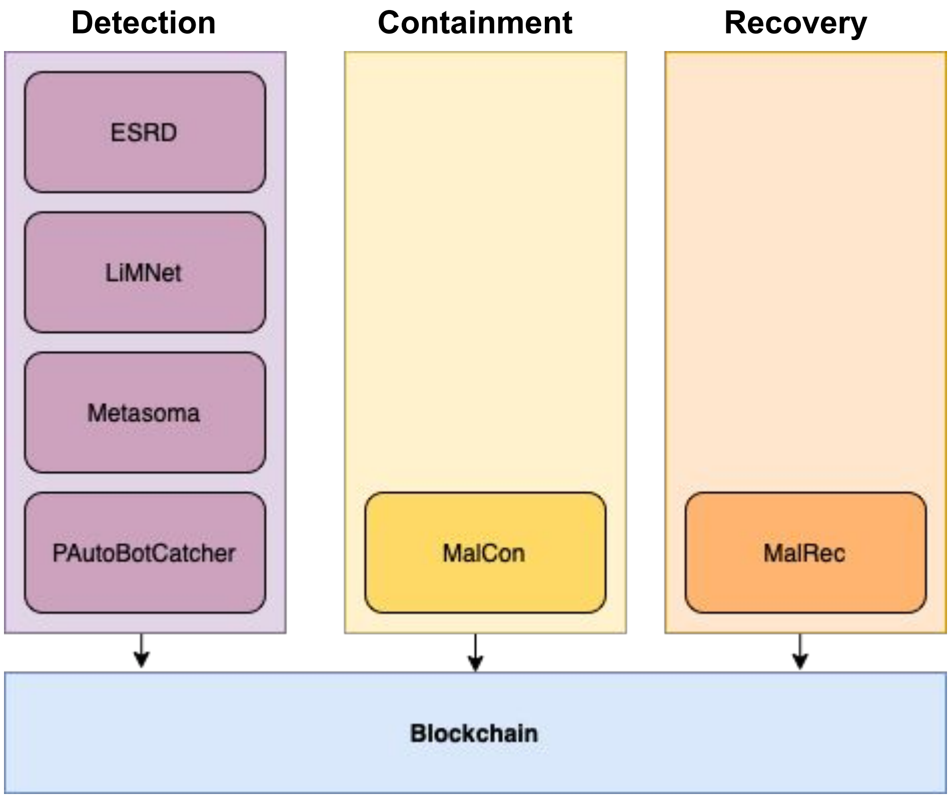
Preparation

Detection and Analysis

Containment and Eradication

Recovery

Our Research (Cont’d)



Lekssays, A., Landa, L., Carminati, B., & Ferrari, E. (2021). **PAutoBotCatcher**: A blockchain-based privacy-preserving botnet detector for Internet of Things. **Computer Networks journal,**, 108512.

Giaretta, L., **Lekssays, A.**, Carminati, B., Ferrari, E., & Girdzijauskas, Š. (2021, October). **LiMNet**: Early-Stage Detection of IoT Botnets with Lightweight Memory Networks. In European Symposium on Research in Computer Security (ESORICS) (pp. 605-625). Springer, Cham.

Lekssays A., Giaretta L., Carminati B., Ferrari E., & Girdzijauskas, Š.: "**Metasoma**: Decentralized and Collaborative Early-Stage Detection of IoT Botnets" ***(under submission, NDSS 23)***

Lekssays A., Coglio F., Carminati B., Ferrari E., & Girdzijauskas, Š.: "**ESRD**: Early-stage Ransomware Detection using Artificial Neural Networks" ***(under preparation)***

Lekssays A., Carminati B., Ferrari E.: "MalCon: A Blockchain-based Malware Containment Framework for IoT" ***(under submission, Computer Networks Journal)***

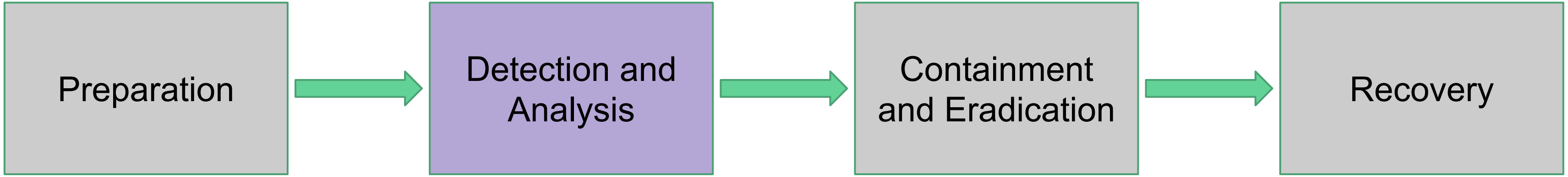
Lekssays A,, Sirigu, G., Carminati, B., & Ferrari, E. (2022, August). MalRec: A Blockchain-based Malware Recovery Framework for Internet of Things. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-8).

Our Research (Cont’d)

- **ESRD**[1] detects ransomware based on their interactions with the kernel through API calls.
- **PAutoBotCatcher**[2] collaboratively detects botnets by leveraging community behavior analysis and blockchain to address trust among devices.

[1] **Lekssays, A.**, Landa, L., Carminati, B., & Ferrari, E. (2021). **PAutoBotCatcher**: A blockchain-based privacy-preserving botnet detector for Internet of Things. **Computer Networks journal,**, 108512.

[2] **Lekssays A**., Coglio F., Carminati B., Ferrari E., & Girdzijauskas, Š.: "**ESRD**: Early-stage Ransomware Detection using Artificial Neural Networks" ***(under preparation)***



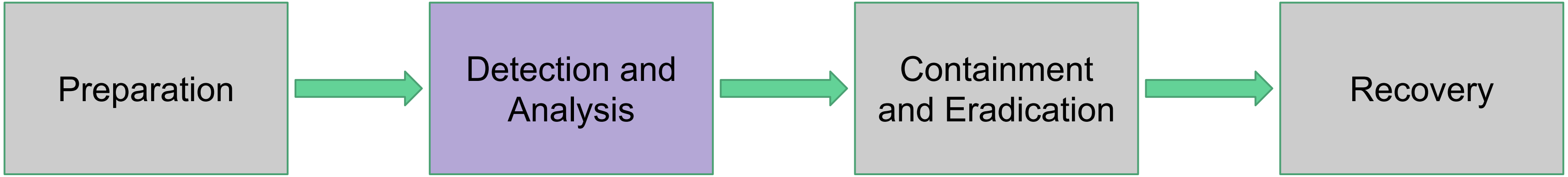
Preparation → Detection and Analysis → Containment and Eradication → Recovery

Our Research (Cont’d)

- **LiMNet**[3] classifies malicious devices and malicious network packets by leveraging Lightweight Memory Networks.
- **Metasoma**[4] is a decentralized version of LiMNet that detects botnets by gossiping memories.

[3] Giaretta, L., **Lekssays, A.**, Carminati, B., Ferrari, E., & Girdzijauskas, Š. (2021, October). **LiMNet**: Early-Stage Detection of IoT Botnets with Lightweight Memory Networks. In European Symposium on Research in Computer Security (ESORICS) (pp. 605-625). Springer, Cham.

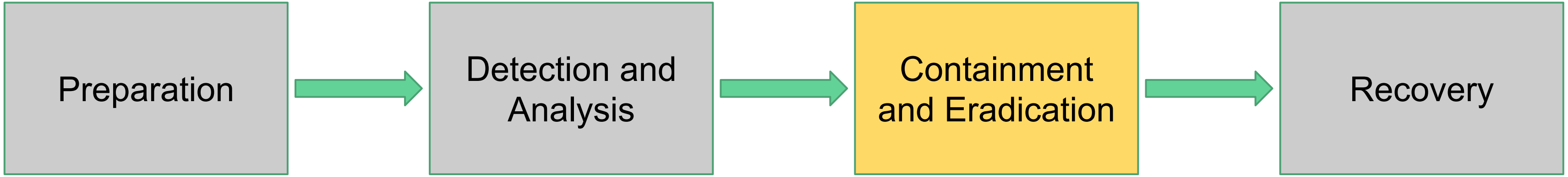
[4] **Lekssays A**., Giaretta L., Carminati B., Ferrari E., & Girdzijauskas, Š.: "**Metasoma**: Decentralized and Collaborative Early-Stage Detection of IoT Botnets" ***(under submission, NDSS 23)***



Our Research (Cont'd)

- **MalCon**[5] aims to contain malware propagation in networks leveraing blockchain's smart contracts on three steps: emergency, healing, and punishment.

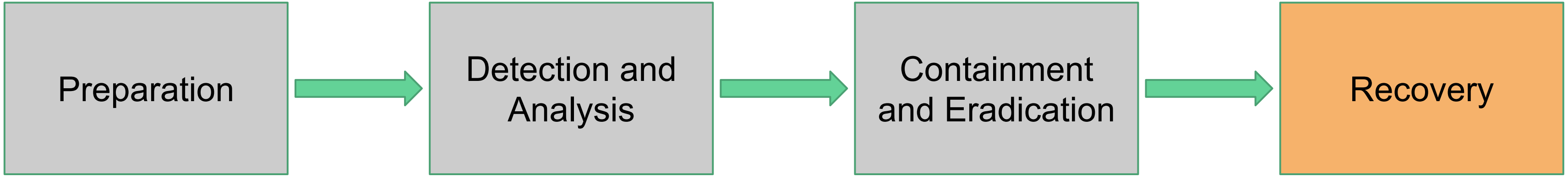
[5] **Lekssays A**., Carminati B., Ferrari E.: "MalCon: A Blockchain-based Malware Containment Framework for IoT" ***(under submission, Computer Networks Journal)***



Our Research (Cont’d)

- **MalRec**[6] aims to make devices able to recover their files through continuous backups using blockchain to store files' metadata and IPFS to store encrypted files.

[6] **Lekssays A,**, Sirigu, G., Carminati, B., & Ferrari, E. (2022, August). MalRec: A Blockchain-based Malware Recovery Framework for Internet of Things. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-8).



Preparation

Detection and Analysis

Containment and Eradication

Recovery

References

Lekssays, A., Landa, L., Carminati, B., & Ferrari, E. (2021). **PAutoBotCatcher**: A blockchain-based privacy-preserving botnet detector for Internet of Things. **Computer Networks journal,**, 108512.

Giaretta, L., **Lekssays, A.**, Carminati, B., Ferrari, E., & Girdzijauskas, Š. (2021, October). **LiMNet**: Early-Stage Detection of IoT Botnets with Lightweight Memory Networks. In European Symposium on Research in Computer Security (ESORICS) (pp. 605-625). Springer, Cham.

Lekssays A., Giaretta L., Carminati B., Ferrari E., & Girdzijauskas, Š.: "**Metasoma**: Decentralized and Collaborative Early-Stage Detection of IoT Botnets" ***(under submission, NDSS 23)***

Lekssays A., Coglio F., Carminati B., Ferrari E., & Girdzijauskas, Š.: "**ESRD**: Early-stage Ransomware Detection using Artificial Neural Networks" ***(under preparation)***

Lekssays A., Carminati B., Ferrari E.: "MalCon: A Blockchain-based Malware Containment Framework for IoT" ***(under submission, Computer Networks Journal)***

Lekssays A,, Sirigu, G., Carminati, B., & Ferrari, E. (2022, August). MalRec: A Blockchain-based Malware Recovery Framework for Internet of Things. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-8).