THE CIRCLE OF LIFE: A LARGE-SCALE STUDY OF THE IOT MALWARE LIFECYCLE

Omar Alrawi, Charles Lever, Kevin Valakuzhy, Ryan Court, Kevin Snow, Fabian Monrose, Manos Antonakakis

Published in 2021

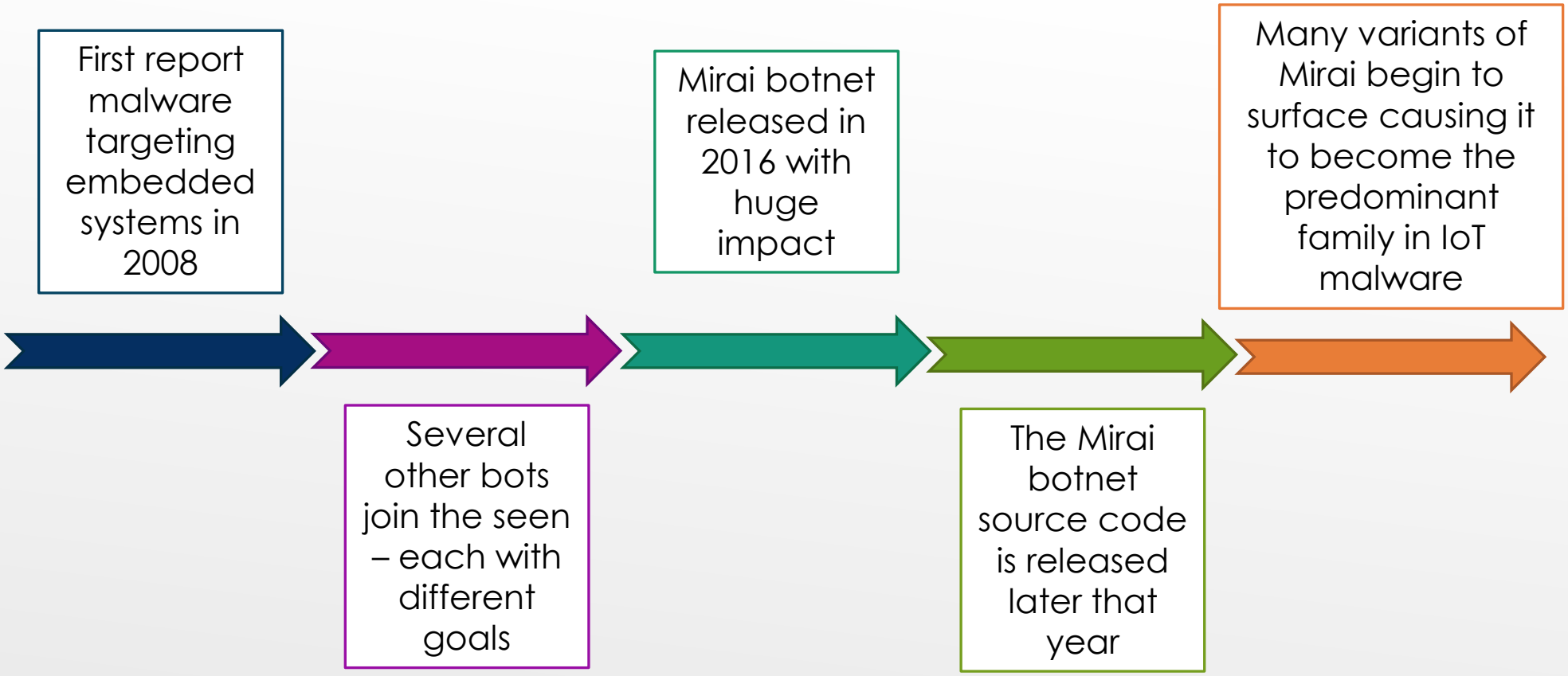
By Gemma Lowe

INTRODUCTION

- Research Questions:
  - How is IoT malware different from traditional malware?
  - And are current antimalware techniques effective against IoT malware?
- Embedded IoT Technology
- Mirai Malware

OVERVIEW

- Introduction
- Background
- Current Research
- Papers Contributions
- Experimental Setup
  - Comparative Framework
  - Static Analysis
  - Dynamic Analysis
  - Infrastructure Analysis
- Measurement Results
  - Detection & Labelling
  - Infection Analysis
  - Payload Analysis
  - Persistence Analysis
  - Capability Analysis
  - C&C Analysis
- Summary and Discussion
  - Conclusion
  - Criticism
  - Questions?


First report malware targeting embedded systems in 2008
Several other bots join the seen – each with different goals
Mirai botnet released in 2016 with huge impact
The Mirai botnet source code is released later that year
Many variants of Mirai begin to surface causing it to become the predominant family in IoT malware

BACKGROUND

CURRENT RESEARCH

- IoT Malware research
  - In-depth analysis of a single family
  - Have small sample size
- Threat frameworks
  - Too complex
  - Heavy focus on traditional malware
  - Heavy focus on infection stages

THIS PAPER MAKES THE FOLLOWING CONTRIBUTIONS:

Five layer novel analysis framework to capture the IoT malware lifecycle

Systemise 25 papers that study traditional malware utilising the framework

Characterise IoT malware utilising a large corpora

Made available the largest and most comprehensive IoT malware corpus to date

EXPERIMENTAL SETUP

COMPARATIVE FRAMEWORK

Infection Vector
Remote Exploit
Default Credentials

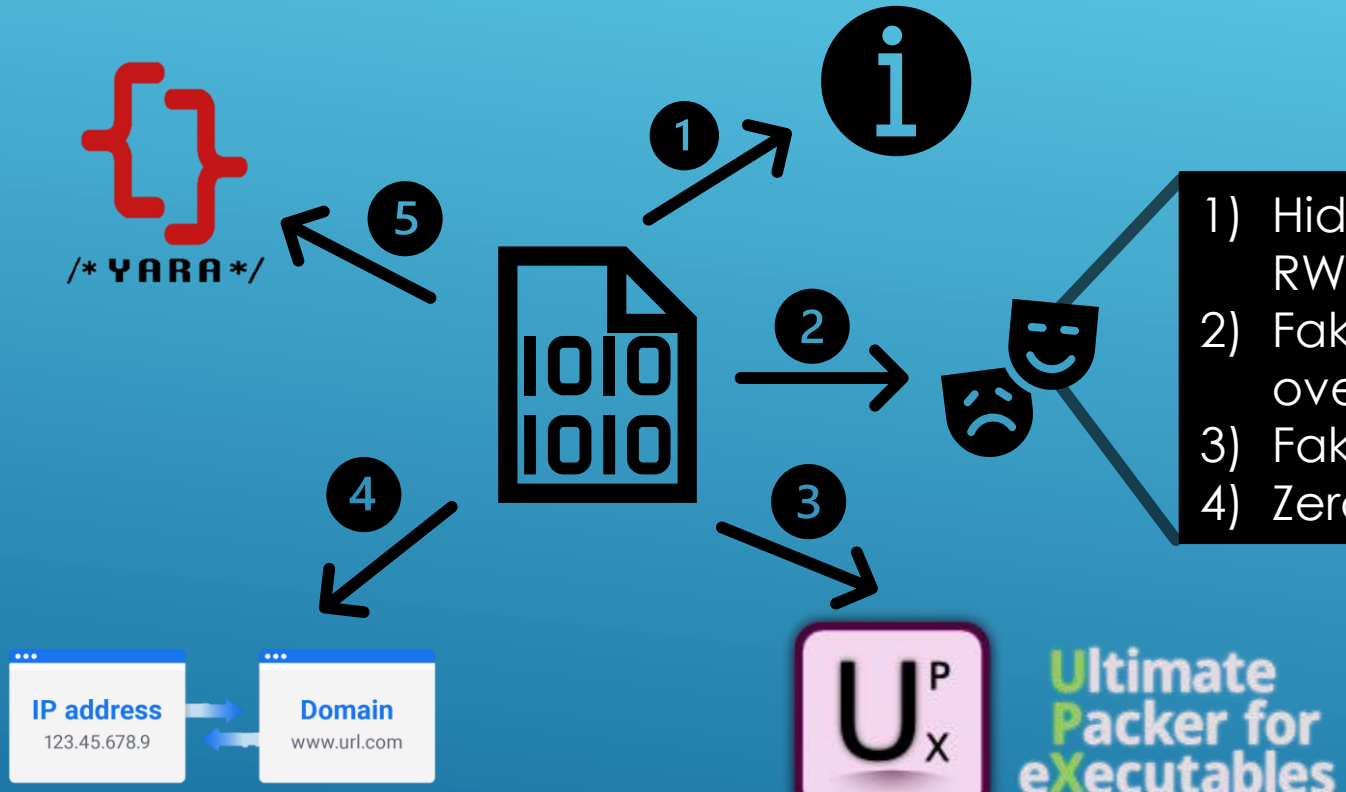
Payload
Packing
Environment Keying
Scripting
Cross Arch/Plat.

Persistence
Firmware
OS – Kernel
OS - User

Capability
Priv. Escalation
Defence Evasion
Info. Theft
Scanning
DDoS
Destruction
Resource Abuse

Command and Control
Peer-2-Peer
Centralised

STATIC ANALYSIS



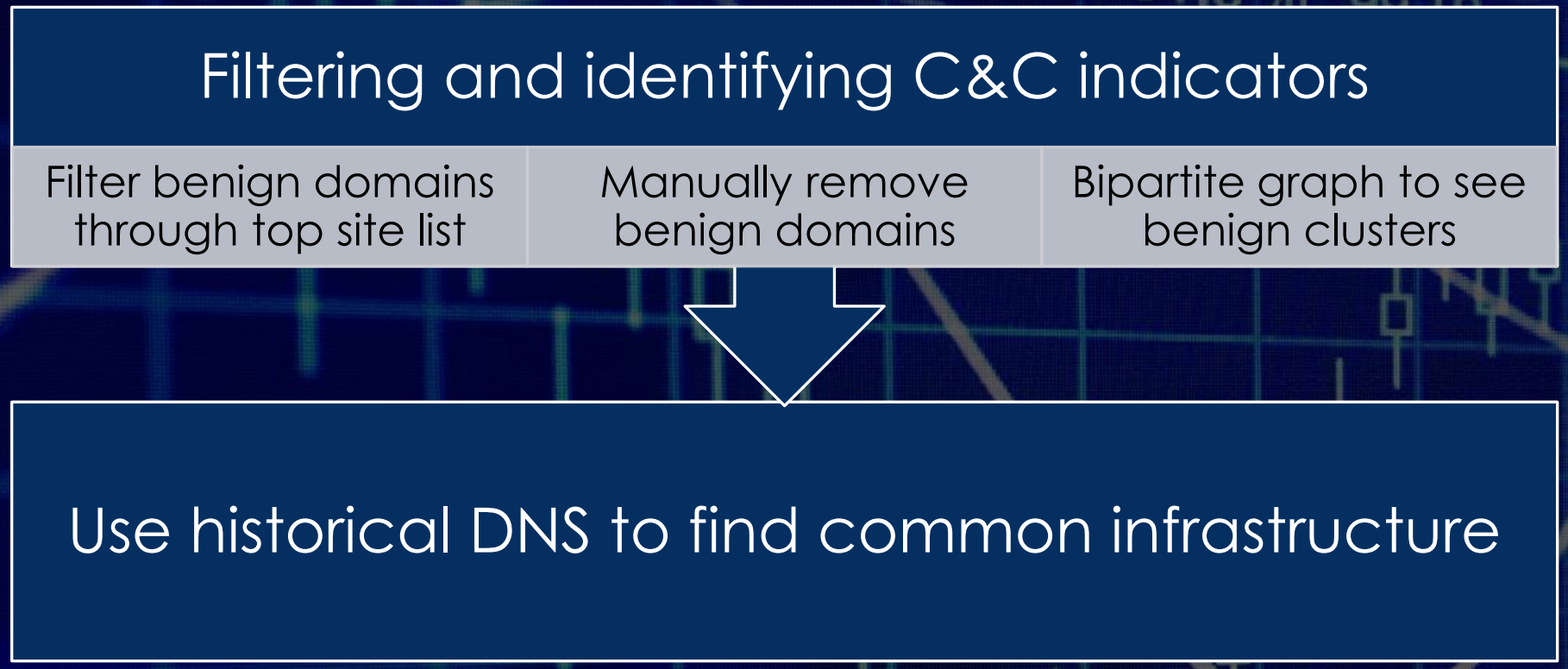
1) Hide programs entry point RWE LOAD segment
2) Fake section headers that overlap entry point
3) Fake dynamic symbol tables
4) Zero values in section header

1) UPX sections
2) Zeroed out headers
3) Corrupt unpacking

DYNAMIC ANALYSIS

- Built virtual machines to execute each sample and collect execution data
  - Each sample run for 60 seconds
  - Would begin to infinitely loop calls after 60 seconds
- Successful execution criteria
  - 3 or more VM processes
  - 100 or more system calls

INFRASTRUCTURE ANALYSIS



MEASUREMENT RESULTS

- No host-based intrusion detection systems run on IoT devices
  - Detecting malware after an infection is not possible.
- Signature-based scanners can detect suspicious binaries forensically captured from the network or the device.
- AV scanners aren't optimized for IoT malware

DETECTION AND LABELLING

- Exploits affect internet-facing devices and devices behind the NAT
- Most of the vulnerability types affect network services by command injection, credential leak, or default credentials.
- Affected device architectures are architecture agnostic
- Headless architecture (no GUI) allows malware to spread rapidly

INFECTION ANALYSIS

PAYLOAD ANALYSIS

- Packing
- Environment keying
- Scripting
  - Python
  - Lua
- Cross-architecture binaries
  - Brute force with many different payloads

PERSISTENCE ANALYSIS

- IoT devices are mostly read only, but have some volatile memory for configurations
- IoT malware use a wide range of persistent methods, making it hard to remove

CAPABILITY ANALYSIS

- Initial variants of IoT malware focused on DDoS and scanning capabilities.
- Capabilities modern IoT malware.
  - Aggressive evasion
  - Privilege escalation
  - Data theft
  - Network scanning and spreading.
  - Device destruction
  - Crypto mining

C&C ANALYSIS

- Network detection of malware communication difficult
- Hard coded IP's make malware it less resilient to takedowns
- Lack of DNS use make IoT hard to track

SUMMARY AND DISCUSSION

CONCLUSION

- Analyses of IoT malware was undergone to compare it to traditional malware
- IoT malware follows a similar lifecycle to traditional malware.
- IoT malware will develop into a much more malicious threat
- The technology exists to protect against IoT malware but isn't utilized properly

CRITICISM

- Comparisons between IoT and traditional malware is lacking
- While analysis into malware is comprehensive, analysis into defences lacks

THANKS FOR LISTENING ☺

ANY QUESTIONS?