IoTPOT: Analysing the Rise of IoT Compromises

Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow

Presented by: Sam Hanna

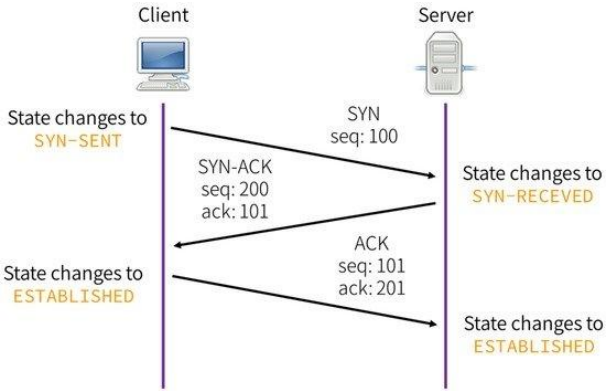
Introduction

Increase in Telnet based attacks on IoT devices

To combat this they propose IoT based Honeypot and Sandbox environments

Introduction: Networking 101

- Networking is based on Protocols
- TCP (Transmission Control Protocol) [1]
  - Runs on the Transport Layer
  - Connects IP to Application
  - Provides a connection between a Client and a Server
  - Secure 3-way handshake
- Ports [2]
  - Specify protocol for TCP
  - Endpoint



[3] TRAP: A Three-Way Handshake Server for TCP Connection Establishment

Introduction: Telnet

- Application Layer Protocol
- Port 23
- Historically used as a remote access command line interface
- SSH mostly replaced it

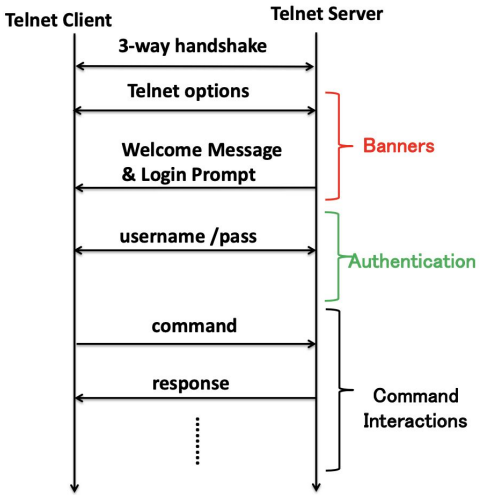


Figure 2 - Telnet Protocol

[4]

Introduction: Security 101

- Honeypot [5]
  - Isolated part of system
  - Contains data that looks real
  - Usually low levels of security
- Sandbox [6]
  - Separate testing environment
  - Used for untrusted code
  - Tightly controlled access
- Malware [7]
  - Code with a malicious intent
  - Family grouped by purpose and techniques [8]

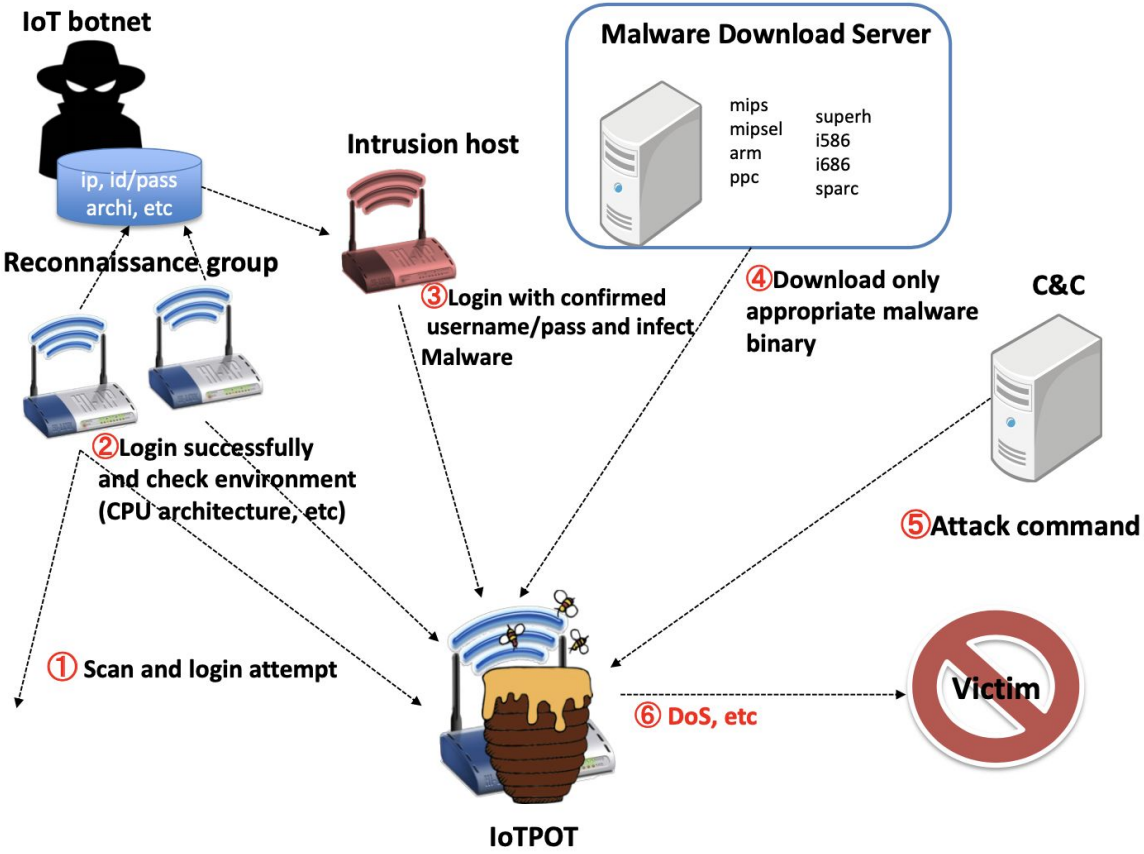


Figure 4 - Coordinated attack of ZORRO family observed by IoTPOT

Problem Definition

- Telnet attacks have increased since 2014
- Seems to be from IoT devices
  - Based on Telnet banners and web contents
- Based on NICTER - A Japanese darknet monitoring survey
  - The number of packets being sent through port 23 have been rapidly increasing
  - More than 209,497 average scans a day
- Categorizing the attacks by device type
  - 34 types of IoT Devices including:
    - DVR
    - IP Camera
    - Wireless Routers

Problem Definition

- Clearly see a spike since 2014
- The spike in 2012 - 2013 is due to the Carna botnet which compromised a large number of IoT devices

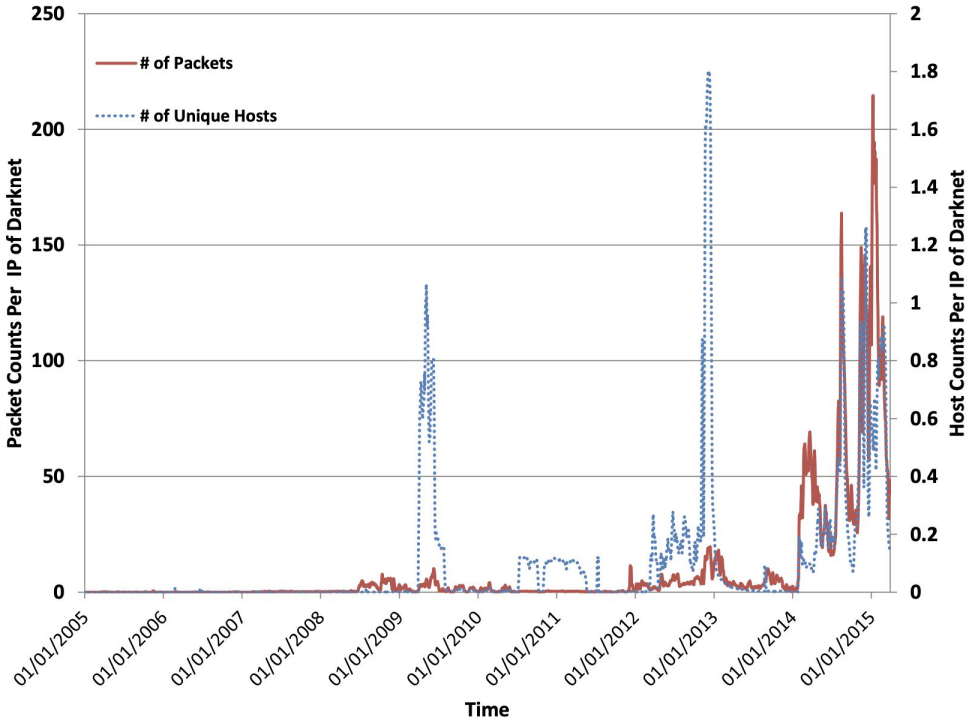


Figure 1 - Packets and hosts on 23/TCP per day per darknet IP

Problem Definition

- Find Malware binaries not on VirusTotal
  - Out of 43 collected samples, 39 were not on VirusTotal
  - Out of the 4 that were on VirusTotal, 2 were not detected by it
- Get an understanding of malware families and their common behavior

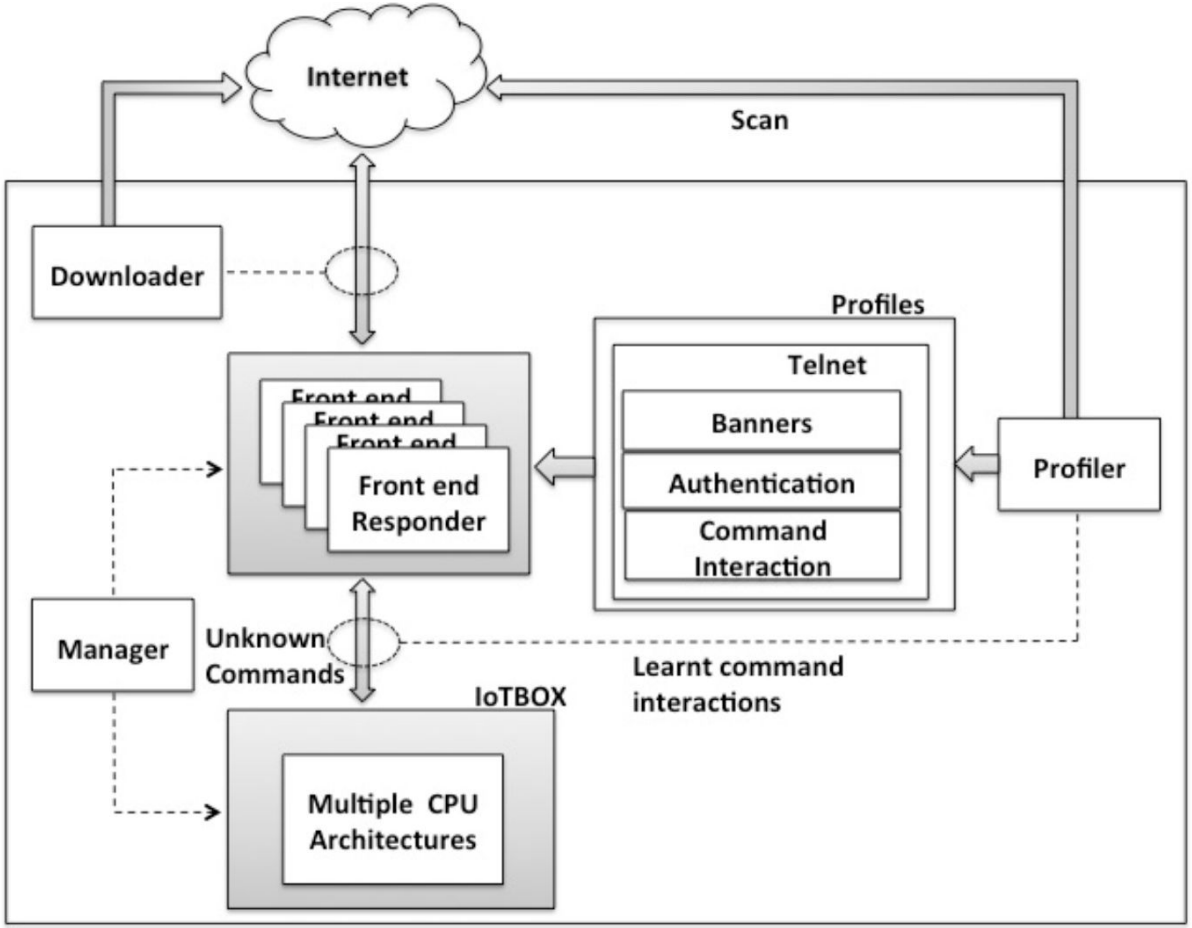


Figure 3 - Overview of IoTPOT

System Design: IoTPOT

- Emulate the Telnet protocol on a variety of IoT devices
- Support options and make realistic welcome messages and login prompts
- Allow for authentication
- Deal with commands
- Support for different CPUs

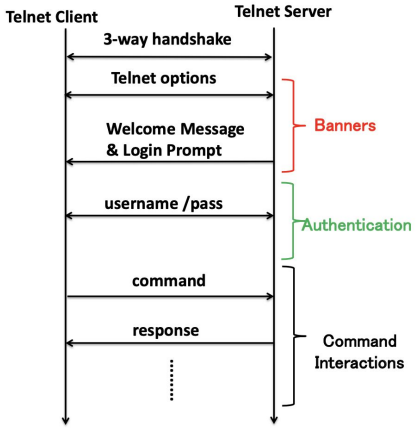


Figure 2 - Telnet Protocol

System Design: IoTPOT

Frontend Responder

- Acts as if it is an IoT device and handles requests
- Have a device profile set up
  - Banner profile
  - Authentication profile
  - Command interaction profile
- If recieves an unknown command connect to IoTBox

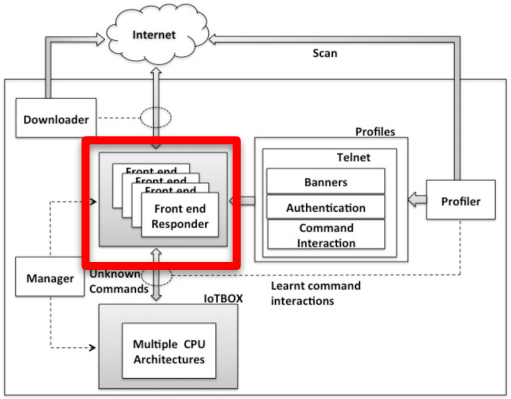


Figure 3 - Overview of IoTPOT

System Design: IoTPOT

Profiler

- The middle-man between the Frontend Responder and the IoTBox
- Gets the command and the response and updates the system that it will be able to deal with the command in the future
- Collects banners from devices so it can emulate more devices

Downloader

- Examines the malware binaries that are downloaded

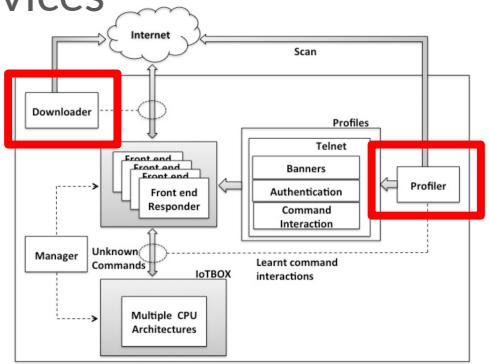


Figure 3 - Overview of IoTPOT

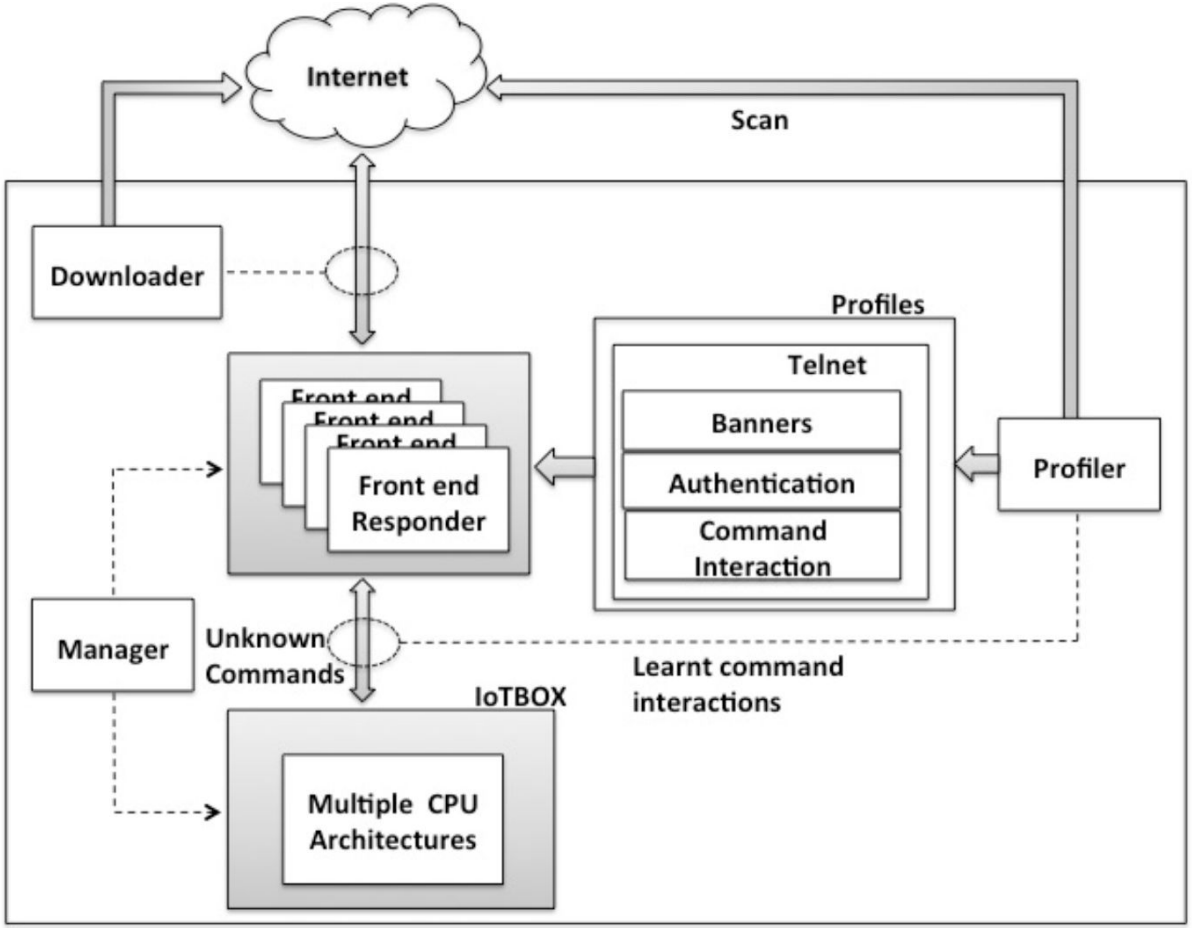


Figure 3 - Overview of IoTPOT

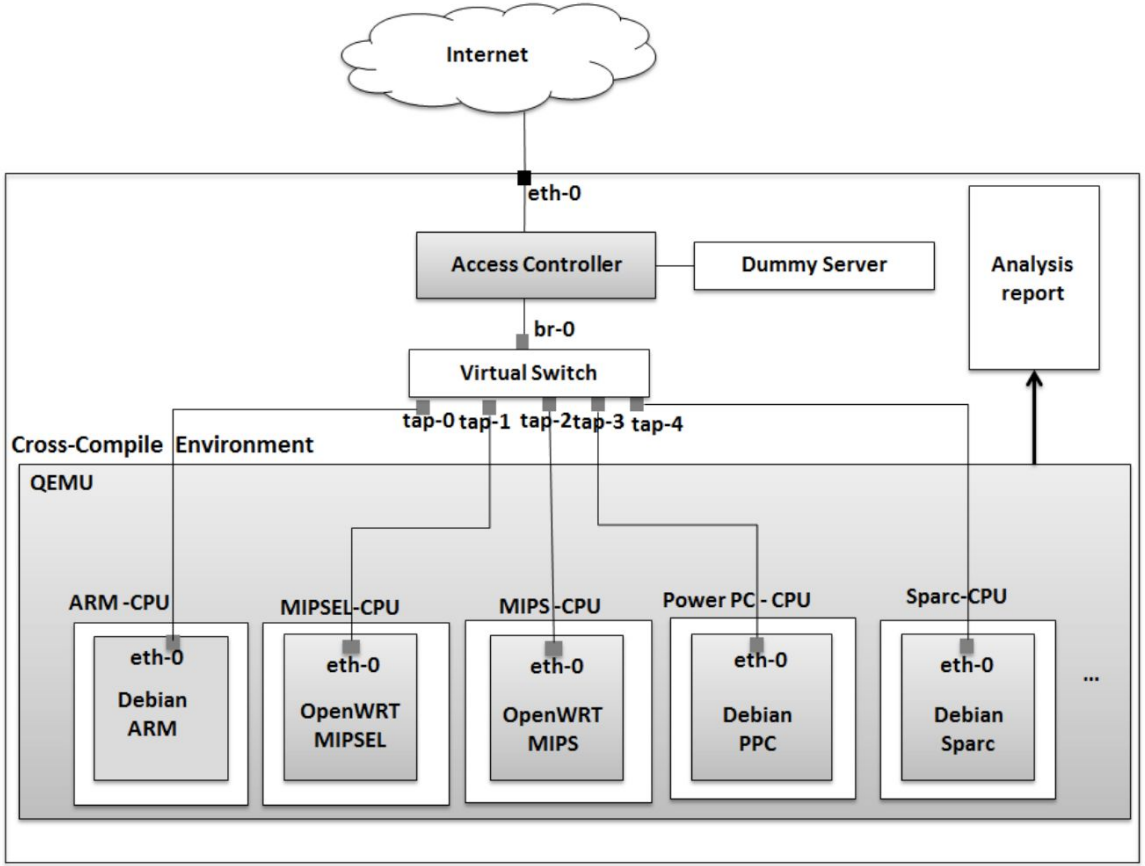


Figure 5 - Overview of IoTBOX

System Design: IoTBOX

- Supports 8 CPU architectures
- Runs QEMU as a cross compilation environment
- Uses OpenWRT for emulated CPU environment
  - Linux based embedded systems OS [9]
- Access Controller
  - Controls all network access
  - Blocks outgoing traffic
  - Port 23 scans are directed to IoTPOT
- Analysis Report
  - Contains results of pcap analysis
  - Summary of commands

Evaluation: IoTPot

- Observed for 39 days
- 76,605 malware download attempts
- 43 downloaded manually
- Found 3 stages of attack
  - Intrusion
  - Infection
  - Monetization
- Some malwares used coordinated intrusions

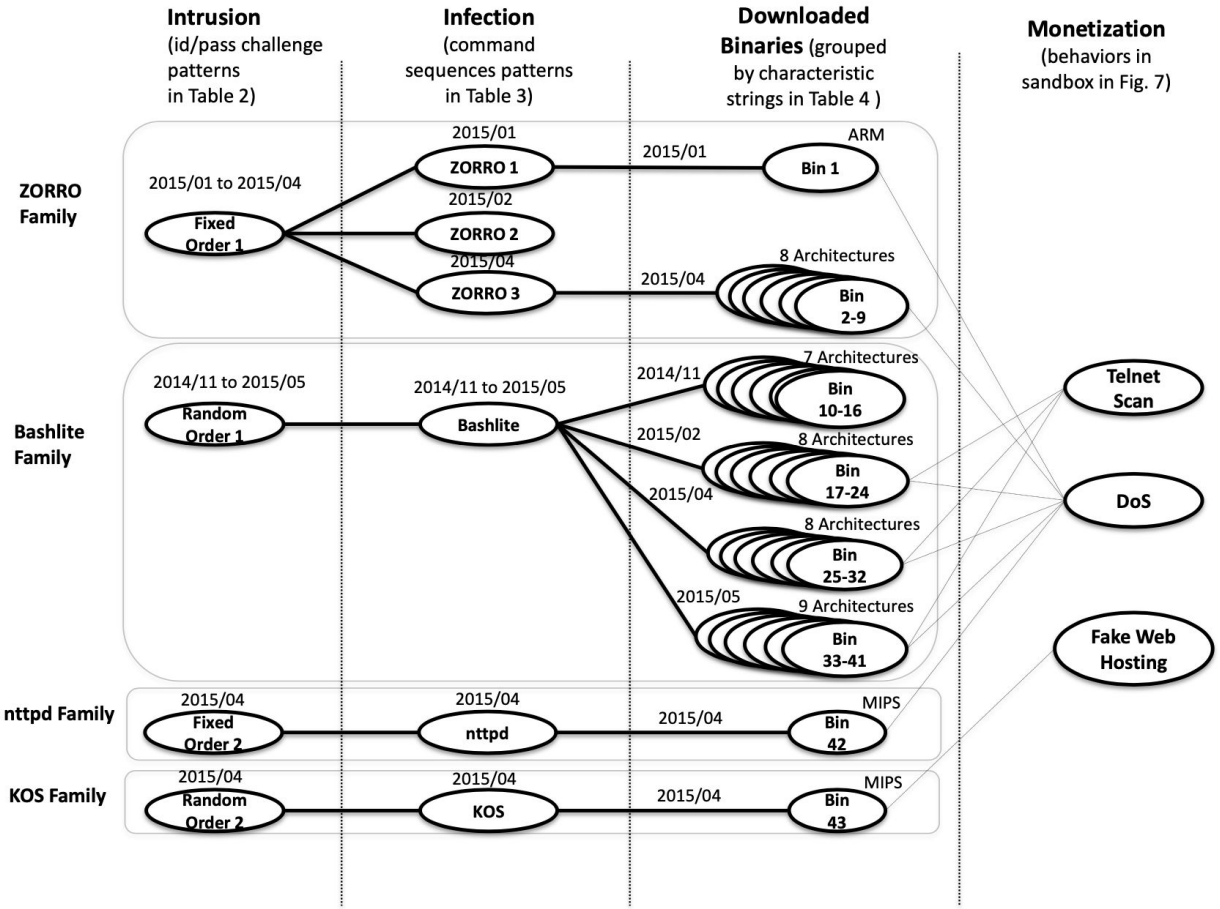


Figure 6 - Overview of Observed Attacks by IoTPOT and IoTBOX

Evaluation: IotBOX

Analyzed 17 different malware binaries

- 10 DoS attacks
  - Mostly TCP/UDP floods
- 2 port 23 scans
- Some DNS based attacks
- One port 5000/UDP opened for further control

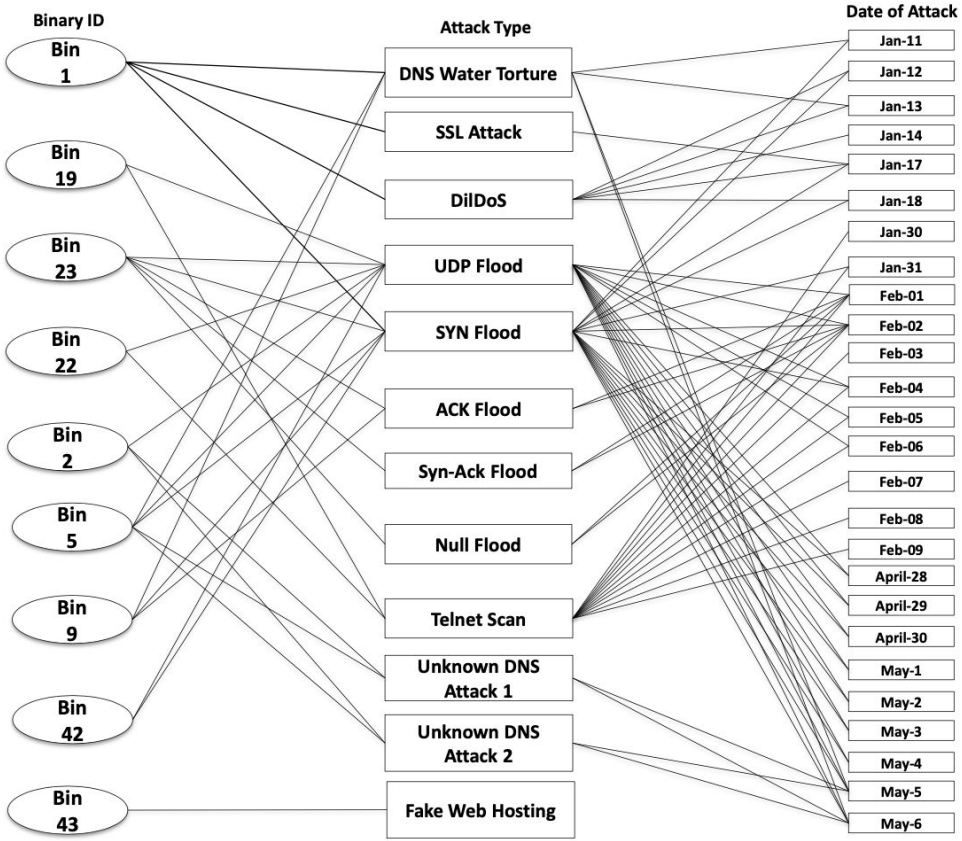


Figure 7 - Observed attacks by IoTBOX

Critique

- They don’t cover use cases and that could help to tie together the problem within the context of IoT on a whole
- The problem is surrounding the vulnerability of IoT devices, but telnet exists on non-embedded systems, they don’t really go into what is special about IoT in this domain
- They talk about why what they do is unique, but I don’t think they talk enough about why it is important

Conclusions

- IoT devices are very vulnerable to Telnet based attacks
- IoTPOT and IoTBOX designed to observe the occurrences of attacks
  - IoTPOT is first honeypot that mimics a number of CPUs and can interact with attackers
  - IoTBOX is first sandbox to handle malware on an array of CPU architectures
- Determined common trends in Telnet based attacks
- Out of sample of 43 found 4 new malware families

GitHub Questions

- @bushidocodes, Sean McBride, Comprehension: What is the advantage of having a slow progressive attack (ZORRO) rather than performing the entire exploit in one go? Is this for security reasons or just for engineering / distributed system reasons (our pool of MIPS penetrators is saturated...)?
- @bushidocodes, Sean McBride, Comprehension: What is it about the telnet protocol that makes is especially vulnerable?
- @AkinoriKahata, Akinori Kahata, Comprehension: What is the recommendation for developers and consumers to improve Cybersecurity as a result of this research?
- @albero94, Alvaro Albero, Critical: How are they logging all the actions that an attacker performs?

GitHub Questions

- @searri, Rick Sear, Comprehension: This paper was published in 2015. What's the landscape like today? Do attackers still go for these easy Telnet attacks? How much have the infection patterns (3.4.2) changed?
- @searri, Rick Sear, Comprehension: Is there any danger that, now that this research is published, attackers will be able to figure out sophisticated ways of avoiding honeypots?
- @ericwendt, Eric Wendt, Critical: Is the system purely for identifying attacks or are there prevention methods built in as well?
- @samfrey99, Sam Frey, Critical: Why is the distribution of devices in section 2 so skewed towards DVRs? Is there something about DVRs that makes them "ideal candidates" for a telnet-based attack?

GitHub Questions

- @samfrey99, Sam Frey, Critical: Were attackers aware that their DoS attacks were being blocked by the Access Controller, or did the IoTPOT have a way to make it appear to the attacker that everything was working the way they expected?
- @reesealanj, Reese Jones, Critical: What about Telnet made it the most significant attack vector?
- @rachellkm, Rachell Kim, Comprehension: What does it mean to categorize device type by HTTP title?

Sources

[1] - https://en.wikipedia.org/wiki/Transmission_Control_Protocol

[2] - https://en.wikipedia.org/wiki/Port_(computer_networking)

[3] - https://www.mdpi.com/applsci/applsci-06-00358/article_deploy/html/images/applsci-06-00358-g001-550.jpg

[4] - https://en.wikipedia.org/wiki/Telnet

[5] - https://en.wikipedia.org/wiki/Honeypot_(computing)

[6] - https://en.wikipedia.org/wiki/Sandbox_(software_development)

[7] - https://en.wikipedia.org/wiki/Malware

[8] - https://www.sciencedirect.com/topics/computer-science/malware-family

[9] - https://en.wikipedia.org/wiki/OpenWrt