Techniques for detecting compromised IoT devices

Ivo van der Elzen, Jeroen van Heugten

RP1 Presentation

UNIVERSITY OF AMSTERDAM

February 6, 2017

Introduction

briankrebs @briankrebs · Sep 21

Holy moly. Prolexic reports my site was just hit with the largest DDOS the internet has ever seen. 665 Gbps. Site's still up. #FAIL

867 1.2K

Octave Klaba / Oles
@olesovhcom

Volgen

This botnet with 145607 cameras/dvr (1-30Mbps per IP) is able to send >1.5Tbps DDoS. Type: tcp/ack, tcp/ack+psh, tcp/syn.

14:31 - 23 september 2016

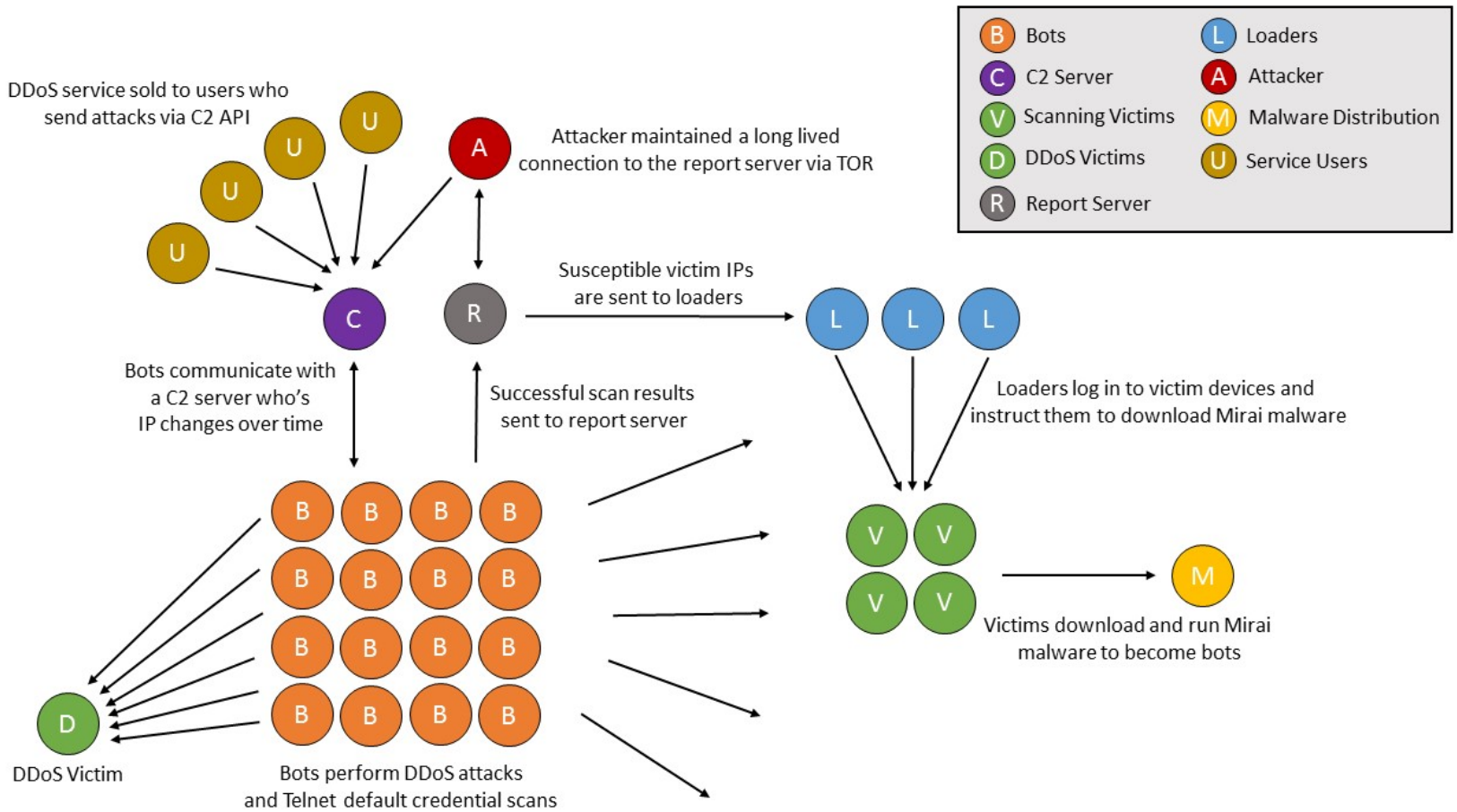
602 402

Research questions

- **Which techniques are feasible in order to gather insight into infected IoT devices?**
  - What are the generic properties of existing IoT malware?
  - What techniques are available to detect IoT malware activity based on these properties?
  - Which technique or combination of techniques is/are most appropriate for a given set of resources or network location?

Malware analysis: Mirai

Mirai overview



Credit: *Level 3 Threat Research Labs*

Malware analysis: Mirai (cont.)

- Scanning
  - Random IP (/32), with exclusions
  - Ports targeted
  - Peculiar window size
- Attacking
  - List of 60 username/password combinations
  - Check string busybox MIRAI & ECCHI
  - Results sent to loader
- Infection
  - Loader delivers malware
  - Removes competing bots
  - Many processor architectures supported

Malware analysis: BASHLITE

AKA: Torlus, gafgyt, Lizkebab

- Very simple client/server setup
- scanner "Lel"
- DDoS attacks
- C&C IRC-derived

Malware analysis: BASHLITE (cont.)

- Scanning
  - Random IP subnet (/24), with exclusions
  - Targets port 23 only
  - Window size unset (system default)
- Attacking
  - Uses random combination of 6 usernames and 14 passwords
  - Bot downloads shell script that downloads the malware
- Infection
  - Script downloads binary for each arch
  - Many processor architectures supported

Other malware targetting IoT devices

Some more

- Zollard
- Hajime
- Anime/Kami
- and many more...

Generic properties of IoT malware

Difficult to be comprehensive... but:

- Lifecycle
  - Scan for devices with open ports
  - Attack devices
  - Infect compromised devices
  - Perform intended actions (DDoS)
  - GOTO 10

Generic properties of IoT malware (cont.)

- Scanning behavior
  - Random scan of IPv4 address space, with exclusions
  - Ports targeted
  - Much code shared, but some peculiarities
- Attacking
  - Main attack method: weak/default username/password
  - Sometimes exploits are used
- Infection method varies
  - BASHLITE: Bots scan & attack, drop/fetch binary
  - Mirai: Bots report results to loader, loader drops binary
  - Hajime: Drops small binary that fetches malware over DHT and uTP

So wat defines IoT malware?

IoT malware is mostly defined by which types of devices it targets:

- IP camera's, DVR's, home routers and other "embedded" devices
- Effective due to support for many architectures, not just x86
- Almost any Linux device with an open telnet and weak password susceptible!

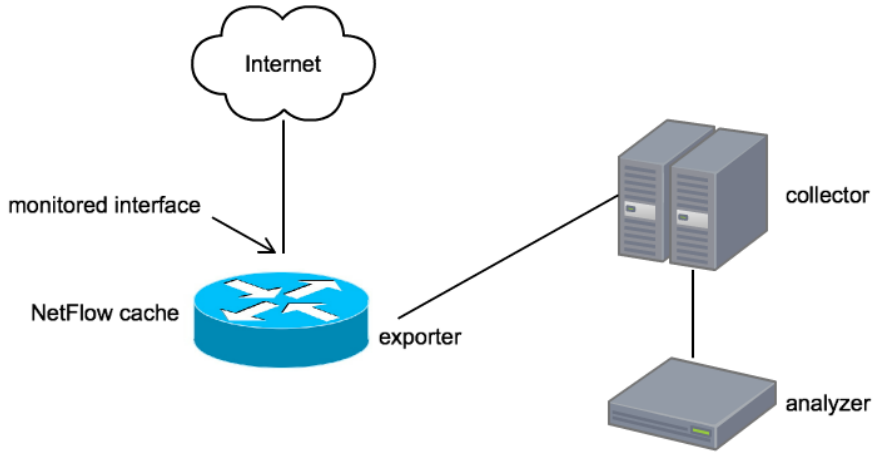
Credit: *Hangzhou Xiongmai Technologies*

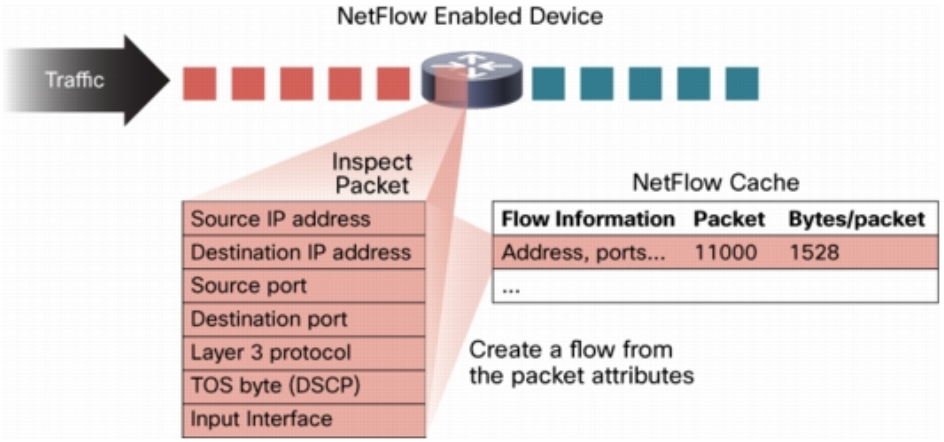
Detection techniques

- NetFlow
- Packet capture
- Honeypots
- Other

Detection techniques: NetFlow

- Lower OSI layers
- Packet headers
- Network monitoring
- Accuracy





Credit: *Cisco Systems*

Detection techniques: Packet capture

- All OSI layers
- Packet headers & payload
- Troubleshooting
- Performance

Detection techniques: Honeypot

- Cowrie (medium-interaction)
  - Tracking malware variants
  - Gathering infected IP addresses
- Full-interaction honeypots
  - DDoS attack targets
  - C&C IP addresses

Credit: *The Honeynet Project*

Detection techniques: Other

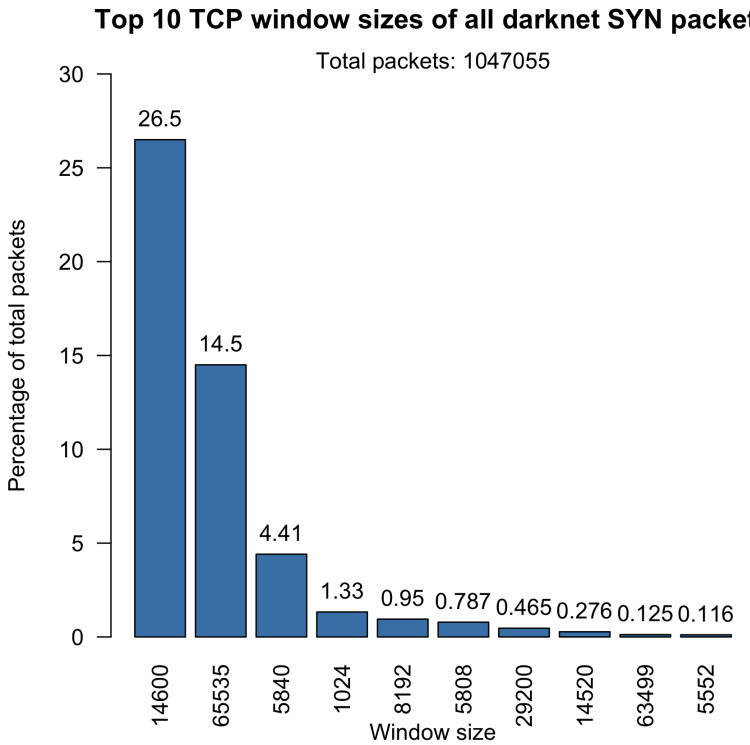
- DNS analysis
  - DGA
- Open/closed port monitoring
  - Shodan
- CAMELIA

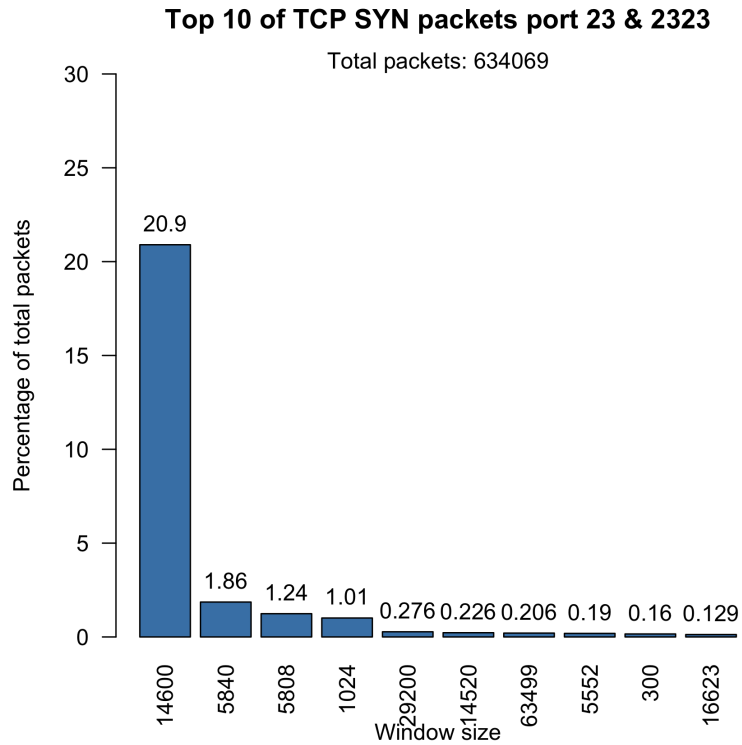
Experiments

- Mirai PRNG window size v.s. darknet scans
- Mirai scanning behavior compared to NetFlow
- Telnet honeypots

Results

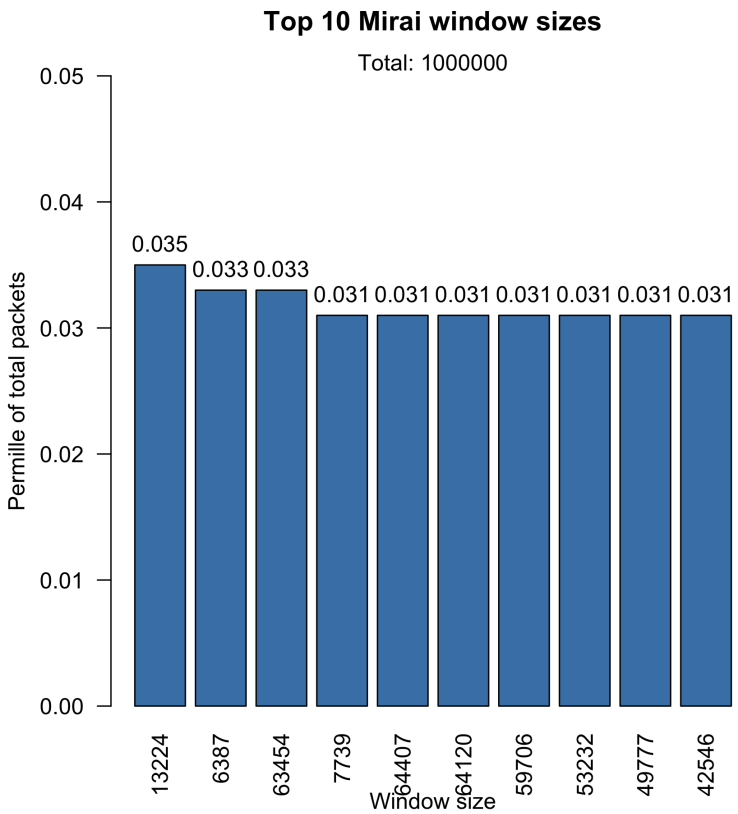
Window sizes of TCP SYN packets captured by darknet monitor

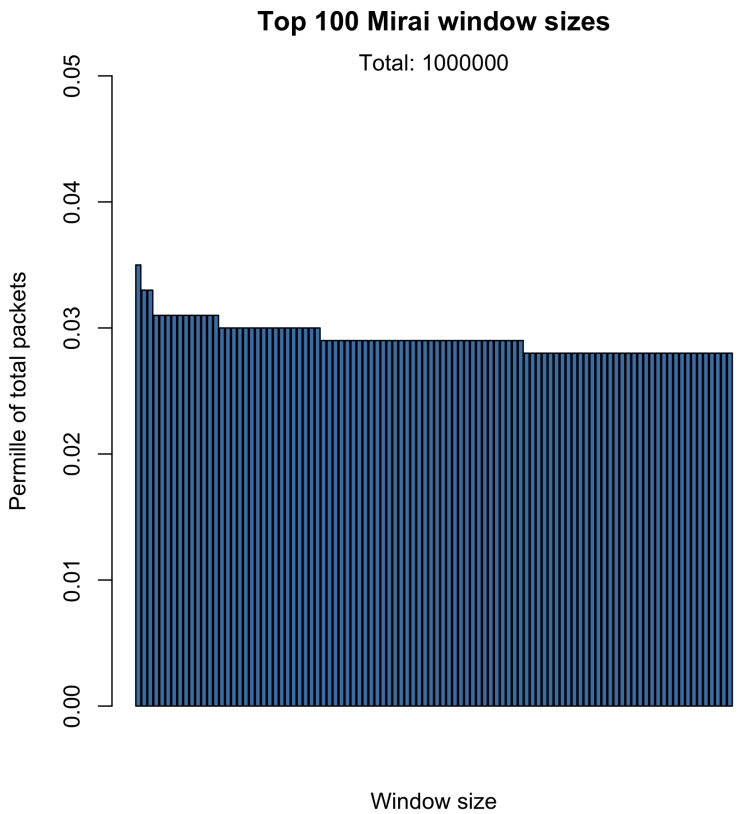




Results (cont.)

Compared to Mirai's window size algorithm (note change of scale!)

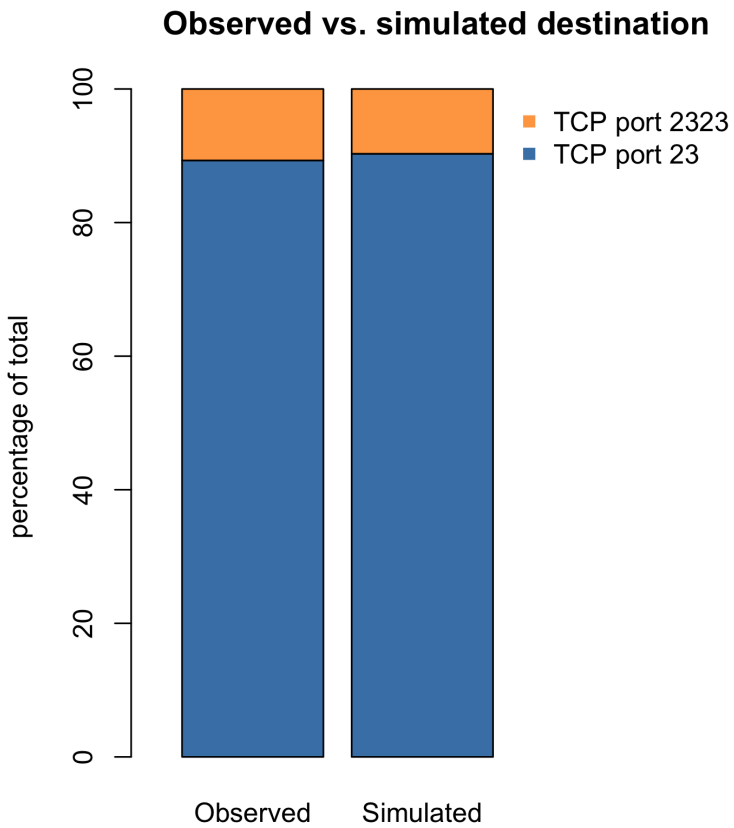




Conclusion: Window sizes used by Mirai very uniformly distributed, this is unusual.

Results (cont.)

Simulated Mirai v.s. suspected Mirai bot



Mirai/Hajime variants seen by honeypots

MIRAI	3147
MASUTA	1835
MM	309
OBJPRN	215
MEMES	29
THTC	18
ECCHI	18
TERROR	5
LLDAN	2
TASKF	2
FBI	2
Subtotal	**5582**

5 random characters	7624
Total	**13224**

Unique source IP / string combinations seen

Conclusion

- Determine generic properties of IoT malware?
  - Yes, but needs to be updated periodically
- Feasible techniques
  - NetFlow analysis
  - Packet capture (Darknet)
  - Honeypot logging
  - Other

Conclusion: Detection techniques can only be effective when applied with knowledge of malware gained from sources such as honeypots and malware analysis.

Questions

Thank you! Any questions?

Special thanks to SURFnet for hosting us and the use of their data and expertise.