

Lecture #4: IoT Botnet Measurements 1

Antonia Affinito, Etienne Khan, Ting-Han Chen,
Cristian Hesselman

University of Twente | May 29, 2024

For 8 years, a hacker operated a massive IoT botnet just to download Anime videos



CITY
SITE.



Admin

Changes based on your feedback

- We'll be using Wooclap to further increase interaction, so keep your cell phone ready :-)
- Your teachers will present fewer slides, allowing for even more time for discussion
- We'll ask you how that went at the end
- Double the number of students is a challenge, so we might be making a few more tweaks



Interactive lectures

- Objective: enable you to learn from each other and further increase your understanding of the papers, contributes to preparing yourself for the oral exam
- Interactive format
 - Teachers summarize two papers per lecture
 - Multiple-choice questions (not graded) and discussion
 - We ask at least one of you to share their thoughts on each paper (pros, cons, surprises)
 - Enables you to learn from each other, so mandatory to participate
- A 7th “re-sit” lecture in case you miss a lecture (optional for everybody else), same format

A woman in a white school shirt and black skirt is shouting into a blue and yellow megaphone. Two men in white school shirts and khaki shorts are standing to her right, covering their ears with their hands. The scene is set in a lush green field with a forested hill in the background.

Speak up!

Interactive lectures

- Overall objective: enable you to learn from each other and further increase your understanding of the papers, contributes to preparing yourself for the written exam
- Interactive format
 - Teachers summarize two papers per lecture
 - Multiple-choice and open questions (not graded) and discussion
 - Enables you to learn from each other
- **Summaries are mandatory!**




Paper summaries

- You must have handed in your two summaries **before 7AM on the day of the lecture**
- Each summary can be **at most 250 words**, at most 1 single-sided A4 page
- You can add figures, and graphs from the paper or add your own if you like (e.g., concept maps)
- You can use the summaries during the oral exam
- Submit through CANVAS
- You **cannot** complete SSI without submitting 12 paper summaries!

Schedule

Lecture	Date	Contents
R1	May 1	Course introduction
R2	May 8	IoT and Internet Core Protocols
G1	May 14	How the core of the Internet works
R3	May 15	IoT Edge Security Systems
	May 22	No lecture (as several of your teachers will be in Dresden :)
R4	May 29	IoT Botnet Measurements 1
R5	Jun 5	IoT Botnet Measurements 2
R6	Jun 12	IoT Security in Non-Carpeted Areas
R7	Jun 19	IoT Device Security
	Jun 26	No lecture (so you can study for the exam :)
G2	TBD	TBD

Important dates

- Two summaries per lecture: **before every lecture at 7 AM CEST**
- Lab report (PDF) and required files: **Wed Jun 19, 9 AM CEST**
- Written exam: **Wed July 3** (timeslot may change, we'll keep you posted)
- Lab groups of 3 people: **Fri May 10, EOB** 
- Alle summaries and lab reports to be submitted through CANVAS

Grading

- $\text{Grade} = (\text{score of written exam}) \times 50\% + (\text{score of the lab assignment}) \times 50\%$
- Where both scores must be a 5.5 or higher. We added this constraint because we'd like folks to focus on both deliverables. This was less of an issue when we used an oral instead of a written exam (2018-2023), because oral exams are more difficult to “slack out of”
- You **MUST** submit summaries for all 12 papers in time to pass SSI. The reason is that the summaries are essential for group learning and help you prepare for your written exam in an incremental way



Introduction to today's lecture

Motivation for today

Viral news story of botnet with 3 million toothbrushes was too good to be true

Journalists reported on hypothetical toothbrush botnet as if it were real.

JON BRODKIN - 2/8/2024, 7:36 PM



Group discussion

- **Discussion** in groups of 5 students
 - Choose 5 students who are sitting close to you
 - If there are no enough students, smaller groups are also acceptable
- Each group chooses one person to summarize the **key points discussed**
 - No longer than **1 minute**



Today's learning objective

- After the lecture, you will be able to discuss how IoT botnets work, such as how they are organized and spread their infections.
- [Mirai] is the infamous botnet that alerted many of the risks of IoT devices.
- [Hajime] is a more advanced IoT botnet, compared to Mirai, when it comes to bot management and usage of exploits.
- Contributes to SSI learning goal #1: “Understand IoT concepts and applications, security threats, technical solutions, and a few relevant standardization efforts in the IETF”

Today's papers: measuring botnets

[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

“Understanding the Mirai Botnet”

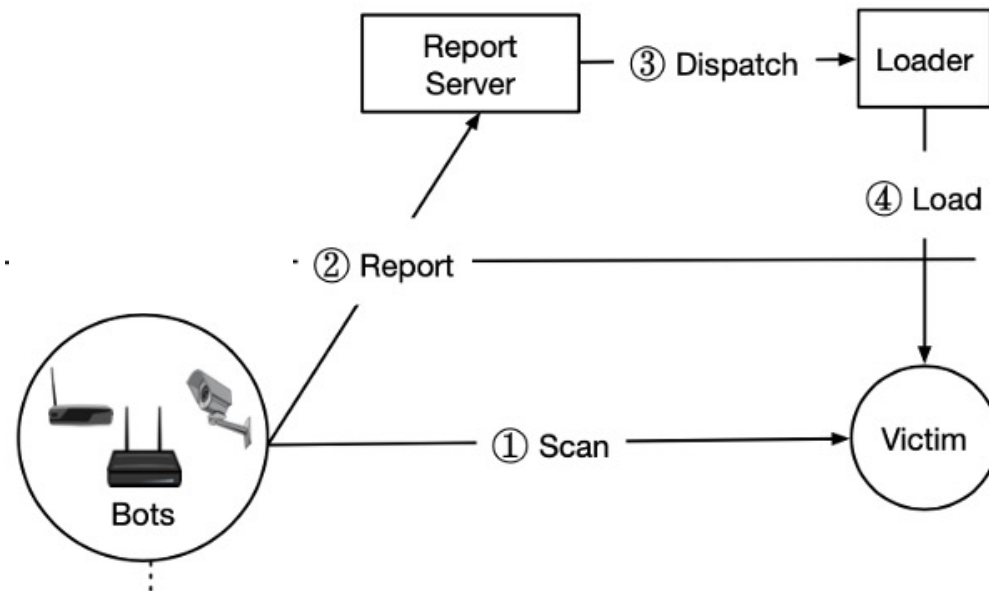
26th USENIX Security Symposium, 2017



What struck you about the paper?

Mirai Botnet Escape Room Challenge

- Puzzle 1: Identify the key components of an IoT botnet
 - **Components:** Botmaster, Bots, Command and Control server, IoT devices, Report Server, Loader Server.
- Puzzle 2: Steps of botnet establishment phase



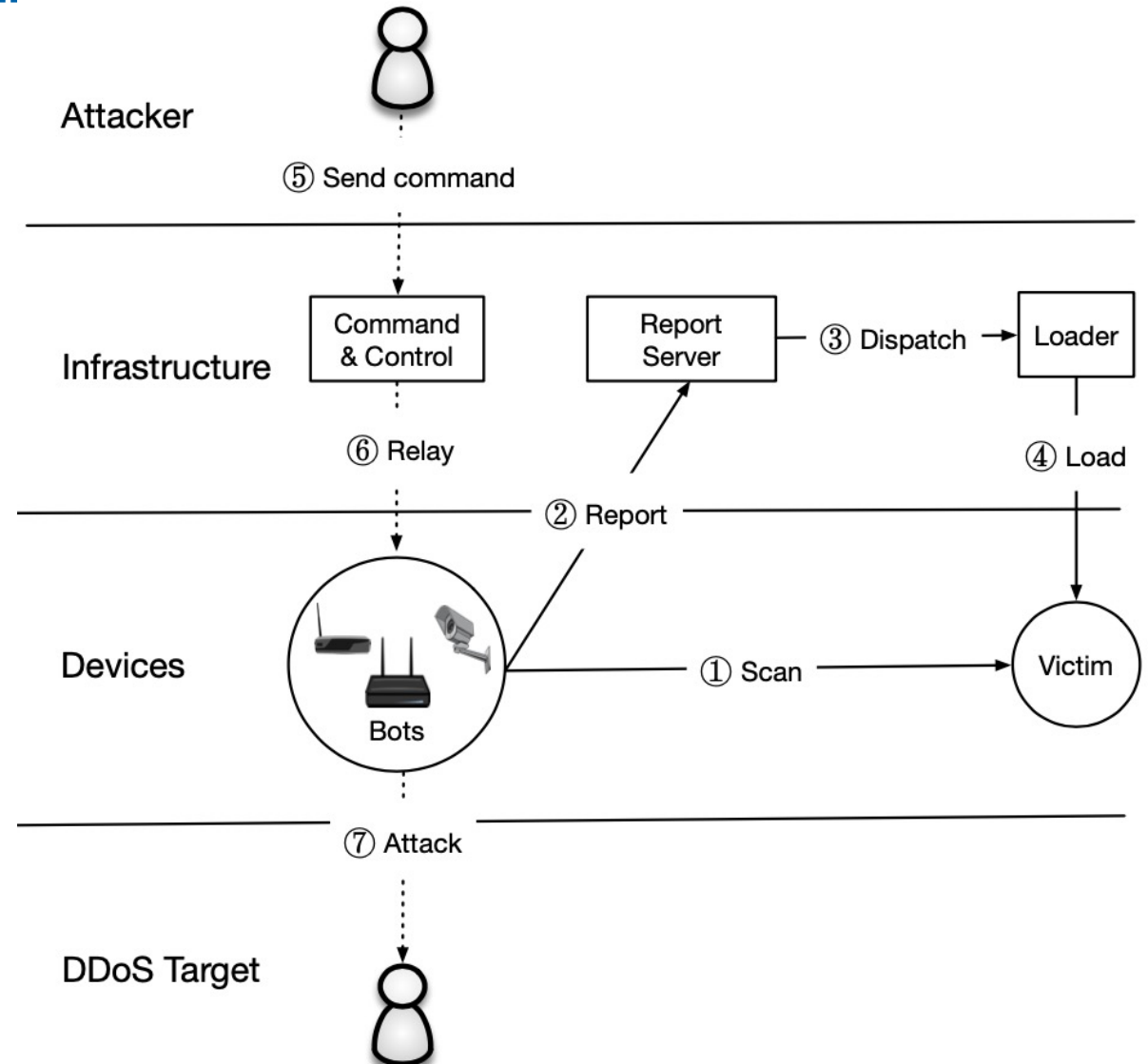
Mirai Botnet Escape Room Challenge

- Puzzle 1: Identify components of an IoT botnet
- Puzzle 2: Steps of botnet establishment phase
- Puzzle 3: Role of IoT devices in a botnet
 - IoT devices receive and execute commands from the command and control (C&C) server and participate in coordinated attacks like DDoS.
- Puzzle 4: Steps of attack launch phase



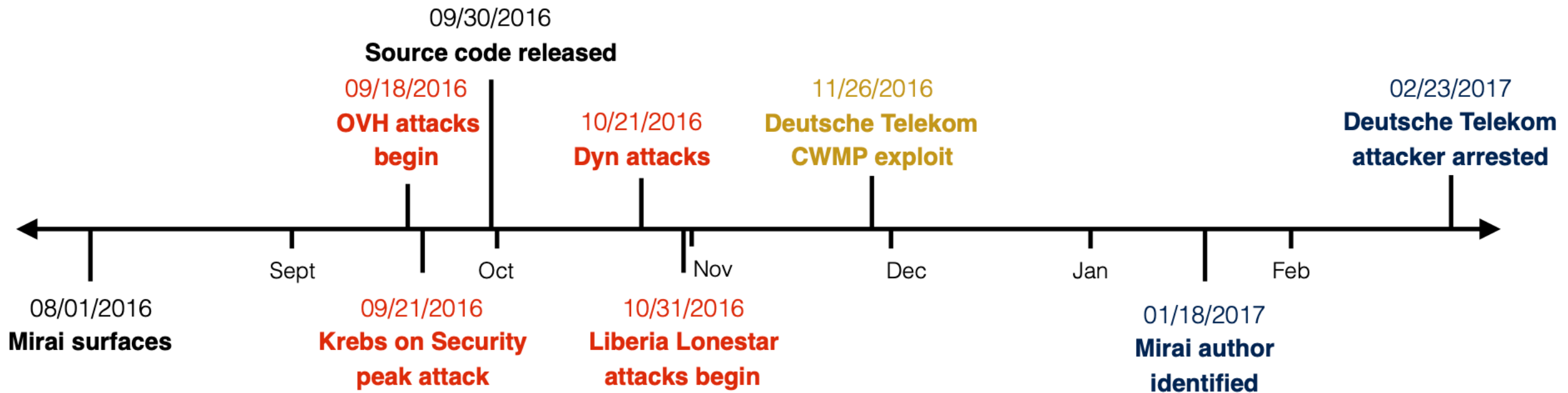
Mirai Botnet Inner Working

- 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.
- C2 await commands



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



Mirai uses default passwords

```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10); // root xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9); // root vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8); // root admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7); // admin admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6); // root 888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5); // root xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5); // root default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5); // root juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5); // root 123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5); // root 54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5); // support support
add_auth_entry("\x50\x4D\x4D\x56", "", 4); // root (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4); // admin password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4); // root root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4); // root 12345
add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3); // user user
add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3); // admin (none)
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3); // root pass
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3); // admin admin1234
```


Scanning the Internet

```
while (o1 == 127 || // 127.0.0.0/8 - Loopback
      (o1 == 0) || // 0.0.0.0/8 - Invalid address space
      (o1 == 3) || // 3.0.0.0/8 - General Electric Company
      (o1 == 15 || o1 == 16) || // 15.0.0.0/7 - Hewlett-Packard Company
      (o1 == 56) || // 56.0.0.0/8 - US Postal Service
      (o1 == 10) || // 10.0.0.0/8 - Internal network
      (o1 == 192 && o2 == 168) || // 192.168.0.0/16 - Internal network
      (o1 == 172 && o2 >= 16 && o2 < 32) || // 172.16.0.0/14 - Internal network
      (o1 == 100 && o2 >= 64 && o2 < 127) || // 100.64.0.0/10 - IANA NAT reserved
      (o1 == 169 && o2 > 254) || // 169.254.0.0/16 - IANA NAT reserved
      (o1 == 198 && o2 >= 18 && o2 < 20) || // 198.18.0.0/15 - IANA Special use
      (o1 >= 224) || // 224.*.*.*+ - Multicast
      (o1 == 6 || o1 == 7 || o1 == 11 ||
      o1 == 21 || o1 == 22 || o1 == 26 ||
      o1 == 28 || o1 == 29 || o1 == 30 ||
      o1 == 33 || o1 == 55 || o1 == 214 ||
      o1 == 215) // Department of Defense
);
```

Scanning the Internet (2)

```
for (i = 0; i < SCANNER_RAW_PPS; i++)
{
    struct sockaddr_in paddr = {0};
    struct iphdr *iph = (struct iphdr *)scanner_rawpkt;
    struct tcphdr *tcph = (struct tcphdr *)(iph + 1);

    iph->id = rand_next();
    iph->saddr = LOCAL_ADDR;
    iph->daddr = get_random_ip();
    iph->check = 0;
    iph->check = checksum_generic((uint16_t *)iph, sizeof (struct iphdr));

    if (i % 10 == 0)
    {
        tcph->dest = htons(2323);
    }
    else
    {
        tcph->dest = htons(23);
    }
    tcph->seq = iph->daddr;
    tcph->check = 0;
    tcph->check = checksum_tcpudp(iph, tcph, htons(sizeof (struct tcphdr)), sizeof (struct tcphdr));

    paddr.sin_family = AF_INET;
    paddr.sin_addr.s_addr = iph->daddr;
    paddr.sin_port = tcph->dest;
}
```

Get your phones ready!

- Wooclap QR code



Quiz - Wooclap

Botnets can be used for purposes other 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

Question - Wooclap

What are the challenges to analyze and/or mitigate Mirai attacks?



Question

- What was the biggest ‘contribution’ of Mirai in your opinion?
- What are the weaknesses of the paper?

Key takeaways

Simple attack, lots of damage

Automatic updates

Device identification on network

IoT end-of-life devices (externality)

Connecting datasets gives a lot of information!



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



What struck you about the paper?

Get your phones ready!



Hajime - はじめ(Ha-ji-mé)



Hajime - はじめ (Ha-ji-mé)

- Mirai - みらい [mí[↓]rài] – future
- Hajime - はじめ [ha-ji-mé] - beginning

Focus

- The important differences between Mirai and Hajime
- Backscatter data from a root DNS server
- Discussions

The 3 big differences

- Peer-to-Peer instead of centralized command & control
 - More exploits based on the Vault7 leak
 - Custom protocol to spread the malware
-
- No malicious activity had been recorded. Does this count as difference?

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

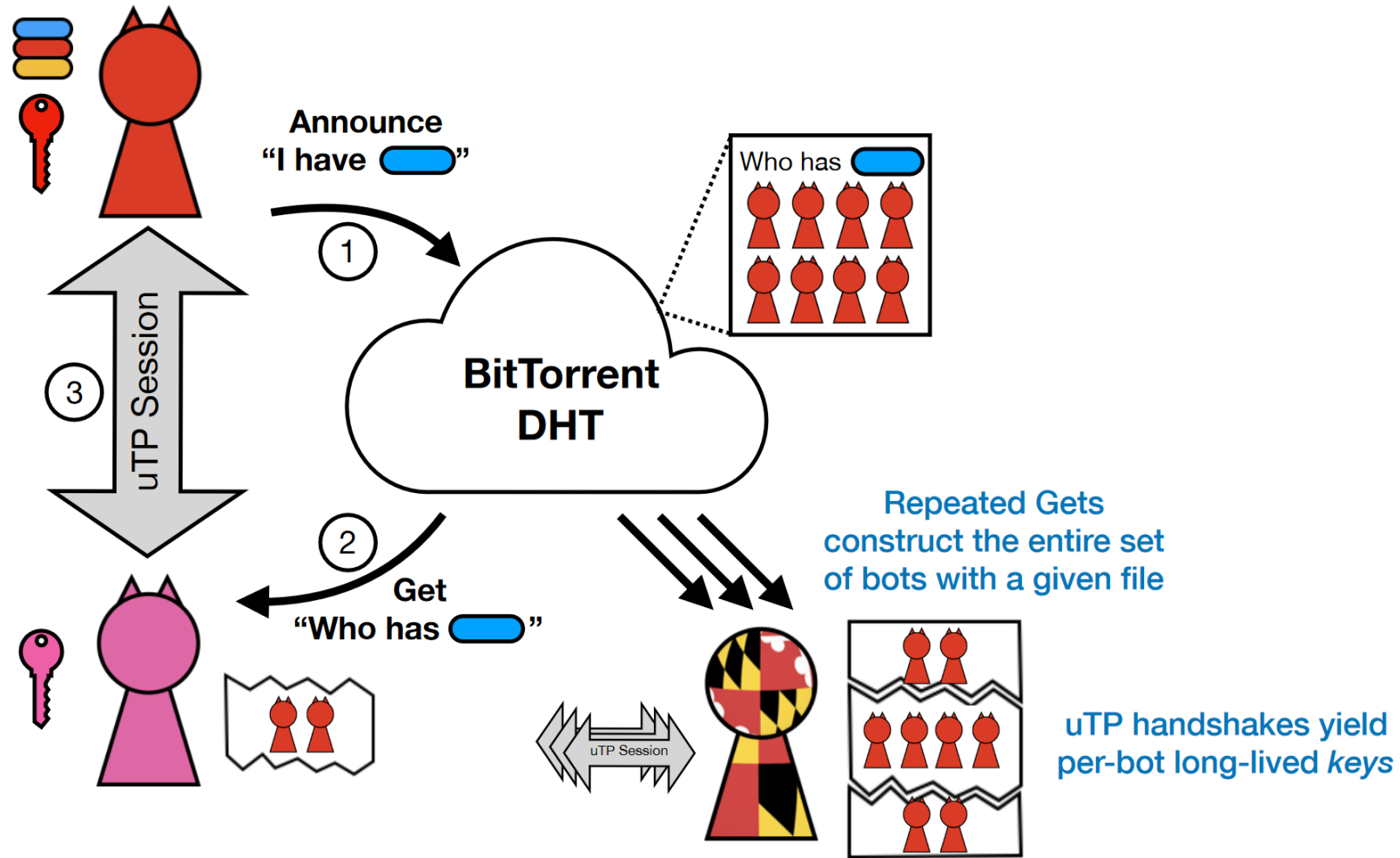
P2P Mechanisms

- DHT (Kademlia) based.
 - Known from e.g. BitTorrent
 - Traditional BitTorrent connections relied on trackers to exchange seeder/leecher information
- Basically, a distributed Key-Value storage
 - Key is filename concatenated with current day' timestamp (SHA1 hashed)
 - Values are IPs which are infected with Hajime and allow for payload downloads

P2P Mechanisms

- “example” on Oct. 1, 2016
- 1. Get the current date, UTC.
- 2. Write the date in the format D-M-Y-W-Z, where D represents the day of the month, M represents the month (0 for January, 1 for February, ...), Y represents the years since 1900, W represents the day of the week (0 for Sunday, 1 for Monday, ...), Z represents the number of days since Jan. 1 of that year.
- Date: 1-9-116-6-274
- Then append SHA1(“example”) (with a dash) -> 1-9-116-6-274-c3499c2729730a7f807efb8676a92dcb6f8a3f8f
- Finally search the DHT for SHA1(previous_step) -> 5dfd959c78d359272d46afd2e3069b34a9455ffd.

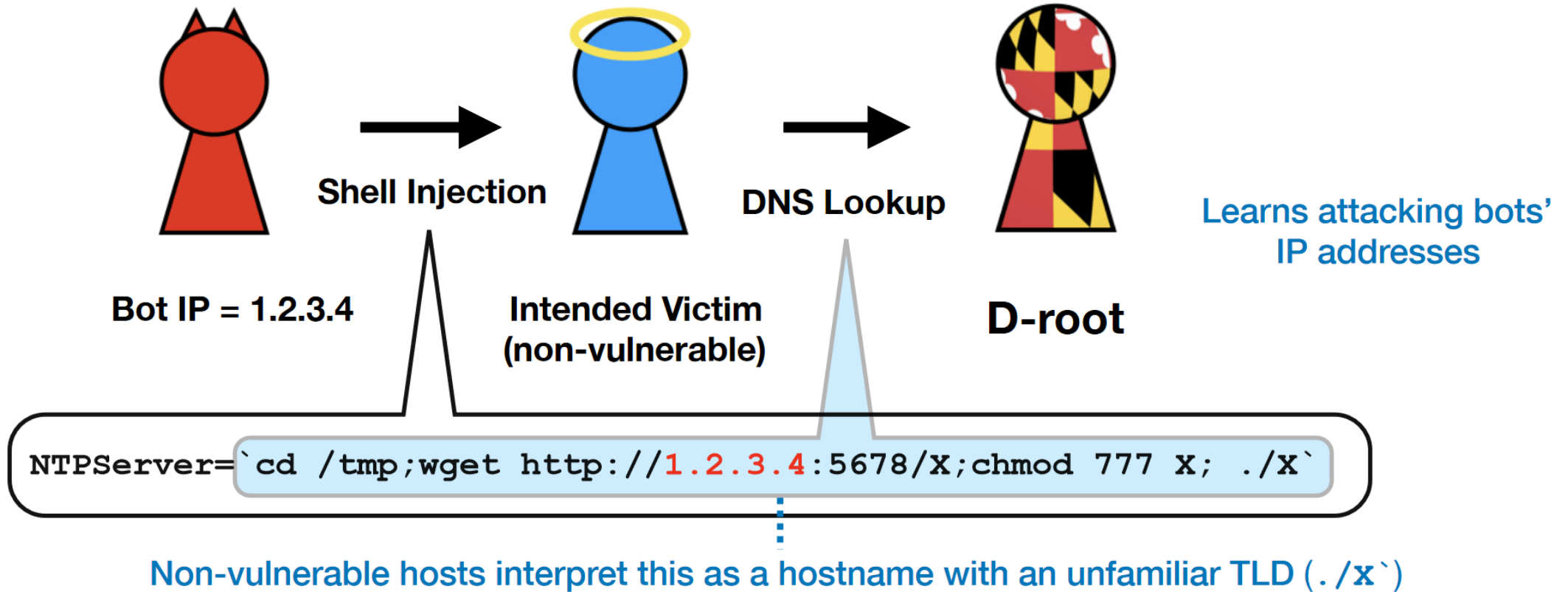
P2P Mechanisms



Custom uTorrent Transport Protocol

- Mirai was enumerable/detectable due to its custom TCP sequence field
- Hajime uses unique cryptographic public keys to allow for a count of infected hosts
- Some churn expected due to recreation of the public key, during updates to the .i module
- Still a stronger identifier, compared to weak identifiers such as IPs (ie. due to carrier grade NAT)

DNS backscatter data



DNS backscatter data

- Based on trying to inject shell-commands into a NTP configuration file
- Vulnerable devices won't sanitize the input and then execute the commands, infecting the device.
- Remember how DNS lookups work? Invalid queries will be sent to the root DNS servers
 - Conveniently the researchers of the paper operate one of the root DNS servers

White hat, grey hat, black hat?

- Communication from the bot author:

Just a white hat, securing some systems.
Important messages will be signed like this!
Hajime Author.
Contact CLOSED Stay sharp!

- Discuss this approach

White hat, grey hat, black hat?



Think like a defender



Think like an attacker



Question



Demo

1. UTC timestamp
2. payload name
3. date used as input for computing the payload's DHT hash ID
4. payload DHT ID (the hash we lookup or announce on the DHT)
5. "seeder" or "leecher" (are we collecting seeders or leechers, respectively)
6. IPv4 address of seeder/leecher bot
7. port number of seeder/leecher bot

Demo (Backup)

```
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 98.43.129.55 62289
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 109.148.173.191 62289
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 79.161.52.82 62289
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 24.88.23.242 62289
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 69.112.168.236 62289
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 108.173.178.204 62289
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 71.210.33.221 62289
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 24.115.107.208 62289
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 176.14.243.44 62289
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 71.190.197.164 62289
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 70.119.82.44 62289
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 184.83.113.35 62289
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 137.25.255.15 62289
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 185.108.162.49 62289
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 176.110.136.21 62289
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 62.46.102.115 62289
1620769710 atk.mipseb.1506215619 2021-05-09 1173332a85f47e1a40b15f3d77a550ff342442c2 seeder 67.251.129.160 62289
1620769711 1173332a85f47e1a40b15f3d77a550ff342442c2 5.139.3.14:49978 117710404a4f6e018508fce5f2855ef7b4b63620 115.
#1620769711 1173332a85f47e1a40b15f3d77a550ff342442c2 117710404a4f6e018508fce5f2855ef7b4b63620 5.139.3.14:49978 Tot
1620769711 1173332a85f47e1a40b15f3d77a550ff342442c2 144.91.111.37:9613 1173332a85f47e1a40b15f3d77a550fa00c24bc9 18
1620769711 1173332a85f47e1a40b15f3d77a550ff342442c2 144.91.111.37:9613 1173332a85f47e1a40b15f3d77a550fa00c24bc9 47
```

Demo (Backup)

```
1620769773 .i.armv6l.1509400182 2021-05-11 2f9f80b52e7df032562bfdc6174733006fb978e9 seeder 173.46.242.130 62289
1620769773 .i.armv6l.1509400182 2021-05-11 2f9f80b52e7df032562bfdc6174733006fb978e9 seeder 174.20.138.204 62289
1620769773 .i.armv6l.1509400182 2021-05-11 2f9f80b52e7df032562bfdc6174733006fb978e9 seeder 79.136.72.19 62289
1620769773 .i.armv6l.1509400182 2021-05-11 2f9f80b52e7df032562bfdc6174733006fb978e9 seeder 87.81.93.7 62289
1620769773 .i.armv6l.1509400182 2021-05-11 2f9f80b52e7df032562bfdc6174733006fb978e9 seeder 154.45.216.220 62289
1620769774 2f9f80b52e7df032562bfdc6174733006fb978e9 144.91.111.37:9613 2f9f80b52e7df032562bfdc6174733fa00c24bc9 173.46.242.130 62289
1620769774 2f9f80b52e7df032562bfdc6174733006fb978e9 144.91.111.37:9613 2f9f80b52e7df032562bfdc6174733fa00c24bc9 174.20.138.204 62289
1620769774 2f9f80b52e7df032562bfdc6174733006fb978e9 144.91.111.37:9613 2f9f80b52e7df032562bfdc6174733fa00c24bc9 79.136.72.19 62289
1620769774 2f9f80b52e7df032562bfdc6174733006fb978e9 144.91.111.37:9613 2f9f80b52e7df032562bfdc6174733fa00c24bc9 87.81.93.7 62289
1620769774 2f9f80b52e7df032562bfdc6174733006fb978e9 144.91.111.37:9613 2f9f80b52e7df032562bfdc6174733fa00c24bc9 154.45.216.220 62289
#1620769774 2f9f80b52e7df032562bfdc6174733006fb978e9 2f9f80b52e7df032562bfdc6174733fa00c24bc9 144.91.111.37:9613 Total seeders: 5 new_r
1620769785 .i.mipseb.1524631409 2021-05-11 5b28b53bc218c21fdd3ec9b11e696c137a7420f8 seeder 174.17.14.156 62289
1620769785 .i.mipseb.1524631409 2021-05-11 5b28b53bc218c21fdd3ec9b11e696c137a7420f8 seeder 64.121.214.41 62289
1620769785 .i.mipseb.1524631409 2021-05-11 5b28b53bc218c21fdd3ec9b11e696c137a7420f8 seeder 79.136.72.19 62289
1620769785 .i.mipseb.1524631409 2021-05-11 5b28b53bc218c21fdd3ec9b11e696c137a7420f8 seeder 188.17.175.246 62289
1620769785 .i.mipseb.1524631409 2021-05-11 5b28b53bc218c21fdd3ec9b11e696c137a7420f8 seeder 81.217.115.184 62289
1620769786 5b28b53bc218c21fdd3ec9b11e696c137a7420f8 144.91.111.37:9613 5b28b53bc218c21fdd3ec9b11e696cfa00c24bc9 174.17.14.156 62289
1620769786 5b28b53bc218c21fdd3ec9b11e696c137a7420f8 144.91.111.37:9613 5b28b53bc218c21fdd3ec9b11e696cfa00c24bc9 64.121.214.41 62289
1620769786 5b28b53bc218c21fdd3ec9b11e696c137a7420f8 144.91.111.37:9613 5b28b53bc218c21fdd3ec9b11e696cfa00c24bc9 79.136.72.19 62289
1620769786 5b28b53bc218c21fdd3ec9b11e696c137a7420f8 144.91.111.37:9613 5b28b53bc218c21fdd3ec9b11e696cfa00c24bc9 188.17.175.246 62289
1620769786 5b28b53bc218c21fdd3ec9b11e696c137a7420f8 144.91.111.37:9613 5b28b53bc218c21fdd3ec9b11e696cfa00c24bc9 81.217.115.184 62289
#1620769786 5b28b53bc218c21fdd3ec9b11e696c137a7420f8 5b28b53bc218c21fdd3ec9b11e696cfa00c24bc9 144.91.111.37:9613 Total seeders: 5 new_r
1620769787 .i.mipseb.1522574410 2021-05-12 09f5299a344afa50742c3f29ac7d9a163fc04b94 seeder 5.146.192.252 62289
1620769788 09f5299a344afa50742c3f29ac7d9a163fc04b94 144.91.111.37:9613 09f5299a344afa50742c3f29ac7d9afa00c24bc9 5.146.192.252 62289
#1620769788 09f5299a344afa50742c3f29ac7d9a163fc04b94 09f5299a344afa50742c3f29ac7d9afa00c24bc9 144.91.111.37:9613 Total seeders: 1 new_r
```

Key Takeaways

1. Command-And-Control impossible to take down, without also affecting legitimate users
2. Multiple identifiers can help in mapping the extent of a botnet (uTP keys, backscatter data)
3. Abandoned botnets float through the Internet, like satellite debris around earth's orbit

Key takeaways

- Analyzing botnets properly requires many vantage points and datasets.
- Mirai ‘shook the world’ and showed potential of IoT botnets in terms of DDoS attacks.
- By leveraging an established decentralized communication protocol for command & control, Hajime circumvents traditional take-down measures for botnets.



Next regular lecture:
Wed June 5, 10:45-12:30
Topic: IoT Botnet Measurements 2