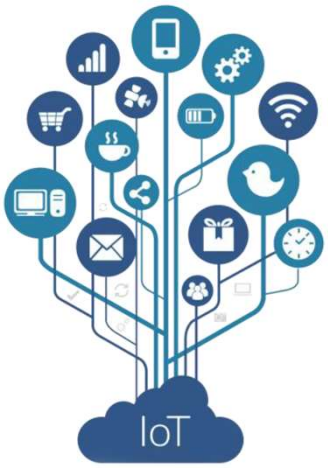
MANCHESTER 1824
The University of Manchester



COMP32412: Internet of Things Architecture and Applications

Case Study: DDoS in IoT- Mirai and other botnets

Mustafa A. Mustafa

mustafa.mustafa@manchester.ac.uk
KB 2.93, 2nd Floor, Kilburn Building

MANCHESTER 1824
The University of Manchester

Overview & Learning Outcomes

- Describe and identify botnet-based DDoS attacks in IoT

MANCHESTER 1824
The University of Manchester

IoT botnets

- The large volume, extensiveness, and high vulnerability of IoT devices have attracted many bad actors, particularly those orchestrating distributed denial-of-service (DDoS) attacks.
- A botnet is network of interconnected devices that could be infected with malicious software acting as bots.
- One of the prominent example of botnets is Mirai botnet - a malware that was identified first in 2016
- The Mirai malware exploits security holes in IoT devices, and has the potential to harness the collective power of millions of IoT devices into botnets, and launch attacks.

3

Botnets can be designed to accomplish illegal or malicious tasks including sending spam,
stealing data, ransomware, fraudulently clicking on ads or distributed denial-of-service
(DDoS) attacks.

- Mirai is malware that infects smart devices, turning them into a network of remotely controlled bots or "zombies“. Mirai causes a DDoS against a set of target servers by constantly propagating to weakly configured IoT devices. The source code of Mirai is publicly available and different variants are used by attackers to infect and control IoT devices
- In September 2016, the website of computer security consultant Brian Krebs was hit with 620 Gbps of traffic. At about the same time, an even bigger DDoS attack using Mirai malware—peaking at 1.1 Tbps— targeted the French webhost and cloud service provider OVH.

Source:

- Kolias, Constantinos, et al. "DDoS in the IoT: Mirai and other botnets." Computer 50.7 (2017): 80-84. https://doi.org/10.1109/MC.2017.201
- “What is the Mirai Botnet” https://www.cloudflare.com/learning/ddos/glossary/miraibotnet/

MANCHESTER 1824
The University of Manchester

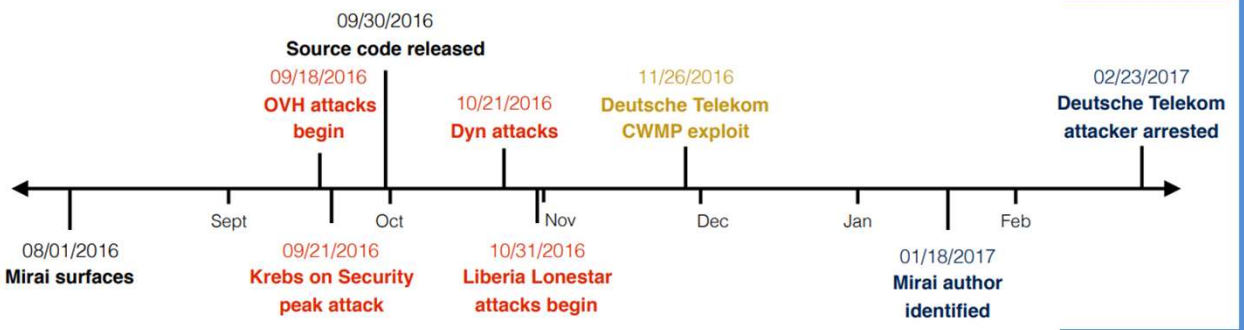
Mirai botnet

4

- Mirai botnet came to prominence in October 2016 when it was responsible for the DDoS attack that took down many large web services such as reddit, AWS, Netflix, spotify, twitter, github, paypal, …
- It was composed of IoT devices such as IP cameras and DVRs.

MANCHESTER 1824
The University of Manchester

Mirai timeline



Major attacks (red), exploits (yellow), and events (black) related to the Mirai botnet

5

- Reports of Mirai appeared as early as August 31, 2016
- It was not until mid-September, 2016 that Mirai grabbed headlines with massive DDoS attacks targeting Krebs on Security and OVH
- Several additional high-profile attacks later targeted DNS provider Dyn and Lonestar Cell, a Liberian telecom.
- In early 2017, the actors surrounding Mirai came to light as the Mirai author was identified.

Source

- Antonakakis, Manos, et al. "Understanding the mirai botnet." *26th USENIX security symposium (USENIX Security 17)*. 2017.

MANCHESTER 1824
The University of Manchester

Mirai lifecycle

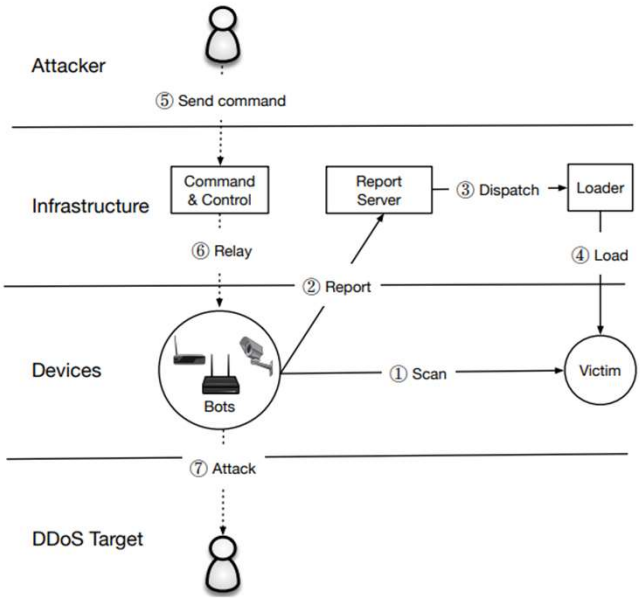
Infection

1. Scan
2. Report
3. Dispatch
4. Load

Hide

Attack

5. Send command
6. Relay
7. Attack



6

Infection phase

1. Rapid scanning for IoT devices with open ports
   a) Brute-force login attempts – using 10 username and password pairs selected randomly from a pre-configured list of 62 credentials.
2. Report
   a) Send victim IP and associated credentials to a hardcoded report server
3. Dispatch
   a) Log-in and determine system environment
4. Load
   a) architecture-specific malware installation

Hide phase

a) obfuscating its process name
b) terminating other processes on the port as well as competing infections on the device
c) constantly listening for commands while scanning for new victim devices.

Attack phase

5. Send command
6. Relay
7. Attack

Source

- Antonakakis, Manos, et al. "Understanding the mirai botnet." *26th USENIX security symposium (USENIX Security 17)*. 2017.

MANCHESTER 1824
The University of Manchester

Targeted / Infected IoT devices

Targeted Devices

Source Code Password List

Device Type	# Targeted Passwords	Examples
Camera / DVR	26 (57%)	dreambox, 666666
Router	4 (9%)	smcadmin, zte521
Printer	2 (4%)	00000000, 1111
VOIP Phone	1 (2%)	54321
Unknown	13 (28%)	password, default

Infected Devices

HTTPS banners

Device Type	# HTTPS banners
Camera / DVR	36.8%
Router	6.3%
NAS	0.2%
Firewall	0.1%
Other	0.2%
Unknown	56.4%

7

- A very good alignment of what Mirai is targeting and what is infecting

Source

- Antonakakis, Manos, et al. "Understanding the mirai botnet." *26th USENIX security symposium (USENIX Security 17)*. 2017.

MANCHESTER 1824
The University of Manchester

Motivation / target victim of Dyn attacks

Targeted IP	rDNS	Passive DNS
208.78.70.5	ns1.p05.dynect.net	**ns00.playstation.net**
204.13.250.5	ns2.p05.dynect.net	**ns01.playstation.net**
208.78.71.5	ns3.p05.dynect.net	**ns02.playstation.net**
204.13.251.5	ns4.p05.dynect.net	**ns03.playstation.net**
198.107.156.219	service.playstation.net	**ns05.playstation.net**
216.115.91.57	service.playstation.net	**ns06.playstation.net**

- Top targets are linked to Sony PlayStation
- Attacks on Dyn interspersed among attacks on other game services

8

- Dyn attack simultaneously attacked six IPs
- When you do reverse DNS lookup, you find that only four are related to Dyn infrastructure
- After using passive DNS data sets, it turns out that these IPs map to playstation name server infrastructure
- Perhaps the attack was gaming-related motivated, and the real target was Sony playstation, but Dyn was just the unintended casualty of the attack

Source

- Antonakakis, Manos, et al. "Understanding the mirai botnet." *26th USENIX security symposium (USENIX Security 17)*. 2017.

MANCHESTER 1824
The University of Manchester

Do not use default passwords

Username	Password
root	xc3511
root	vizxv
root	admin
admin	admin
root	888888
root	xmhdipc
root	default
root	juantech
root	123456
root	54321
support	support
root	(none)
admin	password
root	root
root	12345
user	user
admin	(none)
root	pass
admin	admin1234
root	1111
admin	smcadmin

Username	Password
admin	1111
root	666666
root	password
root	1234
root	klv123
Administrator	admin
service	service
supervisor	supervisor
guest	guest
guest	12345
guest	12345
admin1	password
administrator	1234
666666	666666
888888	888888
ubnt	ubnt
root	klv1234
root	Zte521
root	hi3518
root	jvbzd
root	anko

Username	Password
root	zlxx.
root	7ujMko0vizxv
root	7ujMko0admin
root	system
root	ikwb
root	dreambox
root	user
root	realtek
root	0
admin	1111111
admin	1234
admin	12345
admin	54321
admin	123456
admin	7ujMko0admin
admin	1234
admin	pass
admin	meinsm
tech	tech

9

We need to take lessons from desktop/web security

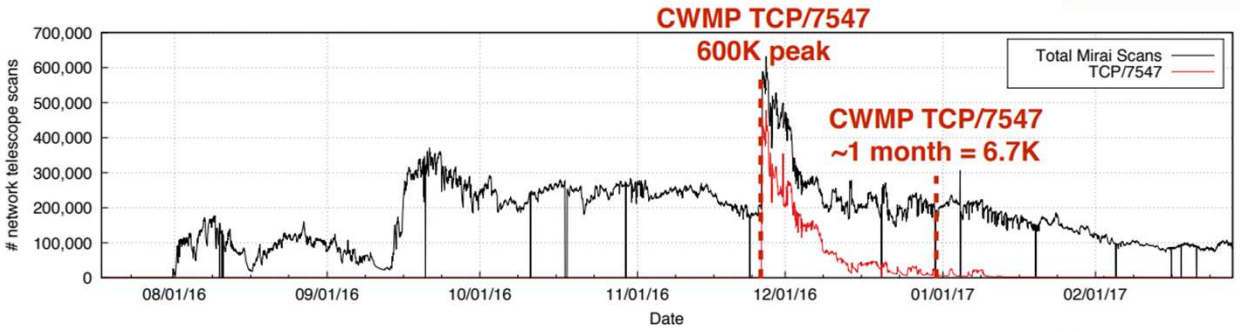
- Close open ports that are not being used
- Require secure and no-default passwords

Source

- Antonakakis, Manos, et al. "Understanding the mirai botnet." *26th USENIX security symposium (USENIX Security 17)*. 2017.

MANCHESTER 1824
The University of Manchester

Use automated updates



10

IoT systems could benefit from automated updates

- Example of the effect of rapid patching by telecoms

Source

- Antonakakis, Manos, et al. "Understanding the mirai botnet." *26th USENIX security symposium (USENIX Security 17)*. 2017.

MANCHESTER 1824
The University of Manchester

DDoS in IoT: Other botnets

Lua Botnet

- The first IoT botnet written in the Lua programming language was reported by MalwareMustDie* in late August 2016.
- So far this malware has targeted Linux-based cable modems using ARM CPUs.
- This botnet uses sophisticated features such as an encrypted C&C communication channel and customized IP tables rules

* blog.malwaremustdie.org/2016/09/mmd-0057-2016-new-elf-botnet-linuxluabot.html

Source:

- Kolias, Constantinos, et al. "DDoS in the IoT: Mirai and other botnets." Computer 50.7 (2017): 80-84. https://doi.org/10.1109/MC.2017.201

MANCHESTER 1824
The University of Manchester

DDoS in IoT: Other botnets

Hajime Botnet

- The Hajime botnet, discovered in October 2016 by Rapidity Networks [1], uses a method of infection similar to that of Mirai.
- Unlike Miriai which uses a centralized architecture, Hajime relies on fully distributed communications
- This botnet makes use of the BitTorrent DHT (distributed hash tag) protocol for peer discovery and the uTorrent Transport Protocol for data exchange
- A report [2] published in 2017 claim that this botnet has had infected 300,000 devices

1: http://security.rapiditynetworks.com/publications/2016-10-16/hajime.pd f
2: https://securelist.com/hajime-the-mysterious-evolving-botnet/78160/

12

Source:

- Kolias, Constantinos, et al. "DDoS in the IoT: Mirai and other botnets." Computer 50.7 (2017): 80-84. https://doi.org/10.1109/MC.2017.201
- https://www.theregister.co.uk/2017/04/27/hajime_iot_botnet/

MANCHESTER 1824
The University of Manchester

DDoS in IoT: Other botnets

Bashlite Botnet

- BASHLITE (also known as Gafgyt, Lizkebab, Qbot, Torlus and LizardStresser) is another malware botnet which target Linux based systems and launches DDoS attacks
- Infected devices connect to the command and control server and receive commands to launch DDoS attacks
- Mirai is more sophisticated and advanced as compared to Bashlite in launching DDoS attacks

13

Source:

- A. Marzano et al., "The Evolution of Bashlite and Mirai IoT Botnets," 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, 2018, pp. 00813-00818. https://ieeexplore.ieee.org/abstract/document/8538636

MANCHESTER 1824
The University of Manchester

DDoS in IoT: Other botnets

Why botnets are targeting IoT devices?

There are five main reasons IoT devices are particularly advantageous for creating botnets

- Constant and unobtrusive operation
- Weak security
- Poor maintenance
- Considerable attack traffic
- Noninteractive or minimally interactive user interfaces.

IoT vendors should provide the automated security updated to its devices

14

- Constant and unobtrusive operation: Unlike laptop and desktop computers, which have frequent on–off cycles, many IoT devices such as webcams and wireless routers operate 24/7 and in many cases aren't properly recognized as computing devices and thus not monitored frequently.
- Feeble protection: In their rush to penetrate the IoT market, many device vendors neglect security in favour of user-friendliness and usability.
- Poor maintenance: Most IoT devices fall under the setup-and-forget umbrella—after initially setting them up, users and network administrators forget about them unless they stop working properly.
- Considerable attack traffic: Contrary to common belief, IoT devices are powerful enough and well situated to produce DDoS attack traffic comparable to that of modern desktop systems.
- Noninteractive or minimally interactive user interfaces: Because IoT devices tend to require minimum user intervention, infections are more likely to go unnoticed. Even when they're noticed, there's no easy way for the user to address them short of replacing the device.

Source:

- Kolias, Constantinos, et al. "DDoS in the IoT: Mirai and other botnets." Computer 50.7 (2017): 80-84. https://doi.org/10.1109/MC.2017.201

MANCHESTER 1824
The University of Manchester

Summary

- Sophisticated Mirai variants and imitators are targeting IoT device at an alarming rate
- These botnet malwares typically runs on multiple platforms and are usually lightweight enough to execute even in resource-constrained IoT devices
- The infection process in botnets is relatively simple which makes every vulnerable device a bot candidate.
- IoT vendors should provide the automated security updated to its devices