# The Research on IoT Botnet

## -- Use Mirai Botnet as an Example

Final Presentation

Internet of Things & Security (Seminar Technische Informatik)

Freie Universität Berlin

Fang Lin

22.06.2021

# Outline

# Part1:

# Introduction

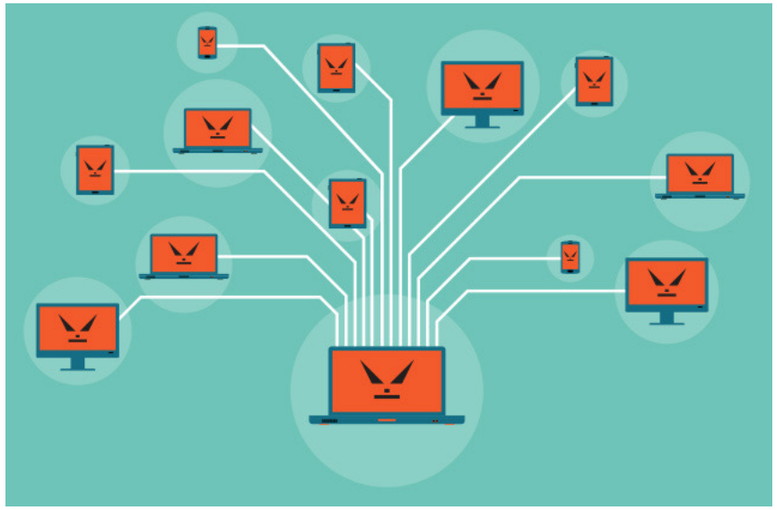
## Research Background

- The Internet of Things (IoT) is becoming an indispensable part of our daily lives, playing an increasingly important role in health, the environment, the family, the military and so on.

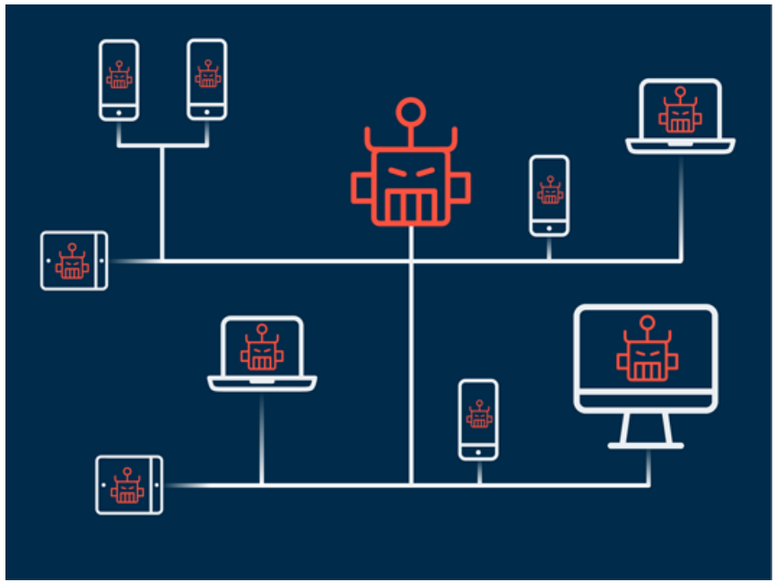
- The Internet of Things has grown tremendously in recent years. However, **IoT devices still suffer from basic security vulnerabilities**. **Hackers** use their computing and communication advantages to perform different types of attacks, **IoT botnet** is one of them.

- The IoT botnet is an important reason that makes IoT devices unable to operate normally and leads to network security issues such as the leakage of private information. IoT botnets mainly interfere with the operation of IoT devices by attacking DDoS.

- Looking back at the history of the IoT botnets invading the IoT devices**, a series of network security incidents have occurred in the economic, smart city and so one.** As a classic botnet, Mirai botnet is worthy of our in-depth research on botnets to explore the reasons for these things.



Source from:
https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.kaspersky.com%2Fblog%2Fbotnet%2F1742%2F&psig=AOvVaw33bsbQAcZXkbCmgVr15Cmv&ust=1620135906225000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCKCWxuPSrfACFQAAAAAdAAAAABAD



Source from:
https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.myrasecurity.com%2Fde%2Fbotnet%2F&psig=AOvVaw33bsbQAcZXkbCmgVr15Cmv&ust=1620135906225000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCKCWxuPSrfACFQAAAAAdAAAAABAJ

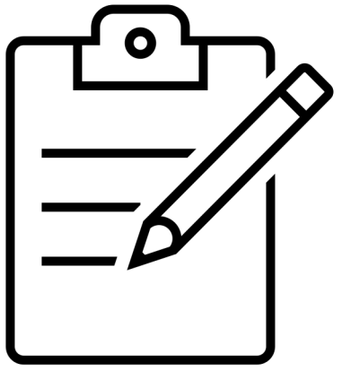
## Research Significance

- Since botnets are so harmful to IoT devices, it is worth studying to understand it and study how to prevent it.

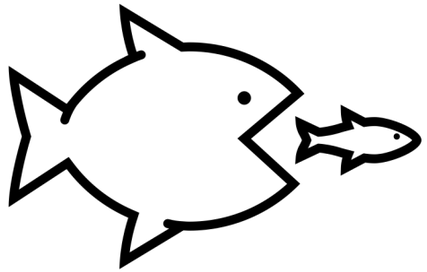
- On the one hand, through the analysis and research of the Mirai botnet, knowing hot it attacks, I can have a deeper understanding of the botnet and also have **a better understanding of the security issues of IoT devices**.

- On the other hand, by understanding how to prevent the infringement of botnets, I can also **improve my awareness of prevention the IoT attacks when using IoT devices.**

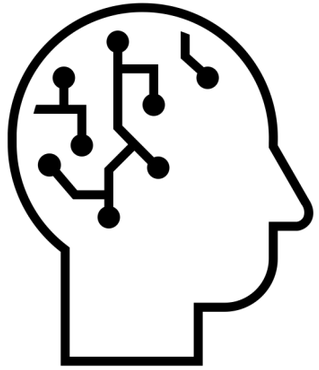
**What is it?**



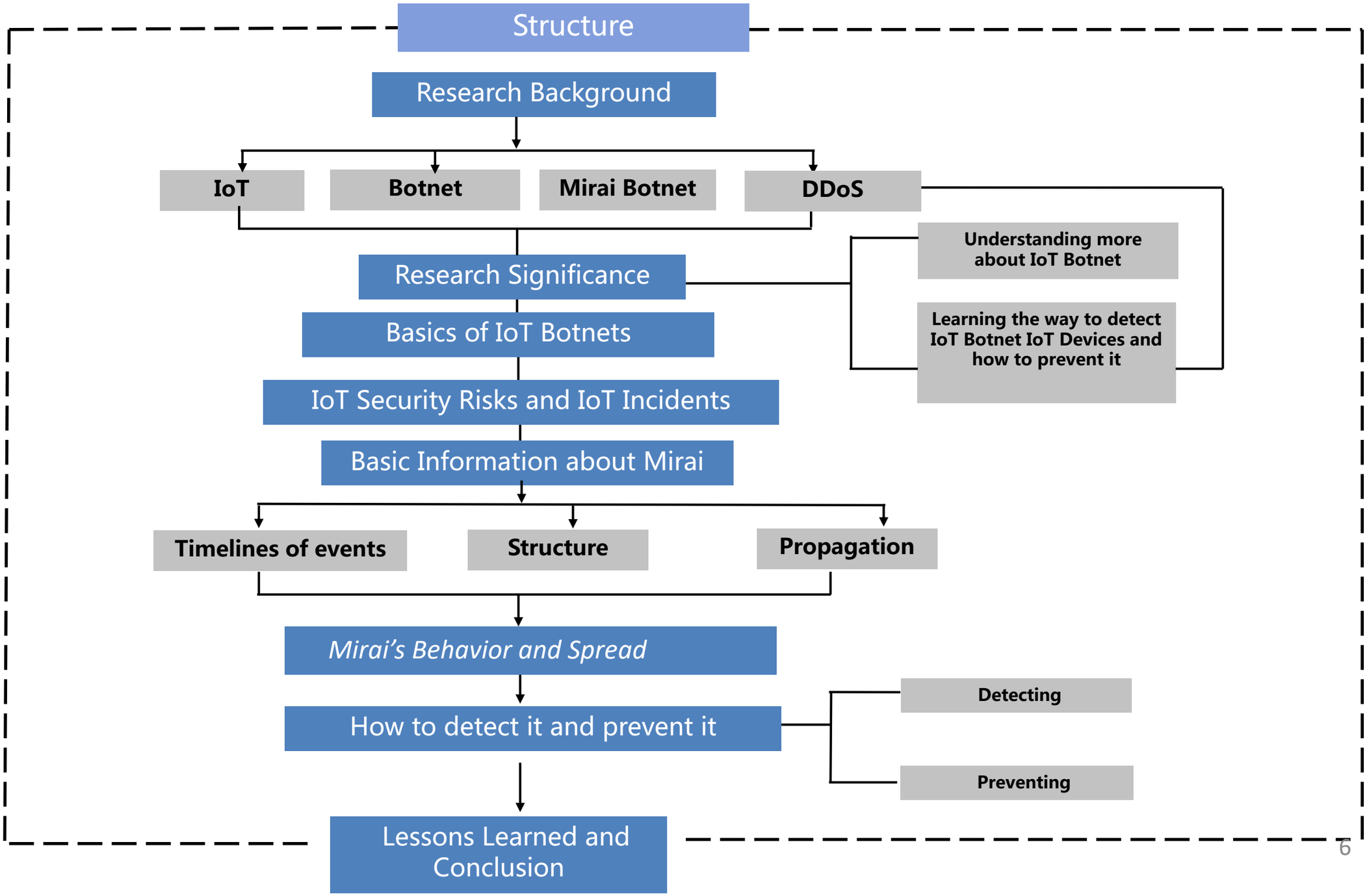
**How it attacks?**



**How to detect and prevent it?**



## Structure


Structure
Research Background
IoT
Botnet
Mirai Botnet
DDoS
Research Significance
Understanding more about IoT Botnet
Learning the way to detect IoT Botnet IoT Devices and how to prevent it
Basics of IoT Botnets
IoT Security Risks and IoT Incidents
Basic Information about Mirai
Timelines of events
Structure
Propagation
Mirai's Behavior and Spread
How to detect it and prevent it
Detecting
Preventing
Lessons Learned and Conclusion

# Part2:

# Basics of IoT Botnet

## IoT Botnet Structure

The left part includes attackers, clients, and targets which are easy to understand.

– **Attackers**

Attackers are those who try to attack the IoT devices to gain profits.

– **Clients**

Clients are the groups who bought IoT devices and use them as a part of normal life, in the context they are also the victims.

– **Targets**

Targets are the IoT devices which suffered from the attacks from the attackers and then the information of the clients may be exposed.

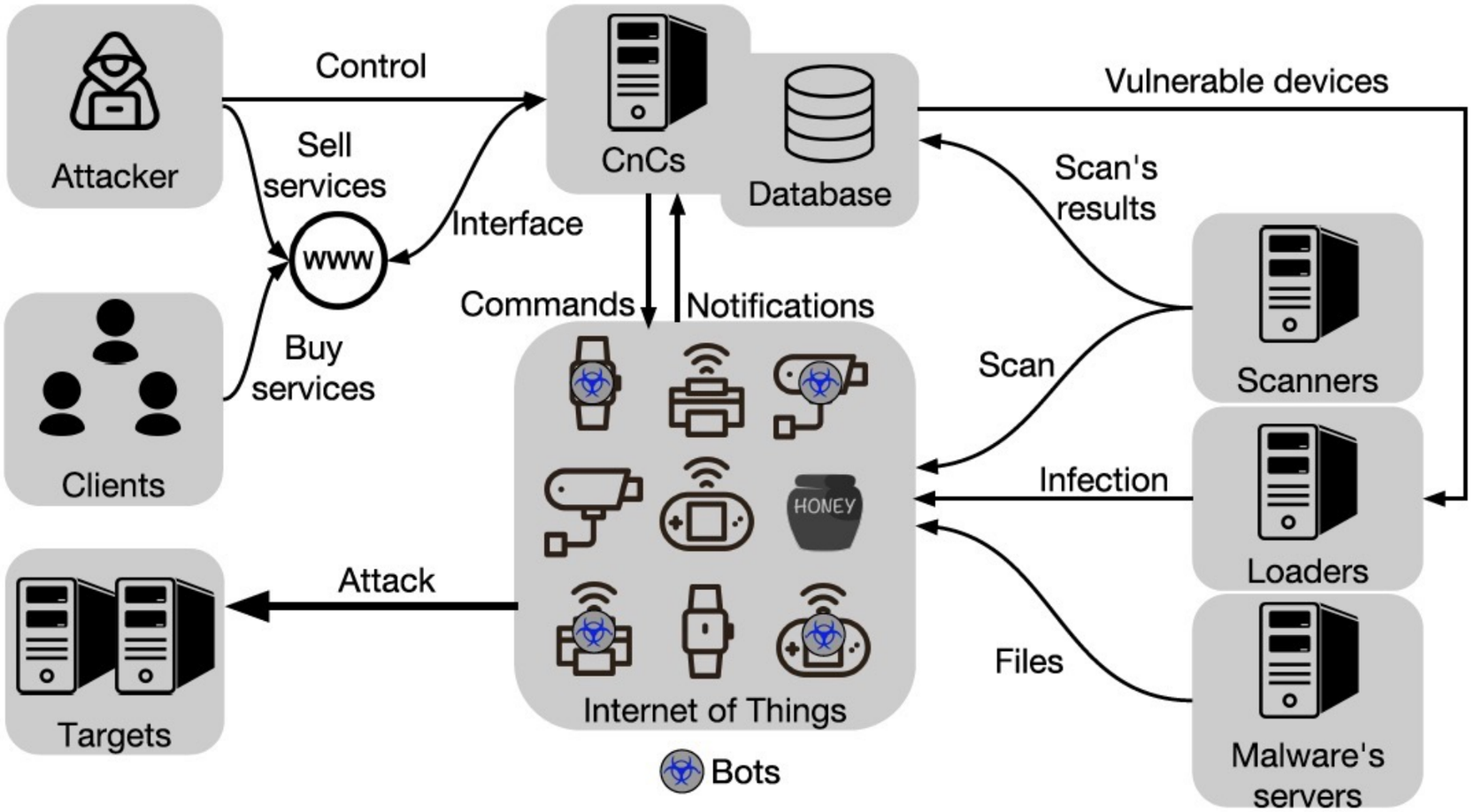



Figure: Overview of an IoT Botnet [3]

## IoT Botnet Structure

The center part includes three domains, which are CnCs, Database and Bots, these should be explained more detailed in the following.

– **CnCs**

Command and control servers (C&C) are the operators' interface to the botnet. C&Cs receive commands from operators and maintain connections with infected devices to broadcast commands. [3]

– **Database**

Database (potentially distributed) stores information collected by the botnet, e.g., active bots and scan results. [3]

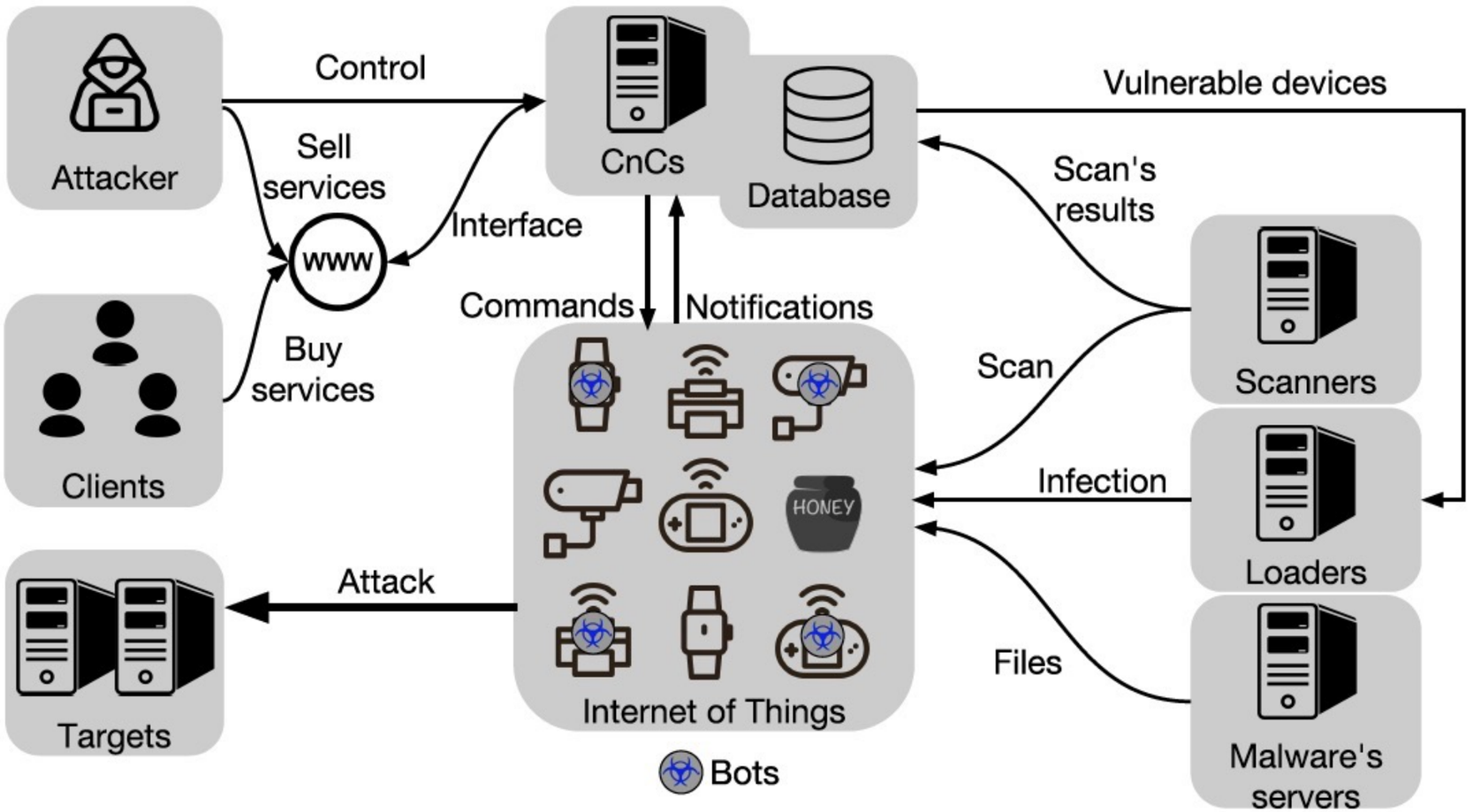



Figure: Overview of an IoT Botnet [3]

– **Bots**

Bots are infected devices that are part of the botnet. Bots report their state to C&Cs and execute the received commands. [3]

## IoT Botnet Structure

In the right part there are scanners, loaders and malware's servers.

**– Scanners**

Scanners probe devices to find telnet and SSH servers to attempt login and identify vulnerable devices. [3]

**– Loaders**

Loaders login to vulnerable devices to download and run the botnet malware, creating a new bot. [3]

**– Malware's servers**

Malware servers host resources used by the botnet such as shell scripts and executable binaries. [3]

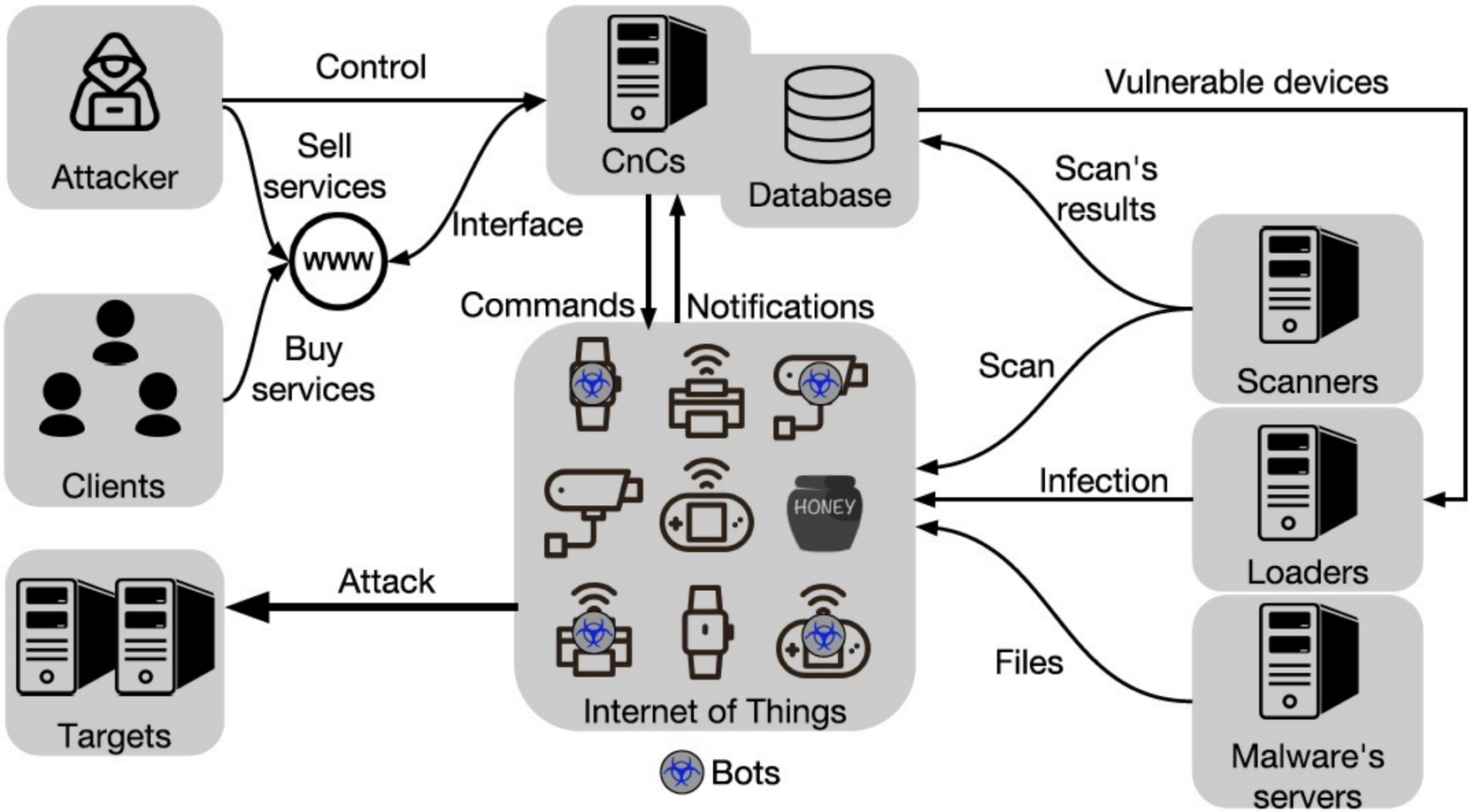



Figure: Overview of an IoT Botnet [3]

## IoT Botnet Structure

How will IoT devices be infected?

– **The scanner first** identifies vulnerable devices and reports to the central database.

– **The loader then** connects to the vulnerable device to download and run the malware. During the infection process, the loader accesses the server to download and run the malware binary file on the vulnerable device.

– **Once infected**, the bot will connect to the C&C of the botnet and wait for commands. To prevent subsequent infection attempts from other botnets, the IoT botnet disables the telnet and SSH services of the infected device.

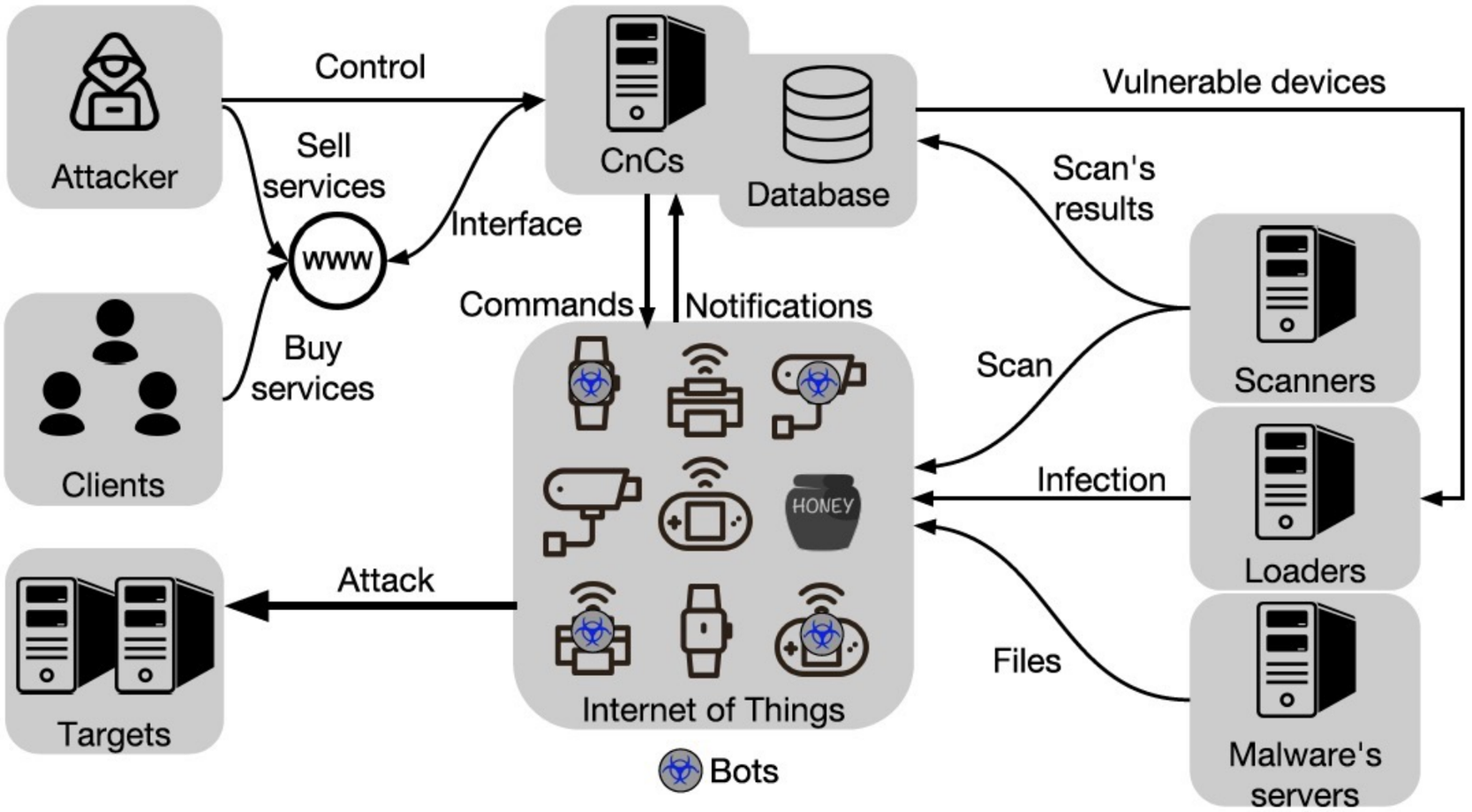



Figure: Overview of an IoT Botnet [3]

– Finally, **operators may sell botnet** services (for example, denial of service attacks), which are usually accessible through the client's web interface

## Different IoT Botnets

- The **first IoT botnet written in the Lua programming language was reported by MalwareMustDie** in late August 2016.

- **The Hajime botnet**, discovered in October 2016 by Rapidity Networks, uses a method of infection similar to that of Mirai. [6]

- **A BusyBox-based IoT botnet like Mirai, BrickerBot** was unearthed by Radware researchers in April 2017.
  - **Mirai** is one of the most predominant DDoS IoT botnet in recent times. Mirai means ”the future” in Japanese.

- **Linux/IRCTelnet is a new IRC botnet ELF malware** aimed at IoT devices with IPv6 capabilities.

# Part3:

# IOT SECURITY RISKS AND IOT INCIDENTS

## IoT Security Risks

| Vulnerability | Examples |
|---|---|
| Insecure web/mobile/cloud interface | Inability to change default usernames and passwords; weak passwords; lack of robust password recovery mechanisms; |
| Insufficient authentication/ authorization | Privilege escalation; lack of granular access control Insecure |
| Insecure network services | Vulnerability to denial-of-service, buffer overflow, and fuzzing attacks; network ports or services unnecessarily exposed to the Internet |
| Lack of transport encryption/ integrity verification | Transmission of unencrypted data and credentials |
| Privacy concerns | Collection of unnecessary user data; exposed personal data; insufficient controls on who has access to user data; |
| Insecure software/ firmware | Lack of secure update mechanism; update files not encrypted; update files not verified before upload; |
| Poor physical security | Device easy to disassemble; access to software via USB ports; removable storage media |

Table: COMMON INTERNET OF THINGS VULNERABILITIES. [10]

## Some Incidents of IoT caused by Botnets

| Incident | What happened |
|---|---|
| KrebsOnSecurity.com | On the evening of September 30, 2016, the blog of security researcher Brain Krebs experienced a 623Gbps DDoS attack from a large number of infected IoT devices [17]. **Mirai and BASHLITE attack** infected these IoT devices. |
| OVH | On September 22, 2016, OVH founder and CTO Octave Klaba posted the news and screenshots on his Twitter account, explaining that the OVH server is undergoing a series of DDoS attacks. **The attack is suspected to come from IoT devices infected with Mirai and BASHLITE malware.** |
| Dyn | On October 21, 2016, Dyn suffered a DDoS attack on its hosted DNS server from 100,000 Internet-enabled IoT devices (such as printers, IP cameras, residential gateways, and baby monitors), it is responsible from **Mira.** |
| Deutsche Telekom | It was discovered that the root cause of the problem **was the new Mirai malware variant**, which tried to actively scan and infect vulnerable devices in order to expand the number of infected devices in its botnet. |
| Liberia | In early November, the @MiraiAttacks Twitter account observed an attack on Liberia's telecommunications infrastructure by the **Mirai IoT botnet.** |
| CCTV vs Small Business Websites | A DDoS attack exploited thousands of websites like small jewelry shop websites. |
| Lappeenranta | In Lappeenranta, two housing blocks experienced disruption of heating distribution, which was due to DDoS attack by the **Mirai botnet**. |
| Russian Banks | At least 5 Russian banks experienced a DDoS attack. |
| US Elections | DDoS attacks were observed on the campaign website of Donald Trump and Hillary Clinton . |

# Part4:

# Basics of Mirai Botnet

## Timeline of events

From the figure under, we see that

- on August 1, 2016, Mirai's surfaces were released.
- Mirai's first attack was on September 18, 2016, which was OVH attacks.
- On the 21st, it attacked DNS provider Dyn.
- During the two attacks, the source code was released on the Internet.
- At the end of November, it exploited the vulnerability of Deutsche Telekom CWMP.
- On January 18, 2017, the author of Mirai was confirmed and arrested at the end of February of the same year.

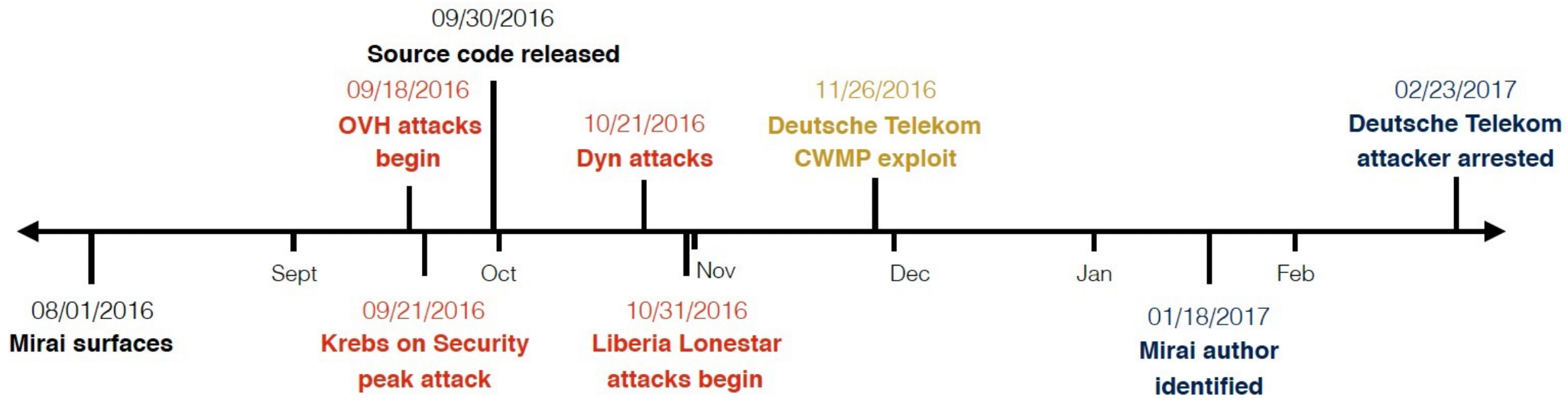



Figure: Timeline of events of Mirai [1]

## The Structure and Propagation of Mirai Botnet

**The Structure of Mirai Botnet:** Compare to figure in 2.2, the components of the structure of Mirai Botnet are almost the same, except there is a **report server** of mirai botnet structure.
- Report Server is a server which Bots will report the victim IP address to it. In the figure right, four layers are designed to describe the mirai botnet structure.

➢ Attacker

The same as in figure 2, it's the hackers who want to attack the IoT devices.

➢ Infrastructure

In Infrastructure Layer, there are three components, C&C, Report Server and Loader.

➢ Devices

The Devices layer is made of bots and victim, the victim here is the victim IoT device.

➢ DDoS Target

Easy to understand, it's the clients of an IoT devices, which their devices are attacked by Mirai Botnet.

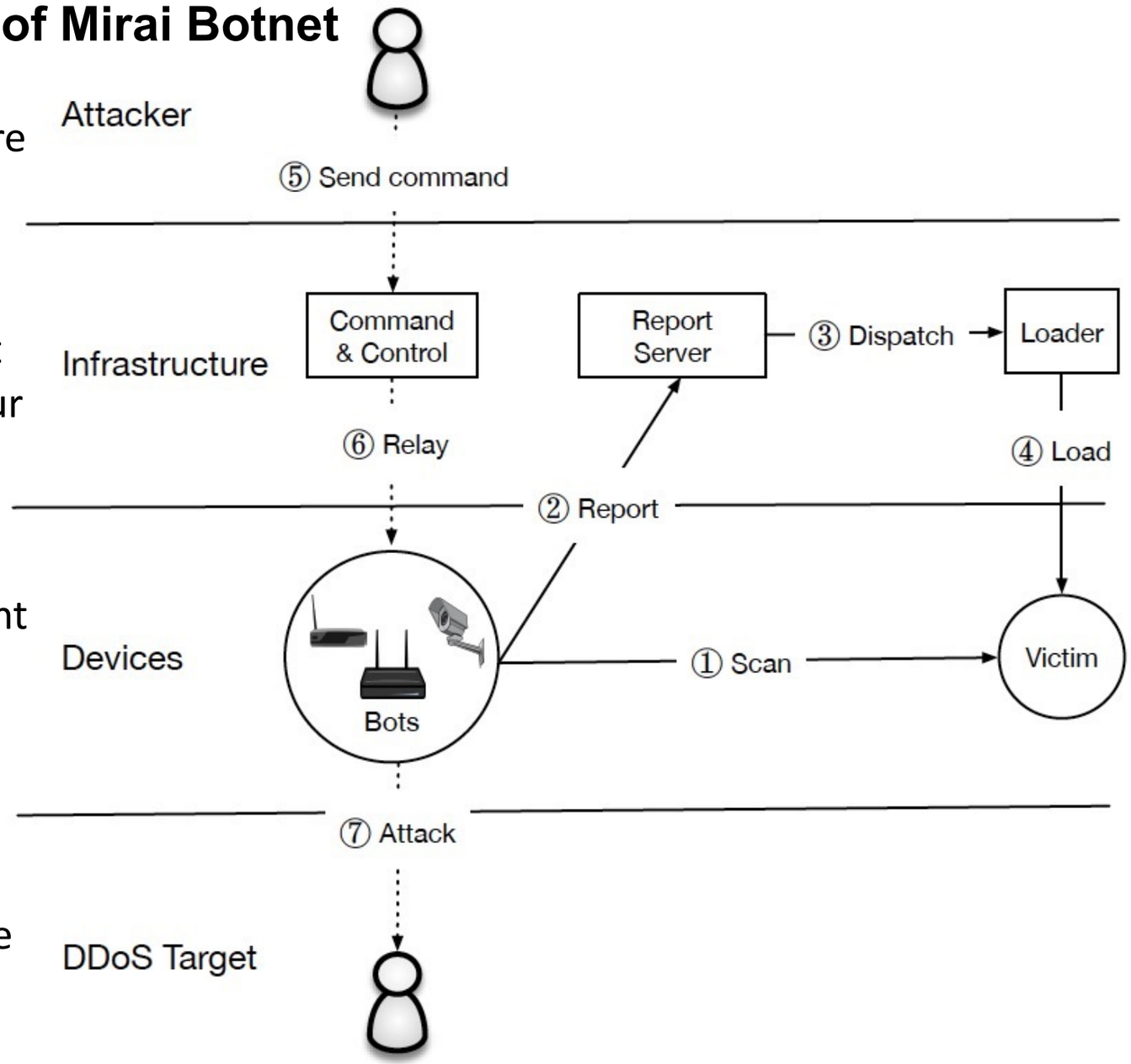



Figure: Overview of an Mirai IoT Botnet [1]

## The Structure and Propagation of Mirai Botnet

**The Propagation of Mirai Botnet:** As we can see in figure right, there are 7 phases about the propagation of Mirai Botnet.

- Phase 1

Mirai spread by first entering a rapid scanning phase 1 where it asynchronously and "statelessly" sent TCP SYN probes to pseudorandom IPv4 addresses, excluding those in a hard-coded IP blacklist, on Telnet TCP ports 23 and 2323 (hereafter denoted TCP/23 and TCP/2323).

If Mirai identifies a potential victim, it entered into a brute-force login phase in which it attempted to establish a Telnet connection using 10 username and password pairs selected randomly from a pre-configured list of 62 credentials. [1]

- Phase 2

At the first successful login, Mirai sent the victim IP and associated credentials to a hardcoded report server.

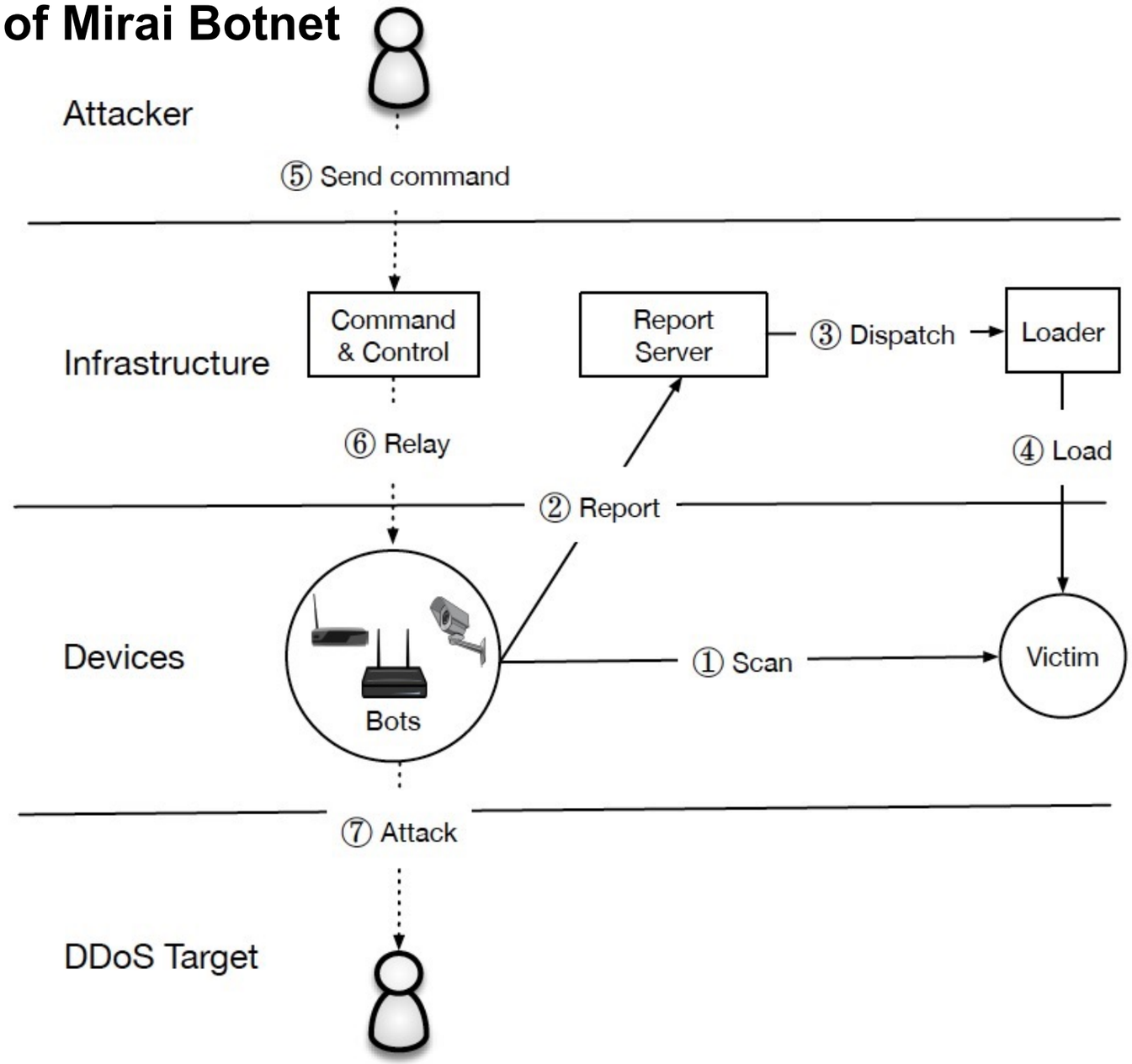



Figure: Overview of an Mirai IoT Botnet [1]

## The Structure and Propagation of Mirai Botnet

**The Propagation of Mirai Botnet:** As we can see in figure right, there are 7 phases about the propagation of Mirai Botnet.

- Phase 3

A separate loader program asynchronously infected these vulnerable devices by logging in, determining the underlying system environment.

- Phase 4

And at the end this separate loader program infected the devices by downloading and executing architecture-specific malware.

- Phase 5

The attackers will send the command to C&C services.

- Phase 6

The C&C services relay the instruction from the attacker to certain bots.

- Phase 7

At the end, the bots will attack the DDoS Target.

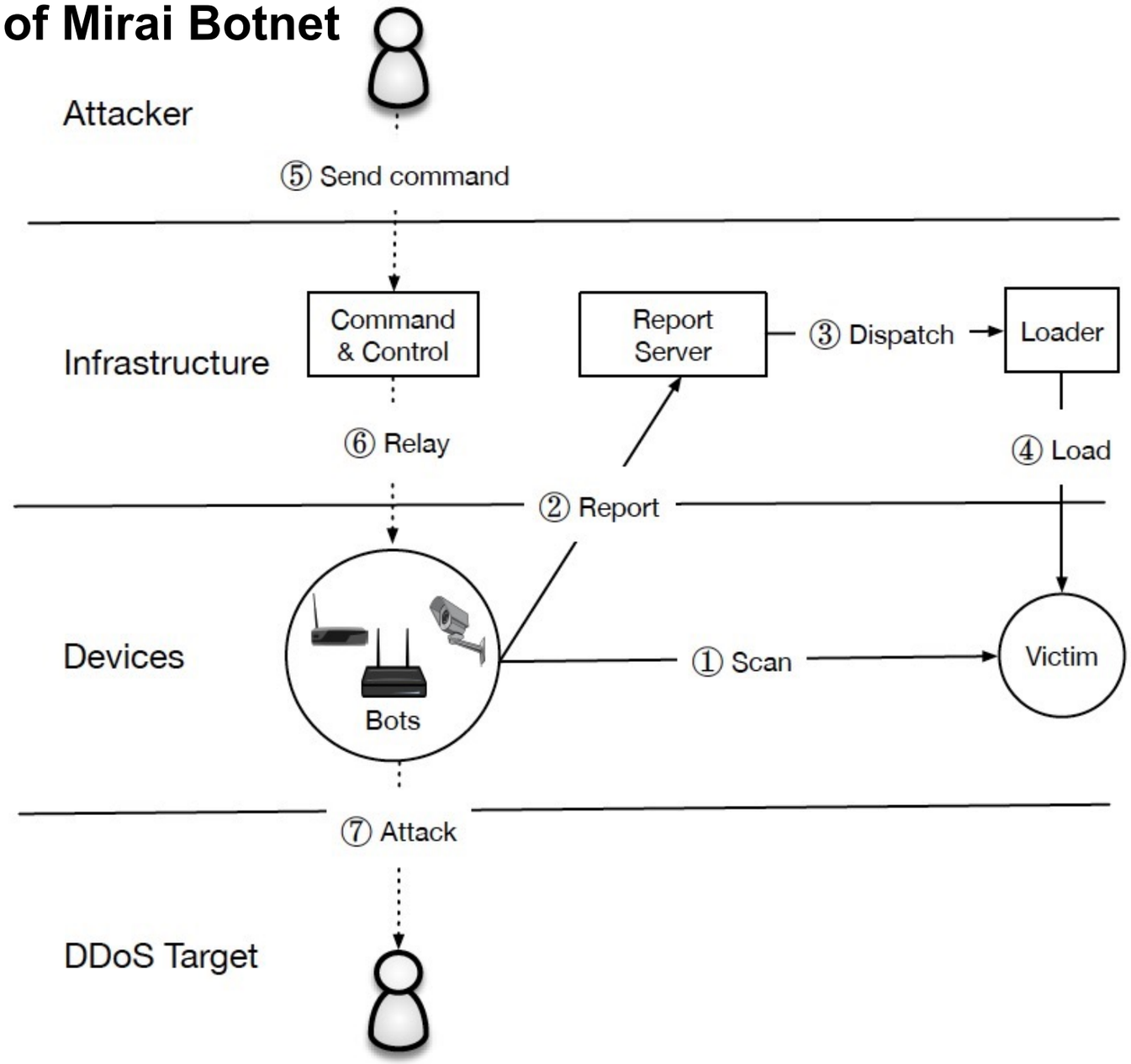



Figure: Overview of an Mirai IoT Botnet [1]

# Part5:

# Mirai’s Behaviour and Spread

## Behaviour

### ➢ Network Telescope

Mirai's indiscriminate, rapid scanning strategy lends itself to tracking the botnet's propagation to new hosts. The authors [1] monitored all network requests to a network telescope composed of 4.7 million IP address operated by Merit Network over a seven month period from July 18, 2016 to February 28, 2017.

On average, the **network telescope received 1.1 million packets from 269,000 IP addresses per minut**e during this period.

### ➢ Active Scanning

In order to determine the manufacturer and model of devices infected with Mirai, the authors[1] leveraged Censys, which actively scans the IPv4 space and aggregates application layer data about hosts on the Internet.

A conclusion is that **devices with open services that are not closed by Mirai (e.g., HTTPS and FTP) can appear repeatedly in Censys banner scans during our measurement window** (due to churn) and thus lead to **over counting** when compared across protocols.

### ➢ Telnet Honeypots:

In order to track the evolution of Mirai's capabilities, the authors[1] collected binaries installed on a set of Telnet honeypots that masqueraded as vulnerable IoT devices. At the end they extracted the set of logins and passwords, IP blacklists, and C2 domains from these binaries**, identifying 67 C2 domains and 48 distinct username/password dictionaries (containing a total 371 unique passwords).**

## Behaviour

### ➢ Passive & Active DNS

Following the public release of Mirai's source code, competing Mirai botnet variants came into operation. the authors [1] disambiguated ownership and estimate the relative size of each Mirai strain by exploring passive and active DNS data for the 67 C2 domains that they found by reverse engineering Mirai binaries. They also leveraged our DNS data to map the IP addresses present in attack commands to victim domain names. **In total, 33 unique DNS clusters of Mirai Botnet are identified.**

### ➢ Attack Commands

The authors[1]note that a naive analysis of attack commands overestimates the volume of attacks and targets: individual C2 servers often repeat the same attack command in rapid succession, and multiple distinct C2 servers frequently issued the same command.

### ➢ DDoS Attack Traces

For Google Shield, The authors[1] shared a list of IP addresses observed by they network telescope and in turn **received aggregate statistics on what fraction matched any of 158.8K IP addresses involved in a 1-minute Mirai HTTP-flood attack** on September 25, 2016.

## Spread

### ➢ Bootstrapping

Mirai's comparatively modest initial growth may be due to the low bandwidth and computational resources of infected devices, **a consequence of the low-accuracy, brute-force login using a small number of credentials, or simply attributable to a bottleneck in loader infrastructure.**

### ➢ Steady State Size

**A**n **initial steady state** of 200,000–300,000 infections in September 2016; **a peak** of 600,000 infections at the end of November 2016; **and a collapse** to roughly 100,000 infections at the end of our observation window in late February 2017. \

### ➢ Global Distribution

As the right figure shows, most Mirai infections originate from Located in Brazil (15.0%), Colombia (14.0%) and Vietnam (12.5%)

### ➢ Device Composition and Device Bandwidth

- Device Composition: The devices they identified were primarily network-attached storage appliances, home routers, cameras, DVRs, printers, and
- Device Bandwidth: Mirai was primarily powered by devices with limited computational capacity and/or located in regions with low bandwidth.

| Country | Mirai Infections | Mirai Prevalence | Telnet Prevalence |
|---|---|---|---|
| Brazil | 49,340 | 15.0% | 7.9% |
| Colombia | 45,796 | 14.0% | 1.7% |
| Vietnam | 40,927 | 12.5% | 1.8% |
| China | 21,364 | 6.5% | 22.5% |
| S. Korea | 19,817 | 6.0% | 7.9% |
| Russia | 15,405 | 4.7% | 2.7% |
| Turkey | 13,780 | 4.2% | 1.1% |
| India | 13,357 | 4.1% | 2.9% |
| Taiwan | 11,432 | 3.5% | 2.4% |
| Argentina | 7,164 | 2.2% | 0.2% |

Figure: Geographic Distributiontai [1]

# Part6:

# Detection and Prevention

## Detection

| Approach | Description |
|---|---|
| Anomaly-based | This approach detects IoT botnet by recognizing malicious behavior in the network; this approach requires storing previous profile for the normal behavior for the network. |
| Signature-based | This approach detects the IoT botnet based on the signature of the botnet stored in the database of the system. |
| Specification-based | This approach is similar to anomaly-based approach but it takes into account system specifications. |
| Hybrid-based | This approach combines two approaches together, anomaly-based and signature-based techniques or anomaly-based and specification-based techniques, to detects the IoT botnet with high detection and low false positive rate. |
| A novel graph-based approach | In paper [5], they propose a lightweight method for detecting IoT botnet, which based on extracting high-level features from function–call graphs, called PSI-Graph, for each executable file. |
| Botnet detection systems using DNS queries | - String similarity detection [13]<br>-DGA detection based deep learning [13] |
| one class support vector machine and Grey Wolf optimization for IoT botnet detection [12] | In this paper, a new unsupervised evolutionary IoT botnet detection method is proposed. The main contribution of the proposed method is to detect IoT botnet attacks launched form compromised IoT devices by exploiting the efficiency of a recent swarm intelligence algorithm called Grey Wolf Optimization algorithm (GWO) to optimize the hyperparameters of the OCSVM and at the same time to find the features that best describe the IoT botnet problem. |

## Prevention

| Method | Description |
|---|---|
| Protection Techniques | ➢ ensuring that all default passwords are changed to strong passwords;<br>➢ updating IoT devices with security patches;<br>➢ disabling Universal Plug and Play (UPnP) on router unless absolutely necessary;<br>➢ monitoring IP ports /TCP and /TCP for attempts to gain unauthorized control over IoT devices using the network terminal (Telnet)<br>➢ monitoring for anomalous traffic on port , as infected devices often attempt to spread malware by using this port to send results to the threat actor.<br>➢ specific end-user actions such as only acquiring IoT devices from companies with a good security reputation and understanding the devices' communication capabilities, as they're at higher risk of malware infection. |
| Longer-Term IoT Security Strategy | ➢ **Preventing bot infection** is the most effective defence measure.<br>➢ It is important to **monitor network and device behavior** for abnormal events or trends that may indicate threats.<br>➢ **Users** can also take a more active role in threat detection by reporting typical machine infection signs.<br>➢ If signs of a potential DDoS attack or infected machine are detected**, prompt response is essential to minimize damage and prevent the spread of malware.**<br>➢ Deploying these various defences won't be trivial given the large number of IoT devices and their inherent vulnerabilities.<br>➢ **Devising methods** for discovering, identifying, and monitoring IoT devices is also critical.<br>➢ The security strategy must also include a **thorough risk assessment.** |

# Part7:

# Lessons Learned and Conclusion

## Lessons Learned

- Thus, in the IoT side, more **research is required to study the vulnerability of IoT devices** and networks, and to protect them against cyber attacks. [11]

- The **huge impact of Mirai, its variants, and other botnet like DDoS attacks highlights** the risks that IoT devices pose to the Internet.
- The Mirai botnet shows that **even a simple dictionary attack can compromise hundreds of thousands of connected devices.**
- **Automatic updates** — which have become the norm in the desktop and mobile operating systems world — provide developers with a timely mechanism to fix bugs and vulnerabilities without burdening consumers with maintenance tasks or requiring recalls.

  - Automatic updates **require a modular software architecture** to safely cover core modules with rollback capabilities in the event
of a failure.

  - They also **need encryption primitives** for resource-constrained devices and build PKI infrastructure to support trusted updates.

- IoT manufacturers **can use a unified way to identify the network model and firmware versi**on—for example, by encoding them into a part of the device's MAC address.
- The IoT ecosystem also includes many different participants, each of which performs security-related functions-assigning identifiers to IoT devices, patching device software, and so on. **Tracking information, such as device keys and who is responsible for which.**
- The impacts of **significant customization** of the botnet was not studied, and might be a topic for future research, although such customizations may be numerous and difficult to predict. [7]

## Conclusion

This research is based on the Internet of Things botnet and has studied many aspects.

- Starting from the basic concepts, I first understand the basic structure and attack methods of IoT,
- and then introduce some classic IoT accidents.
- Many of these events are related to the Mirai botnet, which is one reason why I plan to focus on the Mirai botnet.
- By introducing the timeline of the Mirai botnet and its basic structure, comparing its spread with the Iot Botnet, and observing its behavior and spread through some data, we have a clearer concept of the Mirai botnet.
- Then, through a brief introduction of some methods of detecting IoT botnets, to understand what forms of detection are available, this section does not provide a more in-depth introduction, such as the development of a certain method.
- Then, I put forward some preventive measures and strategies, and finally discussed the lessons learned, mainly for some of the more important features and the work to be done in the future.

Through this extensive research and focus on understanding Mirai Botnet, I have a deeper understanding of IoT botnet. IoT devices have some vulnerabilities that are easy to be attacked. IoT botnet is not the only attack method. In the future, I may be interested in reading some articles on IoT device security to conduct more in-depth research on IoT security, and a more in-depth study of some technical aspects of detection methods which is not that comprehensive in this article, like machine learning, deep learning technics for the Botnet detection.

# References

## References

[1].Manos Antonakakis, Georgia Institute of Technology; Tim April, Akamai; Michael Bailey, University of Illinois, Urbana-Champaign; Matt Bernhard, University of Michigan, Ann Arbor; Elie Bursztein, Google; Jaime Cochran, Cloudflare; Zakir Durumeric and J. Alex Halderman, University of Michigan, Ann Arbor; Luca Invernizzi, Google; Michalis Kallitsis, Merit Network, Inc.; Deepak Kumar, University of Illinois, Urbana-Champaign; Chaz Lever, Georgia Institute of Technology; Zane Ma and Joshua Mason, University of Illinois, Urbana-Champaign; Damian Menscher, Google; Chad Seaman, Akamai; Nick Sullivan, Cloudflare; Kurt Thomas, Google; Yi Zhou, University of Illinois, Urbana-Champaign.**Understanding the Mirai Botnet.** (2017)
URL:https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[2]. Kishore Angrishi. **Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets.** (2017)
URL: https://arxiv.org/pdf/1702.03681.pdf

[3]. Artur Marzano, David Alexander, O. Fonseca, E. Fazzion, C. Hoepers, Klaus Steding-Jessen, M. H. P. Chaves, Ítalo S. Cunha, D. Guedes, W. Meira .**The Evolution of Bashlite and Mirai IoT Botnets.** 2018 IEEE Symposium on Computers and Communications (ISCC)
URL: https://honeytarg.cert.br/honeypots/docs/papers/honeypots-iscc18.pdf

[4]. Basheer Al-Duwairi, Wafaa Al-Kahla, Mhd Ammar AlRefai, Yazid Abdelqader, Abdullah Rawash, Rana Fahmawi. **SIEM-based detection and mitigation of IoT-botnet DDoS attacks.** (2019) URL: https://www.researchgate.net/publication/340357755_SIEM-based_detection_and_mitigation_of_IoT-botnet_DDoS_attacks

[5]. Huy-Trung Nguyen, Quoc-Dung Ngo, Van-Hoang Le. **A novel graph-based approach for IoT botnet detection.** (2019)
URL: https://link.springer.com/article/10.1007/s10207-019-00475-6

[6]. Stephen Herwig, Katura Harvey, George Hughey, Richard Roberts, Dave Levin. **Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet.** (2019) URL: https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_02B-3_Herwig_paper.pdf

[7]. Xiaolu Zhang, Oren Upton, Nicole Lang Beebe, Kim-Kwang Raymond Choo. **IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers.** (2020) URL: https://www.sciencedirect.com/science/article/pii/S2666281720300214

## References - General

[8]. Constantinos Kolias, George Mason University, Georgios Kambourakis, University of the Aegean Angelos Stavrou, George Mason University Jeffrey Voas, IEEE Fellow. **DDoS in the IoT: Mirai and Other Botnets.** (2017)
URL: https://ieeexplore.ieee.org/document/7971869
[9]. Priscilla Moriuchi, Sanil Chohan. **Mirai-Variant IoT Botnet Used to Target Financial Sector in January 2018.** (2018)
URL: https://go.recordedfuture.com/hubfs/reports/cta-2018-0405.pdf
[10]. Elisa Bertino, Purdue University, Nayeem Islam, Qualcomm. **Botnets and Internet of Things Security.** (2017)
URL: https://ieeexplore.ieee.org/document/7842850
[11]. Saleh Soltan, Prateek Mittal, and H. Vincent Poor, Princeton University. **BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid.** (2018) URL: https://www.usenix.org/conference/usenixsecurity18/presentation/soltan
[12]. Amaal Al Shorman, Hossam Faris, Ibrahim Aljarah. **Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection.** (2019) URL: https://link.springer.com/article/10.1007/s12652-019-01387-y
[13]. Vinayakumar R, Mamoun Alazab Senior Member, IEEE, Sriram S, Quoc-Viet Pham, Soman KP, Simran K. **A Visualized Botnet Detection System based Deep Learning for the Internet of Things Networks of Smart Cities.** (2020)
URL: https://ieeexplore.ieee.org/document/8985278
[14] https://en.wikipedia.org/wiki/Denial-of-service attack
[15] https://en.wikipedia.org/wiki/Deep learning
[16] https://en.wikipedia.org/wiki/Internet of things
[17] B. Krebs. **"KrebsOnSecurity hit with record DDoS,"** in KrebsonSecurity. (2016).URL:
https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-withrecord-ddos/
[18] B. Krebs. **"Alleged vDOS Proprietors Arrested in Israel,"** in KrebsonSecurity. (2016).
URL: https://krebsonsecurity.com/2016/09/alleged-vdos-proprietorsarrested-in-israel/
[19] R. Millman. **"OVH suffers 1.1Tbps DDoS attack,"** in News, SC Magazine UK. (2016) URL: http://www.scmagazineuk.com/ovh-suffers-11tbps-ddosattack/article/524826/
[20] Ralf**. "Were 900K Deutsche Telekom Routers Compromised by Mirai?".** (2016). URL:
https://comsecuris.com/blog/posts/were_900k_deutsche_telekom_routers_compromised_by_mirai/
[21] B. Krebs. **"Did the Mirai Botnet really take Liberia Offline?,"** in KrebsonSecurity. 2016.
URL: https://krebsonsecurity.com/2016/11/did-the-mirai-botnet-reallytake-liberia-offline/

Thank you for your listening!