

# A Practical Analysis on Mirai Botnet Traffic

Getoar Galloopeni, Bruno Rodrigues, Muriel Franco, Burkhard Stiller

Universidade Federal do Ceará  
Campus Quixadá  
April 29, 2025

# Motivação do estudo

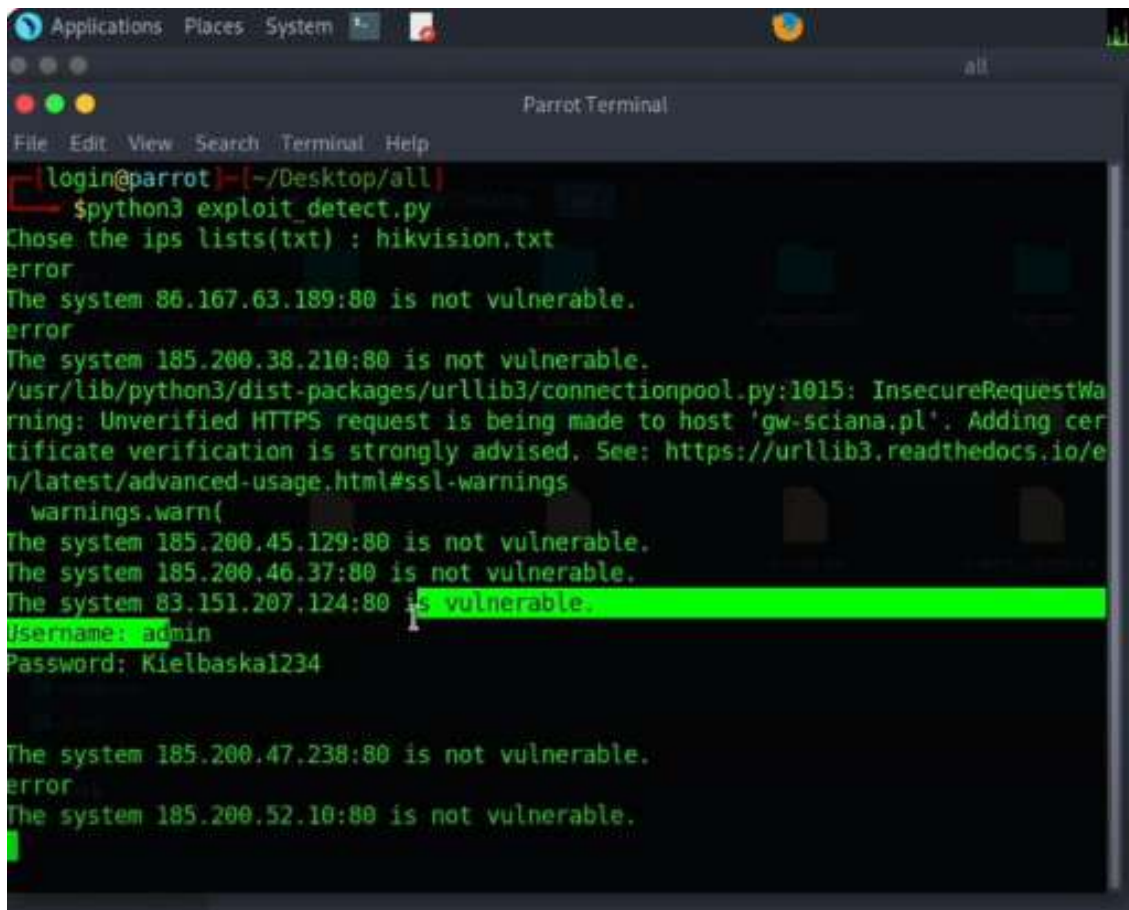
“Distributed Denial-of-Service (DDoS) attacks are one of the biggest threats to the availability of Internet services. Behind these attacks are Botnets, such as Mirai, which exploits default and weak security credentials to take control of the host and spreads itself to other devices.” – [Gallopeni, et al., 2020]

# O botnet Mirai

Dispositivos domésticos inteligentes, por buscarem conveniência, muitas vezes têm suas falhas de segurança ignoradas.

O malware Mirai, famoso em 2016, explorava essas falhas: ele escaneava IPs em busca de dispositivos com credenciais padrão para invadir e controlar. Cada novo IP comprometido era reportado a um servidor, recebia o malware e ajudava a espalhá-lo até receber ordens do servidor de Comando e Controle (CnC).

# Exemplo de falhas em dispositivos IoT



```
login@parrot:~/Desktop/all$ python3 exploit_detect.py
Chose the ips lists(txt) : hikvision.txt
error
The system 86.167.63.189:80 is not vulnerable.
error
The system 185.200.38.210:80 is not vulnerable.
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:1015: InsecureRequestWarning: Unverified HTTPS request is being made to host 'gw-sciana.pl'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
warnings.warn(
The system 185.200.45.129:80 is not vulnerable.
The system 185.200.46.37:80 is not vulnerable.
The system 83.151.207.124:80 is vulnerable.
Username: admin
Password: Kielbaskal234

The system 185.200.47.238:80 is not vulnerable.
error
The system 185.200.52.10:80 is not vulnerable.
```

**ATTACKERKB**

CVE-2017-7921

CVE-2017-7921

 **ATTACKER VALUE**  
**VERY HIGH**

 **EXPLOITABILITY**  
**VERY HIGH**

 5

 1

**CVE-2017-7921** é uma falha em câmeras IP da Hikvision, onde um atacante pode acessar o sistema sem precisar de senha. Ela permite que uma pessoa mal-intencionada, usando comandos especiais na URL, consiga ver imagens da câmera e alterar configurações sem ser autorizada.

# Recursos utilizados

- Roteador Mikrotik e seis ASUS Tinker Board.
- Duas redes separadas (192.168.10.0 e 192.168.20.0 (/24))
- Wireshark (post-mortem) e Pyshark (tráfego em tempo real)

# Componentes do botnet Mirai

**Bots/Agentes/Zumbis:** Dispositivos IoT infectados que podem ser comandados pelo botmaster para escanear novos alvos ou realizar ataques.

**Servidor C&C:** Permite ao botmaster enviar comandos aos bots, como iniciar ataques DDoS, minerar criptomoedas ou enviar spam.

**Scanners:** Buscam dispositivos IoT vulneráveis na internet.

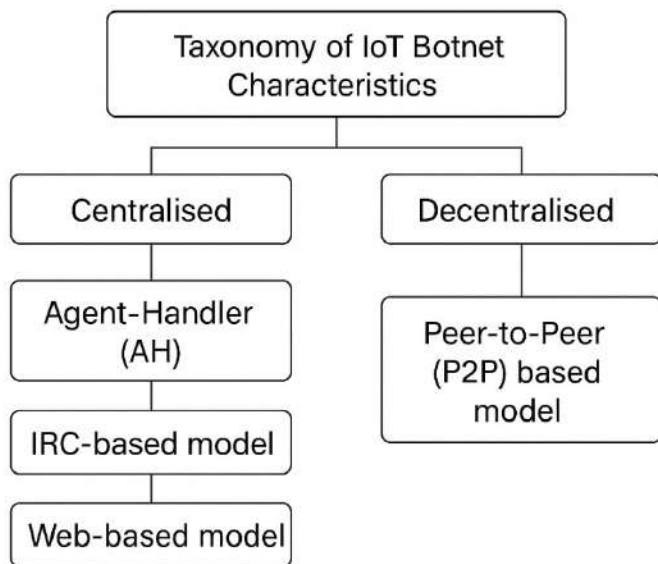
**Servidor de Relatórios:** Recebe os resultados das varreduras feitas pelos scanners ou bots.

# Componentes do botnet Mirai

Loaders: Acessam dispositivos vulneráveis para instalar o malware.

Servidor de Distribuição de Malware: Armazena o malware que será baixado pelos dispositivos infectados.

# Como controlar uma botnet?



Comparison of Centralised and Decentralised IoT Botnets

	Centralised	Decentralised
Control	Centralised	Decentralised
Point of Failure	Single point of failure	No single point of failure
Models	Agent-Handler (AH), IRC-based Web-based	Peer-to-Peer (P2P)
Communication/Command D	Control control and communication	Distributed command delivery



O malware se conectaria à seção de comentários de uma foto publicada na conta de Britney Spears no Instagram e procuraria um comentário que tivesse um hash com o valor 183.

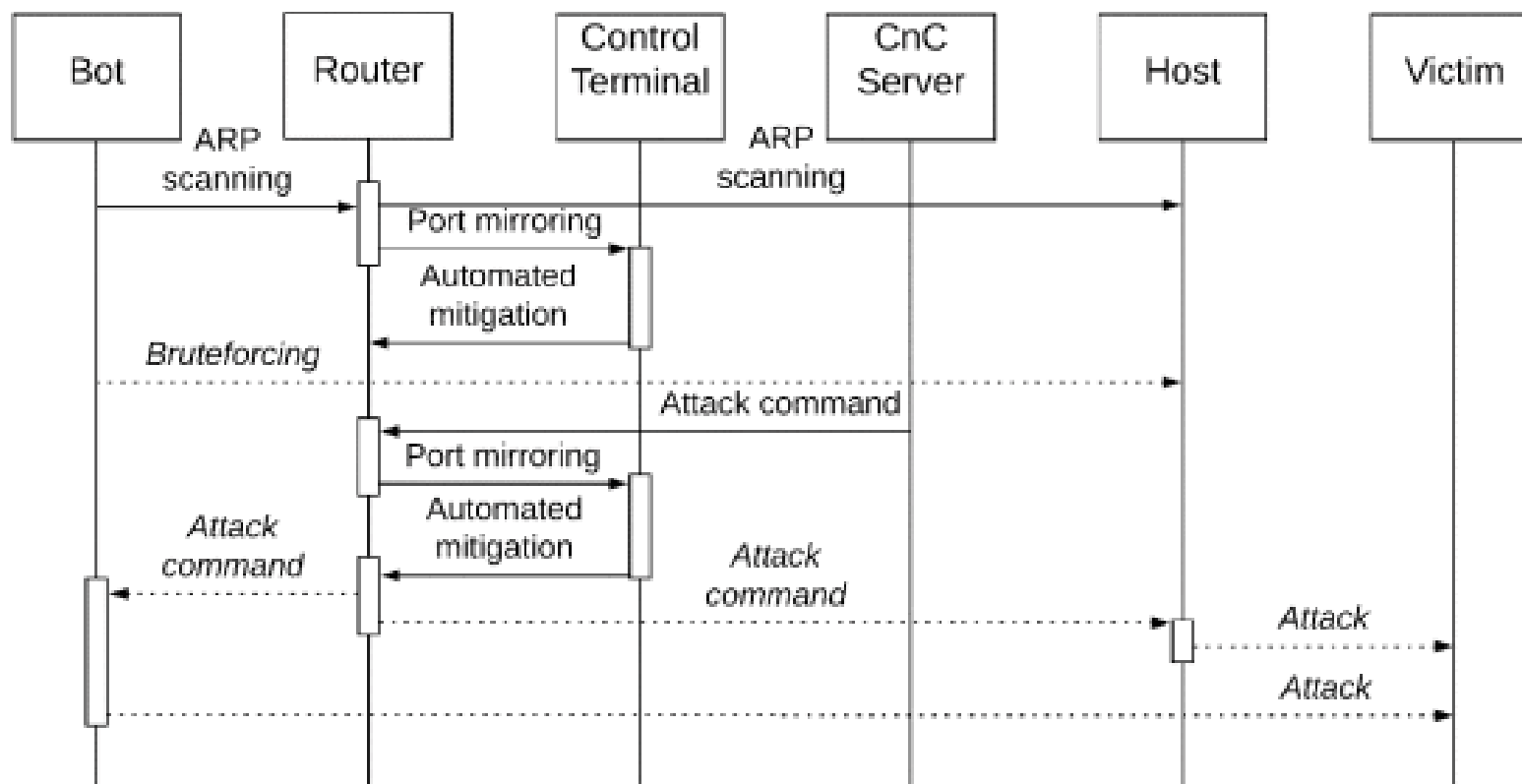


# Estratégias de detecção

Comportamento de varredura: ARP floods

Tráfego CnC: Sessão Telnet

Comandos de ataque: Detecção via análise do payload



# Estratégias de detecção

0000	2c	4d	54	42	c8	78	64	31	50	13	5f	f3	08	00	45	00	,MTB·xd1 P·_· · · E·
0010	00	42	ec	14	40	00	40	06	b9	41	c0	a8	0a	07	c0	a8	·B· · @·@· ·A· · · · ·
0020	0a	08	00	17	d8	50	39	1e	3e	f4	e4	dc	2d	9b	80	18	· · · · · P9· > · · · - · ·
0030	00	e3	ac	cd	00	00	01	01	08	0a	50	e5	83	59	00	13	· · · · · · · P· · Y· ·
0040	0e	95	00	0e	00	00	00	02	03	01	c0	a8	0a	04	20	00	· · · · · · · · · · ·

Attack  
duration

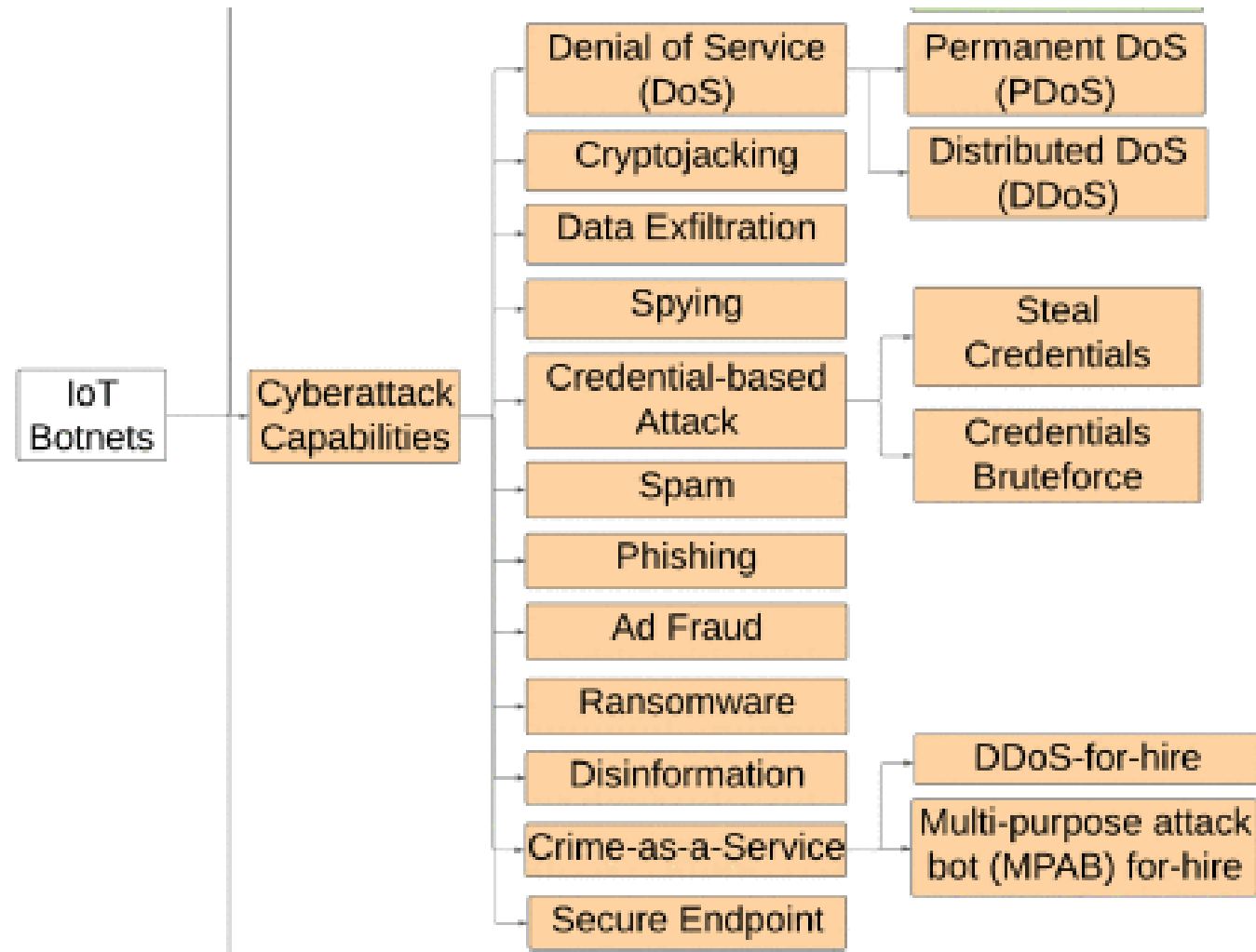
Attack ID

Number  
of  
targets

Victim IP  
192.168.10.4

IP suffix  
32

# Possíveis ataques a partir de dispositivos infectados



A Taxonomy of IoT Botnet Characteristics


# Objetivos e trabalhos futuros


Como trabalho futuro, pretende-se usar detecção baseada em anomalias para identificar outros malwares e variantes do Mirai.






# Referências

G. Galloopeni, B. Rodrigues, M. Franco and B. Stiller, "A Practical Analysis on Mirai Botnet Traffic," *2020 IFIP Networking Conference (Networking)*, Paris, France, 2020, pp. 667-668.


# Código fonte do Mirai - Extra

 jgamblin / Mirai-Source-Code

Q Type  to search


    

[Code](#) [Pull requests](#) 1 [Actions](#) [Projects](#) [Security](#) [Insights](#)


 **Mirai-Source-Code** Public

[Watch](#) 555 [Fork](#) 3.5k [Star](#) 8.8k

[master](#) 1 Branch 0 Tags

Q Go to file 







[Add file](#) [Code](#)

 jgamblin Merge pull request #38 from Red54/patch-1 3273043 · 8 years ago 8 Commits

dlr	Trying to Shrink Size	9 years ago
loader	Trying to Shrink Size	9 years ago
mirai	Trying to Shrink Size	9 years ago
scripts	Transcribe post to markdown while preserving	9 years ago
ForumPost.md	Transcribe post to markdown while preserving	9 years ago
ForumPost.txt	Update ForumPost.txt	9 years ago
LICENSE.md	Trying to Shrink Size	9 years ago
README.md	Fix a typo in README.md	8 years ago

### About

Leaked Mirai Source Code for Research/loC Development Purposes

-  [Readme](#)
-  [GPL-3.0 license](#)
-  [Activity](#)
-  8.8k stars
-  555 watching
-  3.5k forks


[Report repository](#)

### Releases

No releases published

### Packages

# Build Your Own Botnet - Extra

 malwaredllc / byob

malwaredllc / byob

Type / to search

<> Code

Issues 6


Pull requests 1

Actions

Wiki

Security

Insights

 **byob** Public

Sponsor

Watch 323

Fork 2.1k


Star 9.2k

master 2 Branches 1 Tag

Go to file

Add file

<> Code

 **malwaredllc** remove broken build badge b494690 · 9 months ago 765 Commits

.github	remove codeql analysis workflow	3 years ago
byob	misc cleanup	9 months ago
web-gui	misc cleanup	9 months ago
.coveragerc	update coverage config	4 years ago
.gitattributes	Update .gitattributes	4 years ago
.gitignore	fix config files	4 years ago
.travis.yml	update travis build dir	4 years ago
LICENSE	removing ^M from files	7 years ago
README.md	remove broken build badge	9 months ago

## About

An open-source post-exploitation framework for students, researchers and developers.

encrypted-connections

post-exploitation

platform-independent

no-dependencies

reverse-shells

Readme

GPL-3.0 license

Activity

9.2k stars

323 watching

2.1k forks

Report repository



# CPGoiás – Palestra de João Moreno - Extra



João Moreno Falcão - Como explodir uma usina de enriquecimento de urânio? - #CPGoiás2



Campus Party Brasil

11,2 mil inscritos

Inscriver-se



Compartilhar



Todos

De Campus Party Brasil

Relacionados



Final

Obrigado!