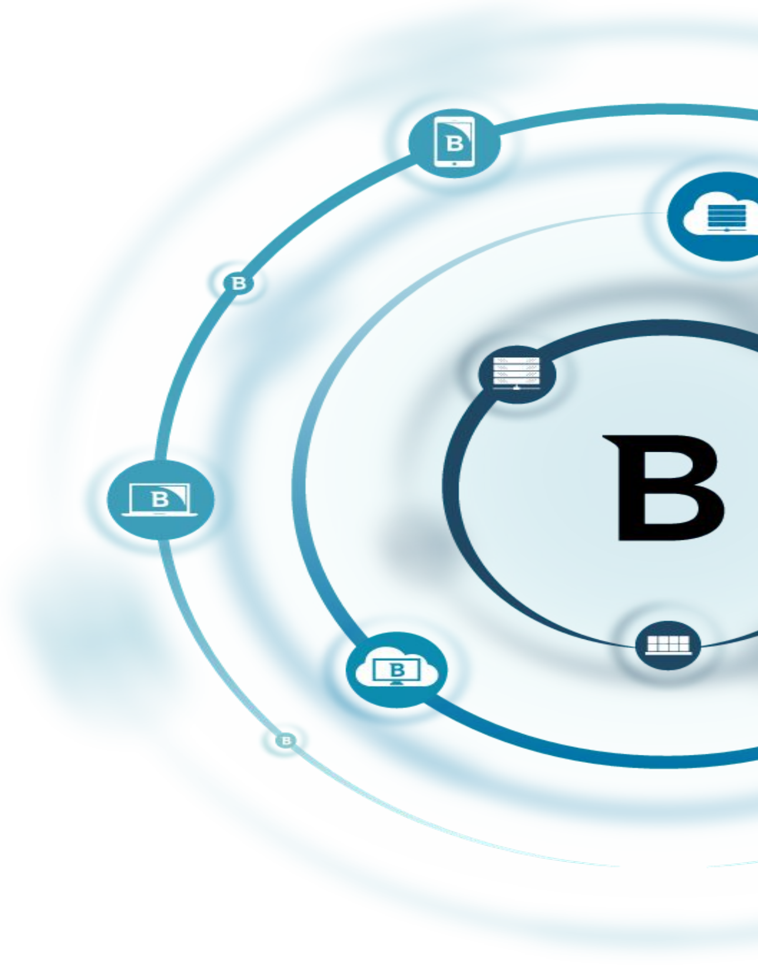
Bitdefender

Hide’n’Seek

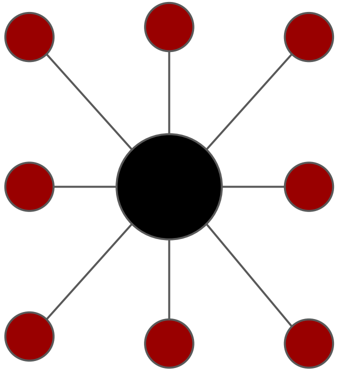
An Adaptive Peer-to-Peer Botnet

Adrian Șendroiu
Vladimir Diaconescu



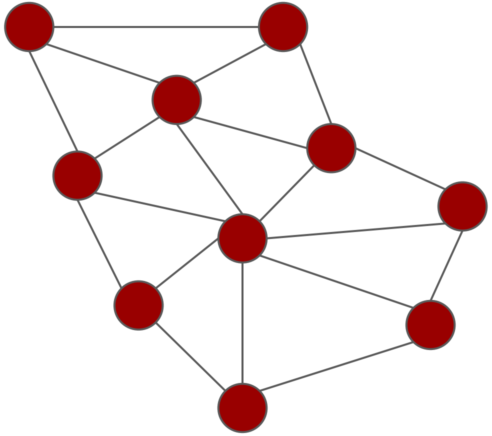
Context

- IoT Botnets increasing in impact and diversity
- Tried and tested models (Mirai)
  - Central C2 Server
  - (Different) Infecting machine
  - (Different) Reporting machine
- Dictionary and CVE extensions
- Main objective: DDoS



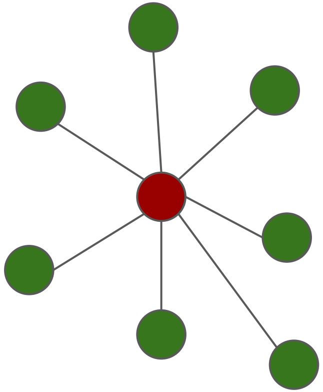
Analysis - Overview

- A new idea: Peer-to-Peer botnet
  - Also seen in Hajime
- Custom protocol
- Modular
- Authenticated
- Different goals



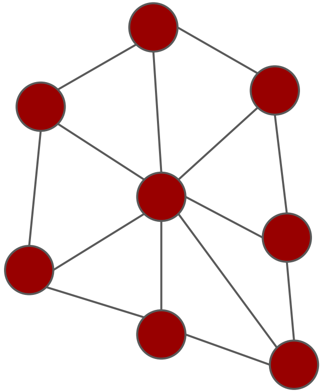
Functionality

- Two main components
  - Scanner



Functionality

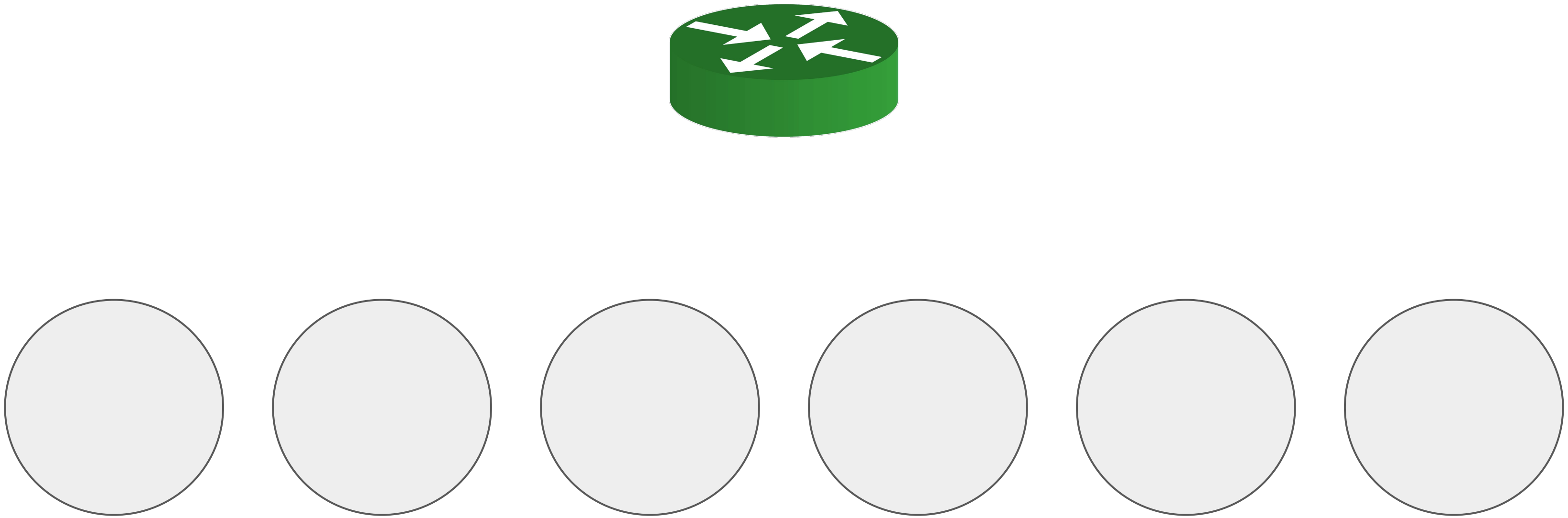
- Two main components
  - Scanner
  - P2P protocol



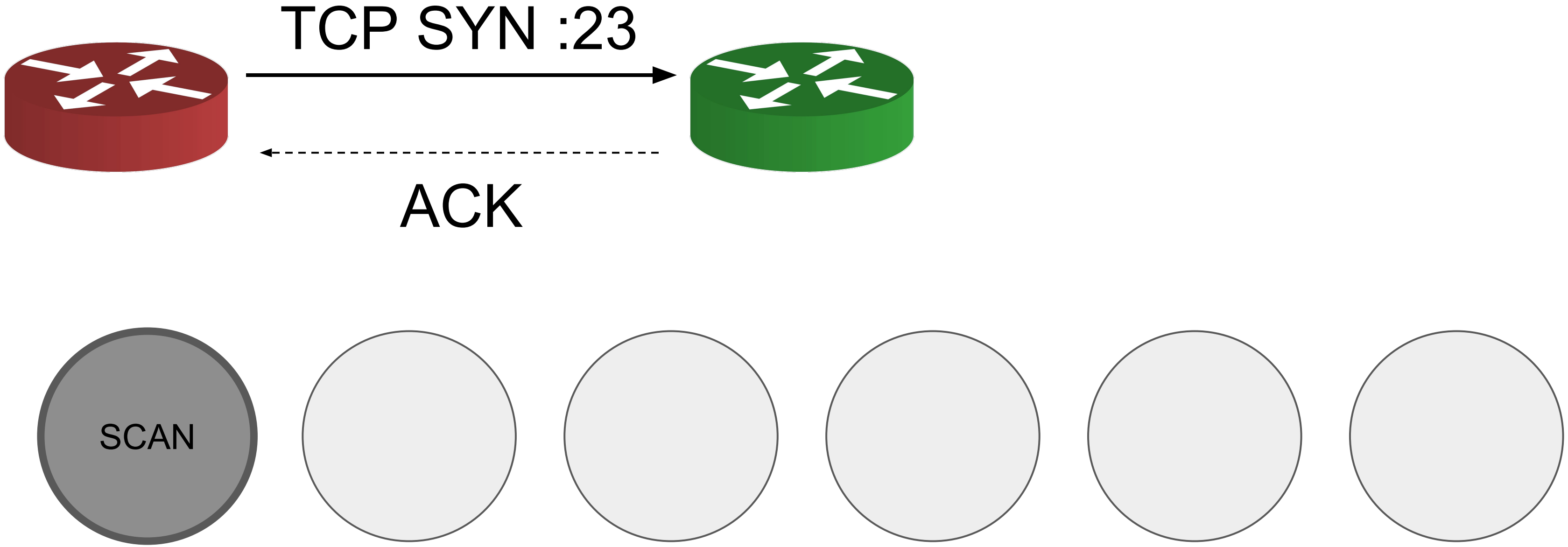
Scanning for victims

- Pick a random IP and a port
  - 23, 2323 (telnet) - try default credentials
  - 80, 8080 (http) - try known IoT exploits
  - 5555 - ADB
  - Others (2480, 5984)

Analysis - Infection process



Analysis - Infection process: Scan

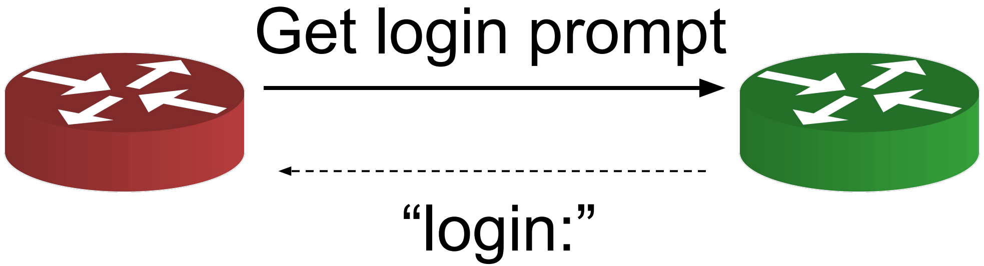


TCP SYN :23

ACK

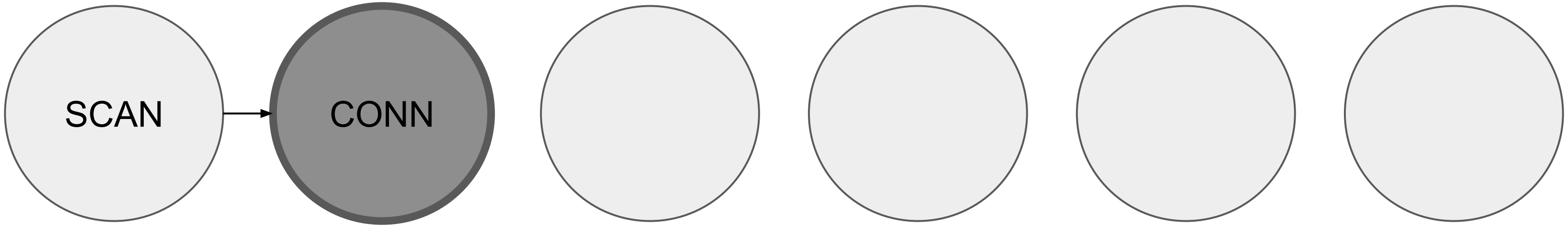
SCAN

Analysis - Infection process: Connect



Get login prompt

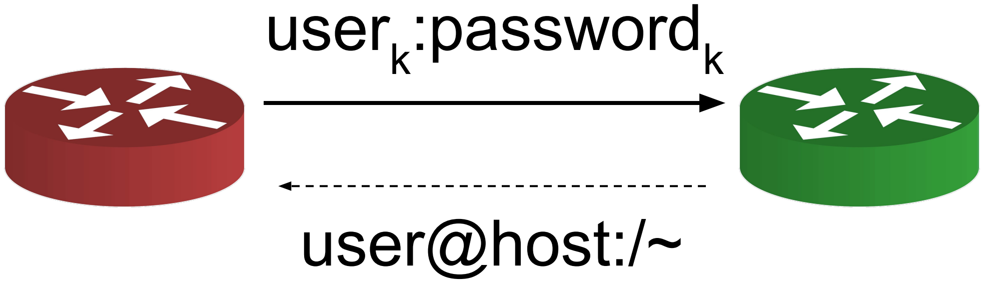
“login:”

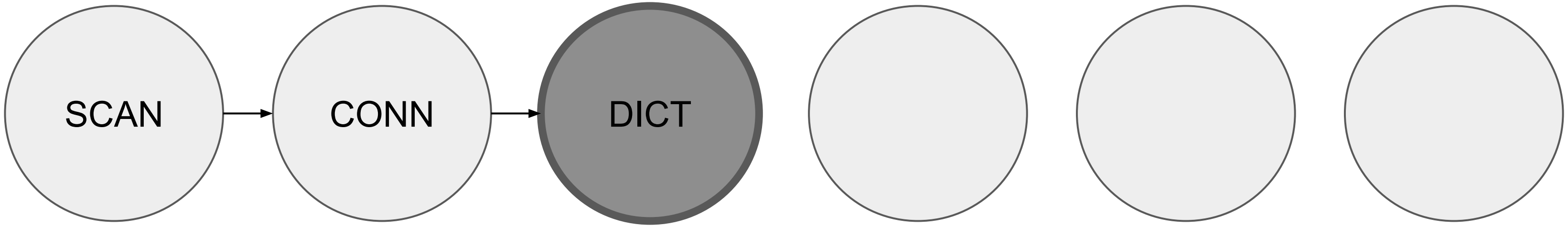


SCAN

CONN

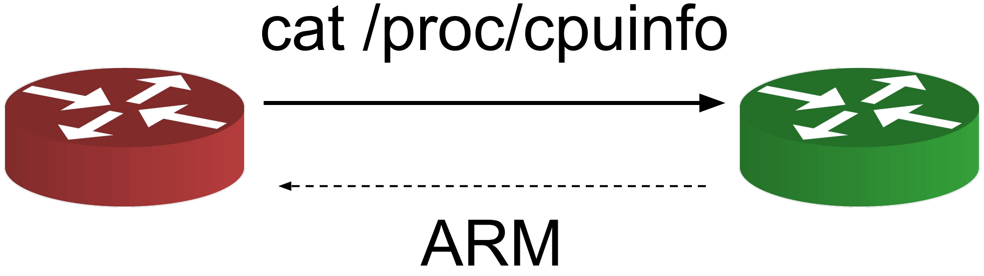
Analysis - Infection process: Dictionary

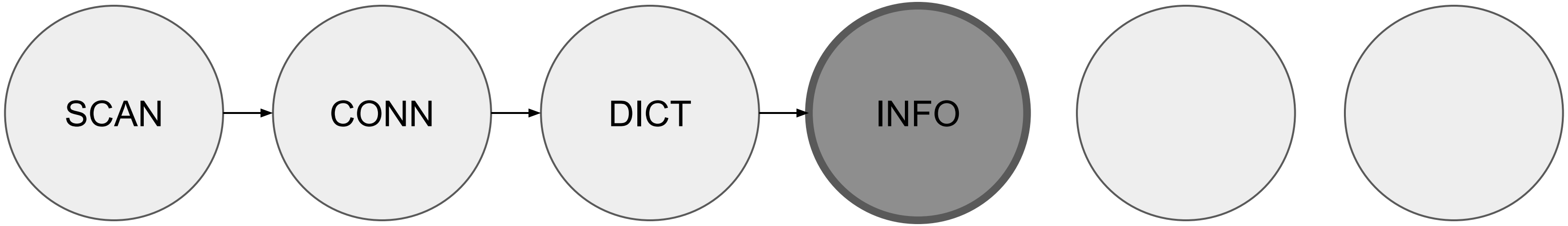




Bitdefender

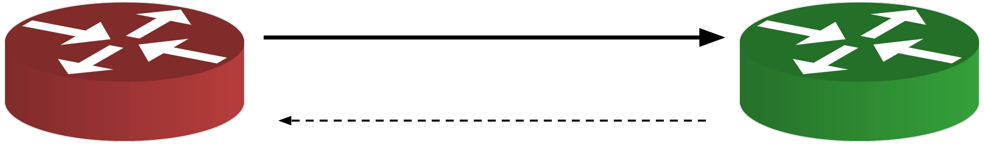
Analysis - Infection process: Sysinfo



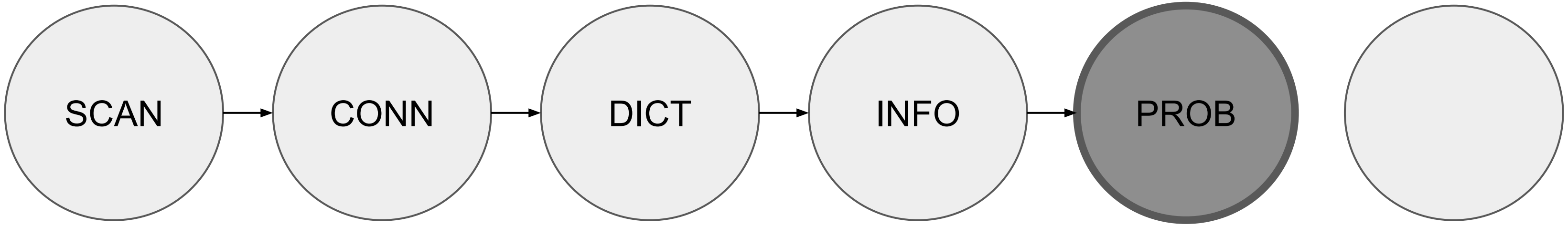


Analysis - Infection process: Probing

wget
curl
base64



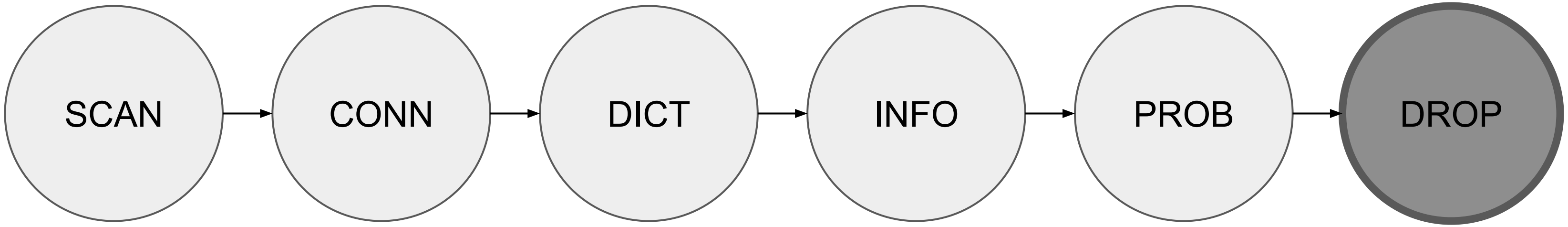
wget: not found
curl: not found



SCAN → CONN → DICT → INFO → PROB →

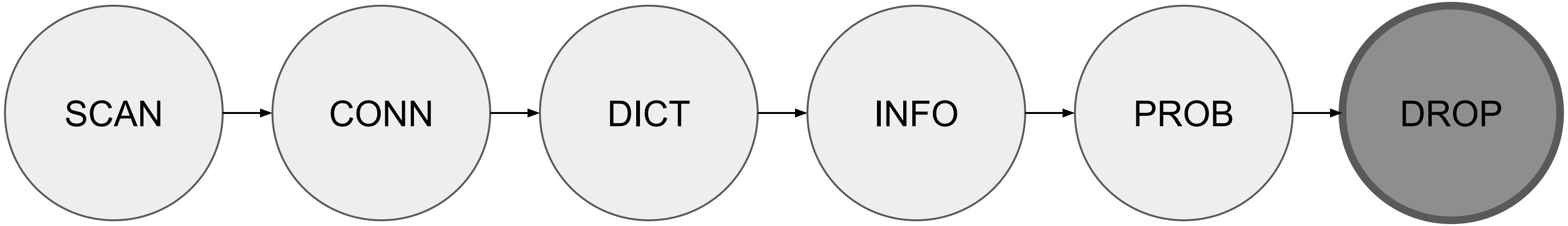
Analysis - Infection process: Dropping

- “echo -e ‘\x7fELF…’ > abc”
- chmod +x abc



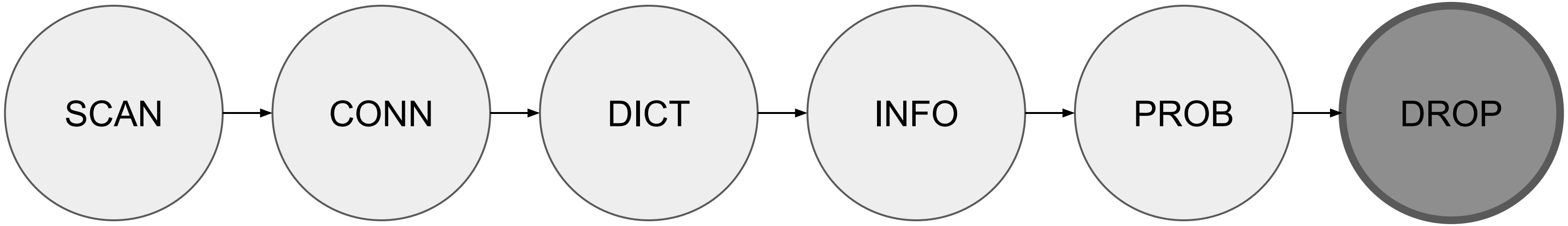
Analysis - Infection process: Dropping

- ./abc a1.2.3.4:5678 k23 l4444 e5.4.3.2:80



Analysis - Infection process: Dropping

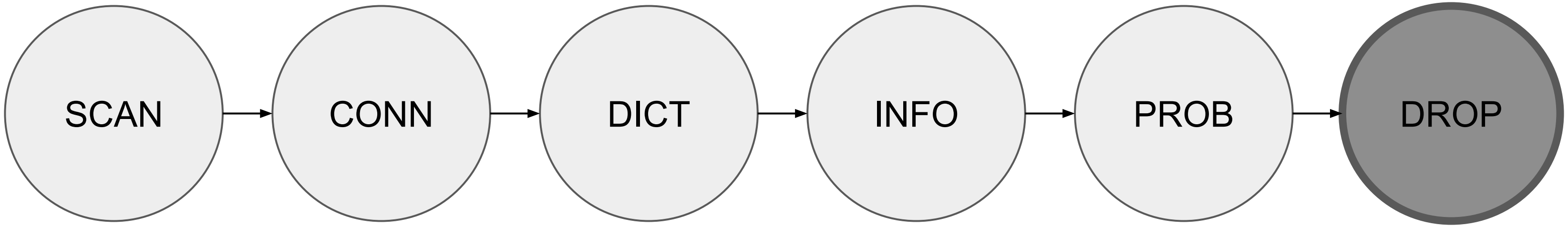
- ./abc a1.2.3.4:5678 k23 l4444 e5.4.3.2:80
  - Initial starting peers



Bitdefender

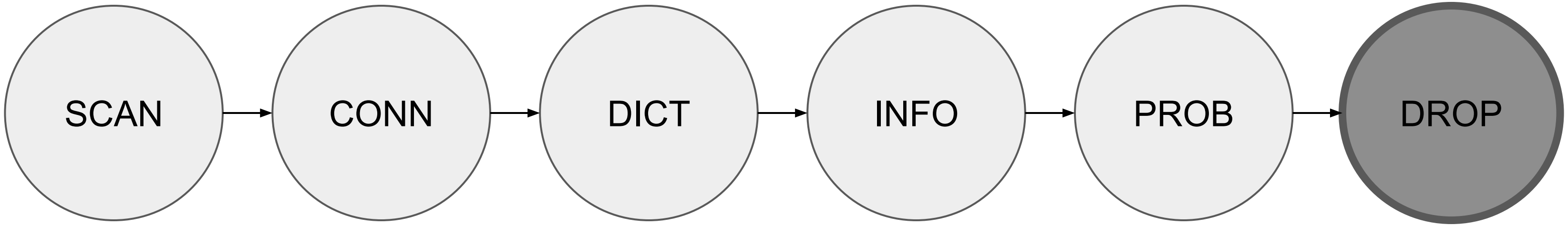
Analysis - Infection process: Dropping

- ./abc a1.2.3.4:5678 k23 l4444 e5.4.3.2:80
  - Initial starting peers
  - Kill port



Analysis - Infection process: Dropping

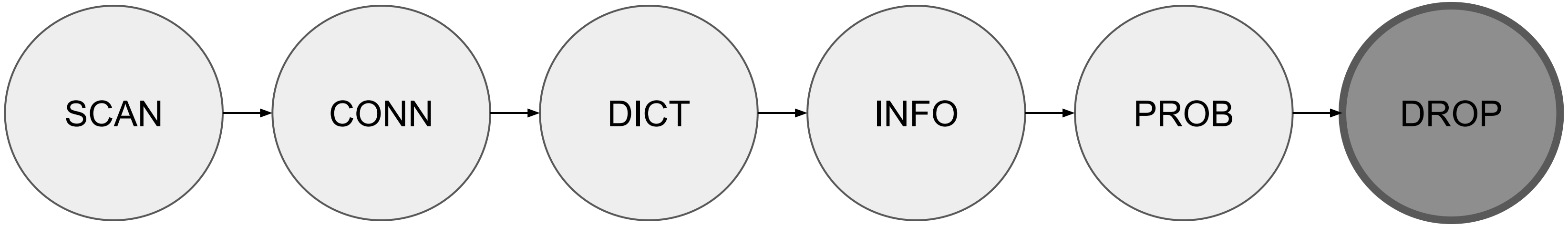
- ./abc a1.2.3.4:5678 k23 l4444 e5.4.3.2:80
  - Initial starting peers
  - Kill port
  - P2P listening port (UDP)



Bitdefender

Analysis - Infection process: Dropping

- ./abc a1.2.3.4:5678 k23 l4444 e5.4.3.2:80
  - Initial starting peers
  - Kill port
  - P2P listening port (UDP)
  - Additional scan targets



Bitdefender

P2P protocol

- Custom UDP protocol
  - Data structures
  - Messages

Data structures - Peer table

IP	port
1.2.3.4	20123
5.6.7.8	30456
4.3.2.1	40789

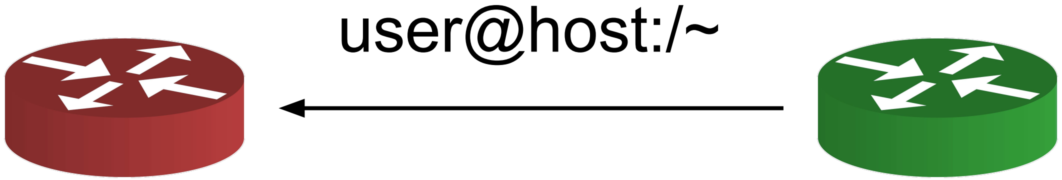
Data structures - Caches

payload id	->	hash
0x15	->	1af3...
0x13	->	3f14...

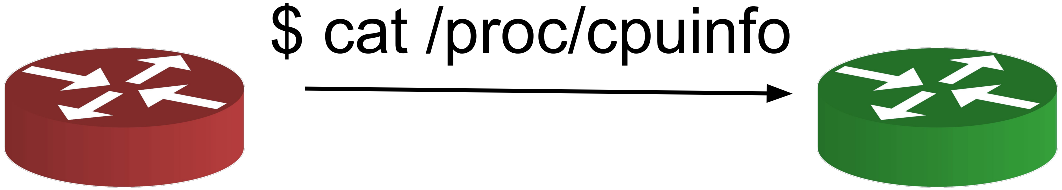
config cache

hash	->	data
3f14…	->	\x7fELF...
1af3...	->	\x7fELF…

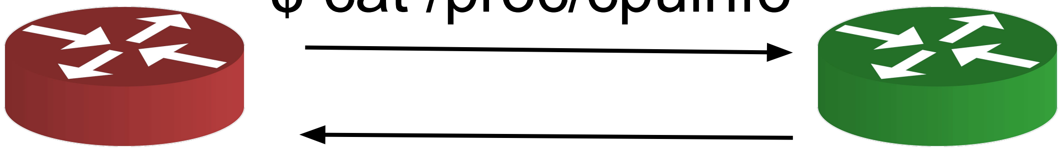
data cache



user@host:/~



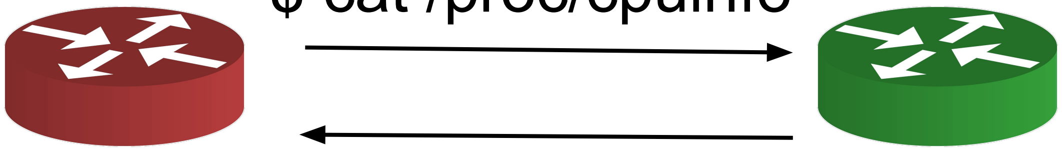
```
$ cat /proc/cpuinfo
```



```
$ cat /proc/cpuinfo
```

```
...
model name      : ARMv7 Processor rev 1
...
```

- What to download?



```
$ cat /proc/cpuinfo
```

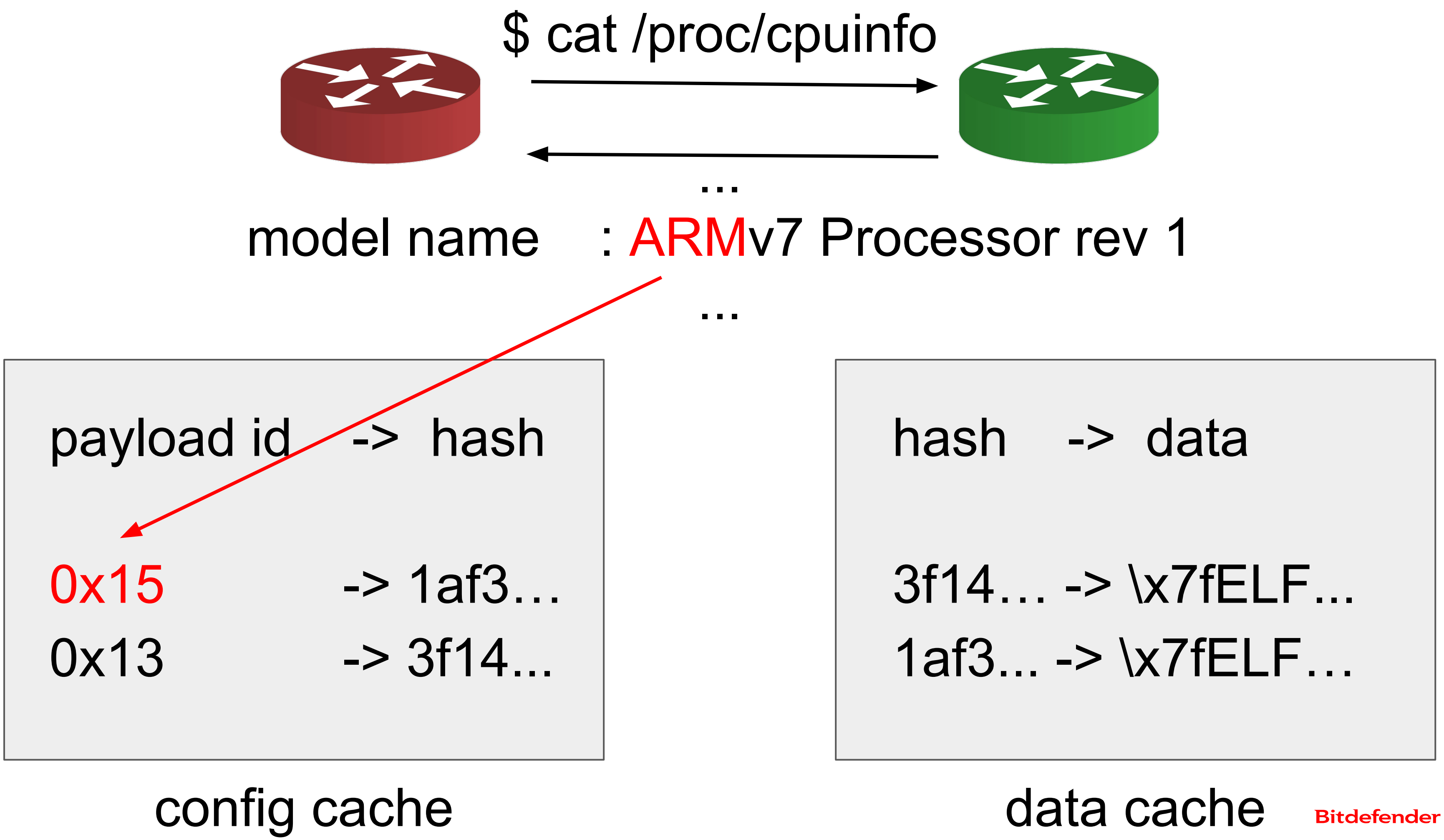
```
...
model name    : ARMv7 Processor rev 1
...
```

```
payload id    ->  hash

0x15          -> 1af3…
0x13          -> 3f14...
```

config cache

```
hash     ->  data

3f14… -> \x7fELF...
1af3... -> \x7fELF…
```

data cache



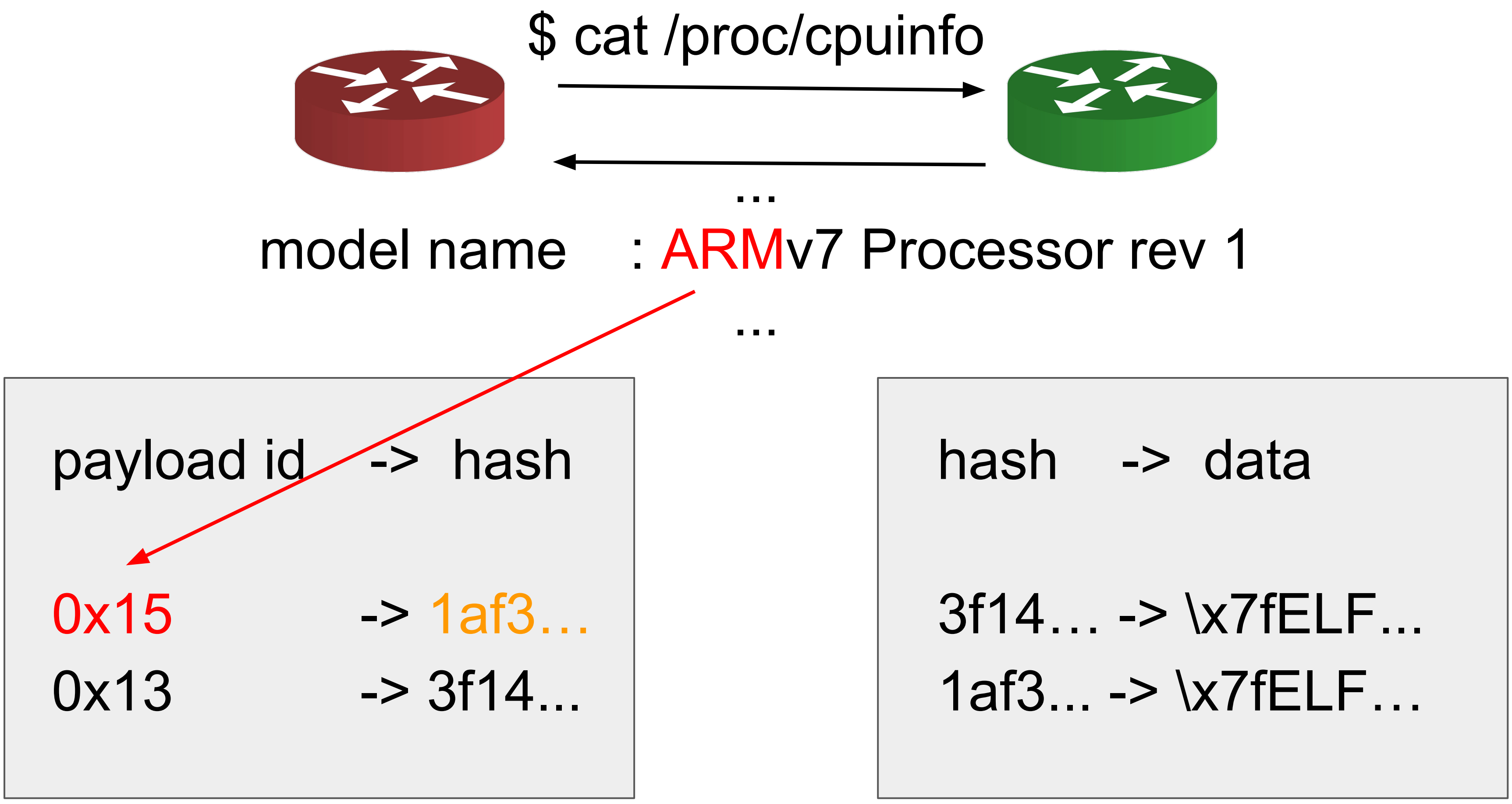
```
$ cat /proc/cpuinfo
...
model name	: ARMv7 Processor rev 1
...
```

payload id	->	hash
0x15	->	1af3…
0x13	->	3f14...

config cache

hash	->	data
3f14…	->	\x7fELF...
1af3...	->	\x7fELF…

data cache



$ cat /proc/cpuinfo

...

model name : ARMv7 Processor rev 1

...

payload id -> hash

0x15 -> 1af3...

0x13 -> 3f14...

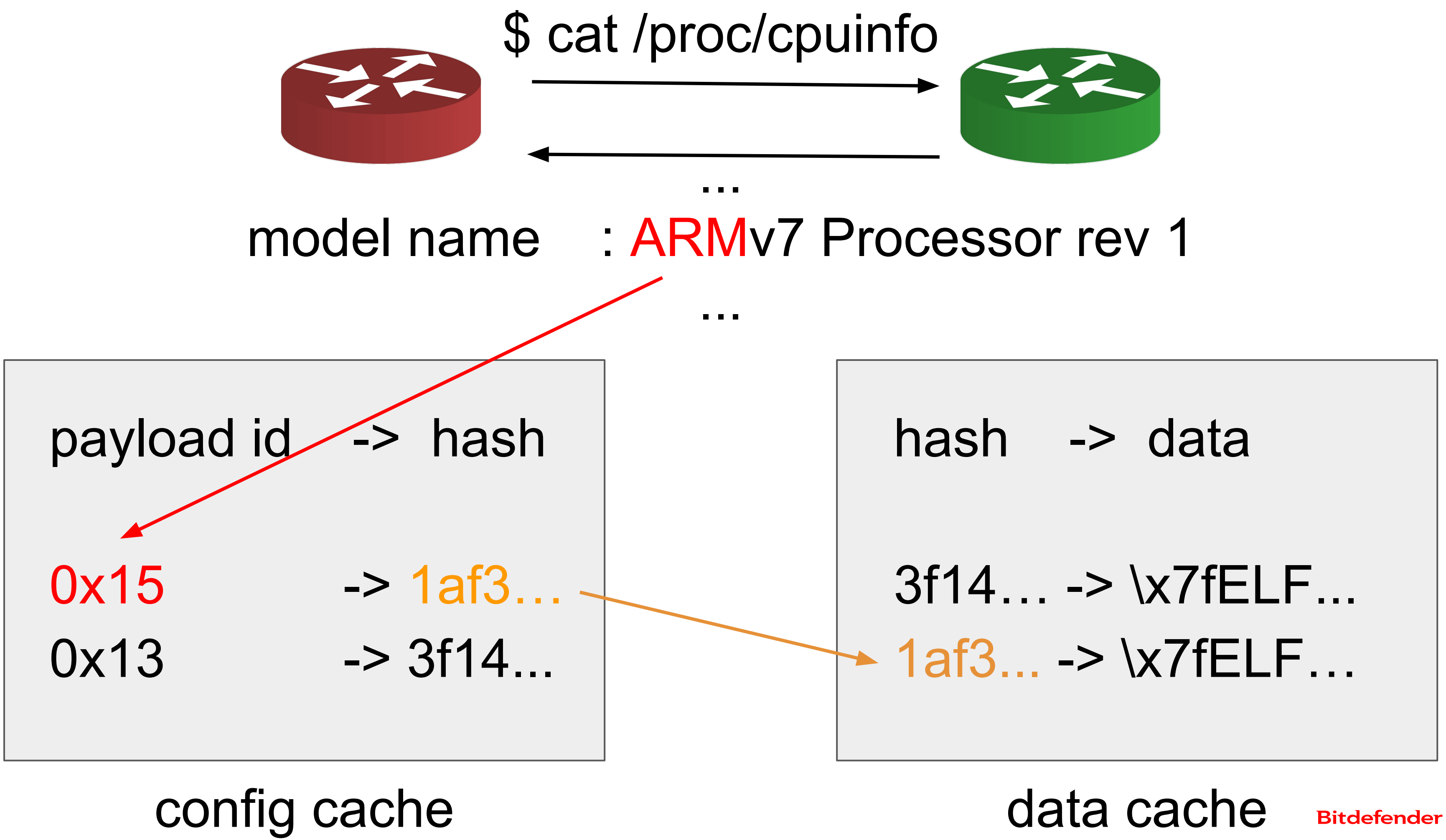
config cache

hash -> data

3f14... -> \x7fELF...

1af3... -> \x7fELF...

data cache



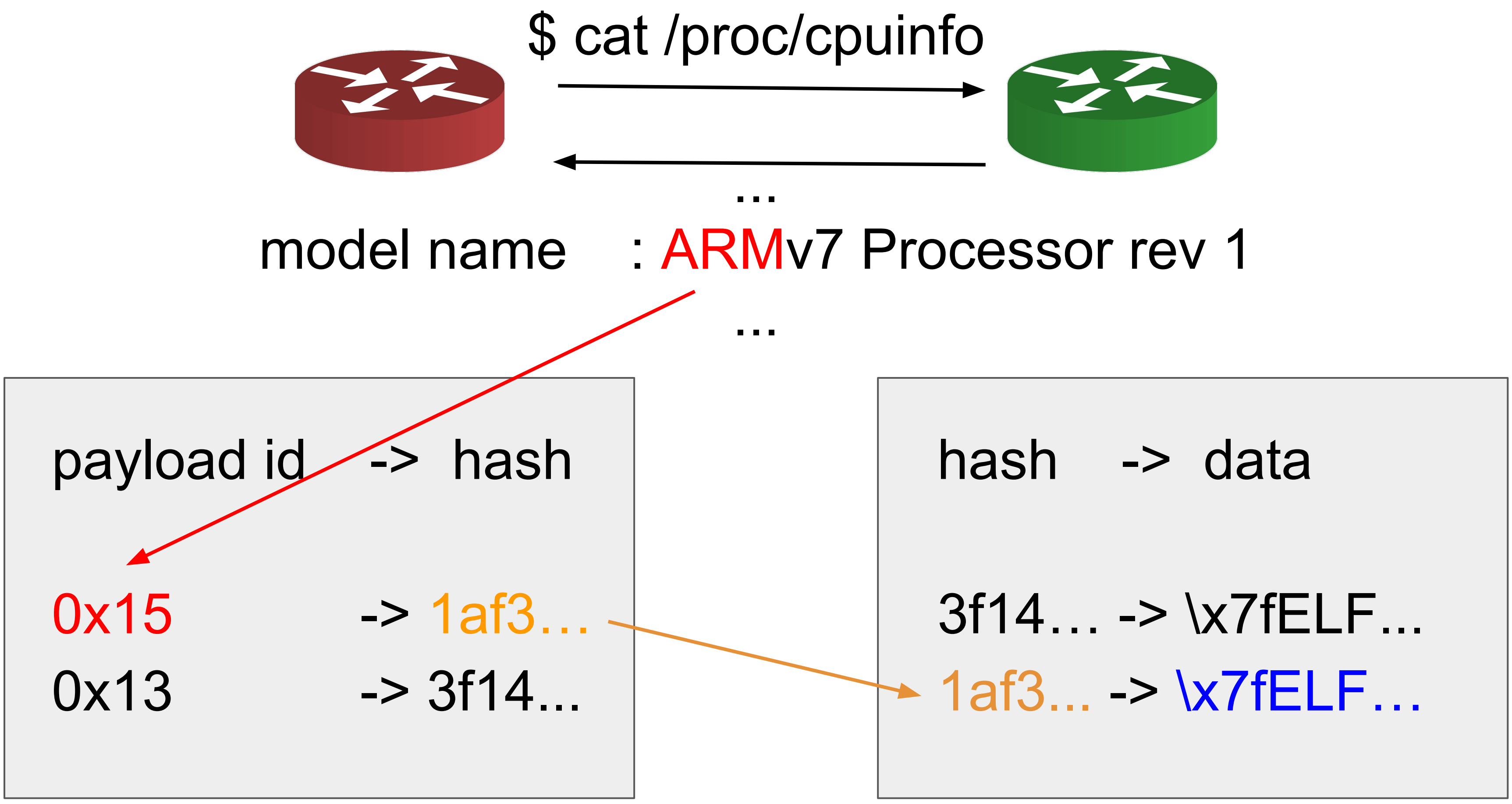
```
$ cat /proc/cpuinfo
...
model name      : ARMv7 Processor rev 1
...
```

payload id	->	hash
0x15	->	1af3...
0x13	->	3f14...

config cache

hash	->	data
3f14...	->	\x7fELF...
1af3...	->	\x7fELF...

data cache



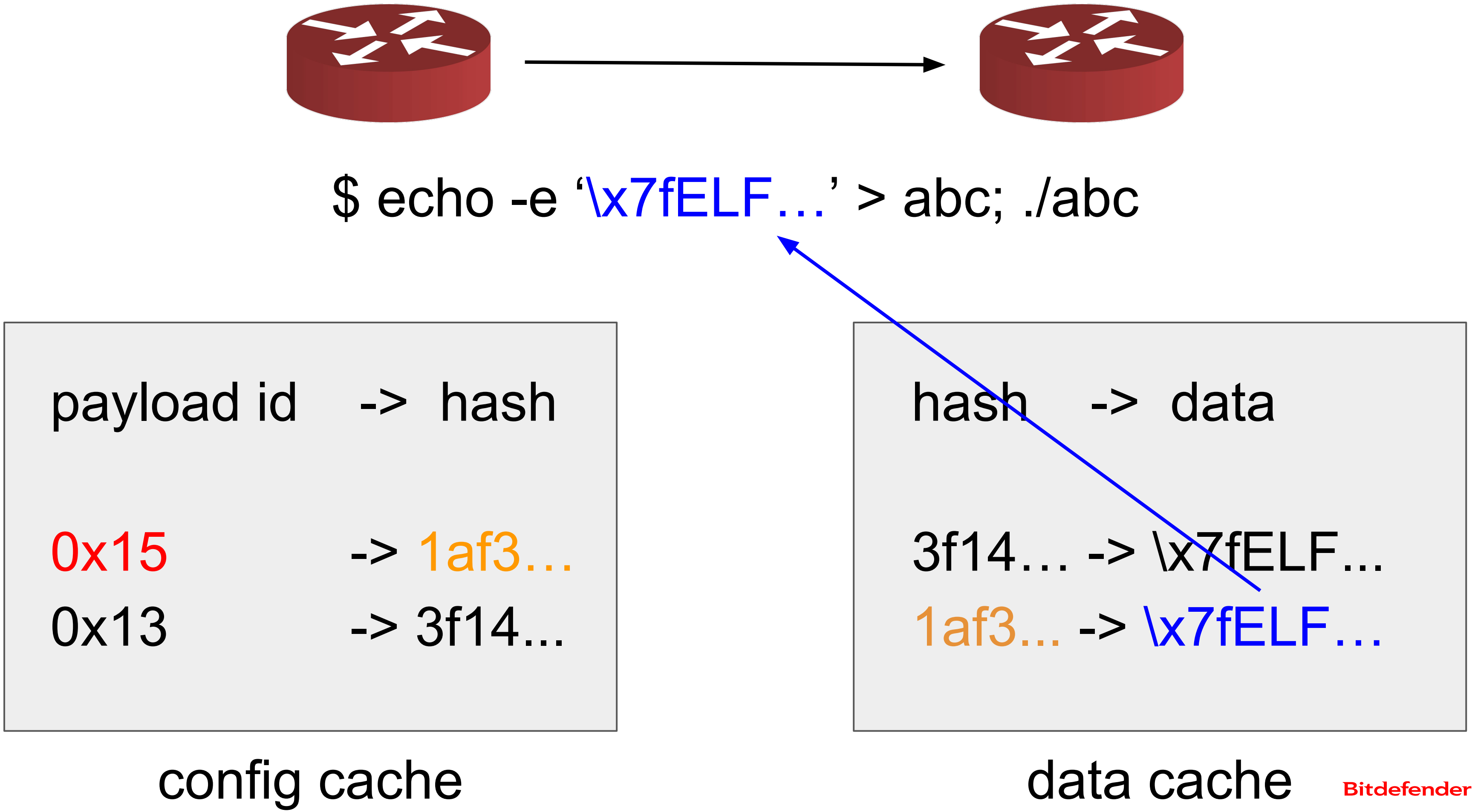
```
$ cat /proc/cpuinfo
...
model name      : ARMv7 Processor rev 1
...
```

config cache

payload id	->	hash
0x15	->	1af3...
0x13	->	3f14...

data cache

hash	->	data
3f14...	->	\x7fELF...
1af3...	->	\x7fELF...



```
$ echo -e ‘\x7fELF…’ > abc; ./abc
```

payload id	->	hash
0x15	->	1af3…
0x13	->	3f14...

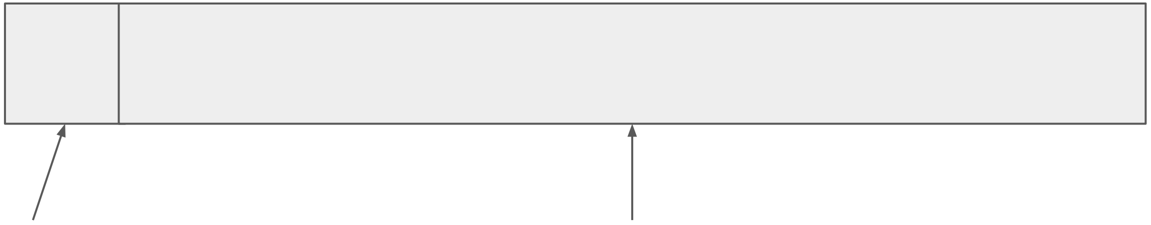
config cache

hash	->	data
3f14…	->	\x7fELF...
1af3...	->	\x7fELF…

data cache

P2P protocol messages

- Config cache update
- Peer management
- Target reporting



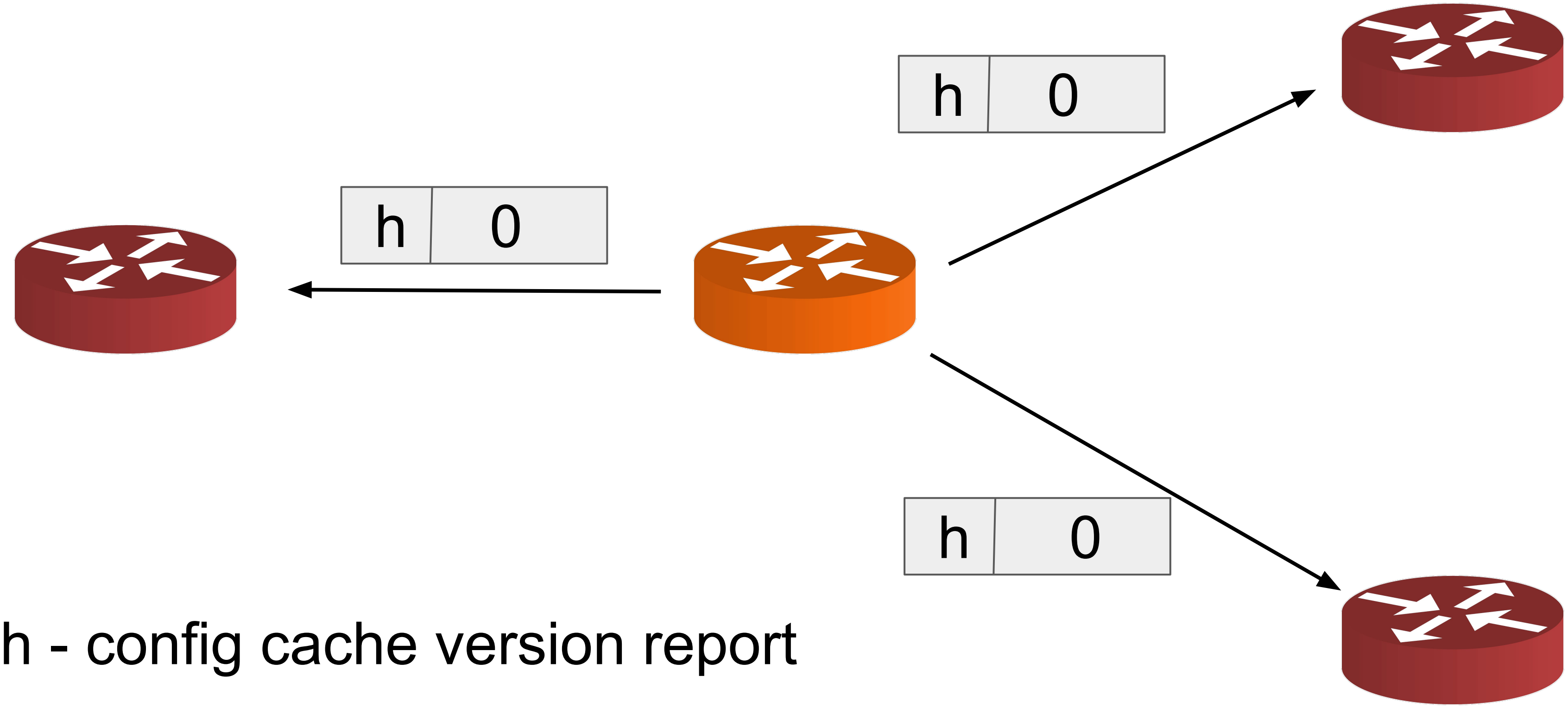
Config cache update

payload id -> hash

Config cache update

payload id	->	hash
0x15	->	1af3…
0x13	->	3f14...

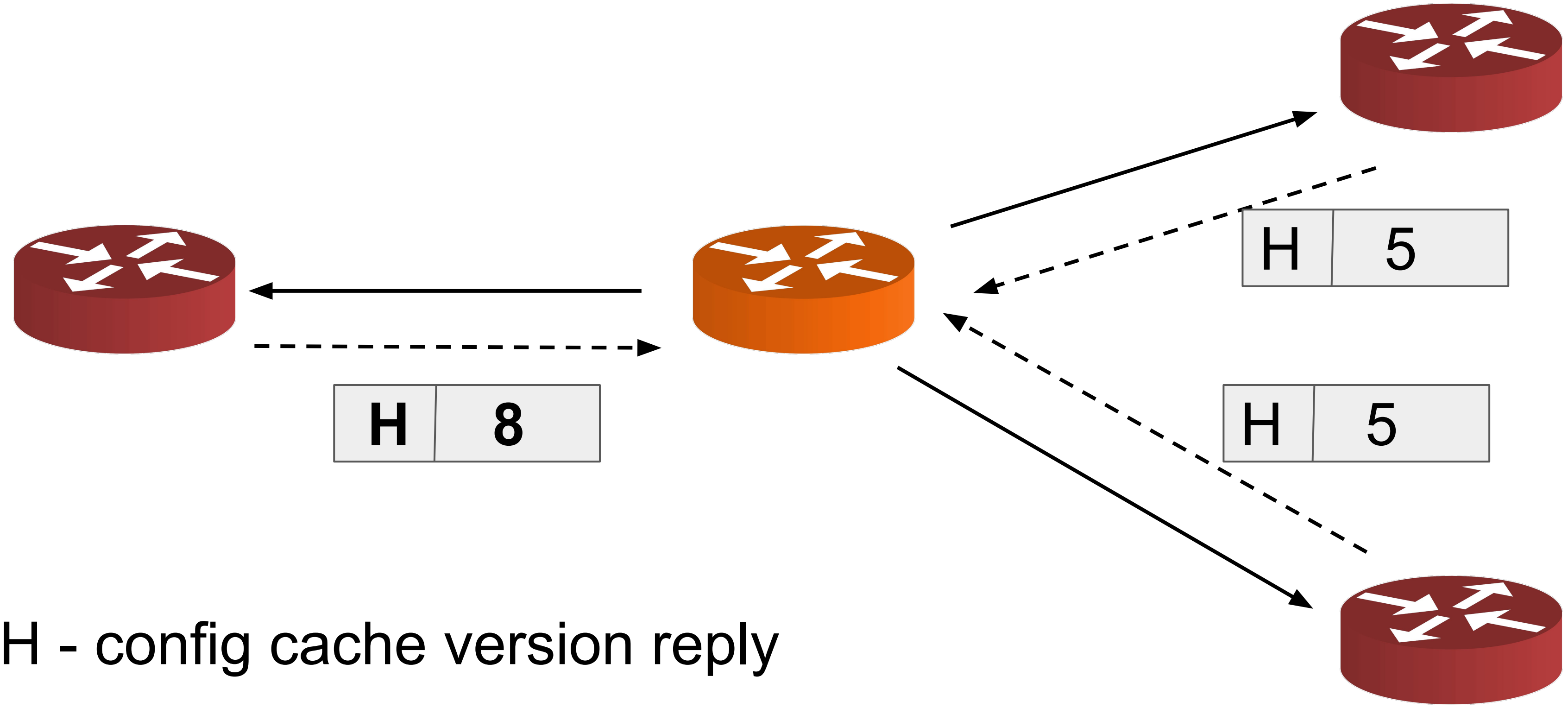
Config cache update



h - config cache version report

Bitdefender

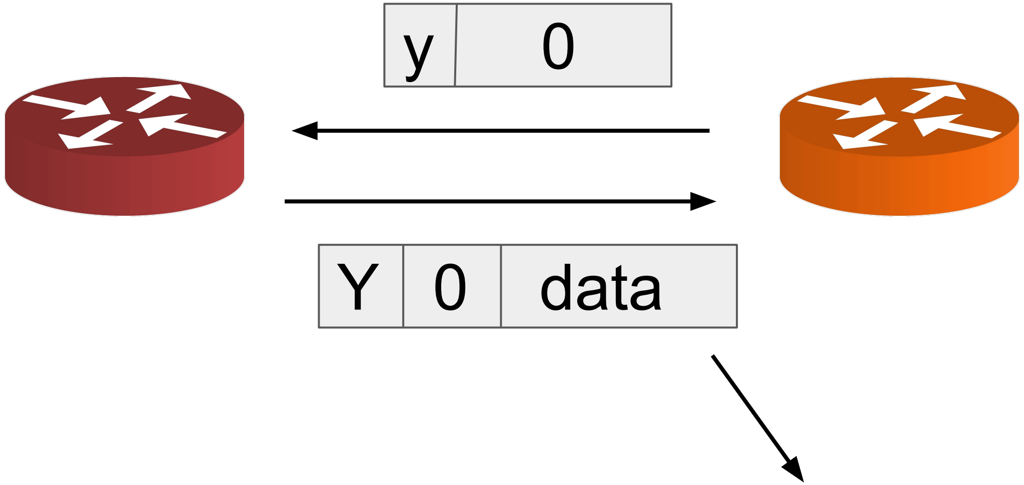
Config cache update



H - config cache version reply

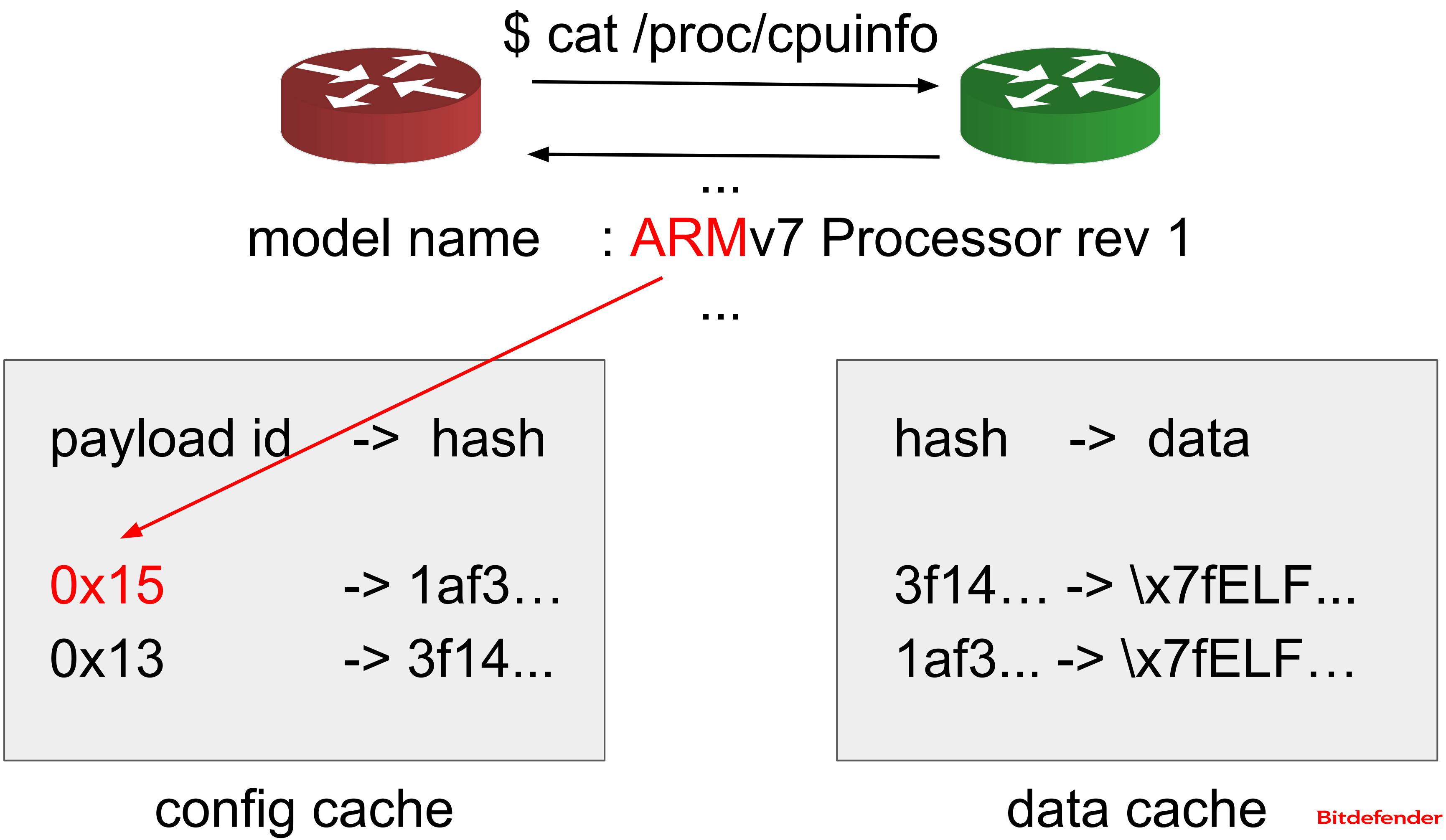
Bitdefender

Config cache update



check signature

y - chunk request
Y - chunk reply



```
$ cat /proc/cpuinfo
```

```
...
model name	: ARMv7 Processor rev 1
...
```

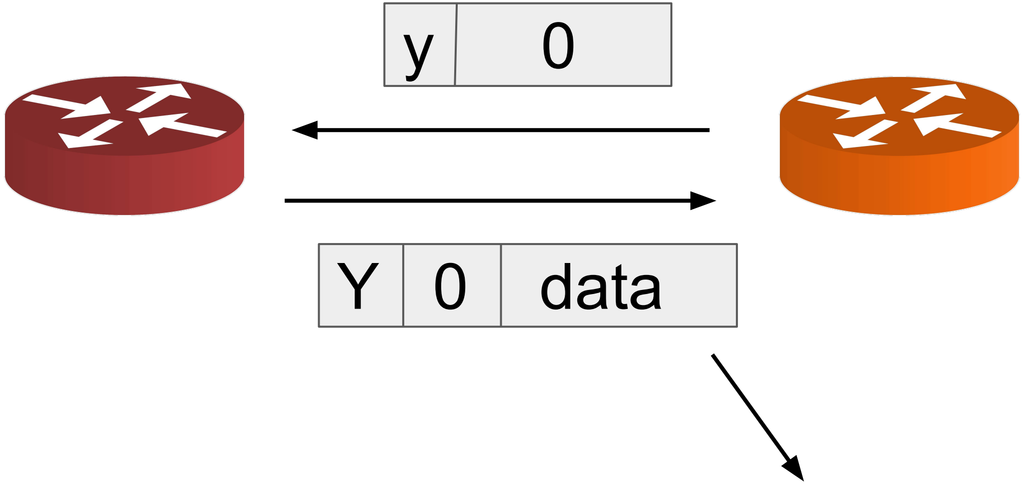
payload id	->	hash
0x15	->	1af3...
0x13	->	3f14...

config cache

hash	->	data
3f14...	->	\x7fELF...
1af3...	->	\x7fELF...

data cache

Config cache update



check signature

y - chunk request
Y - chunk reply

Bitdefender

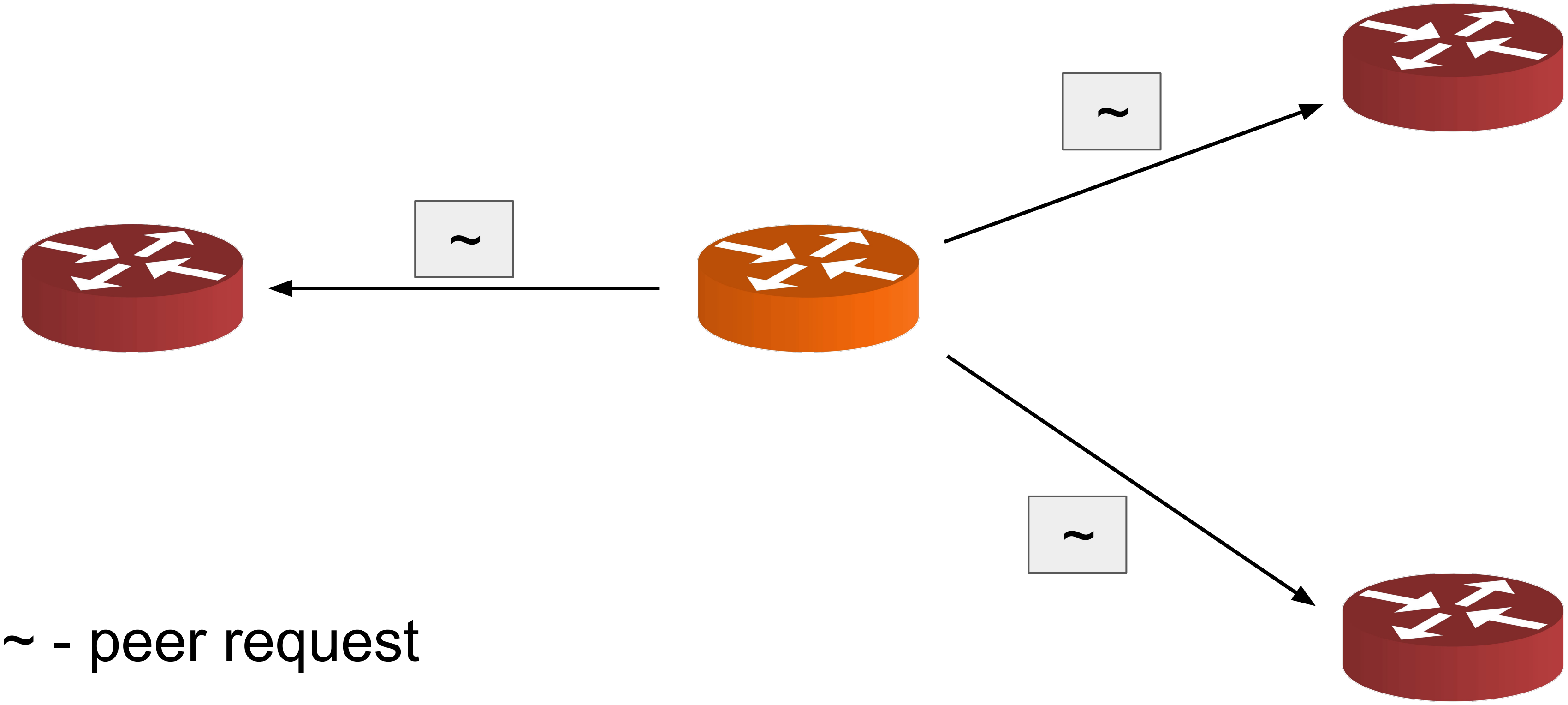
Data cache update

hash -> data

3f14… -> \x7fELF...

1af3... -> \x7fELF…

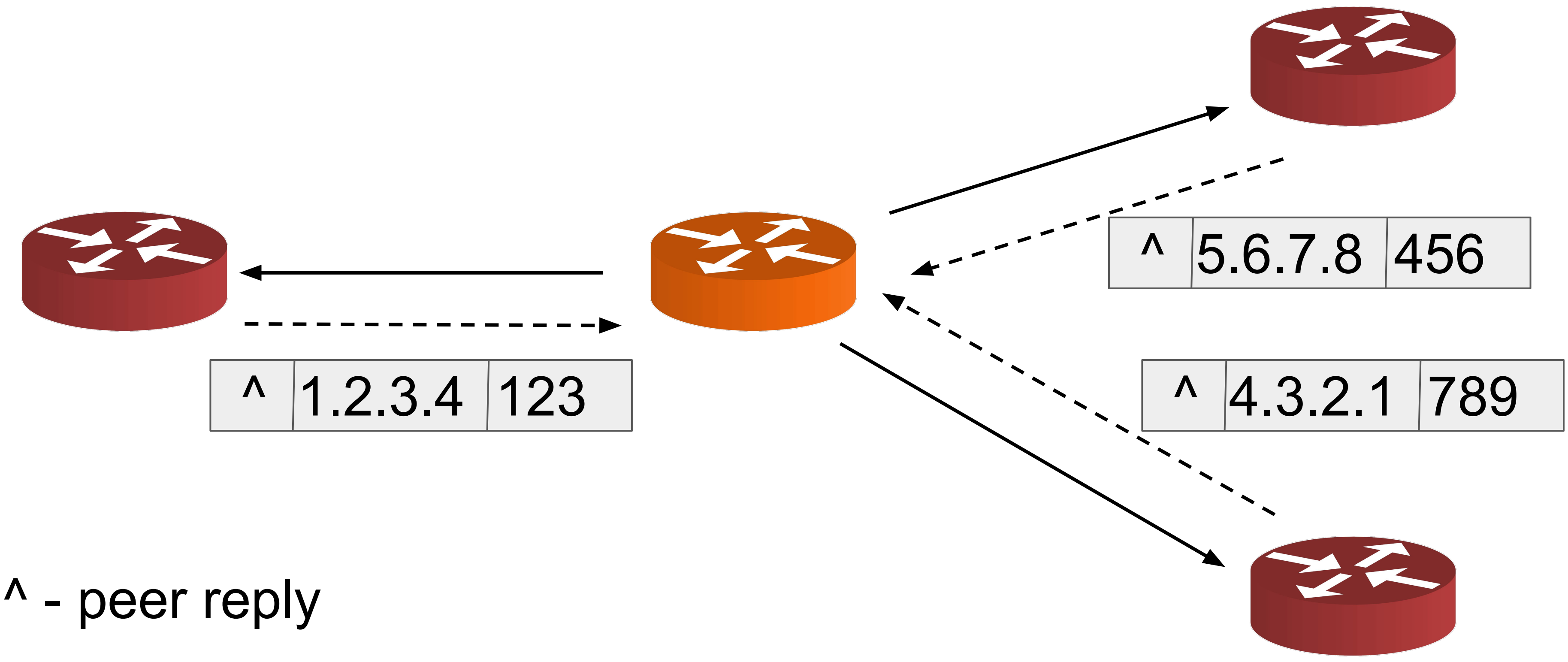
Peer update



~ - peer request

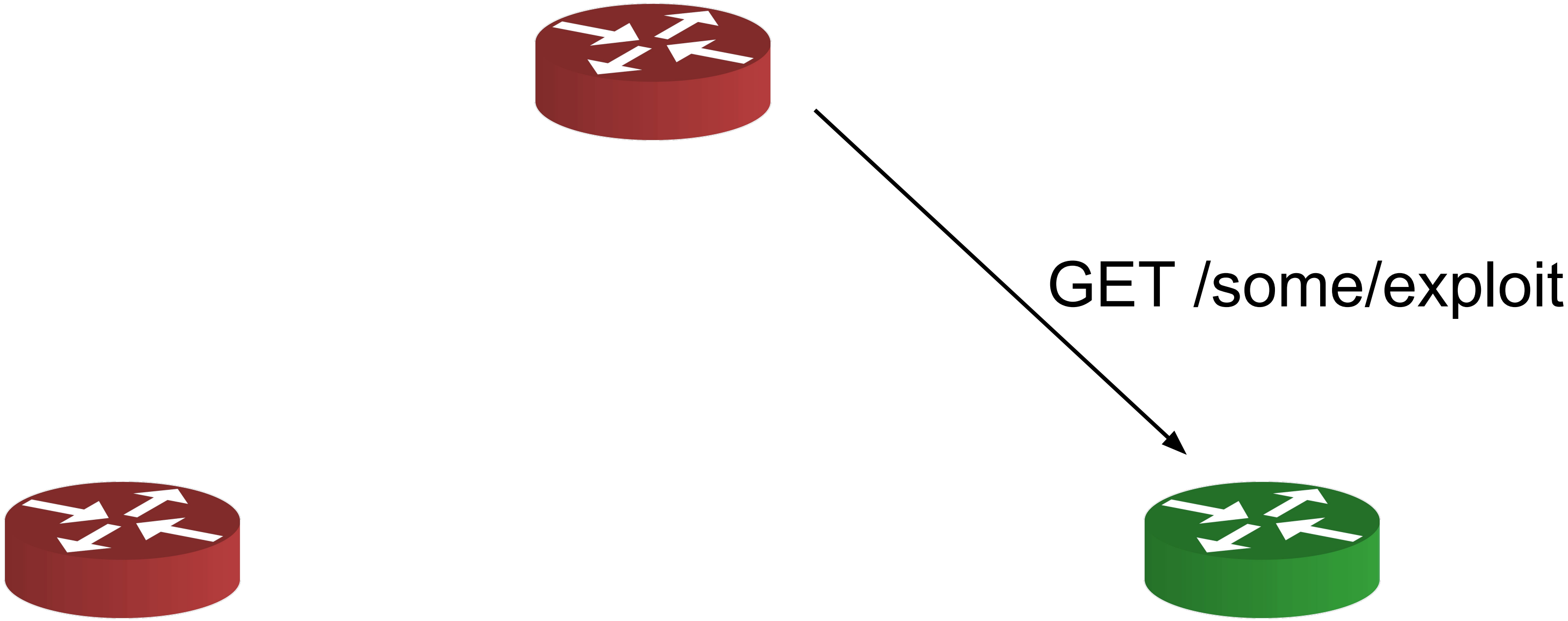
Bitdefender

Peer update

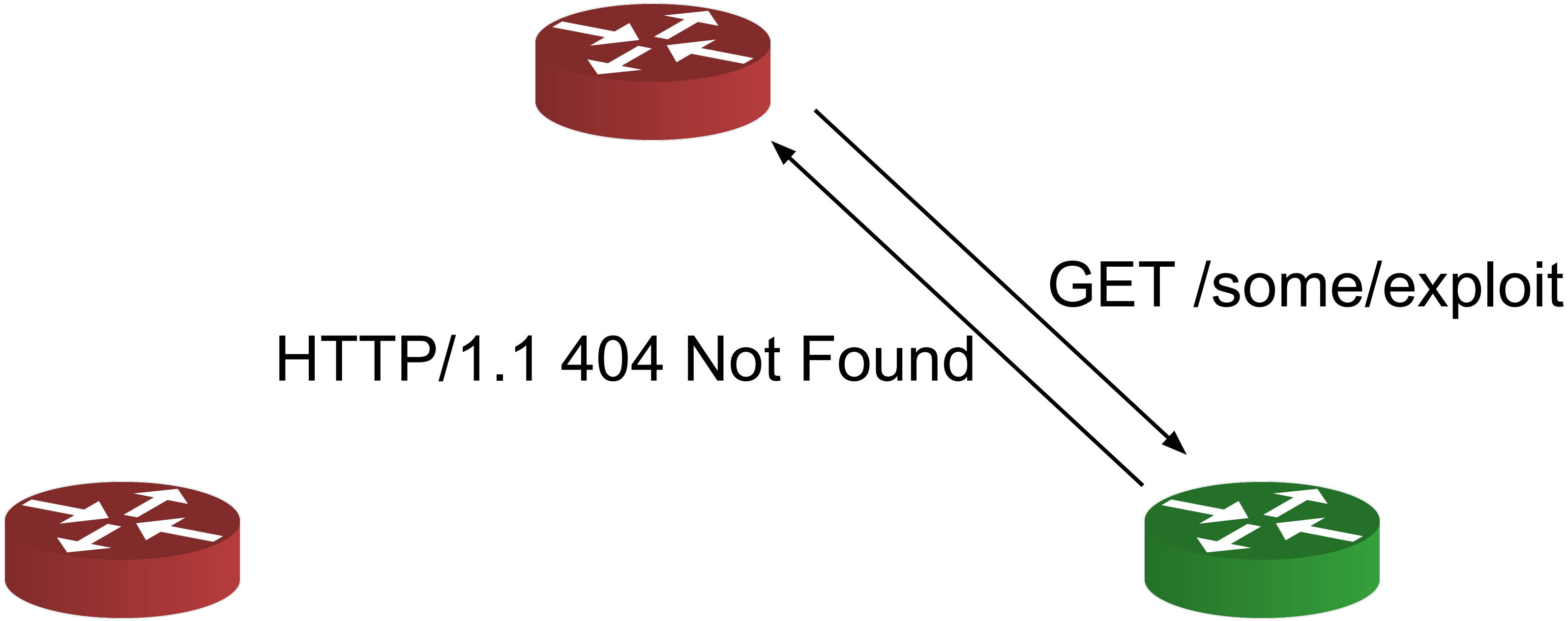


^ - peer reply

Target device reporting



Target device reporting

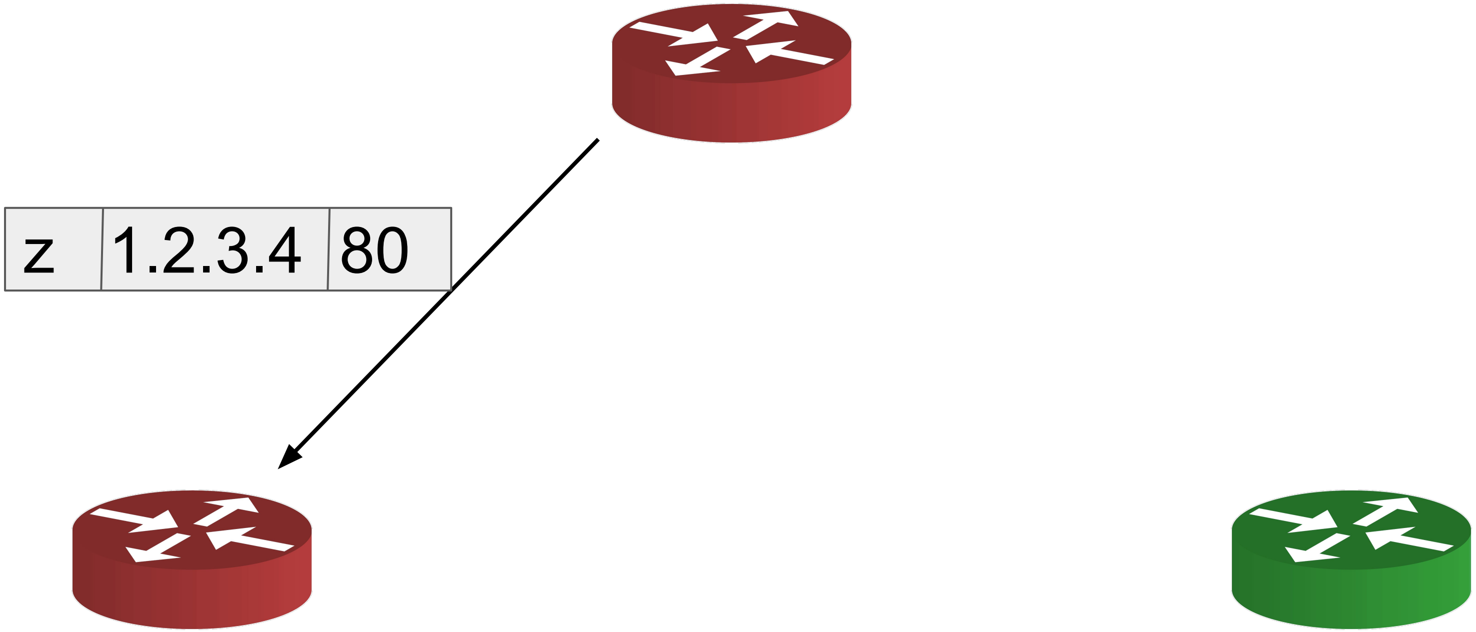


GET /some/exploit

HTTP/1.1 404 Not Found

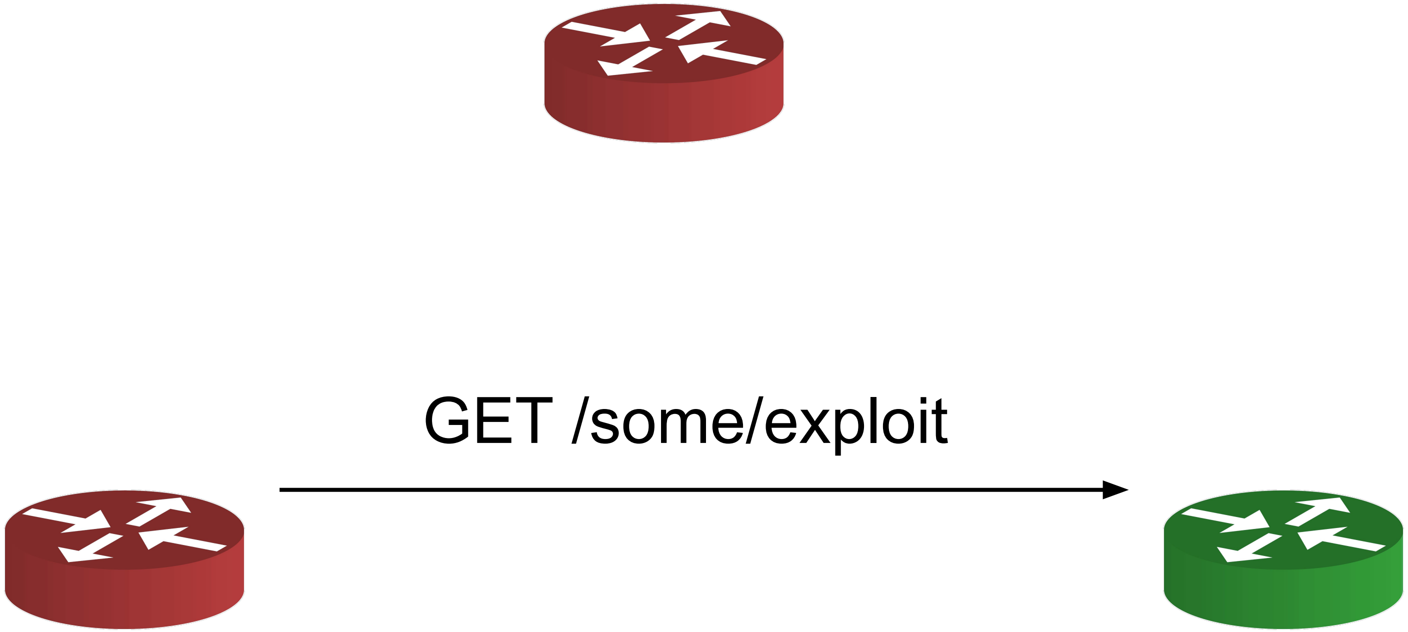
Bitdefender

Target device reporting



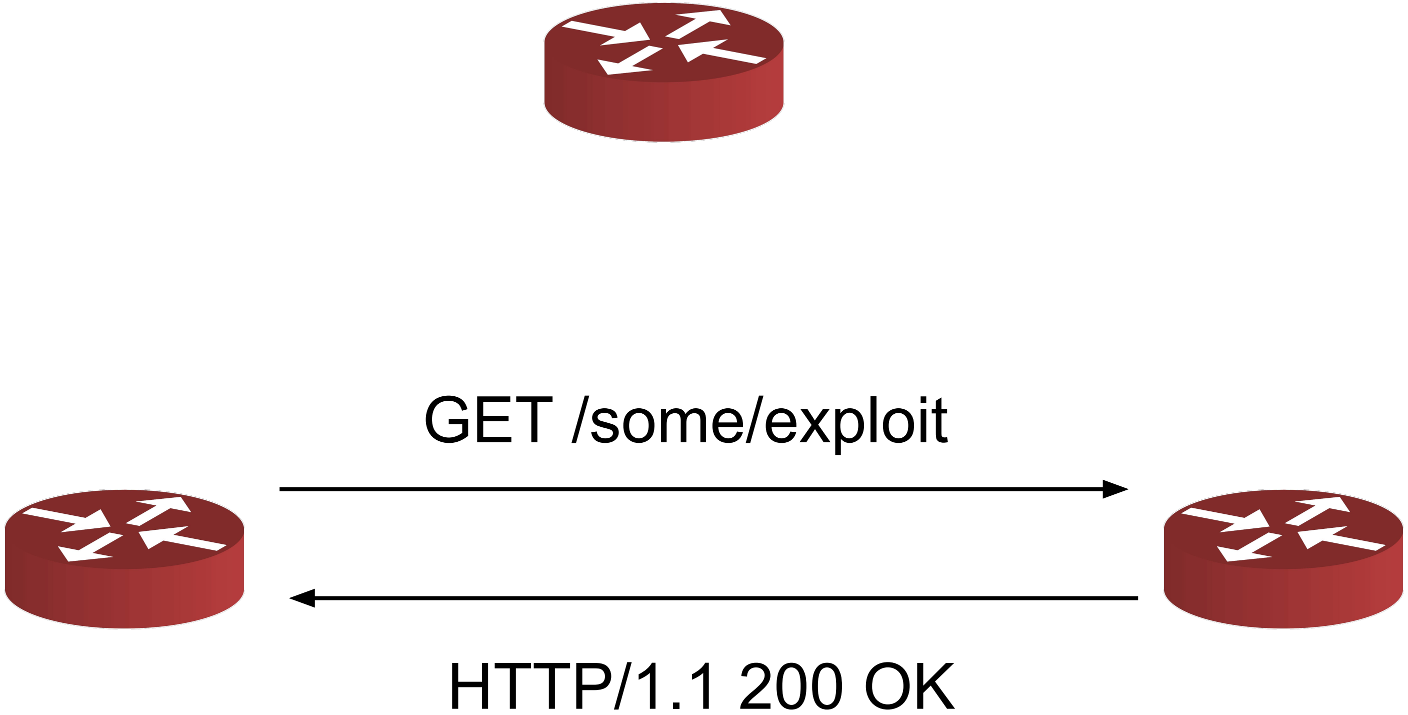
z	1.2.3.4	80

Target device reporting



GET /some/exploit

Target device reporting



GET /some/exploit

HTTP/1.1 200 OK

Hide’n’Seek - Summary

- Infects many kinds of IoT systems
- Decentralized P2P architecture
- Network controlled by the author

Updates

Updates

- ~30 samples
  - Code refactoring
  - New functionality

Updates

- ~30 samples
  - Code refactoring
  - New functionality
- Persistency (copy itself to /etc/init.d/S99abcd)

Updates

- ~30 samples
  - Code refactoring
  - New functionality
- Persistency (copy itself to /etc/init.d/S99abcd)
- Dropping other binaries
  - cpuminer

Updates

- HTTP-based exploits for more IoT vendors

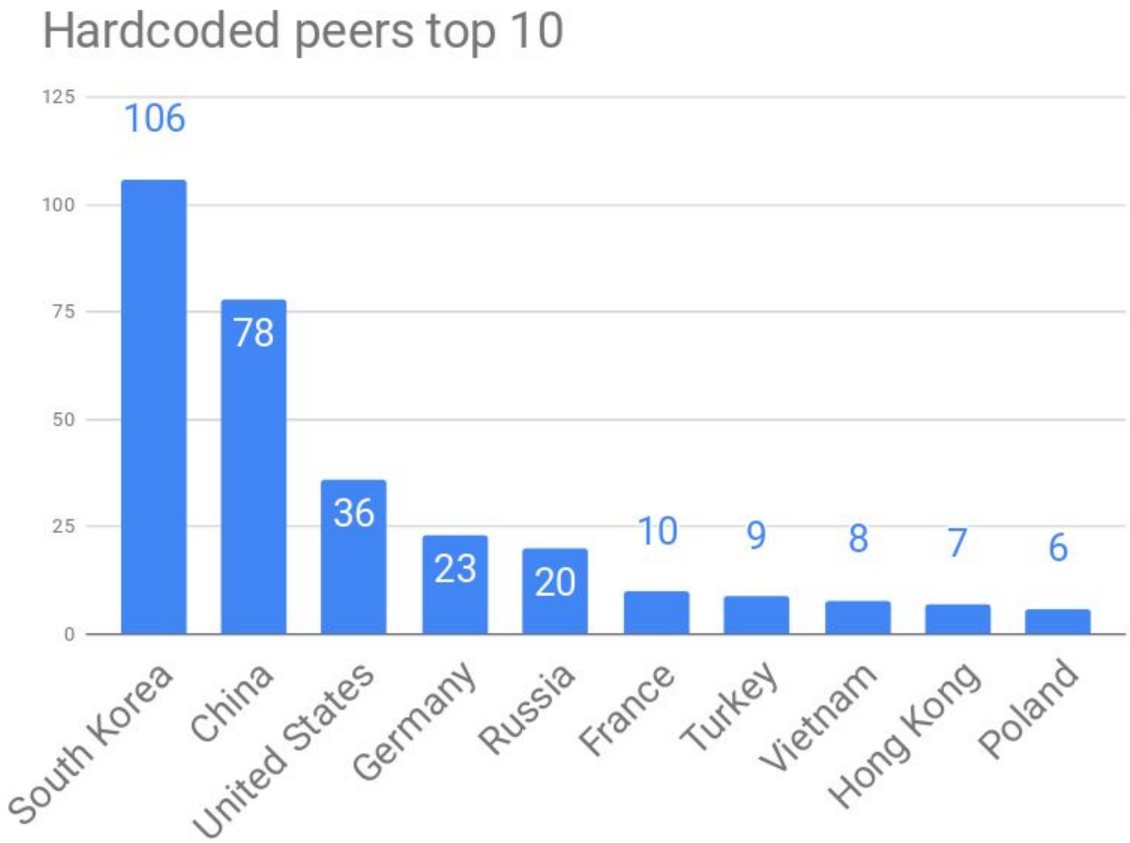
Updates

- HTTP-based exploits for more IoT vendors
- RCE via OrientDB and CouchDB

Updates

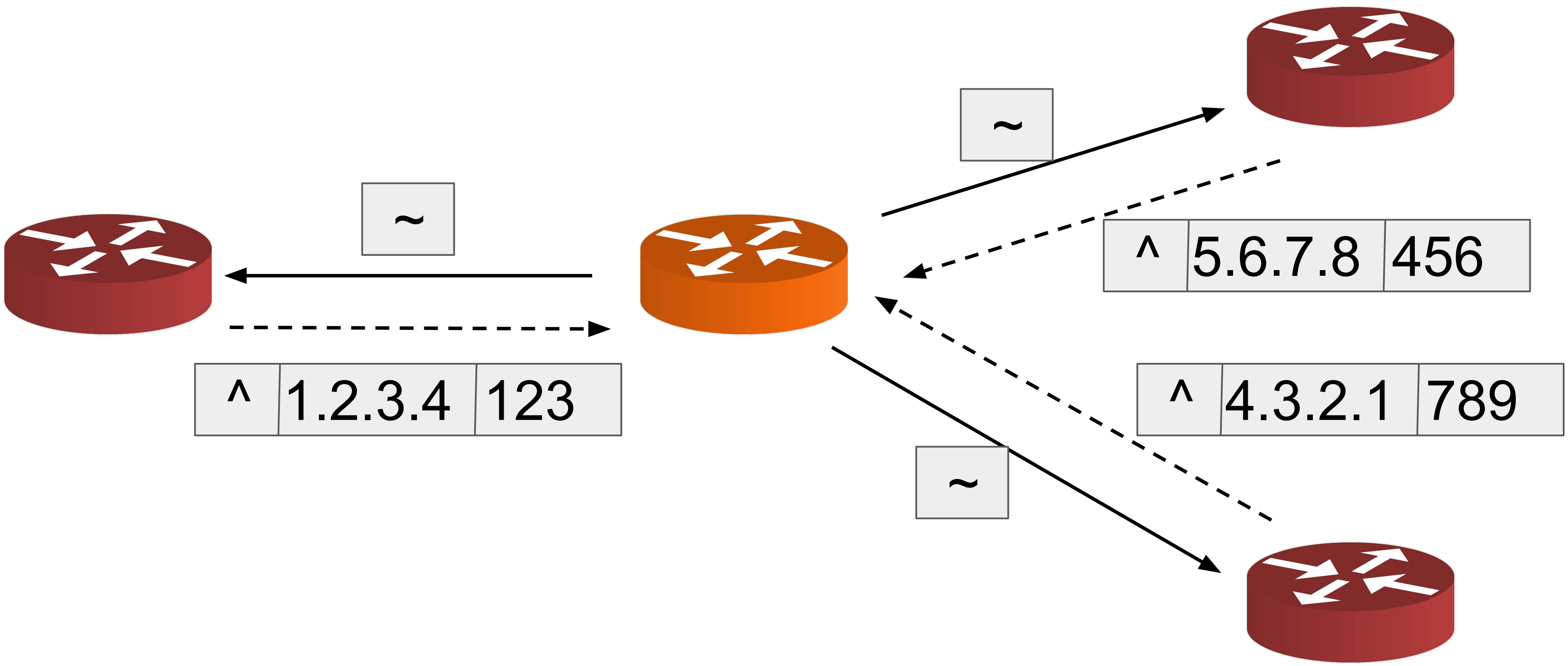
- HTTP-based exploits for more IoT vendors
- RCE via OrientDB and CouchDB
- Hijacking devices via ADB

Monitoring



Hardcoded peers top 10
125
100
75
50
25
0
106
78
36
23
20
10
9
8
7
6
South Korea
China
United States
Germany
Russia
France
Turkey
Vietnam
Hong Kong
Poland

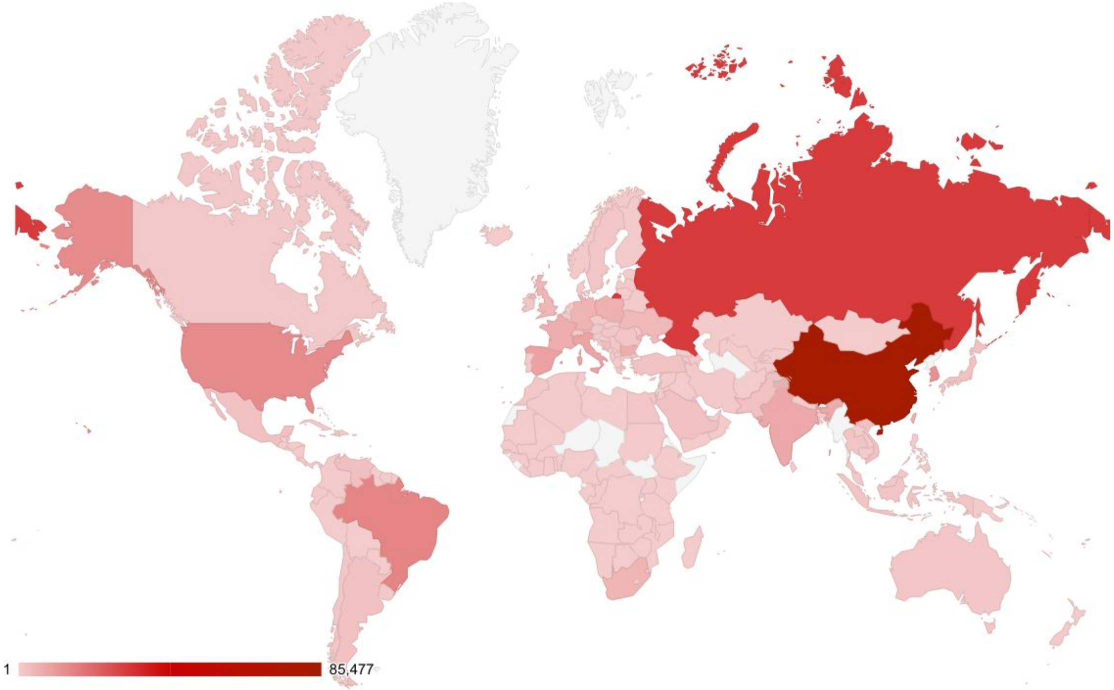
Monitoring



Bitdefender

Monitoring

- ~300,000 peers



Bitdefender

Conclusions

- A new trend in the IoT landscape
  - Qbot, Mirai

Conclusions

- A new trend in the IoT landscape
  - Qbot, Mirai
  - Hajime

Conclusions

- A new trend in the IoT landscape
  - Qbot, Mirai
  - Hajime, Satori

Conclusions

- A new trend in the IoT landscape
  - Qbot, Mirai
  - Hajime, Satori, Reaper

Conclusions

- A new trend in the IoT landscape
  - Qbot, Mirai
  - Hajime, Satori, Reaper, VPNFilter

Conclusions

- A new trend in the IoT landscape
  - Qbot, Mirai
  - Hajime, Satori, Reaper, VPNFilter, HNS

Conclusions

- A new trend in the IoT landscape
  - Qbot, Mirai
  - Hajime, Satori, Reaper, VPNFilter, HNS
- More threats to come

Q&A