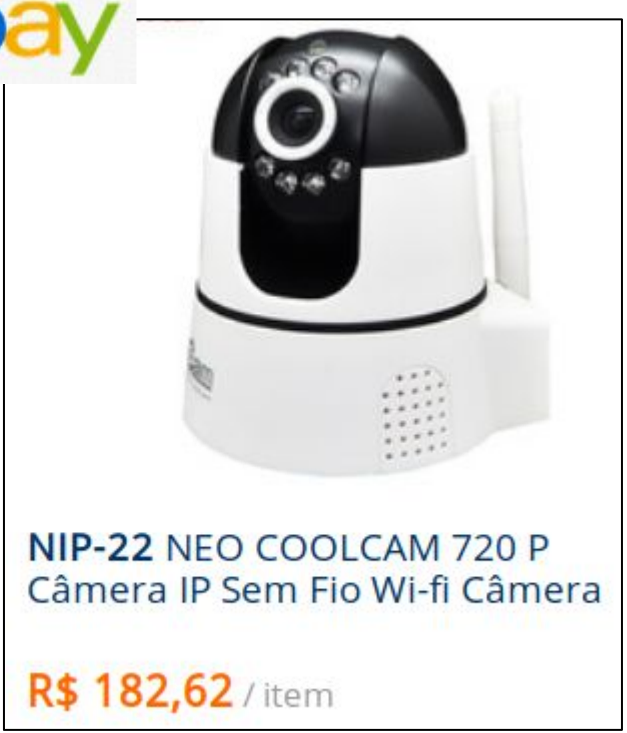
The Evolution of the Bashlite and Mirai IoT Botnets

Ítalo Cunha

Artur Marzano, David Alexander, Elverton Fazzion, Osvaldo Fonseca, Cristine Hoepers, Klaus Steding-Jessen, Marcelo H. P. C. Chaves, Dorgival Guedes, Wagner Meira Jr.

UFMG UFSJ cert.br

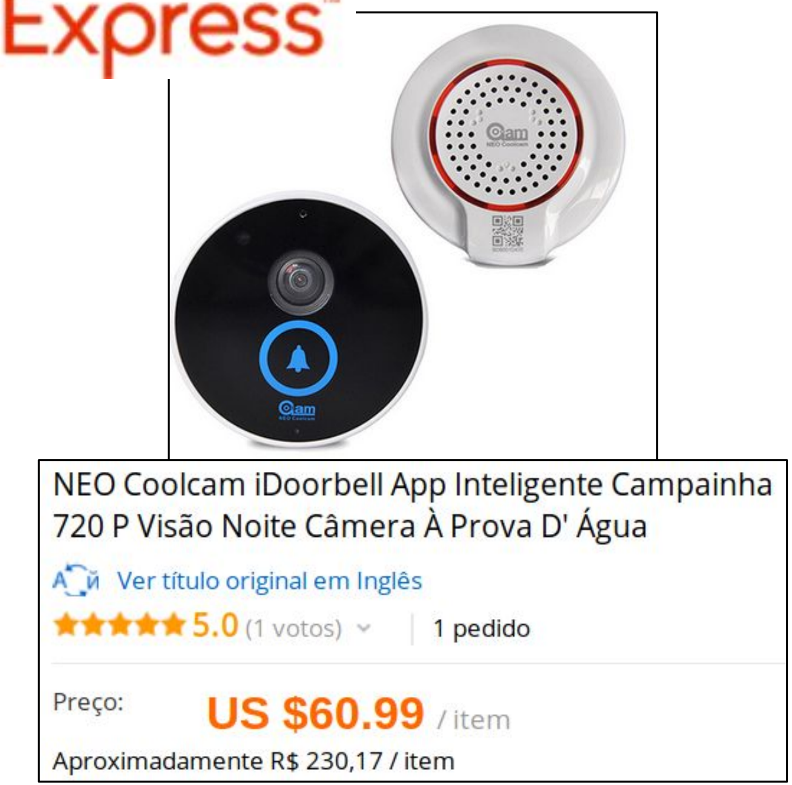
ebay



NIP-22 NEO COOLCAM 720 P Câmera IP Sem Fio Wi-fi Câmera

R$ 182,62 / item

AliExpress™



NEO Coolcam iDoorbell App Inteligente Campainha 720 P Visão Noite Câmera À Prova D' Água

Ver título original em Inglês

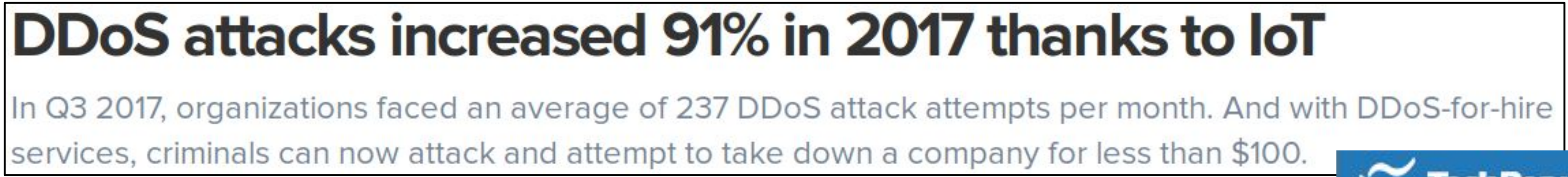
★★★★★ 5.0 (1 votos) | 1 pedido

Preço: US $60.99 / item

Aproximadamente R$ 230,17 / item

IoT Devices Are Vulnerable

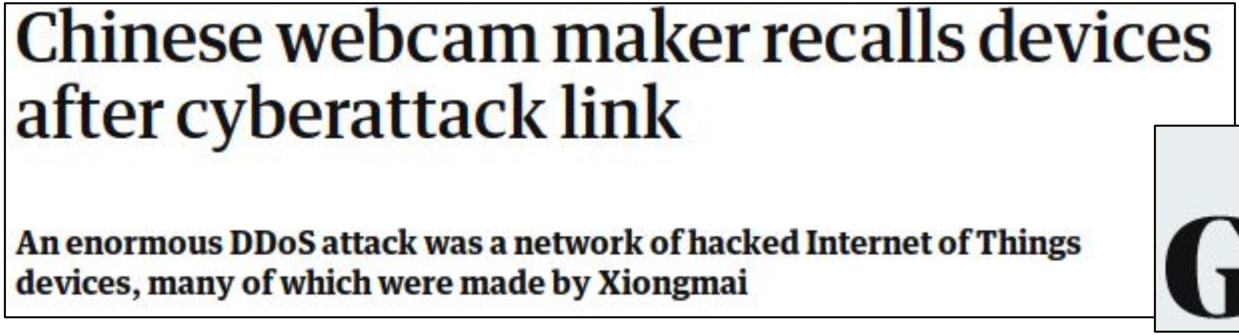
- Very competitive market, small profit margins
- Limited resources for security
- Very hard to update



DDoS attacks increased 91% in 2017 thanks to IoT

In Q3 2017, organizations faced an average of 237 DDoS attack attempts per month. And with DDoS-for-hire services, criminals can now attack and attempt to take down a company for less than $100.

TechRepublic.

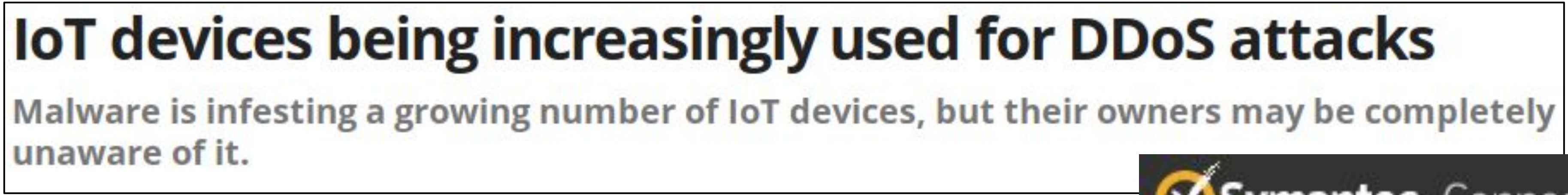


Chinese webcam maker recalls devices after cyberattack link

An enormous DDoS attack was a network of hacked Internet of Things devices, many of which were made by Xiongmai

The Guardian

International edition



IoT devices being increasingly used for DDoS attacks

Malware is infesting a growing number of IoT devices, but their owners may be completely unaware of it.

Symantec. Connect

Goal

Characterize the Bashlite and Mirai botnets
to understand their use and operation,
with a focus on how these practices have evolved

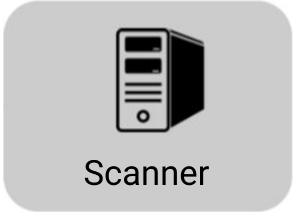
- Identify the infrastructure used to support botnets
- Characterize attack targets

Goal

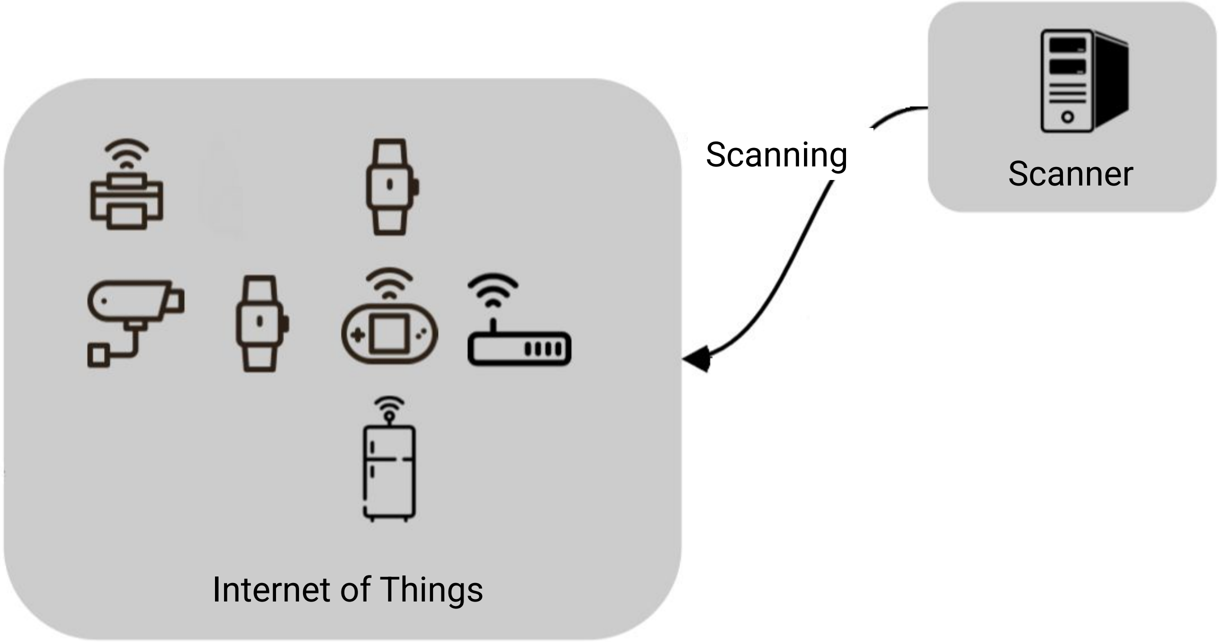
Characterize the Bashlite and Mirai botnets
to understand their use and operation,
with a focus on how these practices have evolved

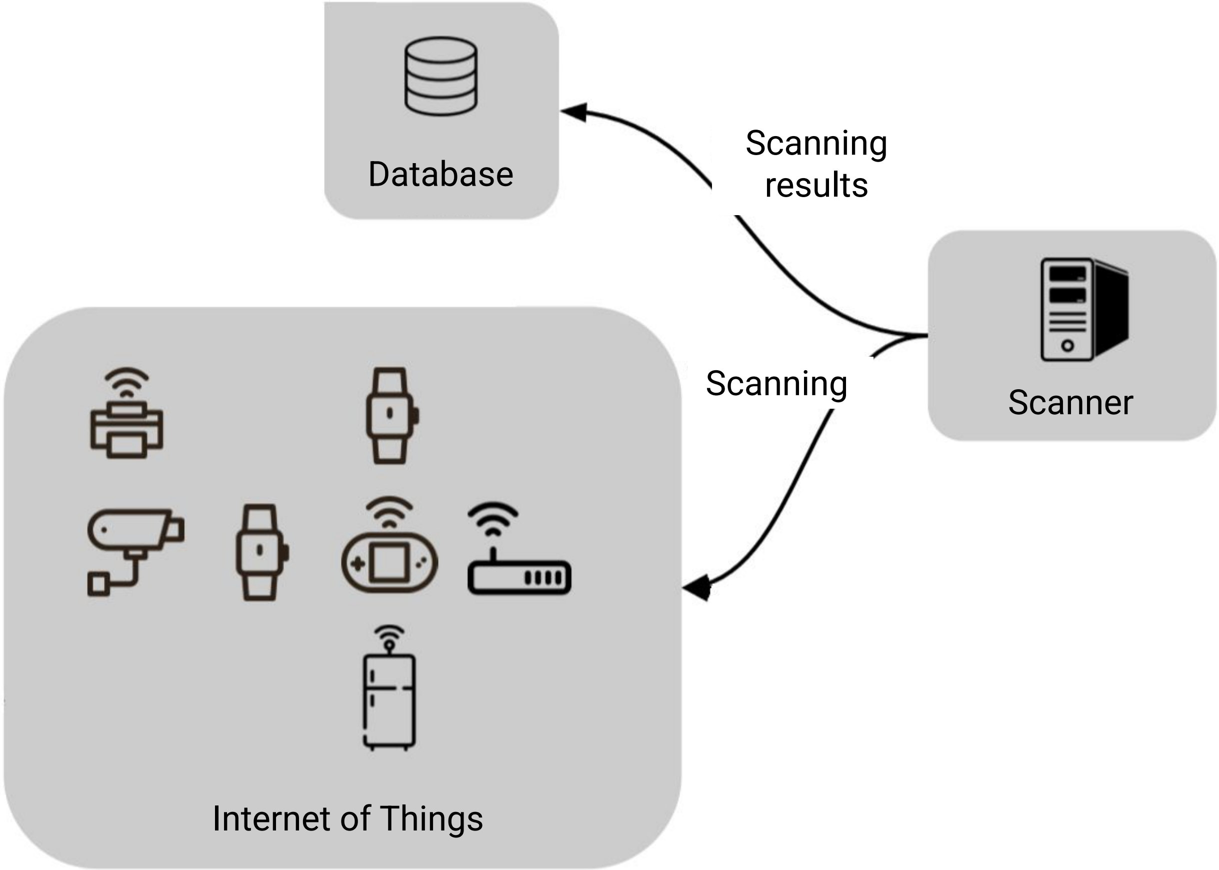
- Identify the infrastructure used to support botnets
- Characterize attack targets
- Operator interactions with botnets

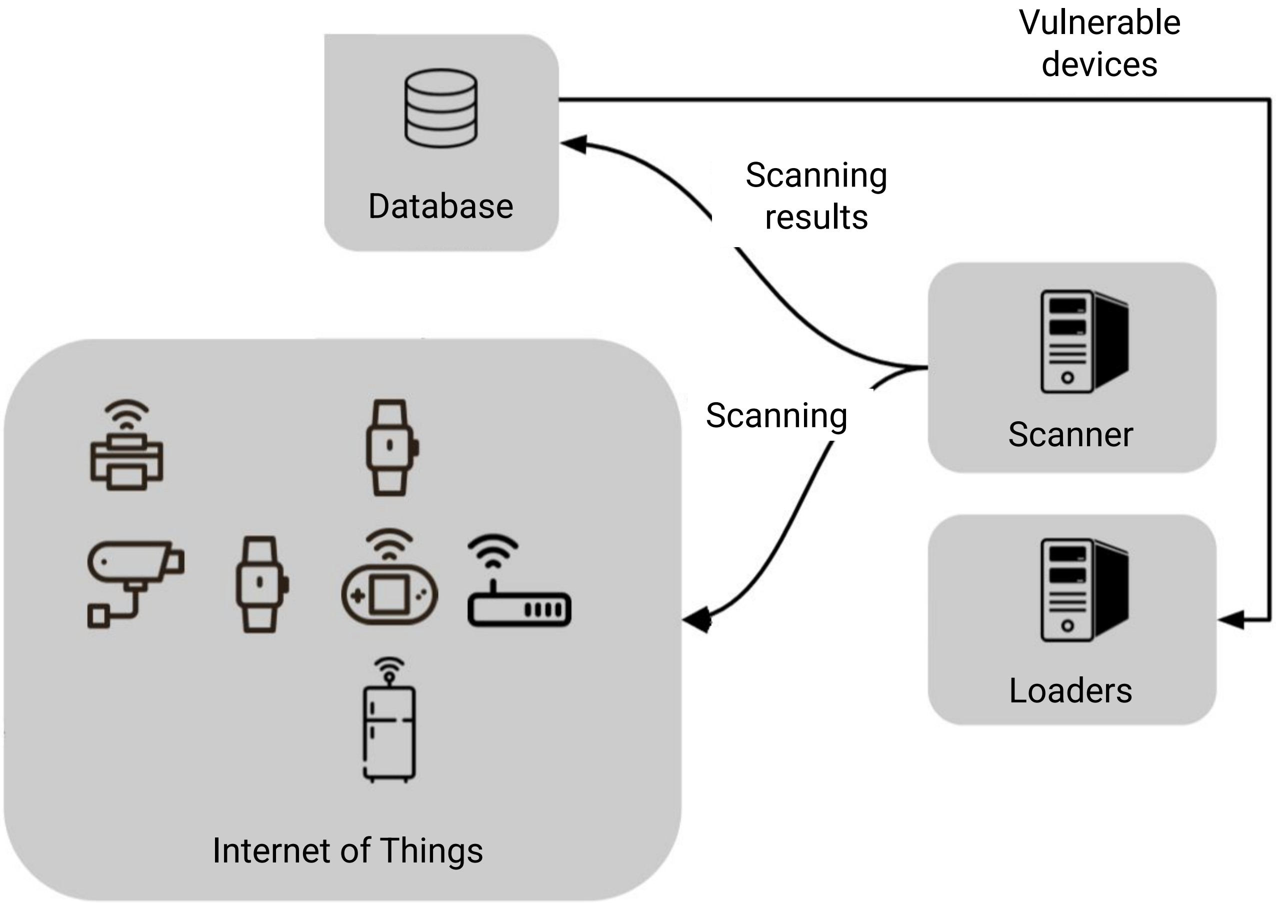
The Bashlite and Mirai Botnets

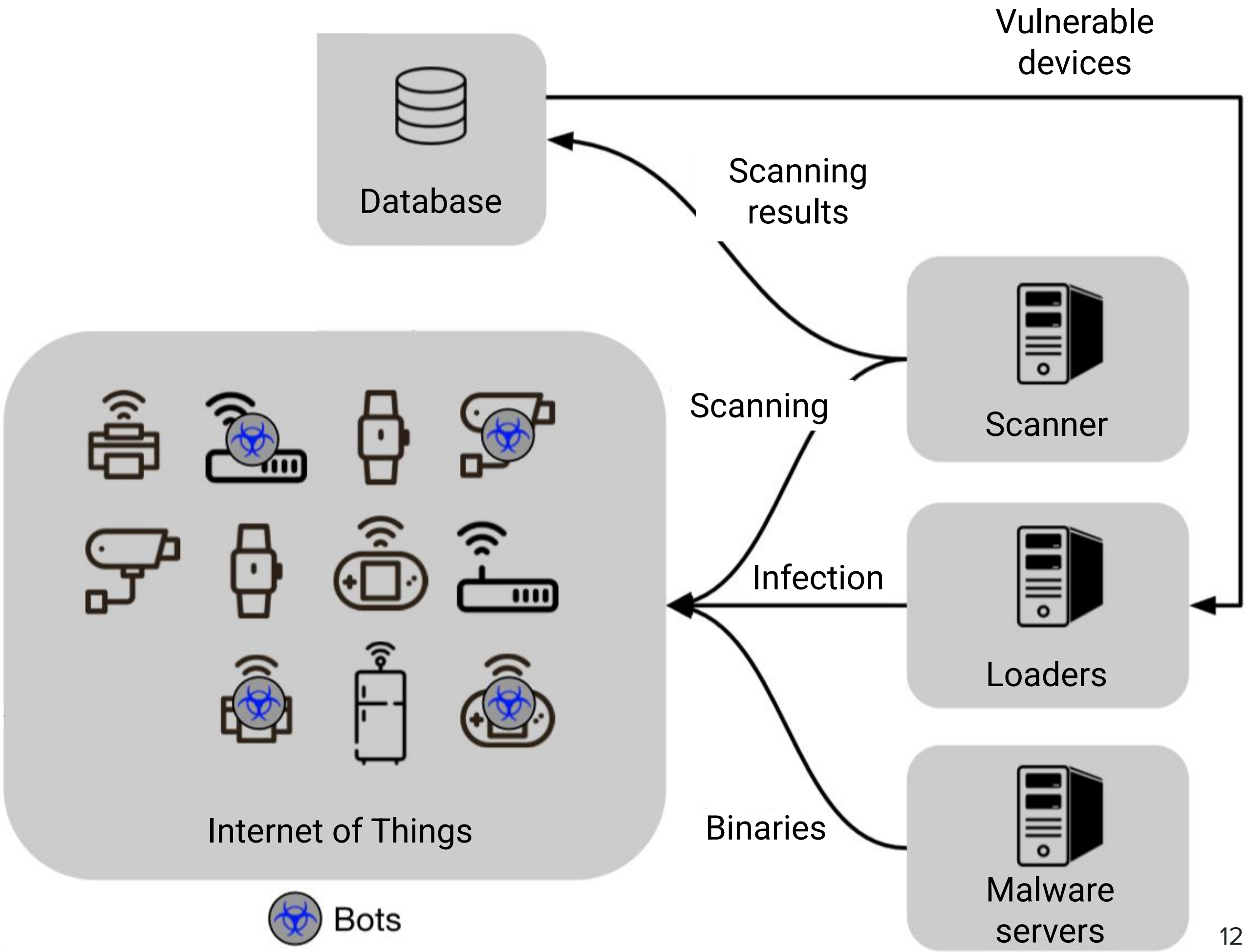


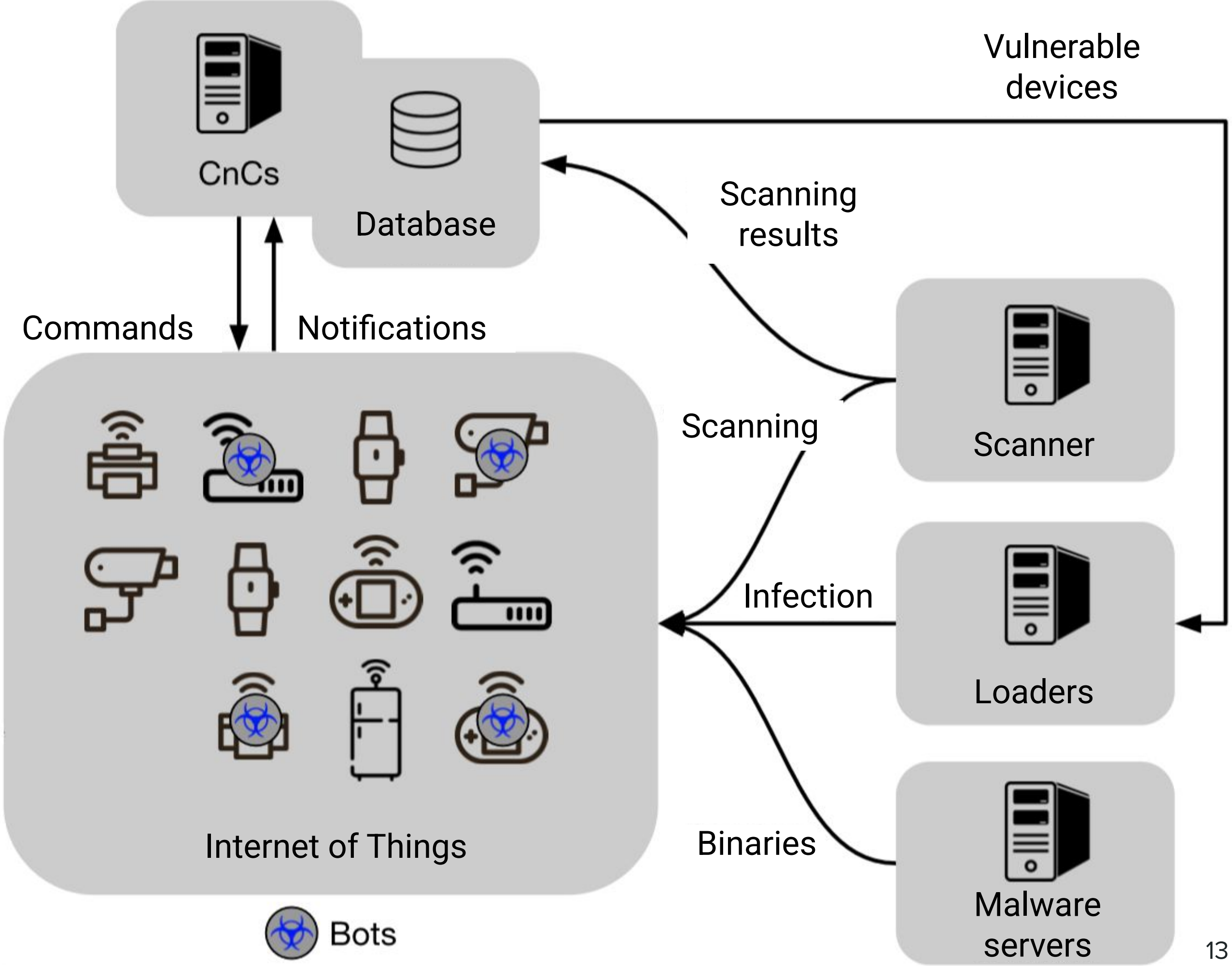
Scanner

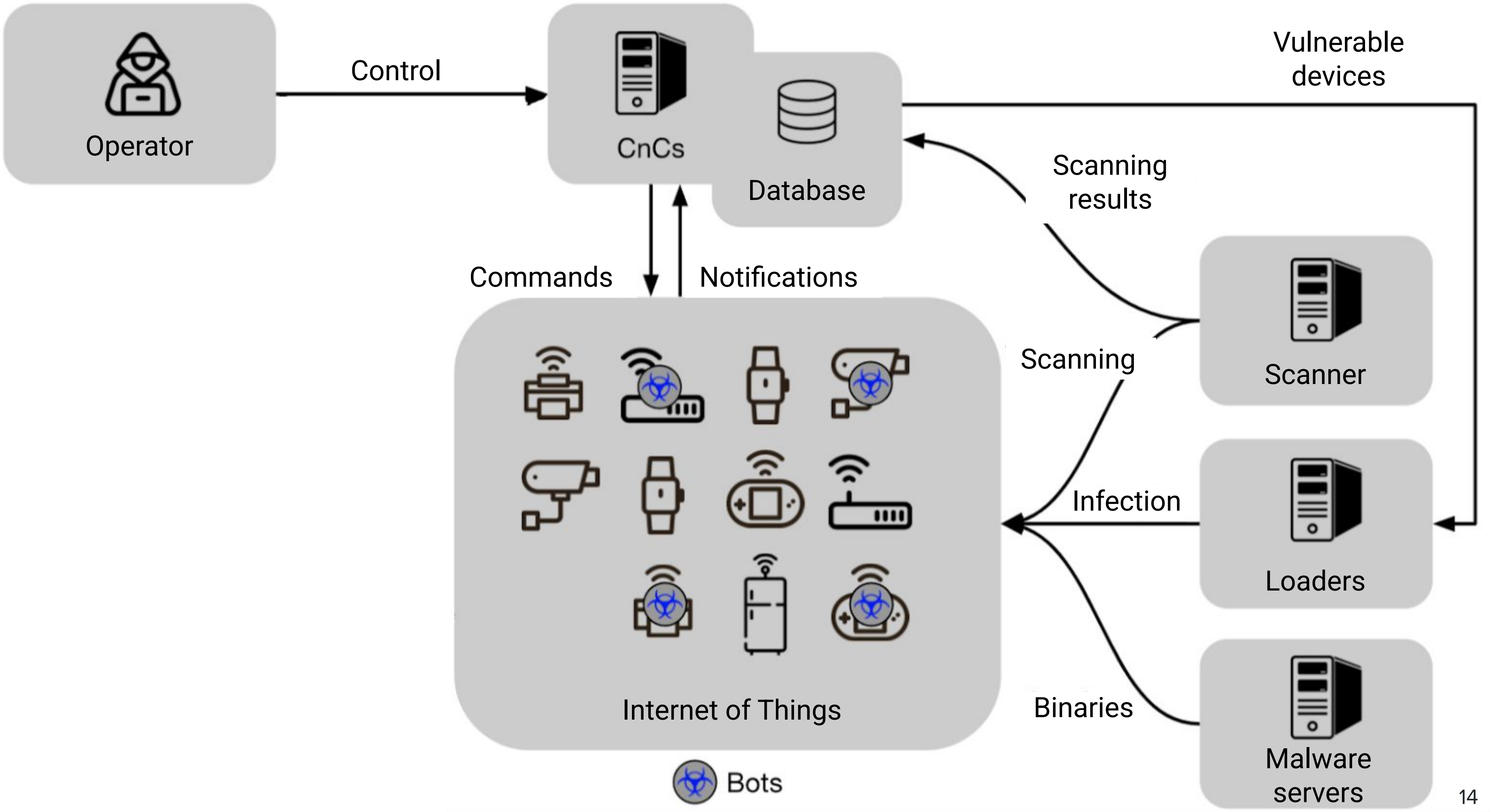

Internet of Things
Scanning
Scanner

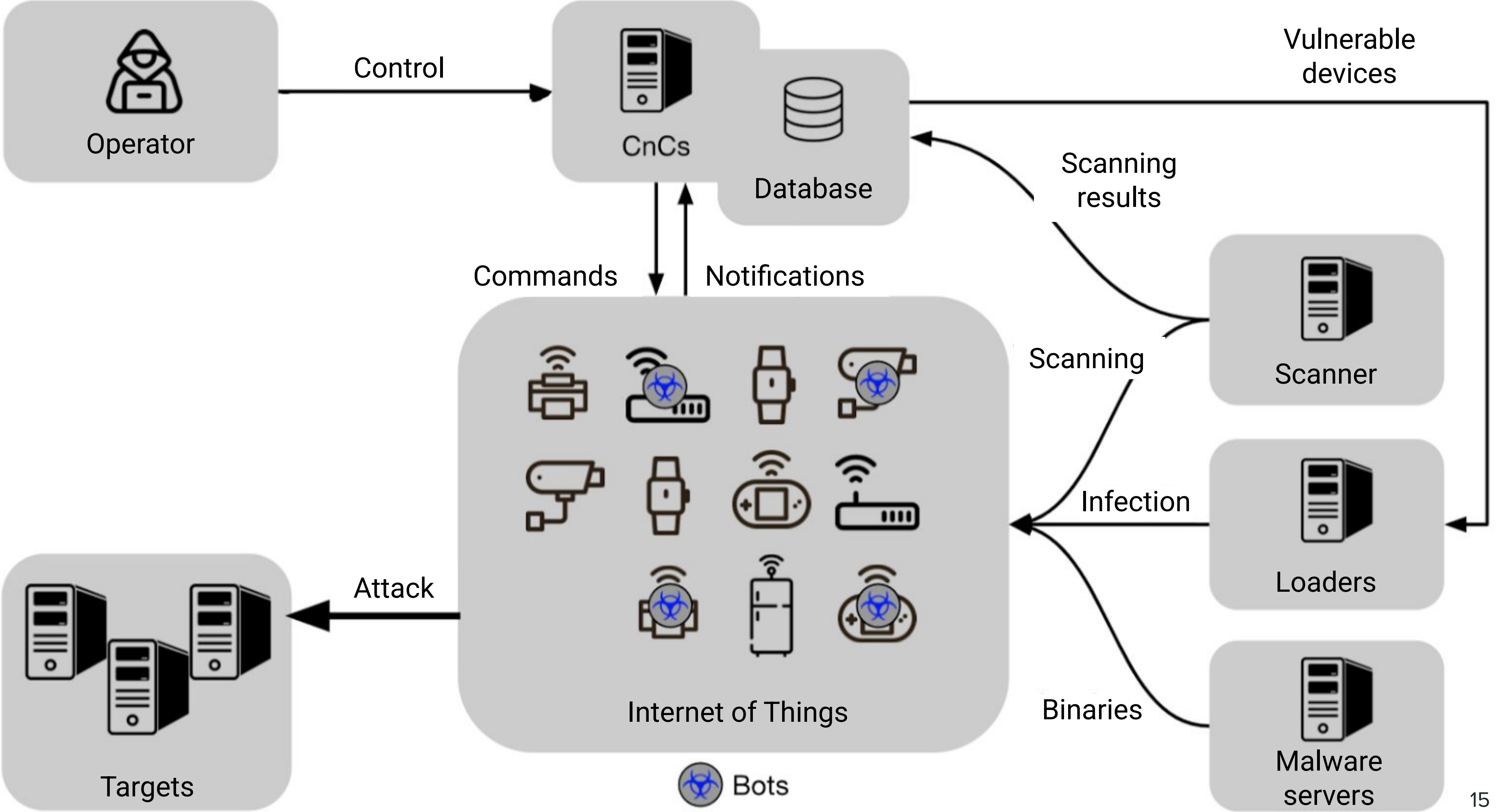

Database
Scanning
results
Scanner
Scanning
Internet of Things

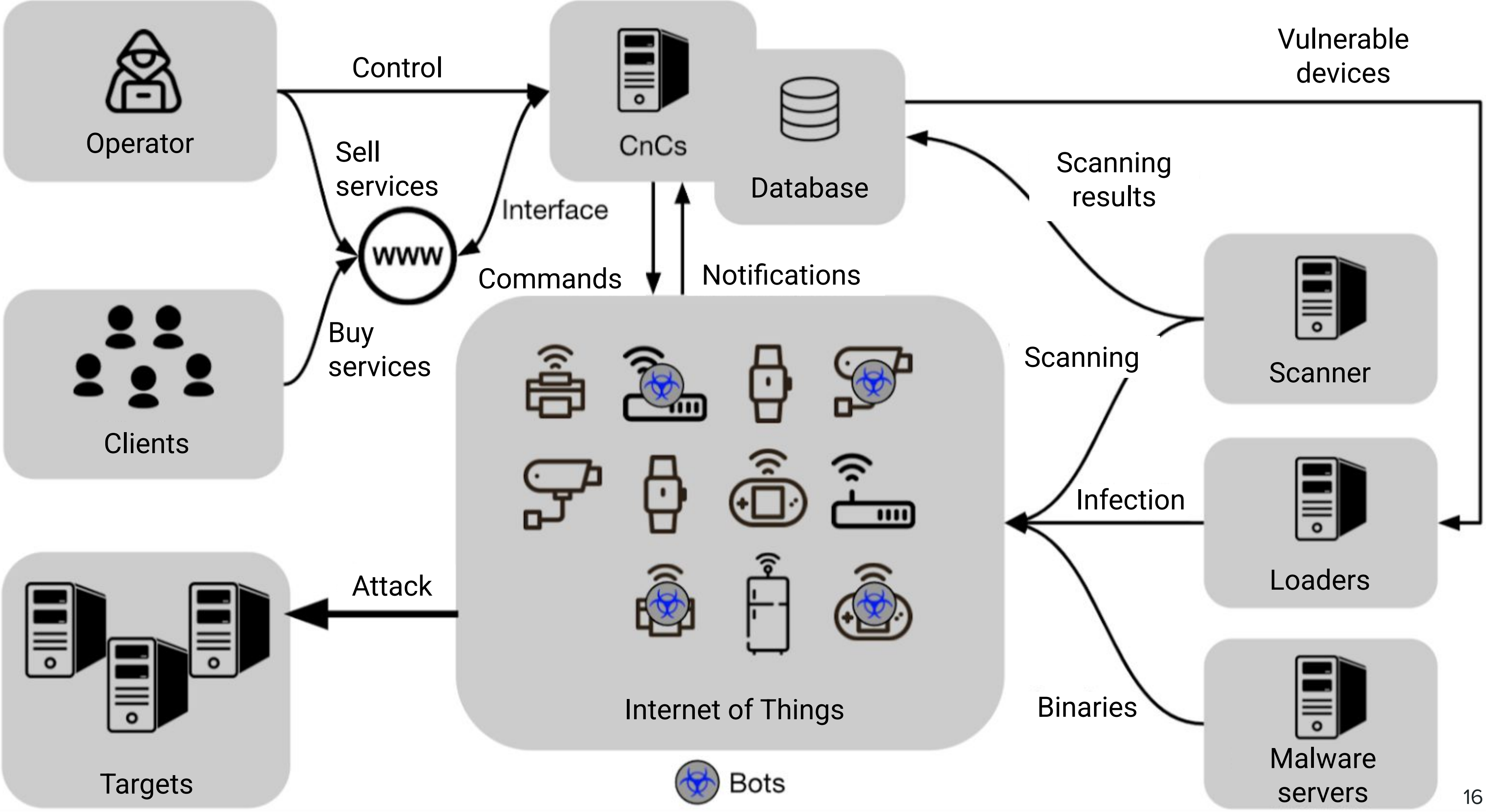

Vulnerable devices
Database
Scanning results
Scanner
Scanning
Loaders
Internet of Things

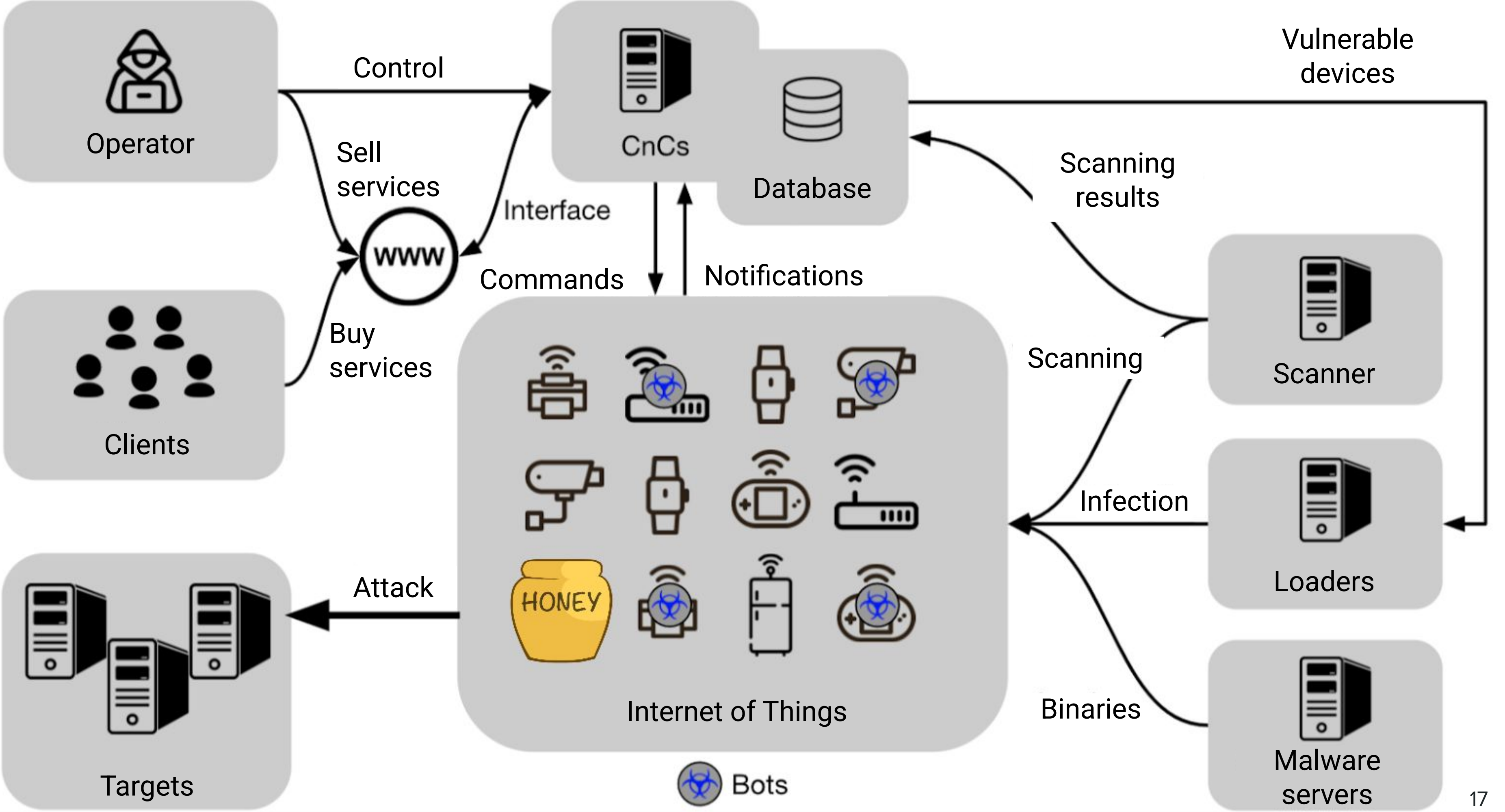

Vulnerable devices
Database
Scanning results
Scanner
Scanning
Infection
Loaders
Binaries
Malware servers
Internet of Things
Bots


Vulnerable devices
CnCs
Database
Scanning results
Commands
Notifications
Scanner
Scanning
Infection
Loaders
Binaries
Malware servers
Internet of Things
Bots


Operator
Control
CnCs
Database
Vulnerable devices
Scanning results
Commands
Notifications
Scanner
Scanning
Infection
Loaders
Binaries
Malware servers
Internet of Things
Bots

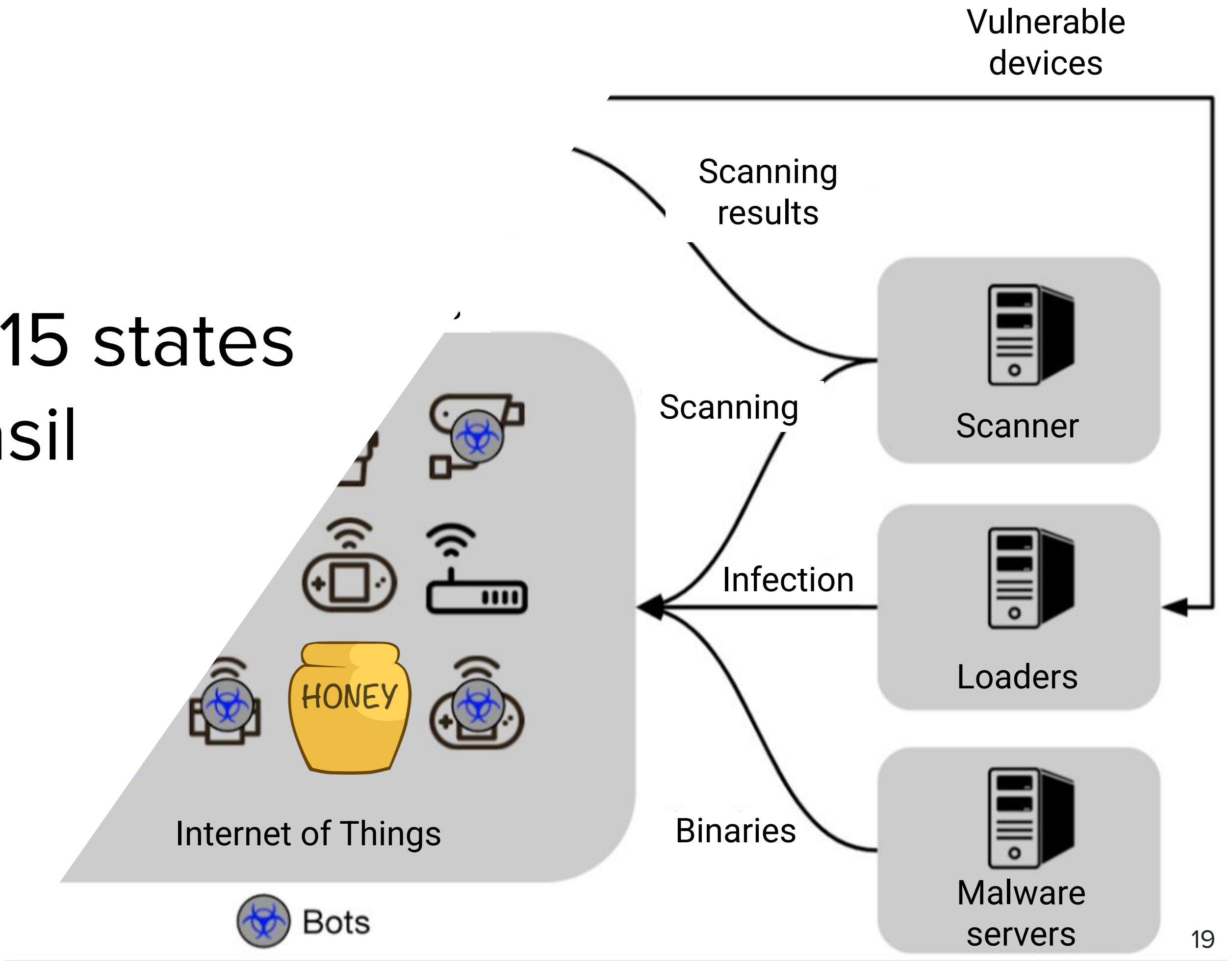

Operator
Control
CnCs
Database
Vulnerable devices
Scanning results
Commands
Notifications
Scanner
Scanning
Infection
Loaders
Attack
Targets
Internet of Things
Bots
Binaries
Malware servers

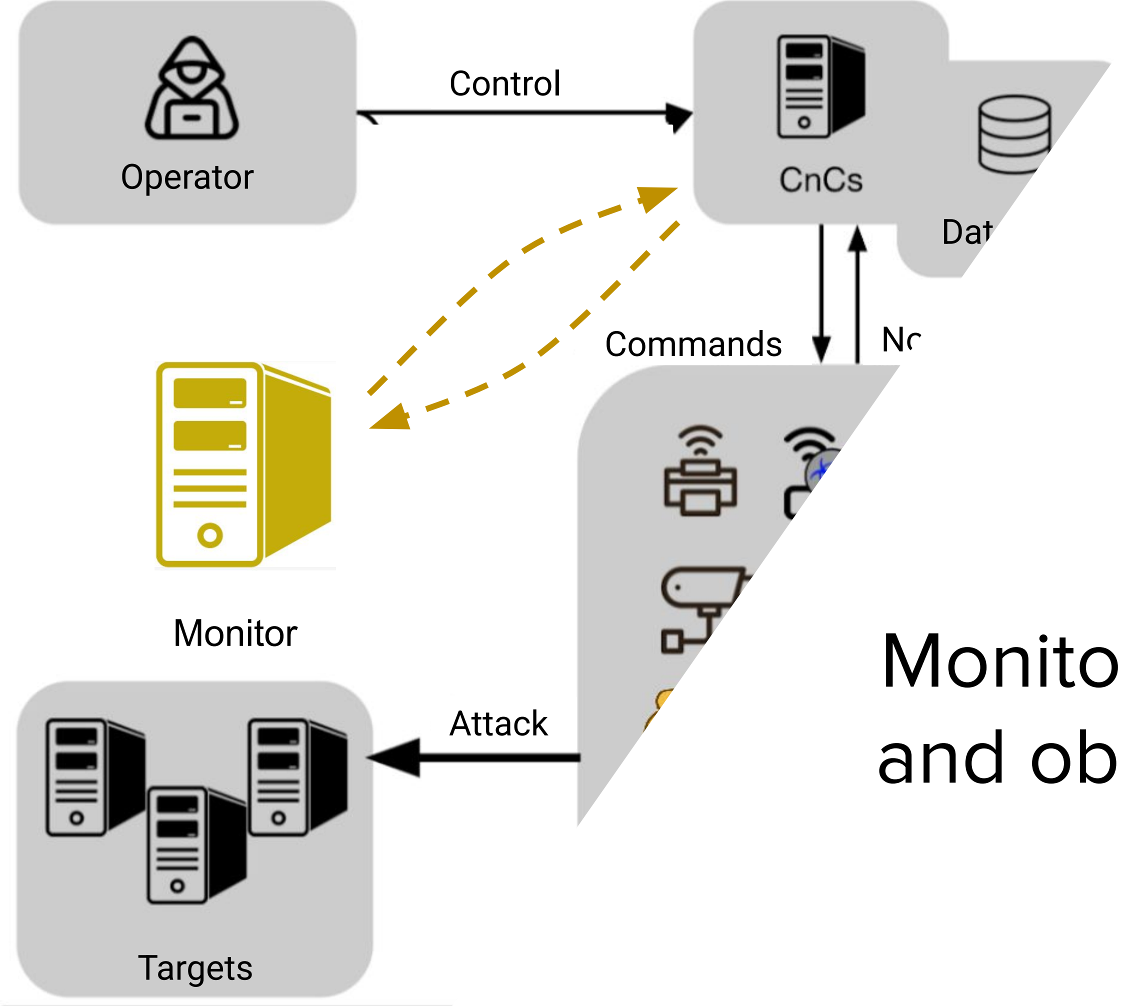

Operator
Control
Sell services
Interface
CnCs
Database
Vulnerable devices
Scanning results
Clients
Buy services
Commands
Notifications
Scanning
Scanner
Infection
Loaders
Binaries
Malware servers
Attack
Targets
Internet of Things
Bots


Operator
Control
CnCs
Database
Vulnerable devices
Sell services
Interface
www
Scanning results
Clients
Commands
Notifications
Buy services
Scanning
Scanner
Infection
Loaders
HONEY
Attack
Targets
Internet of Things
Binaries
Malware servers
Bots

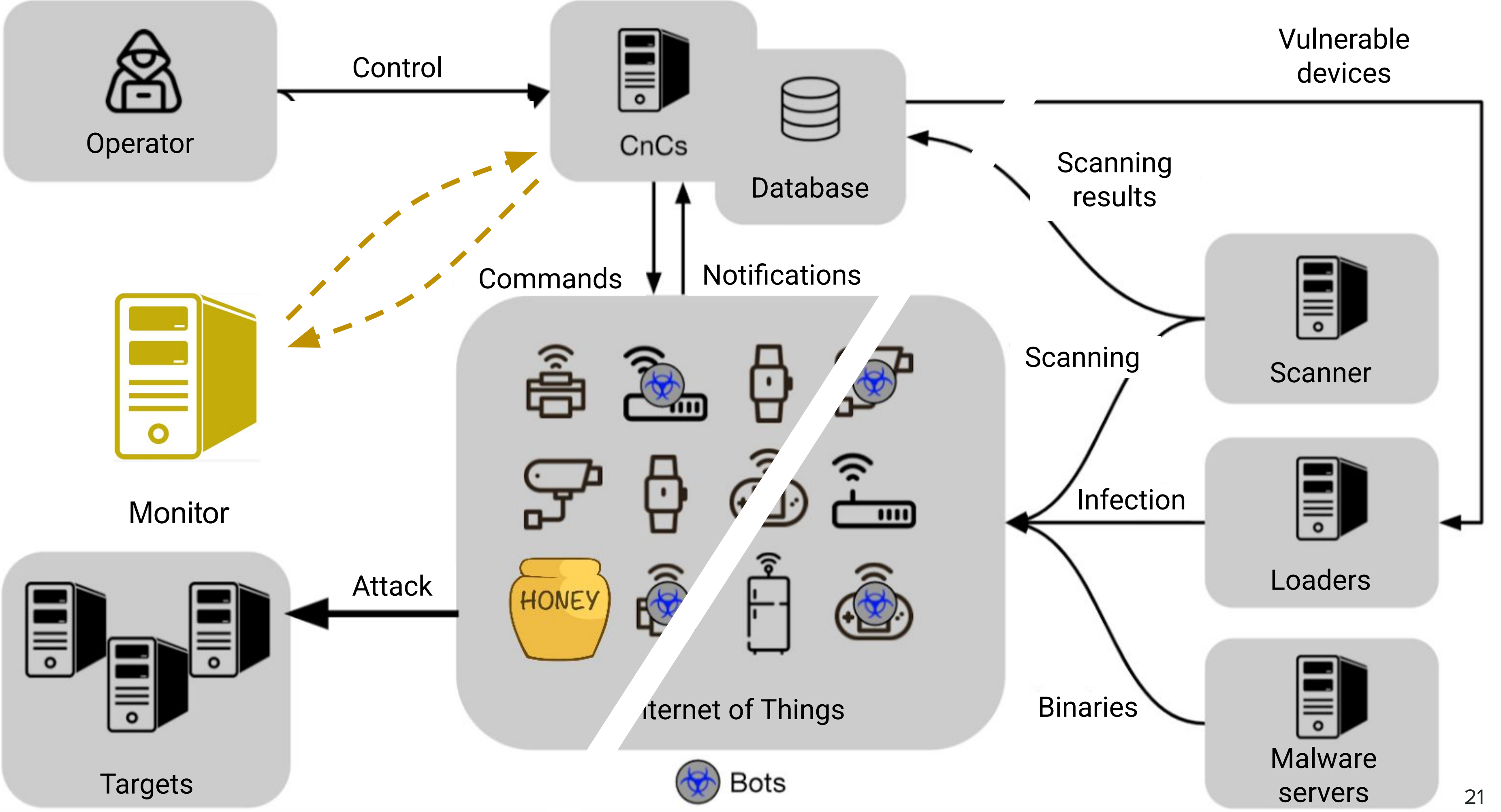
Monitoring Infrastructure

47 honeypots in 15 states across Brasil





Monitor connects to CnC and observes commands


Operator
Control
CnCs
Database
Vulnerable devices
Scanning results
Monitor
Commands
Notifications
Scanner
Scanning
Infection
Loaders
HONEY
Internet of Things
Attack
Targets
Binaries
Malware servers
Bots

Dataset

- Period: **01/01/2017 à 13/11/2017**

- Scanner and loader honeypots
  - **342.001.071** commands attempted
  - **2.385.460** scanner and loader IP addresses

- C&C monitor
  - **486** IP addresses hosting C&Cs
  - **83.101** observed attacks
  - **29.428** different targets

Botnet Infrastructure

- Identify networks that host the botnet infrastructure
  - Map IP addresses to autonomous systems (AS)

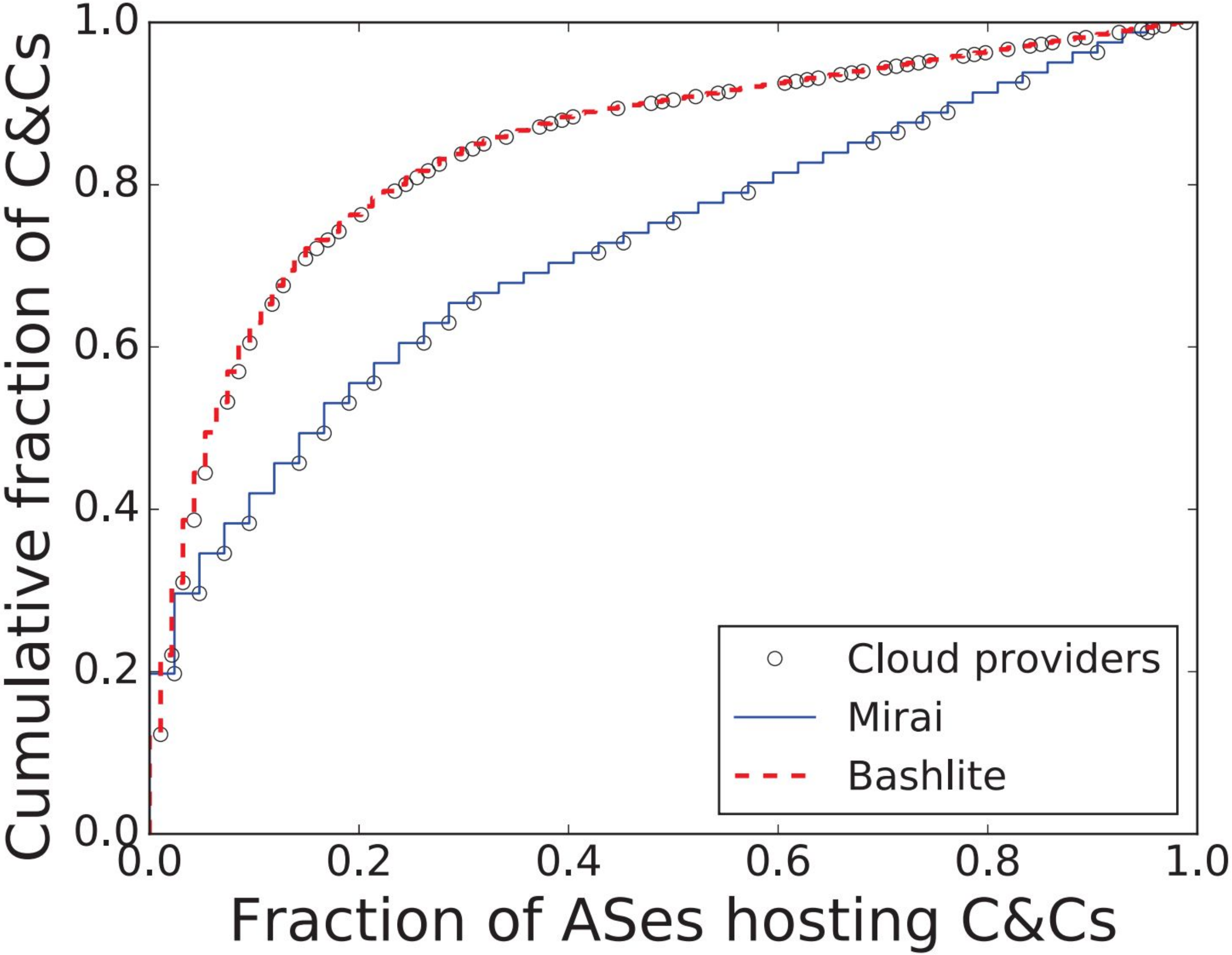
- AS classification using CAIDA’s dataset
  - Transit/access
  - Infrastructure provider (content and hosting)
  - Enterprise

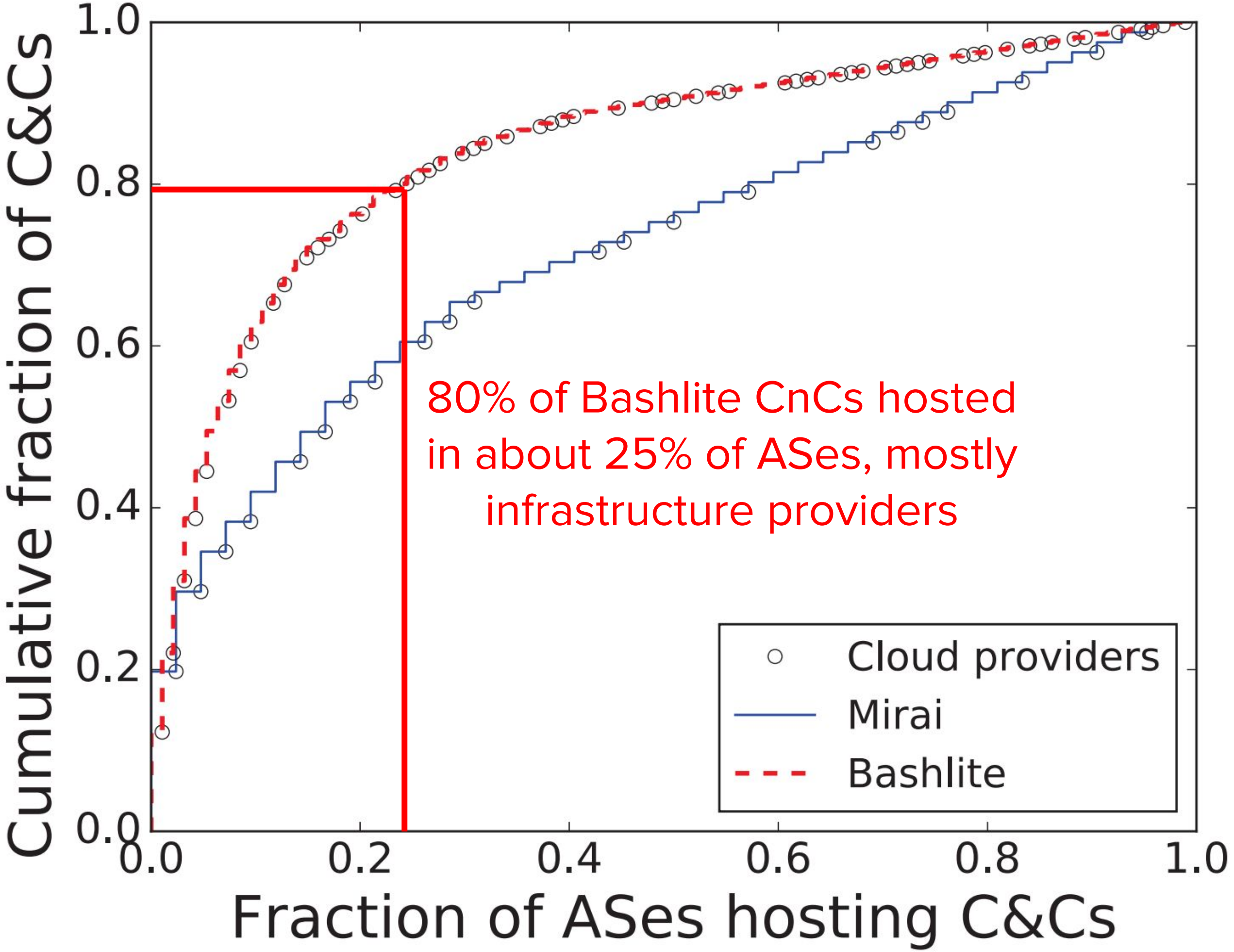
Botnet Infrastructure Location

- *C&C* in 93 ASes
- *Malware server* in 243 ASes

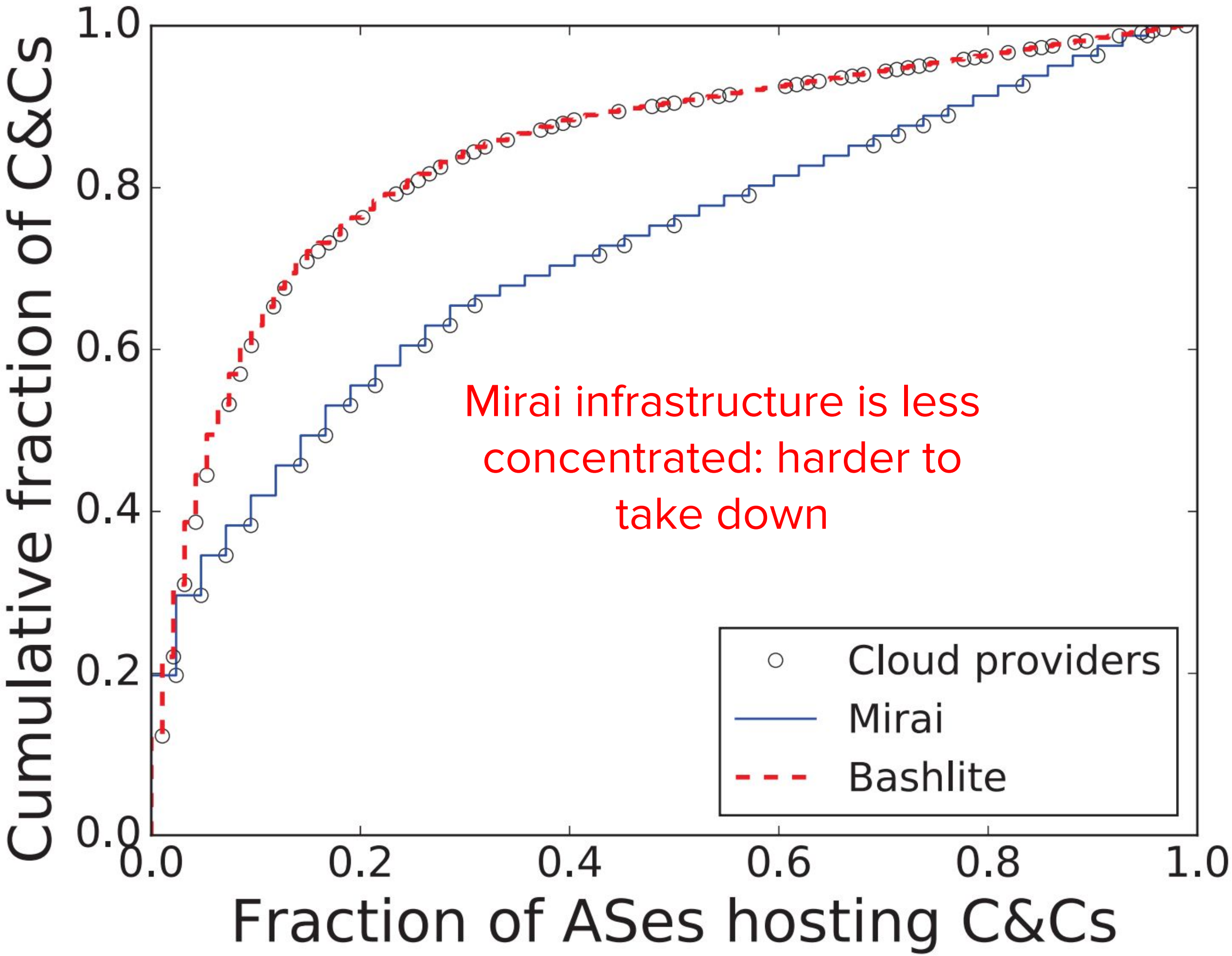
Botnet Infrastructure Location

- *C&C* in 93 ASes
- *Malware server* in 243 ASes
- *Loaders* and *scanners* in 12842 ASes
    - 20% of the Internet

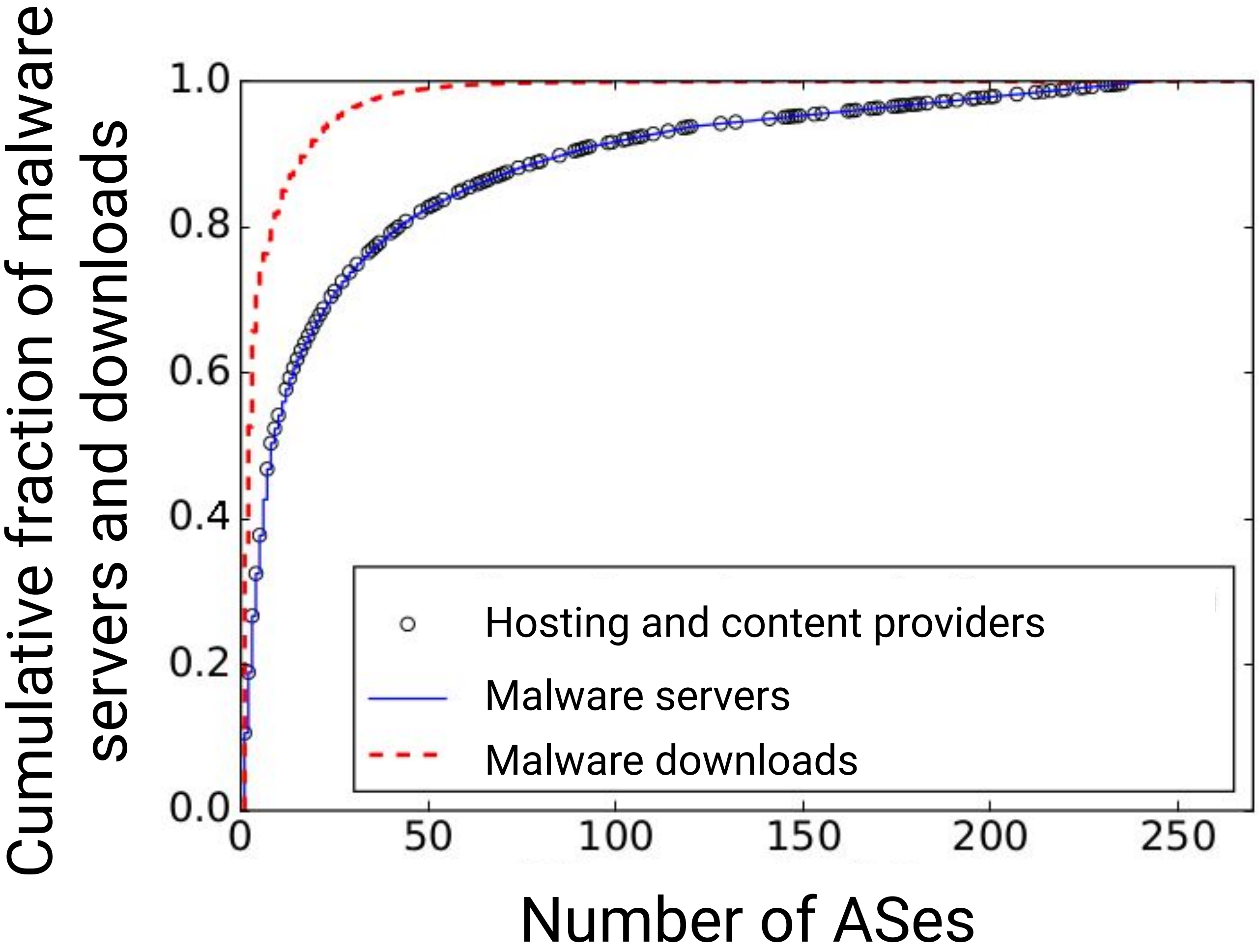

1.0
0.8
0.6
0.4
0.2
0.0
0.0
0.2
0.4
0.6
0.8
1.0
Cumulative fraction of C&Cs
Fraction of ASes hosting C&Cs
○ Cloud providers
Mirai
Bashlite

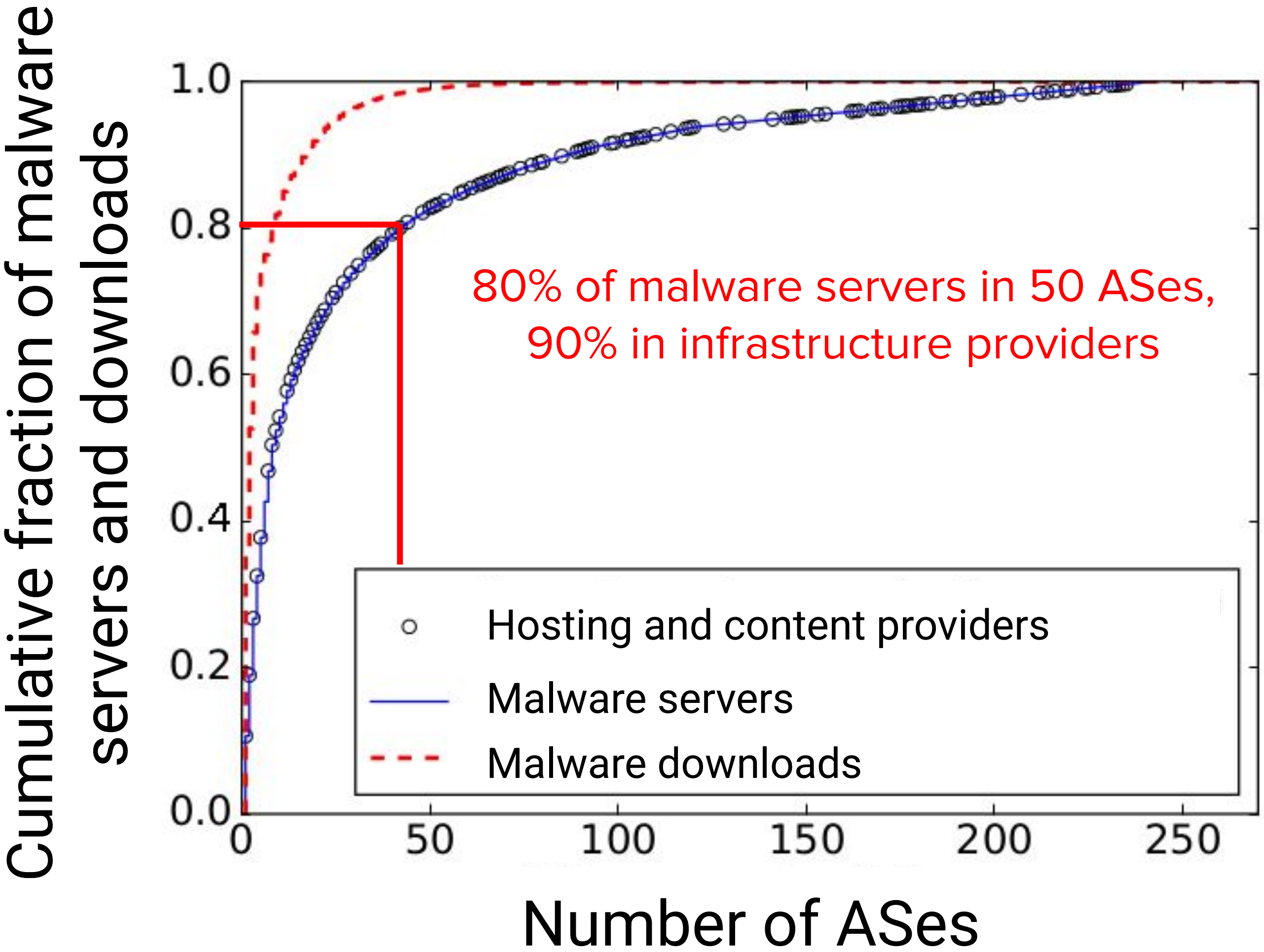


80% of Bashlite CnCs hosted in about 25% of ASes, mostly infrastructure providers



Mirai infrastructure is less concentrated: harder to take down


Cumulative fraction of malware servers and downloads
1.0
0.8
0.6
0.4
0.2
0.0
0
50
100
150
200
250
Number of ASes
○ Hosting and content providers
Malware servers
Malware downloads



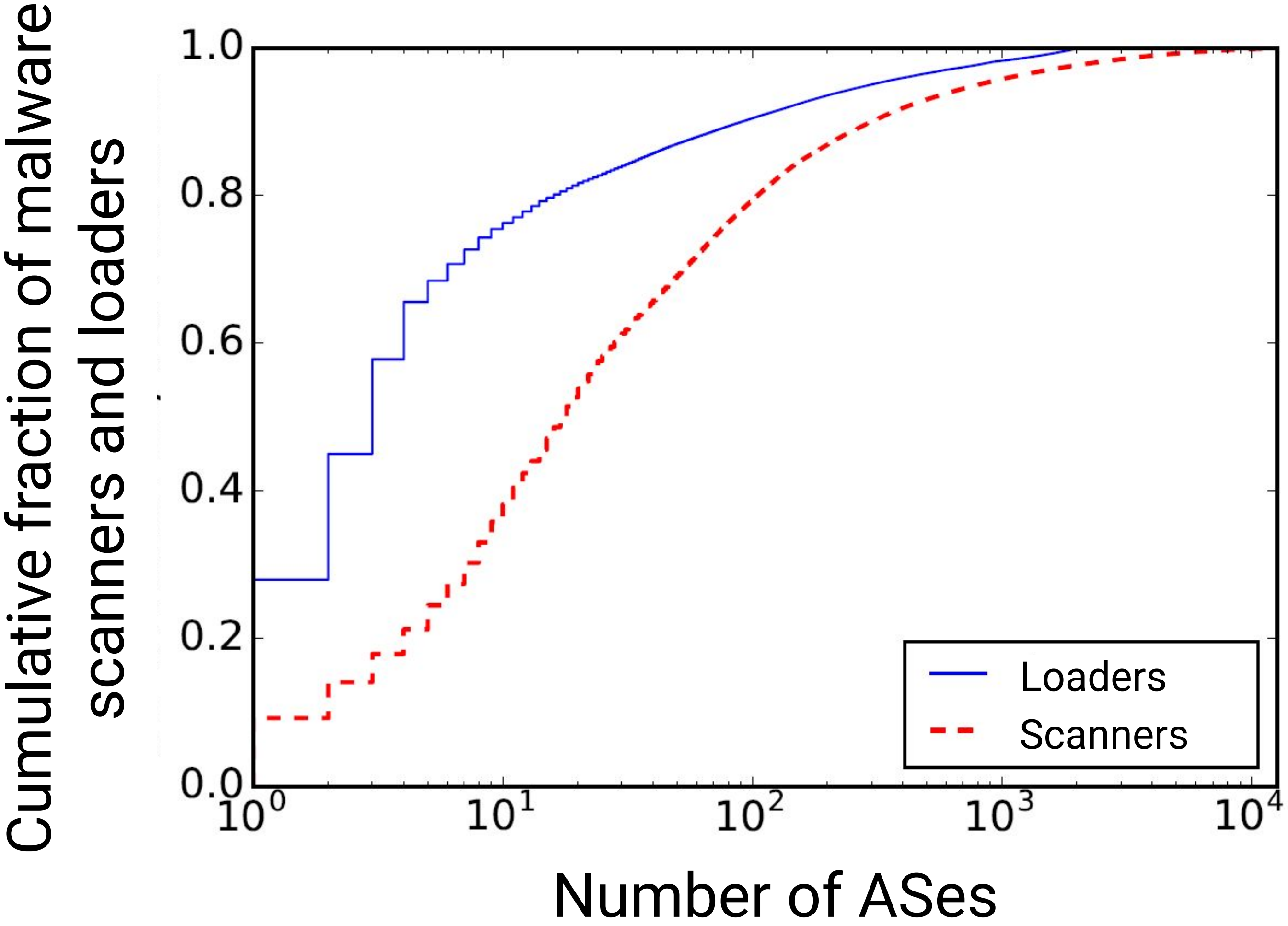
80% of malware servers in 50 ASes,
90% in infrastructure providers

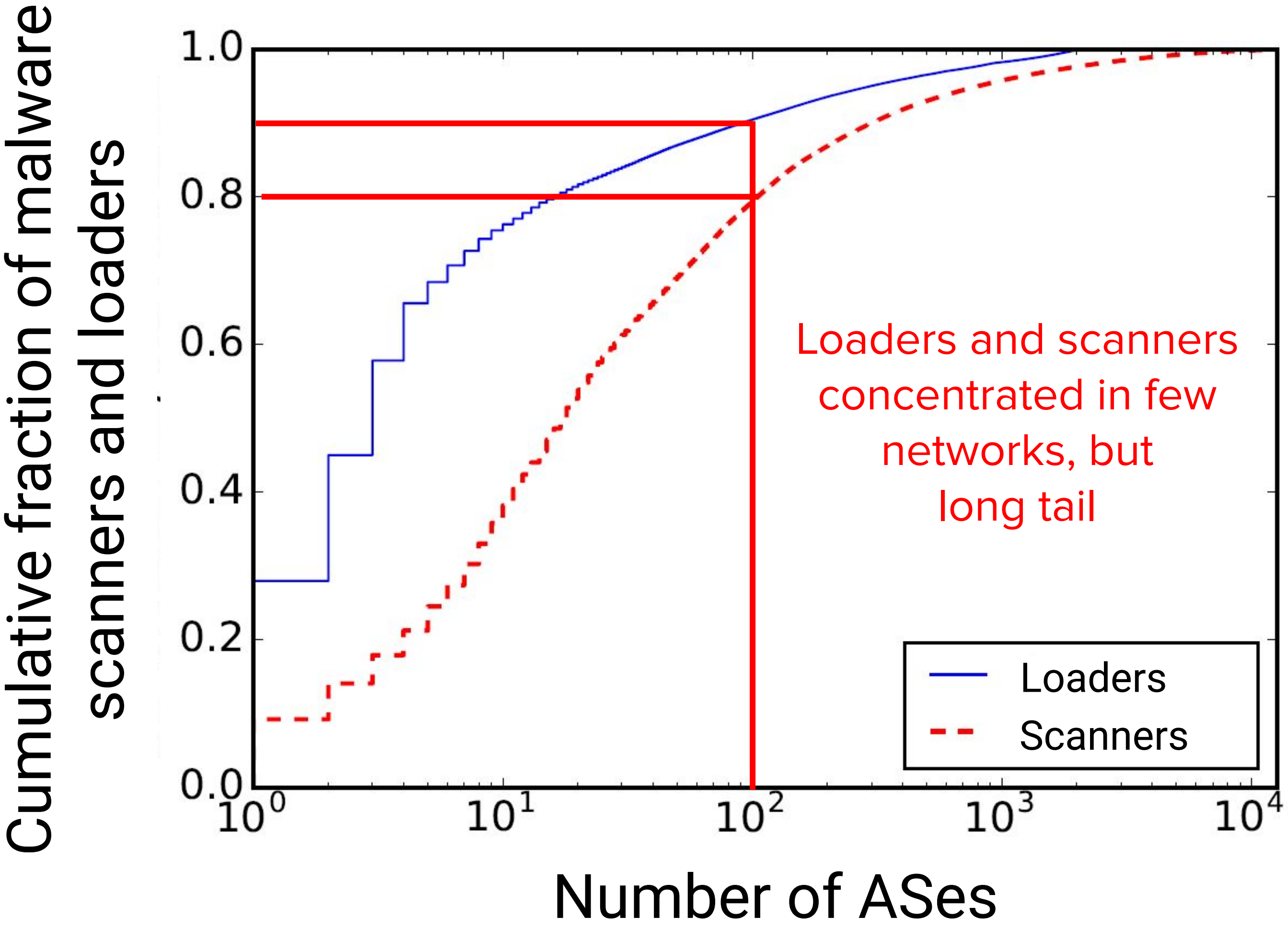
Infrastructure Sharing

- Infrastructure providers host both C&Cs and malware servers
- The top 20 ASes that host C&Cs and the top 20 ASes that host malware servers have 16 ASes in common

Infrastructure Sharing

- Infrastructure providers host both C&Cs and malware servers
- The top 20 ASes that host C&Cs and the top 20 ASes that host malware servers have 16 ASes in common
- Previously reported as *bullet-proof hosting*


Cumulative fraction of malware scanners and loaders
1.0
0.8
0.6
0.4
0.2
0.0
10^0
10^1
10^2
10^3
10^4
Number of ASes
Loaders
Scanners



Loaders and scanners concentrated in few networks, but long tail

Botnet Operation and Use

Botnet Use and Operation

Observed commands

- 583 different command names
- Analyzed the 80 most frequent commands (98,9% of commands)
    - Classified commands into classes

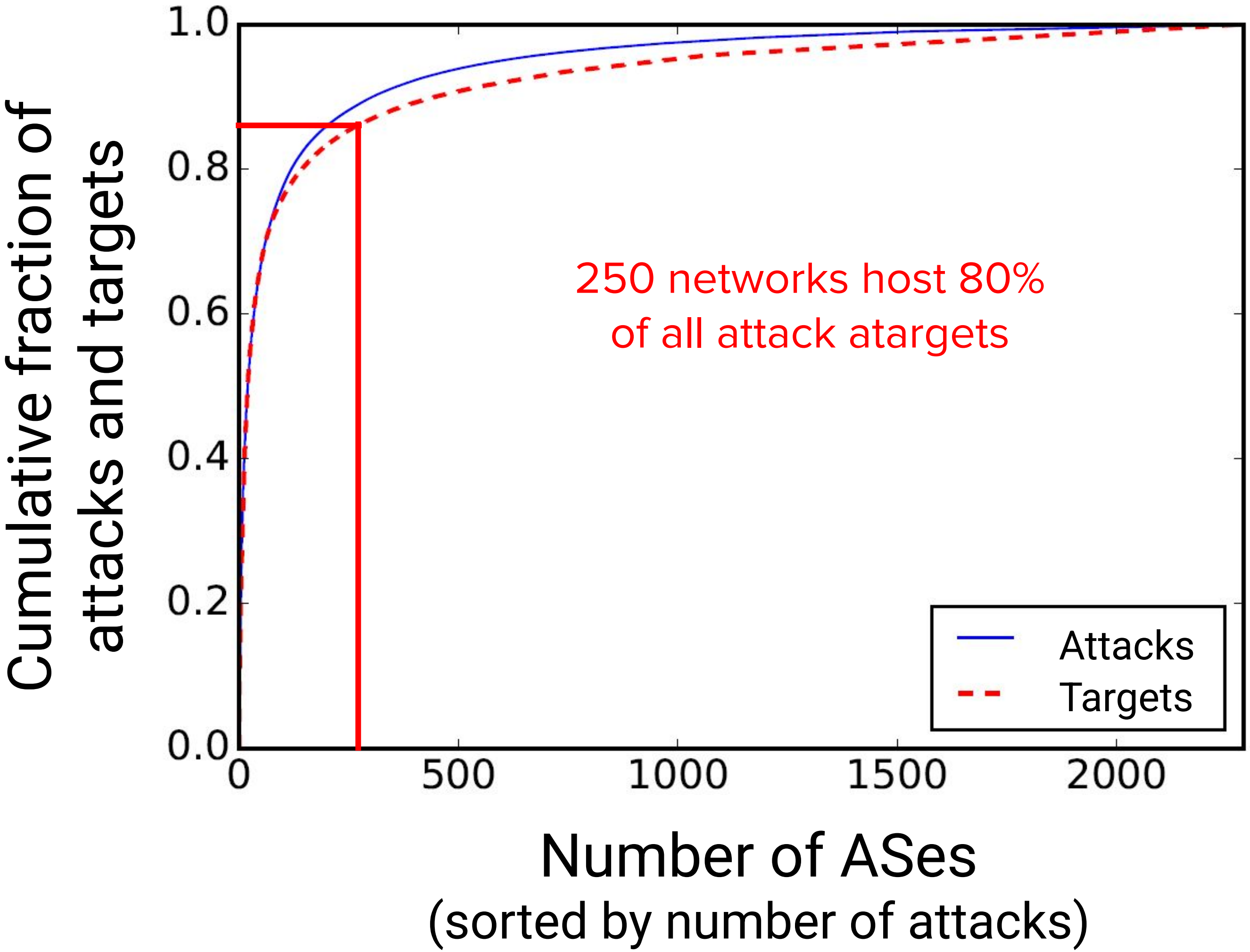
Botnet Use and Operation

Observed commands

- 583 different command names
- Analyzed the 80 most frequent commands (98,9% of commands)
  - Classified commands into classes

Attack targets

- 83,101 attack commands
- 29,286 target IP addresses in 2,289 ASes



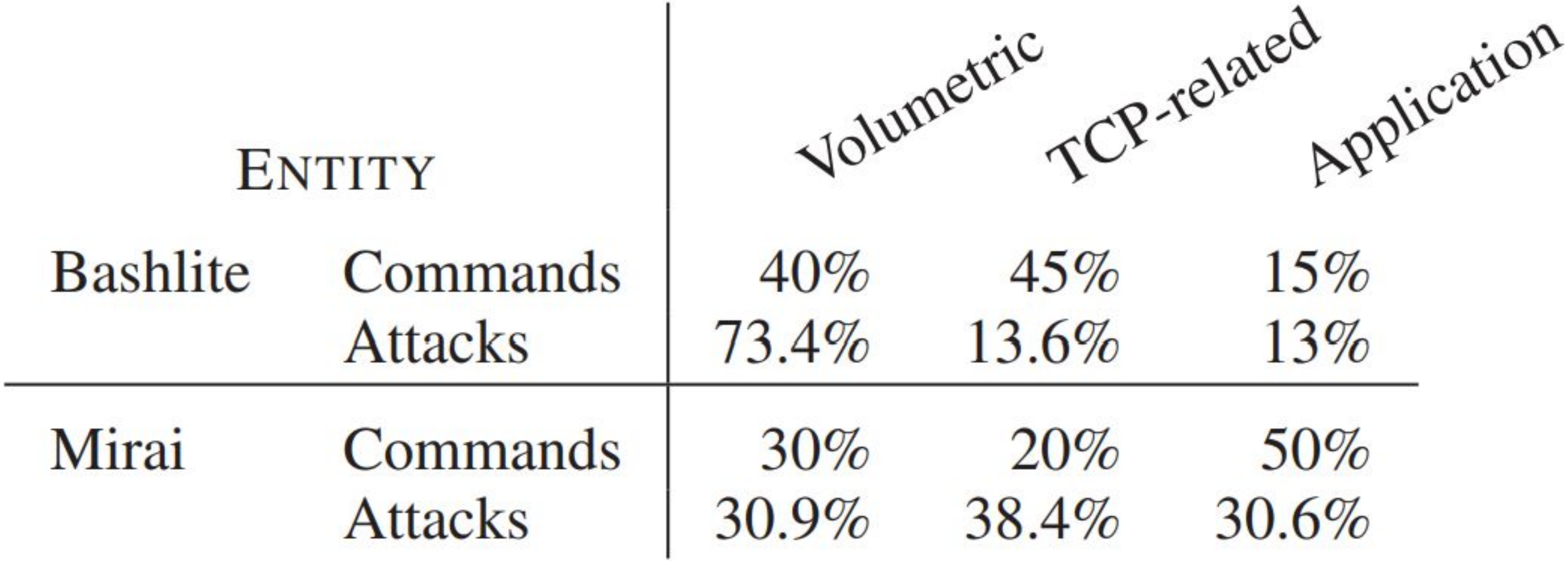
250 networks host 80% of all attack atargets

Common Targets

- Manually inspected the 25 most attacked targets
    - Infrastructure providers
    - Internet service providers
    - Game servers

- Common ports
    - Expected targets: HTTP, SSH, DNS
    - Game servers: Xbox Live, Minecraft

Evolution of Attacks



ENTITY		Volumetric	TCP-related	Application
Bashlite	Commands	40%	45%	15%
	Attacks	73.4%	13.6%	13%
Mirai	Commands	30%	20%	50%
	Attacks	30.9%	38.4%	30.6%

Conclusion

- Characterization of IoT botnets
  - The support infrastructure
  - Their use
- Evolution of IoT botnets
  - More widespread hosting
  - More elaborate attacks

The Evolution of the Bashlite and Mirai IoT Botnets

Italo Cunha

cunha@dcc.ufmg.br

UFMG

UFSJ

cert.br