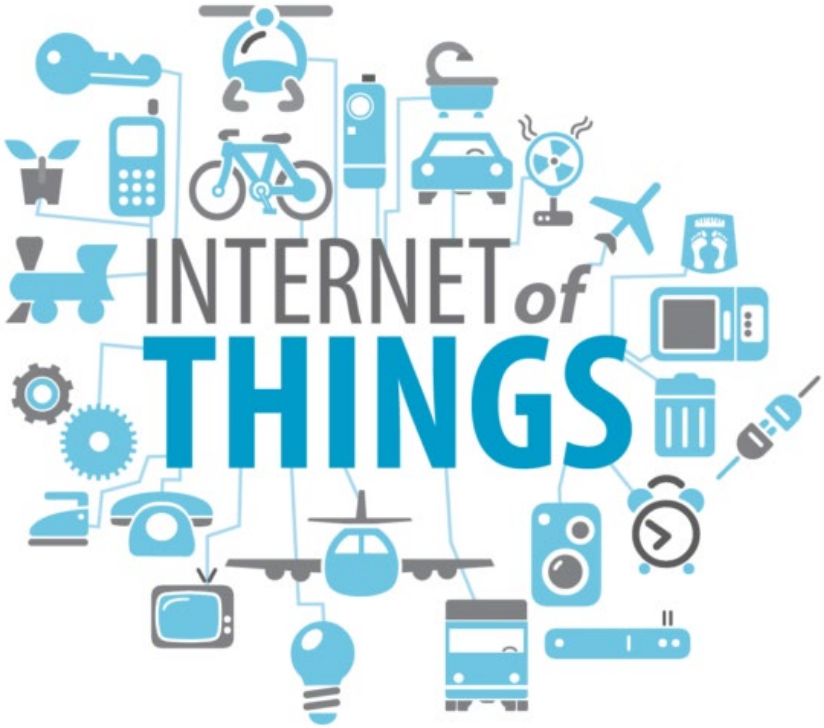
Understanding Fileless Attacks on Linux-based IoT Devices with HoneyCloud

Fan Dang, Zhenhua Li, Yunhao Liu, Ennan Zhai
Qi Alfred Chen, Tianyin Xu, Yan Chen, Jingyu Yang

20 Billion

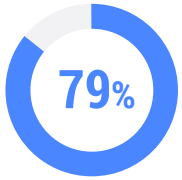
IoT Devices

In 2023

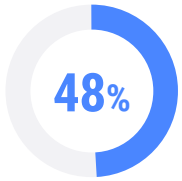


* Gemalto – The State of IoT Security

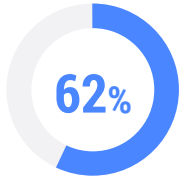
guidelines
required



breach
exists?



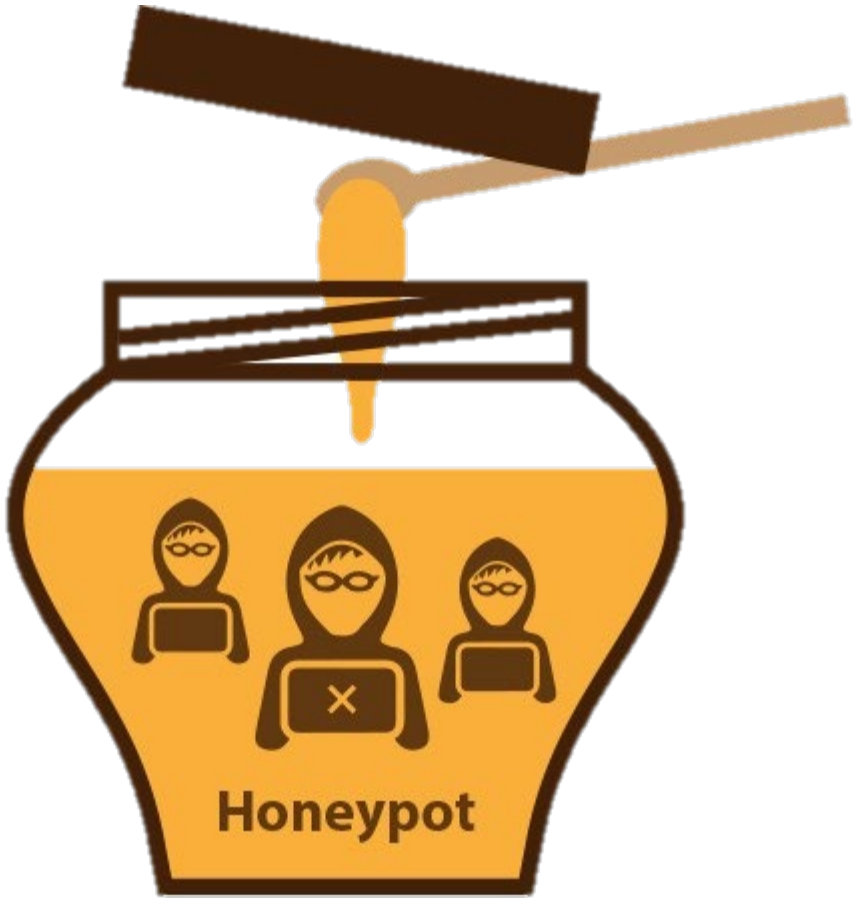
improve
security



* Gemalto – The State of IoT Security

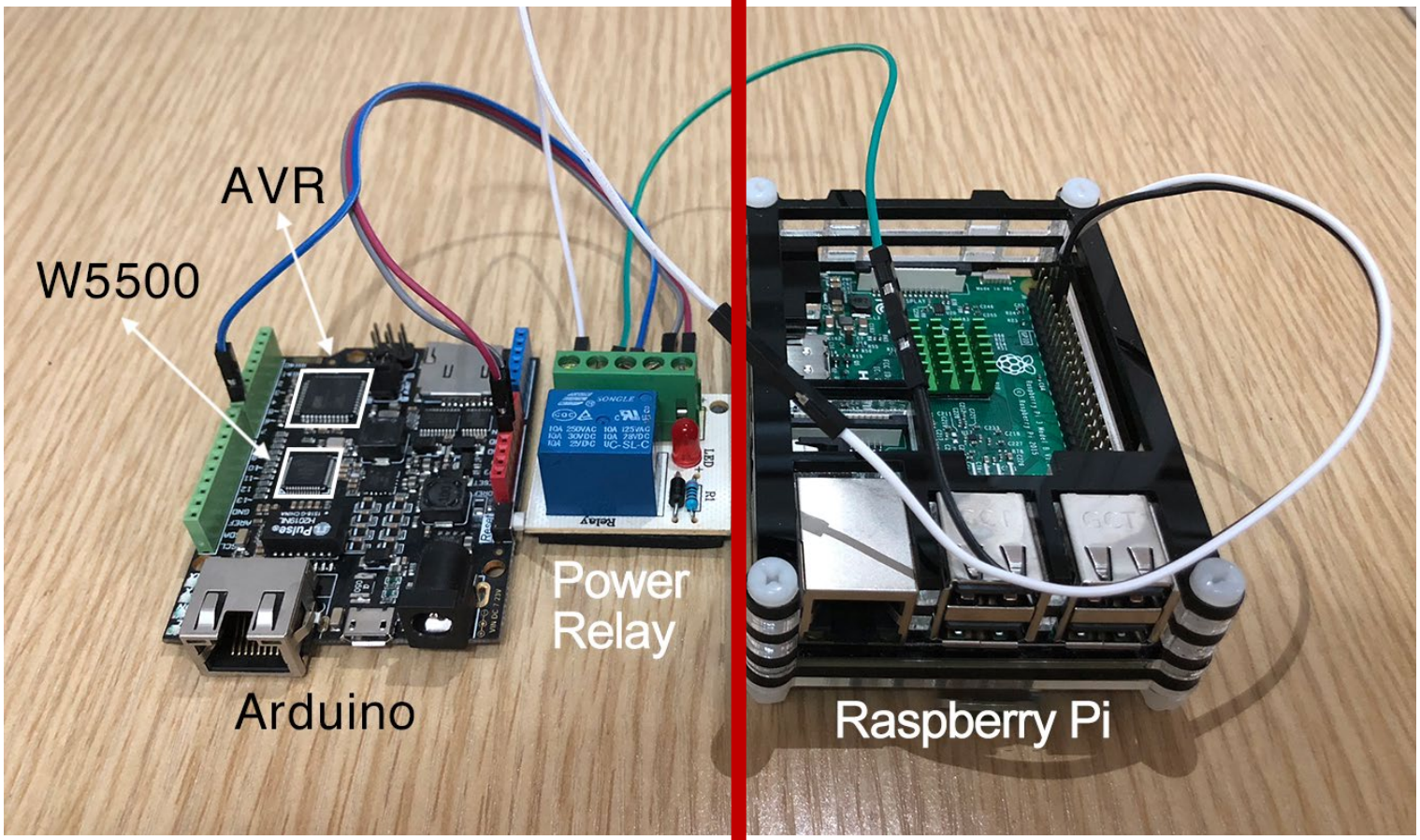
Honeypot

A honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.



Source: – oswalpalash

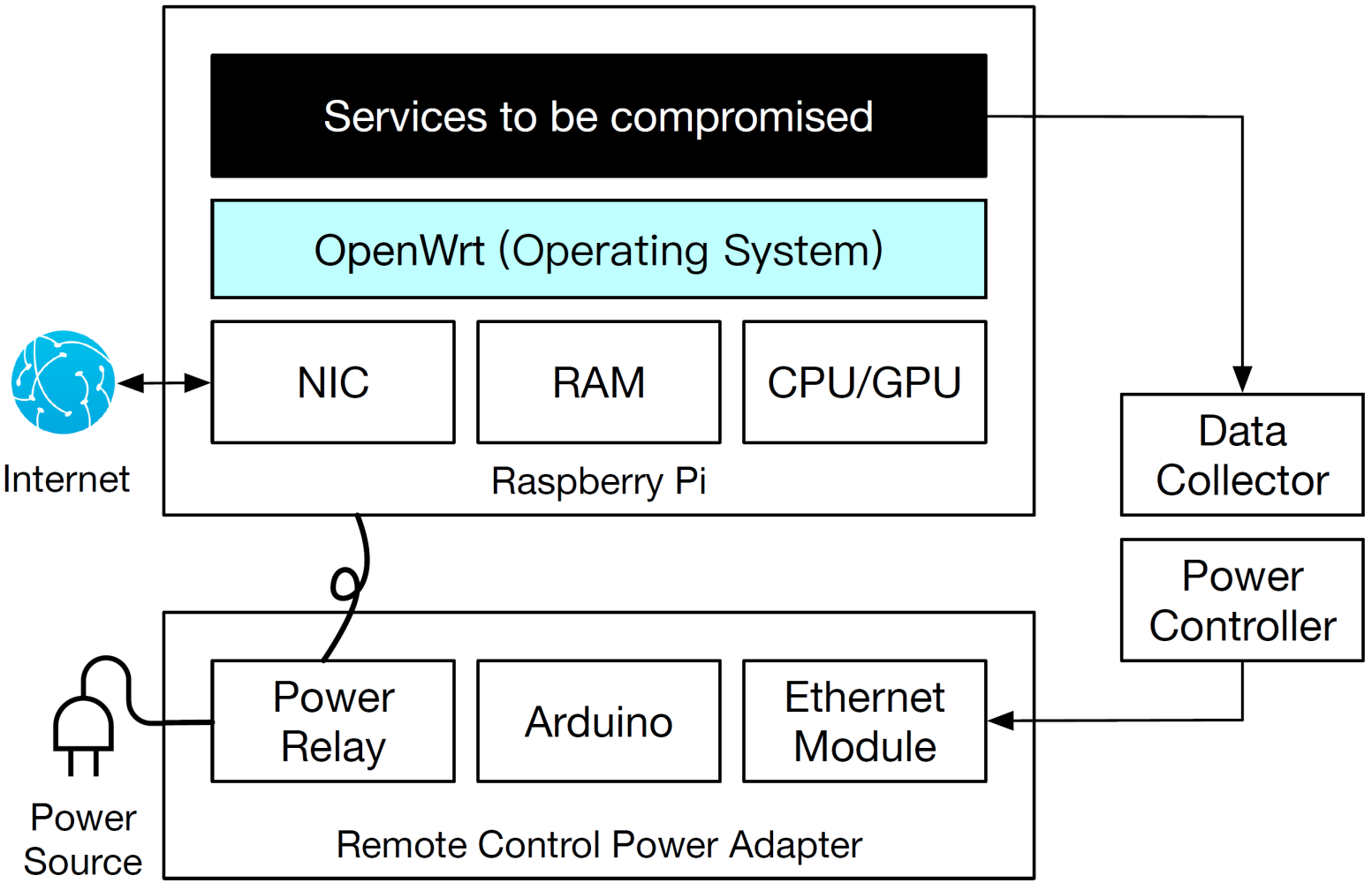
Hardware Honeypot



Remote Control Power Adapter

Hardware Honeypot

Hardware Honeypot

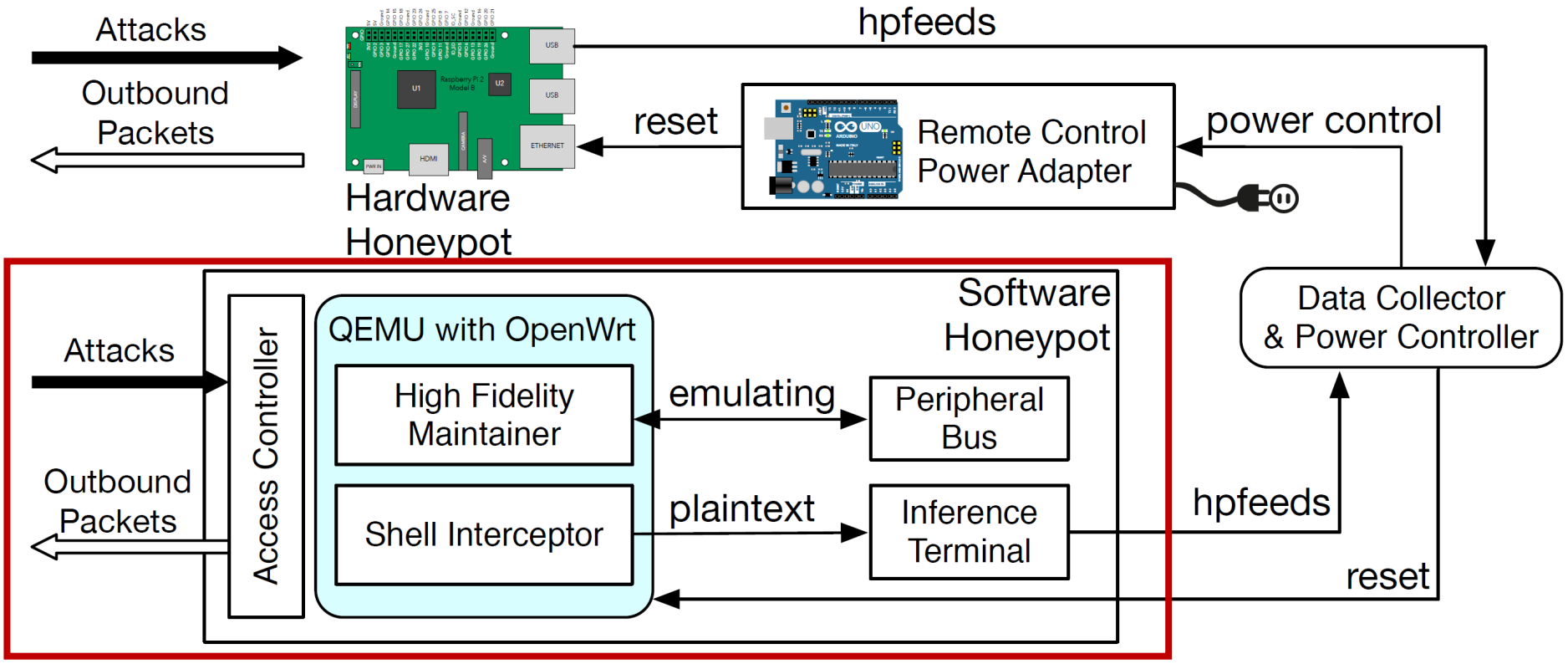


Hardware Honeypot

City	Device	Price	Arch
New York, USA	Raspberry Pi	$20	ARM
San Jose, USA	Netgear R6100	$55	MIPS
Beijing, China	BeagleBone	$45	ARM
Shenzhen, China	Linksys WRT54GS	$40	MIPS
All above	RCPA	$30	-

>$30/month Internet access fee

System Architecture



Software Honeypot
High Fidelity

Customizing QEMU configurations
Proper CPU, memory, and peripheral configurations

Masking sensitive system information
Forge /proc/cpuinfo

VM instances rearrangement
Change IPs and providers

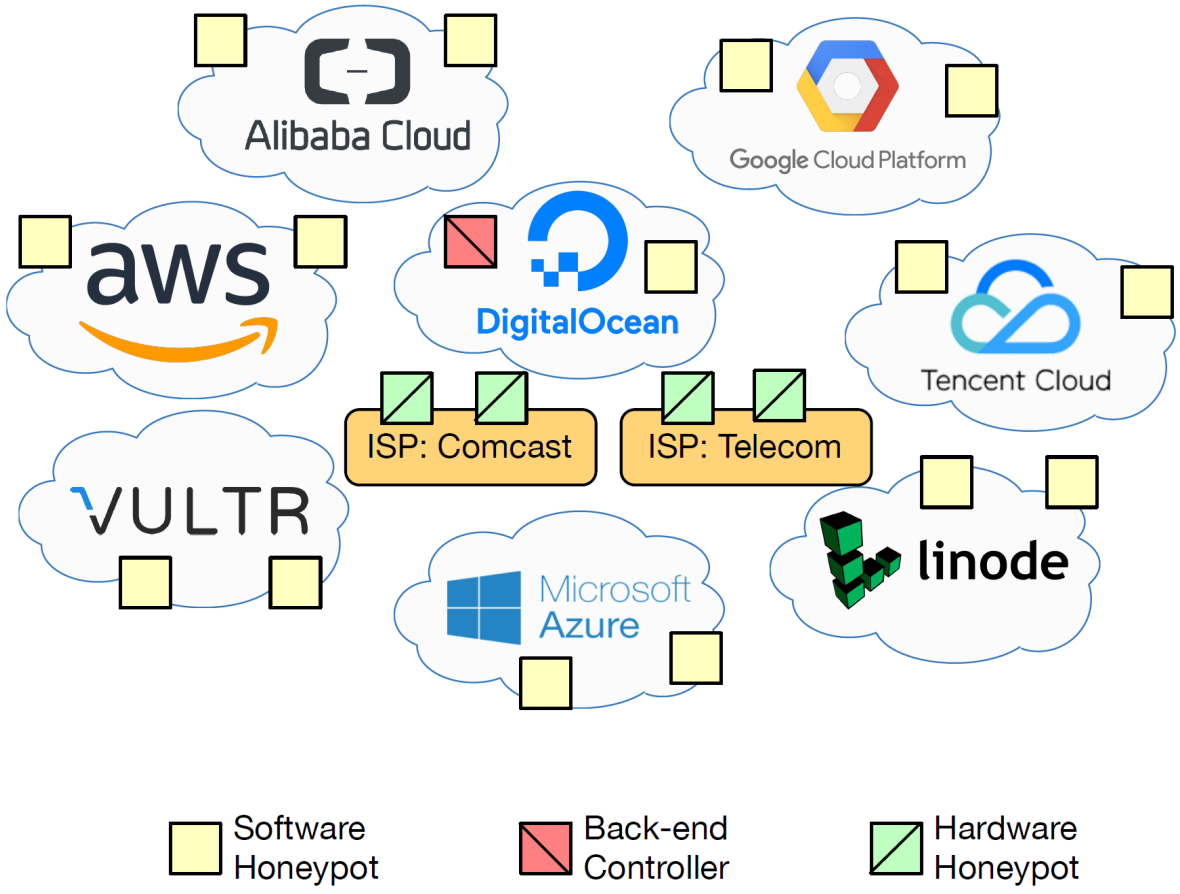
Software Honeypot
Evidence Collection

CPU usage

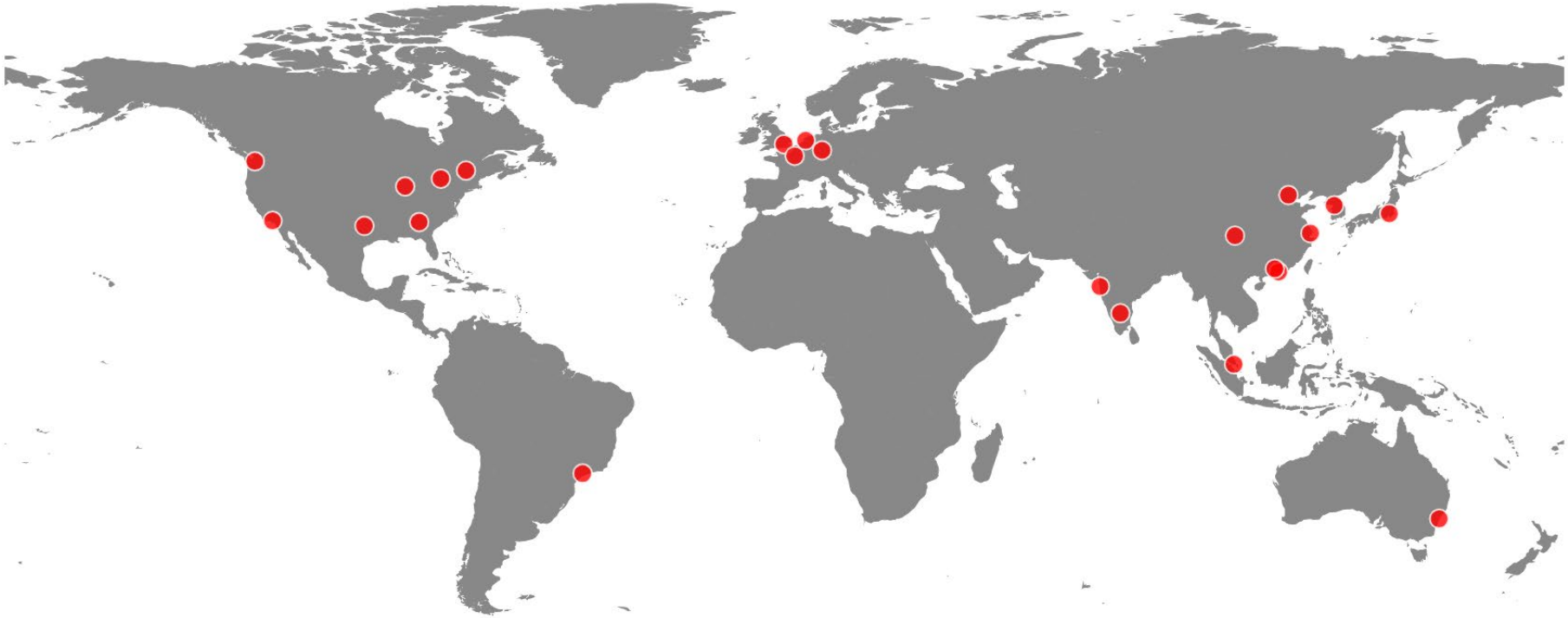
Process list

Network packets

Findings
Deployment Overview



Findings
Geo-distribution

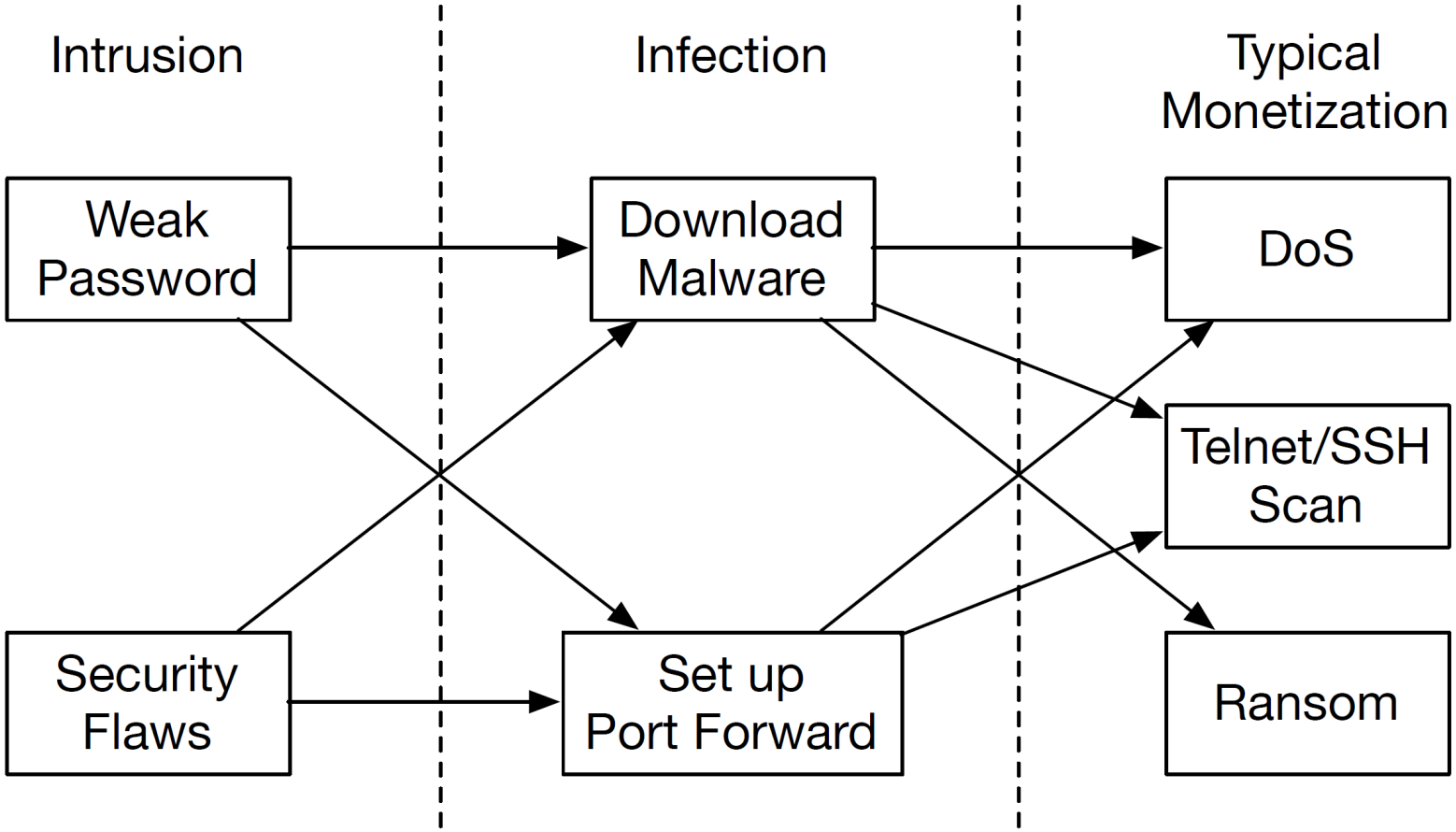


~$6/month

108

Jun. 2017 ~ Jun. 2018

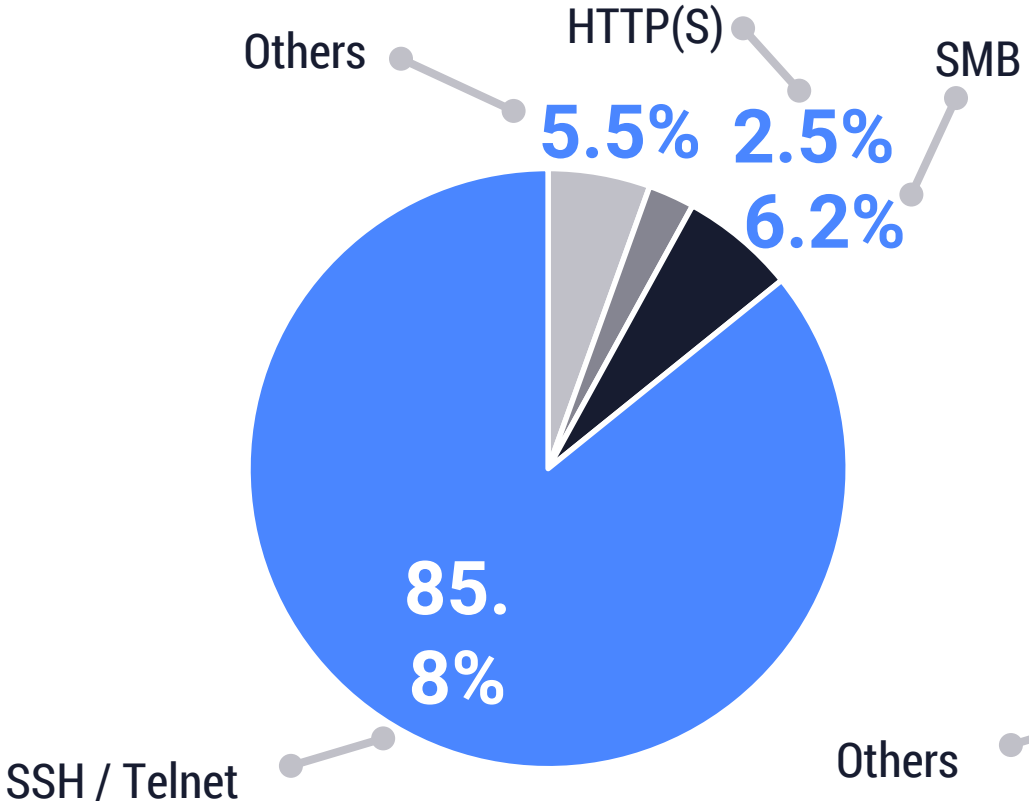
Findings
General Attacking Flows

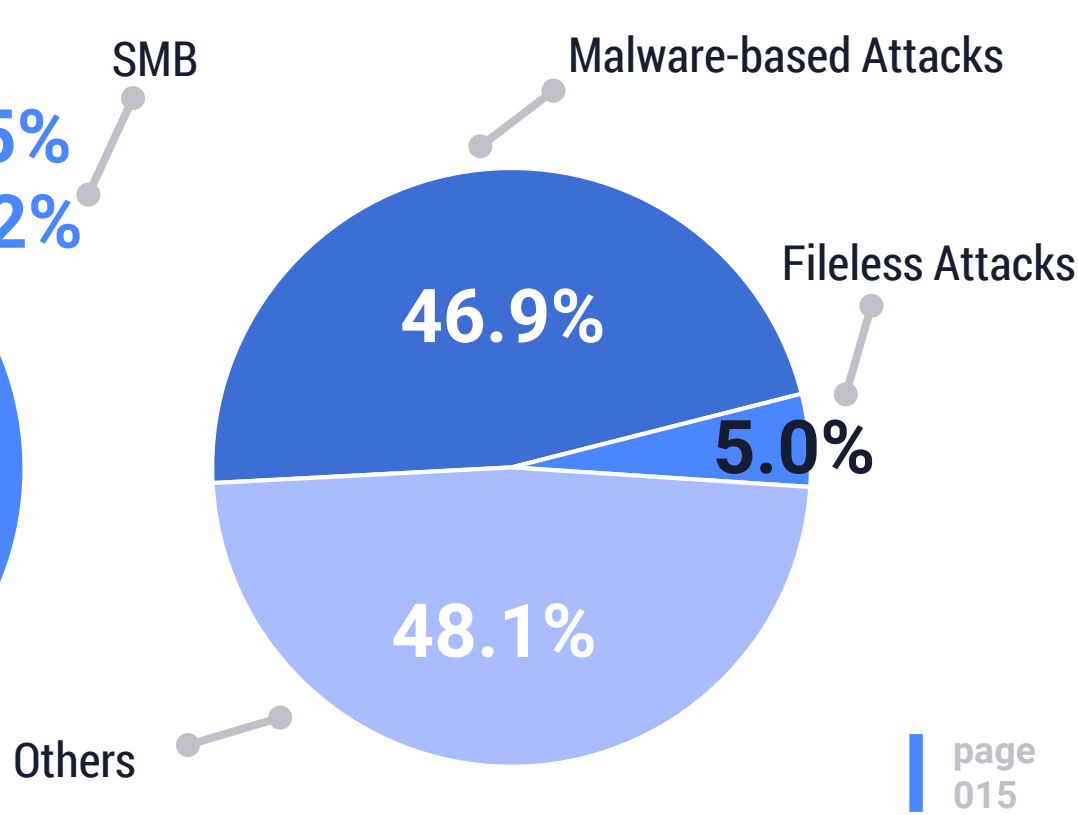


attacks that do not rely on malware files

14.5M | **suspicious connections**

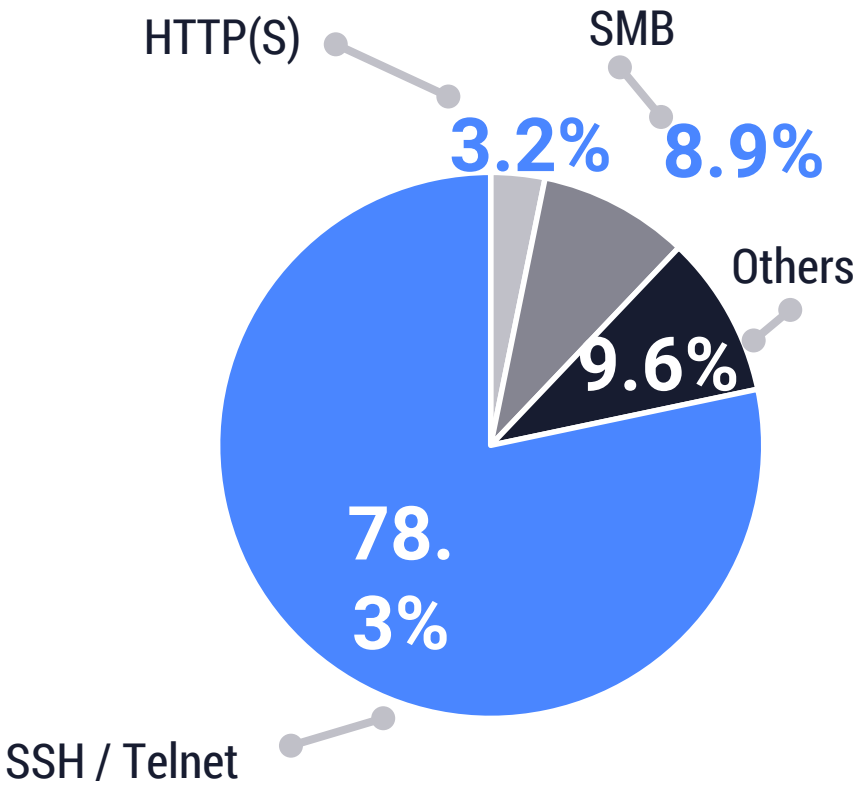
1.6M | **effective attacks**

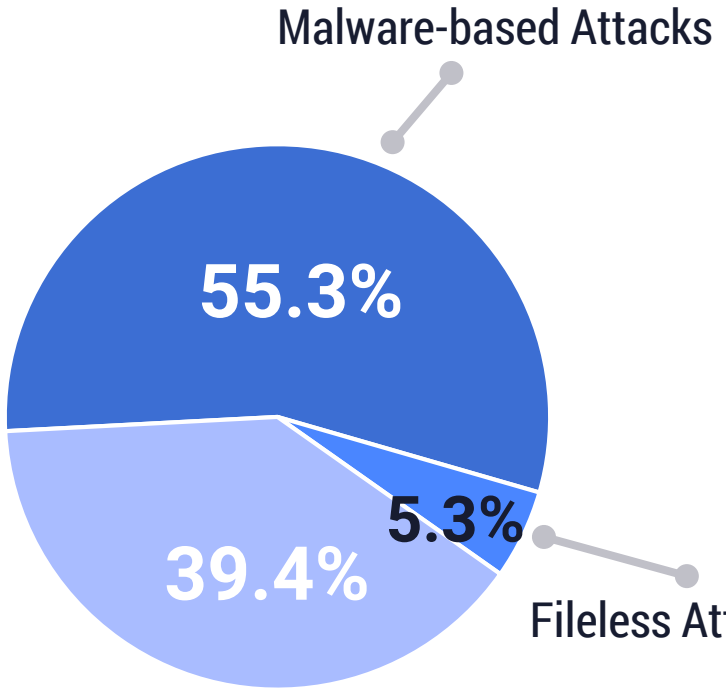




249M | **suspicious connections**

26.4M | **effective attacks**





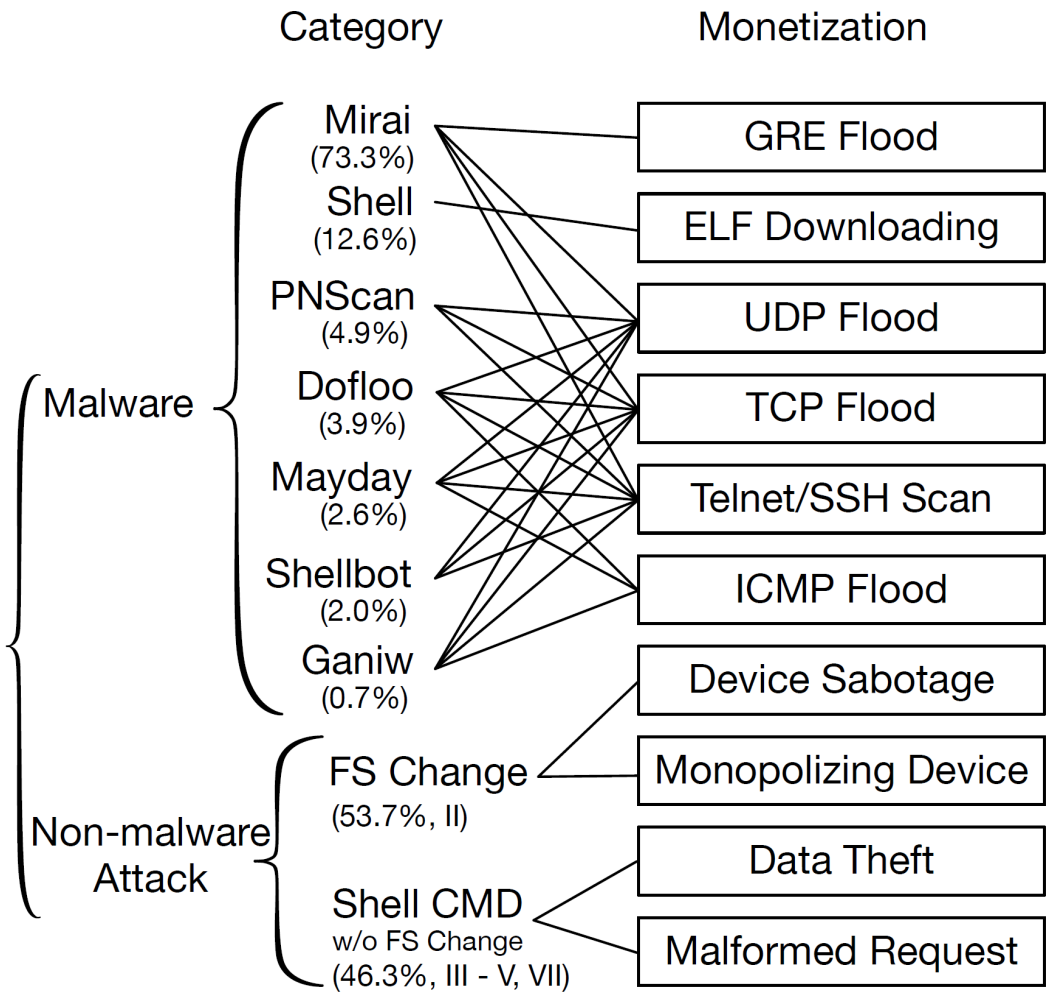
Findings
Less Fidelity

1100/day → **670/day**

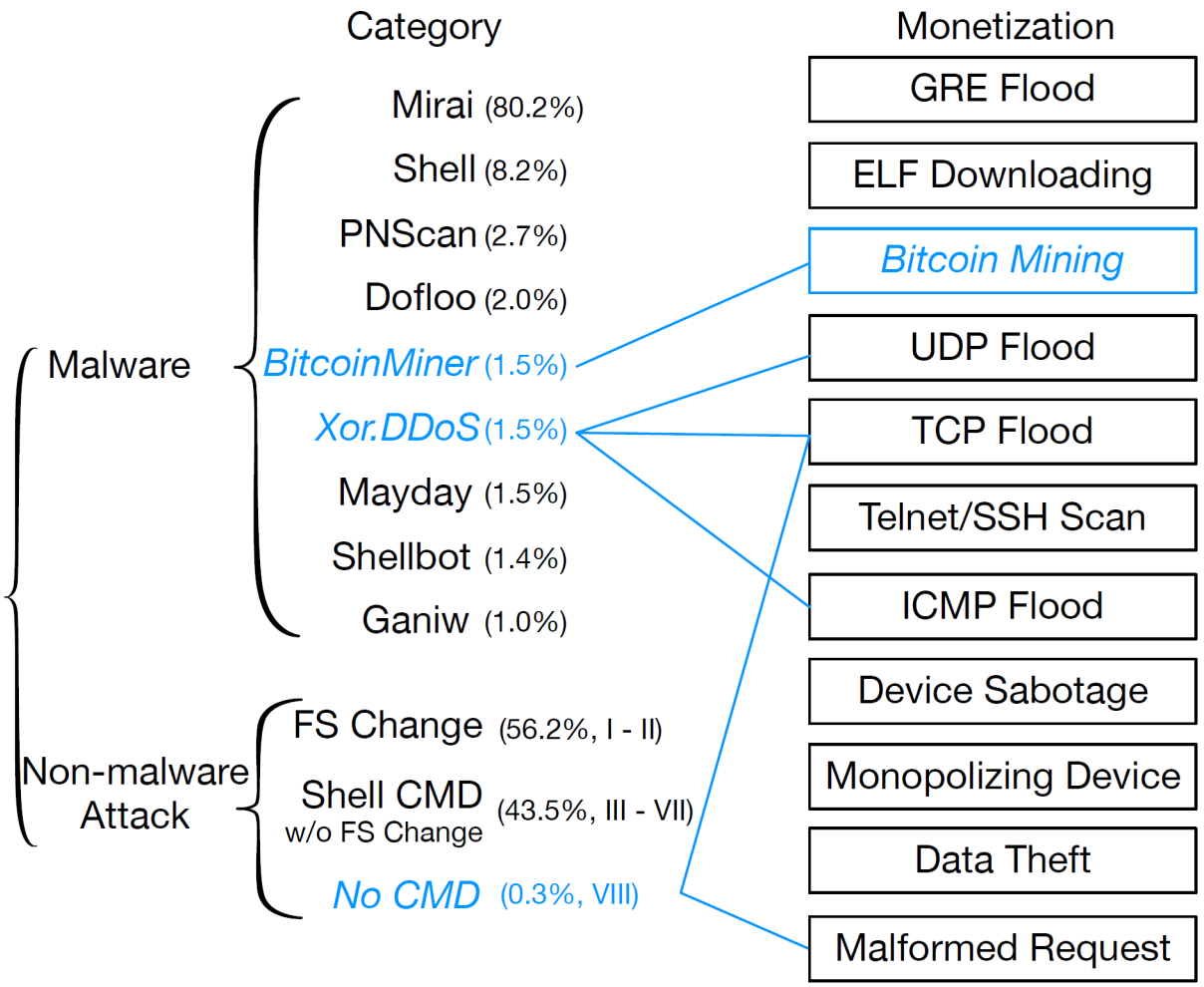
Public clouds
may prevent certain types of attacks

In-depth information
may be used to infer the honeypots

Findings
Hardware



Findings
Software

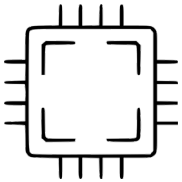


Findings
Malware-based Attacks

598

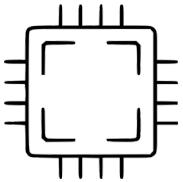
types

malware



27.3%

ARM



25.7%

MIPS

Findings
Fileless Attacks

01 Occupying end systems
e.g., altering passwords

02 Damaging system data
e.g., removing / altering configurations

03 Preventing monitoring
e.g., killing services

04 Retrieving system info
e.g., getting hardware information

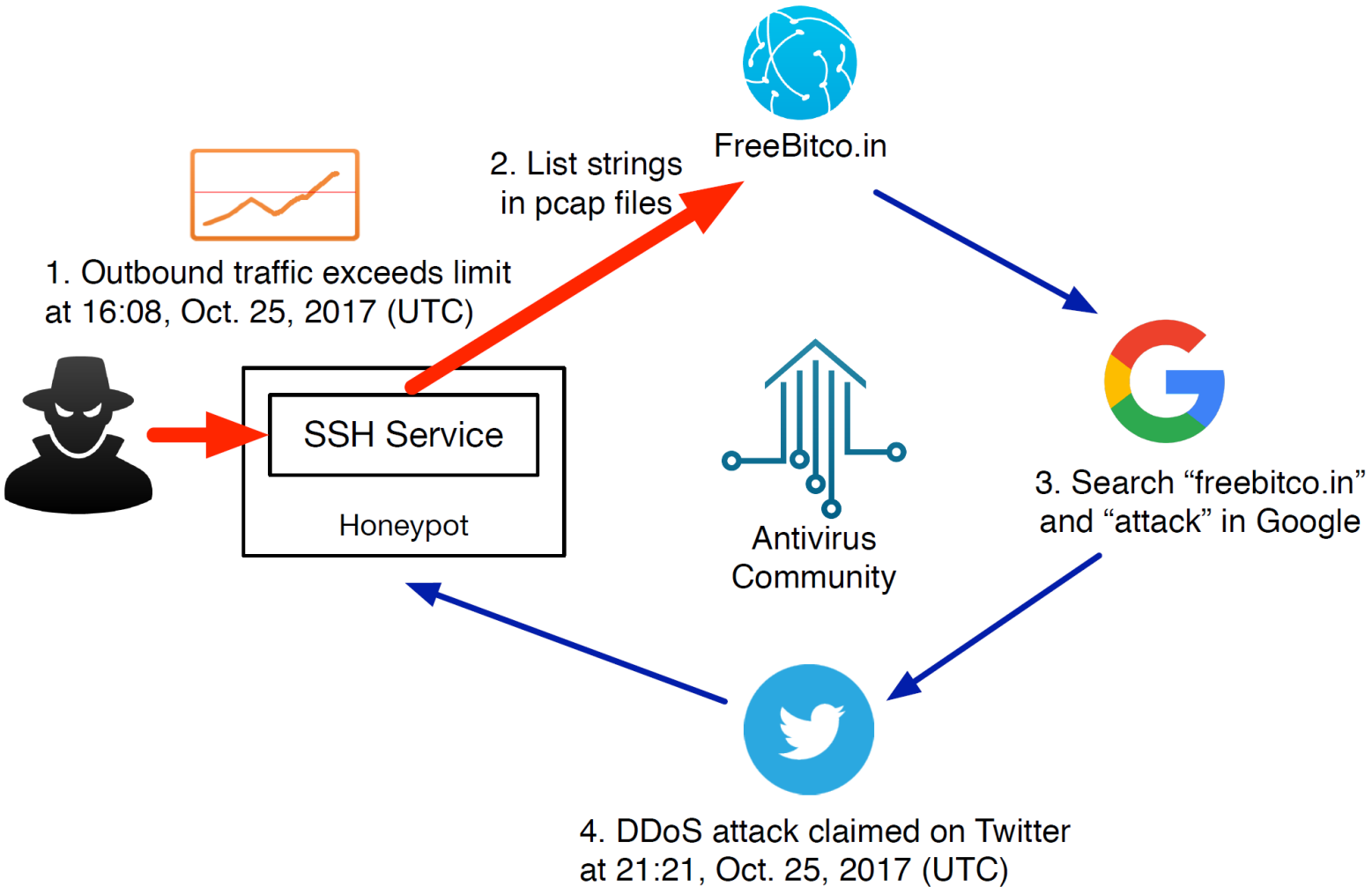
05 Stealing data
e.g., reading the shadow file

06 Launching network attacks
e.g., sending malformed HTTP requests

07 Other commands
e.g., who, lastlog

08 No shell commands
e.g., SSH tunneling attacks

Findings
SSH Tunneling Attack



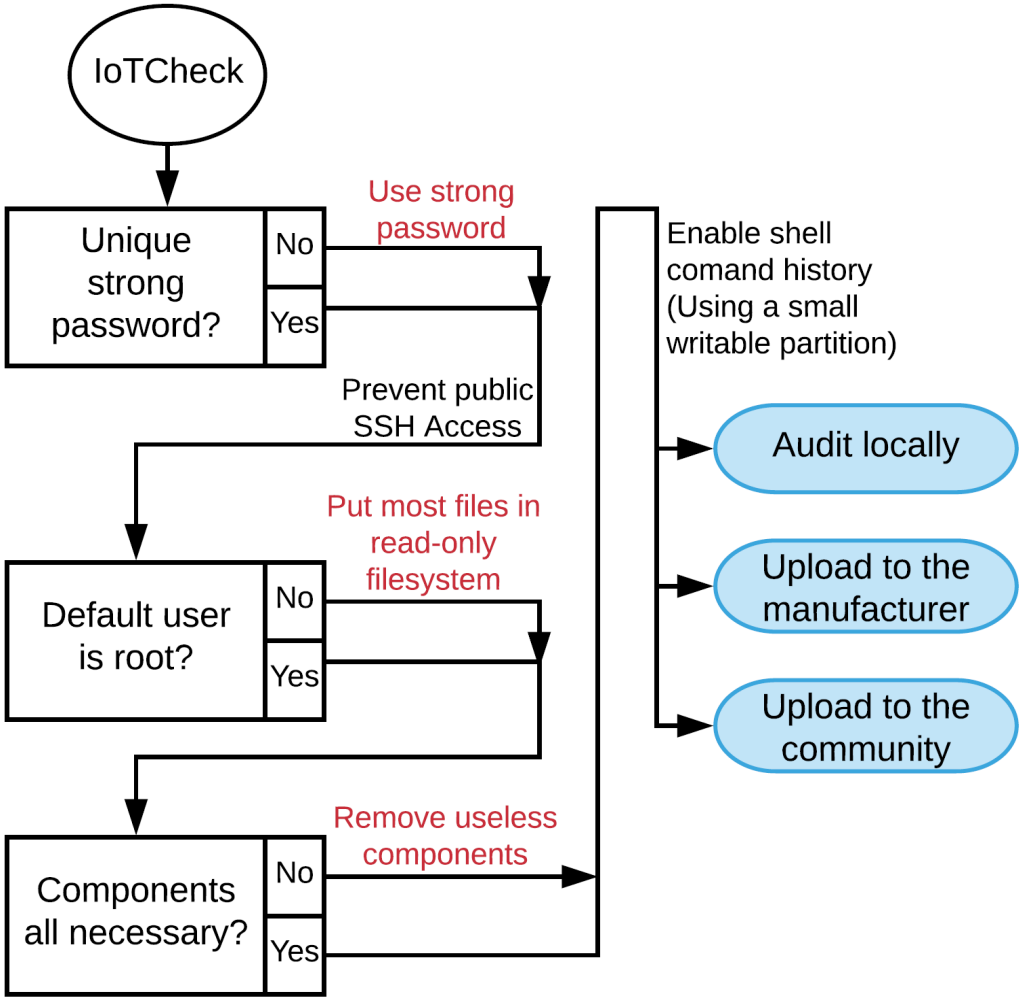
Findings
New Security Challenges & Defense Directions

01 56.2%: modify the filesystem

02 99.7%: using shell commands

03 0.3%: no traces

Findings
New Security Challenges & Defense Directions



Conclusions & Future Work

01 Build and deploy the HoneyCloud system

02 First taxonomy for fileless IoT attacks

01 Support of emerging IoT interfaces

02 Robustness to the interference of VM identity

03 In-depth analysis on advanced attacks

Thanks