

Lecture #6: IoT botnet Measurements 2

Cristian Hesselman, Elmer Lastdrager, Ramin Yazdani, Etienne Khan, and Ting-Han Chen

University of Twente | May 31, 2023

A man in a pinstriped suit and blue shirt is speaking at a podium. To his left is an American flag. The background is a blue wall with a circular logo. The text "ITS NOT MALWARE" is overlaid in large, bold, white letters with a black outline at the top of the image.

ITS NOT MALWARE

WH
.GOV

ITS ALTERNATIVE SOFTWARE

Admin

Interactive lectures

- Overall objective: enable you to learn from each other and further increase your understanding of the papers, contributes to preparing yourself for the oral exam
- Interactive format
 - Teachers summarize two papers per lecture
 - Multiple-choice and open questions (not graded) and discussion
 - Enables you to learn from each other, so mandatory to participate
- **A 7th “re-sit” lecture in case you miss a lecture** (optional for everybody else), same format

Paper summaries

- You must have handed in your two summaries **before 7AM on the day of the lecture**
- Each summary can be at most 250 words, at most 1 single-sided A4 page
- You can add figures, and graphs from the paper or add your own if you like (e.g., concept maps)
- You can use the summaries during the oral exam
- Submit through CANVAS
- You **cannot** complete SSI without submitting 12 paper summaries!

Schedule

No.	Date	Contents
1	Apr 26	Course introduction
2	May 3	Lecture: IoT and Internet Core Protocols
3	May 10	Lecture: IoT Botnet Measurements 1
4	May 17	Lecture: IoT Edge Security Systems
5	May 24	Lecture: IoT Device Security
6	May 31	Lecture: IoT Botnet Measurements 2
7	Jun 1	Guest lecture #1: naval systems, Dr. Sorin Iacob, Thales
8	Jun 5	Lecture: IoT Security in Non-Carpeted Areas
9	Jun 12	Guest lecture #2: product security for Bosch (IoT) products, Stephan van Tienen, Bosch Security Systems
10	Jun 14	Lecture: IoT Honeypots (re-sit)

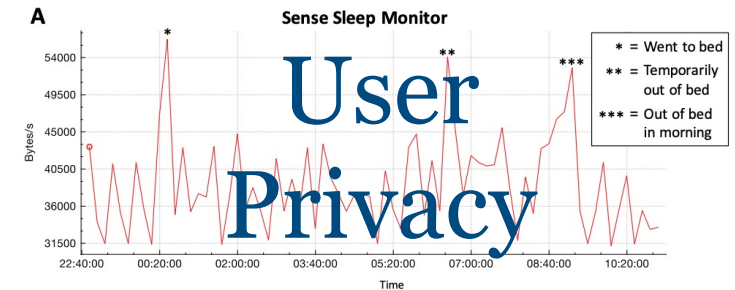
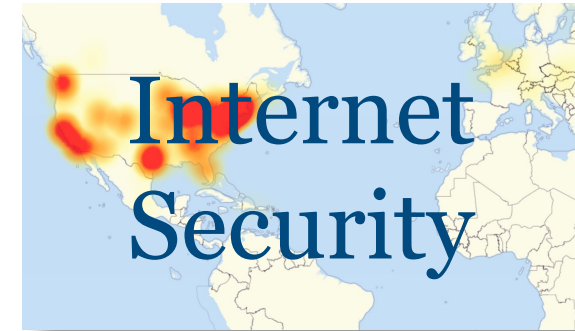
Important dates

- Two summaries per lecture: before the lecture (07:00 CEST) in which the papers will be discussed
- Lab report (PDF) and required files: **Fri June 23, 2023, 23:59 CEST**
- All to be submitted through CANVAS

Introduction to today's lecture

Motivation: mitigation of IoT botnets

- Requires tools and services to understand **different** IoT botnets in a timely way, means to detect and eradicate them, vulnerability scans
- Challenging because of wide variety of IoT devices and their increasing number and distribution across multiple network operators
- Examples: post-mortem analysis [Mirai, Hajime], IoT honeypots [IoTPot, Honware], automated malware analysis [RIoTMAN], firewalls and IDSes [DBolt, FIAT], vulnerability scanning [OpenForHire]



Today's papers

[RIoTMAN] A. Darki, and M. Faloutsos, “RIoTMAN: a systematic analysis of IoT malware behavior”, CoNEXT '20: Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies, November 2020

[OpenForHire] S. Srinivasa, J.M. Pedersen, E. Vasilomanolakis, “Open for hire: Attack trends and misconfiguration pitfalls of IoT devices”, 21st ACM Internet Measurement Conference (IMC 2021), November 2021

Today's learning objective

- After the lecture, you will be able to discuss what it takes to:
 - Analyze different IoT bots/malware at scale (previous lecture focused on individual botnets)
 - Scan IoT devices for vulnerabilities to proactively mitigate botnet risks
- Contributes to SSI learning goal #1: “Understand IoT concepts and applications, security threats, technical solutions, and a few relevant standardization efforts in the IETF”

“RIoTMAN: a systematic analysis of IoT malware behavior”

16th International Conference on emerging Networking
EXperiments and Technologies (CoNEXT), November 2020

Wooclap quizzes



- 1 Go to wooclap.com
- 2 Enter the event code in the top banner

Event code
YLFPJH



- 1 Send **@YLFPJH** to **0970 1420 2908**
- 2 You can participate

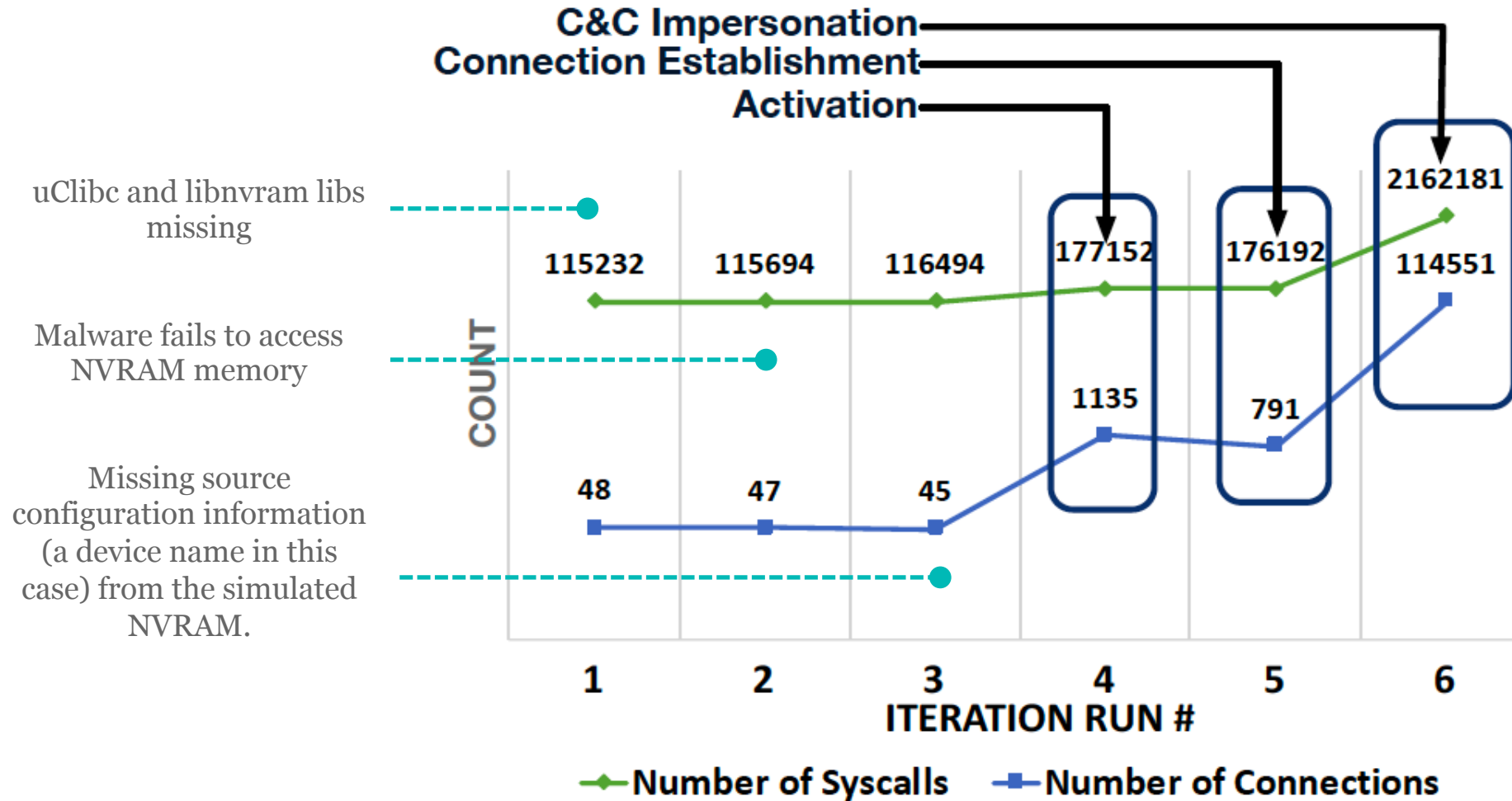
Who would like to take a stab
at summarizing the paper?

TRY NOW

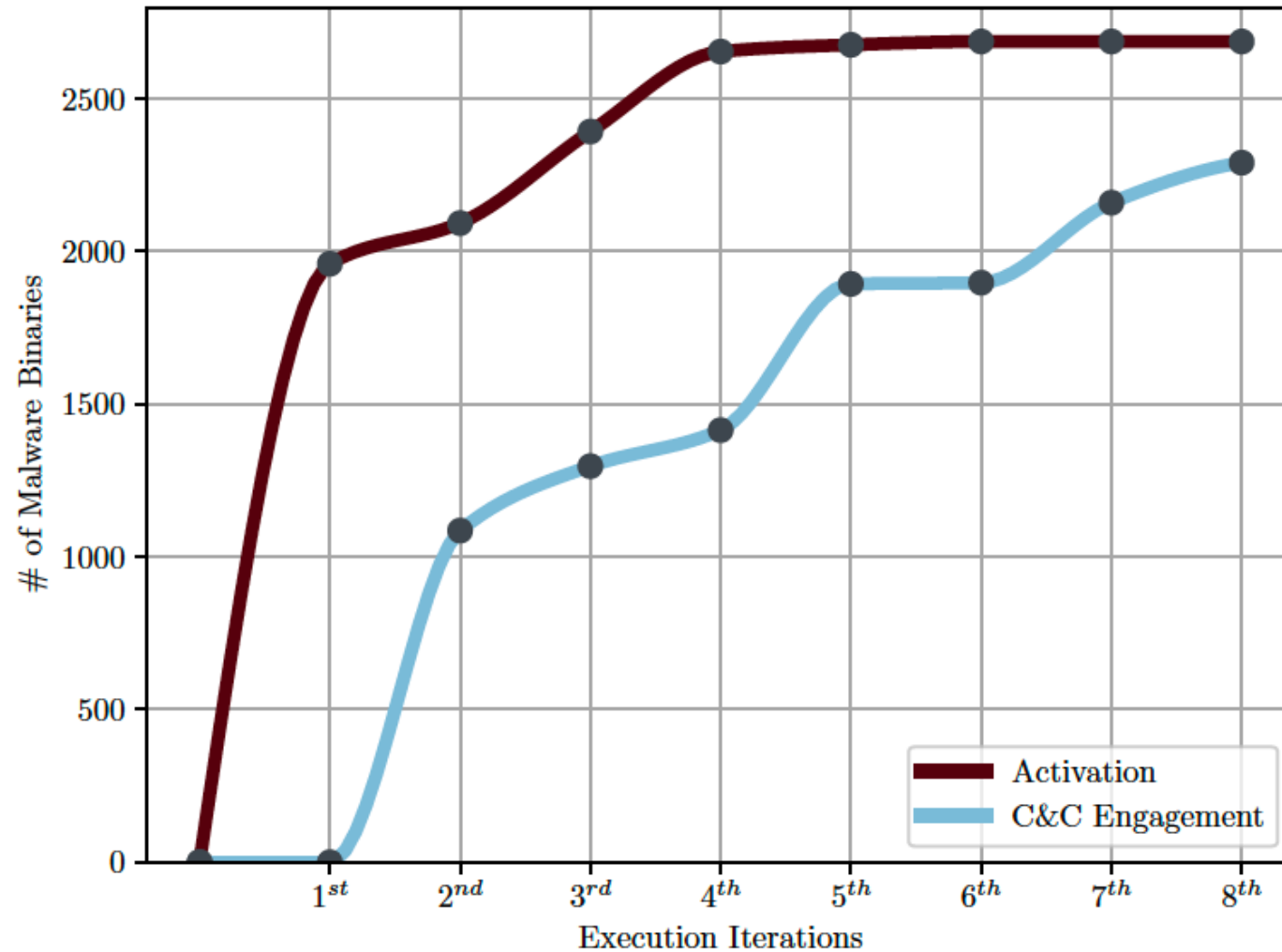
Problem and approach

- Profiling the behavior of IoT malware based on binaries => understand, detect, mitigate
- Labor intensive because of wide variety of a IoT devices and their growing number
- RIoTMAN dynamically analyzes botnets: adaptive sandboxing and communications exploration
- Goal: profile the behavior of IoT malware binaries
- Activated malware: infection complete and establishes comms with outside world
- Engaged malware: instructions result in new traffic/system behavior and connection stays up

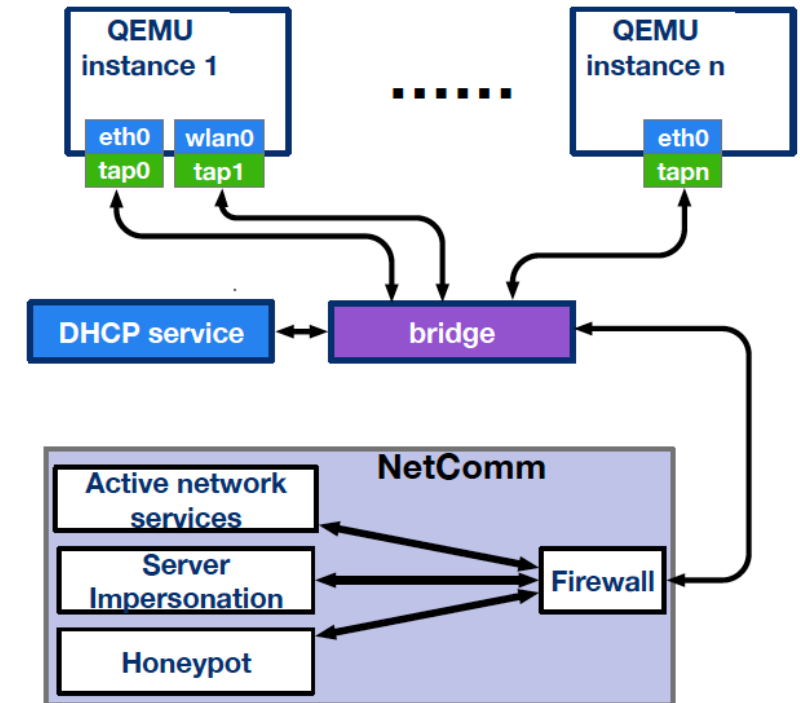
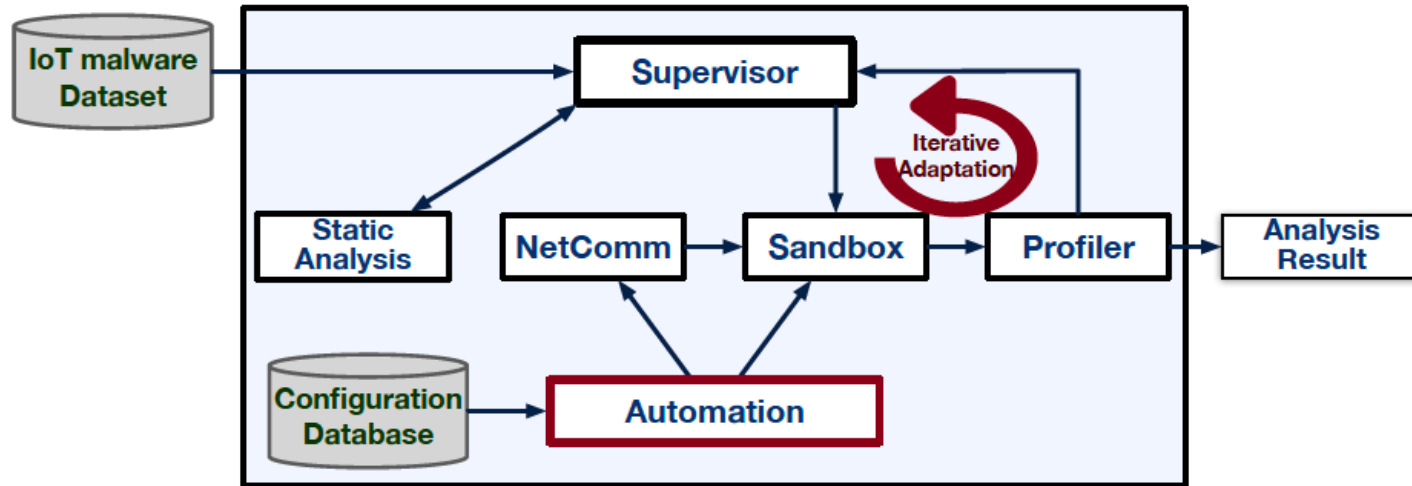
Example: Linux.Tsunami



Key measurement result – what are we looking at?



RIoTMAN measurement architecture



What are the responsibilities of the components?

Discuss!





Measurement results

Total binaries	2885	
Activated	2688	93%
Engaged	2291	79%

Command Type	Malware	
Configuration or Report	1750	61%
Attack	2031	70%
Scanning	1842	64%
Termination	1684	58%



IoT malware behaviors – how can we leverage that?

IP address	Single	2261
	Multiple	62
Domain	Fixed	257
	DGA	5

Family from Virustotal	Impersonation Success	Gafgyt C&C		Tsunami C&C		Aidra C&C	Mirai C&C
		Prometheus	QBot	Remaiten	Capsaicin	Lightaidra	Mirai
Gafgyt (>6 sub-families)	94%	148	1296	-	2	-	5
Tsunami (>2 sub-families)	98%	4	26	43	25	-	-
Aidra (>2 sub-families)	87%	1	5	-	-	2	-
Mirai (>2 sub-families)	86%	-	-	-	-	-	402
IRCBot	76%	-	-	-	13	-	3
IoTReaper	50%	-	-	-	-	-	2
Other (>14 families)	71%	13	120	5	6	1	45
Unclassified	70%	1	76	9	15	1	22
Total (weighted)	79%						

Malware Procedure	Most common techniques					
	Bin.	Technique 1	Bin.	Technique 2	Bin.	Technique 3
Infection	1676	Brute-force login	166	Exploit public facing apps	-	None observed
Persistence	375	Add routine in rc script	333	Add a job to cronjob	15	Specific to IoT device
Defense evasion	1494	Process masquerading	648	Malware binary removal	128	Software packing
Identifying device	1445	Use network config	843	Use config files	286	List processes in device
Impact on host	414	Block OS level access	413	Stop remote services	6	Bitcoin mining



Limitations

- Linux-based IoT devices only
- They exclude botnets that use encryption, P2P botnets, and IPv6 communications

Further discussion

Key takeaways

- Dynamic analysis of IoT malware, limited manual effort
- Important to understand, detect, and mitigate IoT botnets at scale
- One piece of the “IoT botnet mitigation puzzle”
- Significant amount of work in terms of engineering, finding datasets, and analysis
- Next challenge: how will RIoTMAN-like systems work in practice (higher TRLs)?

Coffee break

“Open for hire: Attack trends and
misconfiguration pitfalls of IoT devices”
Internet Measurement Conference 2021

S. Srinivasa, J.M. Pedersen, E. Vasilomanolakis

Question: what is this paper about?
(And the methodology)?

Three-part methodology



Scanning IPv4 or IPv6?



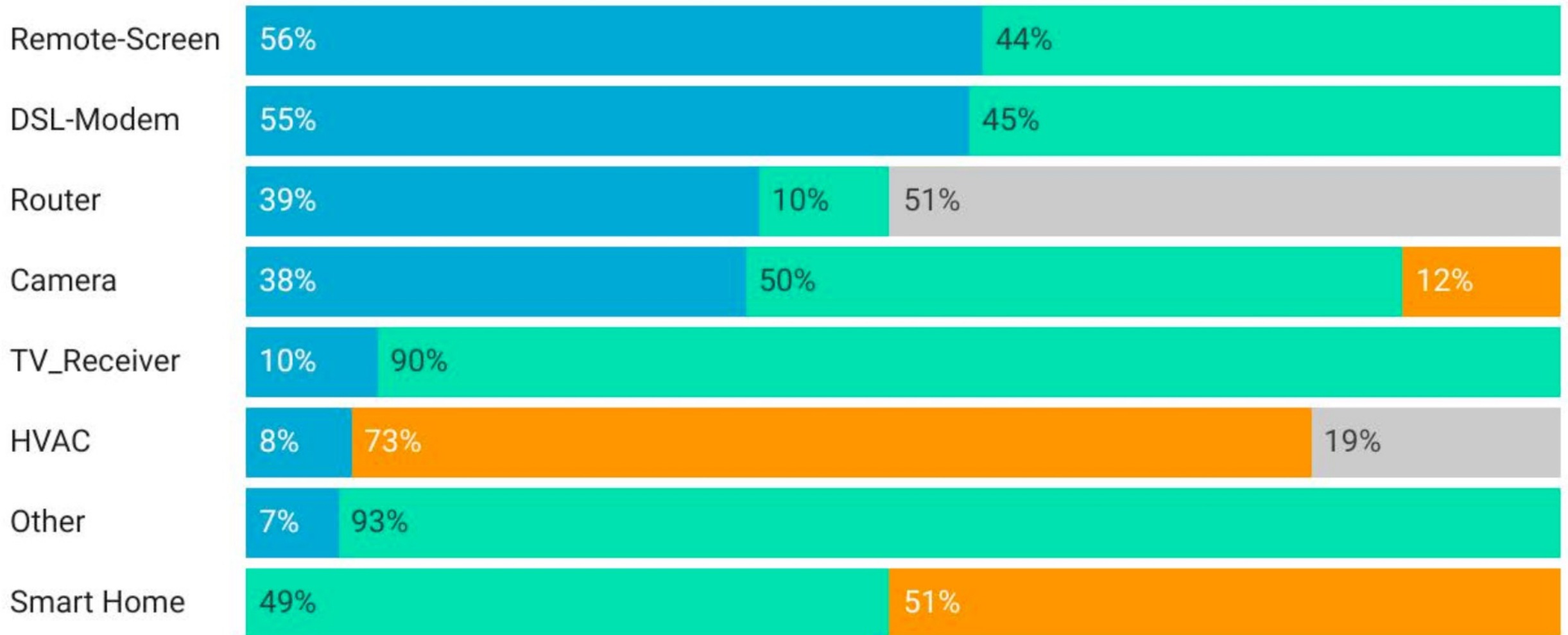
Scanning IPv4: Misconfigurations

Protocol	Vulnerability	#Devices found
CoAP	No auth, admin access	427
AMQP	No auth	2,731
Telnet	No auth	4,013
XMPP	No encryption	5,421
CoAP	No auth	9,067
Telnet	No auth, root access	22,887
MQTT	No auth	102,891
XMPP	Anonymous login	143,986
CoAP	Reflection-attack resource	543,341
UPnP	Reflection-attack resource	998,129
Total		1,832,893

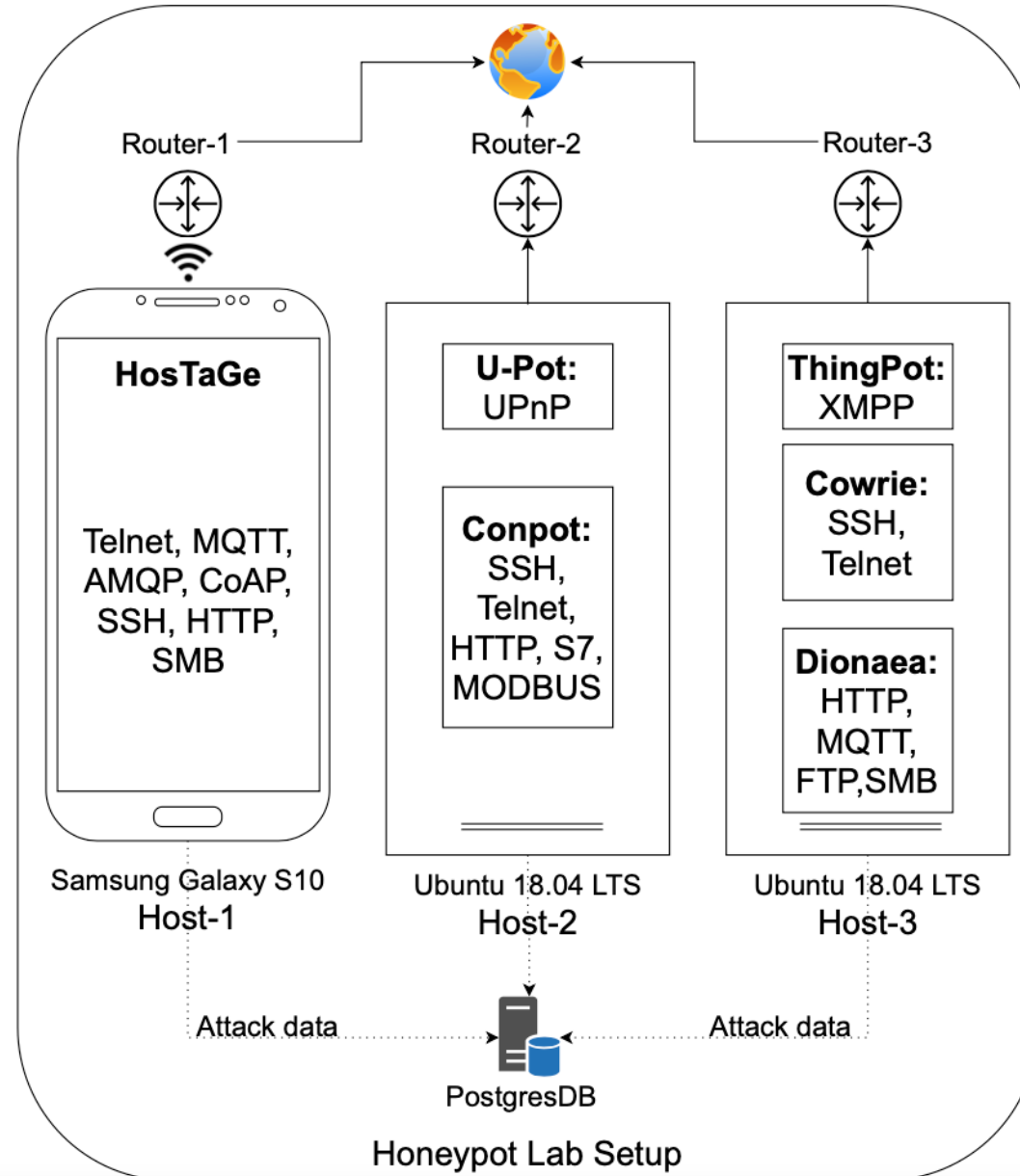
Table 5: Total misconfigured devices per protocol

Scanning: discovered devices

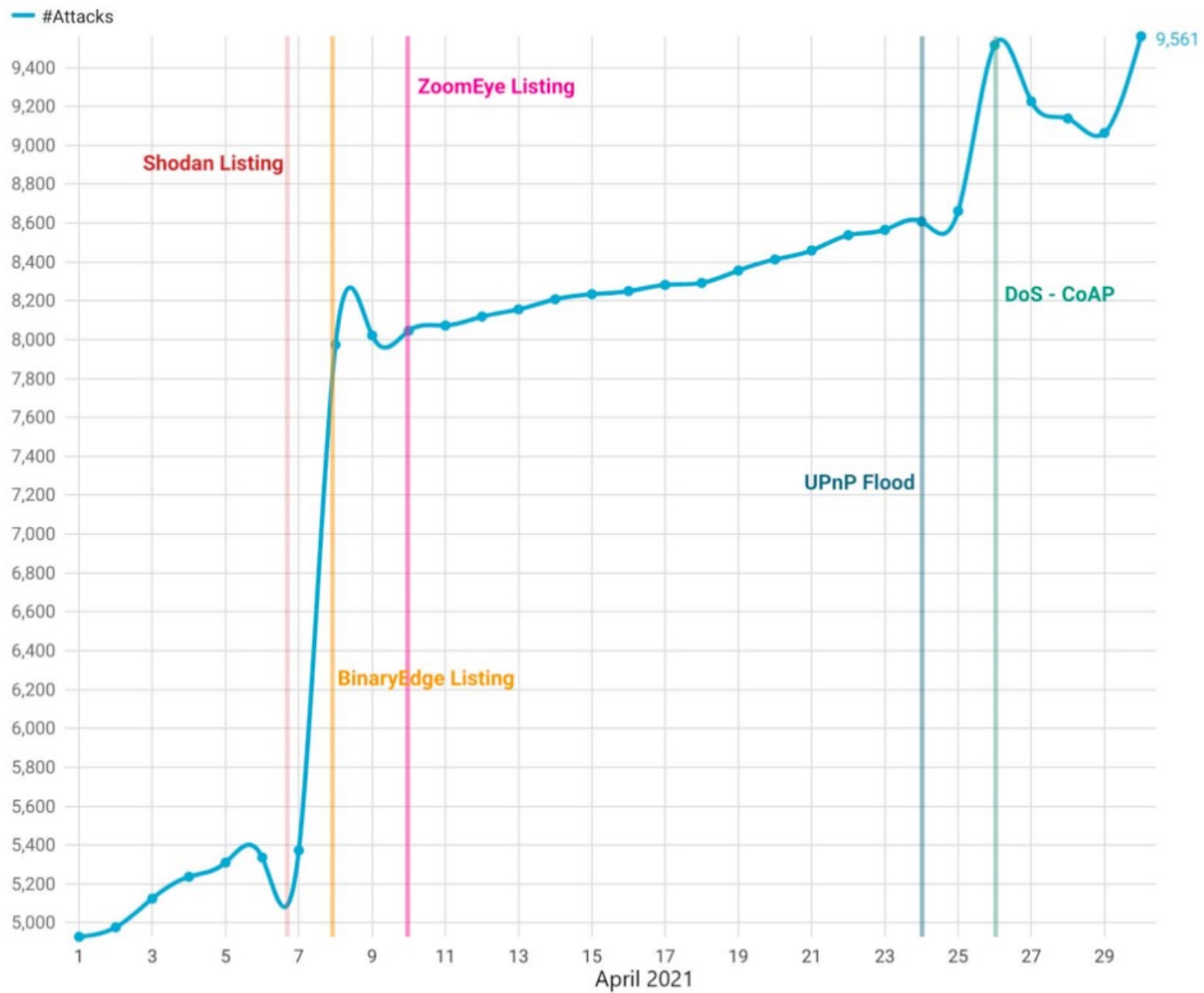
Telnet UPnP MQTT CoAP



Honeypots



What do you conclude?



Attacks per service

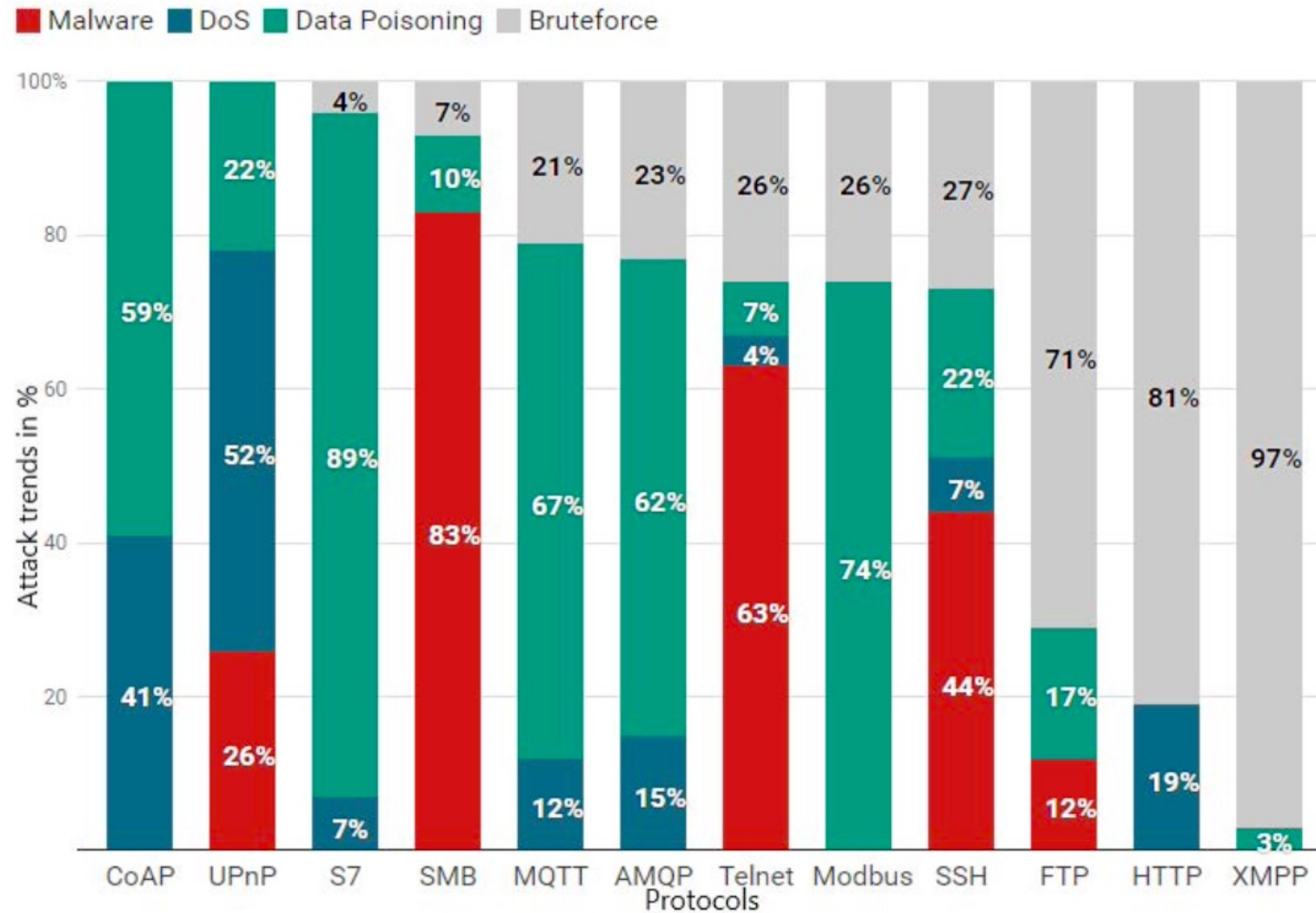


Figure 7: Attack trends by type (%) and protocol

Attacks per honeypot software

Honeypot	Simulated Device Profile	Protocol	#Attack events	Scanning service*	Malicious*	Unknown/Suspicious*
HosTaGe	Arduino Board with IoT Protocols	Telnet	19,733	2,866	21,189	2,347
		MQTT	2,511			
		AMQP	2,780			
		CoAP	11,543			
		SSH	19,174			
		HTTP	16,192			
		SMB	1,830			
U-Pot	Belkin Wemo smart switch	UPnP	17,101	1,121	7,814	1,786
Conpot	Siemens S7 PLC	SSH	12,837	1,678	11,765	1,876
		Telnet	12,377			
		S7	7,113			
		HTTP	11,313			
ThingPot	Philips Hue Bridge	XMPP	11,344	967	2,172	963
Cowrie	SSH Server with IoT banner	SSH	15,459	2,111	12,874	1,113
		Telnet	14,963			
Dionaea	Arduino IoT device with frontend	HTTP	11,974	1,953	13,876	1,694
		MQTT	1,557			
		FTP	3,565			
		SMB	6,873			
Total			200,209	10,696	69,690	9,779

Table 7: Total attack events by type and protocol on honeypots (* unique source IPs)

Telnet and SSH scans



Multistage attacks

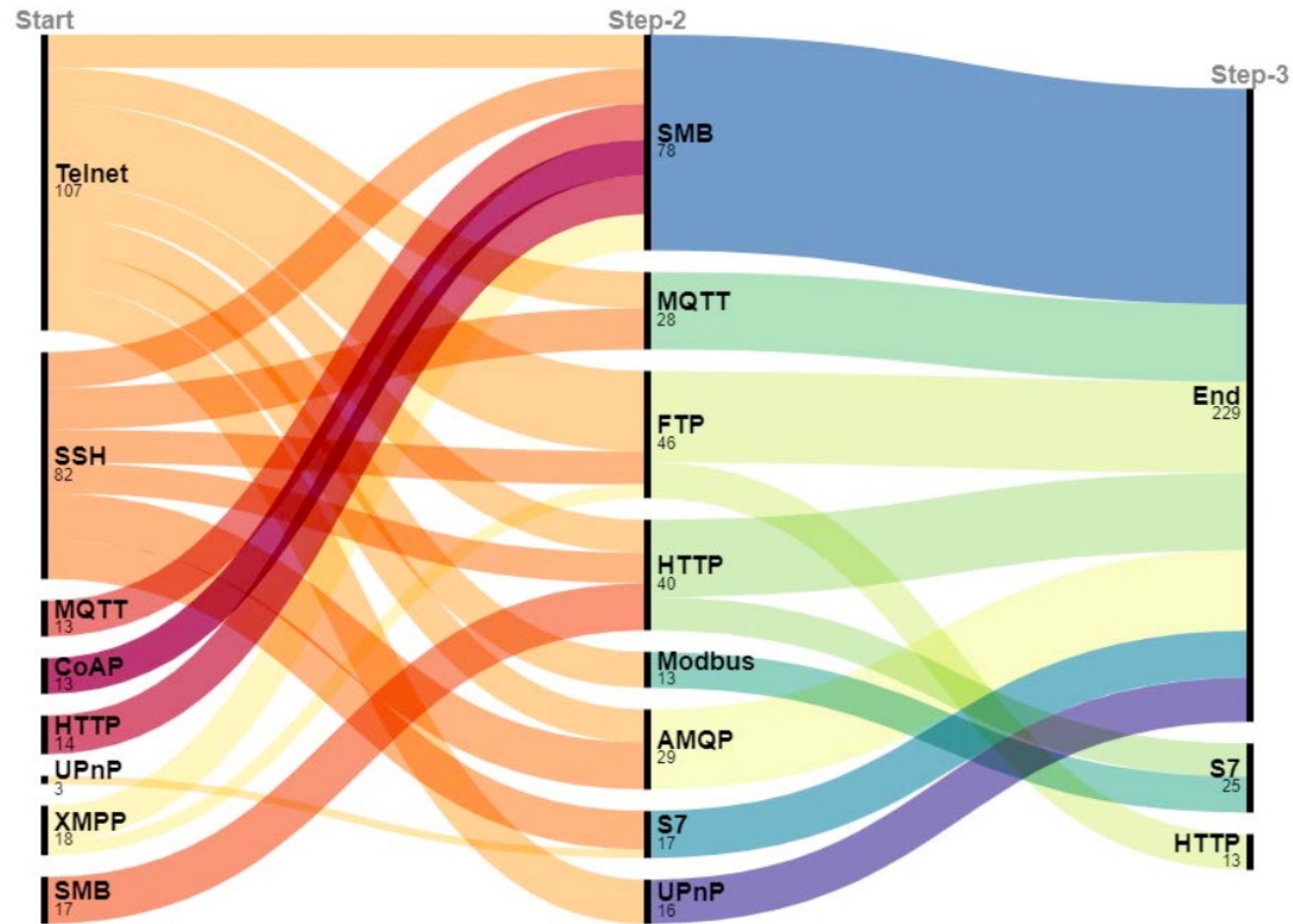


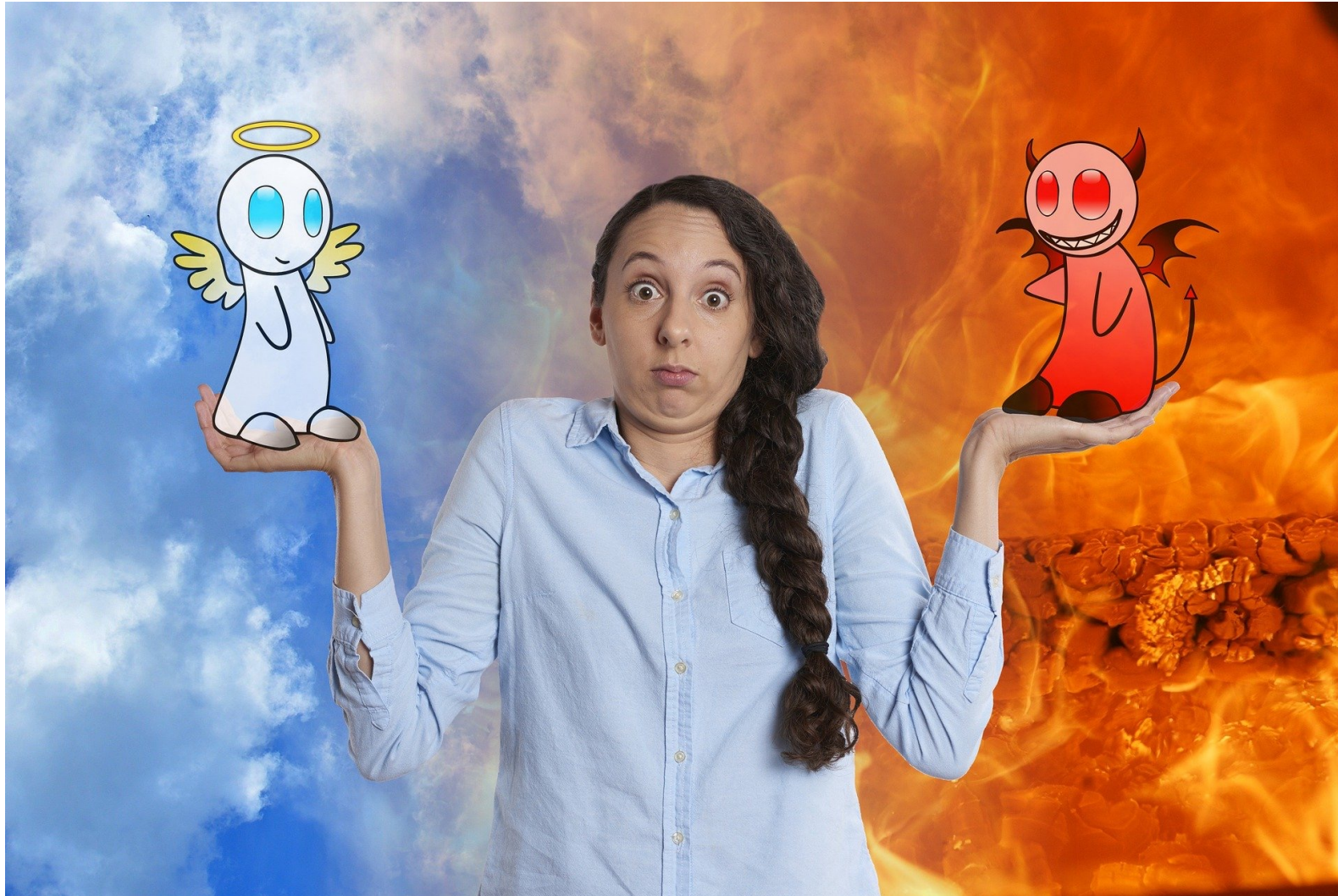
Figure 9: Multistage attacks detected on honeypots

Darknet / Network telescope

Protocol	Daily Avg. Count	Unique IP	Scanning-service	Unknown/Suspicious
Telnet	2,554,585,920	85,615,200	4,142	85,611,058
UPnP	131,794,560	1,8633	2,279	16,354
CoAP	68,353,920	2,342	627	1,715
MQTT	17,072,640	5,572	1,248	4,324
AMQP	13,907,520	7,132	2,256	4,876
XMPP	6,429,600	4,255	1,973	2,282
Total	2.7 Bil.	85.6 Mil.	12525	85.6 Mil.

Table 8: Telescope suspicious traffic classification

Ethics



Linking datasets



Volg ons

 SIDN.nl

 @SIDN

 SIDN

Discussion

Key takeaways

- RIoTMan shows the next steps in analyzing botnets in an automated fashion.
- Combining datasets (just like in the Mirai paper) at scale is feasible (but still a lot of work 😊)
- Today's papers only provide a small piece of the puzzle of how conduct botnet analysis in the future.

Lecture feedback

I am able to discuss analyzing different IoT botnets/malware at scale



Lecture feedback

I am able to discuss scanning IoT devices for vulnerabilities.



Volg ons

 SIDN.nl

 @SIDN

 SIDN

Discussion & feedback

Next lectures:

- **Guest lecture #1: Thu Jun 1, 08:45-10:30 CR 3H**
- **Regular: Mon Jun 5, 15:45-17:30, RA 2502**