Characterizing Background Noise in ICS Traffic Through a Set of Low Interaction Honeypots

Pietro Ferretti, **Marcello Pogliani**, Stefano Zanero

Politecnico di Milano

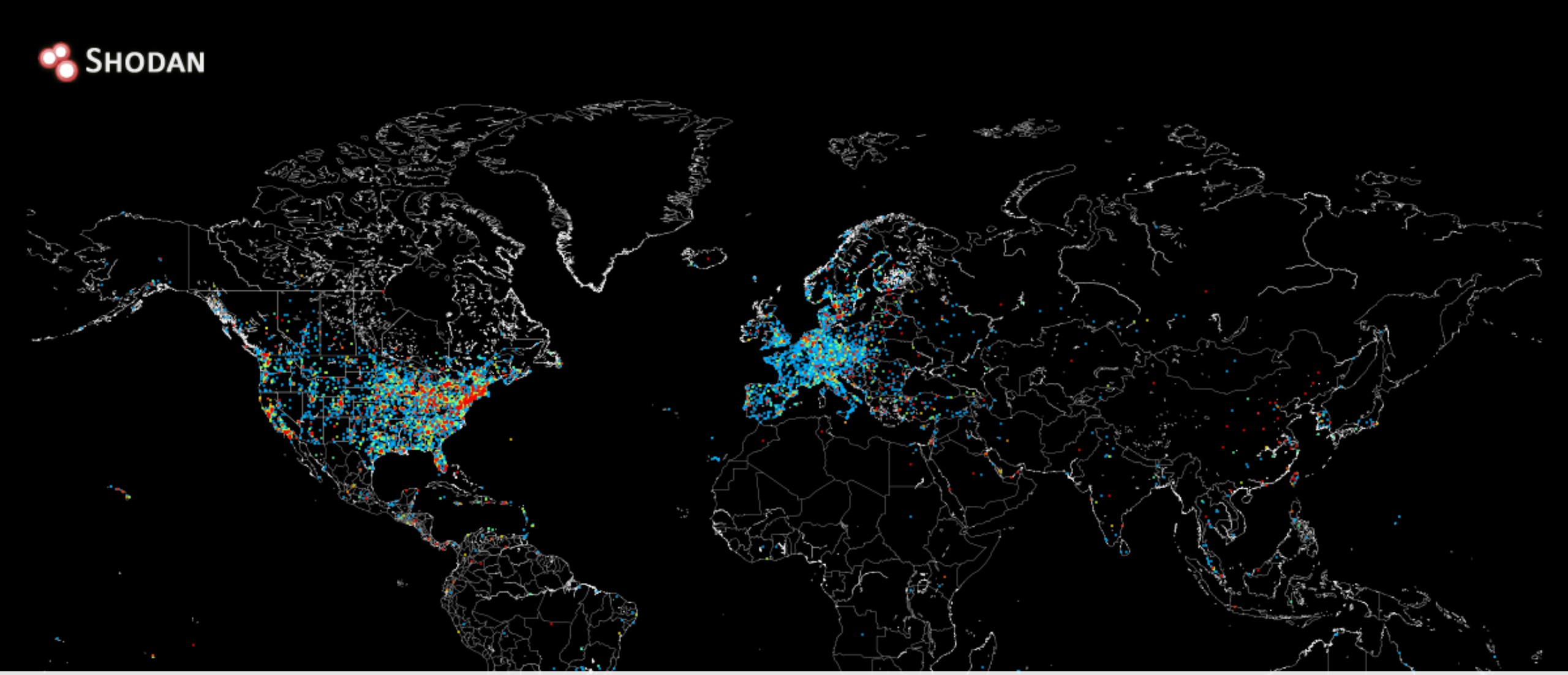
CPS-SPC, London, 11 November 2019

POLITECNICO
MILANO 1863

POLITECNICO MILANO 1863
NECST laboratory

Industrial Control Systems

Systems, devices, networks and controls used to operate and/or automate industrial processes



ICS on the Internet

What happens when you put a host with SSH enabled and a weak password on the Internet?

What happens when you put a ICS protocol (say, Modbus w/o auth) on the Internet?

ICS are on the Internet

ICS on the Internet may be targeted by malicious actors

Who is targeting exposed ICS?

How do these actors interact with them?

- Two different levels
  - Targeted traffic - sophisticated attacks
  - Untargeted traffic - "background noise" <------- our focus
- Prior work:
  - network telescopes \ traffic sniffing (network vantage points) \ honeypots

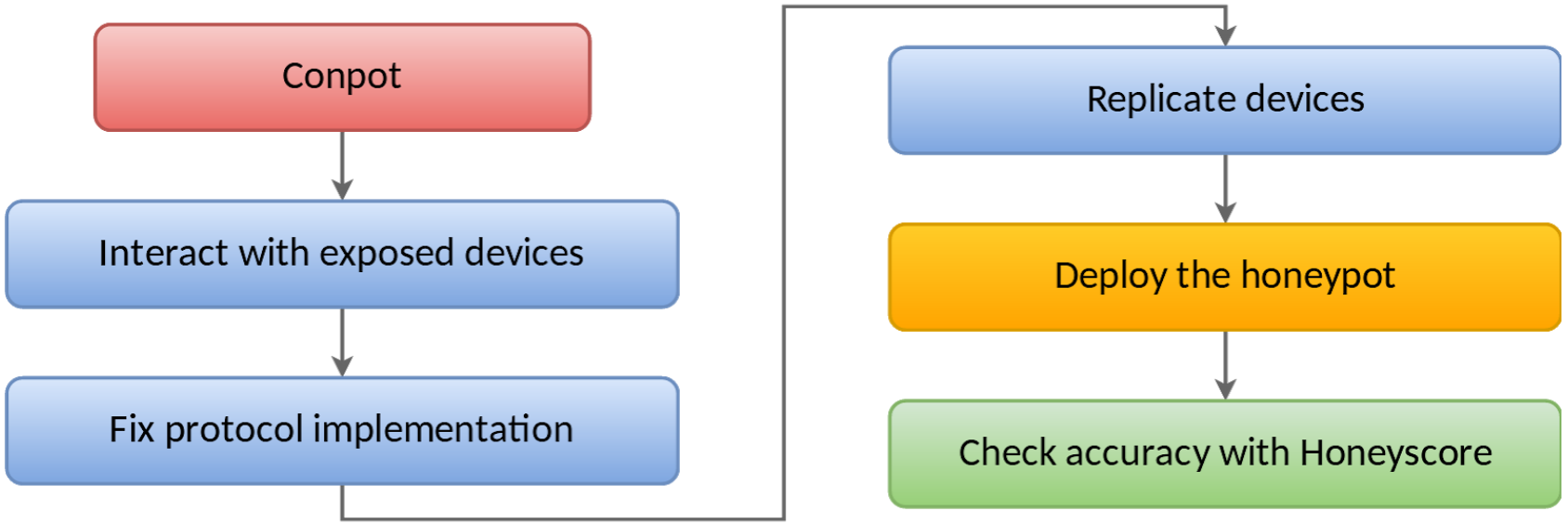
Limits of prior work

- Network telescopes are limited to attempted connections
- Easy-to-recognize honeypots
- Deployed very few honeypots
- Superficial analysis (traffic statistics only)

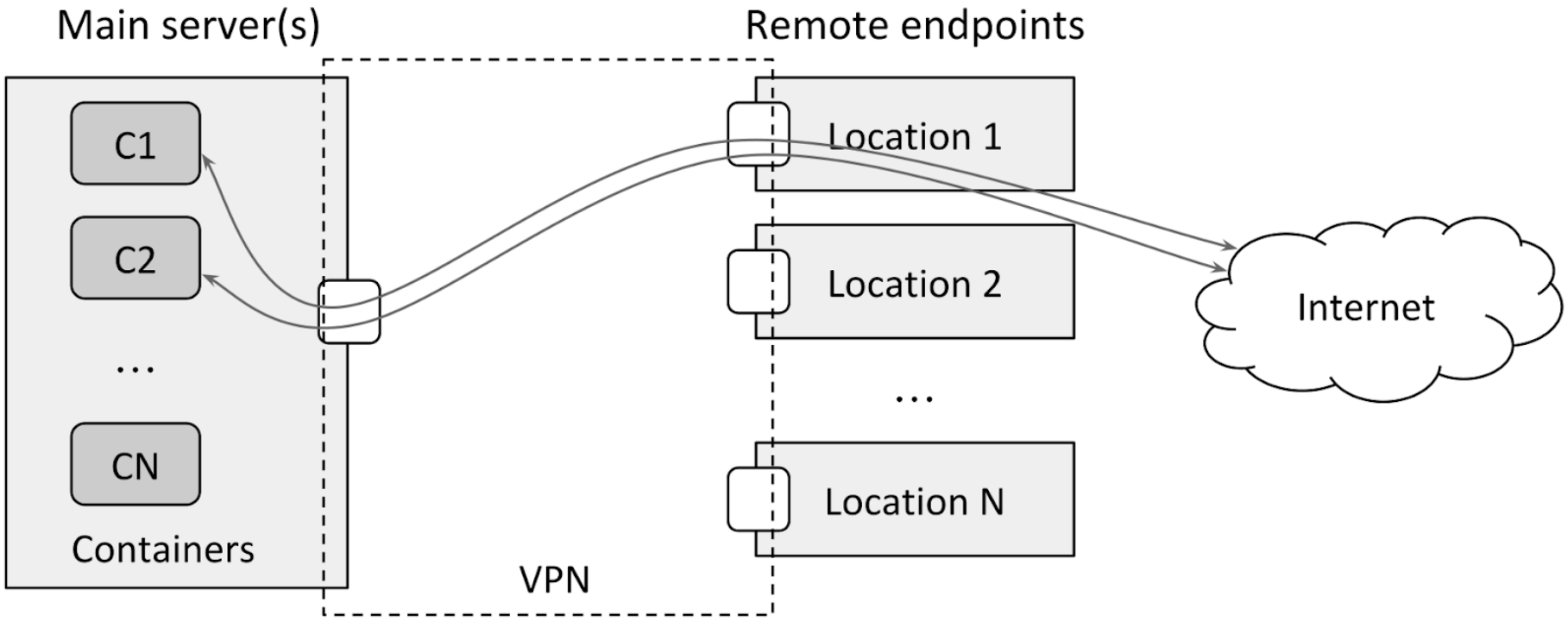
Our proposal:

- Hard-to-fingerprint honeypots
- Many network vantage points
- Comprehensive analysis of the actors

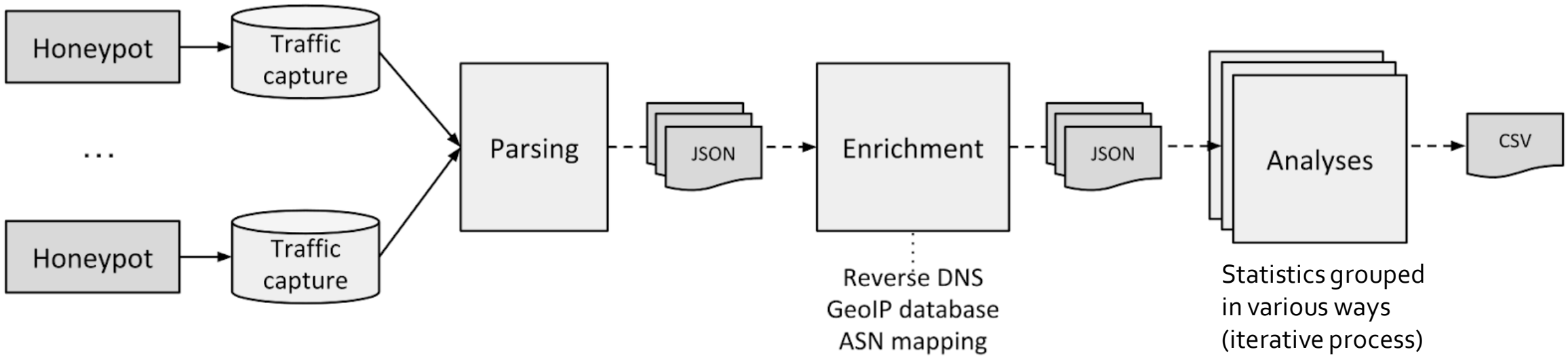
Conpot-based ICS Honeypots



Deployment Architecture



Analysis Pipeline



Deployment

- We exposed 35 Honyepot instances
  - (limit of our analysis – system is more scalable)
- Research network (our institution)
- Cloud services (GCP: US and Asia region)

Implemented Protocols

Process automation

- Siemens S7 (2 templates)
- Modbus (2 templates)
- EhterNet/IP (3 templates)

Power grid

- IEC-104

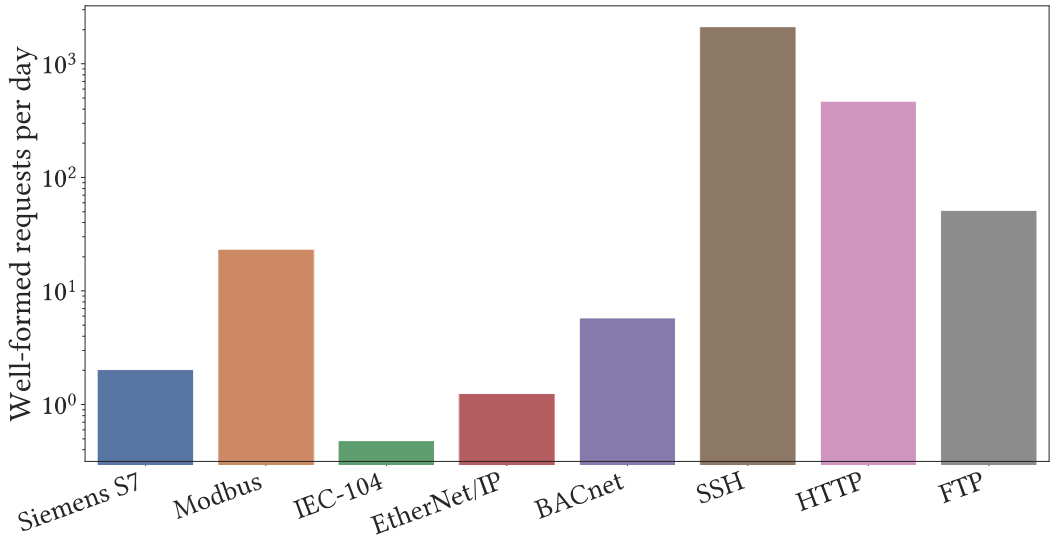
Building automation systems

- BACNet

Results (~ 4 months) – quick summary

- ICS protocol traffic has increased w.r.t. previous measurements
- Great majority of interaction ~= (nmap) scans

	Siemens S7	Modbus	IEC-104	EtherNet/IP	BACnet
Baseline SYN, UDP	1.84	2.28	0.71	2.02	1.73
Baseline inter.	1.58	1.64	0.63	1.99	1.35
SYN and UDP	7.58	33.22	3.01	3.62	9.22
Interactions	2.36	2.00	0.79	1.92	1.43
WF requests	2.42	27.95	0.83	1.12	8.95
WF interactions	0.66	1.24	0.33	0.99	1.40
Mirian et al. [12]	1.98	1.40	–	–	0.37



interaction = all the requests made by a source IP address on a specific instance in 24 hours
well-formed (WF) = protocol and port match

Results - Actors

- 1469 Ip addresses – 832 (57%) at least a **well-formed request**
- 97 distinct actors (DNS PTR or ASN or webpage)
  - 44 did make ICS-specific requests
  - 23 Siemens S7
  - 28 Modbus
  - 14 IEC-104
  - 20 EtherNet/IP
  - 21 BACNet
  - 7 **every supported protocol**
- Beijing University of Telecommunication: **only** S7comm

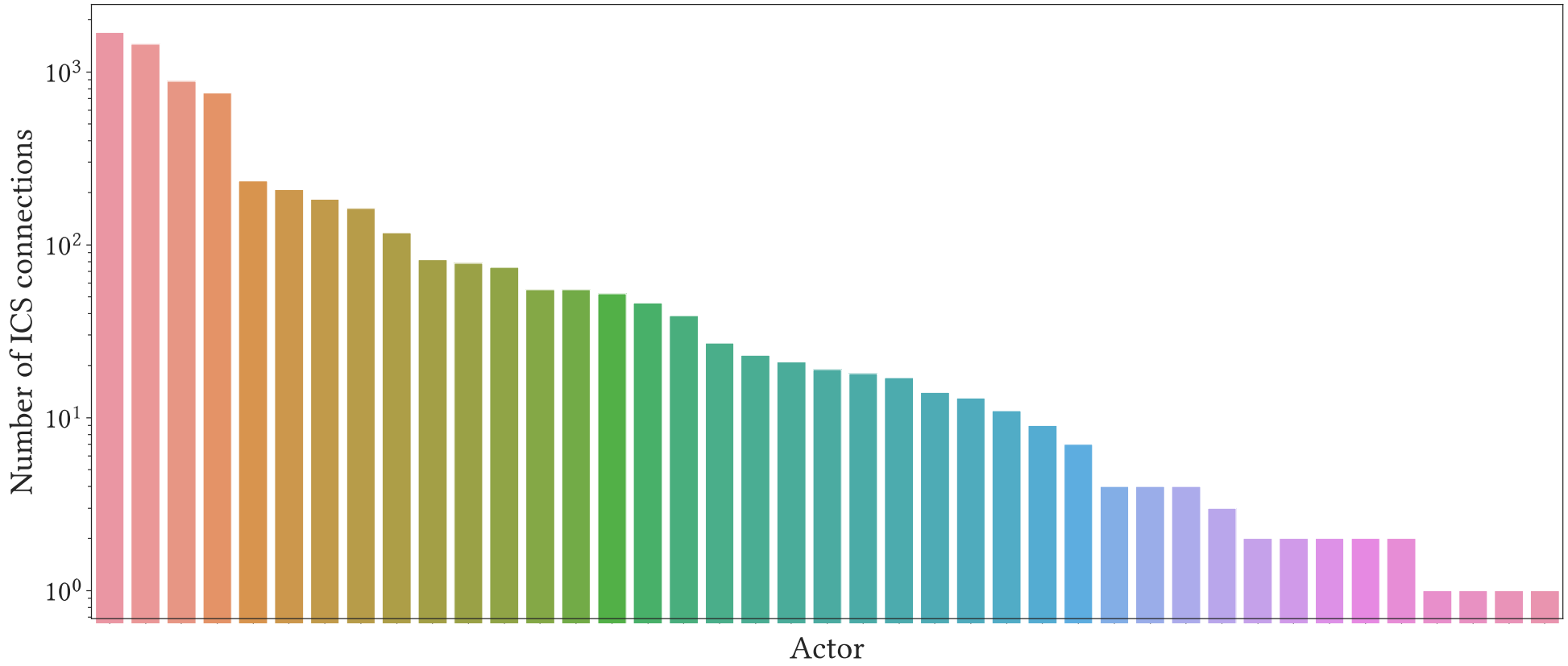
Actors – Public Scanners

Name	Autonomous System	Scanned Protocols
Alphastrike	AS25504	BACNet, EtherNet/IP, S7, Modbus
Beijing University of Telecommunications	AS4538	S7
Binaryedge	AS14061, AS63949	EtherNet/IP, S7, Modbus
Censys	AS237	BACNet, S7, Modbus
F-Secure (Inverse Path)	AS42708	S7
Kudelski Security	AS42570	BACNet, Modbus
Net Systems Research	AS36351, 50562, 60781	BACNet, EtherNet/IP, Modbus
Onyphe	AS12876, 16276, 63949	Modbus
Rapid7 (Project Sonar)	AS10439, 13213, 29302	BACNet
Shodan	AS10439, 174, 29073, 32475, 50613, 9009	BACNet, EtherNet/IP, S7, Modbus, IEC-104
Stretchoid	AS14061	S7, Modbus

Actors – Distribution

Most traffic is from a few regular scanners

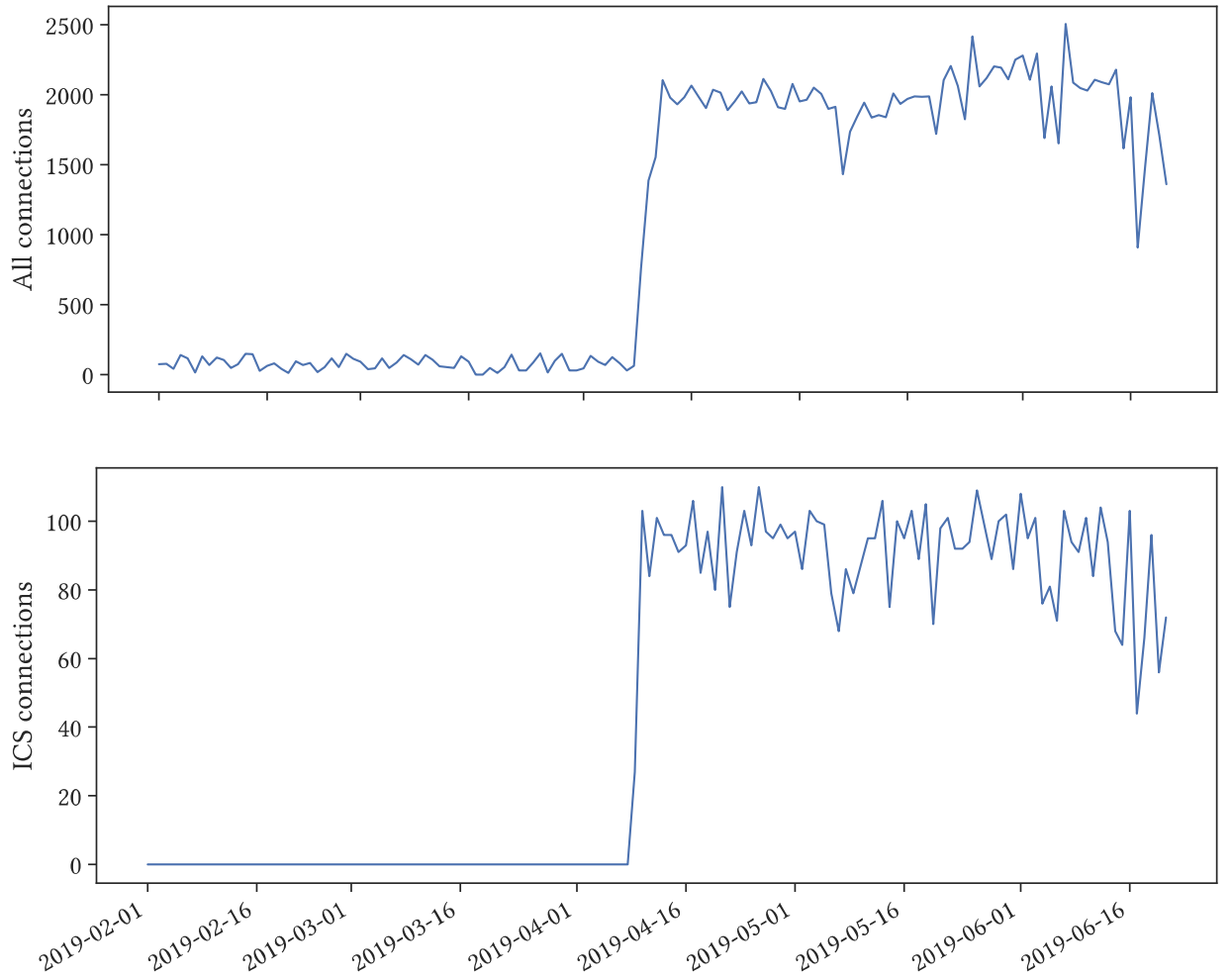
- 83% ICS connections made by four actors (Net Systems Research, Blackhost, Shodan, Censys)
- 92% top 10 actors
- Public scanners are periodic (weekly/monthly)



Actors – Non-public scanners

- 60% connections: Blackhost (US bulletproof)
- Non-cloud-sourced connections:
  - 89% China
  - 5% Vietnam
  - 3% US

Campaigns over time: Example - Blackhost



only target the honeypot instances we deployed on cloud

Requests received (harmless!)

Name	Requests	Description
Siemens S7		
Setup Communication	40.4%	Starts a new connection
Read SZL / Module Id.	34.8%	Basic module information
Read SZL / Component Id.	23.3%	Component information
Read SZL / Read All	1.9%	All available system information
Modbus		
Read Device Identification	51.5%	Requests vendor and model name, revision number
Report Slave Id	48.0%	Type, state, identification of one of the devices connected to the PLC
Unity	0.5%	Schneider Electric-specific request
IEC-104		
TESTFR	41.4%	Checks if the host is active
STARTDT	32.4%	Enables data transfer
C_IC_NA_1	26.1%	General Interrogation Command (returns the current sensor readings)
EtherNet/IP		
Request Session	0.4%	Requests a session token (optional) (Alphastrike)
List Identity	99.6%	Basic information, e.g., vendor ID, device type, model, serial number
BACNet		
Read Property	96.0%	Asks for a specific device property, e.g, device name, model name, location
Read Property Multiple	4.0%	Batched version of Read Property

Interesting Requests (reconnaissance?)

Modbus

Read Holding Registers

4 times

Source: AWS

10 x read holding register (slave units 0 to 9) to read the PLC internal state

Response: “illegal data access”

EtherNet/IP

Identity / Get Attribute All

2 times

Source: Hosting serv. (M247 LTD)

Addresses: 1 to 16

Request standard device info

Interesting Requests (cont'd)

SIEMENS S7

This time, requests to **write** data to memory
or **check** the security status of the device

1 x **read var** @ address 0x0 (Tor exit node)

1 x **read and write var** (AS4134 China Telecom)

1 x SZL 0x232 **communication status data** (China Unicom)

Interesting Requests – S7 – Details

Read and write variable

- Three "read var" requests
  - read 2 bytes at address M100
  - read 1 bit at address M100
  - read 1 byte at address M100
- One "write var" request
  - write 0 at address M100, bit 1
- Again, the three "read var"

Communication status data

- Three requests for the System Status List (SZL) address 0x232 @ index 4
  - CPU protection level
  - operator control settings
  - version ID/checksums

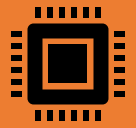
Scanning scripts

Most requests very similar except some parameters (context)

We can attempt to classify scripts according to such parameters

Value	Actors
Modbus: transaction ID identification number for a Modbus request; usually ignored	
`0` (used by Nmap)	ABCDE Group, AS Data, Binaryedge, Capitalonline, China Telecom (AS4134), China Hangzhou Alibaba, China Sichuan, DCS Pacific Star, Dahai Network, Kudelski Security, Shodan, Tamatiya, Vietnam CHT
`1`	China Telecom Chengdu
`4919` (i.e., `0x1337`)	Alphastrike, Blackhost, Censys, NetSystemsReseatch, Onyphe, Softlayer, Stretchoid, Vultr
`23111`	World Hosting Farm
random value	China Ucloud Shangai
IEC-104: QOI used in the IEC-104 General Interrogation Command to further specify the type of sensors to read from; usually ignored.	
`0`	Capitalonline, Shodan, Vietnam CHT, World Hosting Farm
`20` (used by Nmap)	Baidu Netcom, China Hangzhou Alibaba, China Sichuan, China Ucloud Shangai, EHOSTIDC
EtherNet/IP: context works as an identification number for the EtherNet/IP request	
`0`	Alphastrike, Blackhost, NetSystemsResearch, Softlayer
`0xc1debed1` (used by Nmap)	Baidu Netcom, Binaryedge, China Telecom (AS4134), China Sichuan, China Ucloud Shangai, China Wenzhou, Velia, World Hosting Farm
`0x6a0ebe64`	Shodan, Vietnam CHT

Concluding Remarks



ICS scanning is dominated by "centralized" research-oriented scans, rather than malicious actors and botnet-sourced traffic

Most "background noise" traffic are harmless requests for information, matching standard scanning scripts like nmap

We found no instances of *definitely* harmful behavior, and only a few instances of potentially harmful behavior or reconnaissance activities

Limitations and future work

Deployment: more vantage points & study differences

Protocols: support for further and/or proprietary protocols

Low interaction ~> high interaction

Study more complex attacks (it is a different problem, though)

Thanks!

Questions?

marcello.pogliani@polimi.it
@mapogli