WORKSHOP GARR 2020

NET MAKERS

A Honeypot Framework for the Internet of Things

Marco Lucchese and Massimo Merro

Department of Computer Science

University of Verona

A brief history of the Internet of Things

1990

The world's first Internet-connected toaster

1999

The term Internet of Things was invented by Kevin Ashton

2000

Samsung fridge is the first commercial IoT device. With a whopping price of 20000 USD

2004

Tabloids start mentioning IoT

2016

Mirai infects 600k IoT devices

2020

More than 20 billion of IoT devices

Vulnerabilities of IoT

Hackers Remotely Kill a Jeep on the Highway —With Me in It

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

CYBER / NEWS BRIEFS

Kaspersky honeypots find 105 million attacks on IoT devices in first half of 2019

Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

FDA overseeing crucial firmware update in US to patch security holes and prevent hijacking of pacemakers implanted in half a million people

A Hacker Forced 50,000 Printers To Spread PewDiePie Propaganda -- And The Problem Is Much Bigger Than You Know

What is a honeypot?

- VIRTUAL / HARDWARE
- VULNERABLE
- ALLURING
- SAFE

What are honeypots useful for?

- MALWARE ANALYSIS TO COLLECT SIGNATURES
- MALWARE ANALYSIS TO DISCOVER ZERODAYS
- TARGETED ATTACKS RECOGNITION
- INTRUSION DETECTION

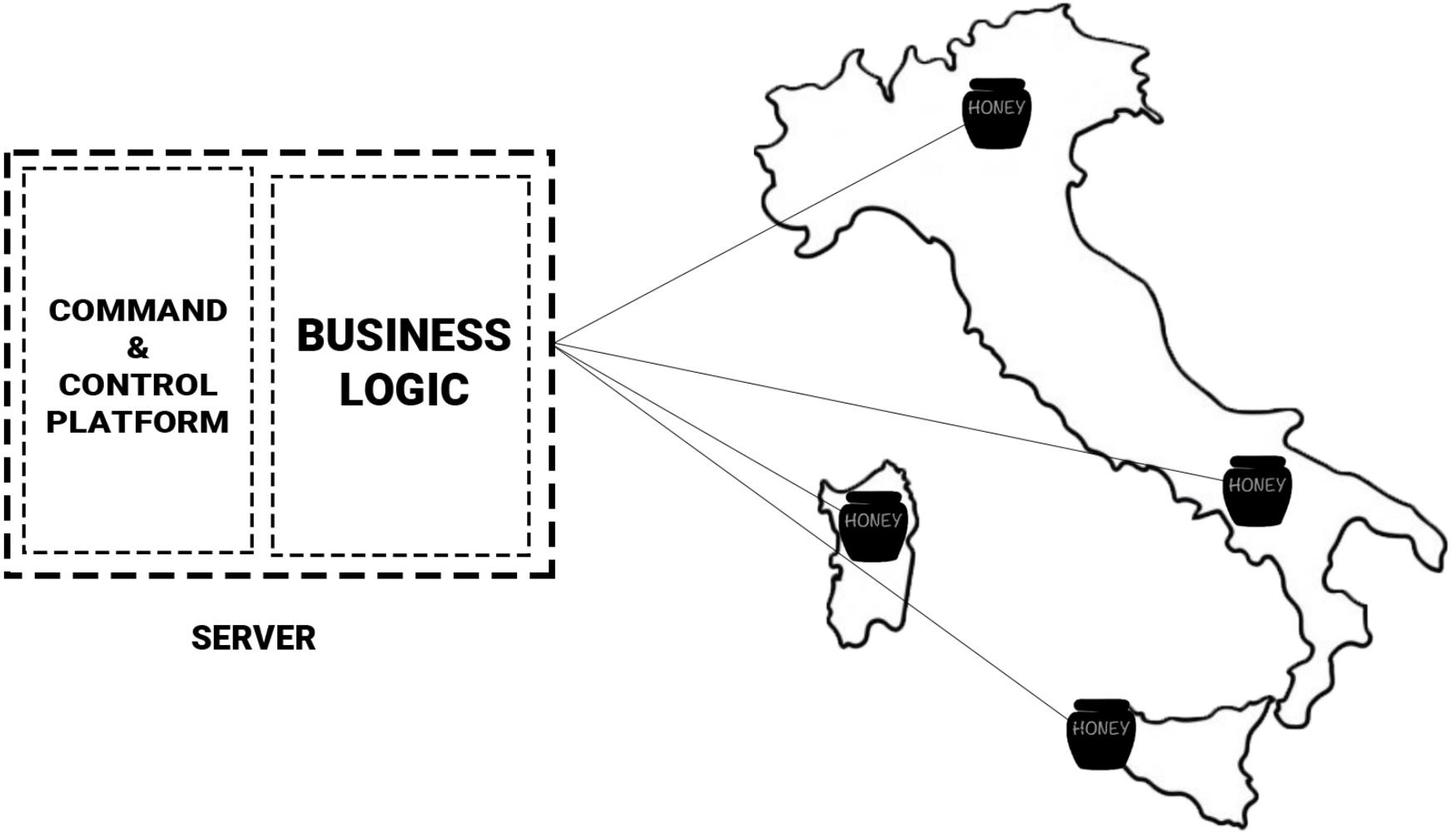
Honeypots for IoT

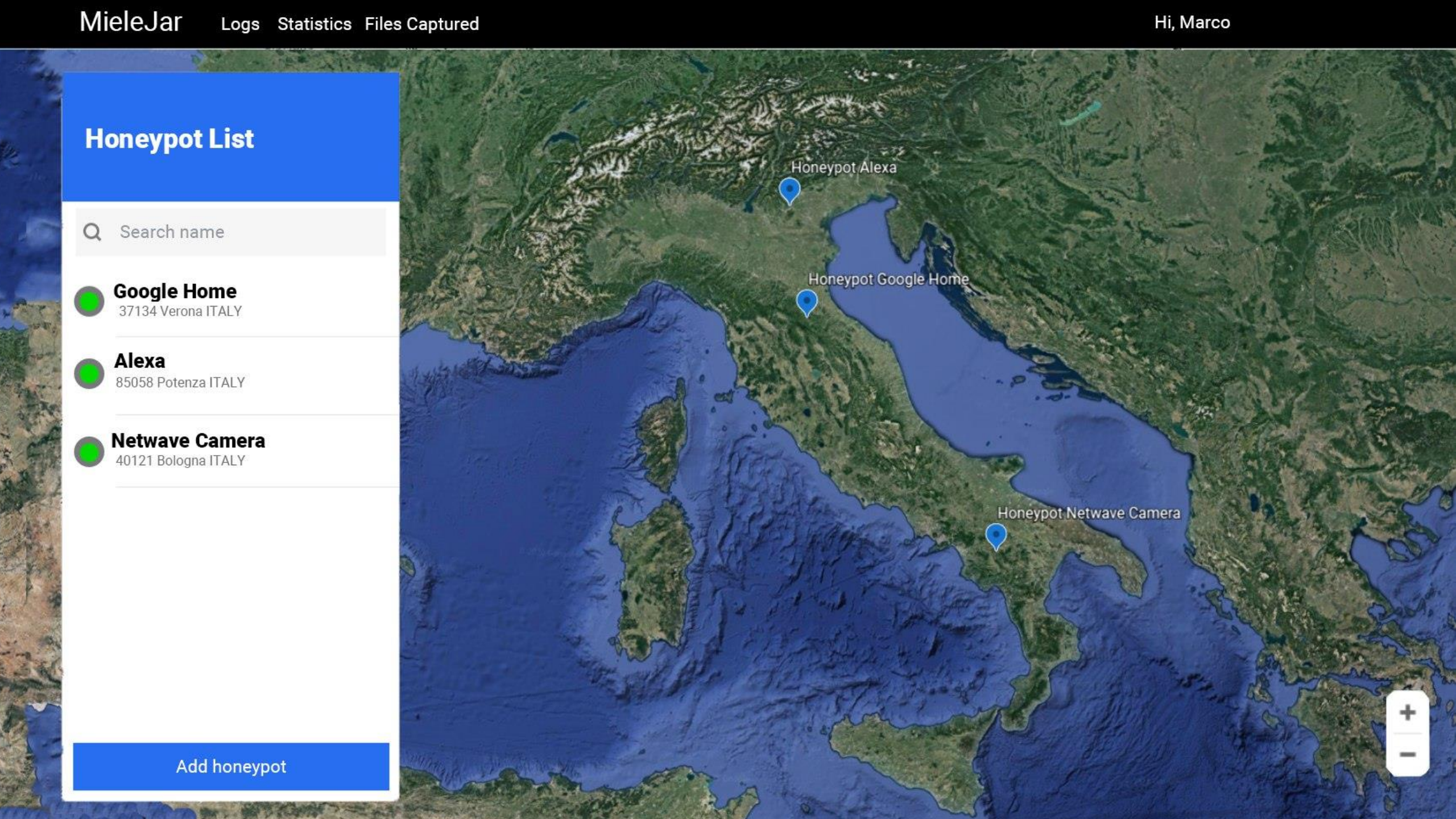
- **IoTPOT** > Honeypot that emulates interactions of the Telnet protocol and a variety of IoT devices.

- **IoTCandyJar** > Honeypot that uses machine learning technology to automatically learn behavioural knowledge of IoT devices.

- **SIPHON** > Honeypot that uses physical IoT devices connected to various geographical locations through so-called wormholes.

MieleJar: A framework for IoT honeypots




MieleJar
Logs
Statistics
Files Captured
Hi, Marco
Honeypot List
Search name
Google Home
37134 Verona ITALY
Alexa
85058 Potenza ITALY
Netwave Camera
40121 Bologna ITALY
Add honeypot
Honeypot Alexa
Honeypot Google Home
Honeypot Netwave Camera

Logs

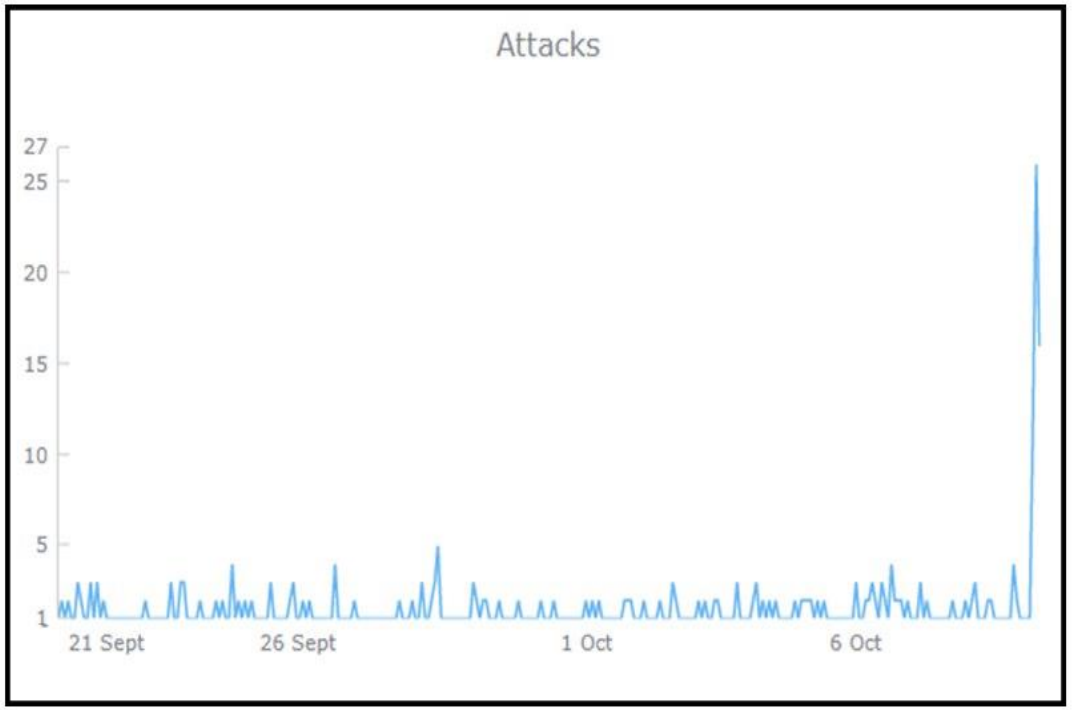
Google Home (Id. 3)

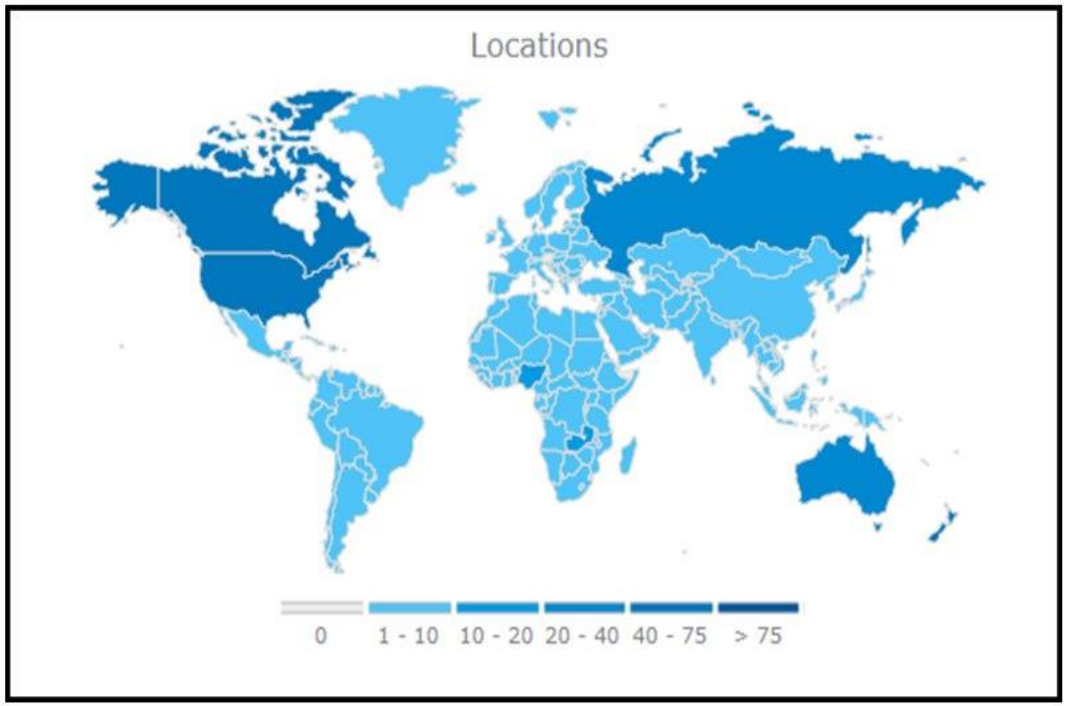
Search Log

Path	IP	Date
GET /setup/bluetooth/status	157.47.21.28	Oct 8, 2020
GET /setup/scan_results	1557.27.34.156	Oct 8, 2020

Statistics

Google Home (Id. 3)





Files Captured

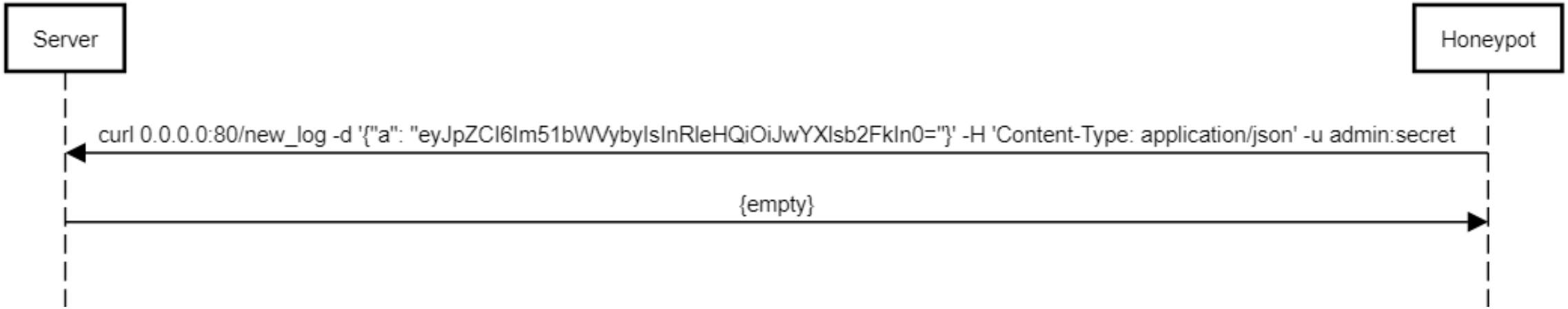
New Archived

Search File

File name	Flag	Size	Capture date
325044.bin ab32064691e52c89b7ac2086ed5dc934	OFF	147 KB	Oct 8, 2020
446436.bin 4bde55d8cea6c4d5305a7894f5273460	OFF	96 KB	Oct 8, 2020

Business logic: Installation protocol

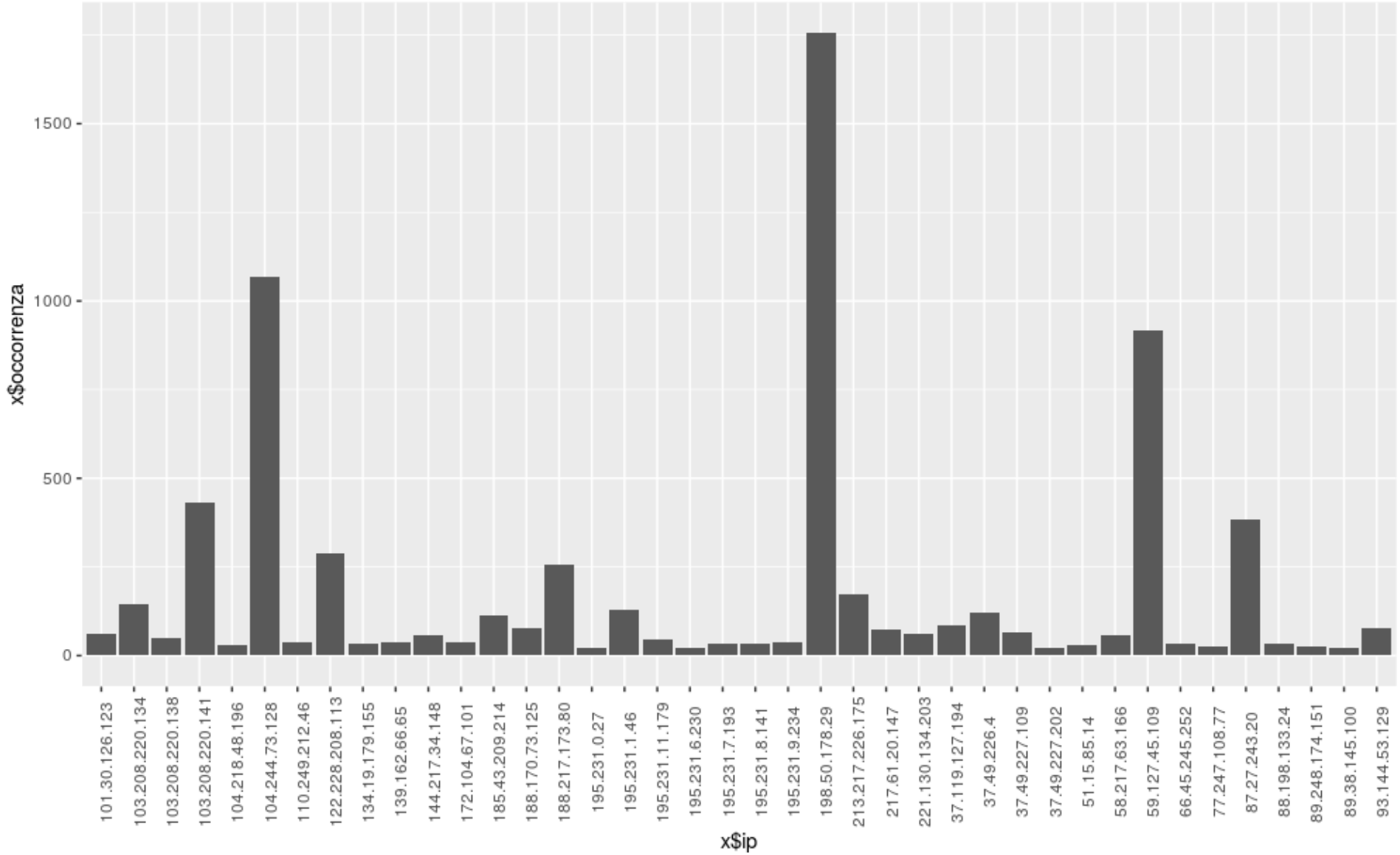
Business logic: Log protocol



Captured Malwares

- **MIRAI** malware for generic IoT devices. Used for botnets
- **HAJIME** variant of Mirai, built on a peer-to-peer network. Used for botnets
- **GAFGYT** malware for BusyBox devices, it connects back to a server. Used for botnets

Attacks in 6 months



Bibliography

- L. Spitzner: **Honeypots: Tracking Hackers**, published by: Addison-Wesley Professional, 2002
- J. D. Guarnizo, A. Tambe, S. S. Bhunia, M. Ochoa, N. O. Tippenhauer, A. Shabtai, Y. Elovici: **SIPHON: Towards Scalable High-Interaction Physical Honeypots** in CPSS@AsiaCCS(2) 2017: 57-68
- C. J. B. Abbas, L. J. G. Villalba, V. Lopez: **Implementation and attacks analysis of a honeypot** in ICCSA (2) 2007: 489-502
- M. F. Razali: **IoT Honeypot: A Review from Researcher's Perspective** in IEEE Conference on AINS 2018: 93–98.
- B. Lingenfelter, I. Vakilinia, S. Sengupta: **Analyzing Variation Among IoT Botnets Using Medium Interaction Honeypots** in CCWC 2020: 761-767
- A. Vetterl, R. Clayton: **Honware: A Virtual Honeypot Framework for Capturing CPE and IoT Zero Days** in eCrime 2019: 1-13
- M. A. Hakim, H. Aksu, A. S. Uluagac, K. Akkaya: **U-PoT: A Honeypot Framework for UPnP-Based IoT Devices** in IPCCC 2018: 1-8

Mirai: the botnet that disrupted Internet