IOT VULNERABILITY ANALYSIS

A CYBERINTELLIGENCE PROJECT

DEVELOPED BY

CAPONE LEONARDO

DI GENOVA MARIO

ROMANI MICHELE

Abstract

Internet of Things devices are an exponentially growing trend.

The world is connected, anything is getting ‘smart’.

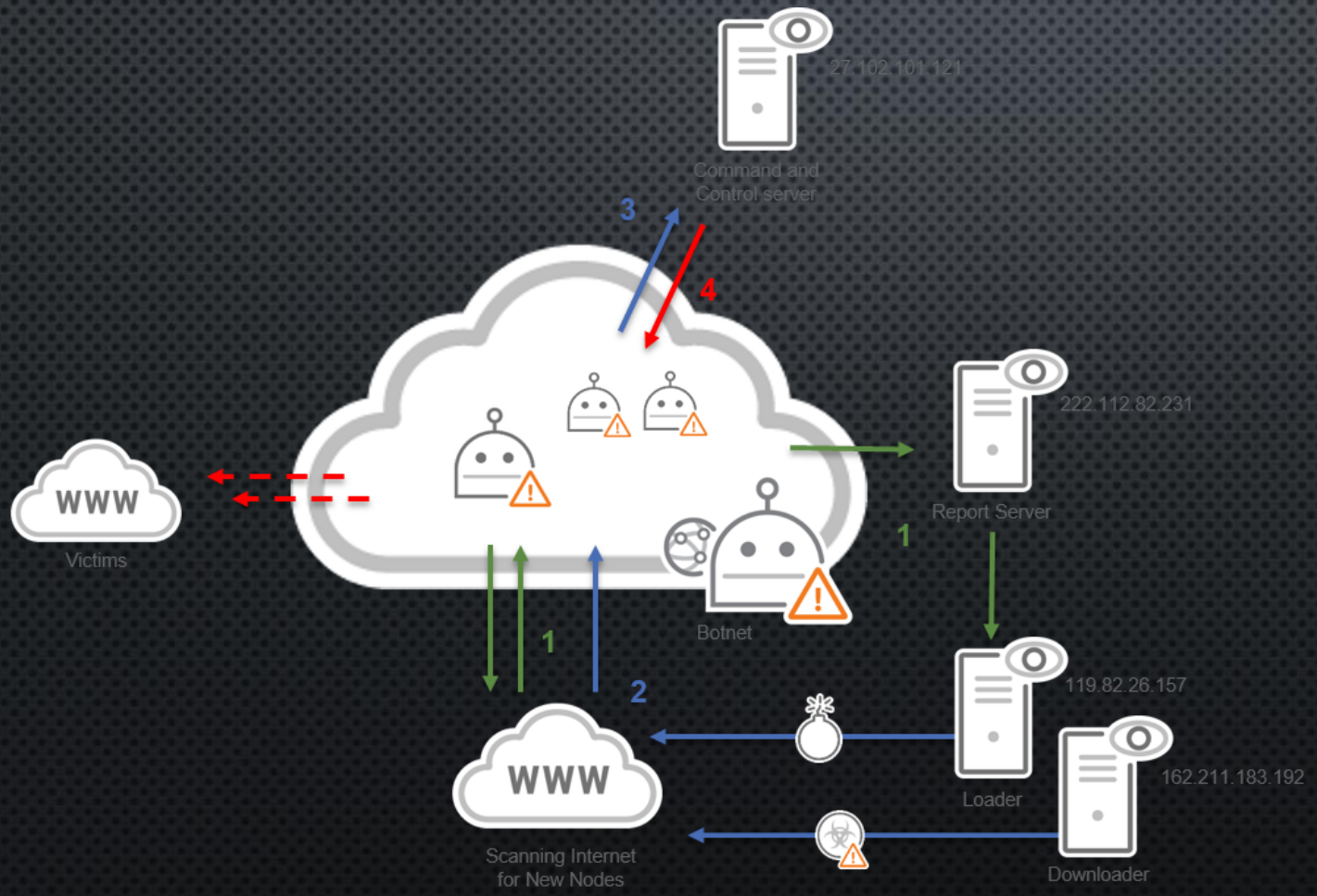
As their number grows the risk of cyberattacks and exploits drastically increases.

Our analysis will show you this threat is real by identifying vulnerable IoT devices…

IOT: QUICK OVERVIEW

- 31 BILLION DEVICES IN 2018
- WEBCAMS, SENSORS, SMARTTV, RASPBERRY, CARS, FRIDGES…
- 237 DDOS ATTACKS PER MONTH IN 2017 (+91%)

DISTRIBUTED DENIAL OF SERVICE ATTACK USING IOT DEVICES: HOW DOES IT WORK



- A MALEVOLENT HACKER EXPLOITS VULNERABLE IOT DEVICES
- THE BOTNET MALWARE SPREADS ON LOCAL NETWORKS
- ALL INFECTED DEVICES JOIN THE 'HEADLESS' ZOMBIE ARMY
- THE DDOS ATTACK BEGINS…

A RECENT EXAMPLE

- In March 2018 Github servers have been targeted by an huge DDoS attack
- ~1,35 Terabytes of data per second
- ~20 minutes of attack
- They luckily managed to survive forwarding traffic to their partners…

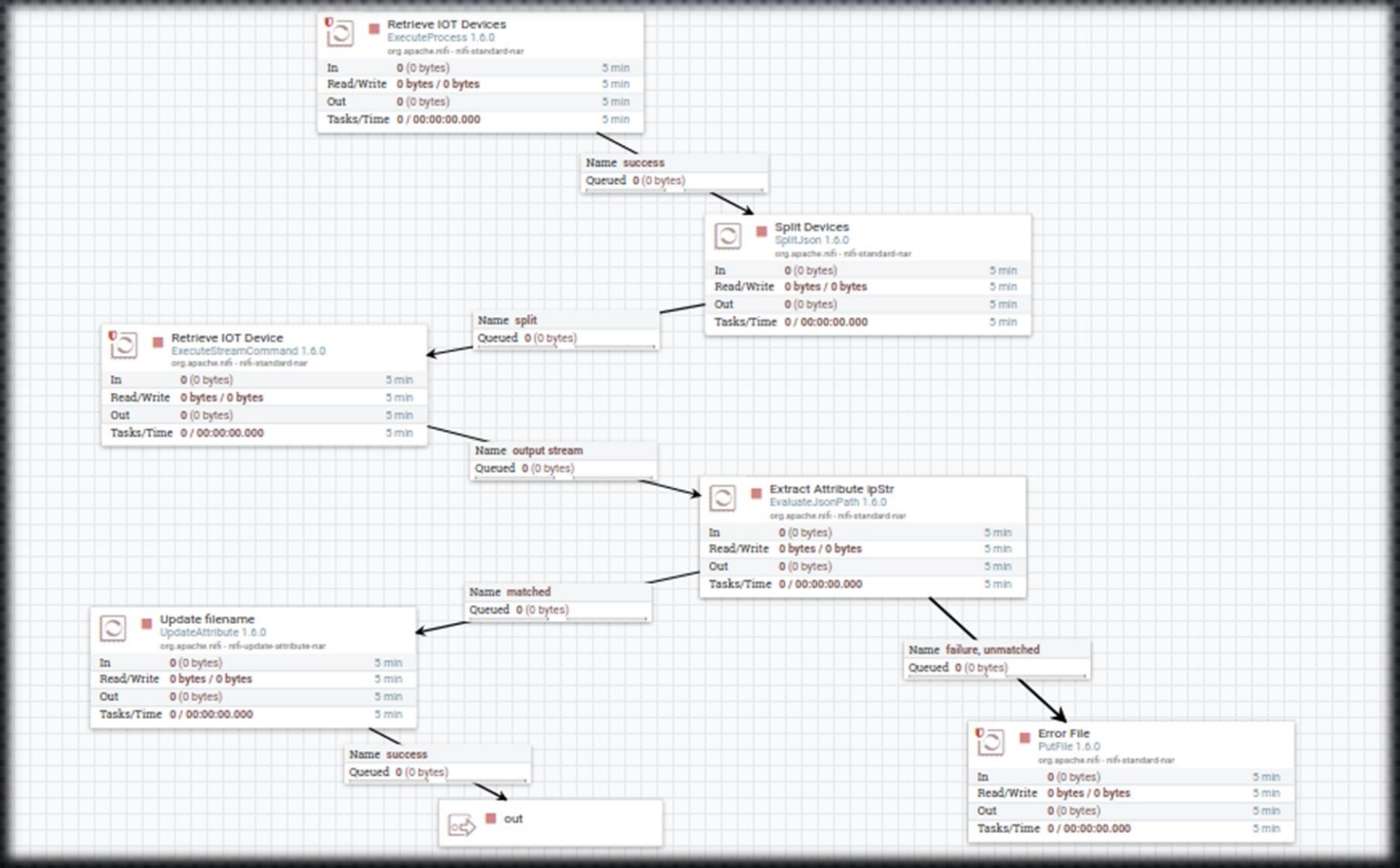
IOT VULNERABILITY ANALYSIS PROJECT

THE SOFTWARE BUILT FOR THIS PROJECT IS CAPABLE OF RETRIEVING CRITICAL DATA FROM HUNDRED OF THOUSANDS OF IOT DEVICES VISIBLE ON THE INTERNET. IT THEN ELABORATES THESE DATA TO EXTRACT USEFUL STATISTICS AND PLOT THEM.

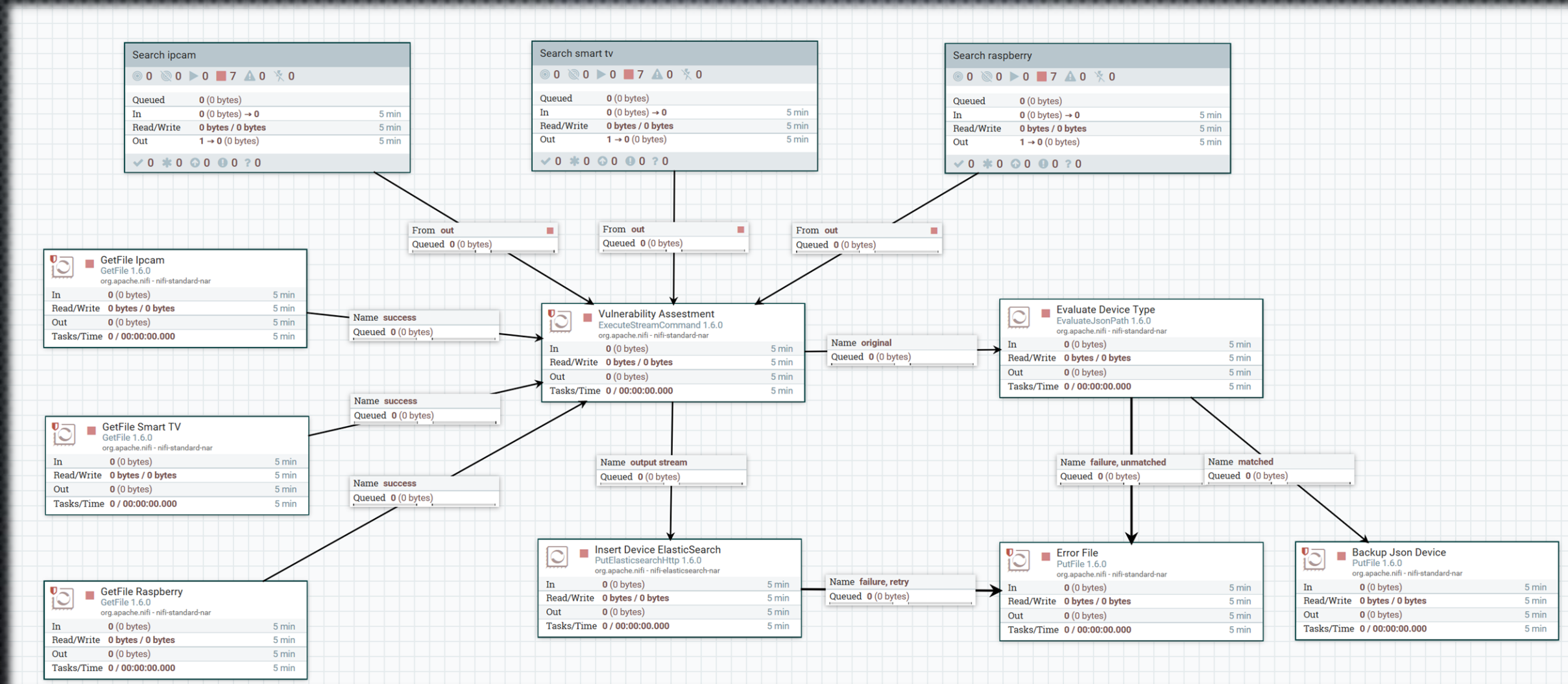
IOT VULNERABILITY ANALYSIS: TOOLS

- SHODAN: A POWERFUL WEB-CRAWLER WITH A LARGE REPOSITORY OF IOT DEVICES AND RESTFUL API
- PYTHON 3.6: A FLEXIBLE HIGH LEVEL PROGRAMMING LANGUAGE TO RETRIEVE AND ELABORATE DATA
- APACHE NIFI: A FLOW-BASED PROGRAMMING SOFTWARE TO MANAGE INTERACTIONS BETWEEN ALL THE OTHER TOOLS
- ELASTICSEARCH: A LUCENE-BASED SEARCH ENGINE TO PERFORM QUERIES ON AN HEAVY LOAD OF DATA. PART OF THE ELK STACK.
- KIBANA: A POPULAR VISUALIZER FOR ELASTICSEARCH TO PLOT THE RESULTS OF OUR ANALYSIS. PART OF THE ELK STACK.

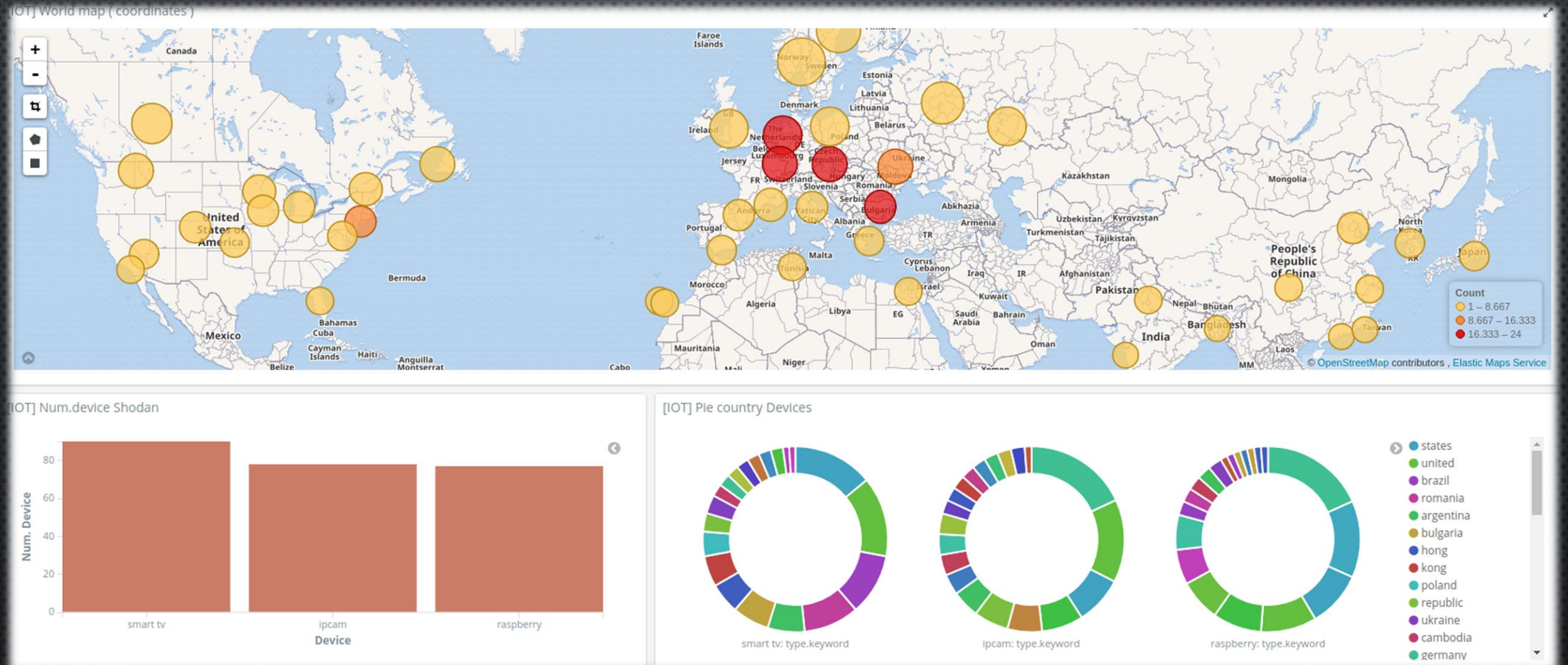
NIFI EXECUTION FLOW FOR RETRIEVING DATA



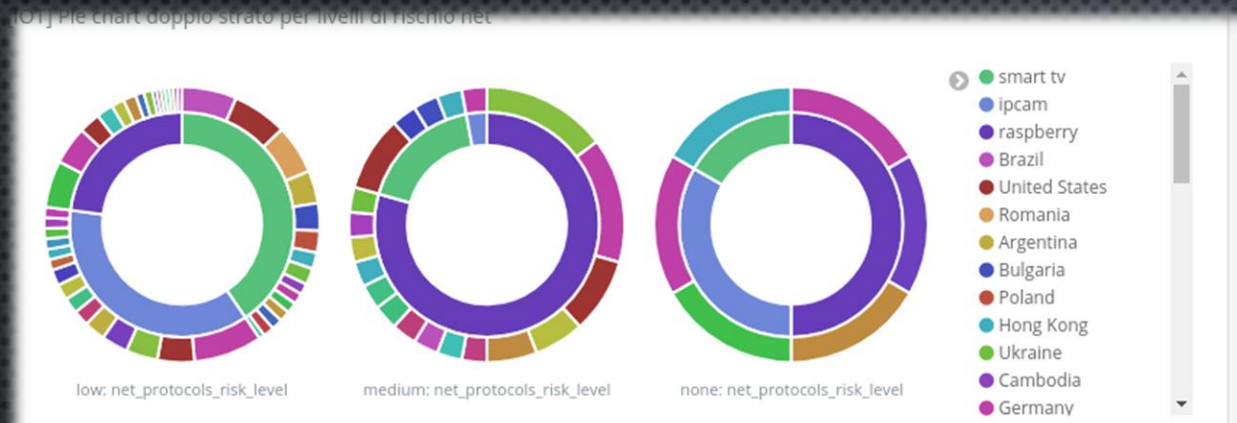
NIFI EXECUTION FLOW OF THE PROJECT



KIBANA DASHBOARDS PT.1



KIBANA DASHBOARDS PT.2



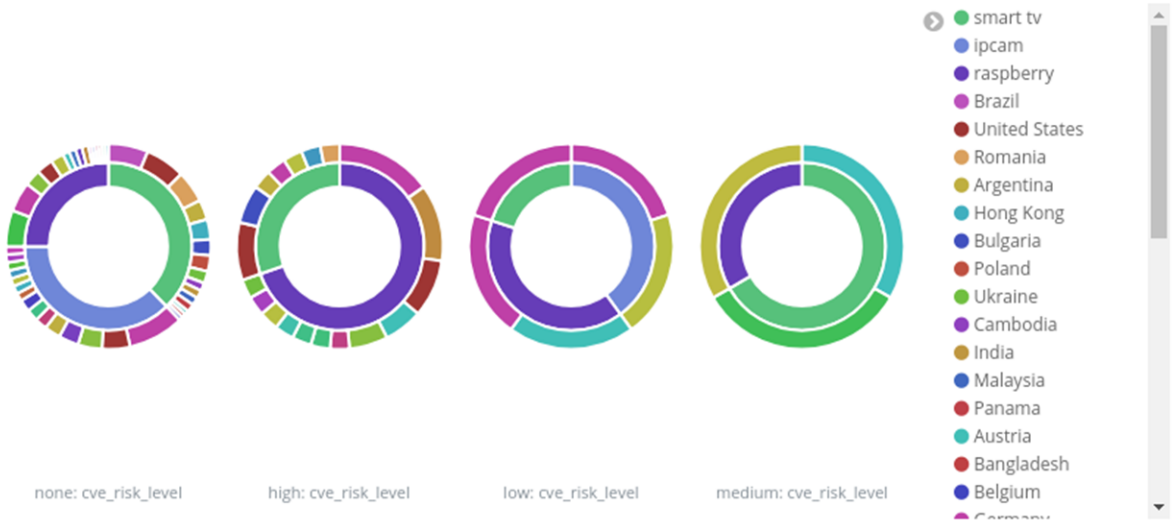
1–50 of 245

Time	ip_str	country_name	type	net_protocols_risk_level	net_protocols_
July 11th 2018, 19:05:46.211	93.223.9.34	Germany	ipcam	low	1
July 10th 2018, 20:06:03.516	151.236.4.155	Austria	raspberry	low	1
July 11th 2018, 19:55:19.670	84.143.245.215	Germany	ipcam	low	1

[IOT] Tag products

KIBANA DASHBOARDS PT.3

[IOT] Pie chart doppio strato per livelli di rischio cve



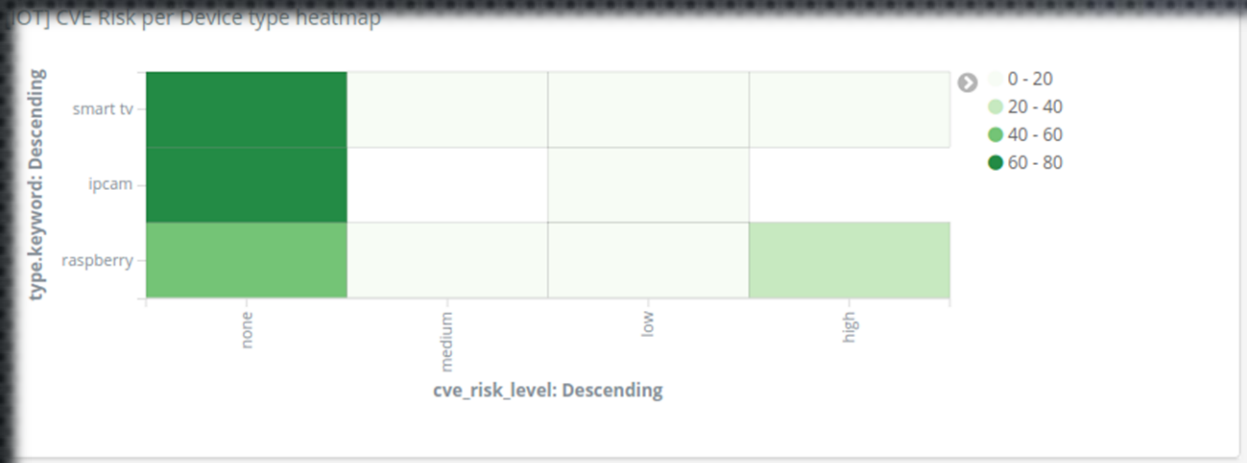
[IOT] Tag vulns cve

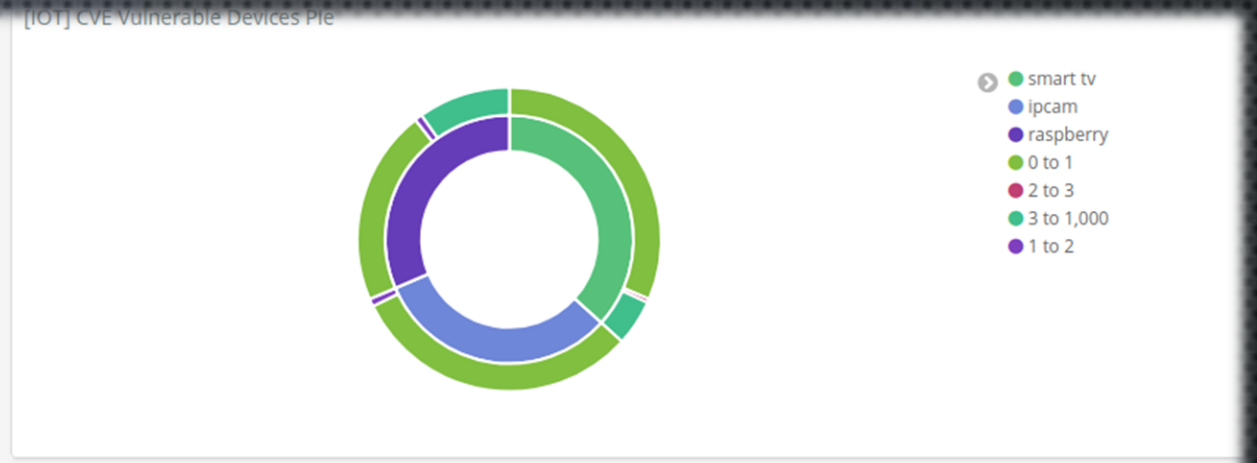
[IOT] Search Table (ip,country,type,cve_risk_level,cve_vuln_count)

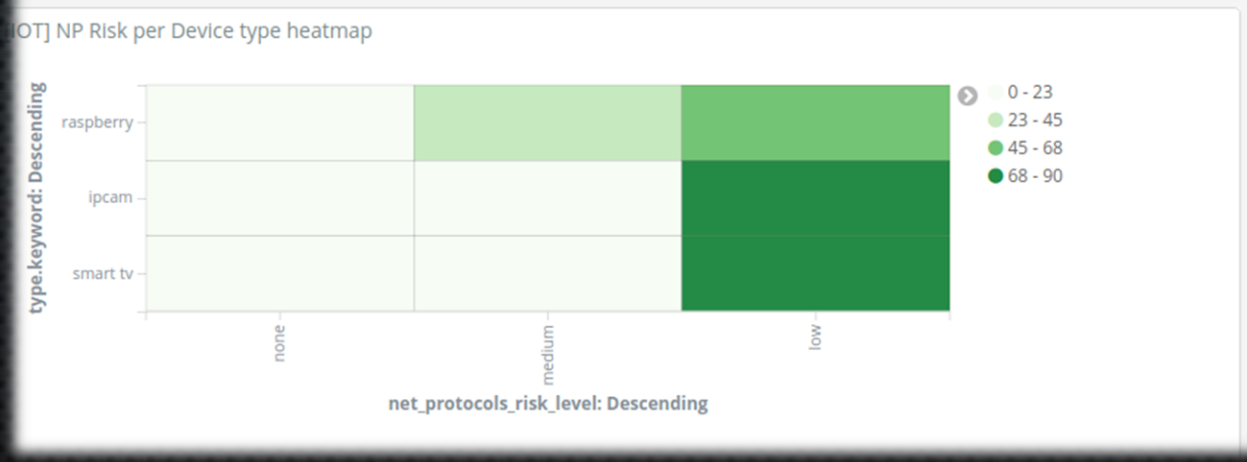
1–50 of 245

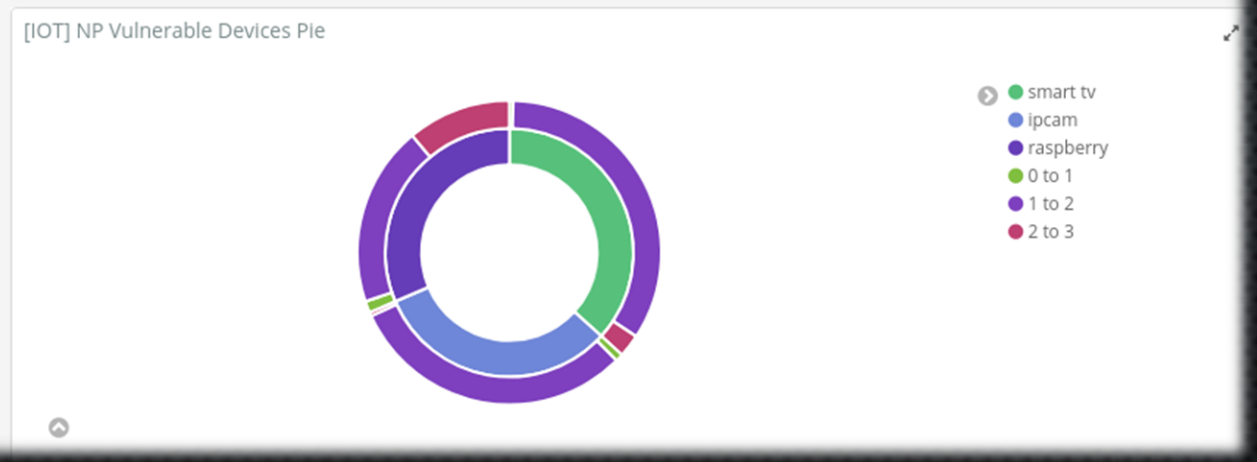
Time	ip_str	country_name	type	cve_risk_level	cve_vuln_count
July 10th 2018, 16:53:31.523	78.137.53.173	Ukraine	raspberry	high	15
July 10th 2018, 20:06:03.516	151.236.4.155	Austria	raspberry	high	18
July 11th 2018, 12:55:20.484	104.159.132.220	United States	raspberry	high	11
July 9th 2018, 17:45:22.723	114.34.246.167	Taiwan	raspberry	high	11
July 9th 2018, 09:15:11.326	84.131.63.108	Germany	raspberry	high	40
July 6th 2018, 14:04:08.665	188.26.98.73	Romania	smart tv	high	22
July 11th 2018, 05:48:06.003	100.34.208.104	United States	raspberry	high	11
July 4th 2018, 11:54:43.842	172.254.163.198	United States	smart tv	high	10
July 9th 2018, 00:11:46.343	91.238.117.56	Italy	raspberry	high	15
July 11th 2018, 00:05:36.422	95.43.105.90	Bulgaria	smart tv	high	11
July 10th 2018, 18:59:20.636	213.145.110.200	Bulgaria	smart tv	high	15
July 11th 2018, 04:10:15.487	85.191.31.84	Denmark	raspberry	high	11
July 10th 2018, 09:53:24.901	190.2.6.166	Argentina	smart tv	high	15

DASHBOARDS PLOTTED USING KIBANA PT.3









SOME RELEVANT RESULTS FROM THE ANALYSIS

//TO BE REVEALED @ LIVE PRESENTATION…