Srujan – Safer Networks For Smart Homes

SANKET KARPE

MANAGER, MALWARE RESEARCH, QUALYS

About Me

- Sanket Karpe

  Manager, Malware Research @ Qualys

  Developed ANWI (All New Wireless IDS)

  https://github.com/SanketKarpe

Agenda

- How IOTs make Smart home networks “dumb”
- Well known attacks carried out using IOT devices
- What is Srujan?
- How Srujan adds “Smartness” to Smart Home networks
- How Srujan Works?
- Demo

How IOTs make Smart home networks “dumb”

- No updates or patching mechanism for majority of devices
- Hard-coded credentials
- No system hardening
- Insecure default configuration
- Phone home to insecure or abandoned domains

Well known attacks carried out using IOT devices

- Mirai botnet used to cause 1 Tbits/s DDOS attack
- Silix Malware bricking devices
- Largest L7 DDoS using 400K IOT devices observed by Imperva recently
- 2019 SonicWall Cyber Threat Report reveals that IoT malware increased 55%

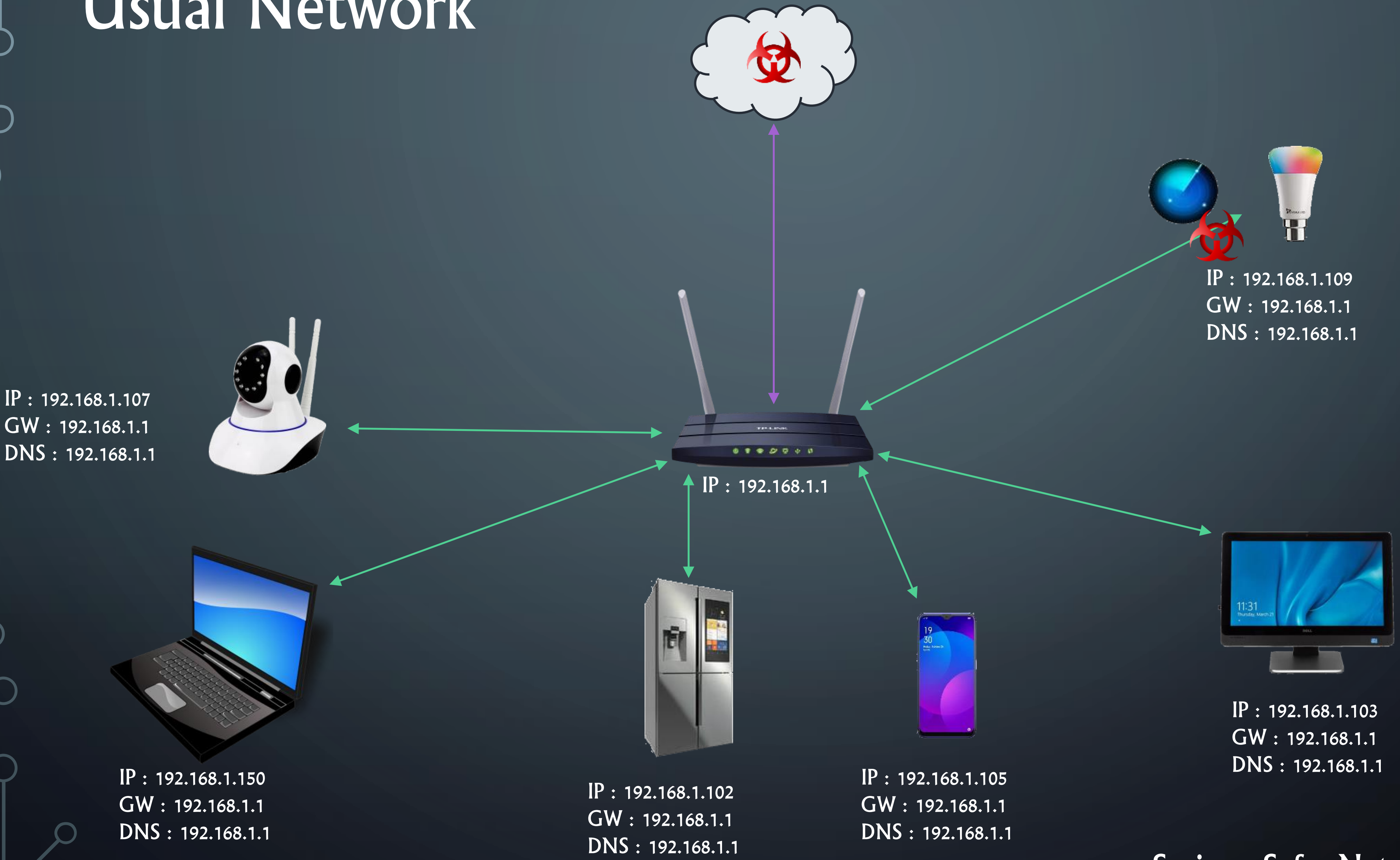
What is Srujan?

- Srujan is ‘smart’ network segregation system
- Segregates computers and mobile devices from low-trust IOT devices to mitigate risk of cross infection.
- Created to address challenges of IOT devices that are vulnerable and do not receive patches.
- Deployable on Raspberry Pi 3B+
- Major Components – Sfw Appliance & Reporting Server

How Srujan adds “Smartness” to Smart Home networks

- Segregation of Low trust devices from other systems
- Periodic scans to identify open ports and services
- Regular report on network usage and anomalies
- Preventing “call-home” connections
- Lookup DNS/IP against blacklist

Usual Network



IP : 192.168.1.109
GW : 192.168.1.1
DNS : 192.168.1.1

IP : 192.168.1.107
GW : 192.168.1.1
DNS : 192.168.1.1

IP : 192.168.1.1

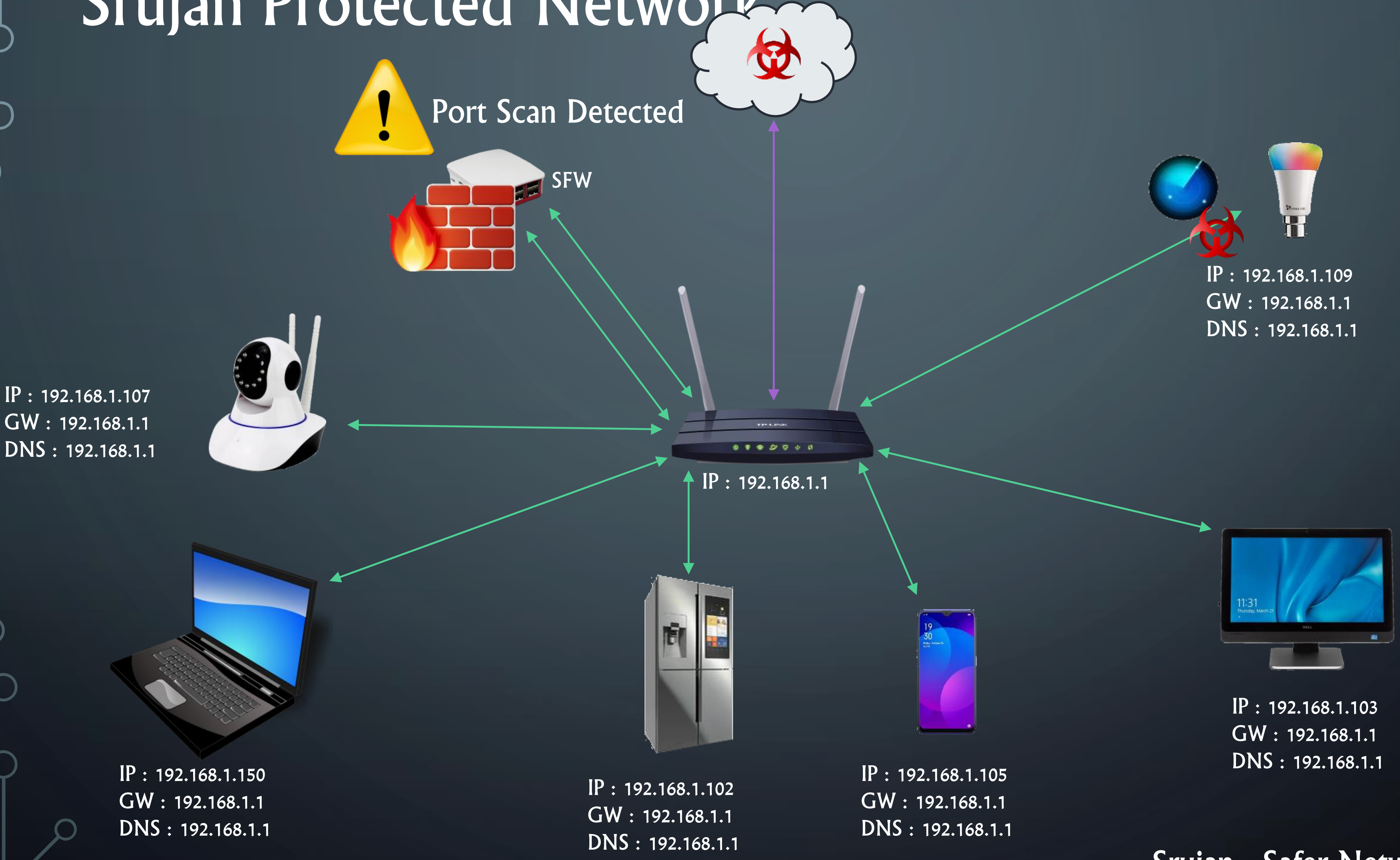
IP : 192.168.1.150
GW : 192.168.1.1
DNS : 192.168.1.1

IP : 192.168.1.102
GW : 192.168.1.1
DNS : 192.168.1.1

IP : 192.168.1.105
GW : 192.168.1.1
DNS : 192.168.1.1

IP : 192.168.1.103
GW : 192.168.1.1
DNS : 192.168.1.1

Srujan Protected Network



Port Scan Detected

SFW

IP : 192.168.1.109
GW : 192.168.1.1
DNS : 192.168.1.1

IP : 192.168.1.107
GW : 192.168.1.1
DNS : 192.168.1.1

IP : 192.168.1.1

IP : 192.168.1.150
GW : 192.168.1.1
DNS : 192.168.1.1

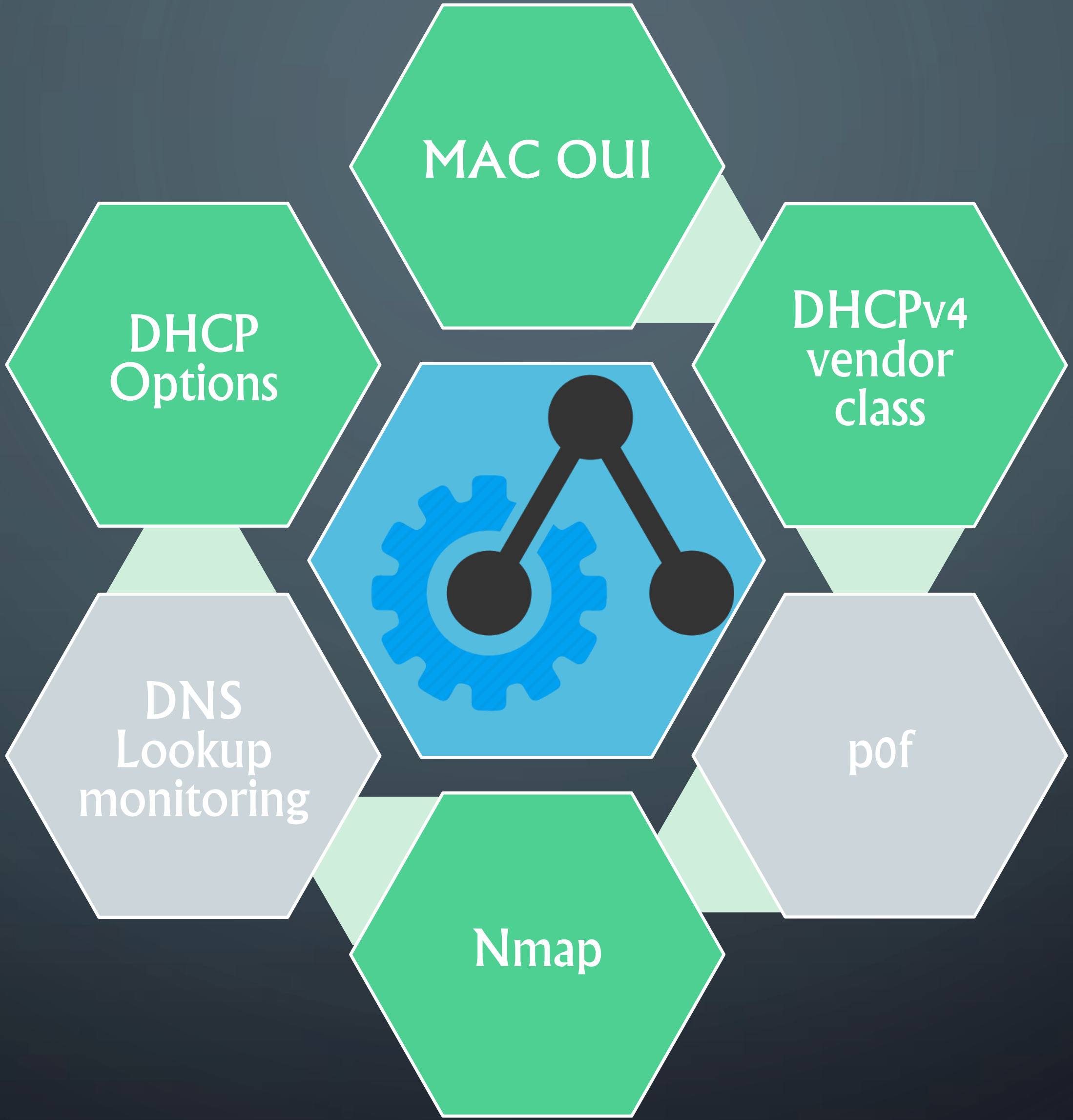
IP : 192.168.1.102
GW : 192.168.1.1
DNS : 192.168.1.1

IP : 192.168.1.105
GW : 192.168.1.1
DNS : 192.168.1.1

IP : 192.168.1.103
GW : 192.168.1.1
DNS : 192.168.1.1

Srujan - Safer Networks For Smart Homes

Identify



MAC OUI

DHCP Options

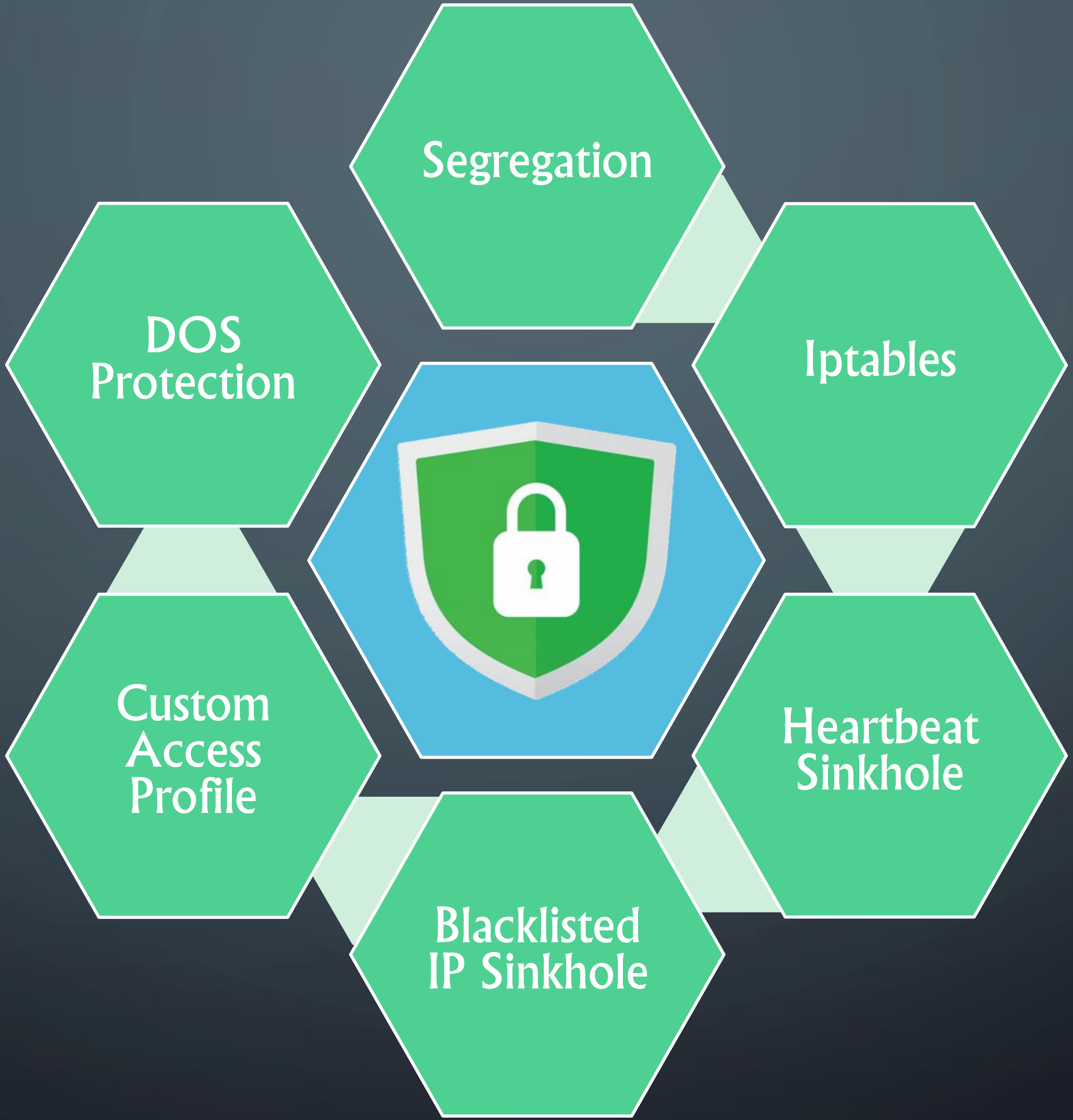
DHCPv4 vendor class

DNS Lookup monitoring

p0f

Nmap

Protect



Segregation

Iptables

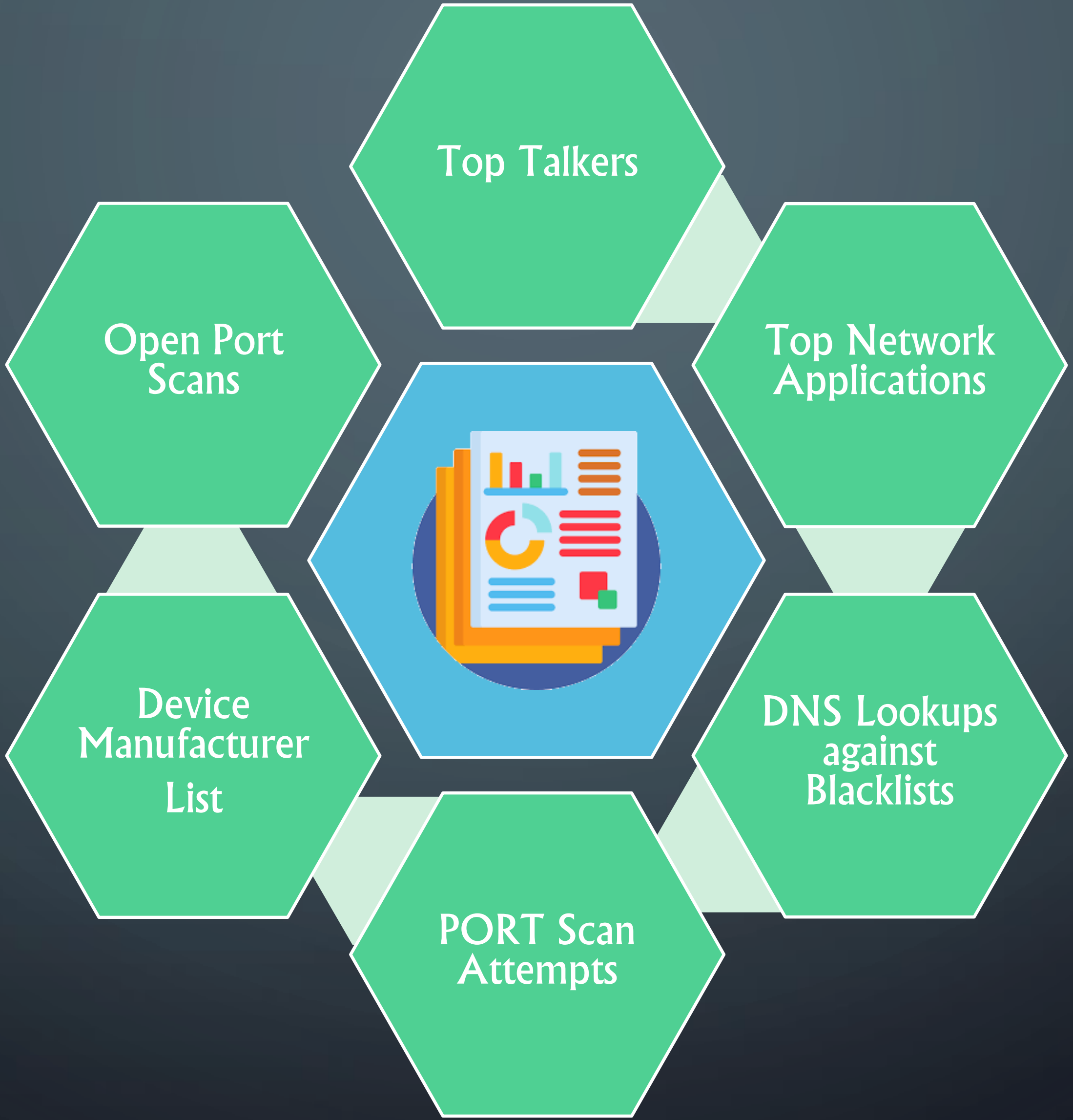
Heartbeat Sinkhole

Blacklisted IP Sinkhole

Custom Access Profile

DOS Protection

Report


Top Talkers
Top Network Applications
DNS Lookups against Blacklists
PORT Scan Attempts
Device Manufacturer List
Open Port Scans

Components

Kibana dashboard displays network usage details and alerts

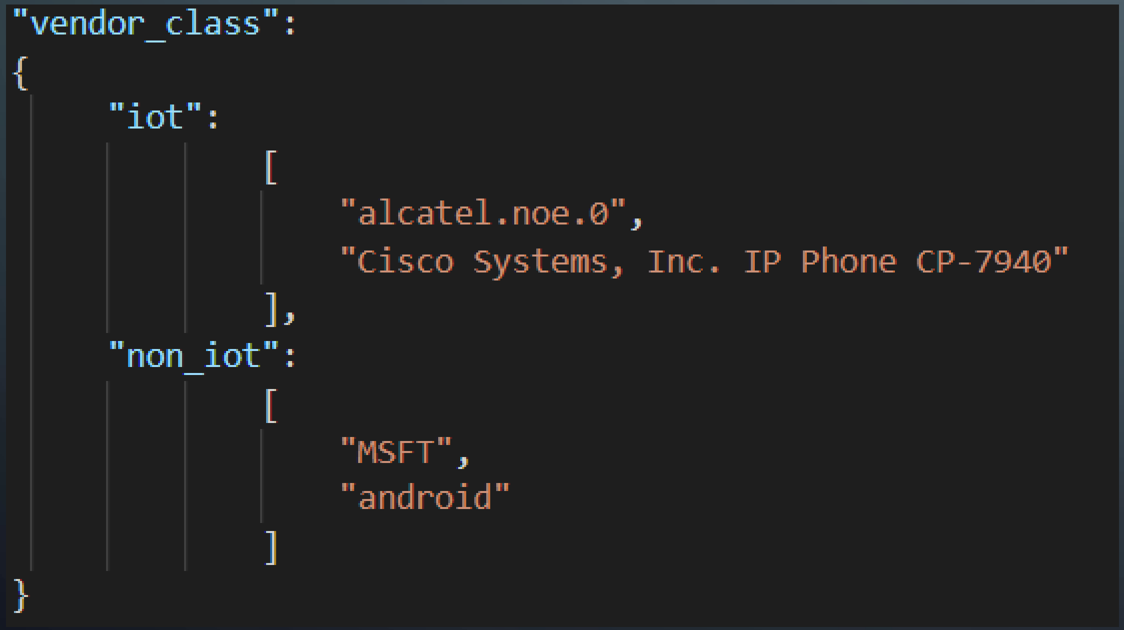
DNS request checked against Google Safe Browsing along with hpHosts, SPAMHAUS to identify connection to malicious domains

NMAP used to port scan each new device for service and OS identification

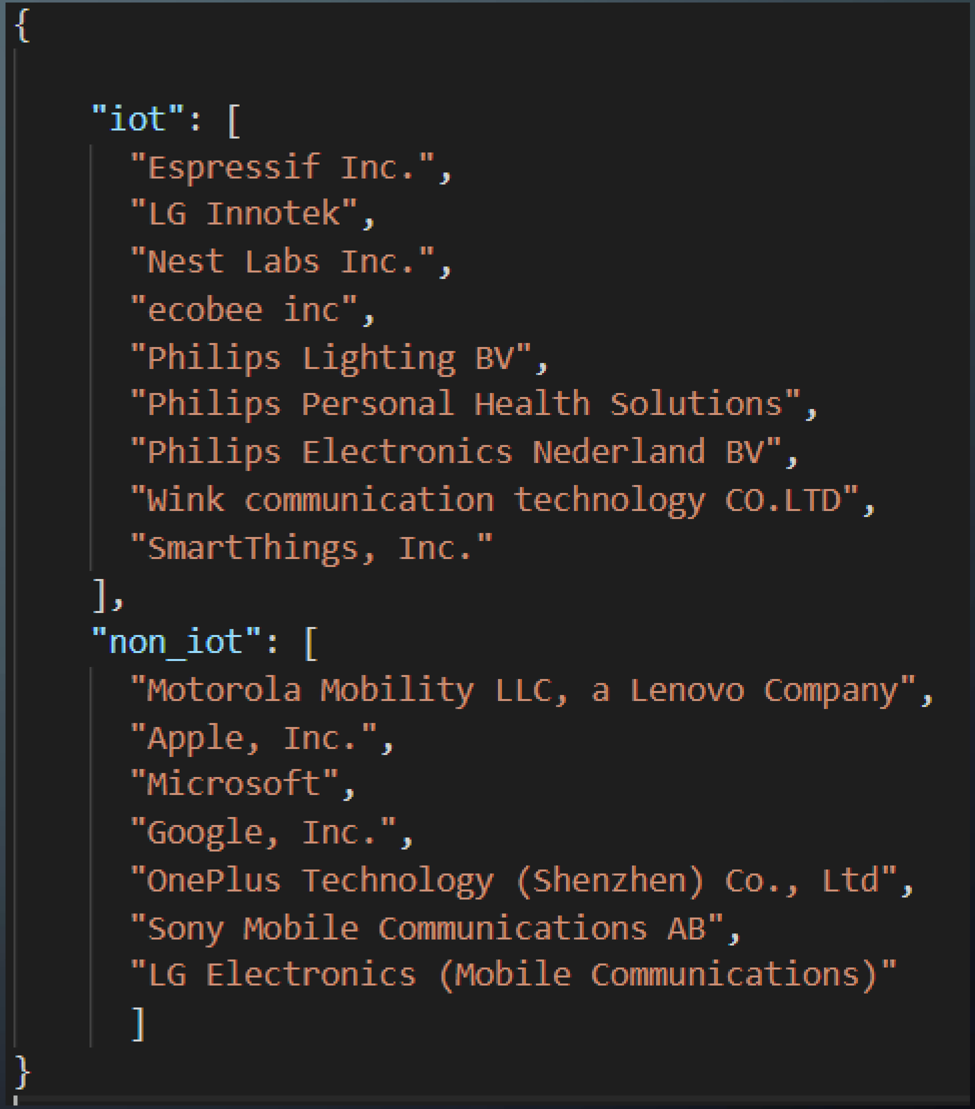
Dnsmasq used for providing DHCP and DNS services

sfw deployed on Raspberry Pi 3 B+

Configuration



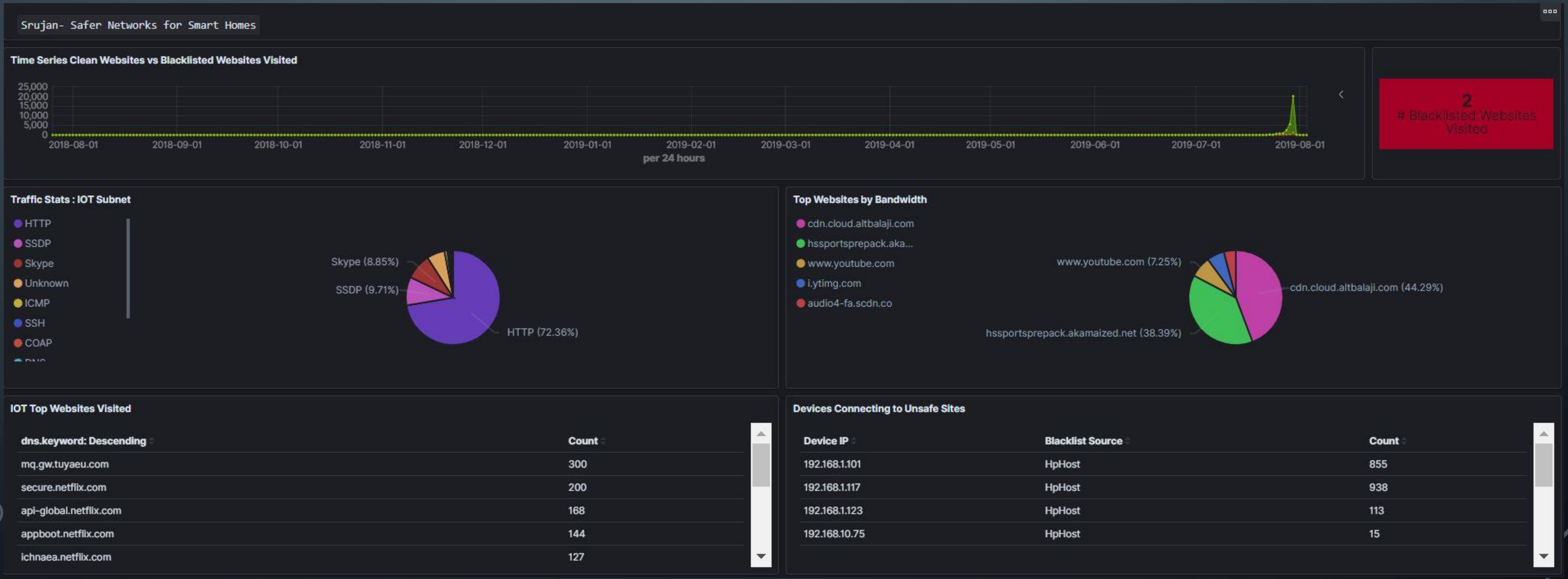
```
"vendor_class":
{
    "iot":
            [
                "alcatel.noe.0",
                "Cisco Systems, Inc. IP Phone CP-7940"
            ],
    "non_iot":
            [
                "MSFT",
                "android"
            ]
}
```



```
{

    "iot": [
      "Espressif Inc.",
      "LG Innotek",
      "Nest Labs Inc.",
      "ecobee inc",
      "Philips Lighting BV",
      "Philips Personal Health Solutions",
      "Philips Electronics Nederland BV",
      "Wink communication technology CO.LTD",
      "SmartThings, Inc."
    ],
    "non_iot": [
      "Motorola Mobility LLC, a Lenovo Company",
      "Apple, Inc.",
      "Microsoft",
      "Google, Inc.",
      "OnePlus Technology (Shenzhen) Co., Ltd",
      "Sony Mobile Communications AB",
      "LG Electronics (Mobile Communications)"
      ]
}
```

Dashboard



Srujan- Safer Networks for Smart Homes

Time Series Clean Websites vs Blacklisted Websites Visited

2
# Blacklisted Websites Visited

Traffic Stats : IOT Subnet

Top Websites by Bandwidth

IOT Top Websites Visited

dns.keyword: Descending	Count
mq.gw.tuyaeu.com	300
secure.netflix.com	200
api-global.netflix.com	168
appboot.netflix.com	144
ichnaea.netflix.com	127

Devices Connecting to Unsafe Sites

Device IP	Blacklist Source	Count
192.168.1.101	HpHost	855
192.168.1.117	HpHost	938
192.168.1.123	HpHost	113
192.168.10.75	HpHost	15

Demo

Future

- Integrate more methods for device identification
- Perform periodic vulnerability scan of devices
- Android app for configuration
- Alert Emails

Thank You!

Any Questions?

sanket.karpe@gmail.com

https://github.com/SanketKarpe/srujan