BehavIoT- Longitudinal Study

Goal of the Project-

- Find out if a device frequently changes its behavior
- Measure any deviations from the expected behavior

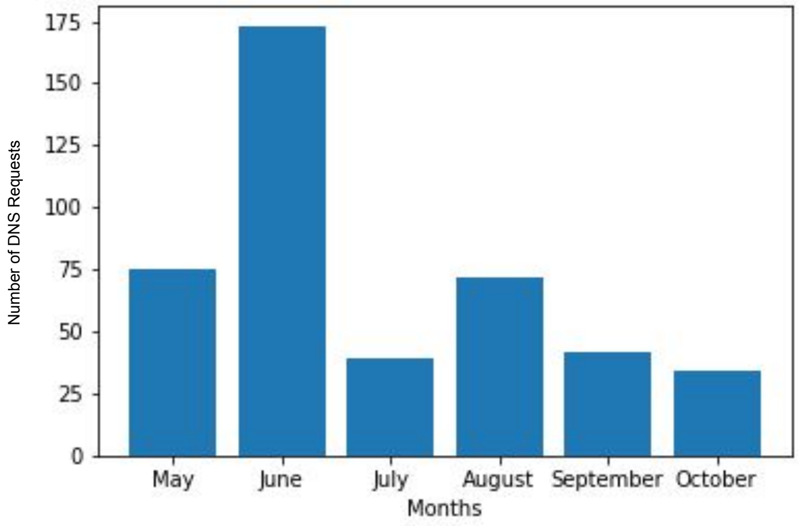
By- Siddhant Sukhatankar and Shubham Bhagwat

Progress of the Project

- Devices analyzed- Brewer, Roku-tv, iKettle, Google home mini, washer, and Tp-Link Bulb.
- Analysis-
    - **Domain Names**, **IP addresses, and TTL**
    - **Protocols**
    - **TLS Destination Names**.

Case Study- iKettle (6 months data)

Analysis of Destination IPs and Domain Names



Number of DNS Requests Vs Months

MONTH	Number of Domains VIsited	Number of Different Distinct Domains Visited
May	3	3
June	3	2
July	3	1
August	3	1
September	3	1
October	4	2

There are mainly 2 types of domain names-

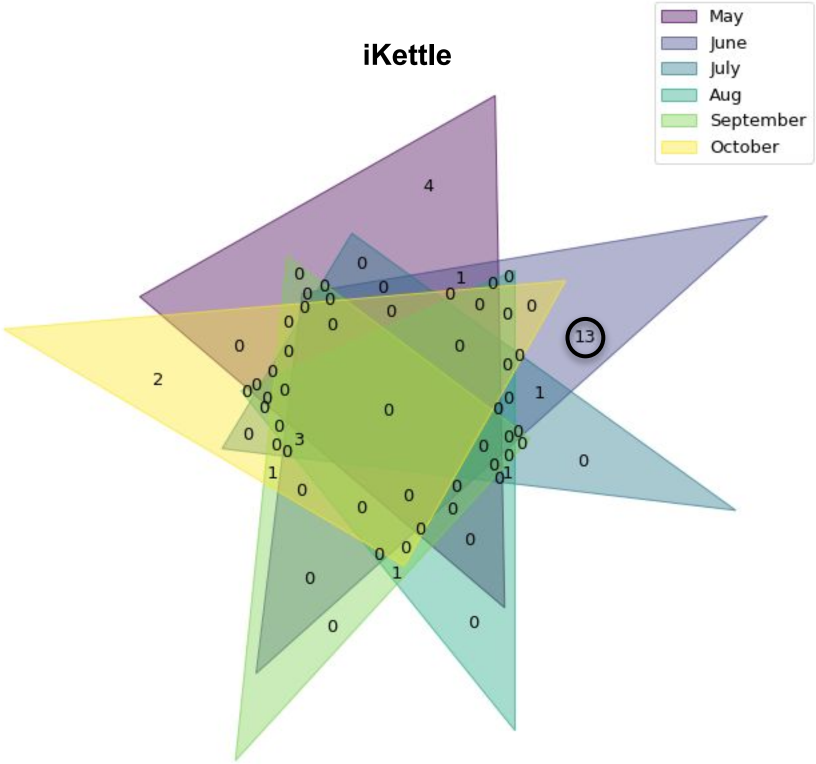
1. Imp-xx-electricimp.com
2. prdxxx.boxen.electricimp.com (This type of domain name remained common for 2 consecutive months)

iKettle: Month-wise distribution of protocols used in packets

	TCP	ARP	TLS	DHCP	EAPOL	UDP	ICMP	DNS	XID
May	415697	122811	719016	18469	4519	0	28	64	28
June	344799	113675	542558	20395	5903	0	6739	8945	1636
July	331406	112270	497736	18018	4702	11	151	527	228
August	584411	136771	1067147	20498	5759	257	5855	7496	1368
September	156713	87325	34339	18548	5896	0	13	38	6312
October	161484	89332	37403	17380	445	3	197	794	105

Based on protocol analysis, it is evident that **August** month shows significant difference.

iKettle: Venn Diagram representation of common IPs between 6 months



iKettle

June 2021 month showed abnormality in number of IPs and Domain Names

iKettle: TLS Destination Counts for 6 months

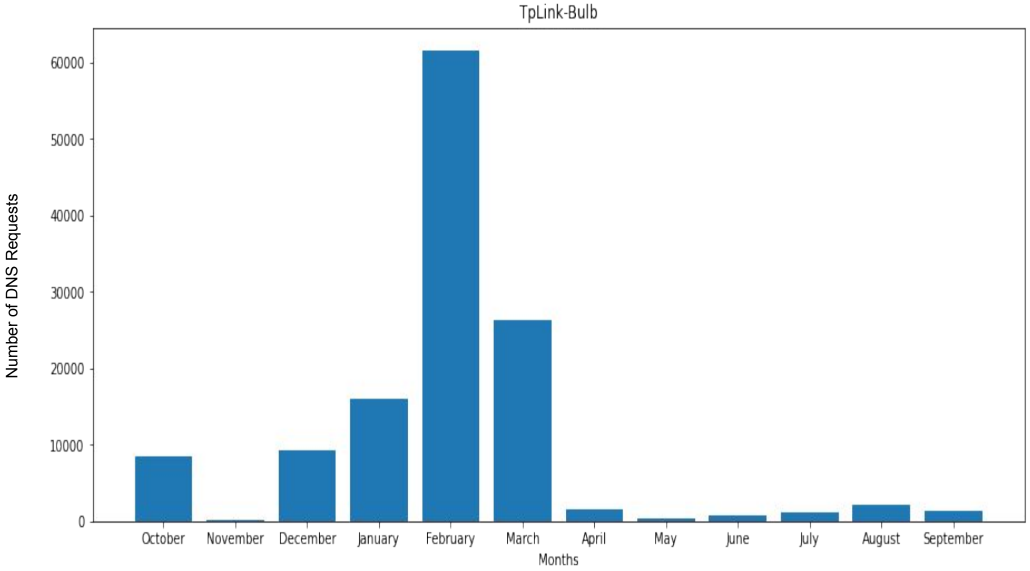
4.215.35.111	2
34.223.189.42	3
34.218.148.111	1
35.85.16.171	1
35.81.248.51	2
44.224.225.197	4
44.234.143.223	2
44.232.230.122	2

52.36.254.224	1
52.34.103.133	1
52.42.162.184	1
52.36.151.253	2
54.214.162.174	5
192.168.10.195	5
192.168.10.144	1
192.168.10.215	2

Case Study- TpLink Bulb (12 months data)

Analysis of Destination IPs and DNS Requests

Month	Number of Domain Names Visited	Number of Different Distinct Domain Names Visited
October	1	1
November	1	0
December	1	0
January	5	4
February	5	0
March	5	0
April	5	0
May	5	0
June	2	0
July	2	0
August	2	0
September	5	0

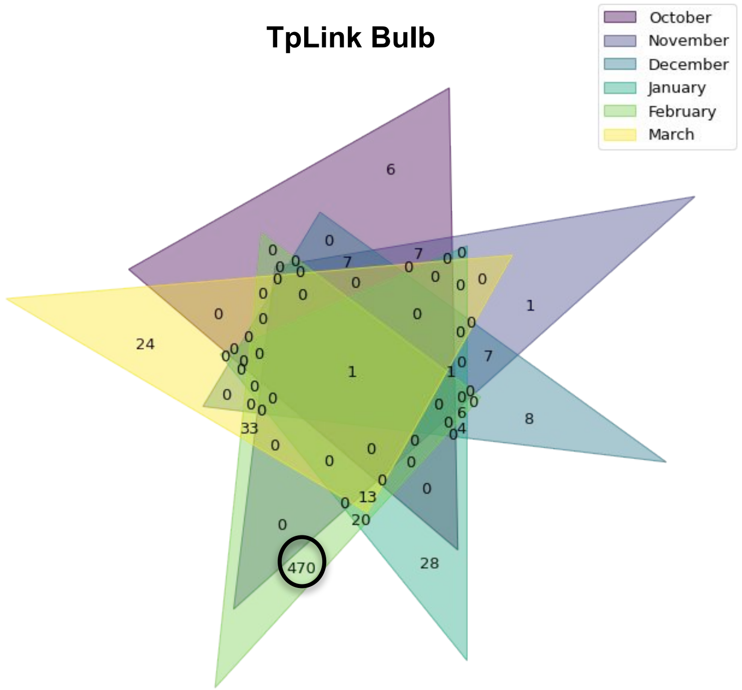


Number of DNS Requests Vs Months

There is one domain name common for all the months and was visited the most number of times,

'devs.tplinkcloud.com'

TpLink Bulb: Venn Diagram representation of common IPs between 6 months

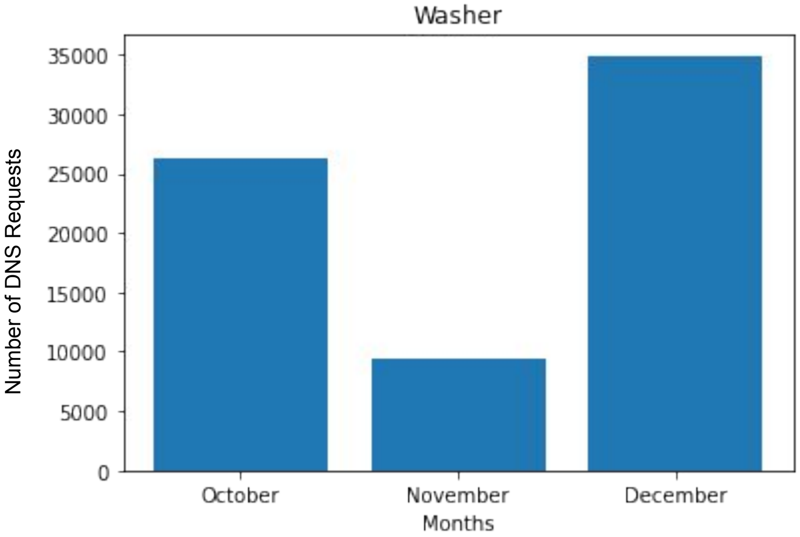


February 2021 month showed abnormality in number of IPs and Domain Names

Case Study- Washer (3 months data)

Analysis of Destination IPs and Domain Names

Month	Number of Domain Names Visited	Number of Different Distinct Domain Names Visited
October	54	54
November	16	15
December	43	11

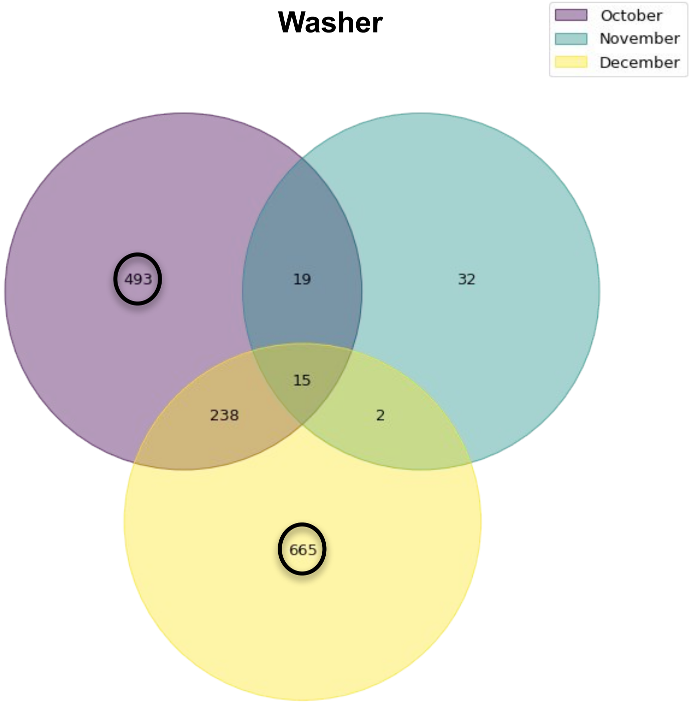


Number of DNS Requests Vs Months

There is one domain name common for all the months and was visited the most number of times,

‘www.googleapis.com’

Washer: Venn Diagram representation of common IPs between 6 months



Overall behavior of Washer is different and needs to be analyzed more.

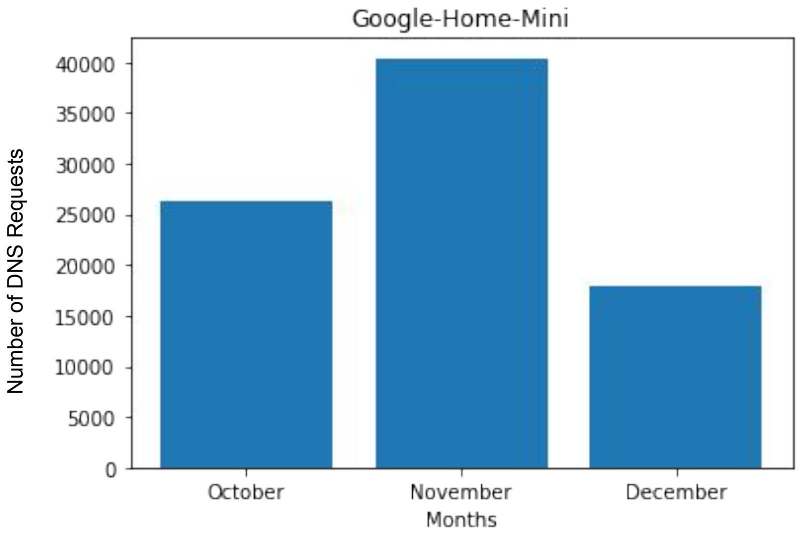
Case Study- Google Home Mini (3 months data)

Analysis of Destination IPs and Domain Names

Month	Number of Domain Names Visited	Number of Different Distinct Domain Names Visited
October	54	54
November	31	0
December	16	16

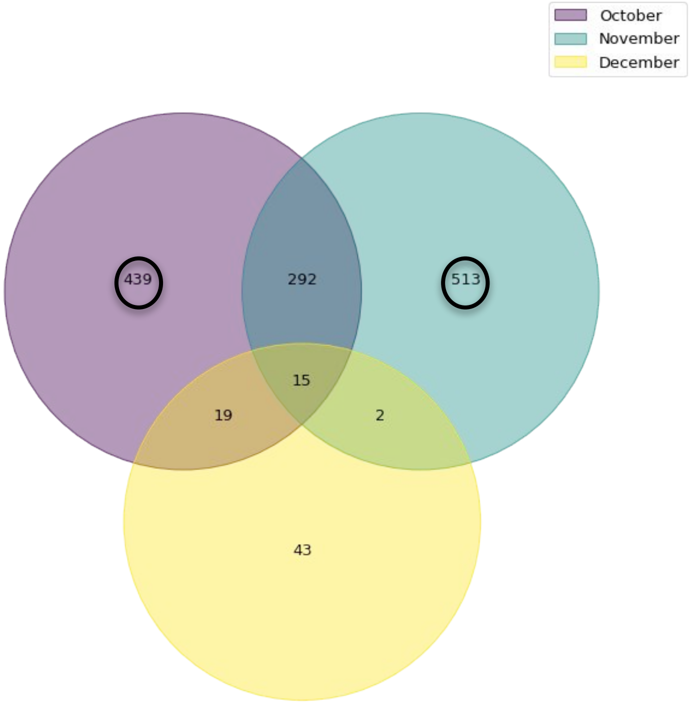
There is one domain name common for all the months and was visited the most number of times,

‘home-devices.googleapis.com’



Number of DNS Requests Vs Months

Google Home Mini: Venn Diagram representation of common IPs between 6 months



Overall behavior of Google Home Mini is different and needs to be analyzed more.

Conclusion

- Found some evidences of abnormality
- Need further filtering of destination IPs as first party, second party or third party.
- Need in-depth analysis for devices like Washer and Google Home Mini (lots of data).

- Future Scope- Further investigation of whether there is any suspicious activity, so that such activity can be blocked.