2020.07.26 WISA2020

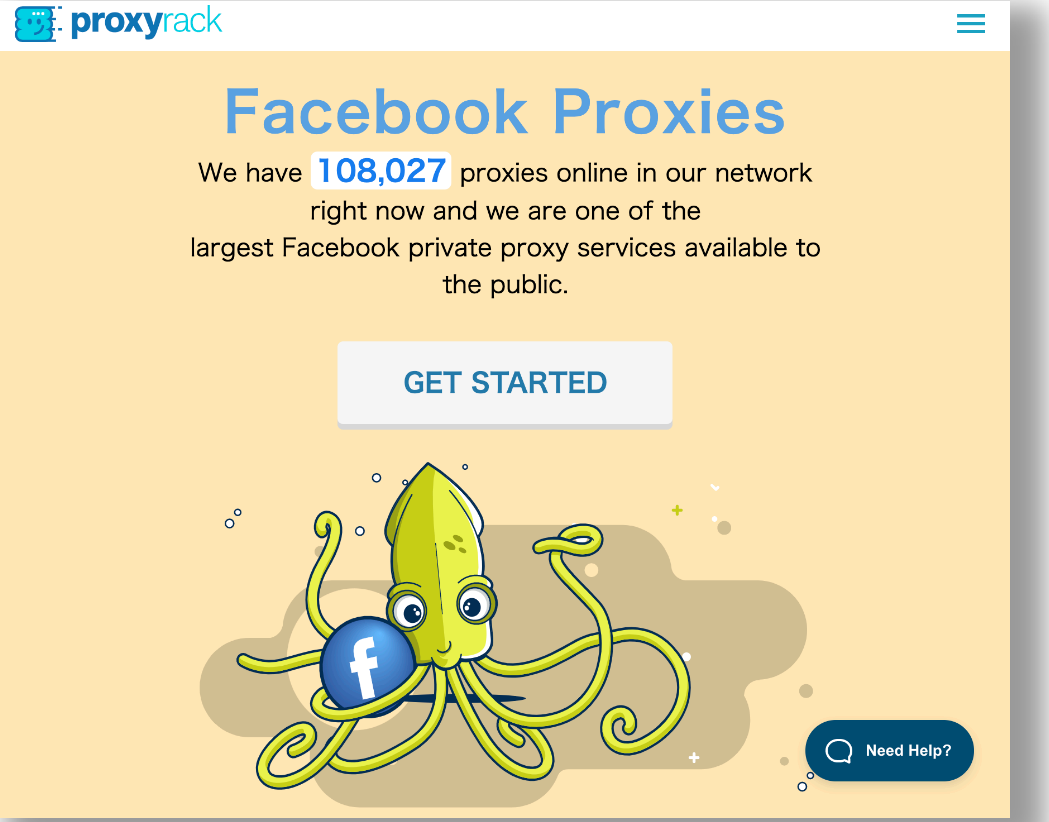
Analysis on Malicious Residential Hosts Activities Exploited by Residential IP Proxy Services

AKIHIRO HANZAWA, HIROAKI KIKUCHI

MEIJI UNIVERSITY

Background: Residential IP Proxies

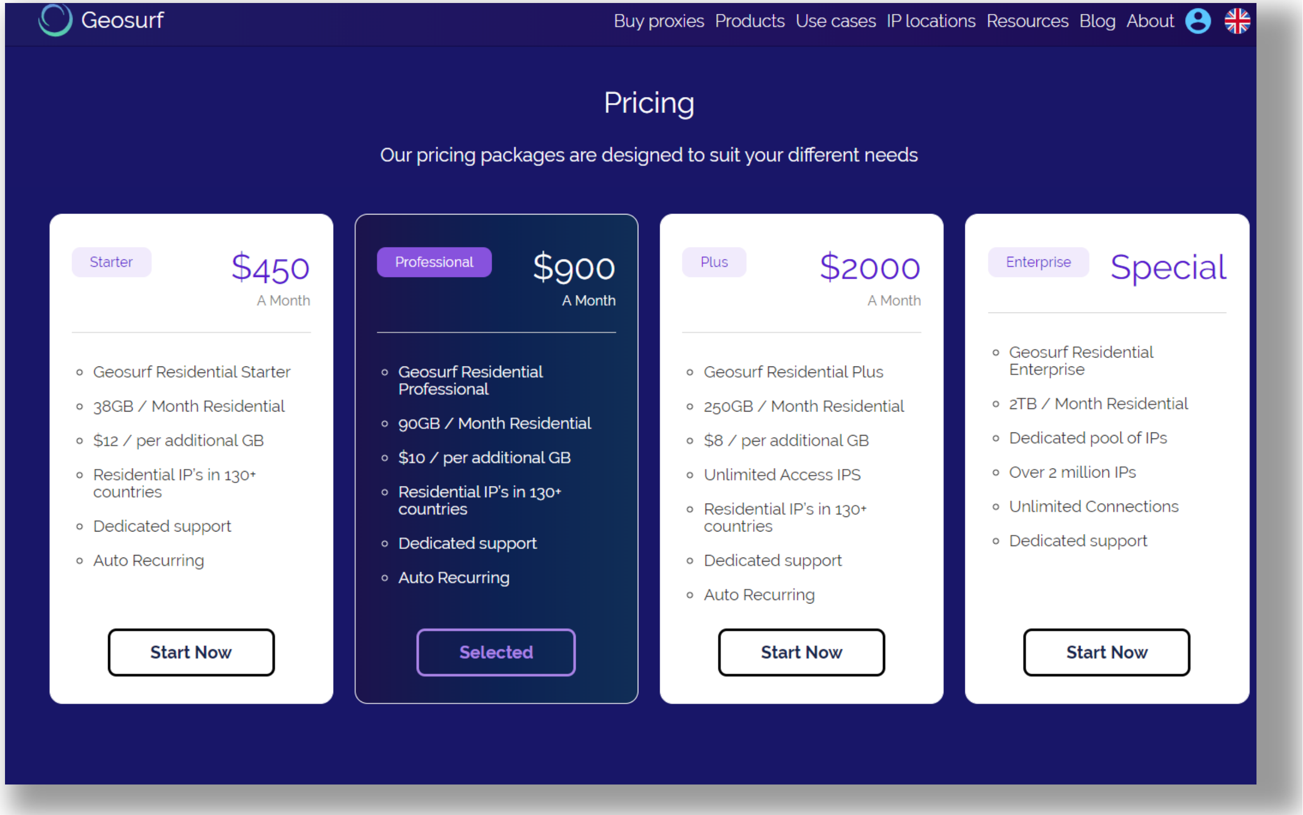
ProxyRack



Facebook Proxies

We have 108,027 proxies online in our network right now and we are one of the largest Facebook private proxy services available to the public.

Geosurf



Pricing

Our pricing packages are designed to suit your different needs

Starter — $450 A Month

- Geosurf Residential Starter
- 38GB / Month Residential
- $12 / per additional GB
- Residential IP's in 130+ countries
- Dedicated support
- Auto Recurring

Professional — $900 A Month

- Geosurf Residential Professional
- 90GB / Month Residential
- $10 / per additional GB
- Residential IP's in 130+ countries
- Dedicated support
- Auto Recurring

Plus — $2000 A Month

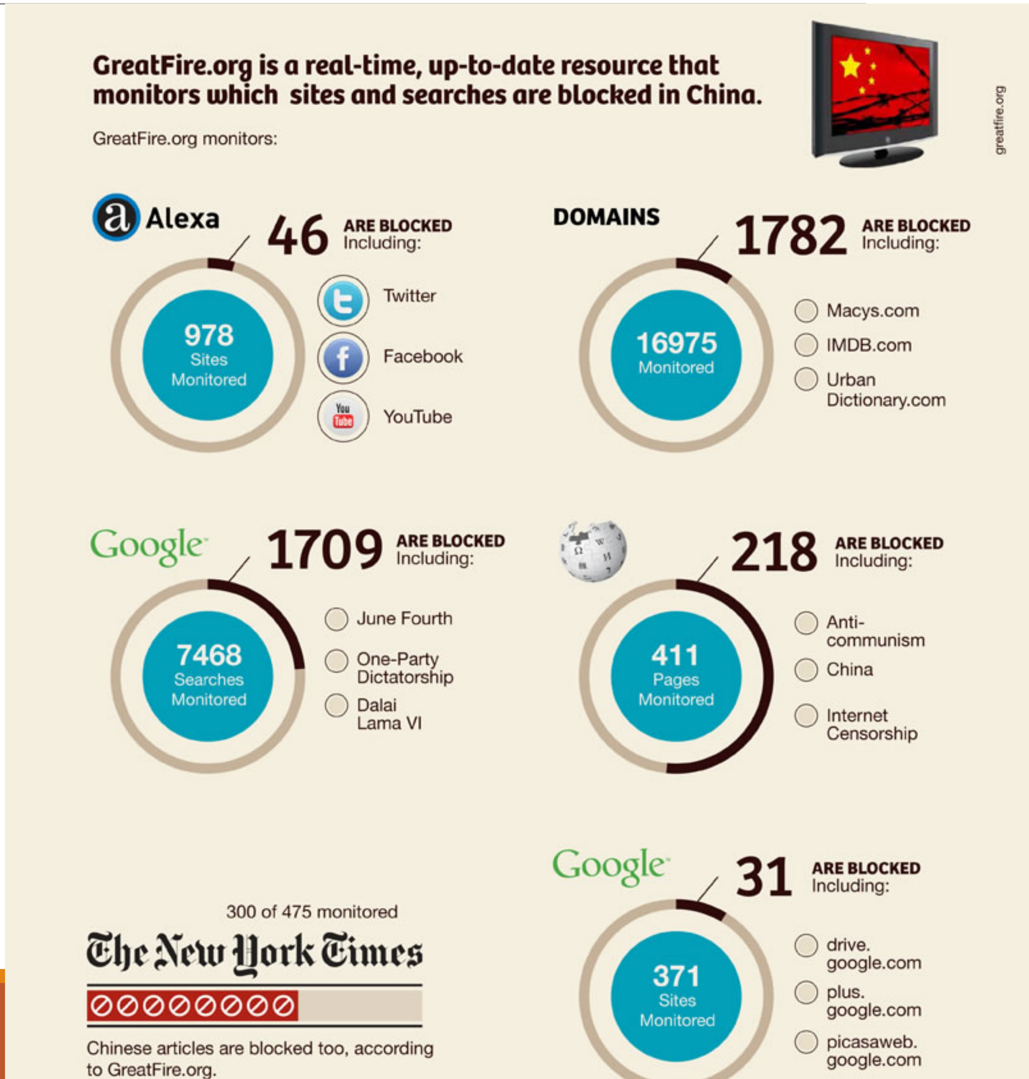
- Geosurf Residential Plus
- 250GB / Month Residential
- $8 / per additional GB
- Unlimited Access IPS
- Residential IP's in 130+ countries
- Dedicated support
- Auto Recurring

Enterprise — Special

- Geosurf Residential Enterprise
- 2TB / Month Residential
- Dedicated pool of IPs
- Over 2 million IPs
- Unlimited Connections
- Dedicated support

Why is the RESIP proxy used?

- Network Censorship, operated by government, aims to prevent citizens from being evil cultures.
  - Political sites
  - Religious sites
  - Pornography

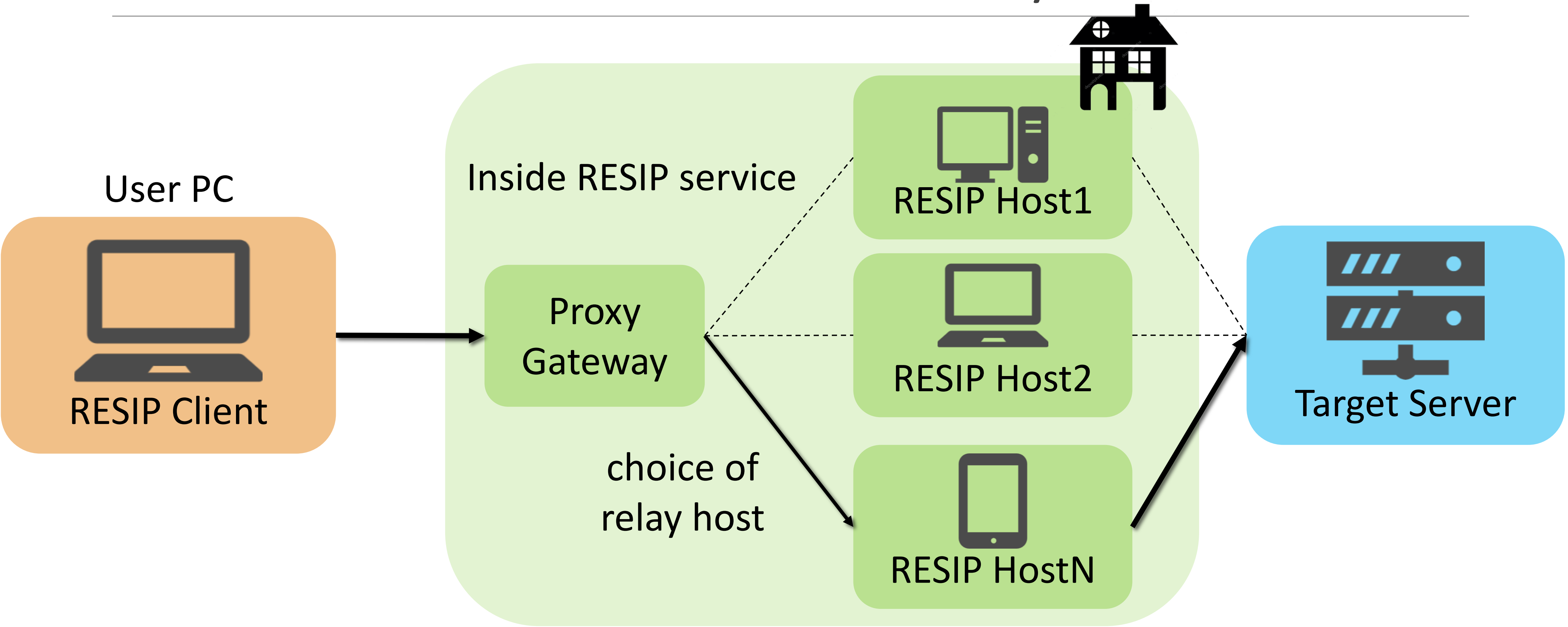


GreatFire.org is a real-time, up-to-date resource that monitors which sites and searches are blocked in China.

GreatFire.org monitors:

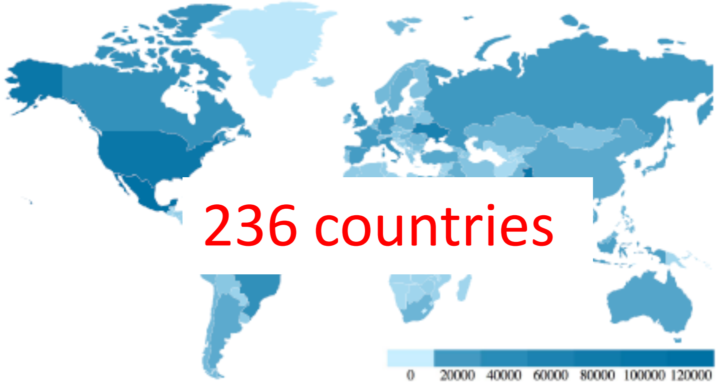
Chinese articles are blocked too, according to GreatFire.org.

What is a Residential IP Proxy ?



The Dark Services

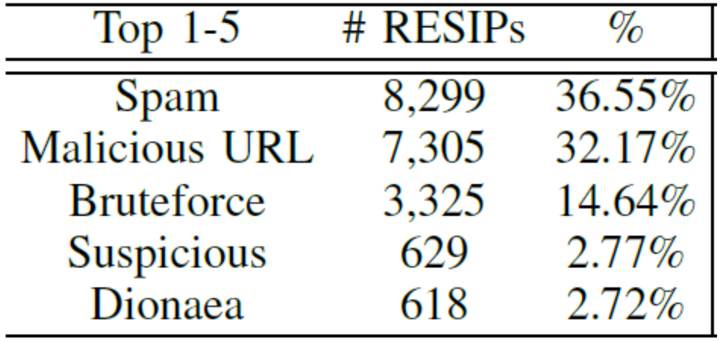
- Mi et al. [1] found that IP addresses provided by RESIP services were tend to be part of illicit activities



236 countries

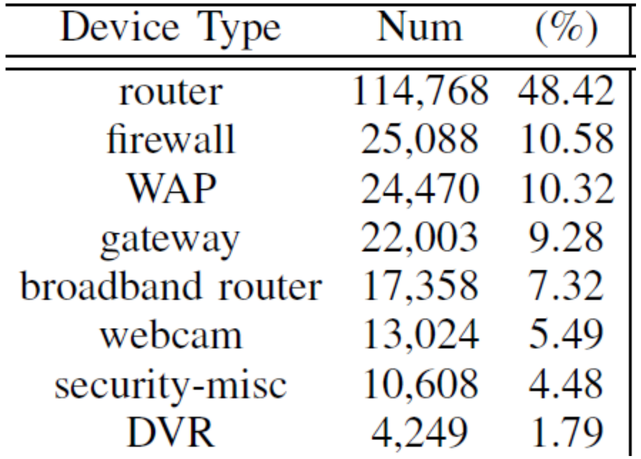
(b) RESIPs responded to our probings.

Malicious



Top 1-5	# RESIPs	%
Spam	8,299	36.55%
Malicious URL	7,305	32.17%
Bruteforce	3,325	14.64%
Suspicious	629	2.77%
Dionaea	618	2.72%

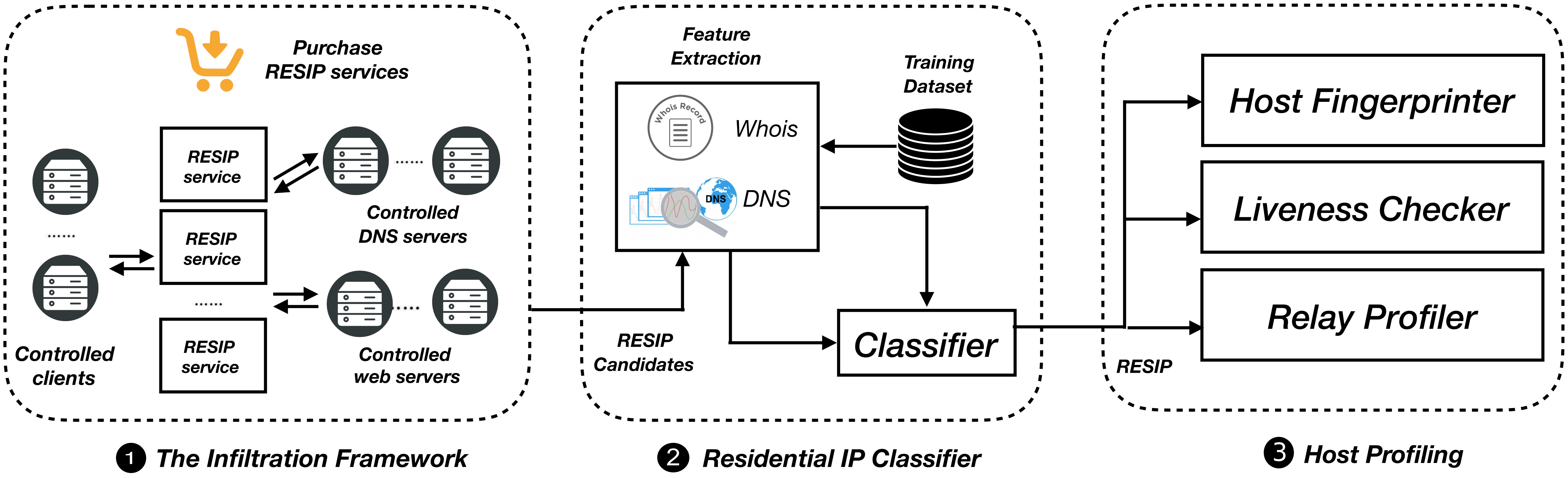
IoT devices



Device Type	Num	(%)
router	114,768	48.42
firewall	25,088	10.58
WAP	24,470	10.32
gateway	22,003	9.28
broadband router	17,358	7.32
webcam	13,024	5.49
security-misc	10,608	4.48
DVR	4,249	1.79

[1] Xianghang Mi, et. Al, "Residential Evil: Understanding Residential IP Proxy as a Dark Service", IEEE S+P 2019.

Mi’s Methodology [1]



Trend of RESIP services

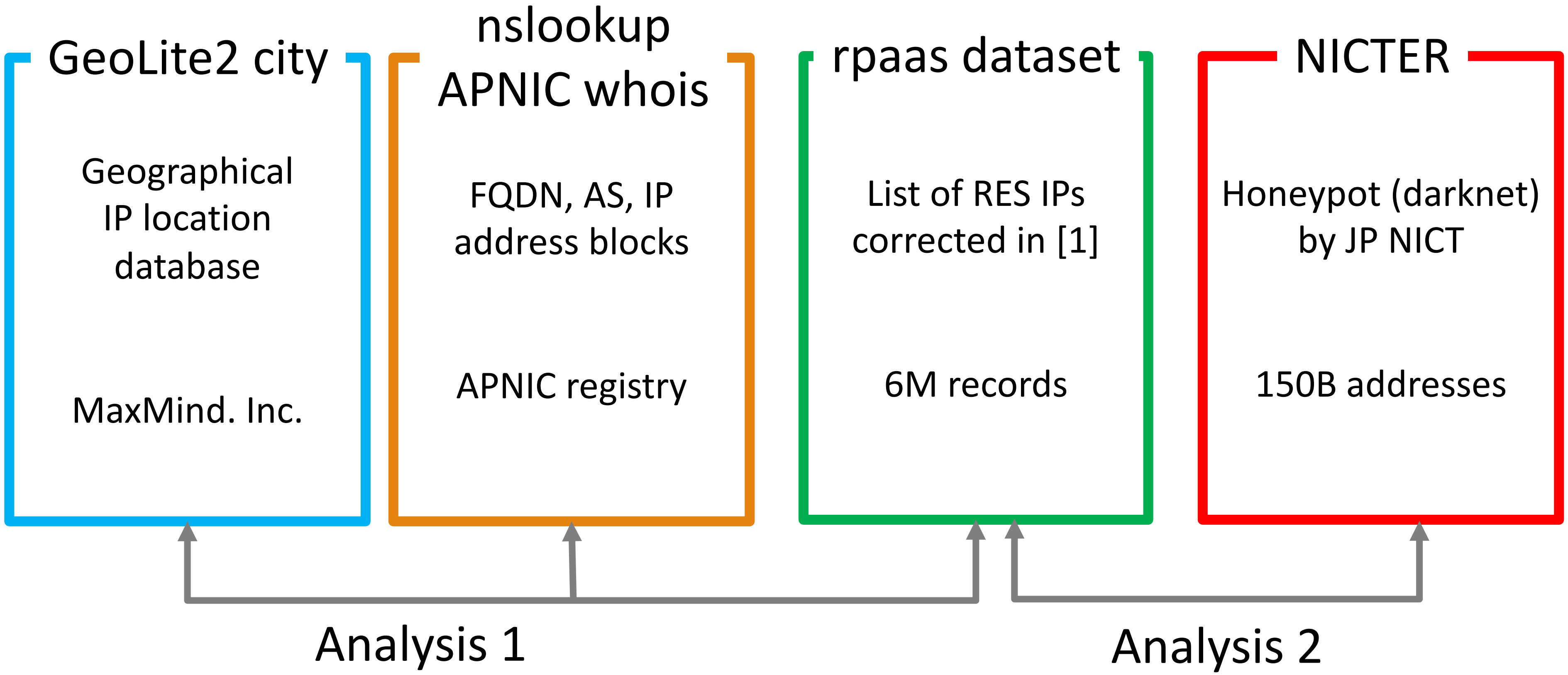
- Basic RESIP service fees in 2017 and 2019

RESIP Provider	2017 [1]	2019
Proxies Online (US)	$25/Gb	(expired)
Geosurf (NL)	$300/month	$450-2000/month
ProxyRack (US)	$40/month	$60-120/month
Luminati (US)	$500/month	$12.5/GB+$500/month
IAPS Security (US)	$500/month	(unavailable)

Questions

- Q1. Where are they?
  - What kinds of networks do RESIPs belong to?
  - How are RESIPs distributed geometrically in Japan?
- Q2. Who are they?
  - What is the major RESIP devices?
- Q3. Why do they do?
  - For what purpose are the RESIPs abused?

Our Resources



GeoLite2 city

Geographical IP location database

MaxMind. Inc.

nslookup APNIC whois

FQDN, AS, IP address blocks

APNIC registry

rpaas dataset

List of RES IPs corrected in [1]

6M records

NICTER

Honeypot (darknet) by JP NICT

150B addresses

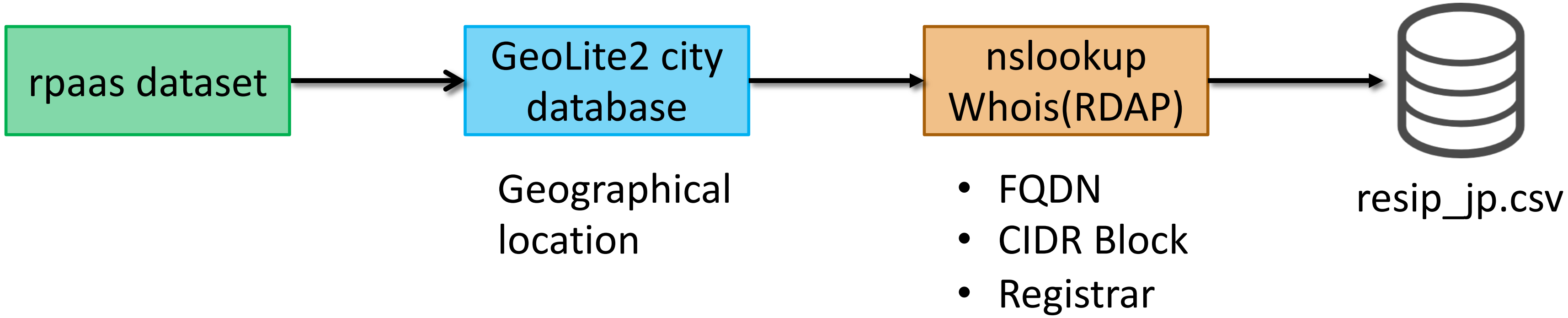
Analysis 1

Analysis 2

Analysis 1: Examine Hosts in Japan

- Purpose

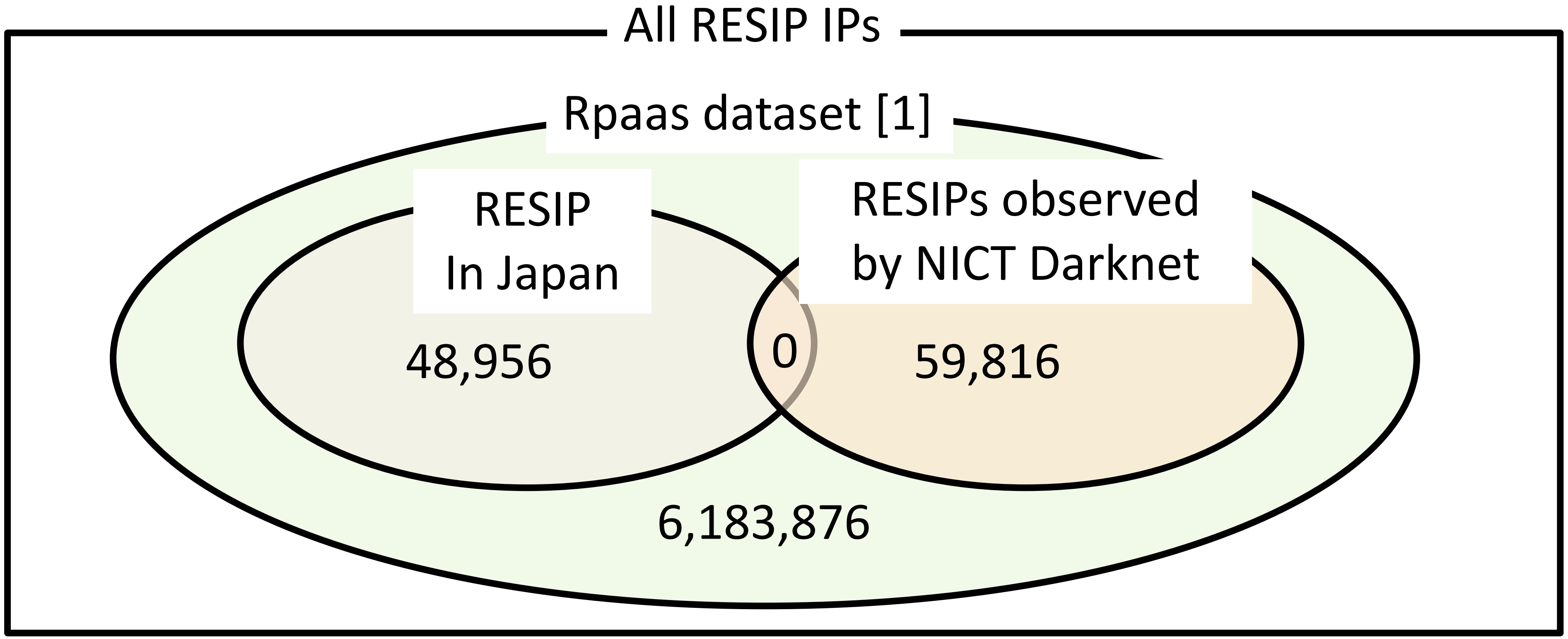
Find geographical location, domains, and ISPs of RESIP hosts.



Geographical location

- FQDN
- CIDR Block
- Registrar

Analysis Results



All RESIP IPs

Rpaas dataset [1]

RESIP In Japan

RESIPs observed by NICT Darknet

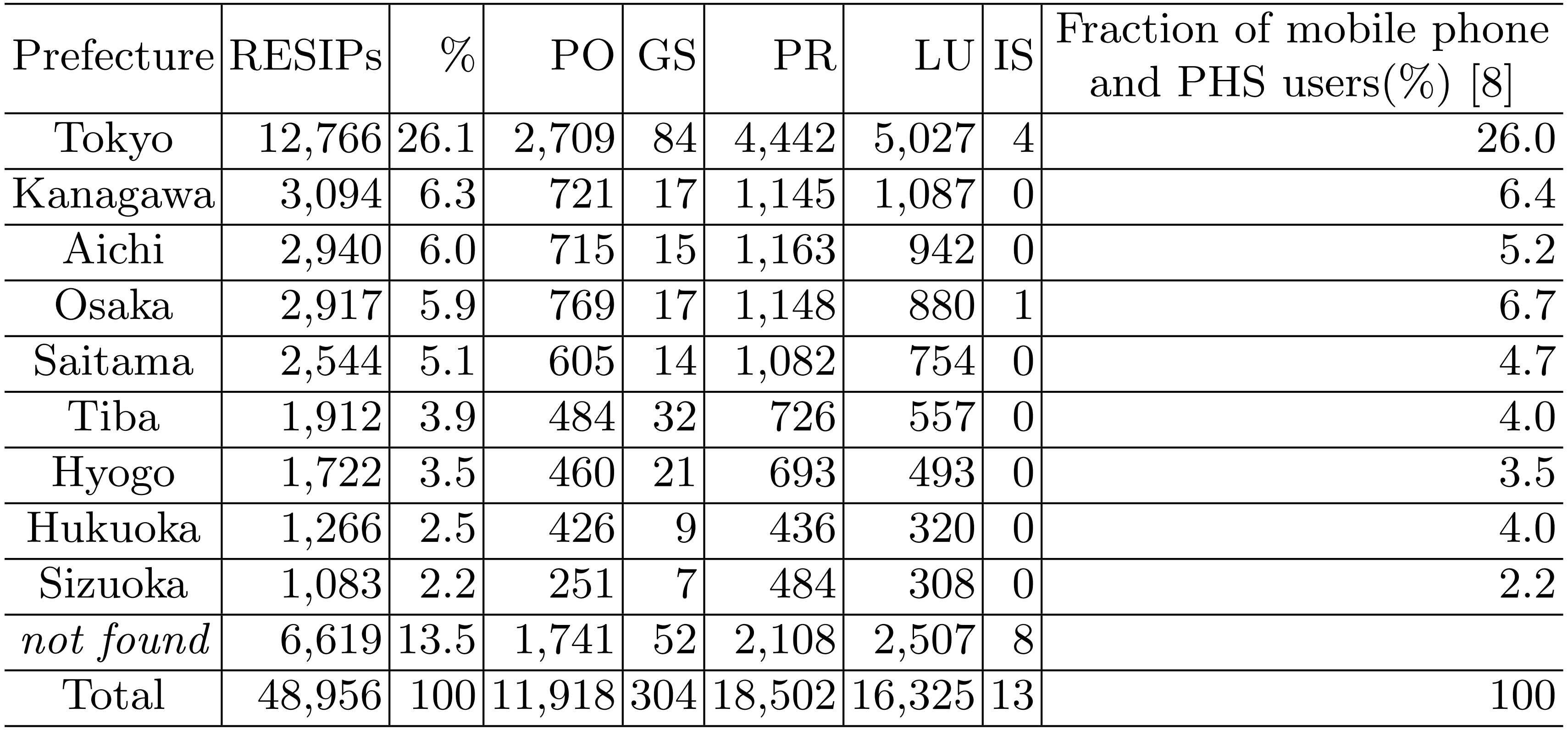
48,956

0

59,816

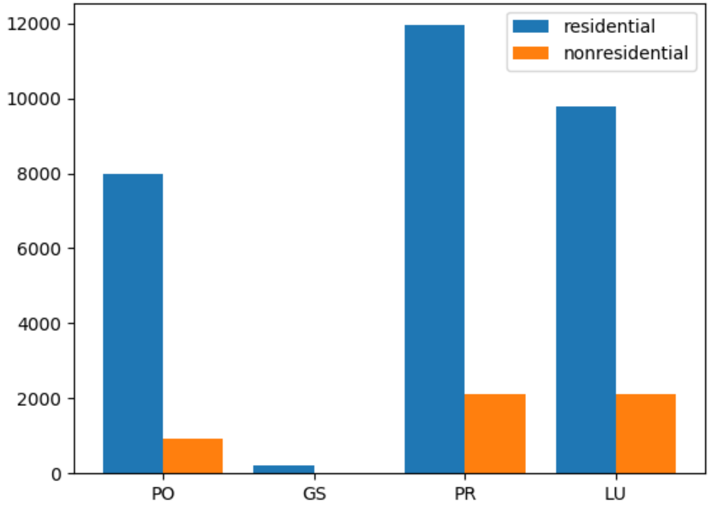
6,183,876

Result 1.1: Top 10 Cities in Japan



Prefecture	RESIPs	%	PO	GS	PR	LU	IS	Fraction of mobile phone and PHS users(%) [8]	Population
Tokyo	12,766	26.1	2,709	84	4,442	5,027	4	26.0	1
Kanagawa	3,094	6.3	721	17	1,145	1,087	0	6.4	2
Aichi	2,940	6.0	715	15	1,163	942	0	5.2	4
Osaka	2,917	5.9	769	17	1,148	880	1	6.7	3
Saitama	2,544	5.1	605	14	1,082	754	0	4.7	5
Tiba	1,912	3.9	484	32	726	557	0	4.0	6
Hyogo	1,722	3.5	460	21	693	493	0	3.5	
Hukuoka	1,266	2.5	426	9	436	320	0	4.0	
Sizuoka	1,083	2.2	251	7	484	308	0	2.2	
not found	6,619	13.5	1,741	52	2,108	2,507	8		
Total	48,956	100	11,918	304	18,502	16,325	13	100	

Result 1.2: Domains



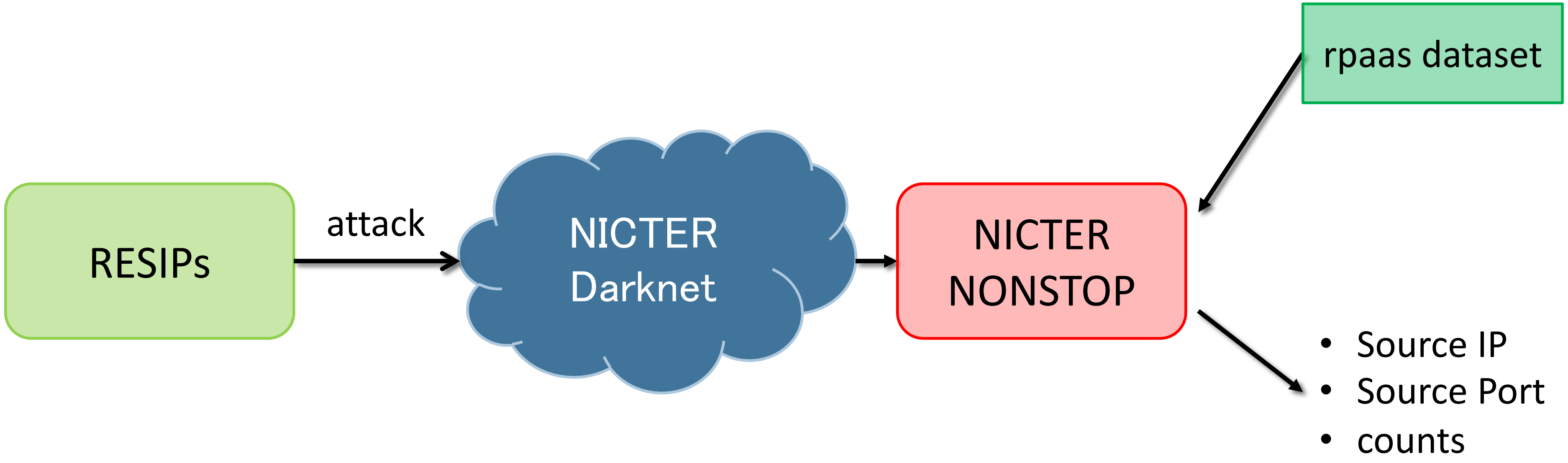
2LD	# Ips	%
ne	28824	74.0%
or	4340	11.1%
ad	2208	5.6%
ac	91	0.2%
co	9	
go	1	
total	38946	

90.8% personal (residential)

133.26.240.58	2017/10/20	Luminati	ocha-mobile58-240.mind.meiji.ac.jp
133.11.114.249	2017/11/1	Luminati	g.h.u-Tokyo.ac.jp
133.70.80.19	2017/11/6	proxies	Gw19.shizuoka.ac.jp

Domains dedicated for mobile

Analysis 2: NICTER Darknet



RESIPs

attack

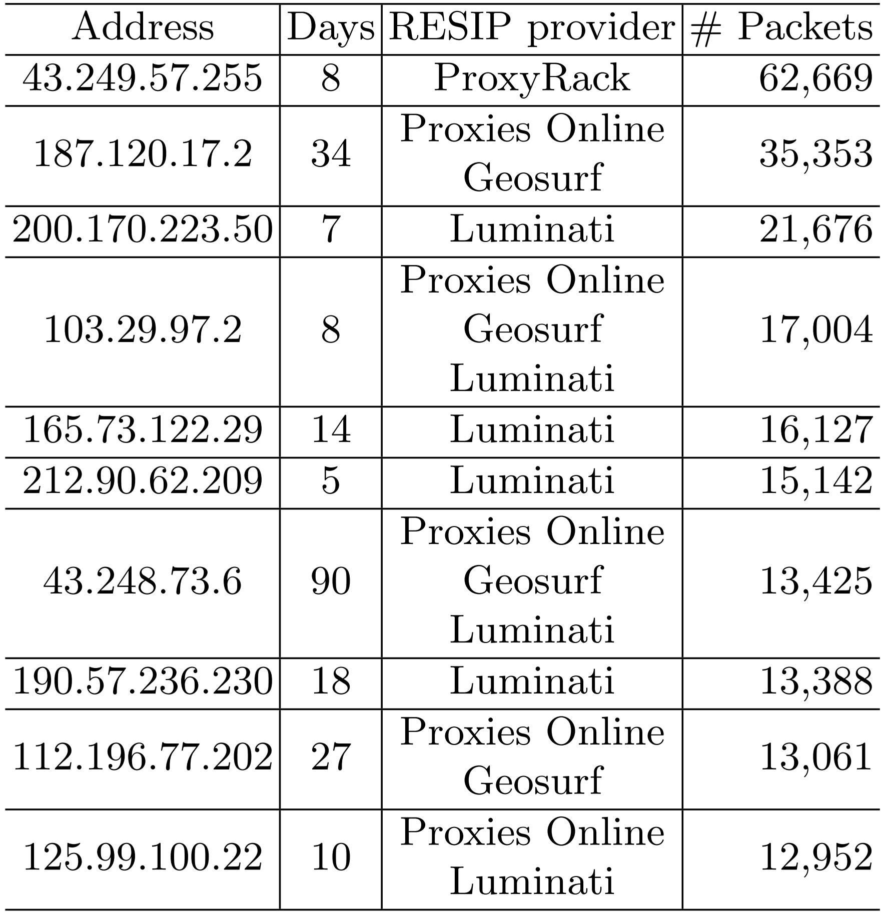
NICTER Darknet

NICTER NONSTOP

rpaas dataset

- Source IP
- Source Port
- counts

Result 2.1: Top 10 *Busy* RESIPs



Address	Days	RESIP provider	# Packets
43.249.57.255	8	ProxyRack	62,669
187.120.17.2	34	Proxies Online Geosurf	35,353
200.170.223.50	7	Luminati	21,676
103.29.97.2	8	Proxies Online Geosurf Luminati	17,004
165.73.122.29	14	Luminati	16,127
212.90.62.209	5	Luminati	15,142
43.248.73.6	90	Proxies Online Geosurf Luminati	13,425
190.57.236.230	18	Luminati	13,388
112.196.77.202	27	Proxies Online Geosurf	13,061
125.99.100.22	10	Proxies Online Luminati	12,952

← Intensive --- 62,669 pkt for 8 days

← extensive --- 13,425 pkt for 3 month

Result 2.2: Top 10 malicious services

Dest. Port	service	Freq.	%
23	Telnet	613,606	36.4
445	SMB	399,250	23.7
21	FTP	193,917	11.5
1433	MSSQL	144,928	8.6
80	HTTP	97,780	5.8
22	SSH	49,767	2.9
2323	(Telnet)	43,310	2.5
25	SMTP	21,732	1.3
2222	(SSH)	16,838	1.0
3389	RDP	9,782	0.5

Port-scanning

SPAM

Summaries

Questions	Our finding 2019, in Japan	Mi [1] 2017
Q1. Where are they	90.8% RESIP are residential (ne, ad, or) RESIPs were distributed widely in all 47 prefectures in Japan.	95.22% residential. 238 countries, 28,035 networks, 52,905 ISPs.
Q2. Who are they?	Mobile IPs and laptop PCs in Japan	IoT devices (237,029) routers, FWs, WAP
Q3. Why do they do?	1. Port-scanning 2. SPAM 1.3 % from world to Japan	SPAM 36.5%

Conclusions

- We have studied RESIP host activities in Japan (0.79%).
- We found that 908 % RESIP were residential and were distributed all around of Japan (47 Prefectures).
- New finding is that the most of devices in Japan were mobile laptop PCs, whereas router, firewalls and WAP devices were majors according to Mi’s report [1]. One more finding is that SPAM (36.5% in [1]) accounted for only 1.3% in 2019, Japan.
- We conclude that more RESIP hosts are still involved in malicious activities and we need countermeasure against the abuse of RESIPs.