IPブラックリストを用いたResidential IP Proxyホスト検知手法の提案

総合数理学部 先端メディアサイエンス学科

菊池研究室4年 北原拓海

背景

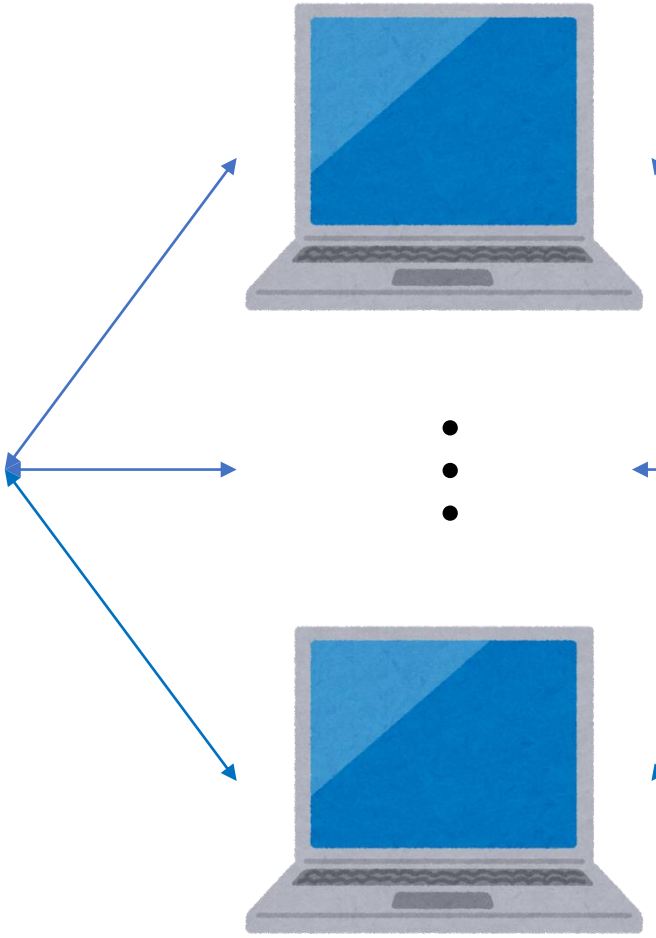
- Residential IP Proxy(RESIP)の利用が盛んに

- **誰かが勝手に自分の家のネットワークを使っているかも？**

→検知したい！

RESIP

プロキシ
ゲートウェイ



RESIP
クライアント

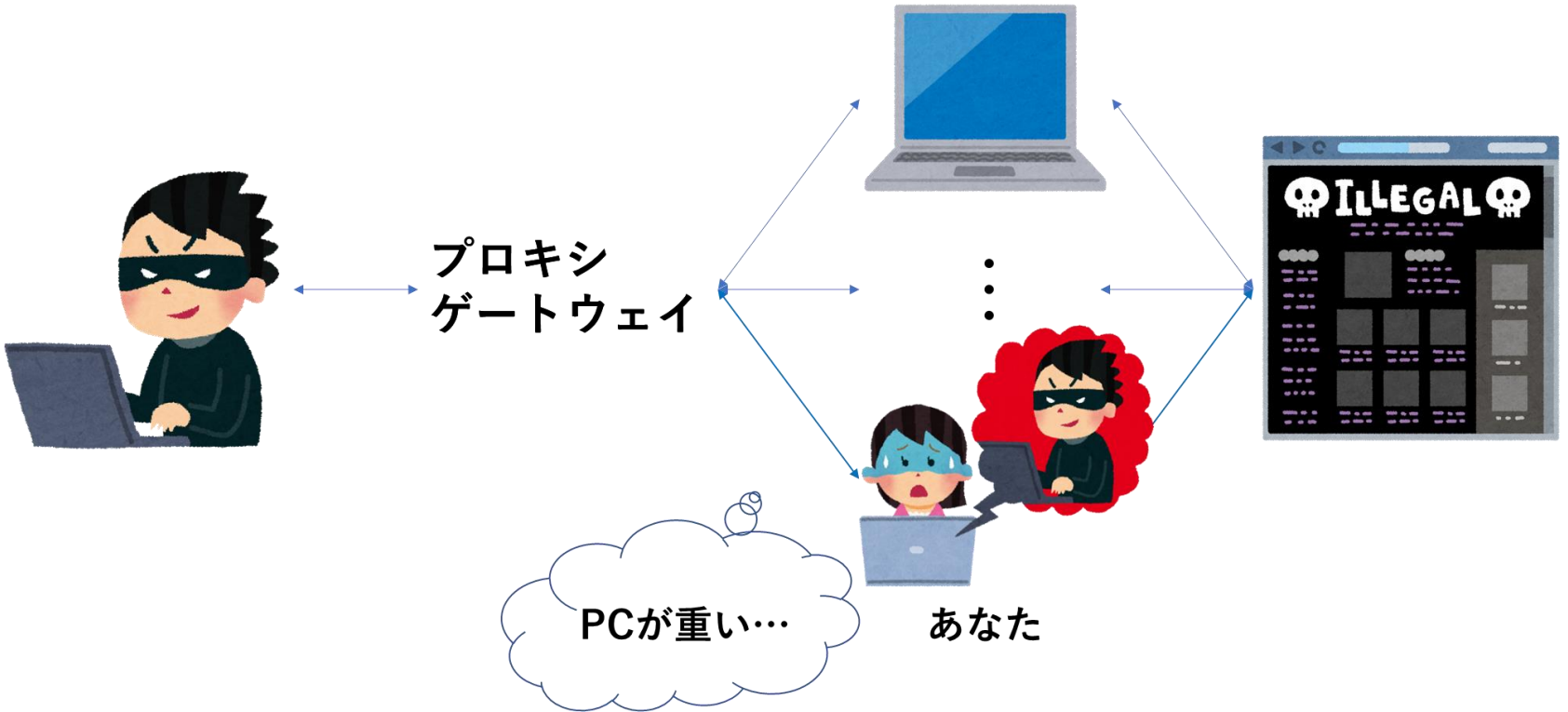
RESIP事業者

RESIPホスト

ターゲット
ウェブサイト

研究目的

- RESIPアプリの通信先の調査
- 新しいRESIP検知手法の提案



先行研究

- RESIPホストの調査[1][2]
- パケットの流れやDNSに着目したRESIP検知プログラム[3]

[1] 半澤 映拓, 菊池 浩明, Residential IP Proxy サービスに悪用される住宅用ホストの調査,CSS2019, pp.918-925,2019.
[2] Xianghang Mi, et al., “Resident Evil: Understanding Residential IP Proxy as a Dark Service”,2019 IEEE Symposium on Security and Privacy,2019,pp. 1185- 1201.
[3] Altug Tosun, et al., “RESIP Host Detection: Identi-fication of Malicious Residential IP Proxy Flows”, 2021 IEEE International Conference on Consumer Electronics, 2021.

検知プログラム　[3]Tosunらの手法

- 3つのアルゴリズムで構成
  - 転送されるパケットの流れ
  - 転送されるパケットのサイズ
  - ホストで行われるDNSルックアップ

- **問題1…実験方法**
  - 実際のRESIP環境との乖離
- **問題2…精度**
  - RESIPアプリが起動してなくても誤検知することがある

検知プログラム　提案手法

- ブラックリスト方式
- 100回中80回以上観測されたIPアドレスをリストに登録
- 調査対象の端末でリストのアドレスと通信していないか？
- Pythonでpysharkライブラリを用いてパケットを取得
- 通信先アドレス一覧とブラックリストを比較

提案手法　アルゴリズム

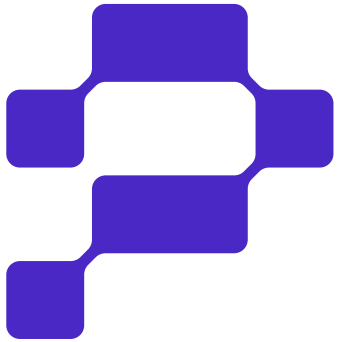
[入力]調査対象PCで取得したパケット***p***，通信先IPアドレスのリスト***a***

1. 5分間パケット***p***を取得する
2. プライベートIPアドレス以外の通信先IPアドレスをリスト***a***に記録する
3. ***a***をブラックリストと照合する

調査したRESIPアプリ

RESIPアプリ	開始年	RESIPプロバイダ
Hola VPN	2007	Brightdata
Proxyrackアプリ	2014	Proxyrack
Honeygain	2019	Oxylab

https://hola.org



https://www.proxyrack.com

https://www.honeygain.com

調査方法

入力：IPアドレス ***ip***, アドレスのリスト ***list***

1. RESIP アプリを起動して 100 秒待機する
2. 5 分間アドレス ***ip*** を取得する
3. ***ip*** がプライベートIPアドレスではなければリスト ***list*** に記録する
4. RESIPアプリを終了する
5. 1.から4.を100回繰り返す

日時	2022/11/23-28
場所	自宅(東京都江東区)
ホスト	Windows 10

観測回数上位10アドレス

- 観測回数は100回

通常時		Hola VPN		Proxyrack		Honeygain	
204.79.197.239	27	162.125.80.18	99	38.84.70.82	98	34.237.55.225	89
20.198.118.190	21	3.94.72.89	55	209.205.197.226	68	20.198.118.190	82
117.18.232.200	17	3.228.177.90	52	23.227.143.219	60	104.26.12.49	75
13.107.5.93	16	3.228.36.186	47	192.30.45.30	58	104.26.13.49	75
20.43.132.130	16	3.94.40.55	44	192.34.234.30	56	104.16.248.249	56
204.79.197.200	9	206.189.231.23	34	23.227.142.26	55	20.198.119.143	55
20.212.97.243	4	40.70.229.150	28	44.233.186.238	55	20.198.119.84	53
117.18.232.240	3	20.198.119.84	26	104.21.57.231	40	104.16.249.249	47
40.90.184.82	3	192.81.214.145	24	199.7.54.30	38	104.16.123.96	41
104.78.85.232	2	159.223.133.120	21	213.248.242.79	32	23.60.109.197	41

1 通常時

- 48のアドレスから1786のパケットを観測
- 7/10がMicrosoftのアドレス

204.79.197.239	27	Microsoft Corporation(MSFT)
20.198.118.190	21	Microsoft Corporation(MSFT)
117.18.232.200	17	EdgeCast Networks Asia Pacific Network
13.107.5.93	16	Microsoft Corporation(MSFT)
20.43.132.130	16	Microsoft Corporation(MSFT)
204.79.197.200	9	Microsoft Corporation(MSFT)
20.212.97.243	4	Microsoft Corporation(MSFT)
117.18.232.240	3	EdgeCast Networks Asia Pacific Network
40.90.184.82	3	Microsoft Corporation(MSFT)
104.78.85.232	2	Akamai Technologies,Inc.

2 Hola VPN

- 通常時と比較して通信先は2.9倍，パケットは6倍
- Dropbox, Amazon, DigitalOceanなどのアドレスが見られた

162.125.80.18	99	Dropbox, Inc. (DROPB)
3.94.72.89	55	Amazon Technologies Inc.
3.228.177.90	52	Amazon Technologies Inc.
3.228.36.186	47	Amazon Technologies Inc.
3.94.40.55	44	Amazon Technologies Inc.
206.189.231.23	34	DigitalOcean, LLC (DO-13)
40.70.229.150	28	Microsoft Corporation (MSFT)
20.198.119.84	26	Microsoft Corporation (MSFT)
192.81.214.145	24	DigitalOcean, LLC (DO-13)
159.223.133.120	21	DigitalOcean, LLC (DO-13)

3 Proxyrackアプリ

- 通常時と比較して通信先は6.8倍，パケットは50倍
- 最も高頻度で観測したアドレスはPSINet

38.84.70.82	98	PSINet, Inc. (PSI)
209.205.197.226	68	24 SHELLS (TS-74)
23.227.143.219	60	24 SHELLS (TS-74)
192.30.45.30	58	VeriSign Global Registry Services
192.34.234.30	56	VeriSign Global Registry Services
23.227.142.26	55	24 SHELLS (TS-74)
44.233.186.238	55	Amazon.com, Inc. (AMAZO-4)
104.21.57.231	40	Cloudflare, Inc. (CLOUD14)
199.7.54.30	38	VeriSign Global Registry Services
213.248.242.79	32	Nominet UK

4 Honeygain

- 通常時と比較して通信先は14.6倍，パケットは116倍
- Amazon, Cloudflareとの通信が上位を占めていた

34.237.55.225	89	Amazon Technologies Inc.
20.198.118.190	82	Microsoft Corporation (MSFT)
104.26.12.49	75	Cloudflare, Inc. (CLOUD14)
104.26.13.49	75	Cloudflare, Inc. (CLOUD14)
104.16.248.249	56	Cloudflare, Inc. (CLOUD14)
20.198.119.143	55	Microsoft Corporation (MSFT)
20.198.119.84	53	Microsoft Corporation (MSFT)
104.16.249.249	47	Cloudflare, Inc. (CLOUD14)
104.16.123.96	41	Cloudflare, Inc. (CLOUD14)
23.60.109.197	41	Akamai Technologies, Inc.

検知プログラム　提案手法

- ブラックリスト方式
- 100回中80回以上観測されたIPアドレスをリストに登録
- 調査対象の端末でリストのアドレスと通信していないか？

3.228.x.x	アメリカ	Amazon Technologies Inc.
3.94.x.x	アメリカ	Amazon Technologies Inc.
162.125.x.x	アメリカ	Dropbox, Inc.
81.31.x.x	ドイツ	JAGEX
23.227.x.x	アメリカ	Leaf Group Ltd.
38.84.x.x	アメリカ	PSINet, Inc.
104.16.x.x	アメリカ	Cloudflare, Inc.
104.26.x.x	アメリカ	Cloudflare, Inc.
18.65.x.x	アメリカ	Amazon Technologies Inc.
34.237.x.x	アメリカ	Amazon Technologies Inc.

結果　比較

- 従来手法と比較して真陽性率(TP)は微減
- 真陰性率(TN)は増加

	Hola VPN	Proxyrackアプリ	Honeygain
[3]Tosunらの手法 TP	100	99	100
[3]Tosunらの手法 TN	88	88	88
提案手法 TP	99	98	100
提案手法 TN	**100**	**100**	**100**

まとめ

- 3つのRESIPアプリが高頻度で通信を行うアドレスを調査した
- 従来手法よりも高い精度でRESIPホスト検知ができた