

Residential IP Proxy サービスを悪用した不正行為の調査

住友 孝彰 †

明治大学総合数理学部 先端メディアサイエンス学科 菊池研究室 †

1 はじめに

近年、住宅用の IP アドレスで動作する PC やスマートフォンをプロキシとして利用する Residential IP Proxy(以下 RESIP とする)サービスの市場規模が拡大している。本来は検閲によりネットワークの利用が制限されているユーザが、アクセス制限を回避して自由なインターネットサービスを利用するために提供されているが、2017年にMiらによって悪用されていることが報告されている [1]。匿名通信路 Tor と同様に、アクセスされたサーバ側からブラウザ側は秘匿されているので、攻撃に悪用されている可能性がある。Miらの2017年を契機として、2019年には半澤らが国内における状況を調査している [2]。

そこで、本研究では RESIP サービスの不正利用の最新状況を明らかにすることを目的とする。代表的なサービスである ProxyRack[4] と Bright Data[5] の proxy IP アドレスを収集し、分析基盤 NONSTOP[3] を介して利用できる情報通信研究機構が保持する非対話型ハニーポッドで得られた情報と脅威情報分析プラットフォーム VirusTotal などを用いて、2つのサービスの不正行為の頻度、種類、および、不正な proxy の分布を報告する。

2 準備

2.1 Residential IP Proxy

RESIP サービスは住宅用 IP をプロキシとして提供する proxy サービスである。サービスの利用者はプロバイダが提供している IP アドレスをプロキシとして利用し、任意のサイトにアクセスを行う。本調査対象である Bright Data[5] は、IP アドレスを提供することでメリットを得られる旨を主張している。

2.2 データセット

本研究で使用したデータセットについて説明する。

NICTER Darknet データセットは情報通信研究機構が保有するダークネットで観測された不正通信の情報である。同機構が提供する分析基盤 NONSTOP[3] から、パケットの到着時間、送信元、送信先の IP アドレス、ポート番号などを得る。

GeoLite2City データベースは MaxMind 社が提供している無償のデータベースである。IP アドレスから国や緯度、経度などの情報を得る。

VirusTotal は Google 社が運営する脅威情報分析プラットフォームである。WEB サイト上でマルウェアやファイルのスキャン、URL や IP アドレスの悪性判定を提供している。API を用いて IP アドレスの悪性判定を行うこともできる。

Shodan はインターネットに接続されたデバイス情報の検索エンジンである。インターネットをクロールし、解放されているポート番号、位置情報、応答から得られるバナー情報を収集し、データベース化して提供している。web ページからの利用、もしくは API が提供されている。

それぞれの概要と本研究での利用目的について表 1 にまとめる。

2.3 先行研究

2017年にMiらは RESIP サービスで提供される IP アドレスを収集し、RESIP サービスのサービスの基盤、規模を明らかにした [1]。

2021年に半澤らは、Miらの研究 [1] で収集された Residential IP Proxy as a Service データセットに含まれる RESIP ホストの IP アドレスから日本のネットワークに不正な通信が継続的に到達していると結論づけた [2]。また、ホストの詳細な所在、ISP、RESIP の不正利用の頻度、RESIP ホストになっているデバイスベンダ等を明らかにした。

3 実験

3.1 実験目的

本研究の実験目的は以下の3つである。

†Kikuchi Laboratory, Department of Frontier Media Science, School of Interdisciplinary Mathematical Science, Meiji University.

表 1: 使用したデータセット・データベースの概要と使用目的

データセット データベース	内容	使用目的
NICTER Darknet[6]	情報通信研究機構が保有する ダークネットで観測されたパケットの情報	Proxy の IP アドレスから国内のダークネットに ポートスキャンが行われているか調査する
VirusTotal[7]	Google 社が提供する 脅威情報分析プラットフォーム	Proxy の IP アドレスの悪性判定
shodan[8]	インターネットに接続された デバイスの情報を検索する検索エンジン	Proxy の IP アドレスで 解放されているポートの調査
GeoLite2City[9]	MaxMind 社提供している Geo location データベース	Proxy の IP アドレスの地理情報の調査

1. 2つのサービスのホストの差を明らかにする。
2. Proxy 経由の通信が国内のダークネットに到達しているか調査する。
3. 悪性利用のポートと用途, 国名, 時系列の変化を明らかにする。

3.2 実験方法

図 1 に IP アドレスの収集方法の概要, 図 2 に IP アドレスの分析方法の概要を示す。クライアント PC から RESIP サービスのプロキシを経由して研究室のサーバ (windy.mind.meiji.ac.jp) にアクセスすることで RESIP ホストの IP アドレスを収集する。アクセスの際に User-Agent 属性に特徴的な文字列を挿入することにより通常の WEB アクセスと実験によるアクセスを判別する。1, NICTER Darknet データセット, 2, VirusTotal, 3, Shodan, 4, GeoLite2City を用いて収集したホストの IP アドレスについて調査する。

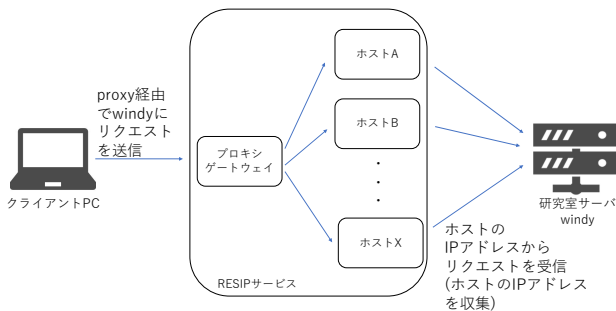


図 1: IP アドレス収集方法の概要図

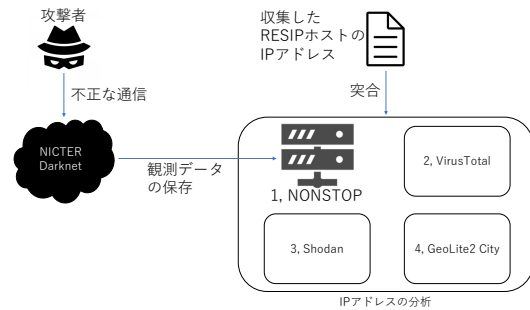


図 2: 収集した IP アドレスの分析方法の概要図

3.3 実験結果

ダークネットは未使用のアドレスブックなので、ここへの通信路要求は全てポートスキャン等の不正目的であると考えられるので、国内のダークネットに不正な通信を行った IP アドレスを不正 IP アドレス、国内のダークネットで観測されたパケットを不正パケットと呼ぶ。また VirusTotal で 1 つでも悪性と判定されたものを悪性と呼ぶ。

表 2 に収集期間, 収集した IP アドレスの総数, 不正 IP アドレスの個数, 不正 IP アドレスの中の悪性 IP アドレスの個数, 不正パケットの総数, 悪性 IP アドレスからの不正パケット数を示す。観測期間で取得されたユニークな IP アドレス数を約 7 万個で共通にした時, ダークネットにスキャンした不正 IP アドレスの個数, 不正 IP アドレスの内悪性と判定された個数は, ProxyRack の方が多い。ProxyRack で 44 個, Bright Data で 2 個の IP アドレスは, 期間中毎日観測されるアクティブなアドレスであった。

表 2: 収集したデータの概要

サービス	ProxyRack		Bright Data		
	期間	2021/7/22-8/7, 8/16-23 計:25 日	2021/9/30-10/13, 10/15-23, 11/19-21 計:26 日		
IP アドレス	IP アドレスの総数	69,369		70,253	
	不正 IP アドレス数	3,092	4.5%	1,545	2.2%
	同アドレス中 悪性 IP アドレス数	1,087	35.2%	307	19.9%
パケット	不正パケット数	526,674		32,724	
	悪性 IP アドレスから 到達したパケット数	252,454	47.9%	15,379	47.0%

図 3 に NICTER Darknet で観測された RESIP ホストの数の変化を示す。図 4 に 1 ホスト当たりの 1 日の平均パケット数を示す。*.mal は不正な通信を行った IP アドレスの内、悪性と判定された数である。

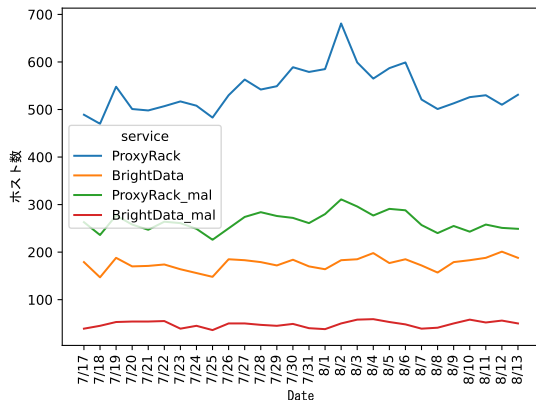


図 3: NICTER Darknet で観測されたホスト数

表 3 に宛先のポート別パケット観測数を示す。図 5a(ProxyRack), 図 5b(Bright Data) に観測された日付と宛先ポートの散布図を示す。

表 4 に Shodan を用いて調査した不正 IP アドレスで外部に開放しているポートを示す。

収集した IP アドレスすべてについて GeoLite2City データベースを用いて国を判別した。図 6a(ProxyRack), 図 6b(Bright Data) に世界地図のマッピングを示す。図 7a(ProxyRack), 図 7b(Bright Data) に不正 IP アドレスの割合の世界地図のマッピングを示す。表 5(ProxyRack), 表 6(Bright Data) にホスト数の上

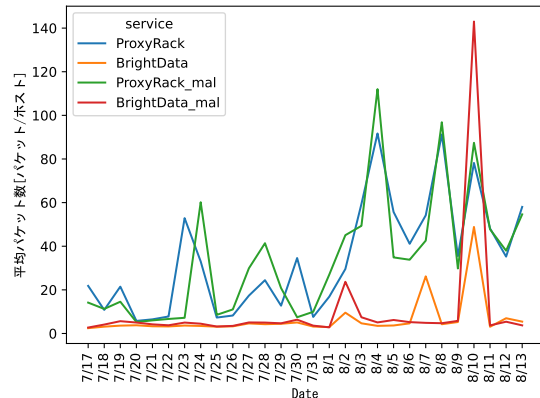


図 4: NICTER Darknet で観測された 1 ホスト当たりの通信数

表 3: サービス別の宛先ポート別パケット観測件数

宛先ポート番号 (サービス)	ProxyRack		Bright Data		半澤	
	観測件数	[%]	観測件数	[%]	観測件数	[%]
21(FTP)	112	0.0	125	0.4	193,917	11.5
22(SSH)	38592	7.3	0	0.0	49,767	2.9
23(Telnet)	32300	6.1	4051	12.4	613,606	36.4
25(SMTP)	0	0.0	0	0.0	21,732	1.3
80(HTTP)	15150	2.9	2044	6.2	97,780	5.8
445(SMB)	19682	3.7	11284	34.5	399,250	23.7
1433(MSSQL)	4671	0.9	524	1.6	144,928	8.6
2222(SSH)	0	0.0	0	0.0	16,838	0.1
2323(Telnet)	754	0.1	363	1.1	43,310	2.5
3389(RDP)	64	0.0	0	0.0	9,782	0.5

位 10 位とその国の不正ホスト率を示す。表 7 に 2 つのサービスでホスト数の上位 15 位以内で共通している国のホスト数と不正ホスト率を示す。

表 4: サービス別の不正 IP アドレスのホストのソース

ポート番号	ProxyRack				Bright Data			
	不正 IP 数	[%]	悪質な不正 IP 数	[%]	不正 IP 数	[%]	悪質な不正 IP 数	[%]
2000	169	5.47	33	19.53	48	3.11	4	8.33
80(HTTP)	119	3.85	15	12.61	28	1.81	2	7.14
1723(PPTP)	100	3.23	21	21.00	32	2.07	2	6.25
8291	75	2.43	11	14.67	18	1.17	2	11.11
53(DNS)	66	2.13	13	19.70	25	1.62	2	8.00
21(FTP)	53	1.71	10	18.87	6	0.39	0	0.00
22(SSH)	49	1.58	5	10.20	10	0.65	1	10.00
443(SMB)	48	1.55	8	16.67	28	1.81	2	7.14
7547(CWMP)	41	1.33	4	9.76	4	0.26	0	0.00
8080(HTTP)	29	0.94	7	24.14	5	0.32	1	20.00
5555	20	0.65	3	15.00	1	0.06	0	0.00
23(Telnet)	20	0.65	3	15.00	7	0.45	0	0.00

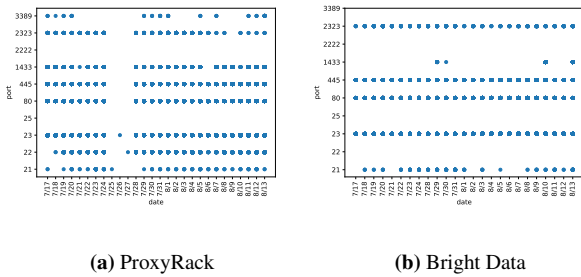


図 5: 宛先ポート

表 5: ProxyRack のホスト数上位 10 か国と不正ホスト率

国名	ホスト数	不正ホスト率 [%]
大韓民国	16114	1.9
日本	5836	1.0
香港	5521	4.2
台湾	3655	3.2
ブラジル	3151	3.9
ロシア連邦	2988	5.6
タイ	2757	7.7
アメリカ合衆国	2715	3.6
ウクライナ	2293	7.0
中華人民共和国	2181	7.5

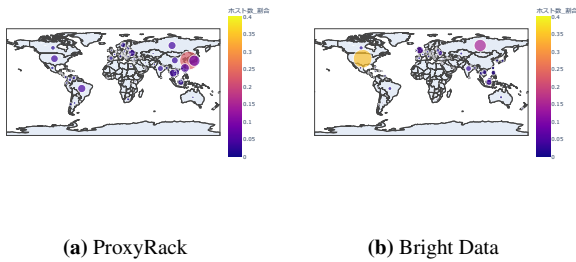


図 6: ホストの分布

表 6: Bright Data のホスト数上位 10 か国と不正ホスト率

国名	ホスト数	不正ホスト率 [%]
アメリカ合衆国	24258	0.05
ロシア連邦	10578	3.0
イギリス	3715	0.1
インドネシア	2415	7.0
インド	2284	7.2
ウクライナ	2104	2.1
マレーシア	1691	6.0
ベトナム	1677	4.2
フィリピン	1555	13.5
カナダ	1214	0.6

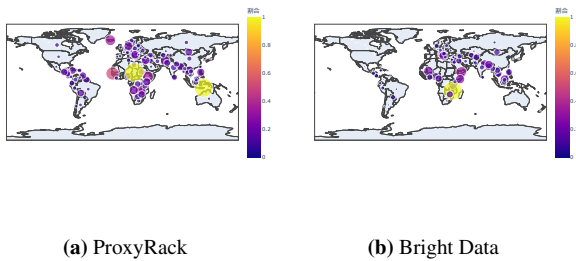


図 7: 不正ホストの割合

3.4 考察

本研究で対象とした期間において、両サービスのホストから継続的に国内のダークネットにポートスキャンが行われていることが分かった。不正な通信を行って

表 7: ホスト数上位 15 개국と不正ホスト率の比較

国名	ProxyRack		Bright Data	
	ホスト数	[%]	ホスト率	[%]
ブラジル	3151	3.9	1060	1.9
カナダ	1002	6.1	1214	0.6
インドネシア	1656	8.8	2415	7.0
インド	1647	11.8	2284	7.2
大韓民国	16114	1.9	695	0.7
ロシア連邦	2988	5.6	10578	3.0
タイ	2757	7.7	1058	3.9
台湾	3655	3.2	749	1.5
ウクライナ	2293	7.0	2104	2.1
アメリカ合衆国	2715	3.6	24258	0.05
ベトナム	2109	6.9	1677	4.2

るホストの割合、悪性と判定された割合、パケットの総数において ProxyRack の方が多い。ホスト数、1 ホスト当たりの通信数ともに全ての日数においても ProxyRack の方が多い。

パケットの到達ポートに着目してみると、ProxyRack は 748 個、Bright Data は 365 個と ProxyRack の方が幅広いポートに通信が到達し、スキャン目的の通信が多いといえる。表 3 で挙げた 10 個のポートにおいても ProxyRack は 8 個、Bright Data は 6 個と差が見られた。例えば、22(SSH) は ProxyRack では 10 個の中で第 1 位であったが Bright Data では 0 であった。半澤らの研究では 10 個のポート全てに通信が確認されており、変化が見られた。一方、Bright Data は到達パケット数こそ少ないものの、ポート別の割合に着目すると Telnet と SMB への通信の割合が高い。スキャンではない意図的な行動の拠点になっていると考える。

外部に開放されているポートに着目してみると、マルウェア Mirai やその亜種が標的とするポートと報告されている 7547[10]、マルウェア Mirai やその亜種に探索対象のポートとして追加されたと考えられている、5555[11]、MikroTik 製のルータの Winbox がデフォルトで利用するポート番号でリモートから任意のコードを実行できる (RCE) 脆弱性が報告されている 8291[12]、同様に MikroTik 製のルータを標的とする通信の標的ポートである 2000[13] が解放されていた。特に、2000 は両サービス共に割合が第 1 位であり、悪性と判定されたホストの割合も第 4 位と高い。このことより、両サービスの proxy ホストは Mirai などのマルウェアに感染したデバイス、もしくは脆弱性を利用されたデバイスの割合が高いと考える。

ホストの分布はサービスごとに差があることが分かっ

た。ProxyRack はアジア圏に集中しているのに対し、Bright Data は北米に分布している。

4 おわりに

2 つの RESIP サービスを調査した。不正 IP アドレスの割合や宛先ポート、不正 IP アドレスの解放ポートには RESIP サービスごとの差があることが分かった。IP アドレスを収集した期間に差があるため、今後、同一の期間で条件を揃えて再実験する予定である

参考文献

- [1] Xianghang Mi et al. “Resident Evil: Understanding Residential IP Proxy as a Dark Service”, IEEE Symposium on Security and Privacy (SP), volume: 1, pp. 170-186, 2019.
- [2] 半澤, “Residential IP Proxy サービスに悪用される住宅用ホストの調査”, 2020 年度明治大学菊池研究室修士論文, 2021.
- [3] 竹久達也, 神菌雅紀, 笠間貴弘, 中里純二, 衛藤将史, 井上大介, 中尾康二, サイバーセキュリティ情報遠隔分析基盤 NONSTOP の利活用について, コンピュータセキュリティシンポジウム 2014 論文集, volume: 2, pp. 207-214, 2014.
- [4] ProxyRack (<https://www.ProxyRack.com/>) (2021/11/27 参照)
- [5] Bright Data (<https://BrightData.com/>) (2021/11/27 参照)
- [6] NICTER WEB (<https://www.nicter.jp/>) (2021/11/27 参照)
- [7] Virsutotal (<https://www.virustotal.com/>) (2021/11/27 参照)
- [8] Shodan (<https://www.shodan.io/>) (2021/11/27 参照)
- [9] MAX MIND, GeoLite2 Free Geolocation Data (<https://dev.maxmind.com/geoip/geolite2-free-geolocation-data?lang=en>) (2021/11/27 参照)
- [10] TrendMicro, 「Mirai」亜種か? 海外製ルータを狙うアクセスが急増 (<https://www.trendmicro.com/jp/iot-security/news/3086>) (2021.12.19 参照)
- [11] NICTER Blog (<https://blog.nicter.jp/2018/10/android-5555/>) (2021.12.19 参照)
- [12] tenable, MikroTik RouterOS Vulnerabilities: There’s More to CVE-2018-14847 (<https://www.tenabl>

e.com/blog/mikrotik-routeros-vulnerabilities-there-s-more-to-cve-2018-14847)
(2021.12.19 参照)

[13] NICTER 観測レポート 2018 (https://www.nict.go.jp/cyber/report/NICTER_report_2018.pdf) (2021.12.19 参照)