

Residential IP Proxy サービスを悪用した不正行為の調査

住友 孝彰† 菊池 浩明†

明治大学総合数理学部†

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、本研究では代表的な RESIP サービス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*と Bright Data†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 実験

2.1 実験方法

図 1 に IP アドレスの収集方法の概要を示す。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。1, NICTER Darknet データセット‡, 2, VirusTotal§, 3, Shodan¶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。

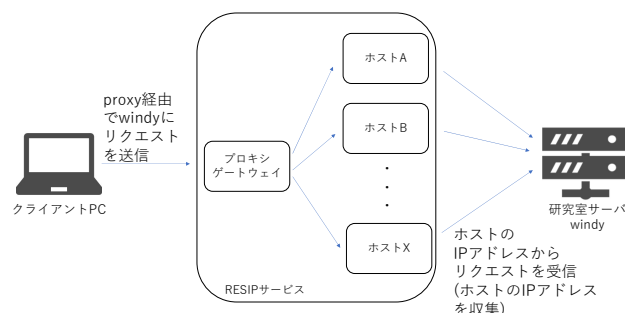


図 1: IP アドレス収集方法の概要図

2.2 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。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 1 に収集期間、収集した IP アドレスの総数、不正な通信を行った 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 1: 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
	不正 IP アドレス数	3,092
	同アドレス中 悪性 IP アドレス数	1087
パケット	不正パケット数	526,674
	悪性 IP アドレスから 到達したパケット数	252,454

図 2 に NICTER Darknet で観測された RESIP ホストの数の変化を示す。図 3 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。表 2 に送信先のポート別パケット観測数を示す。表 3 に Shodan を用

Study on malicious activities via Residential IP Proxy services

†Takaaki Sumitomo, Hiroaki Kikuchi, School of Interdisciplinary Mathematical Science, Meiji University.

*<https://www.ProxyRack.com/>

†<https://BrightData.com/>

‡<https://www.nicter.jp/>

§<https://www.virustotal.com/>

¶<https://www.shodan.io/>

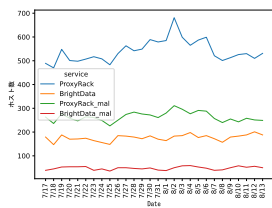


図 2: ホスト数

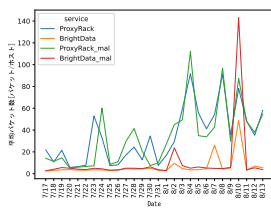


図 3: 平均パケット数

表 2: 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

表 3: 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

いて調査した不正な通信を行った IP アドレスで外部に開放しているポートを示す。

2.3 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いるホストの割合、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 2 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[4], 5555[5], MikroTik RouterOS の脆弱性を狙った攻撃の標的ポートである 8291[6], 2000[7] 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。

3 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 Symp. on Security and Privacy (SP), 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 年度明治大学大学院修士論文, 2021.
- [3] 竹久, 神蘭, 笠間, 中里, 衛藤, 井上, 中尾, 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, CSS 2014, 2, pp. 207-214, 2014.
- [4] 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).
- [5] NICTER Blog, (<https://blog.nictcr.jp/2018/10/android-5555/>), 2021.12.19 参照).
- [6] tenable, MikroTik RouterOS Vulnerabilities: There's More to CVE-2018-14847, (<https://www.tenable.com/blog/mikrotik-routeros-vulnerabilities-there-s-more-to-cve-2018-14847>), 2021.12.19 参照).
- [7] NICTER 観測レポート 2018, (https://www.nict.go.jp/cyber/report/NICTER_report_2018.pdf), 2021.12.19 参照).