5ZC-06

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

北原 拓海 †　菊池 浩明 †

明治大学総合数理学部 先端メディアサイエンス学科 †

1　はじめに

近年，住宅用の IP アドレスを使用したプロキシアプリである Residential IP Proxy(RESIP) の利用が盛んになってきている．主な用途としては，IP アドレスに基づく検閲や，データスクレイピングによるアクセス制限を回避する場合などが挙げられる．

しかし RESIP はそのような用途の他にも，自身の身元を秘匿することを利用した不正アクセスや攻撃の踏み台としても悪用が疑われている．Mi らは 2017 年に RESIP ホストの 95% が住宅用の IP アドレスであり，その内の 43% が IoT 機器のものであることを報告している [1]．半沢らは国内のダークネットを観測し，所有する機器が意図せずに RESIP ホストとなり悪意を持った第三者に利用されている可能性があることを指摘している [2]．そのためユーザーは所有する機器が悪用されていることを検知して防ぐことが重要である．Tosun らは端末で取得したパケットの特徴を分析してホストで稼働している RESIP アプリを検知するアルゴリズム [3] を提案している．しかし，誤検知の頻度が高く，精度に問題があった．

そこで本稿では RESIP アプリについて，従来の方法とは異なる IP アドレスのブラックリストを作成することで主要な RESIP アプリの検知を提案する．また，実験に基づく検出精度を報告する．

2　提案手法

2.1　予備調査

自身が RESIP ホストになっていることを判断するには，ホストでパケットを観測してその通信路の情報を調査する方法がある．RESIP ホストとなって様々なアドレスにアクセスする際，RESIP アプリのゲートウェイとの定期的な通信が行われる．

そこで本調査では Hola VPN[4], Proxyrack アプリ [5], Honeygain[6] の 3 つの RESIP アプリのホストとなり，各アプリについて 5 分× 100 回の通信を観測して図 1 におけるプロキシゲートウェイとターゲットサイトの通信先 IP アドレスを収集し，各 RESIP アプリの通信の特徴を定量化する．

†Takumi Kitahara, Hiroaki Kikuchi, Proposal on Node Detection to be used as RESIP Host based on IP Black list, Department of Frontier Media Science, School of Interdisciplinary Mathematical Science, Meiji University.

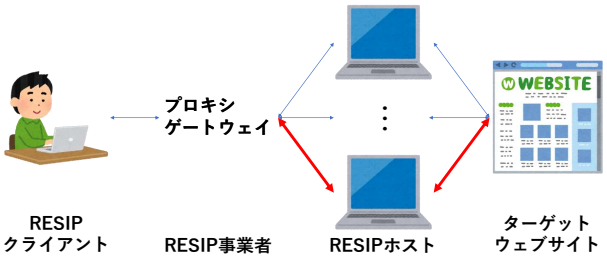

図 1　実験環境

表 1　調査した RESIP のアプリ開始年，使用している SDK

名称	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

2.2　観測方法

本観測では RESIP アプリを起動した後 100 秒待機してからホストの通信を 5 分間観測し，その後 RESIP アプリを再起動することで，確立された接続をリセットするようにした．

3　RESIP 検知プログラムの開発

3.1　概要

本ツールは前述の観測ツールで収集された IP アドレスを元に作成されたブラックリストを使用し，RESIP アプリとの関係が疑われる通信先との通信を検知する．

3.2　実験方法

本実験では調査対象の RESIP アプリの通信を観測して定期的にアクセスを行う IP アドレスを記録することで，各 RESIP アプリの通信の特徴と RESIP 検知プログラムのブラックリストに登録すべきアドレスについて調査を行う．実験で使用したアプリを起動する OS は Windows 10 である．調査した RESIP アプリは Hola VPN, Proxyrack アプリ, Honeygain の 3 つである．

(1) 表 1 の 3 つの RESIP アプリについて，5 分のパケット収集を 100 回行う．

(2) 実験 1 で収集した IP アドレスについて，継続的に通信が行われていたものを IP ブラックリストに記録し，作成した RESIP 検知プログラムの精度を調査する．

表 2　実験で使用した RESIP アプリ及び収集した IP アドレスとパケット数

使用した RESIP	IP	パケット
なし (通常時)	48	1786
Hola VPN	141	11192
Proxyrack アプリ	325	89416
Honeygain	703	208820

3.3　実験 1 結果 (通信先)

通常時と 3 つの RESIP アプリについて収集した IP アドレスの数とパケットの数を表 2 に示す．本調査は東京都の自宅から，家庭内 LAN に接続した Windows 10 端末で行った．

2022 年 11 月 24 日 5:53-14:06 に観測した通常時の通信では 48 のアドレスから 1786 のパケットを収集した．継続的に通信を行っていた IP アドレスの中で最も観測された回数が多かったのは，100 回中 27 回観測した 204.79.x.x(Microsoft) だった．

2022 年 11 月 23 日 5:28-16:29 に観測した Hola VPN の通信は通常時の通信と比較すると通信先は 2.9 倍，パケットは 6 倍であり，通信先には通常時には見られなかった Dropbox, Amazon, DigitalOcean などのアドレスが多く見られた．

2022 年 11 月 24 日 7:49-18:52 に観測した Proxyrack アプリの通信は通常時の通信と比較すると通信先は 6.8 倍，パケットは 50 倍であった．最も観測された回数が多かった IP アドレスは 100 回中 98 回観測された 38.84.x.x(PSINet) であり，その他には 24 SHELLS, VeriSign のアドレスが上位 10 アドレス中 6 つを占めた．

2022 年 11 月 28 日 1:30-13:22 に観測した Honeygain の通信は通常時の通信と比較すると通信先は 14.6 倍，パケットは 116 倍であった．最も観測された回数が多かった IP アドレスは 100 回中 89 回観測された 34.237.x.x(Amazon) であり，その他には Cloudflare のアドレスが上位 10 アドレスの半分を占めた．

3.4　実験 2　結果 (ブラックリストの作成)

調査 1 で収集した IP アドレスを元に RESIP ホスト検知プログラムに使用するブラックリストを作成した．登録した IP アドレスの割当国と whois 情報を表 3 に示す．登録した IP アドレスは，実験 1 での 100 回の観測のうち 80 回以上観測したアドレスの上位 16 ビットに限定した．ただし Honeygain のパケットの観測でのべ 190 回観測した 20.198.x.x は通常時でも観測されるアドレスのため，最終的にはその 1 つを除いた計 10 個の IP アドレスをブラックリストに登録した．

作成したブラックリストを用いて，収集したパケットを判定した結果を表 4 に示す．

RESIP ホストでない通常時のパケットで RESIP ホストであると誤判定される偽陽性は 100 回の実験では起こらなかった．

表 3　ブラックリストに登録した IP アドレスの割当国

IP アドレス	割当国	whois
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.

表 4　RESIP 検知プログラムの精度 [%]

	Hola VPN	Proxyrack アプリ	Honeygain
従来手法 TP	100	99	100
従来手法 TN	88	88	88
提案手法 TP	99	98	100
提案手法 TN	100	100	100

4　おわりに

本研究では RESIP アプリのホストとなる 3 つのアプリについて通信先 IP アドレスを観測することで，各 RESIP アプリが高頻度で定期的に通信する IP アドレスを確認した．またそれらの IP アドレスに基づいて，対象の端末が RESIP ホストとなっているかを高い精度で判別する方法を提案した．

参考文献

[1] 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.

[2] 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.

[3] Altug Tosun, et al., “RESIP Host Detection: Identification of Malicious Residential IP Proxy Flows”, 2021 IEEE International Conference on Consumer Electronics，2021.

[4] Get The Free and Premium Hola Online — Proxy Unblocker，(閲覧日 2022/11/15，https://hola.org/)

[5] Proxyrack: Buy Proxies HTTP, UDP, SOCKS Proxy，(閲覧日：2022/11/15，https://www.proxyrack.com/)

[6] Passive Income – Effortlessly — Honeygain，(閲覧日：2022/11/15，https://www.honeygain.com/)