

総集編：国内悪性プロキシサービスとの闘争

Combatting residential proxy services in Japan

STB経由不正アクセスとは？ 犯罪プロキシサービスの実態解説

NICT協力研究員
猪野裕司

注意書き Notes

- 本プレゼンテーションではレジデンシャルプロキシの現状を幅広く解説させていただきます。
- 本プレゼンテーションで提供される情報は、情報提供のみを目的としたものであり、専門的な助言として解釈されるものではありません。
- 本資料に掲載された情報のご利用は、閲覧者ご自身の責任において行ってください。利用を推奨するものではありません。
- 本プレゼンテーションにおける意見は発表者個人のものであり、発表者の所属会社またはその関連組織の見解を反映するものではありません。
- 本プレゼンテーションは、明示または黙示を問わず、いかなる種類の保証も行いません。
- This presentation is for informational purposes only and does not constitute professional advice.
- Use of the information is at the viewer's own responsibility.
- Opinions expressed are the presenters' own and do not necessarily represent their organizations.
- No warranties of any kind are provided.

自己紹介



■ **氏名:**猪野 裕司 (いのゆうじ)

■ **所属:** NICT協力研究員

■ **資格:** CISSP、GCIH、GCTI、GNFA

書籍: 「実践CSIRT 現場で使えるセキュリティ事故対応」(共著)
「Hitachi Systems Security Journal vol. 63」

X: @yumano

■ 主要なキャリア

大手SI研究開発、海外製品拡販 …10年
2011-海外駐在 アライアンス担当 …4年
2016- CSIRTリーダー (リクルート転職) …5年
2021-サイバー犯罪対策 …4年

■ その他のキャリア

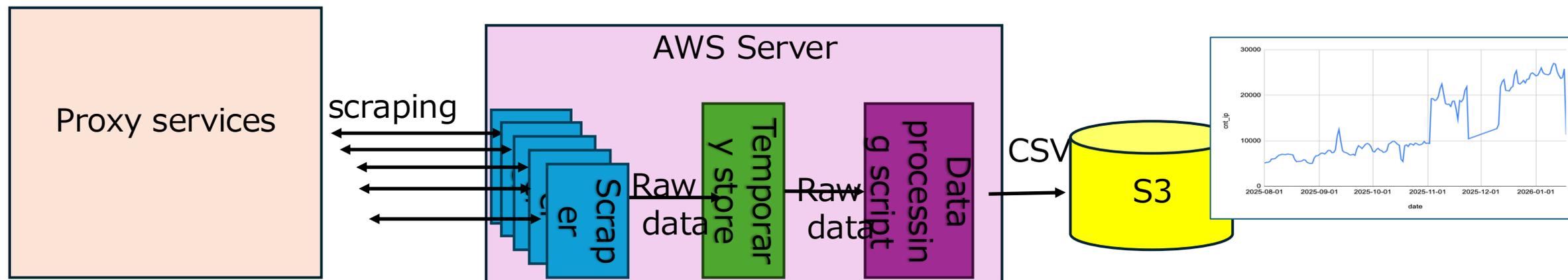
日本フィッシング対策協議会 運営委員
日本サイバー犯罪対策センター幹事

■ 発表/講演:

JSAC2022 「国内悪性プロキシサービスとの闘争」
JSAC2024/ NCFTA2025 / NCA2024
「フィッシングサイトに対するDeceptionアプローチ」
JSAC2025 / Cyber Intelligence Summit 2025
「Active Monitoring and Response to User Credential Leaks」
情報セキュリティワークショップ越後湯沢2025/
サイバー犯罪に関する白浜シンポジウム2026
「民間企業における警察対応の勘所」
JSAC2026/JANOG57
「続・国内悪性プロキシサービスとの闘争」

趣味でやってるプロキシ研究プロジェクト

- 我々は2020年からRESIPプロキシのアドレスを継続的に収集してきました。
We have been continuously collecting RESIP proxy addresses since 2020.



プロキシサービスから直接IPを収集。対象は日本国内のみにフォーカス。
We collect IP addresses directly from proxy services. Focus is exclusively on Japan.

日次20000ユニークIP、月次で11万ユニークIPを観測。
We observe ~10,000 unique IPs daily and 110,000 unique IPs per month.

STB？！テレビ受信機？！

外付け「テレビ受信機」にマルウェア潜伏、サイバー攻撃の踏み台に

事件・司法 [+ フォローする](#)

2025年9月18日 10:10 (2025年9月18日 11:01更新) [会員限定記事]

保存     

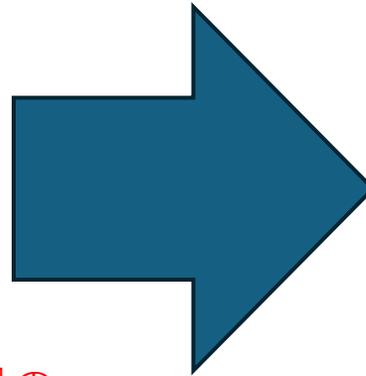
海外からのサイバー攻撃に一般家庭のテレビ用受信機が悪用されている。金融機関に対する不正アクセスの「踏み台」とされている実態が警察当局の分析で浮かび上がった。犯罪集団が乗っ取るためのマルウェア（悪意のあるプログラム）が仕込まれた機器も流通する。購入者は気づかぬうちにサイバー攻撃へ加担するおそれがある。

上記の記事が話題に・・・有料部分に該当の機器の詳細が記載されていたが読まれずに界隈がざわつき

攻撃者は受信機を経由すれば日本国内の通信と偽装できる。これまでもルーターといったIoT機器が踏み台とされる事例はあった。セットトップボックスを中継点とするのは新手で、遅くとも23年ごろに悪用が始まったとみられる。

問題がある機器の多くは海外製で、「海外動画を無料で視聴できる」などとうたう例がある。マルウェアが仕込まれた経緯や攻撃者との関係性は分かっていない。警察庁は4月、実態を解明するため積極的な捜査を推進するよう都道府県警へ通達した。

<https://www.nikkei.com/article/DGXZQOUD11ACS0R10C25A9000000/>



証券口座乗っ取りの“STBが踏み台”報道がケーブルテレビ業界に波紋 問題は「ネット通販等で売られている管理されていない端末」

2025年10月02日 13時46分 公開

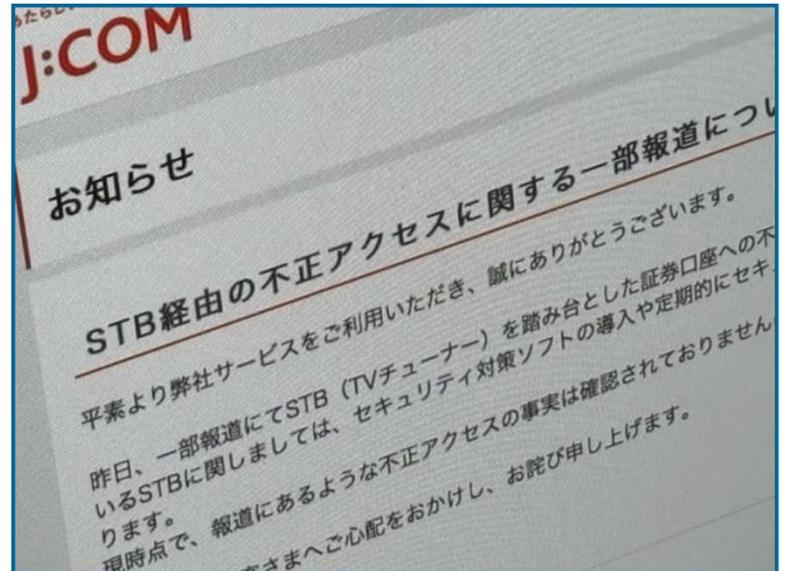
[芹澤隆徳, ITmedia]

 印刷  見る  Share  46  0

PR メール処理に資料作成…… 日々の業務をスマートにこなすには？ **Push!**

PR 兼務や出向の「ID二重管理」を解消 情シスの隠れた手間をゼロにする新手法

日本経済新聞が9月27日に報じた「証券口座乗っ取り、家庭のテレビ受信機『STB』経由か 警察が回収」という記事がケーブルテレビ業界に波紋を広げた。捜査関係者への取材をもとに、不正アクセスの際に一般家庭のテレビ用受信機が悪用された疑いがあると指摘したものの「STB」という言葉が誤解を招いた可能性がある。



J:COMのお知らせ (出典: J:COMのWebサイト)

<https://www.itmedia.co.jp/news/articles/2510/02/news081.html>

これまでのお話



https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_3_ino_jp.pdf

レジデンシャルプロキシとは

RESIDENTIAL = 住宅の PROXY = プロキシ

**一般家庭のインターネット接続（ISPが割り当てるIPアドレス）
を踏み台にするプロキシ**

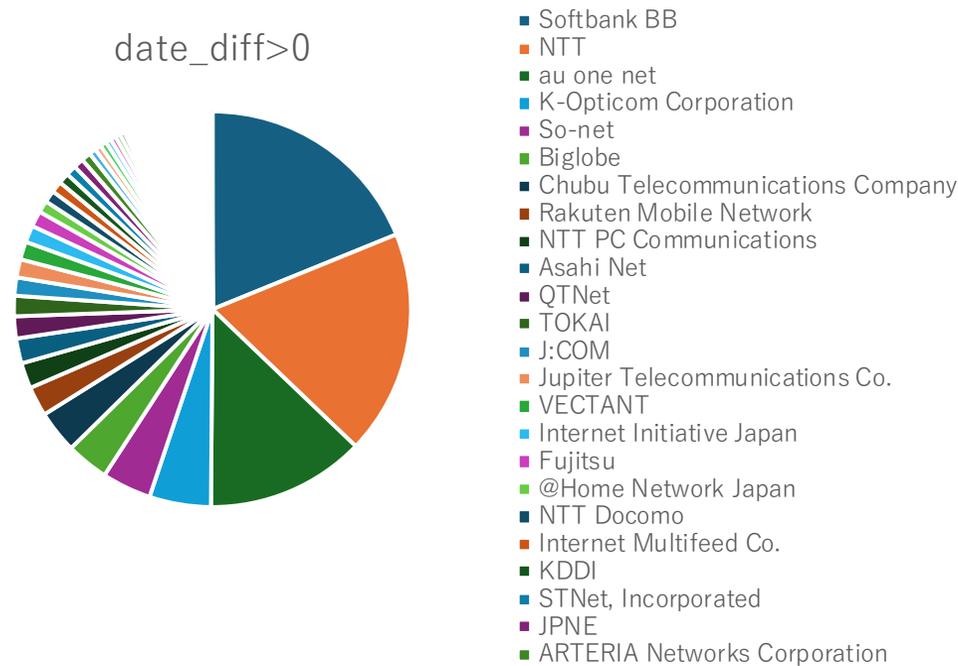
JSAC2022：発表

- 最大手レジデンシャルプロキシサービス 911 S5の出口IPを分析、以下のことが判明した：

- ・ 匿名性が高く、特徴検出が非常に困難：
普通のユーザーのアクセスのフリができる
地域、国などをごまかせる
アクセスの流量制限を掻い潜れる
IPブロックされても回避できる
(非常に多くの出口IPアドレスが利用できる)

RESIPデータの分析(911S5 : JSAC2022)

- 特に突出したASNは見つからず



asn	cnt_ip	割合	累積
Softbank BB	49290	19%	19%
NTT	48021	18%	37%
au one net	33896	13%	50%
K-Opticom Corp	13130	5%	55%
So-net	10523	4%	59%
Biglobe	9052	3%	63%
Chubu Telecomr	9051	3%	66%
Rakuten Mobile	6334	2%	68%
NTT PC Commu	5469	2%	71%
Asahi Net	5347	2%	73%
QNet	4714	2%	74%
TOKAI	4375	2%	76%
J:COM	3891	1%	78%
Jupiter Telecom	3885	1%	79%
VECTANT	3844	1%	81%
Internet Initiative	3603	1%	82%
Fujitsu	3362	1%	83%
@Home Network	2557	1%	84%
NTT Docomo	2552	1%	85%
Internet Multifee	2425	1%	86%
KDDI	2296	1%	87%
STNet, Incorpora	2236	1%	88%
JPNE	2142	1%	89%
ARTERIA Netwo	2023	1%	89%
Energia Commu	1479	1%	90%
NTT-ME Corpor	1359	1%	90%

RESIPデータの分析(911S5 : JSAC2022)

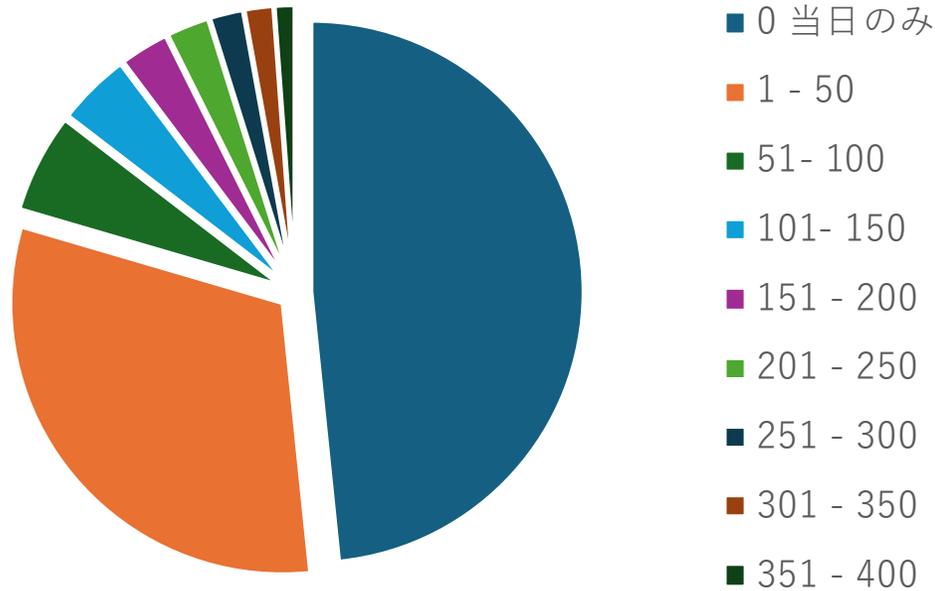
• キャリアごとの生存期間

行	asn	Softbank BB	NTT	au one net	K-Opticom Corp	So-net	Biglobe	Chubu Telecomr	Rakuten Mobile	NTT PC Commu	Asahi Net	QTNet	TOKAI	J-COM	Jupiter Telecomr	VECTANT	Internet Initiati	Fujitsu	@Home Networ	NTT Docomo	Internet Multifee	KDDI	STNet, Incorpor	JPNE	ARTERIA Netwo	Energia Commu	NTT-ME Corpor.	freet	Softl	Oper	Newi	its	cc	DTI	Katc	EDICKN	NTT	Itec	Com	Wire	Data	Star		
0日	10	###	###	###	###	###	###	###	913	###	###	###	###	559	963	###	###	###	840	###	###	78	813	188	276	498	579	671	498	513	384	105	317	409	302	90	197	149	126	20	34	93		
20	20	###	###	###	###	###	958	###	264	407	561	772	527	236	311	317	431	429	261	156	213	43	329	74	117	231	195	179	135	121	80	35	84	45	47	32	70	46	35	8	31	30		
30	30	###	###	###	###	###	670	624	882	256	251	352	443	369	191	221	199	278	280	228	80	164	55	201	81	87	114	122	79	73	94	50	24	71	30	32	31	42	36	37	5	29	29	
40	40	###	###	###	###	###	982	494	449	572	277	235	286	288	256	215	220	180	180	208	168	54	113	49	124	90	87	114	75	57	58	71	43	21	49	33	36	33	25	30	31	3	39	25
50	50	###	###	###	###	###	792	451	390	420	280	187	247	203	213	229	235	183	178	156	140	36	84	69	125	85	79	77	66	54	50	53	54	20	32	28	27	29	37	42	31	7	33	19
60	60	###	###	###	###	###	494	292	266	283	256	135	173	116	153	94	118	78	126	99	115	42	65	15	92	85	50	54	52	30	41	35	23	19	24	27	26	14	21	12	9	16	15	
70	70	828	###	959	341	244	192	208	258	124	131	92	97	69	109	84	104	76	99	38	62	45	7	66	57	29	43	30	23	25	37	45	13	16	14	26	14	14	13	8	8	13	27	
80	80	729	###	###	329	184	186	180	261	109	130	84	95	57	92	82	76	68	92	38	29	12	57	60	38	30	23	29	26	17	28	24	19	14	24	17	8	7	8	8	7	13		
90	90	677	955	###	269	163	148	137	242	87	133	77	75	72	92	84	64	51	84	32	41	15	58	53	35	39	26	25	19	12	30	20	16	12	24	12	9	7	7	11	4	8		
100	100	586	940	###	265	194	130	134	218	76	122	74	84	99	98	70	64	58	30	39	15	55	52	38	33	28	23	16	21	25	14	12	18	13	15	16	7	15	5	13				
110	110	588	807	999	259	168	113	91	262	65	110	71	70	98	101	71	52	41	68	42	34	16	38	53	61	33	20	24	20	18	24	22	16	14	23	19	9	17	11	17	4	13		
120	120	516	788	###	229	187	108	98	247	62	111	50	74	115	126	79	48	46	54	44	41	38	26	65	40	23	16	16	22	17	19	19	13	14	18	16	9	15	9	9	8	17		
130	130	465	646	###	182	146	109	84	217	50	97	43	54	90	95	81	34	33	72	41	38	19	20	42	50	31	16	8	19	9	27	21	9	15	15	20	8	16	12	18	4	11		
140	140	416	610	###	138	137	89	51	211	47	97	47	47	84	104	59	32	22	61	48	41	22	16	52	44	17	13	10	14	11	20	29	12	8	18	15	7	4	13	20	3	9		
150	150	386	550	900	132	157	78	60	193	46	72	39	46	86	83	70	33	23	66	45	18	31	28	51	56	19	14	9	7	5	14	20	9	15	13	18	13	13	11	19	5	12		
160	160	333	519	869	113	134	87	41	166	50	66	27	36	89	77	49	33	23	53	32	25	29	27	47	35	11	11	15	12	8	15	20	7	5	12	28	8	6	7	24	11	10		
170	170	308	483	765	96	110	60	42	151	26	61	23	44	78	48	34	24	19	37	42	26	25	23	48	32	13	12	9	14	7	19	21	11	8	10	12	5	9	8	15	18	9		
180日	180	297	375	801	73	113	53	33	162	26	73	22	22	75	42	49	23	19	37	34	35	39	13	52	31	14	4	6	11	9	13	18	10	6	10	13	4	11	9	18	4	5		
190	190	289	408	719	75	90	58	34	119	25	46	22	21	99	54	51	24	15	15	36	35	24	15	52	31	7	8	6	5	13	20	18	4	12	7	15	10	5	8	20	7	11		
200	200	269	354	671	53	93	45	30	121	33	55	13	16	112	60	39	21	15	29	40	27	8	28	33	8	5	7	13	7	12	26	4	7	5	13	11	7	14	24	1	8			
210	210	267	294	695	48	105	46	28	122	24	56	14	22	107	58	40	16	6	41	32	26	10	31	22	6	3	7	5	6	9	22	4	4	6	10	3	5	11	18	2	5			
220	220	274	274	703	37	83	61	23	112	15	52	15	26	89	54	65	12	10	32	41	39	6	38	39	3	2	7	8	6	11	17	5	10	6	6	5	5	15	26	6	5			
230	230	270	288	680	33	85	52	14	126	25	43	14	10	111	47	49	15	17	31	34	37	9	36	40	9	4	6	5	5	12	27	5	9	8	15	4	9	15	16	6	10			
240	240	295	262	693	45	105	65	13	112	21	39	17	17	80	44	47	9	16	35	21	61	12	45	46	8	4	2	3	5	10	33	9	10	9	11	4	5	9	18	12	3			
250	250	354	368	764	38	128	60	15	130	13	43	13	31	85	55	47	25	12	45	28	69	10	48	46	5	2	2	8	4	9	24	7	6	6	7	11	6	11	20	12	15			
260	260	311	248	729	23	116	60	8	124	17	34	8	17	94	48	73	11	16	50	10	81	5	42	46	3	3	9	2	8	30	6	6	5	13	7	9	14	17	8	12				
270	270	269	239	641	31	128	49	6	74	24	32	5	18	90	44	39	16	12	36	8	88	11	39	49	4	4	1	11	3	9	35	6	9	2	9	7	4	12	21	5	2			
280	280	274	233	571	19	118	58	11	100	18	34	5	12	66	48	62	16	6	38	4	79	9	41	46	3	3	2	4	8	7	25	2	3	2	12	5	4	10	15	7	8			
290	290	192	193	475	9	98	53	5	67	15	28	4	7	38	28	43	8	11	39	3	65	3	31	42	4	4		2	3	22	3	2	2	12	3	5	6	14	14	8				
300	300	201	178	437	5	73	52	9	61	11	26	1	7	29	15	40	12	3	26	4	58	3	26	32	3	1	5	8	4	7	17	4	2	2	11	2	5	8	6	8				
310	310	142	142	396	3	77	27	5	50	6	20	4	8	28	17	38	2	4	24	6	49	2	23	19	1	1	4	1	3	11	5	3	5	6	3	9	6	16	6	3				
320	320	176	150	482	9	69	38	7	40	6	17	2	9	37	21	29	5	3	22	7	55	5	21	23	4		1	3	2	2	21	1	3	1	10	1	3	10	17	23	2			
330	330	266	161	531	9	113	50	5	45	9	21	7	10	50	23	37	5	4	34	13	95	2	40	43	3	3	2	3	2	6	17	7	1	4	6	3	6	10	23	8	4			
340	340	274	190	477	11	106	51	5	38	11	26	5	8	42	30	45	8	2	30	3	121	4	48	41	5	1	3	3	1	3	28	7	2	2	19	4	4	11	17	24	6			
350	350	340	191	461	9	129	69	2	39	12																																		

RESIPデータの分析(911S5 : JSAC2022)

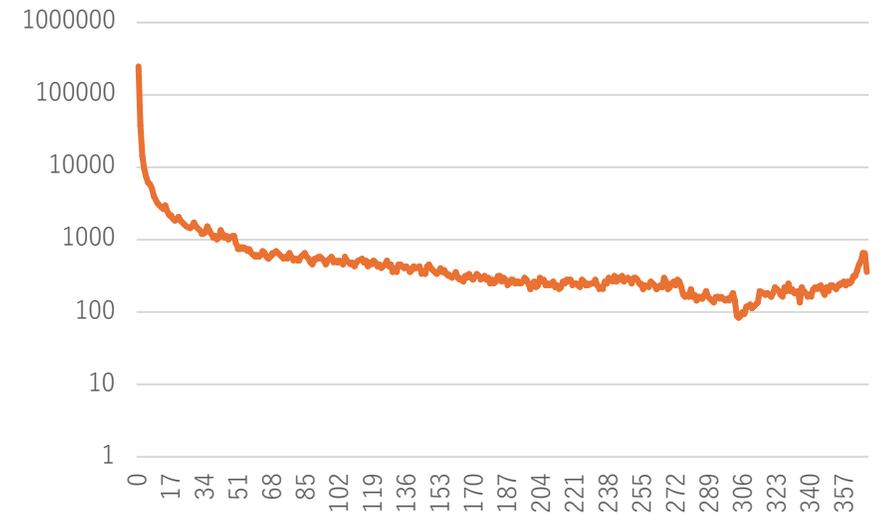
- IPごとの生存期間 ($\text{date_diff} = \text{last_seen} - \text{first_seen}$)
- **5割のIPが1日しか出現しない。**

RESIPの生存期間



n=507546

RESIPの生存期間



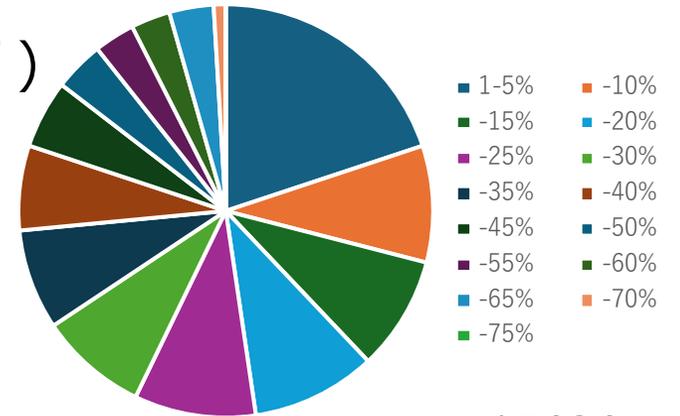
RESIPデータの分析(911S5 : JSAC2022)

- 長期活動が観測されるIPにおけるアクティブ率 (days / date_diff)

days 出現が観測された日数

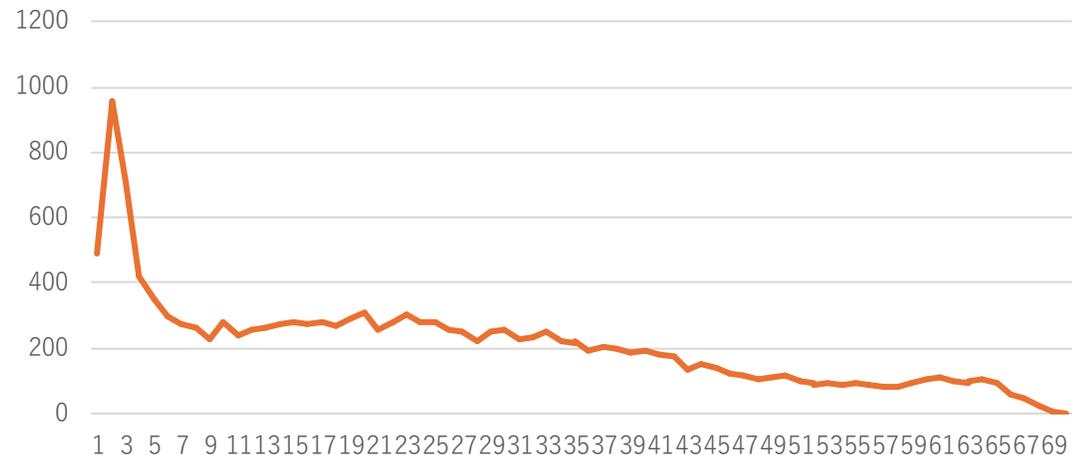
生存期間が 300日以上に対して分析

約30% が観測日数が30日以下



n=15424

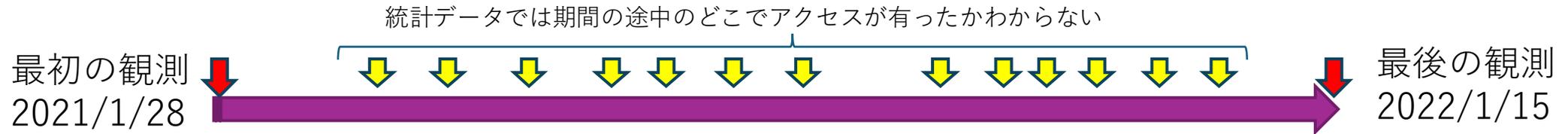
→ **長期間生存するIPであったとしても、常に悪性とは限らない**



RESIPデータの分析(911S5 : JSAC2022)

- IP統計データの問題点

ip_address	days	first_seen	last_seen	date_diff
222.8.74.188	19	2021/1/28	2022/1/15	352

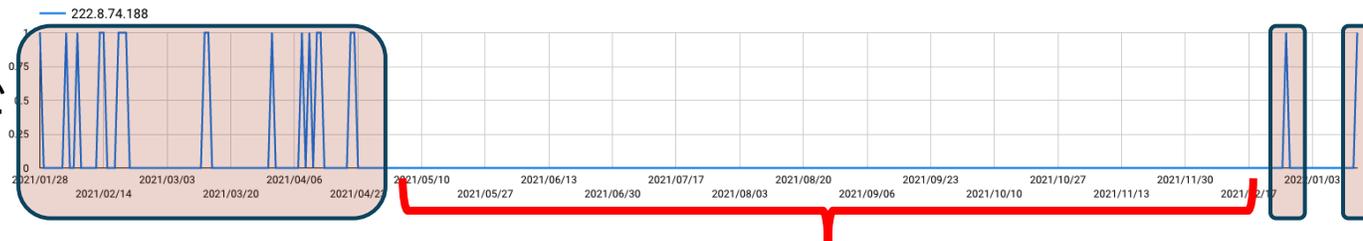


- Livefeedとの突合は役に立つ。**

(現在の攻撃と24時間以内のデータとの突き合わせ)

- 過去のインシデント分析において、**IP統計データでは不正発生時点でのプロクシかどうかを判定できない。**

- 取得時の生データ



RESIPとの関連性強い

この間に事件があっても、RESIPとの関連性が弱い

行	unixtime	ip_address	date
1	1611795448	222.8.74.188	2021-01-28
2	1611795506	222.8.74.188	2021-01-28
3	1612429028	222.8.74.188	2021-02-04
4	1612652208	222.8.74.188	2021-02-07
5	1613188622	222.8.74.188	2021-02-13
6	1613285815	222.8.74.188	2021-02-14
7	1613620622	222.8.74.188	2021-02-18
8	1613689001	222.8.74.188	2021-02-19
25	1619013394	222.8.74.188	2021-04-21
26	1619062088	222.8.74.188	2021-04-22
27	1619087685	222.8.74.188	2021-04-22
28	1640564592	222.8.74.188	2021-12-27
29	1640566119	222.8.74.188	2021-12-27
30	1640568210	222.8.74.188	2021-12-27
31	1640568212	222.8.74.188	2021-12-27
32	1642212280	222.8.74.188	2022-01-15

レジデンシャルプロキシとは

- 悪の利用法：

Ad Fraud

不正アクセス

複垢

SNSスパム

DDOS

詐欺

- 意図した利用法：

グレートファイアウォール回避

ターゲティング広告のチェック、SEOチェック

スクレイピング・データ収集

- 競合価格調査

- AIエージェントのアクセス

- AI学習データの収集

プロキシ出口ノードを観測する。
通常の通信が多数発生。

正規利用法の一つ

深刻な問題になりつつある

スクレイピングとコンテンツ保護

- **米国:** *Meta v. Bright Data* 判決。2024年「認証なしの公開データ収集」は契約違反に当たらない（適法）。
- **著作権法30条の4:** AI学習・情報解析目的のスクレイピングを明示的に許可（世界的優位性）。

プラットフォームにとって、スクレイピングはビジネス阻害要因。しかし、スクレイピングを防ぐには自己防御する必要があり。一方、データ取得側はレジデンシャルプロキシを用いて取得。プラットフォーム側の対策を困難に。

911帝国の滅亡

- 2022以前は「911 S5」が市場を支配していた
- Krebsによる記事を受け、突然サイトを閉鎖(2022)
- 国際捜査によって運営者は逮捕 (2024)



PRESS RELEASE

911 S5 Botnet Dismantled and Its Administrator Arrested in Coordinated International Operation

Wednesday, May 29, 2024

For Immediate Release
Office of Public Affairs

We regret to inform you that we permanently shut down 911 S5 services on July 28th.

For the past 2 years, 911 S5 has been the target of global law enforcement agencies. They closed the front end and back end, registered hundreds of similar domains and established websites, placed paid search ads on search engines, and social media. When 911 S5 users log in to the phishing website, they used our login credentials, and even asked you to give the account number of your account. For further use of our 911 S5 account (if you recharge on the phishing website, your recharge will also be stolen). These stolen accounts can be used for illegal use and draining our group account. When it comes to the 911 S5, about the already occurred, and account balances have been stolen.

911 S5 would not have any intention for legitimacy and about our proxy network. Over the years we have been thousands of accounts for violating our terms of service. We actively follow up on any abuse complaints we receive. We also assisted the German and Polish police in handling some more things. Our intention is to provide our program and tools to help you to avoid domains and websites that are not yours, such as selling your own information to third parties, etc. We are responsible for the 911 S5 network. But it is not our goal to provide many services unless the accounts are used for program. For example, it is not using a proxy to visit another site for shopping, it is difficult to determine whether the user is logged in with his own account and whether he is using his own bank card to pay. But if we think these things are not other normal users. Therefore, in order to increase the security level of selling, it is not impossible, and some users are required to manually analyze all user behaviors. But this is a huge challenge for us, and the cost is too high and ability. This is one of the main reasons why we decided to shut down the service.

The most unfortunate thing is that our recharge system was hacked in early July, and it was found that someone manipulated the balance of a large number of our accounts by using the API of the recharge system. Our team now did the hacker get in. Therefore, we urgently shut down the recharge system, new user registration and activation started.

On July 28th, a large number of users reported that they could not log in to the system. We found that the user on the server was maliciously changed by the hacker, resulting in the loss of data and business. After analyzing the investigation by the SOC, we found that the hacker first invaded the SargNet server through a new version vulnerability. The historical records sent by the SOC contain the log and password of the account 911 S5 users. As a consequence of the SOC's findings, the hacker reported the server and hacked the API through a company. The further invasion, he confirmed that the recharge system was also hacked the same way. We were forced to make the difficult decision due to the loss of important data that made the service unworkable.

Sorry to hear goodbye to everyone. 911 S5 would like to thank you all for your continued support and trust over the years.

Finally, please note that the shutdown of 911 S5 is permanent. But after we shut down the service, the console who do phishing attacks may still use their own activities. They use our the new website listed below to pretend to be us, continue to trick people into using them.

date	cnt_ip
2022/7/21	19656
2022/7/20	25696
2022/7/19	26281
2022/7/18	26811
2022/7/17	26042
2022/7/16	26484
2022/7/15	21669
2022/7/14	25040
2022/7/13	25003
2022/7/12	23953
2022/7/11	24242
2022/7/10	24082
2022/7/9	24047
2022/7/8	24348
2022/7/7	23752
2022/7/6	24290

<https://krebsonsecurity.com/2022/07/a-deep-dive-into-the-residential-proxy-service-911/>
<https://krebsonsecurity.com/2024/05/treasury-sanctions-creators-of-911-s5-proxy-botnet/>

閉鎖直前、**1日あたり国内で24000IP程度観測**

911は滅亡後、Proxyサービスが爆増

- 「911 S5」閉鎖後、蜘蛛の子を散らすようにユーザーが分散
- After 911 S5 shut down, users dispersed across many services
- その結果、プロキシ出口のモニタリングが困難になった
- Monitoring Proxy Exit Nodes Has Become Difficult

 IPIDEA

 ABC S5 PROXY

 S5Proxy®

 PIA S5 Proxy®



一部のサービスは911の代替品であることを明確にPRして集客。
Some services openly promote themselves as replacements for 911.

レジプロを取り巻く最悪な状況

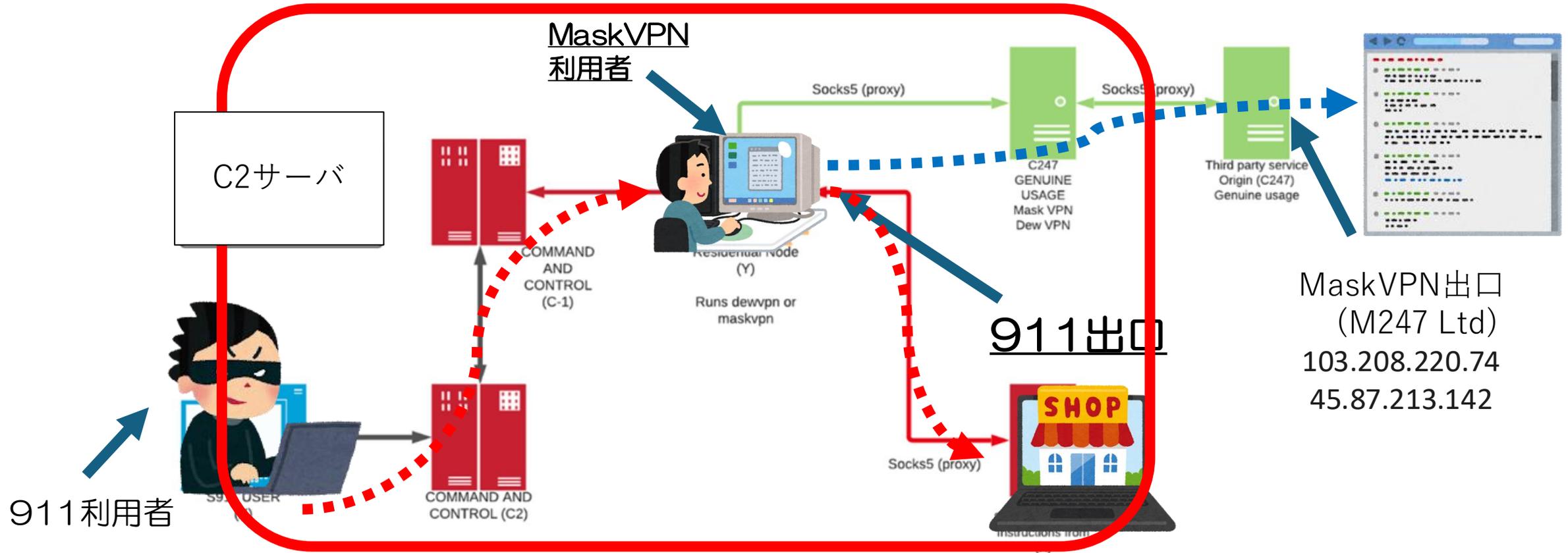
The Hopeless Crisis Surrounding Residential Proxies

入口／出口の分断
取得経路の多様化（STB/SDK）
ノード数の爆発
匿名支払い／ログなしポリシー
地域偽装・レート回避が標準機能

Fragmentation of entrance and exit layers
Diversified acquisition channels (STB, SDK, etc.)
Explosive growth in the number of nodes
Anonymous payment & no-log policies
Geo-spoofing and rate-limit evasion as standard features

911のサービス構造

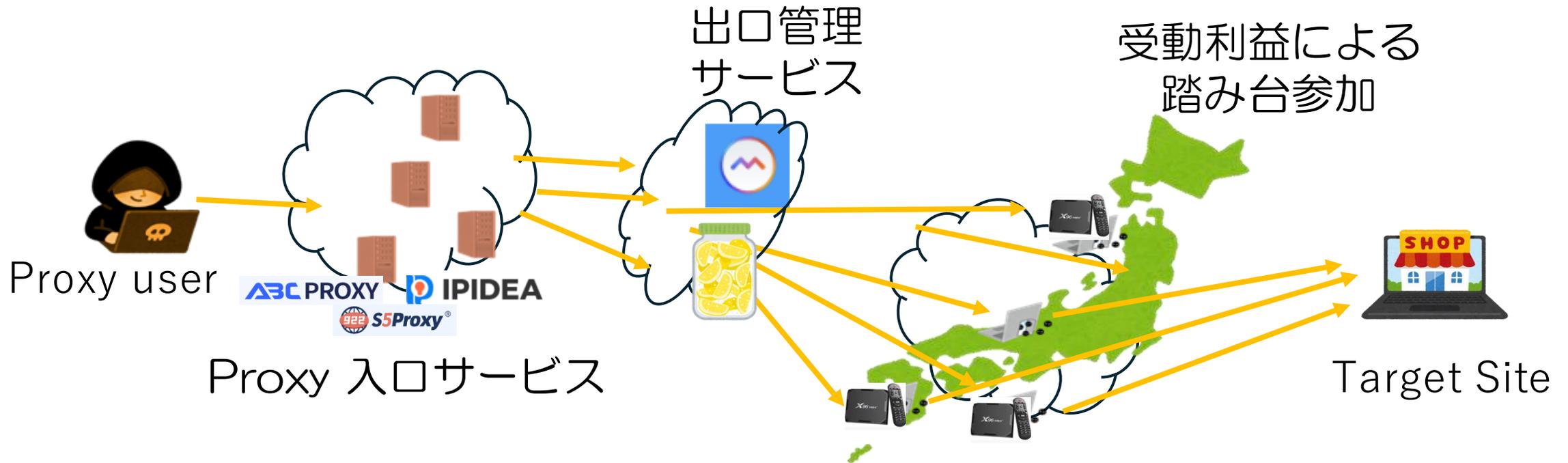
同一企業 (Krypt technologies) によって管理



<https://krebsonsecurity.com/2022/07/a-deep-dive-into-the-residential-proxy-service-911/>

F. M, P. Plante, and G. Joly. Illegitimate residential proxy services: the case of 911.re and its iocs, <https://gric.recherche.usherbrooke.ca/rpaas/>

レジデンシャルプロキシの3層アーキテクチャ



入口サービスと出口管理サービスが別企業にすることで、責任の所在を不明瞭に、より潰しにくくなった・・・

出口IPの取得

・ 出口IPは倫理的な取得、グレーな手法、不正な手段で取得するプロバイダーが混在

正規：

ISPとのパートナーシップ、プロバイダーとの契約

ユーザーのオプトイン：

ユーザーのオプトイン

ユーザーへの報酬アプリのインストール

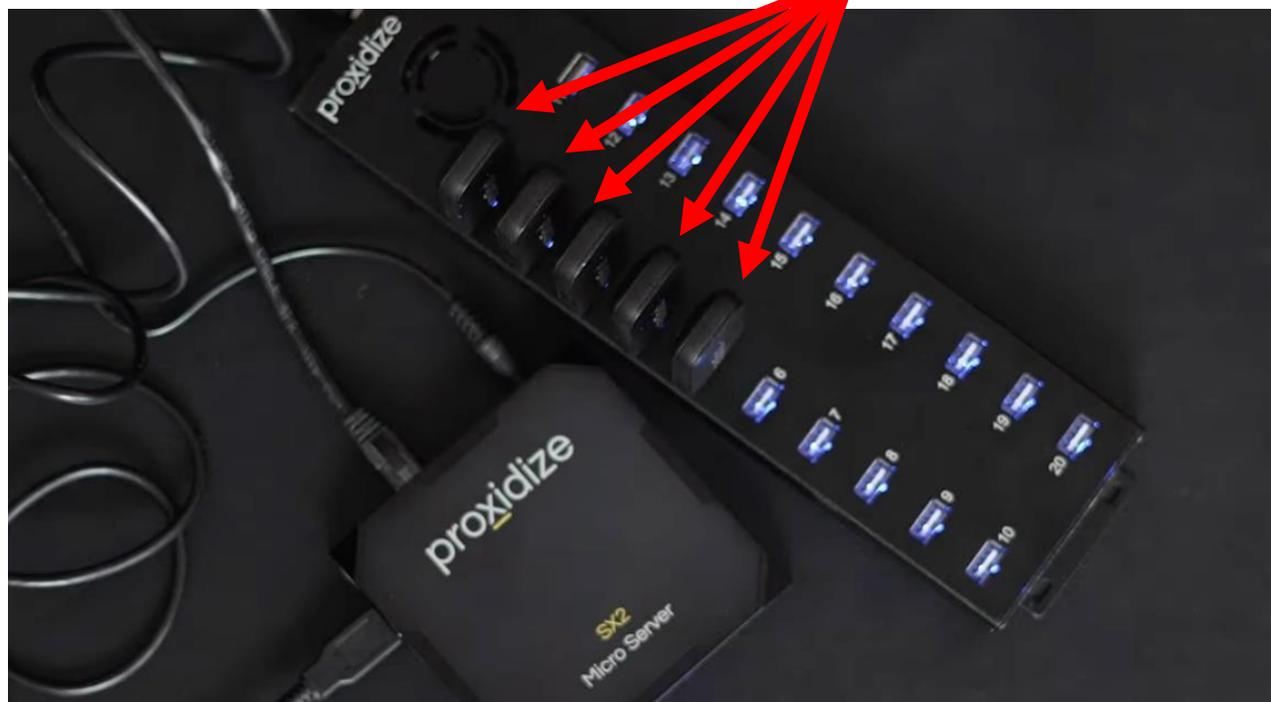
不正な手段：ユーザーに気が付かずに勝手に踏み台に

フリーウェアのバンドル、SDKによるアプリ組み込み
Browser Extension (開発者による組み込み？ 見たことないが・)
IoT機器のハッキング、著作権違反ソフトのバンドル、
STB組み込み、違法動画ソフト

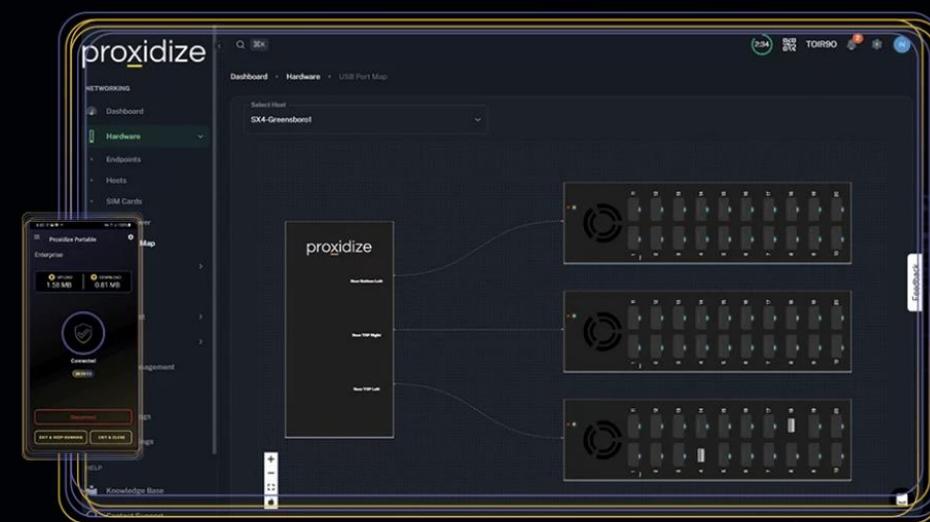
正規 Legitimate Methods:

- プロキシ専用のUSBデバイスにモバイル回線モデムを大量に接続
- Deploy multiple mobile broadband modem dongles on a USB-hub-based dedicated proxy device to provide scalable upstream connectivity.

USB-Modem



Centralized Management Solution



ユーザーのオプトイン：受動利益

- **P2P（ピア・ツー・ピア）エコノミーモデル** だから倫理的であると主張
- ユーザーが自身のデバイスにアプリケーションをインストールし、未使用の帯域幅（Bandwidth）をプロキシネットワークに提供することに同意。
- **パッシブインカム：Honeygain、PacketStream、GrassNetwork、IPRoyal Pawns**などのサービスでは、ユーザーのインターネット接続を共有する対価として、共有したデータ量（GB単位）に応じた報酬を受け取ります。



完全放置で1日数十円稼ぐHoneygainの始め方【月に2000円近くの不労所得を作る】



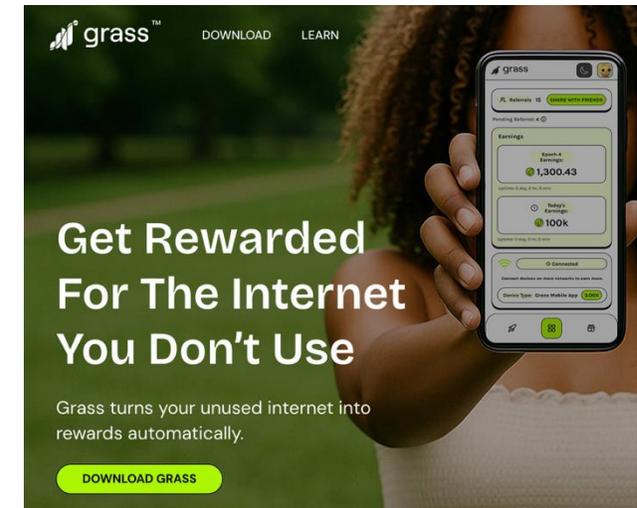
honeygain

Download Ref

Excellent ★★★★★ 22,888 reviews on ★ Trustpilot

Earn money online effortlessly with Honeygain

Start earning with Honeygain just by sharing your connection - no extra effort needed. Join now and get a \$2 starting gift!



grass

DOWNLOAD LEARN

Get Rewarded For The Internet You Don't Use

Grass turns your unused internet into rewards automatically.

DOWNLOAD GRASS

https://note.com/hon_ahir/n/ne561d1a14a20

ユーザーのオプトイン：受動利益

出口ノードの運用は通信事業者に該当するのでは？

A. 「他人の通信の媒介」への該当性

- 出口ノードは、第三者の通信リクエストを受け取り、それを宛先に転送し、返答を戻す役割を果たす。これは明確に「通信の媒介」に該当します。

B. 「業として（事業性）」の判断

- 出口ノード提供者（個人）：
 - **反復継続性:** アプリを常駐させていれば「反復継続」しています。
 - **営利性:** 金銭の対価を得ているため、営利性が認められる可能性があります。

ユーザーのオプトイン：価値交換モデル

・価値交換モデル（SDK統合）—無償アプリのマネタイズ—

アプリ開発者向けにSDKを提供。
開発者は、自身の無料アプリ（ゲームやユーティリティツールなど）にこのSDKを組み込みます。ユーザーがアプリを利用する際、「広告を非表示にする」「プレミアム機能を開放する」といった特典と引き換えに、デバイスの帯域共有にオプトイン（同意）します。これにより、開発者は広告を表示することなく収益化が可能となり、プロバイダーは安定したIPプールを確保できます。

ユーザーのオプトイン：価値交換モデル

- **論点：**
有効なユーザーの同意を取得しているのか？同意したとしても、ユーザーは犯罪の幫助になることまで認識していないのでは？
- 悪名高き 911 S5もオプトインでノードを取得したと主張。
(実際はmaskvpn, proxygateがバンドルでインストールされていた)

SCAMS, THREAT INTEL

Fake 7-Zip downloads are turning home PCs into proxy nodes

by Stefan Dasic | February 9, 2026

CyberCrime Control Project

令和3年 第1号

広島県警察本部
サイバー犯罪対策課
082-228-0110
(内線 705-586)

— 知らないうちに踏み台に —

インターネット上には、便利なソフトウェアがたくさんあり、中には無料でダウンロードできるものもあります。しかし、無料でダウンロードしたソフトウェアをインストールした際に、**利用者の知らないうちに、踏み台として利用されるアプリケーションソフトウェア（踏み台アプリ）も同時にインストールされてしまい、不正アクセス等の犯罪に悪用される事例が多発しています。**
不正なプログラムがインストールされていないかを今一度確認しましょう。

踏み台とは 第三者に乗っ取られた状態のコンピュータやサーバのこと

【踏み台にされたしまった場合の一例】 ※無料でダウンロードできるソフトウェアに踏み台アプリが仕込まれている場合が多い

攻撃者が作成又は改ざんした Webサイト

アクセス

無料ダウンロード

攻撃者は、踏み台となったパソコン等を経由して攻撃をする

本正アクセス

問題のある中華製 Set Top Box

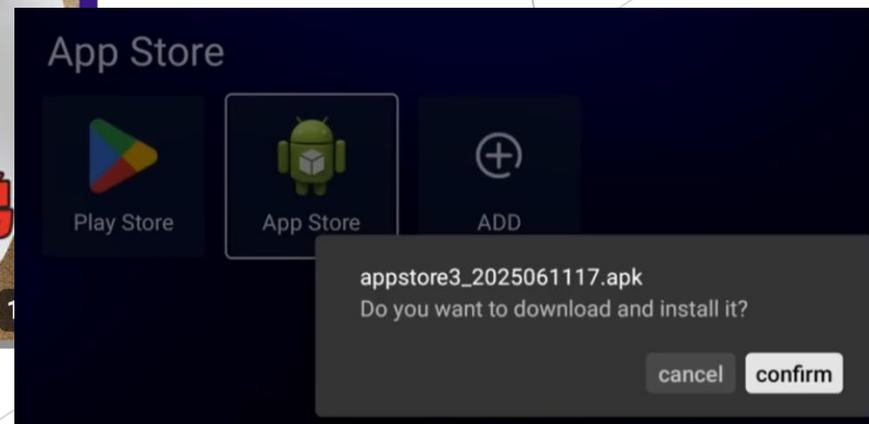
- BADBOX 出荷時のOSに組み込みで悪性プログラムがインストールされていた。
- STBを調査、出荷時にオリジナルAppストアが同梱、アプリインストールの手順が同梱。有料動画が無料で見られるとしてユーザーを獲得。裏でプロキシが動作する仕組み (調査中) デバイス事業者は「あくまでインストールするのはユーザーの責任」と主張。



Digibox D3 Plus スマートテレビボックス Androidプレーヤー アメリカのスポーツや世界中の映画を楽しむWiFi 6対応...

3.8 ★★★★★ (187)
過去1か月で300点以上購入されました

¥33,830 過去: ¥39,800

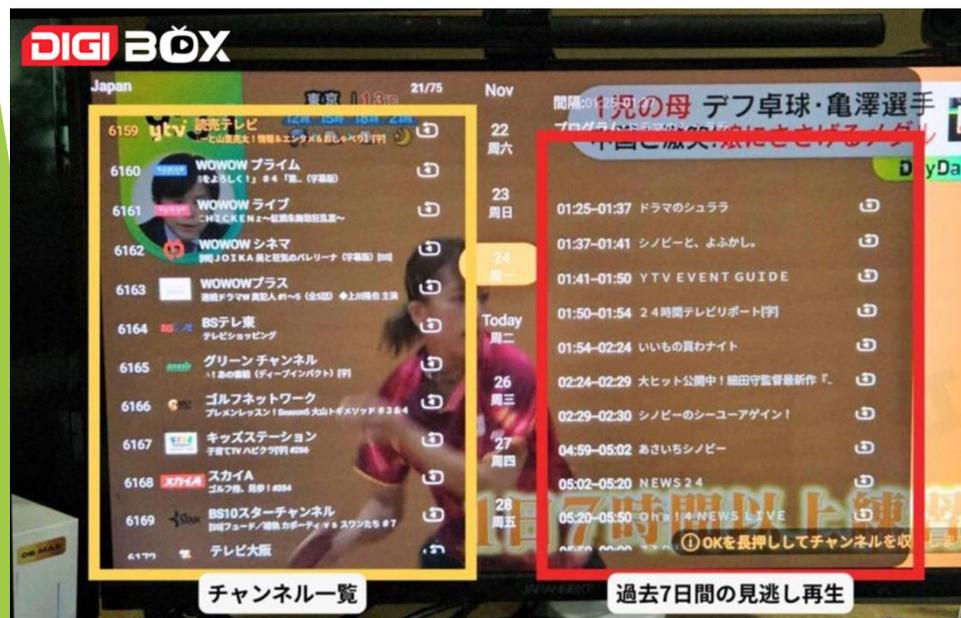


問題のある中華製 Set Top Box

- 利用ユーザーとしては「永久無料で有料番組を見ることができる」という強力なインセンティブに突き動かされ、購入、利用。
- あくまでストリーミングであるため、違法でないと主張。
- 日次でドンドン広まっている状況。早急に販売を禁止できるようにしないと、手が打ちようない・・・

[Digibox D6 MAXレビュー](#)

https://www.youtube.com/watch?v=0AU_B7XaB1A&t=190s



全く新しいDIGIBOX D6 MAX | 2026年版 究極のAndroid TV Box グローバルエンターテイメント

DIGIBOX D6 MAX

- 一度支払えば、月額料金はかかりません！高額なケーブルテレビ料金の支払いはもう終わりです。
- 3,000以上のプレミアムDIGIBOXチャンネル。
- 40,000以上の映画とテレビ番組 (VOD)。
- キッズ&アダルトチャンネルもご利用いただけます。
- 最高のスポーツストリーミングサービスデバイス。ライブスポーツチャンネルを無料で視聴できます。
- より安定しており、常に99.99%の稼働率。
- 100%正規品保証。100%満足保証。
- 世界中への送料無料。ユニバーサルバージョン。

STB分析

- ▶ STBとC2サーバー間の暗号化された接続と5秒間のハートビートが観測されました。調査対象となったボックスはすべて、CloudFlareの背後にあるC2サーバーに接続していました。
- ▶ signal.googol(.)comやdata-google(.)comといったドメインを使用することで、悪意のある動作を難読化する試みが少なくともいくつか見られます。
- ▶ 観測されたドメインはすべて過去24ヶ月以内に登録されているため、2年ごと、あるいはそれより短い期間でローテーションされていると考えられます。

Pls input the PSW of ^_^

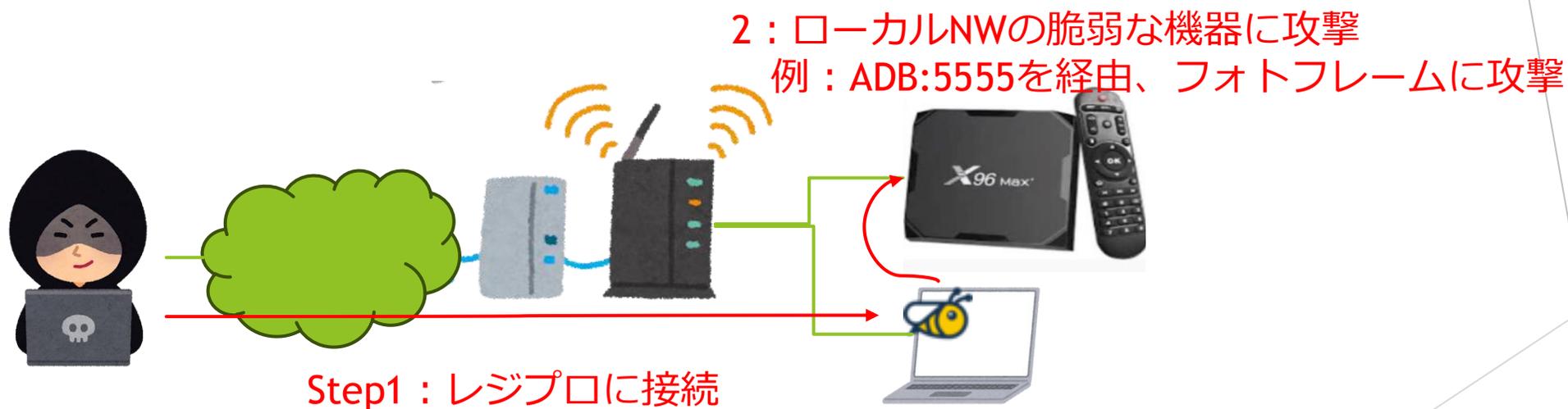
The English is machine translated using older systems, resulting in occasionally fascinating wordings

Confirm exit

think about it again

出口を経由したローカルネットワークへの侵入

- ▶ プロキシ出口経由でローカルNWへアクセスできる。
Kimwolf ボットネットにより、出口ノード経由でさらに大量のプロキシが生成



<https://krebsonsecurity.com/2026/01/the-kimwolf-botnet-is-stalking-your-local-network/>

<https://www.quokka.io/blog/major-security-issues-digital-picture-frames>

<https://synthient.com/blog/a-broken-system-fueling-botnets>

海外の状況

- NANOG 94 (2025/06開催)ではすべてのセッションがプロキシ
<https://nanog.org/events/nanog-94/agenda/>
- 安全保障上の問題、セキュリティ侵害の利用などにより、海外ではすでに大きな問題になっている。

  **Security Track: Technical Deep Dive into Residential Proxies**
Ryan Mechem

  **Security Track: Crimes within a Crime: Illicit residential proxy services and cybercriminal enablement from a law enforcement perspective**
Ryan Bradbury - Defense Criminal Investigative Service

  **Security Track: ORBs - How a new method of proxy chains are eluding security teams**
Scott Fisher - Team Cymru

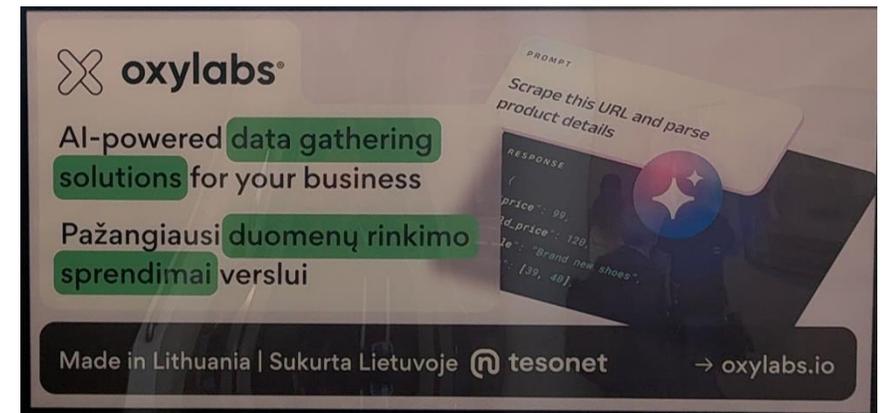
  **Security Track: Trojan Tunnels: Abuse Behind the Promise of Passive Income**
Riley Kilmer - Spur Intelligence

  **Security Track: North American Residential Botnet and Proxy Infrastructure**
Craig Labovitz - Nokia

  **Security Track: Panel on Criminal Proxies**
Krassimir Tzvetanov - Hydrolix / Purdue University
Ryan Bradbury - Defense Criminal Investigative Service
Chris Formosa - Lumen
Ryan Mechem
Sean Simmons
Scott Fisher - Team Cymru

海外の状況

- レジプロは帯域を販売する商売。AIによるニーズを受けて、いろいろな会社がプロキシ事業に参入。
(AIニーズの後押し。データ収集ソリューションとして空港に広告。グレービジネスからホワイトビジネスへの転換)
- DDoSより攻撃性が低いため、健全な事業を装って、ボットネットをマネタイズできる状況になってきた。
(1GB 数ドル)



International Situation—海外の状況—

1月上旬：

Operation to Disrupt Proxy Botnets by Black Lotus Labs, SPUR, and Synthient /Registrar of Last Resort Foundation (RoLR) and Shadowserver Foundation

対策として上記のオペレーションが実施。Ipmoyuに対するテイクダウン。

ウォール・ストリート・ジャーナル日本版から

+フォロー

グーグルが中国企業に致命的打撃、大規模サイバー兵器に関連

ウォール・ストリート・ジャーナル日本版

2026年2月9日



Google、世界最大級の悪性プロキシ「IPIDEA」を無力化 数百万台のデバイスを解放

© 2026年01月30日 06時58分 公開

[!Tmedia]

1月下旬

- ipidea系サービス（フロントサービス）のドメインがテイクダウン。いくつかのサービスは停止したが、サービスが復活したところもある。（バックエンドのインフラは死んでない）



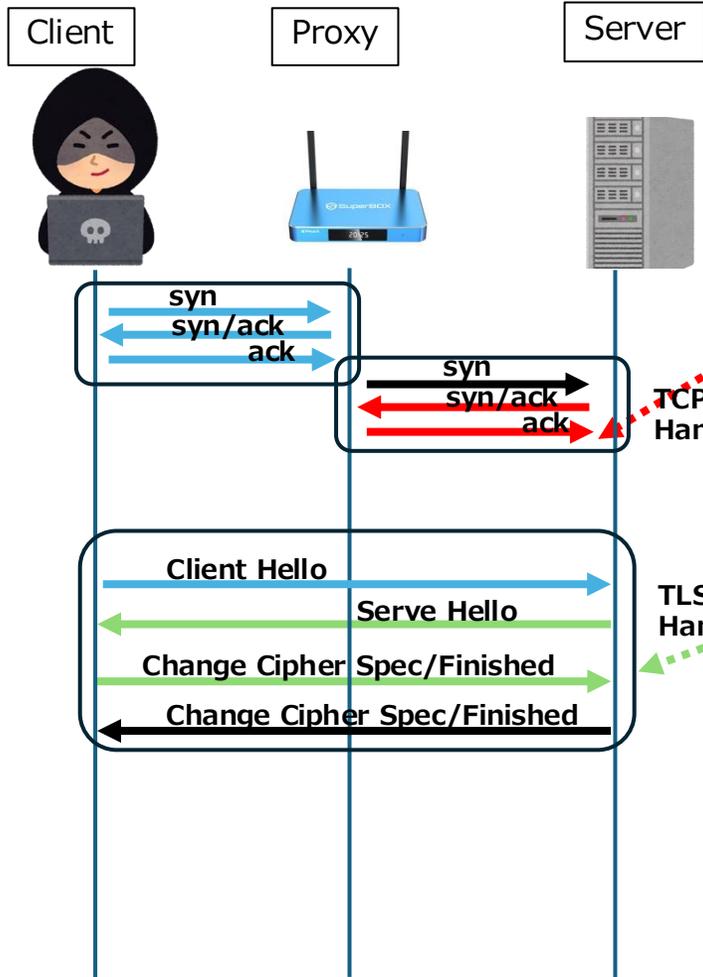
レジデンシャルプロキシ対策の検討

- パケットフィンガープリンティングの活用(企業側での対策)
- 出口IPアドレス収集／出口ノードの観測
- DNS シンクホール／NULL ルーティングキャンペーン(ISP/オペレーターレベル)／C2ドメインテイクダウン

パケットフィンガープリンティングでの検出(企業側での対策)

Packet Fingerprinting Techniques (Enterprise Detection)

Use JA4L and TCP/TLS response-time patterns to estimate proxy-like behavior



a) TCP syn/ack → ack の時間を測定
(サーバ<->プロキシ)

120655_51_302067
120181_51_309496

c) ServerHello→Client Finishedの時間を測定
(サーバ<->クライアント)

プロキシ利用で
違いが発生

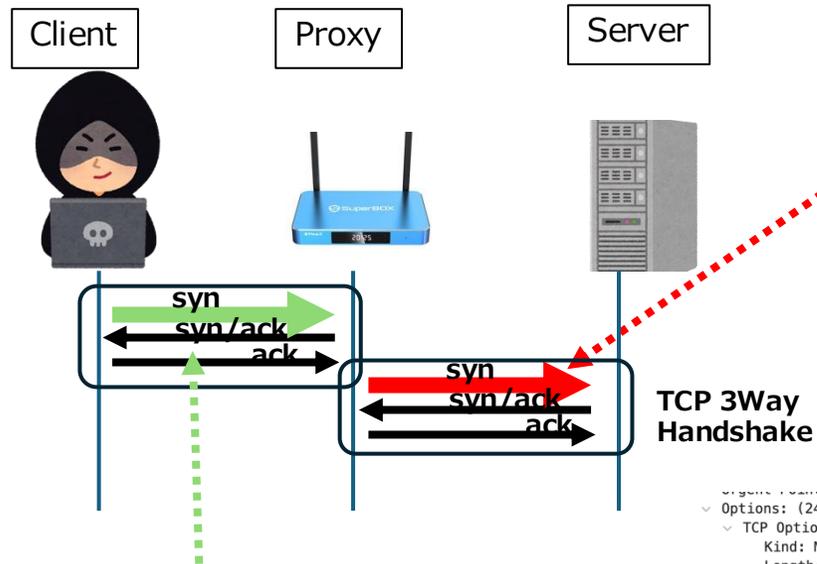
brows	proxy	回数	ja4l	abs(a-c)
chrome	プロキシなし		239_63_753	514
chrome	プロキシなし		15087_46_12293	2794
chrome	プロキシなし		15187_48_12378	2809
chrome	iproyal	1回目	120655_51_302067	181412
chrome	iproyal	1回目	120181_51_309496	189315
chrome	iproyal	2回目	88405_115_229545	141140
chrome	iproyal	2回目	19999_47_305245	285246
chrome	iproyal	3回目	97037_114_495422	398385

brows	proxy	回数	ja4l	abs(a-c)
chrome	プロキシなし		239_63_753	514
chrome	プロキシなし		15087_46_12293	2794
chrome	プロキシなし		15187_48_12378	2809
chrome		922 1回目	12351_53_283844	271493
chrome		922 1回目	9948_53_227509	217561
chrome		922 2回目	11023_53_218652	207629
chrome		922 2回目	9891_53_218073	208182
chrome		922 3回目	21036_53_284776	263740
chrome		922 3回目	9928_53_218318	208390

パケットフィンガープリンティングでの検出(企業側での対策)

Packet Fingerprinting Techniques (Enterprise Detection)

Proxy routing alters TCP parameters (e.g., MSS, window size), causing JA4T fingerprints to differ from the client's real device fingerprint



プロキシ経由のJA4T Fingerprint

65535_2-4-8-1-3_1382_6
65535_2-4-8-1-3_1414_6

MSS decreases when routed through a proxy.

Macで直接アクセスした時の JA4T Fingerprint

65535_2-1-3-1-1-8-4-0-0_1460_6

```
Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window
  TCP Option - Maximum segment size: 1460 bytes
    Kind: Maximum Segment Size (2)
    Length: 4
    MSS Value: 1460
  TCP Option - No-Operation (NOP)
    Kind: No-Operation (1)
  TCP Option - Window scale: 6 (multiply by 64)
    Kind: Window Scale (3)
    Length: 3
    Shift count: 6
    [Multiplier: 64]
  TCP Option - No-Operation (NOP)
    Kind: No-Operation (1)
  TCP Option - No-Operation (NOP)
    Kind: No-Operation (1)
  TCP Option - Timestamps: Sval 390880287, TSecr 0
    Kind: Time Stamp Option (8)
    Length: 10
    Timestamp value: 390880287
    Timestamp echo reply: 0
  TCP Option - SACK permitted
    Kind: SACK Permitted (4)
    Length: 2
  TCP Option - End of Option List (EOL)
    Kind: End of Option List (0)
  TCP Option - End of Option List (EOL)
    Kind: End of Option List (0)
```

JA4T - TCP Client Fingerprint Examples	
OS / Device	JA4T
Windows 10	64240_2-1-3-1-1-4_1460_8
Ubuntu 22.04 on Win10 WSL	64240_2-4-8-1-3_1460_7
AWS Windows Server 2022	62727_2-1-3-1-1-4_1460_8
AWS Unix	62727_2-4-8-1-3_1460_7
AWS Unix (internal)	62727_2-4-8-1-3_8961_7
Android 12	42600_2-4-8-1-3_1460_12
Android 13	65535_2-4-8-1-3_1460_9
OSX/iOS (all versions)	65535_2-1-3-1-1-8-4-0-0_1460_6

検出できない方式

1. 外部スキャンはカバーできない

- レジデンシャルプロキシは 家庭用ルータ/ファイアウォールの内側に存在する。
- そのため Shodan など外部スキャンサービスでは検出できない。

2. IPレピュテーションDBも微妙

- RESIP の特徴は、家庭用のクリーンな正規IPに偽装すること。
- 鮮度の高いリアルタイムなIPフィードを提供するサービスでなければ、検出は困難。
 - 統計データは賞味期限切れ
 - ライブデータでないと役に立たない

Conclusion : プロキシとの戦いは終わりが見えない まだ続く・・・ **To be continued**.....

レジデンシャルプロキシは、入口・出口・管理の分断により、従来の対策では捉えきれない“新しい匿名化インフラ”へ進化した。

STB / Passive Income / SDK / IoT など、出口ノード獲得手法の多様化と爆発的增加により、状況は悪化し続けている。

プロキシを利用した攻撃（不正送金・詐欺・情報窃取・ローカルNW侵害）は既に日常化し、国家・企業レベルのリスクとなっている。

これに対抗するためには、研究者・ISP・企業・法執行が連携したエコシステム全体での対処が必須。