

# Disrupting the World's Largest Residential Proxy Network

---

 [cloud.google.com/blog/topics/threat-intelligence/disrupting-largest-residential-proxy-network](https://cloud.google.com/blog/topics/threat-intelligence/disrupting-largest-residential-proxy-network)

Google Threat Intelligence Group

January 28, 2026



Google Cloud

## Threat Intelligence

Google Threat Intelligence

Visibility and context on the threats that matter most.

[Contact Us & Get a Demo](#)

### Introduction

---

This week Google and partners took action to disrupt what we believe is one of the largest residential proxy networks in the world, the IPIDEA proxy network. IPIDEA's proxy infrastructure is a little-known component of the digital ecosystem leveraged by a wide array of bad actors.

This disruption, led by Google Threat Intelligence Group (GTIG) in partnership with other teams, included three main actions:

1. Took legal action to take down domains used to control devices and proxy traffic through them.
2. Shared technical intelligence on discovered IPIDEA software development kits (SDKs) and proxy software with platform providers, law enforcement, and research firms to help drive ecosystem-wide awareness and enforcement. These SDKs, which are offered to developers across multiple mobile and desktop platforms, surreptitiously enroll user devices into the IPIDEA network. Driving collective enforcement against these SDKs helps protect users across the digital ecosystem and restricts the network's ability to expand.

3. These efforts to help keep the broader digital ecosystem safe supplement the protections we have to safeguard Android users on certified devices. We ensured Google Play Protect, Android's built-in security protection, automatically warns users and removes applications known to incorporate IPIDEA SDKs, and blocks any future install attempts.

We believe our actions have caused significant degradation of IPIDEA's proxy network and business operations, **reducing the available pool of devices for the proxy operators by millions**. Because proxy operators share pools of devices using reseller agreements, we believe these actions may have downstream impact across affiliated entities.

## Dizzying Array of Bad Behavior Enabled by Residential Proxies

---

In contrast to other types of proxies, residential proxy networks sell the ability to route traffic through IP addresses owned by internet service providers (ISPs) and used to provide service to residential or small business customers. By routing traffic through an array of consumer devices all over the world, attackers can mask their malicious activity by hijacking these IP addresses. This generates significant challenges for network defenders to detect and block malicious activities.

A robust residential proxy network requires the control of millions of residential IP addresses to sell to customers for use. IP addresses in countries such as the US, Canada, and Europe are considered especially desirable. To do this, residential proxy network operators need code running on consumer devices to enroll them into the network as exit nodes. These devices are either pre-loaded with proxy software or are joined to the proxy network when users unknowingly download trojanized applications with embedded proxy code. Some users may knowingly install this software on their devices, lured by the promise of "monetizing" their spare bandwidth. When the device is joined to the proxy network, the proxy provider sells access to the infected device's network bandwidth (and use of its IP address) to their customers.

While operators of residential proxies often extol the privacy and freedom of expression benefits of residential proxies, Google Threat Intelligence Group's (GTIG) research shows that these proxies are overwhelmingly misused by bad actors. IPIDEA has become notorious for its role in facilitating several botnets: its software development kits played a key role in adding devices to the botnets, and its proxy software was then used by bad actors to control them. This includes the [BadBox2.0 botnet we took legal action against](#) last year, and the Aisuru and Kimwolf botnets more recently. We also observe IPIDEA being leveraged by a vast array of espionage, crime, and information operations threat actors. In a single seven day period in January 2026, GTIG observed over 550 individual threat groups that we track utilizing IP addresses tracked as IPIDEA exit nodes to obfuscate their activities, including groups from China, DPRK, Iran and Russia. The activities included access to victim SaaS environments, on-premises infrastructure, and password spray attacks. Our research has found significant overlaps between residential proxy network exit nodes, likely because of reseller and partnership agreements, making definitive quantification and attribution challenging.

In addition, residential proxies pose a risk to the consumers whose devices are joined to the proxy network as exit nodes. These users knowingly or unknowingly provide their IP address and device as a launchpad for hacking and other unauthorized activities, potentially causing them to be flagged as suspicious or blocked by providers. Proxy applications also [introduce security vulnerabilities](#) to consumers' devices and home networks. When a user's device becomes an exit node, network traffic that they do not control will pass through their device. This means bad actors can access a user's private devices on the same network, effectively exposing security vulnerabilities to the internet. GTIG's analysis of these applications confirmed that IPIDEA proxy did not solely route traffic through the exit node device, they also sent traffic to the device, in order to compromise it. While proxy providers may claim ignorance or close these security gaps when notified, enforcement and verification is challenging given intentionally murky ownership structures, reseller agreements, and diversity of applications.

## The IPIDEA Proxy Network

---

Our analysis of residential proxy networks found that many well-known residential proxy brands are not only related but are controlled by the actors behind IPIDEA. This includes the following ostensibly independent proxy and VPN brands:

- 360 Proxy (360proxy\.
- 922 Proxy (922proxy\.
- ABC Proxy (abcproxy\.
- Cherry Proxy (cherryproxy\.
- Door VPN (doorvpn\.
- Galleon VPN (galleonvpn\.
- IP 2 World (ip2world\.
- Ipidea (ipidea\.
- Luna Proxy (lunaproxy\.
- PIA S5 Proxy (piaproxy\.
- PY Proxy (pyproxy\.
- Radish VPN (radishvpn\.
- Tab Proxy (tabproxy\.

The same actors that control these brands also control several domains related to Software Development Kits (SDKs) for residential proxies. These SDKs are not meant to be installed or executed as standalone applications, rather they are meant to be embedded into existing applications. The operators market these kits as ways for developers to monetize their applications, and offer Android, Windows, iOS, and WebOS compatibility. Once developers incorporate these SDKs into their app, they are then paid by IPIDEA usually on a per-download basis.

Figure 1: Advertising from PacketSDK, part of the IPIDEA proxy network

Once the SDK is embedded into an application, it will turn the device it is running on into an exit node for the proxy network in addition to providing whatever the primary functionality of the application was. These SDKs are the key to any residential proxy network—the software they get embedded into provides the network operators with the millions of devices they need to maintain a healthy residential proxy network.

While many residential proxy providers state that they source their IP addresses ethically, our analysis shows these claims are often incorrect or overstated. Many of the malicious applications we analyzed in our investigation did not disclose that they enrolled devices into the IPIDEA proxy network. Researchers have previously found uncertified and off-brand Android Open Source Project devices, such as television set top boxes, with [hidden residential proxy payloads](#).

The following SDKs are controlled by the same actors that control the IPIDEA proxy network:

- Castar SDK (castarsdk\com)
- Earn SDK (earn sdk\io)
- Hex SDK (hexsdk\com)
- Packet SDK (packetsdk\com)

## Command-and-Control Infrastructure

---

We performed static and dynamic analysis on software that had SDK code embedded in it as well as standalone SDK files to identify the command-and-control (C2) infrastructure used to manage proxy exit nodes and route traffic through them. From the analysis we observed that EarnSDK, PacketSDK, CastarSDK, and HexSDK have significant overlaps in their C2 infrastructure as well as code structure.

### Overview

---

The infrastructure model is a two-tier system:

1. Tier One: Upon startup, the device will choose from a set of domains to connect to. The device sends some diagnostic information to the Tier One server and receives back a data payload that includes a set of Tier Two nodes to connect to.

2. Tier Two: The application will communicate directly with an IP address to periodically poll for proxy tasks. When it receives a proxy task it will establish a new dedicated connection to the Tier Two IP address and begin proxying the payloads it receives.

Figure 2: Two-tier C2 system

### Tier One C2 Traffic

---

The device diagnostic information can be sent as HTTP GET query string parameters or in the HTTP POST body, depending on the domain and SDK. The payload sent includes a **key** parameter, which may be a customer identifier used to determine who gets paid for the device enrollment.

```
os=android&v=1.0.8&sn=993AE4FE78B879239BDC14DFBC0963CD&tag=OnePlus8Pro%23*%2311%23*%2330%23*%23QKR1.191246.002%23*%230nePlus&key=cskfg9TAn9Jent&n=tlaunch
```

Figure 3: Sample device information send to Tier One server

The response from the Tier One server includes some timing information as well as the IP addresses of the Tier Two servers that this device should periodically poll for tasking.

```
{"code":200,"data":{"schedule":24,"thread":150,"heartbeat":20,"ip":  
[redacted],"info":"US","node":  
[{"net_type":"t","connect":"49.51.68.143:1000","proxy":"49.51.68.143:2000"},  
{"net_type":"t","connect":"45.78.214.188:800","proxy":"45.78.214.188:799"}]}
```

Figure 4: Sample response received from the Tier One Server

### Tier Two C2 Traffic

---

The Tier Two servers are sent as **connect** and **proxy** pairs. In all analyses the pairs have been IP addresses, not domains. In our analysis, the pairs are the same IP address but different ports. The **connect** port is used to periodically poll for new proxy tasking. This is performed by sending TCP packets with encoded JSON payloads.

```
{"name": "0c855f87a7574b28df383eca5084fcdc", "o": "eDwSokuy0uMHcF10", "os": "windows"}
```

Figure 5: Sample encoded JSON sent to Tier Two connect port

When the Tier Two server has traffic to route to the device, it will respond back with the FQDN to proxy traffic to as well as a connection ID.

```
www.google.com:443&c8eb024c053f82831f2738bd48afc256
```

Figure 6: Sample proxy tasking from the Tier Two server

The device will then establish a connection to the **proxy** port of the same Tier Two server and send the connection ID, indicating that it is ready to receive data payloads.

```
8a9bd7e7a806b2cc606b7a1d8f495662|ok
```

Figure 7: Sample data sent from device to the Tier Two proxy port

The Tier Two server will then immediately send data payloads to be proxied. The device will extract the TCP data payload, establish a socket connection to the specified FQDN and send the payload, unmodified, to the destination.

## Overlaps in Infrastructure

---

The SDKs each have their own set of Tier One domains. This comes primarily from analysis of standalone SDK files.

### PacketSDK

---

- <http://{random}.api-seed.packet-sdk.xyz>
- <http://{random}.api-seed.packet-sdk.net>
- <http://{random}.api-seed.packet-sdk.io>

### CastarSDK

---

- [dispatch1.hex-sdk.com](http://dispatch1.hex-sdk.com)
- [cfe47df26c8eaf0a7c136b50c703e173.com](http://cfe47df26c8eaf0a7c136b50c703e173.com)
- [8b21a945159f23b740c836eb50953818.com](http://8b21a945159f23b740c836eb50953818.com)
- [31d58c226fc5a0aa976e13ca9ecebcc8.com](http://31d58c226fc5a0aa976e13ca9ecebcc8.com)

### HexSDK

---

Download requests to files from the Hex SDK website redirect to [castar-sdk.com](http://castar-sdk.com). The SDKs are exactly the same.

### EarnSDK

---

The EarnSDK JAR package for Android has strong overlaps with the other SDK brands analyzed. Earlier published samples contained the Tier One C2 domains:

- [holadns.com](http://holadns.com)
- [martianinc.co](http://martianinc.co)
- [okamiboss.com](http://okamiboss.com)

Of note, these domains were observed as part of the BadBox2.0 botnet and were sinkholed in our earlier litigation. Pivoting off these domains and other signatures, we identified some additional domains used as Tier One C2 domains:

- [v46wd6uramzkmeeo.in](http://v46wd6uramzkmeeo.in)

- 6b86b273ff34fce1\online
- 0aa0cf0637d66c0d\com
- aa86a52a98162b7d\com
- 442fe7151fb1e9b5\com
- BdRV7WlBszf0TkqF\uk

## Tier Two Nodes

---

Our analysis of various malware samples and the SDKs found a single shared pool of Tier Two servers. As of this writing there were approximately 7,400 Tier Two servers. The number of Tier Two nodes changes on a daily basis, consistent with a demand-based scaling system. They are hosted in locations around the globe, including the US. This indicates that despite different brand names and Tier One domains, the different SDKs in fact manage devices and proxy traffic through the same infrastructure.

## Shared Sourcing of Exit Nodes

---

### Trojanized Software Distribution

---

The IPIDEA actors also control domains that offer free Virtual Private Network services. While the applications do seem to provide VPN functionality, they also join the device to the IPIDEA proxy network as an exit node by incorporating Hex or Packet SDK. This is done without clear disclosures to the end user, nor is it the primary function of the application.

- Galleon VPN (galleonvpn\com)
- Radish VPN (radishvpn\com)
- Aman VPN (defunct)

### Trojanized Windows Binaries

---

We identified a total of 3,075 unique Windows PE file hashes where dynamic analysis recorded a DNS request to at least one Tier One domain. A number of these hashes were for the monetized proxy exit node software, PacketShare. Our analysis also uncovered applications masquerading as OneDriveSync and Windows Update. These trojanized Windows applications were not distributed directly by the IPIDEA actors.

### Android Application Analysis

---

We identified over 600 applications across multiple download sources with code connecting to Tier One C2 domains. These apps were largely benign in function (e.g., utilities, games, and content) but utilized monetization SDKs that enabled IPIDEA proxy behavior.

## Our Actions

---

This week we took a number of steps designed to comprehensively dismantle as much of IPIDEA's infrastructure as possible.

### Protecting Devices

---

We took legal action to take down the C2 domains used by bad actors to control devices and proxy traffic. This protects consumer devices and home networks by disrupting the infrastructure at the source.

To safeguard the Android ecosystem, we enforced our platform policies against trojanizing software, ensuring [Google Play Protect](#) on certified Android devices with Google Play services automatically warns users and removes applications known to incorporate IPIDEA software development kits (SDKs), and blocks any future install attempts.

### Limiting IPIDEA's Distribution

---

We took legal action to take down the domains used to market IPIDEA's products, including proxy software and software development kits, across their various brands.

### Coordinating with Industry Partners

---

We've shared our findings with industry partners to enable them to take action as well. We've worked closely with other firms, including Spur and Lumen's Black Lotus Labs to understand the scope and extent of residential proxy networks and the bad behavior they often enable. We partnered with Cloudflare to disrupt IPIDEA's domain resolution, impacting their ability to command and control infected devices and market their products.

## Call to Action

---

While we believe our actions have seriously impacted one of the largest residential proxy providers, this industry appears to be rapidly expanding, and there are significant overlaps across providers. As our investigation shows, the residential proxy market has become a "gray market" that thrives on deception—hijacking consumer bandwidth to provide cover for global espionage and cybercrime. More must be done to address the risks of these technologies.

### Empowering and Protecting the Consumer

---

Residential proxies are an understudied area of risk for consumers, and more can be done to raise awareness. Consumers should be extremely wary of applications that offer payment in exchange for "unused bandwidth" or "sharing your internet." These applications are primary ways for illicit proxy networks to grow, and could open security vulnerabilities on the device's home network. We urge users to stick to official app stores, review permissions for third-party VPNs and proxies, and ensure built-in security protections like [Google Play Protect](#) are active.

Consumers should be careful when purchasing connected devices, such as set top boxes, to make sure they are from reputable manufacturers. For example, to help you confirm whether or not a device is built with the official Android TV OS and Play Protect certified, our [Android TV website](#) provides the most up-to-date list of partners. You can also take [these steps](#) to check if your Android device is Play Protect certified.

**Proxy Accountability and Policy Reform**

---

Residential proxy providers have been able to flourish under the guise of legitimate businesses. While some providers may indeed behave ethically and only enroll devices with the clear consent of consumers, any claims of "ethical sourcing" must be backed by transparent, auditable proof of user consent. Similarly, app developers have a responsibility to vet the monetization SDKs they integrate.

**Industry Collaboration**

---

We encourage mobile platforms, ISPs, and other tech platforms to continue sharing intelligence and implementing best practices to identify illicit proxy networks and limit their harms.

**Indicators of Compromise (IOCs)**

---

To assist the wider community in hunting and identifying activity outlined in this blog post, we have included a comprehensive list of indicators of compromise (IOCs) in a [GTI Collection for registered users](#).

**Network Indicators**

---

|                                      |
|--------------------------------------|
| 00857cca77b615c369f48ead5f8eb7f3.com |
| 0aa0cf0637d66c0d.com                 |
| 31d58c226fc5a0aa976e13ca9ecebcc8.com |
| 3k7m1n9p4q2r6s8t0v5w2x4y6z8u9.com    |
| 442fe7151fb1e9b5.com                 |
| 6b86b273ff34fce1.online              |
| 7x2k9n4p1q0r5s8t3v6w0y2z4u7b9.com    |
| 8b21a945159f23b740c836eb50953818.com |

|                                      |
|--------------------------------------|
| 8f00b204e9800998.com                 |
| a7b37115ce3cc2eb.com                 |
| a8d3b9e1f5c7024d6e0b7a2c9f1d83e5.com |
| aa86a52a98162b7d.com                 |
| af4760df2c08896a9638e26e7dd20aae.com |
| asdk2.com                            |
| b5e9a2d7f4c8e3b1a0d6f2e9c5b8a7d.com  |
| bdrv7wlbszfotkqf.uk                  |
| cfe47df26c8eaf0a7c136b50c703e173.com |
| hexsdk.com                           |
| e4f8c1b9a2d7e3f6c0b5a8d9e2f1c4d.com  |
| packetsdk.io                         |
| packetsdk.net                        |
| packetsdk.xyz                        |
| v46wd6uramzkmeeo.in                  |
| willmam.com                          |

## File Indicators

---

### Cert

---

---

SIGNER\_IDENTITY=/1.3.6.1.4.1.311.60.2.1.3=HK/businessCategory=Private  
Organization/serialNumber=69878507/C=HK/L=Hong Kong Island/O=HONGKONG LINGYUN  
MDT INFOTECH LIMITED/CN=HONGKONG LINGYUN MDT INFOTECH LIMITED

---

SIGNER\_IDENTITY=/businessCategory=Private  
Organization/1.3.6.1.4.1.311.60.2.1.3=HK/serialNumber=2746134/C=HK/L=Wan  
Chai/O=HONGKONG LINGYUN MDT INFOTECH LIMITED/CN=HONGKONG LINGYUN MDT  
INFOTECH LIMITED

---

SIGNER\_IDENTITY=/1.3.6.1.4.1.311.60.2.1.3=HK/businessCategory=Private  
Organization/serialNumber=74092936/C=HK/L=HONG KONG ISLAND/O=FIRENET  
LIMITED/CN=FIRENET LIMITED

---

SIGNER\_IDENTITY=/1.3.6.1.4.1.311.60.2.1.3=HK/businessCategory=Private  
Organization/serialNumber=3157599/C=HK/L=Wan Chai/O=FIRENET LIMITED/CN=FIRENET  
LIMITED

---

SIGNER\_IDENTITY=/1.3.6.1.4.1.311.60.2.1.3=HK/businessCategory=Private  
Organization/serialNumber=74097562/C=HK/L=Hong Kong Island/O=PRINCE LEGEND  
LIMITED/CN=PRINCE LEGEND LIMITED

---

SIGNER\_IDENTITY=/1.3.6.1.4.1.311.60.2.1.3=HK/businessCategory=Private  
Organization/serialNumber=73874246/C=HK/L=Kowloon/O=MARS BROTHERS  
LIMITED/CN=MARS BROTHERS LIMITED

---

SIGNER\_IDENTITY=/1.3.6.1.4.1.311.60.2.1.3=HK/businessCategory=Private  
Organization/serialNumber=3135905/C=HK/L=Cheung Sha Wan/O=MARS BROTHERS  
LIMITED/CN=MARS BROTHERS LIMITED

---

SIGNER\_IDENTITY=/1.3.6.1.4.1.311.60.2.1.3=HK/businessCategory=Private  
Organization/serialNumber=3222394/C=HK/L=WAN CHAI/O=ATALABS  
LIMITED/CN=ATALABS LIMITED

---

## Example Hashes

---

| File<br>Type | Description | SHA-256 |
|--------------|-------------|---------|
|--------------|-------------|---------|

---

|     |                                                    |                                                                  |
|-----|----------------------------------------------------|------------------------------------------------------------------|
| DLL | Packet SDK package found inside other applications | aef34f14456358db91840c416e55acc7d10185ff2beb362ea24697d7cdad321f |
| APK | Application with Packet SDK Code                   | b0726bdd53083968870d0b147b72dad422d6d04f27cd52a7891d038ee83aef5b |
| APK | Application with Hex SDK Code                      | 2d1891b6d0c158ad7280f0f30f3c9d913960a793c6abcda249f9c76e13014e45 |
| EXE | Radish VPN Client                                  | 59cbdecfc01eba859d12fbef48f96fe3fe841ac1aafa6bd38eff92f0dcfd4554 |
| EXE | ABC S5 Proxy Client                                | ba9b1f4cc2c7f4aeda7a1280bbc901671f4ec3edaa17f1db676e17651e9bff5f |
| EXE | Luna Proxy Client                                  | 01ac6012d4316b68bb3165ee451f2fcc494e4e37011a73b8cf2680de3364fcf4 |

Posted in

[Threat Intelligence](#)