Pablo Rosado González y Enrique de la Hoz, 22 de Mayo de 2025

EVOLUCIÓN DE LOS SERVICIOS DE ANONIMIZACIÓN EMPLEADOS PARA EL ACCESO INICIAL EN INTRUSIONES:

EL CASO DE LOS PROXYS RESIDENCIALES

Quiénes somos

Pablo Rosado González

Líder Técnico CSIRT
Telefónica España

Enrique de la Hoz

Profesor Titular de UniversidadDepartamento de Automática - Universidad de Alcalá

This work has been partially supported by the Madrid Community Regional funded project RAMONES-CM (Research in Advanced Monitoring and Optimization for Next-gen post-quantum Encryption and cyberSecurity Ref TEC-2024/COM-504).

Fuente: Mandiant M-Trends 2025 Report

Initial Infection Vector, 2024

Ransomware-Related

Acceso Inicial

Credenciales Válidas

- Existen distintos orígenes de las credenciales empleadas para el acceso inicial: *phishing*, Ingeniería social, *stealers*, Fuerza bruta, ...
- La detección del procedimiento de sustracción es compleja y exige trabajar sobre distintas fuentes
- La extensión de mecanismos como el **MFA** ha incentivado la aparición de **técnicas de evasión de MFA**
- El **bloqueo o detección de accesos sospechosos** es una barrera adicional de protección que es independiente del origen de las credenciales sustraídas y complementa la adopción del MFA

Ocultación del origen de un acceso

Aproximaciones prácticas

- El objetivo original es **dificultar la identificación del origen real** de una comunicación
  - Contexto: investigaciones criminales, atribución,…
- Podemos enunciar los siguientes requisitos:
  - El **origen de la comunicación** no debería revelar nada sobre la verdadera identidad o el origen del actor
  - El **servicio empleado** para la proteger la comunicación debería ofrecer también garantías de privacidad del actor malicioso

Ocultación del origen de un acceso

Servicios de Intermediación

- Existen multitud de servicios libremente accesibles, comerciales o no, para “ocultar” el origen real de una comunicación
- Obviamente, el empleo de un servicio de este tipo **no implica ninguna intención maliciosa**
- Podemos señalar, entre otros públicamente accesibles:
  - Servicios tipo proxy
  - Servicios tipo VPN comercial

Utilización de VPN

Servicios de Intermediación

- Desde el punto de vista de la inteligencia de amenazas, sí que podemos afirmar que **algunos actores amenaza priorizan la utilización de algunos servicios por criterios como**:
  - Anonimato
  - Ausencia de trazabilidad de las acciones
- Es habitual la aparición de servicios como **Mullvad** en incidentes

https://mullvad.net/es/help/how-we-handle-government-request-user-data

Algunos ejemplos

Helldown Ransomware

"It was shared that after compromising the Zyxel firewall, the attacker used the OKSDW82A account to connect via SSL VPN using an IP from **Mullvad VPN**"

Muddled Libra

"**Muddled Libra** […] preferred **Mullvad VPN**"

UNC5537

"***UNC5537*** *primarily used* ***Mullvad*** *or* ***Private Internet Access (PIA)*** *VPN IP addresses to access victim Snowflake instances*"

IntelBroke

"**Mullvad** is the most commonly used VPN by **IntelBroker**, followed by **TunnelBear**"

Scatter Swine

If the threat actor successfully harvests user credentials[…], attempts are made to authenticate using […] **Mullvad VPN.**

¿Es efectivo el uso de VPNs?

Bloqueo y detección

- Desde el punto de vista de ocultación del origen real de una conexión, sí
- Sin embargo, **el mero hecho de usar una VPN puede hacer que esa conexión sea lo suficientemente distinta al resto como para ser *identificada***
- Algunas estrategias de baja/media complejidad:
  - *Geofencing:* o bloqueo de accesos desde ciertas ubicaciones
  - *Listados de IPs de salida de servicios de anonimización: https://spur.us/*
- Para un atacante esto puede suponer no solamente el bloqueo de esa conexión sino la detección de una credencial comprometida

Evolución de los accesos anónimos

Características deseables

- Debería ser posible seleccionar la **ubicación geográfica** del punto de salida
  - Al menos en cuanto a país
- El número de elementos de salida debería ser **elevado y dinámico**
  - Para dificultar la trazabilidad y el mantenimiento de listas
- Los elementos de salida deberían ser **diversos** en cuanto a ubicación, ISP, tipo de conexión de red…
  - Para dificultar la categorización

Ser uno más

Características deseables

- El objetivo final es que una conexión anónima **no tenga atributos que la distingan de las conexiones de otros usuarios**
- Hay una solución obvia:
  - **Usar las conexiones de otros usuarios**

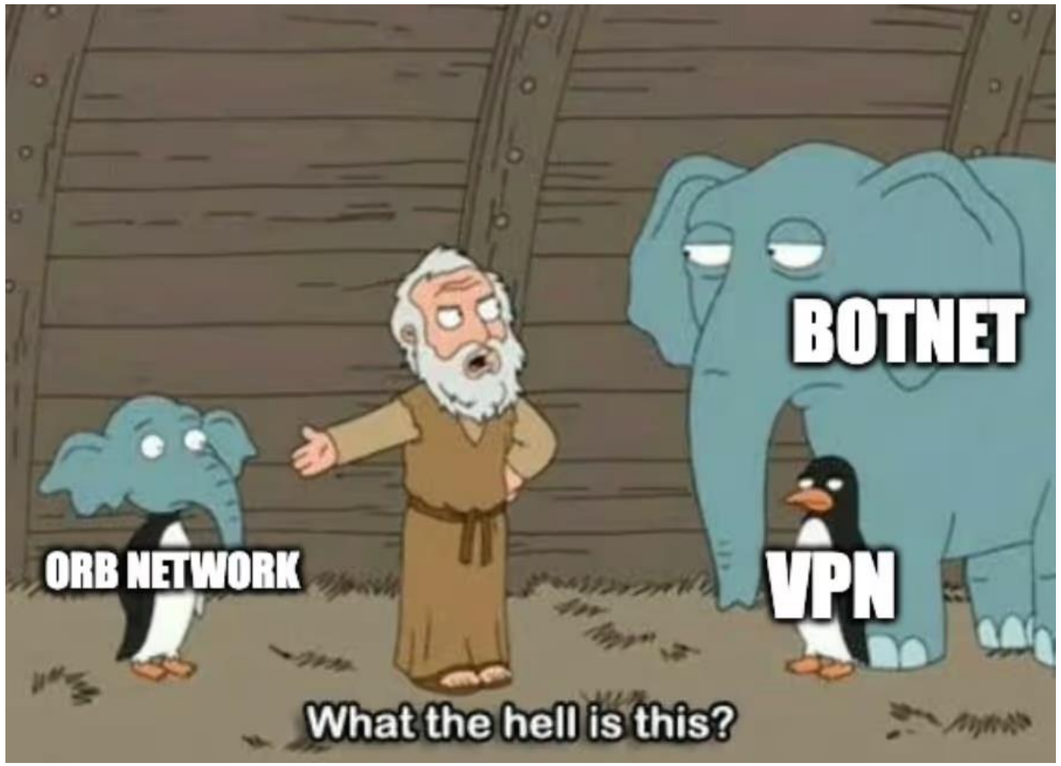
Construye tu propia red de anonimización

Alternativas

- Depende de los recursos, motivación y de las capacidades de las que disponga cada actor
  - Creación de una red de nodos a partir de la explotación de vulnerabilidades en equipos conectados a Internet → **Modelo botnet**
  - Despliegue de servidores virtuales (VPS) en distintos datacenters de Internet → **Modelo VPN**

Operation Relay Boxes

¿Lo peor de los dos mundos?

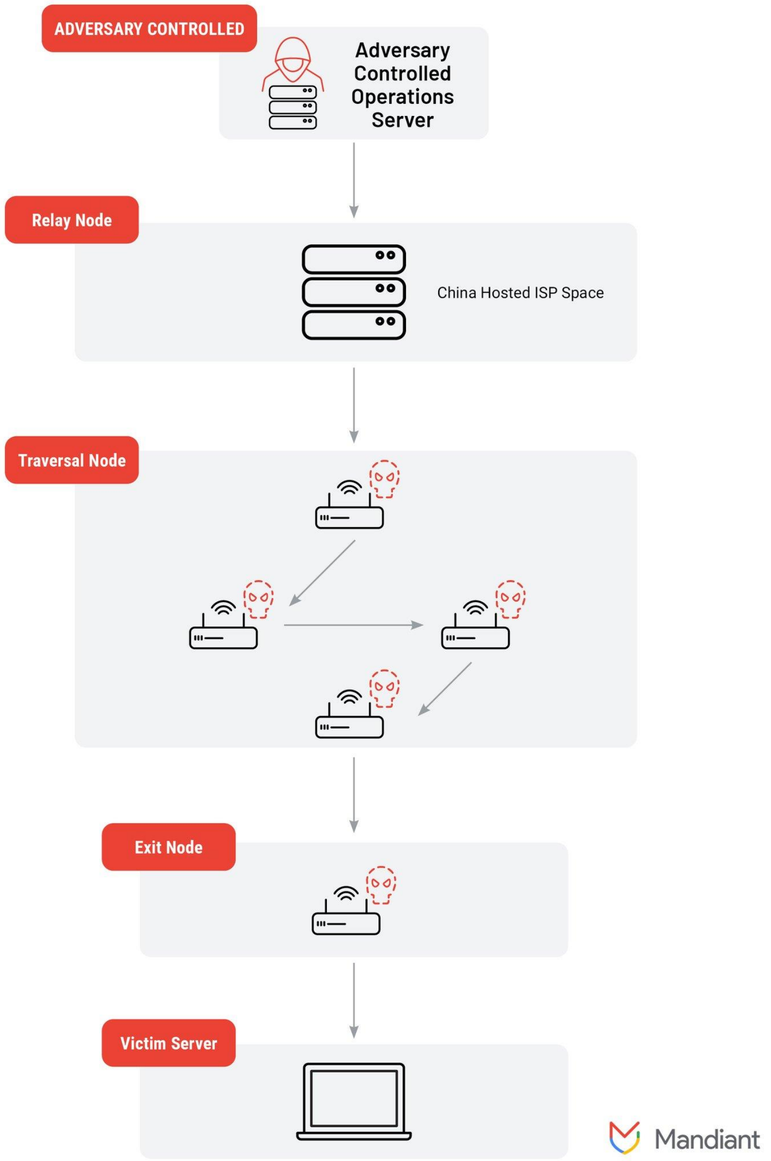


Fuente: https://www.team-cymru.com/post/an-introduction-to-operational-relay-box-orb-networks-unpatched-forgotten-and-obscured

ORB Networks

Arquitectura

- **ACOS**
  - Servidor de administración de la red
- ***Relay node***
  - *Típicamente un VPS hospedado en jurisdicciones amables para el actor*
- ***Traversal nodes***
  - *Una o varias capas de VPS o nodos comprometidos*
- ***Exit Node***
  - *Nodo seleccionado por al atacante para la salida*



Fuente: https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks

Operation Relay Boxes (ORB)

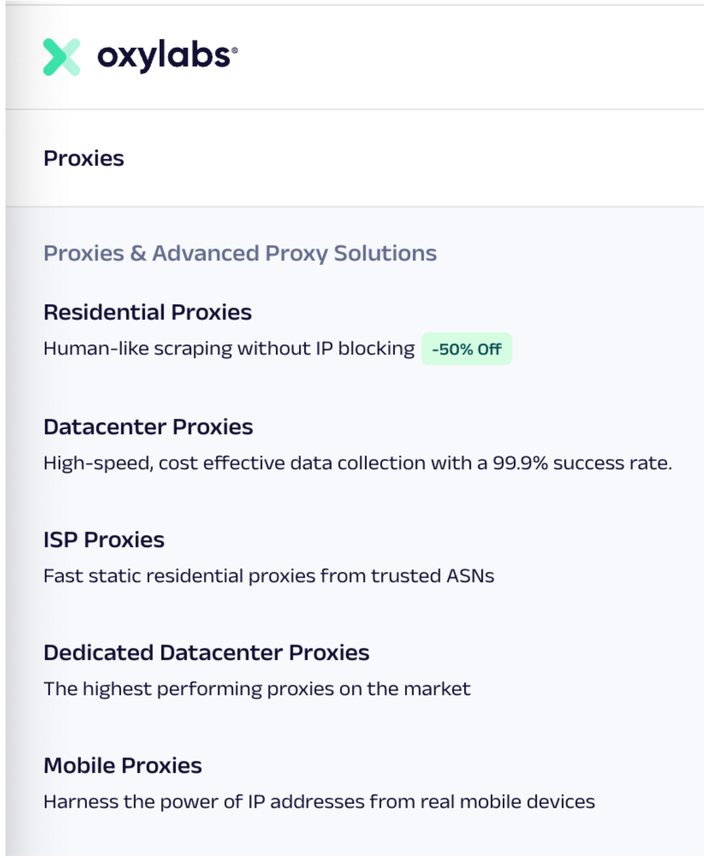
Características

- Arquitectura de **red mesh**
- Se difumina el concepto de ’infraestructura del atacante’
- La red tiene una **naturaleza más transitoria** lo que disminuye el valor de manejar indicadores de compromiso
- Se dificultan las tareas de investigación y atribución
- Desde el punto de vista de las víctimas, sólo se observa un acceso desde una ubicación que puede se perfectamente un **acceso residencial**

Proxys como Servicio

Sé quién quieras ser

- Servicios comerciales orientados a la **redirección del tráfico** elegido por el cliente hacia puntos de salida que cumplan unas **determinadas características**:
  - **Proxys de datacenter**
  - **Proxys ‘móviles’**
  - **Proxys residenciales**
  - **…**

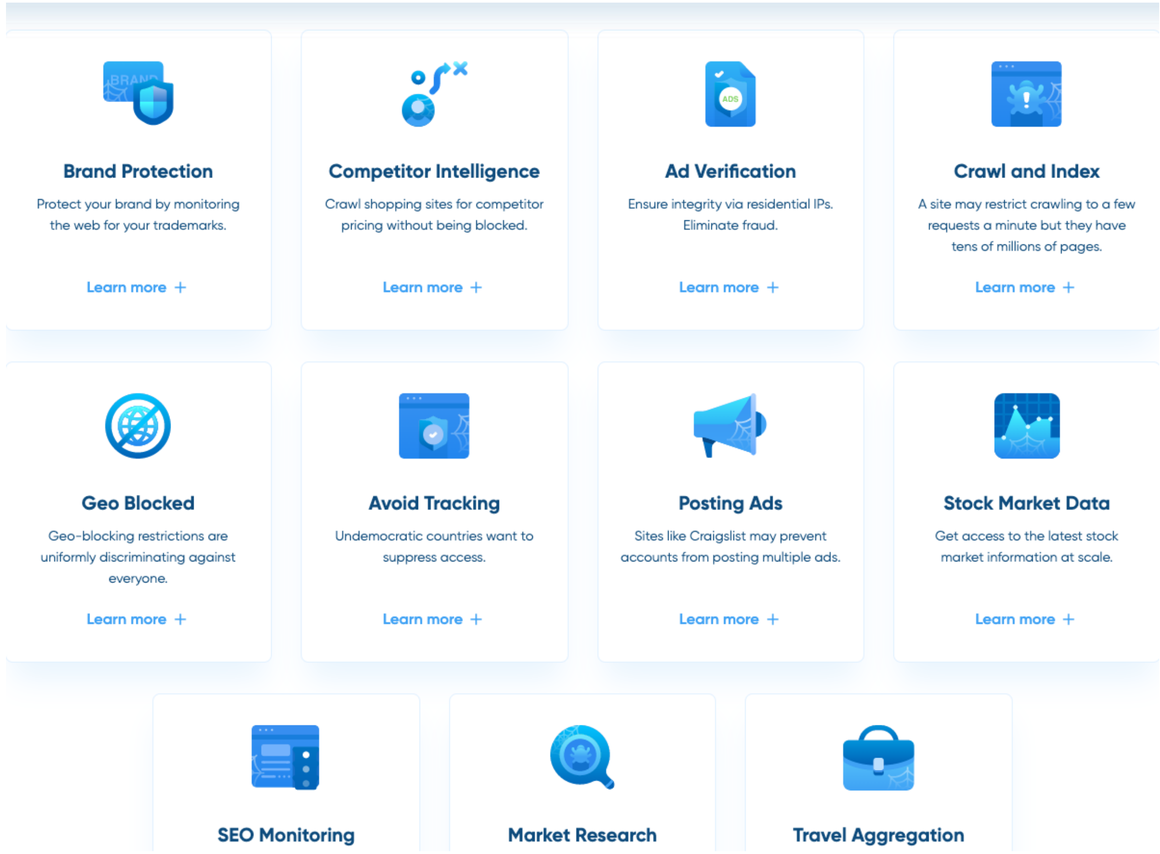


Fuente: https://oxylabs.io/

Proxys Residenciales

Usos legítimos

- Existe un conjunto de **casos de uso ‘legítimos’** asociados a estos servicios
- Cada proveedor tiene una sensibilidad distinta con respecto al abuso de sus servicios
- ¿**Cómo construyen sus redes**?

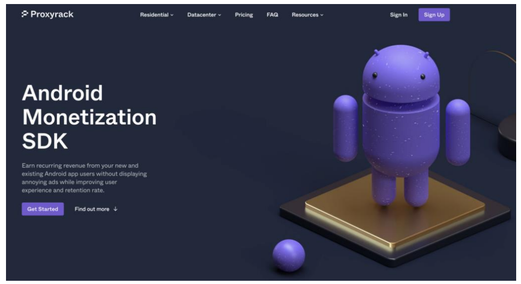


Proxys Residenciales

Your Phone is my proxy

- Mediante la instalación de aplicaciones específicamente para este uso

- A través de apps **cuyos términos de uso mencionan estos servicios**



Your Phone is My Proxy: Detecting and Understanding Mobile Proxy Networks

Proxys Residenciales

Creación de su red

ANONYMIZERS ON THE CHEAP

Thousands of phones and routers swept into proxy service, unbeknownst to users

Two new reports show criminals may be using your device to cover their online tracks.

PROXYLIB Timeline

May 2023

MAY 15, 2023
IAS published a report on an ad fraud scheme conducted via an Android free VPN application called "**Oko VPN**".

June 2023

July 2023

MAY 24, 2023
Hacker forums and new VPN applications have references to **lumiapps[.]io**, a monetization SDK that adds a Golang library to APKs submitted by users and provides a developer SDK.

August 2023

September 2023

AUGUST 2023
Increase of repacked/modified APKs with an SDK facilitating residential proxy activity: **PROXYLIB**.

October 2023

November 2023

DECEMBER 2023
- HUMAN confirmed *LumiApps* and *Asocks* (a residential proxy service provider) are associated.
- A new version of the LumiApps SDK was found. This version has essentially the same Go library but is implemented differently on the Java side.

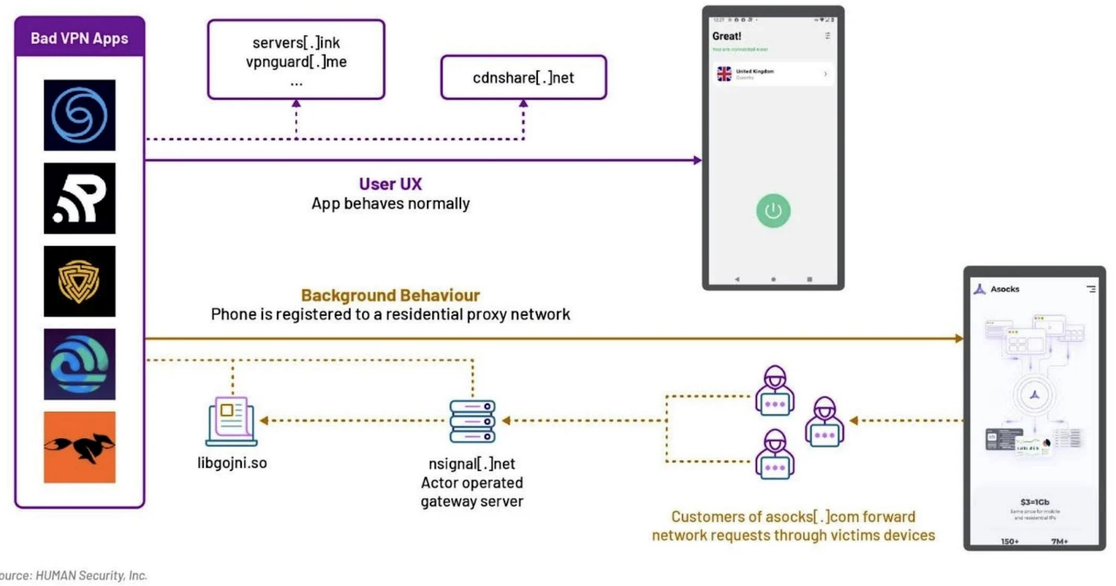
December 2023

January 2024

JANUARY 2024
- A subsequent version of the LumiApps SDK is released. According to LumiApps support, it addresses integration issues users have with the previous version.
- Google Play Store removes new and remaining apps with LumiApps SDK present.

February 2024

PROXYLIB Process



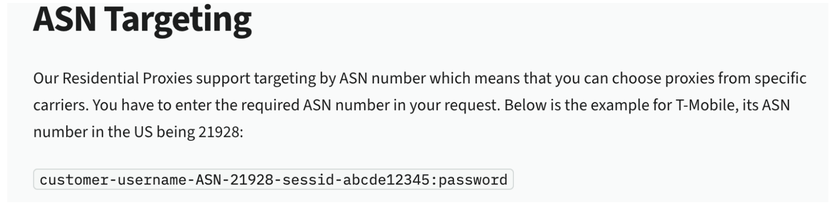
Source: HUMAN Security, Inc.

Fuente: https://www.humansecurity.com/learn/blog/satori-threat-intelligence-alert-proxylib-and-lumiapps-transform-mobile-devices-into-proxy-nodes/

¿Puedo indicar qué dirección quiero?

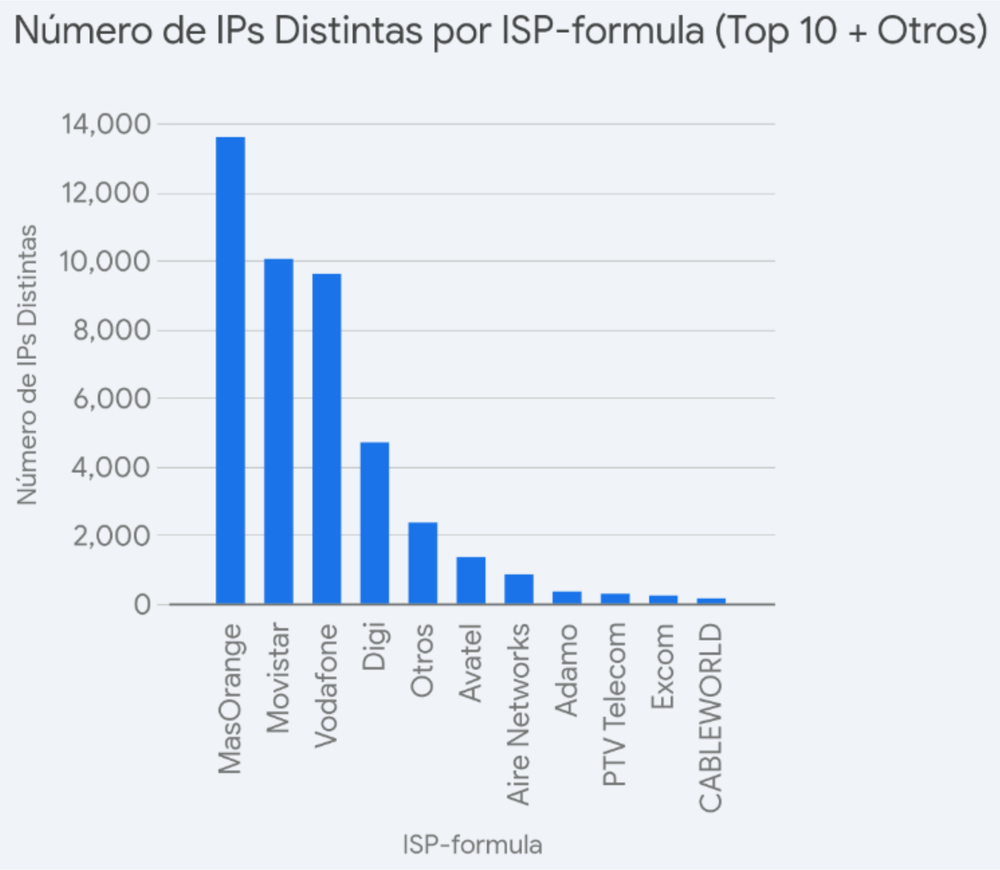
Granularidad de la elección

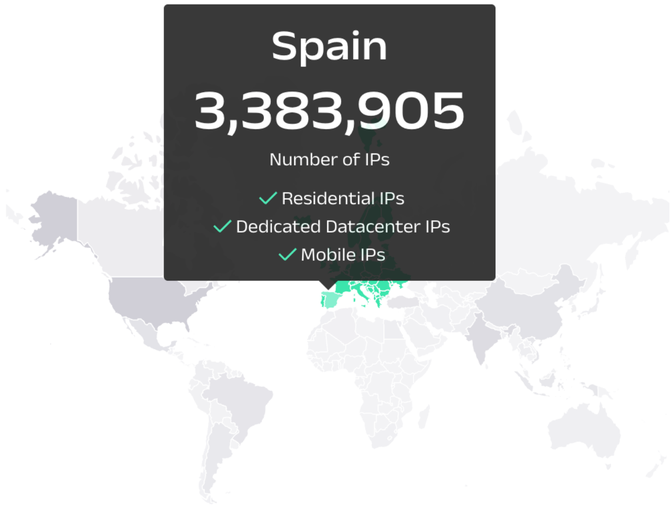
- Selección por:
  - Tipo de acceso: residencial, móvil
  - ISP
  - Ciudad
  - ASN
- ¿Podría solicitar una dirección IP de una universidad?



Accesos residenciales en España

Distribución por proveedores





RESIP providers[...] claiming to have access to tens of millions of residential Ips […] even if these sizes were real, ***some pools of IPs are not uniquely used by a single provider***

(*Resident evil: Understanding residential IP proxy as a dark service*)

Estudio de 4 proveedores durante 48 horas – Aprox. 30.000 IPs

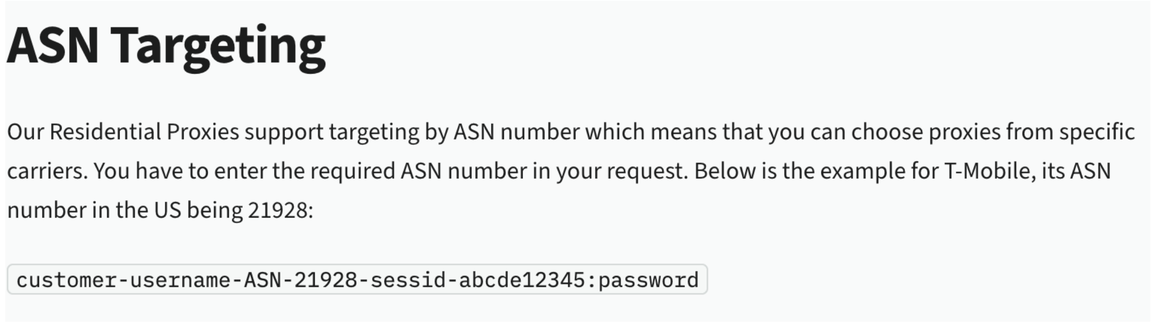
¿Salida desde Universidades?

- Nuestra explotación nos permitió obtener
  - IPs de salida pertenecientes a **más de 50 instituciones afiliadas**
  - Repartidas entre los **cuatro proveedores** que se han analizado en el estudio
- Estudio realizado a partir de los datos de WHOIS
- Junto con direccionamiento perteneciente a **múltiples empresas e instituciones**

¿Acceso desde una universidad?

Solicitud de IP del ASN 766

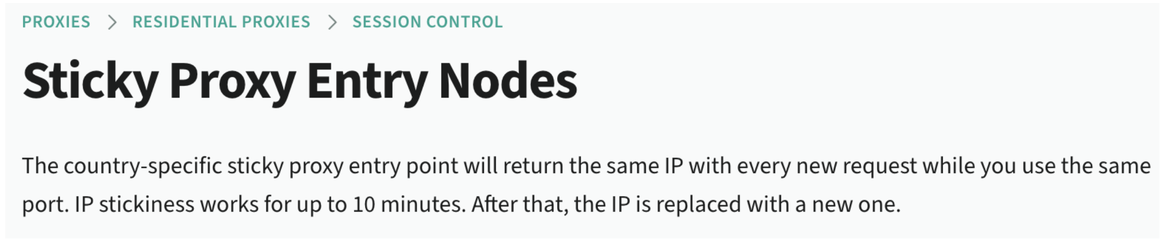
- Típicamente, **dispositivos móviles conectados a eduroam**
- Evasión de controles de autenticación basados en IP
- ¿Es posible acceder a direcciones IP internas?
  - ***Dependiendo del servicio empleado***



ASN Targeting

Our Residential Proxies support targeting by ASN number which means that you can choose proxies from specific carriers. You have to enter the required ASN number in your request. Below is the example for T-Mobile, its ASN number in the US being 21928:

```
customer-username-ASN-21928-sessid-abcde12345:password
```



PROXIES > RESIDENTIAL PROXIES > SESSION CONTROL

Sticky Proxy Entry Nodes

The country-specific sticky proxy entry point will return the same IP with every new request while you use the same port. IP stickiness works for up to 10 minutes. After that, the IP is replaced with a new one.

PoC: Acceso a Artículos científicos IEEE

Evasión de control de acceso

En general, podría emplearse para cualquier servicio que emplee únicamente validación por IP origen

Conclusiones

We no longer operate in the world of "block and move on" where IPs are part of APT's weaponization and C2 kill chain phase. Instead, infrastructure is a living artifact of an ORB network that is a distinct and evolving entity where the characteristics of IP infrastructure itself, including ports, services, and registration/hosting data, can be tracked as evolving behavior by the adversary administrator responsible for that ORB network.

"IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders"

Conclusiones

- El **abuso de credenciales** es uno de los vectores de entrada más habituales en intrusiones
- La eficacia de medidas como el **bloqueo por rangos o por geolocalización** se ve **afectada por la adopción de nuevas técnicas** por parte de los actores amenaza
- Existen **servicios comerciales** que permite a cualquier usuario, con pocos conocimientos y pocos recursos obtener una dirección IP de salida prácticamente desde cualquier ubicación y proveedor
- Es necesario **reevaluar controles** a partir de la situación realmente existente

Referencias

Informes de Ciberamenazas

Google Cloud. (2024, June 10). *UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion*. Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

KELA. (2025, January 14). *IntelBroker Unmasked: KELA's In-Depth Analysis of a Cybercrime Leader*. KELA Cyber Threat Intelligence. https://www.kelacyber.com/blog/intelbroker-unmasked-kelas-in-depth-analysis-of-a-cybercrime-leader/

Okta Security. (2022, August 25). *Detecting Scatter Swine: Insights into a Relentless Phishing Campaign*. Okta. https://sec.okta.com/articles/scatterswine/

Russo, K., Dever, A., & Elsad, A. (2025, May 16). *Threat Group Assessment: Muddled Libra*. Unit 42 | Palo Alto Networks. https://unit42.paloaltonetworks.com/muddled-libra/

Referencias

Orb Networks

Mandiant. (2024, May 22). *IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders*. Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks

Intel471. (2024, November 19). *A Look at Trending Chinese APT Techniques*. Intel471 Blog. https://intel471.com/blog/a-look-at-trending-chinese-apt-techniques

Scion, J., Aimé, F., & Sekoia TDR. (2025, February 25). *PolarEdge: Unveiling an uncovered ORB network*. Sekoia.io Blog. https://blog.sekoia.io/polaredge-unveiling-an-uncovered-iot-botnet/

Huntress. (2023, December 27). *Combating Emerging Microsoft 365 Tradecraft: Initial Access*. Huntress Blog. https://www.huntress.com/blog/combating-emerging-microsoft-365-tradecraft-initial-access

National Security Agency, Cybersecurity and Infrastructure Security Agency, & Federal Bureau of Investigation. (2024, September 18). *Cybersecurity Advisory: PRC-Linked Actors Botnet*. U.S. Department of Defense. https://media.defense.gov/2024/Sep/18/2003547016/-1/-1/0/CSA-PRC-LINKED-ACTORS-BOTNET.PDF

Team Cymru. (n.d.). *An Introduction to Operational Relay Box (ORB) Networks - Unpatched, Forgotten, and Obscured*. Team Cymru. Retrieved May 20, 2025, from https://www.team-cymru.com/post/an-introduction-to-operational-relay-box-orb-networks-unpatched-forgotten-and-obscured

Google Cloud. (n.d.). *Chinese Espionage Tactics*. Google Cloud Blog. Retrieved May 20, 2025, from https://cloud.google.com/blog/topics/threat-intelligence/chinese-espionage-tactics/

Mandiant. (2025, March 12). *Ghost in the Router: China-Nexus Espionage Actor UNC3886 Targets Juniper Routers*. Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-targets-juniper-routers

Referencias

Proxys Residenciales

Krebs, B. (2021, March 1). *Is Your Browser Extension a Botnet Backdoor?* Krebs on Security. https://krebsonsecurity.com/2021/03/is-your-browser-extension-a-botnet-backdoor/

HUMAN Security. (2023, October 24). *Satori Threat Intelligence Alert: PROXYLIB and LumiApps Transform Mobile Devices into Proxy Nodes*. HUMAN Security Blog. https://www.humansecurity.com/learn/blog/satori-threat-intelligence-alert-proxylib-and-lumiapps-transform-mobile-devices-into-proxy-nodes/

Sekoia.io. (2024, March 14). *Unveiling the depths of Residential Proxies providers*. Sekoia.io Blog. http://blog.sekoia.io/unveiling-the-depths-of-residential-proxies-providers/

Spur.us. (n.d.). *The market for clean IP addresses: The good, the bad, and the ugly*. Retrieved May 20, 2025, from https://spur.us/the-market-for-clean-ip-addresses/

Oxylabs. (2020, September 24). *Residential Proxy Acquisition: Best Practices*. Oxylabs Blog. https://oxylabs.io/blog/proxy-acquisition-best-practices

Goodin, D. (2024, March 26). *Thousands of phones and routers swept into proxy service, unbeknownst to users*. Ars Technica. https://arstechnica.com/security/2024/03/thousands-of-phones-and-routers-swept-into-proxy-service-unbeknownst-to-users/

Intel471. (2023, March 14). *A Look at the Residential Proxy Market*. Intel471 Blog. https://intel471.com/blog/a-look-at-the-residential-proxy-market

Spur.us. (n.d.). *Proxy Diversity (or Lack Thereof)*. Retrieved May 20, 2025, from https://spur.us/proxy-diversity-or-lack-thereof/

Spur Intel. (n.d.). *Monocle-plugin-nginx*. GitHub. Retrieved May 20, 2025, from https://github.com/spurintel/monocle-plugin-nginx

Referencias

Proxys Residenciales – Trabajos Académicos

Liu, Y., Ma, X., Li, Z., Li, T., Liu, B., Yang, A., Sun, D., Li, Z., & Zou, W. (2021). Resident evil: Understanding residential IP proxy as a dark service. *Proceedings of the 30th USENIX Security Symposium*.

Mi, X., Tang, S., Li, Z., Liao, X., Qian, F., & Wang, X. (2021). Your Phone is My Proxy: Detecting and Understanding Mobile Proxy Networks. *Proceedings of the Network and Distributed System Security Symposium (NDSS)*.

Wang, Y., Wang, Y., Luo, S., Zhang, X., Liu, C., & Fu, X. (2024). Shining light into the tunnel: Understanding and classifying network traffic of residential proxies. *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*.

Abman, A., Lee, W., Lee, J., Lee, D., Kim, Y., & Mohaisen, A. (2024). Unmasking the shadows: Understanding and detecting residential IP proxies. *Proceedings of the ACM Web Conference 2024*.

Pultr, D., Kolcun, R., Valenta, L., Tran, S., Ivan, J., Fiebig, T., & Uhlir, V. (2024). Inside residential IP proxies: Lessons learned from large measurement campaigns. *Proceedings of the ACM SIGCOMM 2024 Conference*.