Residential proxy software found on White House network: a prompt to check your own



Researchers report that residential proxy software on staff devices exposed White House IP addresses for public rental. The same software is common on corporate and government networks, so regulated firms should check their own.

- Layer3 Intel saw residential proxy nodes beaconing from the Executive Office of the President network (AS2650) between October 5 and November 3.
- Traffic exited the network 236 times, from six addresses on 26 of 30 days, mostly between 5 p.m. and midnight.
- Synthient linked part of the activity to Windows 11 installations of Infatica, a proxy program often bundled into free apps.
- Layer3 found 28 separate proxy services able to exit through this network, accessible to anyone for

a few dollars.

- Spur and Infoblox data indicate such proxies are widespread in government, utility, healthcare and financial networks.

Security researchers have reported that several White House staff are using computers or mobile devices running residential proxy software, which lets third parties rent the device's internet address. The White House had not responded to a request for comment at the time of reporting.

What was observed

Layer3 Intel detected proxy nodes beaconing from the network reserved for the Executive Office of the President (AS2650), persistently from October 5 to November 3. Traffic exited 236 times from six addresses, on 26 of 30 days, mostly in the evening. Synthient tied some of the activity to Windows 11 installations of Infatica, a proxy program often embedded in free desktop and mobile apps. Layer3 said 28 separate proxy services could exit through the network, and that it found this by chance, not by targeting it.

Why it matters

Residential proxies let customers hide their origin, so traffic appears to come from the host's address. They are linked to account takeover, ad fraud and content scraping. Vulnerabilities in these services have also let criminals reach devices on the local networks of proxy hosts, and dozens of providers had to patch in January 2026. A Synthient founder noted that resellers can skip customer-identity checks.

The issue is not limited to government. Spur reported residential proxies in nearly 300 government networks, 318 utilities, 166 healthcare organizations and 141 banking and finance companies. Infoblox found 65% of its customers querying proxy-related domains. Often the cause is an app with an embedded SDK that pays developers per installation, running on a device an employee brought to work.

Regulated institutions should treat this as a practical check on their own environment rather than a reason for alarm.

What to do now

1. Query DNS and proxy logs for domains and traffic patterns associated with residential proxy services, including Infatica.
2. Inventory applications on corporate and BYOD devices and remove free software that embeds proxy SDKs.
3. Enforce application allow-listing and restrict installation rights on endpoints.
4. Alert on outbound connections from your public IP ranges to known proxy networks, especially in evening hours.
5. Add residential proxy SDKs to BYOD and acceptable-use policies and brief staff.

6. Segment guest and personal-device traffic from internal systems.