# Kimwolf Botnet Lurking in Corporate, Govt. Networks

Published: 2026-01-20 · Archived: 2026-04-06 00:40:39 UTC

A new Internet-of-Things (IoT) botnet called **Kimwolf** has spread to more than 2 million devices, forcing infected systems to participate in massive distributed denial-of-service (DDoS) attacks and to relay other malicious and abusive Internet traffic. Kimwolf's ability to scan the local networks of compromised systems for other IoT devices to infect makes it a sobering threat to organizations, and new research reveals Kimwolf is surprisingly prevalent in government and corporate networks.

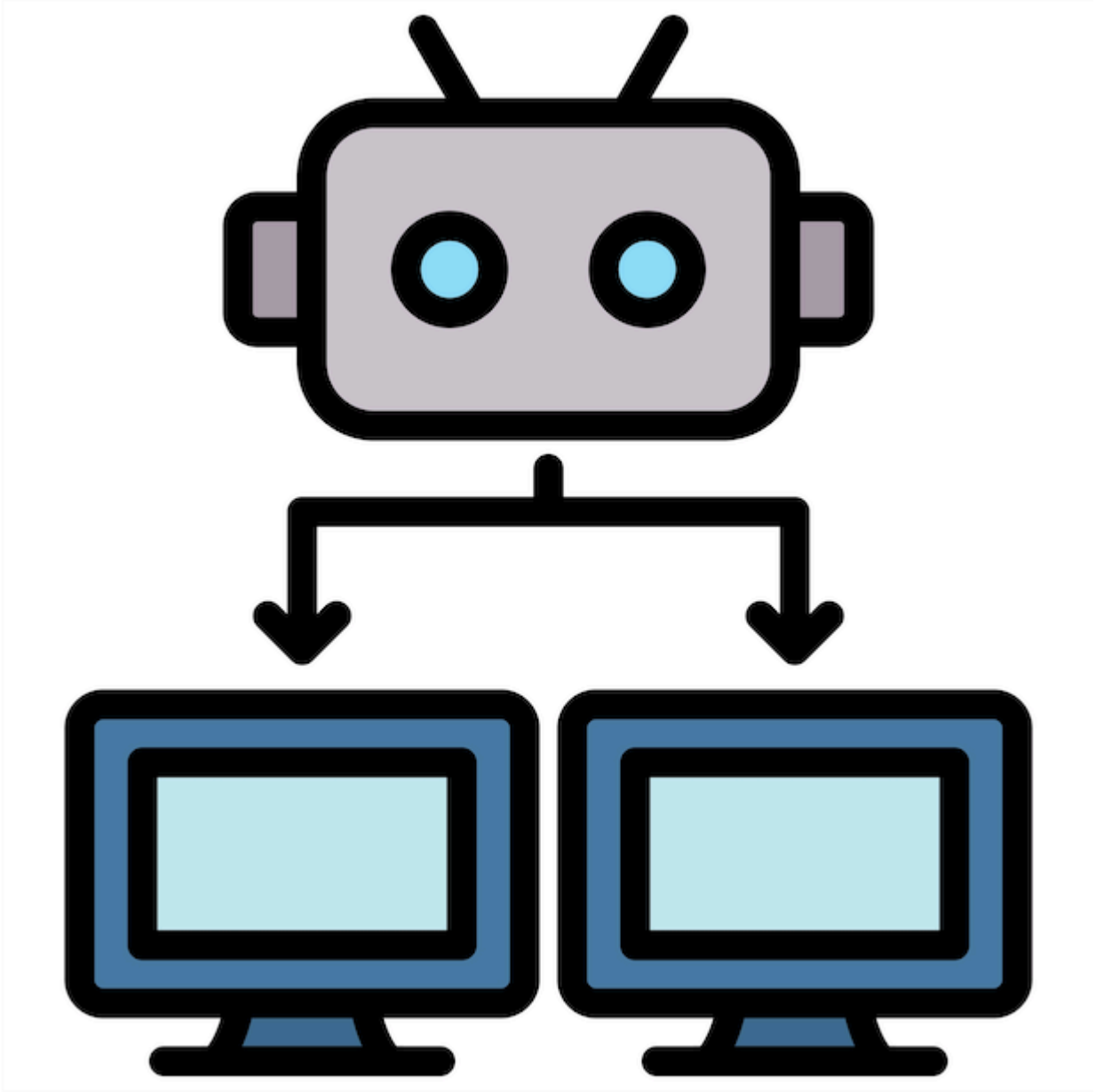


Image: Shutterstock, @Elzicon.

Kimwolf grew rapidly in the waning months of 2025 by tricking various “residential proxy” services into relaying malicious commands to devices on the local networks of those proxy endpoints. Residential proxies are sold as a way to anonymize and localize one’s Web traffic to a specific region, and the biggest of these services allow customers to route their Internet activity through devices in virtually any country or city around the globe.

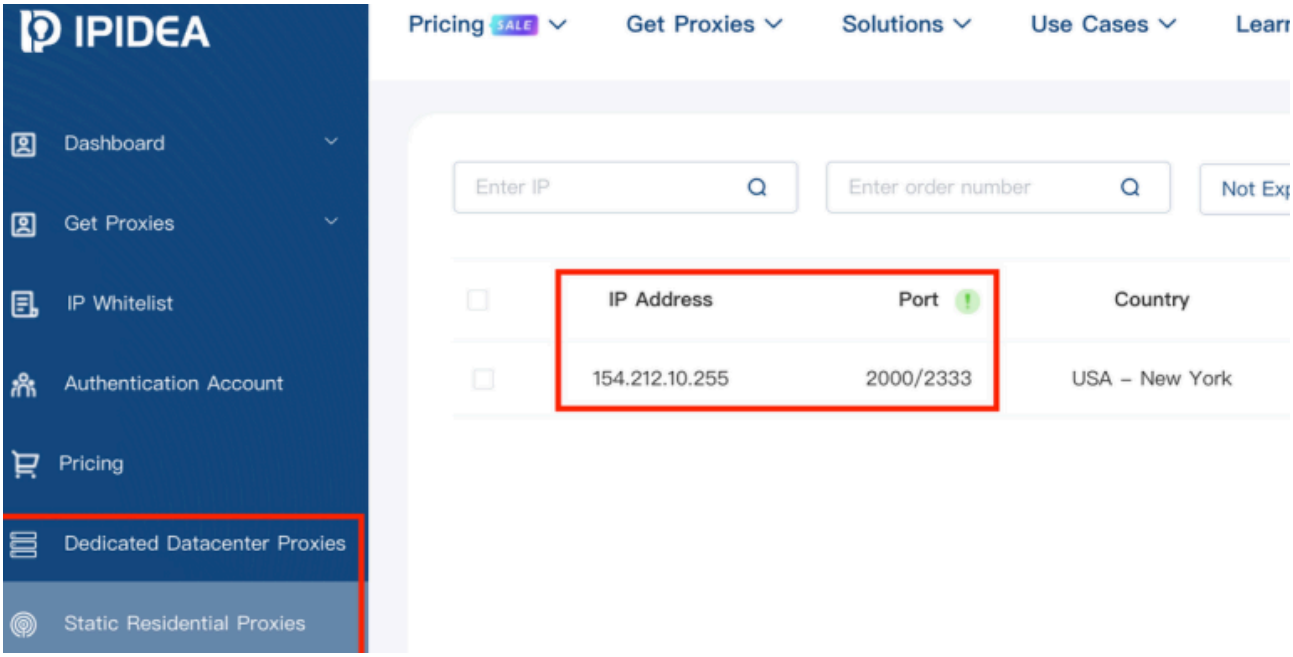
The malware that turns one’s Internet connection into a proxy node is often quietly bundled with various mobile apps and games, and it typically forces the infected device to relay malicious and abusive traffic — including ad fraud, account takeover attempts, and mass content-scraping.

Kimwolf mainly targeted proxies from **IPIDEA**, a Chinese service that has millions of proxy endpoints for rent on any given week. The Kimwolf operators discovered they could forward malicious commands to the internal networks of IPIDEA proxy endpoints, and then programmatically scan for and infect other vulnerable devices on each endpoint’s local network.

Most of the systems compromised through Kimwolf’s local network scanning have been unofficial Android TV streaming boxes. These are typically Android Open Source Project devices — not Android TV OS devices or Play Protect certified Android devices — and they are generally marketed as a way to watch unlimited (read:pirated) video content from popular subscription streaming services for a one-time fee.

However, a great many of these TV boxes ship to consumers with residential proxy software pre-installed. What’s more, they have no real security or authentication built-in: If you can communicate directly with the TV box, you can also easily compromise it with malware.

While IPIDEA and other affected proxy providers recently have taken steps to block threats like Kimwolf from going upstream into their endpoints (reportedly with varying degrees of success), the Kimwolf malware remains on millions of infected devices.



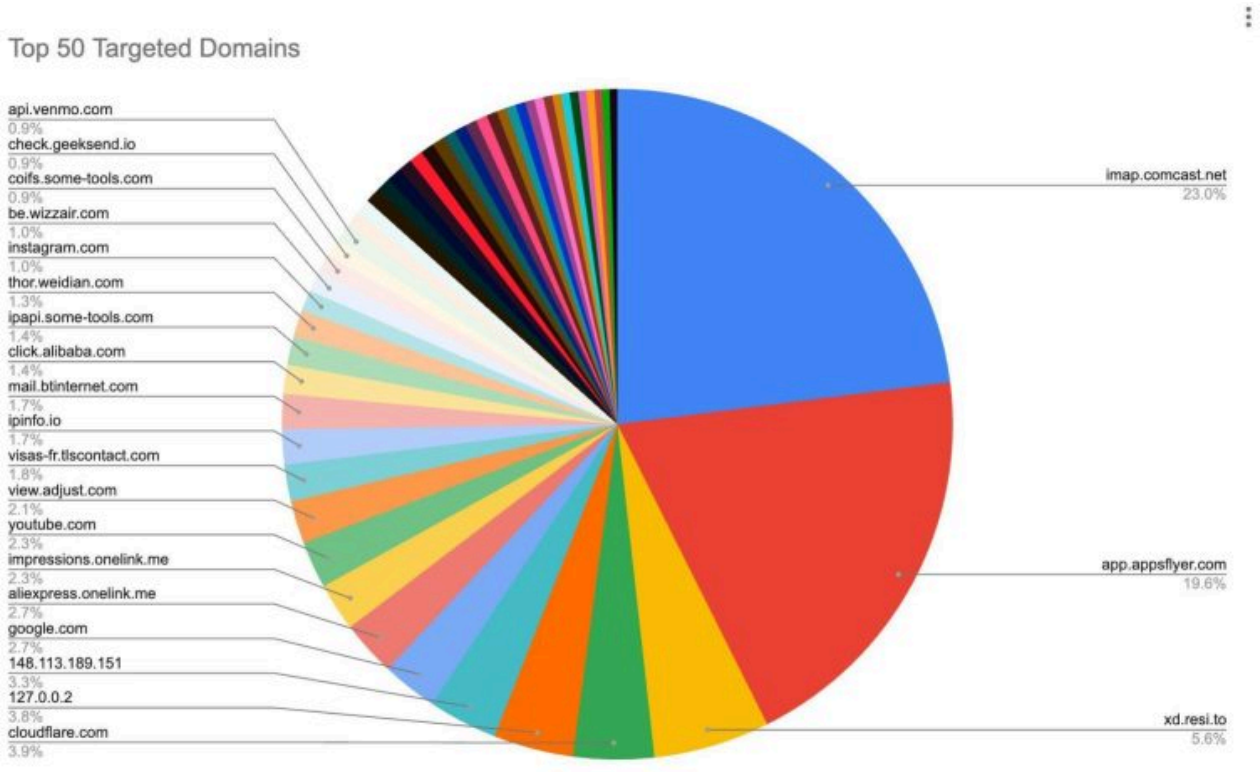

A screenshot of IPIDEA’s proxy service.

Kimwolf's close association with residential proxy networks and compromised Android TV boxes might suggest we'd find relatively few infections on corporate networks. However, the security firm **Infoblox** said a recent review of its customer traffic found *nearly 25 percent of them made a query to a Kimwolf-related domain name since October 1, 2025*, when the botnet first showed signs of life.

Infoblox found the affected customers are based all over the world and in a wide range of industry verticals, from education and healthcare to government and finance.

"To be clear, this suggests that nearly 25% of customers had at least one device that was an endpoint in a residential proxy service targeted by Kimwolf operators," Infoblox explained. "Such a device, maybe a phone or a laptop, was essentially co-opted by the threat actor to probe the local network for vulnerable devices. A query means a scan was made, not that new devices were compromised. Lateral movement would fail if there were no vulnerable devices to be found or if the DNS resolution was blocked."

**Synthient**, a startup that tracks proxy services and was the first to disclose on January 2 the unique methods Kimwolf uses to spread, found proxy endpoints from IPIDEA were present in alarming numbers at government and academic institutions worldwide. Synthient said it spied at least 33,000 affected Internet addresses at universities and colleges, and nearly 8,000 IPIDEA proxies within various U.S. and foreign government networks.




The top 50 domain names sought out by users of IPIDEA's residential proxy service, according to Synthient.

In a webinar on January 16, experts at the proxy tracking service **Spur** profiled Internet addresses associated with IPIDEA and 10 other proxy services that were thought to be vulnerable to Kimwolf's tricks. Spur found residential proxies in nearly 300 government owned and operated networks, 318 utility companies, 166 healthcare companies or hospitals, and 141 companies in banking and finance.

“I looked at the 298 [government] owned and operated [networks], and so many of them were DoD [U.S. Department of Defense], which is kind of terrifying that DoD has IPIDEA and these other proxy services located inside of it,” Spur Co-Founder **Riley Kilmer** said. “I don’t know how these enterprises have these networks set up. It could be that [infected devices] are segregated on the network, that even if you had local access it doesn’t really mean much. However, it’s something to be aware of. If a device goes in, anything that device has access to the proxy would have access to.”

Kilmer said Kimwolf demonstrates how a single residential proxy infection can quickly lead to bigger problems for organizations that are harboring unsecured devices behind their firewalls, noting that proxy services present a potentially simple way for attackers to probe other devices on the local network of a targeted organization.

“If you know you have [proxy] infections that are located in a company, you can chose that [network] to come out of and then locally pivot,” Kilmer said. “If you have an idea of where to start or look, now you have a foothold in a company or an enterprise based on just that.”

This is the third story in our series on the Kimwolf botnet. Next week, we’ll shed light on the myriad China-based individuals and companies connected to the **Badbox 2.0 botnet**, the collective name given to a vast number of Android TV streaming box models that ship with no discernible security or authentication built-in, and with residential proxy malware pre-installed.

Further reading:

The Kimwolf Botnet is Stalking Your Local Network

Who Benefitted from the Aisuru and Kimwolf Botnets?

A Broken System Fueling Botnets (Synthient).

---

Source: https://krebsonsecurity.com/2026/01/kimwolf-botnet-lurking-in-corporate-govt-networks/