Kimwolf Android Botnet Grows Through Residential Proxy Networks

By Ionut Arghire

Published: 2026-01-05 · Archived: 2026-04-05 20:39:42 UTC

The Kimwolf botnet has infected over 2 million Android devices, mainly through residential proxy networks, cybersecurity firm Synthient says.

Active since at least August 2025, the Kimwolf botnet was recently detailed by XLab, which warned that it could launch massive distributed denial-of-service (DDoS) attacks.

Mainly consisting of Android TV set-top boxes deployed on residential networks, Kimwolf provides its operators with other monetization opportunities as well, including application installs and the selling of proxy bandwidth, Synthient explains.

According to the cybersecurity firm, the botnet's size may be much larger than previously estimated, with roughly 12 million unique IP addresses associated with it seen every week.

Synthient cautiously estimates that Kimwolf has infected just over 2 million devices, mainly through the exploitation of an exposed Android Debug Bridge (ADB) service. Many of these devices are in Vietnam, Brazil, India, and Saudi Arabia.

The botnet grew fast over the past two months, due to a novel technique targeting residential proxy networks, with many of the infections associated with proxy IP addresses offered for rent by China-based IPIDEA, one of the largest residential proxy networks in the world.

As investigative journalist Brian Krebs points out, the botnet mainly targets unofficial Android TV boxes that come at low prices, but which come with insecure components and often require users to install software that turns them into proxy nodes.

Synthient's investigation revealed that many of the newly ensnared devices were sold pre-infected with malware. Instead of IPIDEA's legitimate binaries, they contained modified ones that turned them into Kimwolf bots.

In late December, IPIDEA deployed a patch to address the underlying issue and block access to numerous exposed ports.

"We sent 11 vulnerability emails on December 17 to the top proxy providers. Each notified provider was impacted to varying degrees, with a significant portion allowing access to devices on the local network," Synthient notes.

"Synthient's Research Team is unable to assess with confidence the complete list of targeted providers by Kimwolf. Current evidence indicates that IPIDEA was the main target because it enabled access to all ports," the cybersecurity firm continues.

In addition to abusing the infected devices in DDoS attacks of around 30Tbps (such attacks have been mistakenly attributed to Aisuru), Kimwolf's operators also engage in aggressive sales of residential proxies, for as low as 0.20 cents per Gb.

"The discovery of pre-infected TV boxes and the monetization of these bots through secondary SDKs like Byteconnect indicates a deepening relationship between threat actors and commercial proxy providers. While the collaboration with IPIDEA led to a successful patch, the broader landscape remains precarious," Synthient notes.

Related: RondoDox Botnet Exploiting React2Shell Vulnerability

Related: New 'Broadside' Botnet Poses Risk to Shipping Companies

Related: Exposed Docker APIs Likely Exploited to Build Botnet

Related: RapperBot Botnet Disrupted, American Administrator Indicted

---

Source: https://www.securityweek.com/kimwolf-android-botnet-grows-through-residential-proxy-networks/