BadBox 3.0 Ad Fraud Botnet Disrupted: Uncertified Android Devices at Risk



Human Security says it disrupted BadBox 3.0, the largest ad fraud botnet by bid volume. It infects low-cost Android devices to show hidden ads and route third-party traffic through them as residential proxies.

- At its peak BadBox 3.0 generated about 40 billion bid requests a day and over 4% of CTV traffic seen by Human's platform.
- It targets low-cost, uncertified Android Open Source Project devices carrying backdoors that deliver fraud and proxy modules.
- Infected devices were enrolled in eleven residential proxy networks, including PXYEDGE.
- Human Security found several links to the Chinese manufacturer TXCZ.
- The real number of infections is likely significantly higher than the 367,000 requests seen on one

> repository mirror in a month.

Human Security reports that it has disrupted BadBox 3.0, which it describes as the largest ad fraud botnet by bid volume. It is the third iteration of an operation aimed at low-cost Android devices. BadBox 2.0 was first seen on more than 1 million devices and eventually reached more than 10 million.

What the botnet does

The botnet runs on uncertified Android Open Source Project devices infected with backdoors. These deliver fraud modules that render video ads in a hidden window, so bid requests appear to come from well-known apps that the operators impersonate. The owner sees nothing, while advertisers are billed for inventory that was never shown to a real viewer.

The same devices are also enrolled in eleven residential proxy networks, including PXYEDGE, a rebranded version of IpMoYu. Because much of the traffic came from residential proxy addresses, it passed as ordinary household viewing. At its peak the botnet produced about 40 billion bid requests a day.

Attribution and scale

Human Security found several links to the Chinese manufacturer TXCZ, including build property checks in the modules and a TXCZ domain serving payload routes and ad configurations. Some command-and-control domains were disrupted when Google took down XCPE, a botnet of over 1.3 million Android set-top boxes.

Human has not given a total size. One repository mirror served over 367,000 requests in a month, but the firm stresses this covers a single repository and a backup delivery channel, so actual infections are presumed significantly higher.

Relevance for organisations

The source does not mention Saudi Arabia. Still, low-cost connected devices used in offices, meeting rooms or digital signage could be enrolled as proxies, which would route third-party traffic through the organisation's network. Procurement and network controls are the practical defence.

What to do now

1. Inventory Android-based devices on your network, such as set-top boxes, signage players and streaming sticks, and flag uncertified or unknown-origin models.
2. Restrict such devices to an isolated network segment with no access to internal systems.
3. Monitor egress traffic from these segments for unusual outbound connections or residential proxy behaviour, and block unneeded access.
4. Add certification and supply chain checks to procurement of low-cost connected devices.

5. Remove or replace devices that show signs of preinstalled backdoors, and include them in your third-party and asset risk registers.