Industry Takedown of Botnet Hidden in More Than 1.3 Million TV Set-Top Boxes across 200 Countries

Google, Plume, TrendAI™, Lumen, HUMAN Security, Synthient and Japan's National Police Agency form coordinated effort combining security research, threat intelligence and network expertise to identify and disrupt X.CPE botnet

MOUNTAIN VIEW, Calif., Nov. 2, 2026 /PRNewswire/ -- Today, a group of private and public sector partners announced a coordinated takedown of X.CPE, a global botnet hidden in more than 1.3 million set-top boxes across more than 200 countries. Hidden on devices before they were ever sold, the botnet used subscribers' devices and home internet connections without their knowledge or consent. This takedown was led by Google, Plume, TrendAI™, Lumen, HUMAN Security and Synthient, along with Japan's National Police Agency.

"Operations like this raise the cost for criminals and show that the infrastructure they rely on isn't out of reach," **said Charley Snyder, Head of Disruption Operations at Google Threat Intelligence Group**. "Disrupting X.CPE took partners across industry working together. It's proof that collaboration is one of the most powerful tools we have against threats that cross borders and industries."

A familiar device hiding an unfamiliar threat

X.CPE was embedded in firmware, the software that controls a device's basic operations, before set-top boxes reached subscribers' homes. X.CPE was built to evade pre-release security checks, and Google has since updated its review process in response, as well as banned the responsible OEM and any future subsidiaries or affiliates from making devices with preloaded Google apps. Unlike infections that depend on a user opening a suspicious attachment or installing an application, this threat arrived as part of the device itself. Subscribers received no consent request, notification or opt-out options.

Google, Plume, TrendAI™, Lumen, HUMAN Security, Synthient, working with Japan's National Police Agency, carried out a coordinated disruption campaign against X.CPE. Each organization contributed in its own way, applying its expertise in connected-device security, malware analysis, network visibility and digital fraud to analyze the botnet and disrupt its operations.

Together they dismantled a threat hiding behind seemingly routine device activity: software embedded in TV set-top boxes that gave botnet controllers remote access and allowed them to exploit home broadband connections without subscriber consent. The takedown also disrupted the command-and-control domains that operate the criminal affiliates' malware modules. Because these affiliates distribute their modules through channels beyond X.CPE, Google assesses that taking down these domains will sever access to at least 10 million additional compromised devices.

The effort demonstrates the importance of connecting intelligence across organizations to confront threats that cross technology and network boundaries. By bringing together distinct perspectives on compromised devices, malicious software and internet traffic, the partners supported a coordinated takedown aimed at disrupting unauthorized access and monetization and addressing risks to subscriber privacy, broadband resources and trust in connected devices.

Turning home broadband into a business without permission

The botnet generated revenue from compromised devices in a variety of ways, including: reselling bandwidth, delivering video content, ad fraud, loading additional backdoors and, in earlier versions, installing apps for payment.

Residential proxy software allowed third-party traffic to pass through subscribers' internet connections, using their home internet addresses and bandwidth without permission. Researchers also found collection of device, network and account information, alongside persistent remote access capabilities.

For service providers, the findings highlight a supply chain risk that may not be apparent from a device's everyday performance. A functioning streaming box can still generate unexplained traffic and undermine trust in the broadband service.

"Protecting the connected home requires visibility into threats that subscribers cannot see and should not be expected to detect," said **Chris Griffiths, Chief Technology Officer at Plume**. **"**By contributing broadband intelligence to this joint effort, we helped expose hidden supply chain risks and support coordinated action to make networks safer for service providers and their subscribers**."**

Complementary expertise, coordinated action

The partners contributed to the Google-led effort to disrupt X.CPE:

TrendAI™
Robert McArdle, Director of Cybercrime Research at TrendAI™
"We applaud Google's decisive action in removing this threat. Our research identified over 1.3 million devices affected by this

"We applaud Google's decisive action in removing this threat. Our research identified over 45 million devices affected by this campaign. That's millions of households and businesses completely unaware that their equipment was being used as an accessory in active criminality - whether defrauding advertisers or piggybacking on their connections to carry out other attacks via residential proxies - which would commonly include identity theft impersonating people in their region. This action by Google and research partners significantly sets back these attackers, and TrendAI research will be watching them closely if they attempt to rebuild."

HUMAN
Gavin Reid, CISO at HUMAN
"Compromised-device networks are sustained by profit: operators take control of devices and household connections without consent, then monetise that access through proxy services and various fraud activities. Group action, as exemplified in this operation, interrupts the infrastructure needed for monetisation, raising the cost of operating these networks and weakening the incentives that sustain them. "

SYNTHIENT
Benjamin Brundage, CEO at Synthient.
"Illicit pay-per-install networks provide a significant backbone to the larger fraud ecosystem, powering everything from direct ad fraud to unregulated proxy networks that push credential stuffing and DDoS botnets. The takedown of X.Cpe helps protect this space as a whole, as well as the unsuspecting consumers victimized by this scheme." - Benjamin Brundage

Research and resources:

Google: https://cloud.google.com/blog/topics/threat-intelligence/shutting-the-door-on-the-xcpe-botnet
Plume: http://www.plume.com/xcpe-botnet-whitepaper-pdf
TrendAI™: https://www.trendaisecurity.com/en-us/resources-insights/trendai-security-blog/trendaitm-research-helps-disrupt-android-tv-botnet-of-more-than-13-million-pre-infected-devices

About Plume

Plume provides an AI-powered platform that enables internet service providers improve connectivity, security and the subscriber experience. Combining cloud-managed Wi-Fi, network intelligence and customer care orchestration, Plume helps service providers across more than 60 countries build subscriber confidence and operate more efficiently. More details about Plume.

About TrendAI™

TrendAI™, the global AI security leader and enterprise business unit of Trend Micro, empowers organizations with full AI visibility, governance, and consolidated security that inspires confidence, drive innovation, and eliminate risk. Trusted by the largest enterprises and governments across 185 countries, TrendAI™ secures the entire organization, from identities to infrastructure to data. Global Fortune 500 companies rely on TrendAI™ to stop threats up to 115 days earlier, powered by world-leading threat and attack intelligence. More details about trendaisecurity.com.

About Lumen

Lumen Technologies connects people, data and applications through its network and technology services. Its Black Lotus Labs threat research and operations team uses global network visibility to identify malicious activity, generate threat intelligence and help protect businesses and the internet. More details about Lumen Technologies.

About HUMAN Security

HUMAN Security helps organizations protect digital experiences by detecting and disrupting automated threats, fraud and abuse. Its technology and threat intelligence help enterprises and platforms verify digital interactions and establish trust across the customer journey. More details about humansecurity.com.

About Synthient

Synthient provides intelligence to identify residential proxies, VPNs and bot infrastructure, helping organizations assess traffic risk and investigate abuse. Its researchers analyze proxy networks, botnets and adversary infrastructure to expose emerging threats. More details about Synthient.

SOURCE Plume Design, Inc.

---

https://newsroom.trendmicro.com/2026-11-02-Industry-Takedown-of-Botnet-Hidden-in-More-Than-1-3-Million-TV-Set-Top-Boxes-across-200-Countries