TP-Link faces possible US ban as hijacked routers fuel Chinese attacks

Chinese hackers use botnet of TP-Link routers

Microsoft warned on October 31 that hackers working for the Chinese government are using a botnet of thousands of routers, cameras, and other Internet-connected devices for attacks on users of Microsoft's Azure cloud service. Microsoft said that "SOHO routers manufactured by TP-Link make up most of this network," referring to routers for small offices and home offices.

The WSJ said its sources allege that "TP-Link routers are routinely shipped to customers with security flaws, which the company often fails to address" and that "TP-Link doesn't engage with security researchers concerned about them." The article notes that "US officials haven't disclosed any evidence that TP-Link is a witting conduit for Chinese state-sponsored cyberattacks."

We contacted TP-Link today and will update this article if it provides a response. A TP-Link spokesperson told the WSJ that the company "welcome[s] any opportunities to engage with the US government to demonstrate that our security practices are fully in line with industry security standards, and to demonstrate our ongoing commitment to the US market, US consumers, and addressing US national security risks."

A March 2024 Hudson Institute policy memo by Michael O’Rielly, a former Federal Communications Commission member, said it remained “unclear how prevalent TP-Link’s vulnerabilities are compared to other wireless routers—from China or elsewhere—as there is no definitive comparison or ranking of routers based on security.” O’Rielly urged federal agencies to “keep track of TP-Link and other manufacturers’ cybersecurity practices and ownership structure, including any ties to the Chinese government,” but said “there is no evidence to suggest negligence or maliciousness with regard to past vulnerabilities or weaknesses in TP-Link’s security.”

New push against Chinese tech

TP-Link routers don’t seem to be tied to an ongoing Chinese hack of US telecom networks, dubbed Salt Typhoon. But that attack increased government officials’ urgency for taking action against Chinese technology companies. For example, the Biden administration is “moving to ban the few remaining operations of China Telecom,” a telco that was mostly kicked out of the US in 2021, The New York Times reported on Monday.

https://arstechnica.com/tech-policy/2024/12/report-us-considers-banning-tp-link-routers-over-security-flaws-ties-to-china/