Chinese hacking group APT31 uses mesh of home routers to disguise attacks

By Catalin Cimpanu

Published: 2022-12-12 · Archived: 2026-04-06 03:26:32 UTC

A Chinese cyber-espionage group known as APT31 (or Zirconium) has been seen hijacking home routers to form a proxy mesh around its server infrastructure in order to relay and disguise the origins of their attacks.

In a security alert published today, the French National Cybersecurity Agency, also known as ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), published a list of 161 IP addresses that have been hijacked by APT31 in recent attacks against French organizations.

The agency said the APT31 attacks started at the beginning of 2021 and are still ongoing.

French officials said that APT31's proxy botnet was used to perform both reconnaissance operations against their targets, but also to carry out the attacks themselves.

In a series of tweets today, Ben Koehl, a security researcher for the Microsoft Threat Intelligence Center, said APT31 was using this proxy network to make it appear that attacks are coming from the target organization's national IP address space.

One of the reasons for this tactic is that some organizations might be blocking incoming traffic from international IP addresses as a security measure.

> On the other side they are able to exit in the countries of their targets to _somewhat_ evade basic detection techniques.
>
> — bk (Ben Koehl) (@bkMSFT) July 21, 2021

ANSSI officials are now urging companies, both in France and in other countries, to take the 161 IP addresses and see if connections have been detected in network logs this year, which would suggest that an organization might have been the target of an APT31 operation.

"Finding one of the IOCs in logs does not mean the entire system has been compromised and further analysis will be required," the agency said.

According to William Thomas, a security researcher at security firm Cyjax, the IP addresses were located all over the world, and not all were located in France. A copy of the APT31 malware implant installed on the hacked routers was also identified on VirusTotal.

> — Will (@BushidoToken) July 21, 2021

APTs have used proxy meshes since 2018

The operational tactic of using home routers to create proxy meshes to disguise the origin of web attacks is a common tactic these days.

In most cases, hacked routers and IoT devices are assembled into botnets, which are then rented to cybercrime groups. These groups use the botnets as giant proxy meshes to relay a wide variety of malicious activity, such as brute-force attacks, vulnerability exploitation, port scanning operations, and traffic carrying stolen data.

But while the tactic has been widely used by financially motivated cybercrime groups, it has also been seen as part of the arsenal of nation-state hacking groups since at least April 2018, when Akamai mentioned APT abuse in a report [PDF] on the UPnProxy technique.

On another note, APT31 was also one of the two Chinese hacking groups, together with APT40, that the US and its allies accused on Monday of orchestrating a hacking campaign against Microsoft Exchange servers earlier this year.

The Record understands that APT31 used proxy meshes made of home routers as a way to scan the internet and then launch and disguise its attacks against Exchange email servers earlier this year; however, the technique was also used for other operations as well.

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
