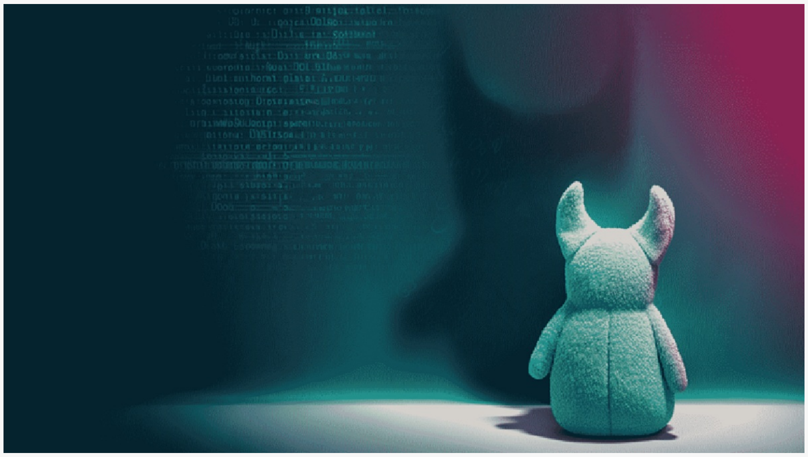
EINPRESSWIRE

ESET Research: Chinese PlushDaemon group compromises network devices for adversary-in-the-middle attacks



DUBAI , DUBAI, UNITED ARAB EMIRATES, November 24, 2025 /EINPresswire.com/ -- ESET researchers discovered that China-aligned threat group PlushDaemon performs adversary-in-the-middle attacks using a previously undocumented implant for network devices (e.g., a router) that ESET named EdgeStepper, which redirects all DNS queries to a malicious external DNS server that replies with the address of another node that performs the hijacking of updates. Effectively rerouting software updates traffic to attacker-controlled infrastructure with the aim of deploying the downloaders LittleDaemon and DaemonicLogistics in targeted machines and to ultimately distribute the SlowStepper implant. SlowStepper is a backdoor toolkit with dozens of components used for cyberespionage. These implants give PlushDaemon the capability to compromise targets anywhere in the world.

Since 2019, this China-aligned group has deployed attacks in the United States, New Zealand, Cambodia, Hong Kong, Taiwan, and mainland China itself. Among their victims were a university in Beijing, a Taiwanese company that manufactures electronics, a company in the automotive sector, and a branch of a Japanese company in the manufacturing sector.

In the discovered attack scenario, PlushDaemon first compromises a network device to which their target might connect; the compromise is probably achieved by exploiting a vulnerability in the software running on the device or through weak and/or well-known default administrative credentials, enabling the attackers to deploy EdgeStepper (and possibly other tools).

“Then, EdgeStepper begins redirecting DNS queries to a malicious DNS node that verifies whether the domain in the DNS query message is related to software updates, and if so, it replies with the IP address of the hijacking node. Alternatively, we have also observed that some servers are both the DNS node and the hijacking node; in those cases, the DNS node replies to

DNS queries with its own IP address,” says ESET researcher Facundo Muñoz, who discovered and analyzed the attack. “Several popular Chinese software products had their updates hijacked by PlushDaemon via EdgeStepper,” he adds.

PlushDaemon is a China-aligned threat actor active since at least 2018 that engages in espionage operations against individuals and entities in East Asia-Pacific and the United States. It uses a custom backdoor that ESET tracks as SlowStepper. In the past, ESET Research has observed the group gaining access via vulnerabilities in web servers, and in 2023 it performed a supply-chain attack.

For a more detailed analysis of the latest PlushDaemon activity, check out the latest ESET Research blogpost “PlushDaemon compromises network devices for adversary-in-the-middle attacks” on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge cybersecurity to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown—securing businesses, critical infrastructure, and individuals. Whether it’s endpoint, cloud, or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit ESET Middle East or follow us on LinkedIn, Facebook & X.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here
