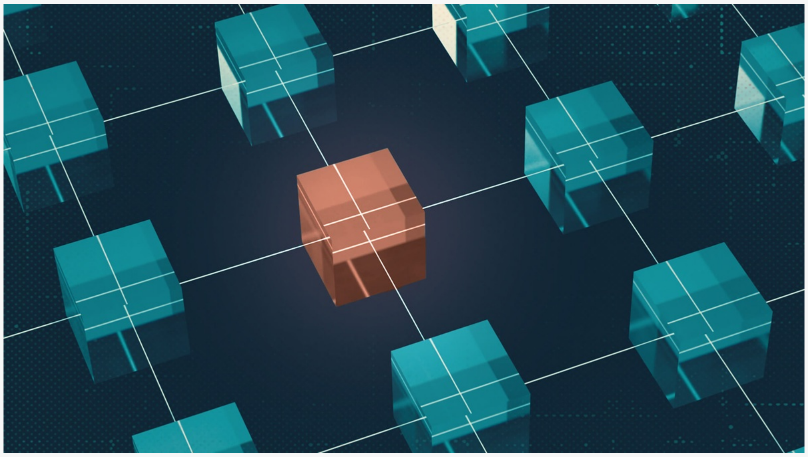
EINPRESSWIRE

ESET discovers new China-aligned APT group PlushDaemon and its supply chain attack on South Korean VPN service



DUBAI , DUBAI, UNITED ARAB EMIRATES, January 24, 2025 /EINPresswire.com/ -- ESET researchers have discovered a supply-chain attack against a VPN provider in South Korea by a newly discovered and previously undetected China-aligned APT group that ESET has named PlushDaemon. In this cyberespionage operation, the attackers replaced the legitimate installer with one that also deployed the group's signature implant, which ESET has named SlowStepper — a feature-rich backdoor with a toolkit of more than 30 components. The China-aligned threat actor has been active since at least 2019, engaging in espionage operations against individuals and entities in mainland China, Taiwan, Hong Kong, South Korea, the United States, and New Zealand.

“In May 2024, we noticed detections of malicious code in an NSIS installer for Windows that users from South Korea had downloaded from the website of the legitimate VPN software IPany. In further analysis, we discovered that the installer was deploying both the legitimate software and the backdoor. We contacted the VPN software developer to inform them of the compromise, and the malicious installer was removed from their website,” says ESET researcher Facundo Muñoz, who made the discovery.

Additionally, PlushDaemon gains initial access via the technique of hijacking legitimate updates of Chinese applications by redirecting traffic to attacker-controlled servers. ESET has also observed the group gaining access via vulnerabilities in legitimate web servers.

The SlowStepper backdoor is used exclusively by PlushDaemon. This backdoor is notable for its multistage C&C protocol using DNS, as well as its ability to download and execute dozens of additional Python modules with espionage capabilities.

The malware collects a wide range of data from web browsers; is capable of taking photos; scans for documents; collects information from various applications, including messaging applications (e.g., WeChat, Telegram); can spy via audio and video; and steals password credentials.

“The numerous components in the PlushDaemon toolset, and its rich version history, show that, while previously unknown, this China-aligned APT group has been operating diligently to develop a wide array of tools, making it a significant threat to watch out for,” concludes Muñoz.

For a more detailed analysis and technical breakdown of PlushDaemon’s toolset, check out the latest ESET Research blogpost “China-aligned PlushDaemon compromises supply chain of Korean VPN service” on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge digital security to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of known and emerging cyberthreats — 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. An 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 www.eset.com or follow us on LinkedIn, Facebook, and X.

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