Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:39:19 UTC

APT group: PlushDaemon

Names	PlushDaemon *(ESET)*
Country	China
Motivation	Information theft and espionage
First seen	2019
Description	(ESET) 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 (https://ipany.kr/; see Figure 1), which is developed by a South Korean company. Upon further analysis, we discovered that the installer was deploying both the legitimate software and the backdoor that we've named SlowStepper. We contacted the VPN software developer to inform them of the compromise, and the malicious installer was removed from their website. We attribute this operation to PlushDaemon – a China-aligned threat actor active since at least 2019, engaging in espionage operations against individuals and entities in China, Taiwan, Hong Kong, South Korea, the United States, and New Zealand. PlushDaemon uses a custom backdoor that we track as SlowStepper, and its main initial access technique is to hijack legitimate updates by redirecting traffic to attacker-controlled servers. Additionally, we have observed the group gaining access via vulnerabilities in legitimate web servers.
Observed	Countries: China, Hong Kong, New Zealand, South Korea, Taiwan, USA.
Tools used	SlowStepper.
Information	<https://www.welivesecurity.com/en/eset-research/plushdaemon-compromises-supply-chain-korean-vpn-service/>

Last change to this card: 22 February 2025

Download this actor card in PDF or JSON format