LevelBlue - Open Threat Exchange

By dekaRituraj

Archived: 2026-04-05 21:56:56 UTC

Two previously undocumented pieces of malware, a downloader and a backdoor, were used in a watering hole operation attributed to the Russian-based threat group Turla. To reach targets of interest, the hackers compromised at least four websites, two of them belonging to the Armenian government. This indicates that the threat actor was after government officials and politicians. The new tools are a .NET malware dropper called NetFlash and a Python-based backdoor named PyFlash. They would be delivered following a fake Adobe Flash update notification received by victims. After gaining access to the website, the hackers added a piece of malicious JavaScript code that loaded from the external source ‘skategirlchina[.]com’ a script designed to fingerprint the visitor’s web browsers.
