LevelBlue - Open Threat Exchange

By TheNewRaikage

Archived: 2026-04-06 00:49:04 UTC

FileHash-SHA256: 5 | **IPv4:** 1 | **URL:** 2 | **Hostname:** 1

For the past several weeks, Forcepoint Security Labs have been tracking a seemingly low-profile piece of malware which piqued our interest for a number of reasons: few samples appear to be available in the wild; there is no previous documentation referring to the C2 domains and IP addresses it uses (despite the domains appearing to be at least twelve months old); and, if its compilation timestamps are to be trusted, the campaign itself may have been active for at least six months before samples started to surface... The primary samples examined appear in the wild with filenames mimicking that of Adobe's Content Management System [1] and offers a range of commands typical of Remote Access Tools: file upload, file download, file execution, and command execution.
