LevelBlue - Open Threat Exchange

By AlienVault

Archived: 2026-04-05 18:45:16 UTC

FileHash-MD5: 7 | **FileHash-SHA1:** 7 | **FileHash-SHA256:** 32 | **URL:** 3 | **YARA:** 16 | **Hostname:** 4

Unit 42 discovered new activity that appears related to an adversary group previously called “C0d0so0” or “Codoso”. This group is well known for a widely publicized attack involving the compromise of Forbes.com, in which the site was used to compromise selected targets via a watering hole to a zero-day Adobe Flash exploit. Compared to other adversary groups, C0d0so0 has shown the use of more sophisticated tactics and tools and has been linked to leveraging zero-day exploits on numerous occasions in combination with watering hole and spear phishing attacks. In the newly discovered attack campaign, Unit 42 identified attacks targeting organizations within the telecommunications, high tech, education, manufacturing, and legal services industries. The attacks likely were initially delivered via spear-phishing e-mails, or as demonstrated by C0d0so0 in the past, legitimate websites that had been previously compromised then used as watering holes for the selected victims.
