LevelBlue - Open Threat Exchange

By zer0daydan

Archived: 2026-04-05 15:46:28 UTC

Palo Alto observed an attack led by the APT group Wekby targeting a US-based organization in recent weeks. Wekby is a group that has been active for a number of years, targeting various industries such as healthcare, telecommunications, aerospace, defense, and high tech. The group is known to leverage recently released exploits very shortly after those exploits are available, such as in the case of HackingTeam’s Flash zero-day exploit. The malware used by the Wekby group has ties to the HTTPBrowser malware family, and uses DNS requests as a command and control mechanism. Additionally, it uses various obfuscation techniques to thwart researchers during analysis. Based on metadata seen in the discussed samples, Palo Alto has named this malware family ‘pisloader’.
