LevelBlue - Open Threat Exchange

By Tr1sa111

Archived: 2026-04-05 17:48:16 UTC

- 258 Subscribers

- 181 Subscribers

Threat Research | FireEye Inc

Find out more about FireEye.com, the world's leading cyber security company, which provides security services to more than 1.5 million customers across the globe, and offers a wide range of products and services.

- 17 Subscribers

Downeks and Quasar RAT Used in Recent Targeted Attacks Against Governments

FileHash-SHA256: 101 | **Domain:** 14 | **Hostname:** 20

DustySky is a campaign which others have attributed to the Gaza Cybergang group, a group that targets government interests in the region. The initial infection vector in this attack is not clear, but it results in installing the “Downeks” downloader, which in turn infects the victim computer with the “Quasar” RAT. Downeks uses third party websites to determine the external IP of the victim machine, possibly to determine victim location with GeoIP. It also drops decoy documents in an attempt to camouflage the attack. Quasar is a .NET Framework-based open-source RAT. The attackers invested significant effort in attempting to hide the tool by changing the source code of the RAT and the RAT server, and by using an obfuscator and packer.

- 373,953 Subscribers

Source: https://otx.alienvault.com/browse/pulses?q=tag:Downeks