SilkParasite: government networks across Central Asia and Georgia

Bitdefender has published a campaign running against government bodies in five Central Asian states and Georgia since late 2025. Seven remote access tool families, five newly named, and lures written to impersonate specific ministries.

INCIDENT DETAILS · 5WH

Who A cluster Bitdefender tracks as SilkParasite and assesses at medium confidence to be China-nexus. That assessment is one vendor's and is uncorroborated.
What Seven RAT families, five previously undocumented and newly named. About 65 machines carried the principal tool.
Where Government targets in Uzbekistan, Turkmenistan, Kyrgyzstan, Tajikistan, Kazakhstan and Georgia.
When Activity from late 2025 to at least August 2026; disclosed 19 Aug 2026.
Why Consistent with state collection against the governments concerned, but no motive established.
How Spear-phishing with password-protected archives; the macro checks whether Kaspersky is running and adapts before side-loading.

IMPACT

- Confidentiality: persistent remote access to government networks across six states, with unquantified loss.
- Detection cost: five new tool families in one disclosure means five sets of indicators to deploy and no history of them.
- Sovereignty: six governments with limited independent capability carrying external access to their own information.
- Regional: Central Asia and the South Caucasus are of interest to more than one external party.

SEQUENCE OF EVENTS

Late 2025 First activity observed
19 Aug 2026 Bitdefender publishes
Prior UAC-0063 and FamousSparrow here

1 A password-protected archive arrives
2 The lure impersonates a named ministry
3 The macro checks for Kaspersky and adapts
4 Tools side-loaded via a legitimate program
5 About 65 machines carry the main tool

ASSESSMENT, LESSONS, AND RECOMMENDATIONS

- The macro adapting to the antivirus present is target-aware tradecraft, not commodity malware.
- Password-protected archives work because the gateway cannot see inside them and the recipient supplies the key.
- The AI finding is narrower than the headlines: assisted development, not generated malware.
- The attribution has a stated basis and remains one vendor at medium confidence.