

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:42:55 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool SilkBean

Tool: SilkBean

Names	SilkBean
Category	Malware
Type	Reconnaissance , Backdoor , Info stealer , Exfiltration , Downloader
Description	(Lookout) A hallmark of SilkBean is the comprehensive RAT (remote access trojan) functionality that allows an attacker to execute over 70 different commands on an infected device. SilkBean is delivered via applications that possess malicious functionality, but mimic titles and icons that a target may want to install. The legitimate app with functionality the user expects is packaged within the malware and installed after SilkBean successfully infects a target device.
Information	< https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf >
MITRE ATT&CK	< https://attack.mitre.org/software/S0549/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/apk.silkbean >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:SilkBean >

Last change to this tool card: 30 December 2022

Download this tool card in [JSON](#) format

All groups using tool SilkBean

Changed	Name	Country	Observed
APT groups			
	Ke3chang , Vixen Panda , APT 15 , GREF , Playful Dragon		2010-Oct 2024

1 group listed (1 APT, 0 other, 0 unknown)

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=747eae20-6c45-4079-b4f3-8f841b60c32d>