Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:26:33 UTC

Tool: DoubleAgent

Names	DoubleAgent
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Lookout) In 2013 Citizen Lab reported on a compromised version of KakaoTalk, which had been used to target a prominent individual in the Tibetan community. This app was the first publicly exposed sample of a malware family called DoubleAgent. When Lookout initially investigated DoubleAgent in 2015, it was already an advanced Android remote access tool (RAT). Early versions of this family trojanized apps such as Voxer and TalkBox, as well as Amaq News, the official Daesh news application. The extent of this malware family and its connections to other campaigns has not been publicly reported on until now. Lookout researchers have seen DoubleAgent used exclusively against groups with contentious relationships with the Chinese government. Although Lookout has been tracking this malware family for many years, new samples discovered in the last year indicated that the actors behind DoubleAgent were continuing to evolve the surveillanceware and use new infrastructure. However, they maintained the same targeting, as well as several key malware characteristics, such as similar decryption keys for configuration files. These recent samples, discovered in late 2019, are the focus of this section on DoubleAgent. A decryption of the configuration files from these samples revealed a direct overlap in C2 infrastructure between the operators of DoubleAgent and SilkBean at a time when both malware families appeared to be active.
Information	<https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf> <https://citizenlab.ca/2013/04/permission-to-spy-an-analysis-of-android-malware-targeting-tibetans/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0550/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.doubleagent>

AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:DoubleAgent>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool DoubleAgent

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.etda.or.th/cgi-bin/listgroups.cgi?u=70767fb4-c613-4566-837f-81dc2e9d5ece