Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:56:19 UTC

Tool: ActionSpy

Names	ActionSpy AxeSpy
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Trend Micro) This malware impersonates a legitimate Uyghur video app called Ekran. The malicious app has the same appearance and features as the original app. It is able to achieve this with VirtualApp. In addition, it's also protected by Bangcle to evade static analysis and detection. Every 30 seconds, ActionSpy will collect basic device information like IMEI, phone number, manufacturer, battery status, etc., which it sends to the C&C server as a heartbeat request. The server may return some commands that will be performed on the compromised device. All the communication traffic between C&C and ActionSpy is encrypted by RSA and transferred via HTTP.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.actionspy>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:actionspy>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool ActionSpy

Changed	Name	Country	Observed
APT groups			

	Poison Carp, Evil Eye		2018-Jun 2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f1efe8d0-5fcc-4443-b2aa-cfe89f0ff366