Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:49:10 UTC

Tool: AndoServer

Names	AndoServer
Category	Malware
Type	Backdoor, Reconnaissance, Info stealer, Exfiltration
Description	(Lookout) Some AndoServer samples are purely surveillanceware that do not even pretend to be anything else, while others, like this sample here, contain legitimate applications inside the malware, with the benign APK hidden in the res/raw folder. AndoServer samples receive commands, and are capable of: • Taking a screenshot • Getting battery levels and if the device is plugged in • Reporting location (latitude and longitude) • Getting a list of installed applications • Launching an application specified by the malicious actor • Checking the number of cameras on a device • Choosing a specific camera to access • Creating a specific pop-up message (toast) • Recording audio • Creating a file on external storage • Exfiltrating call logs • Listing files contained in a specified directory • Calling a phone number • Exfiltrating SMS messages • Sending SMS to a phone number • Exfiltrating the contact list • Playing a ringtone and then sleeping AndoServer malware has its C2 domain or IP address hard coded into the source code. Each sample also has its own unique identifier string at the start of its communication with C2 servers, that appears to be for the actor to monitor which application in their arsenal is responsible for the compromise, as they can see the unique application installed by the specific victim. While not always the case, some unique identifiers are similar to the name of the C2

	domain, while other times they refer to the title of the application, highlighting another level of customization of this malware.
Information	<https://blog.lookout.com/nation-state-mobile-malware-targets-syrians-with-covid-19-lures>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool AndoServer

Changed	Name	Country	Observed	
APT groups				
	Syrian Electronic Army (SEA), Deadeye Jackal		2011-Aug 2021	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=07eb732e-d8d4-45a1-8727-f5ef8f8f3ef6