Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:48:57 UTC

Tool: CarbonSteal

Names	CarbonSteal
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Lookout) CarbonSteal is Android surveillanceware that has been tracked by Lookout since 2017, and more than 500 samples have been seen to date. While not as sophisticated as HenBox, certain samples of CarbonSteal do make use of a combination of native libraries and DEX classes, while others do not and are much simpler. Hallmarks of CarbonSteal include extensive audio recording functionality in a variety of codecs and audio formats, as well as the capability in later samples to control an infected device through specially crafted SMS messages. Attackers can also perform audio surveillance through the malware's ability to silently answer a call from a specific phone number and allow the attacker to listen in to sounds around an infected device. Based on this functionality, we suspect that CarbonSteal might be deployed in areas with insufficient or no mobile data coverage. Samples of CarbonSteal and HenBox also use the same non-compromised signing certificates in many cases, suggesting the actor behind their deployment is the same. Furthermore, overlapping validity dates of these certificates may indicate that the samples were produced around the same time frame. This evidence led Lookout researchers to the theory that these tools were primarily used in an ongoing malware campaign (at the time) and against similar targets, with titles and languages once again suggesting a Uyghur focused interest.
Information	<https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0529/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.carbonsteal>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:CarbonSteal>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool CarbonSteal

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=b0732e1a-4e75-4e04-9115-2e8c7fbd19c9