Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:49:12 UTC

Tool: scanbox

Names	scanbox
Category	Malware
Type	Reconnaissance, Info stealer, Keylogger, Downloader
Description	(Recorded Future) Scanbox is a reconnaissance framework that enables attackers to track visitors to compromised websites, performs keylogging, and harvests data that could be used to enable follow-on compromises. It has also been reported to have been modified in order to deliver secondary malware on targeted hosts. Written in Javascript and PHP, Scanbox deployment negates the need for malware to be downloaded onto the host device.
Information	<https://www.recordedfuture.com/scanbox-framework-campaign/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/js.scanbox>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:scanbox>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool scanbox

Changed	Name	Country	Observed	
APT groups				
	Leviathan, APT 40, TEMP.Periscope		2013-Jul 2021	

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