Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:15:54 UTC

Tool: TOUCHSHOT

Names	TOUCHSHOT
Category	Malware
Type	Info stealer
Description	(Mandiant) TOUCHSHOT takes screenshots of the system on which it is running and saves them to a file to be retrieved by the threat actor at a later time. TOUCHSHOT is configured to take a screenshot every three seconds, and then uses ZLIB to compress the images. The compressed data is then appended to a file that it creates and continues appending new screenshots to this file until the file reaches five megabytes in size, at which point it will create a new file with the same naming convention. TOUCHSHOT was seen embedded in the same instance of TOUCHSHIFT as TOUCHKEY.
Information	<https://www.mandiant.com/resources/blog/lightshow-north-korea-unc2970>

Last change to this tool card: 25 April 2023

Download this tool card in JSON format

All groups using tool TOUCHSHOT

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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