Threat Group Cards: A Threat Actor Encyclopedia

Tool: TOUCHSHIFT

Names	TOUCHSHIFT
Category	Malware
Type	Dropper
Description	(Mandiant) TOUCHSHIFT is a malicious dropper that masquerades as mscoree.dll or netplwix.dll. TOUCHSHIFT is typically created in the same directory and simultaneously as a legitimate copy of a Windows binary. TOUCHSHIFT leverages DLL Search Order Hijacking to use the legitimate file to load and execute itself. TOUCHSHIFT has been observed containing one to two various payloads which it executes in-memory. Payloads that have been seen include TOUCHSHOT, TOUCHKEY, HOOKSHOT, TOUCHMOVE, and SIDESHOW.
Information	<https://www.mandiant.com/resources/blog/lightshow-north-korea-unc2970>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.touchshift>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool TOUCHSHIFT

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

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