Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:13:11 UTC

Tool: TOUCHMOVE

Names	TOUCHMOVE
Category	Malware
Type	Loader
Description	(Mandiant) TOUCHMOVE is a loader that decrypts a configuration file and a payload, both of which must be on disk, and then executes the payload. TOUCHMOVE generates an RC6 key to decrypt the two files by querying the system's BIOS date, version, manufacturer, and product name. Once decrypted, the results are XOR encoded with a hardcoded key. If the generated RC6 key is incorrect, the configuration and payload files will not successfully decrypt, indicating that UNC2970 compiles instances of TOUCHMOVE after having already conducted reconnaissance on the target victim system. Once the RC6 key is successfully generated, a handle is created to the configuration file, and the decryption process is conducted. If the configuration file is successfully decrypted, the payload's full path is located within it, and the same decryption process then occurs on the payload. Following this, the payload is executed.
Information	<https://www.mandiant.com/resources/blog/lightshow-north-korea-unc2970>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.touchmove>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool TOUCHMOVE

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

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