Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:22:16 UTC

Tool: Hotwax

Names	Hotwax HOTWAX
Category	Malware
Type	Loader
Description	HOTWAX is a module that upon starting imports all necessary system API functions, and searches for a .CHM file. HOTWAX decrypts a payload using the Spritz algorithm with a hard-coded key and then searches the target process and attempts to inject the decrypted payload module from the CHM file into the address space of the target process.
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf> <https://content.fireeye.com/apt/rpt-apt38> <https://www.welivesecurity.com/2017/02/16/demystifying-targeted-malware-used-polish-banks/> <https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Kalnai-Poslusny.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.hotwax>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool Hotwax

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

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