Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:24:00 UTC

Tool: Hermes

Names	Hermes
Category	Malware
Type	Ransomware
Description	(Malwarebytes) The ransomware copies itself into %TEMP% under the name svchosta.exe and redeploys itself from that location. The initial sample is then deleted. The ransomware is not particularly stealthy—some windows pop up during its run. For example, we are asked to run a batch script with administrator privileges. The authors didn't bother to deploy any UAC bypass technique, relying only on social engineering for this. The pop-up is deployed in a loop, and by this way it tries to force the user into accepting it. But even if we don't let the batch script be deployed, the main executable proceeds with encryption.
Information	<https://blog.malwarebytes.com/threat-analysis/2018/03/hermes-ransomware-distributed-to-south-koreans-via-recent-flash-zero-day/> <https://blog.dcso.de/enterprise-malware-as-a-service/> <https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.hermes>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool Hermes

Changed	Name	Country	Observed
APT groups			

	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=af449984-8b3c-48da-aec9-bf6a133f3f8c