Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:58:17 UTC

Tool: LEMPO

Names	LEMPO
Category	Malware
Type	Reconnaissance, Info stealer, Exfiltration
Description	(Proofpoint) Once the malware, which is an updated version of Liderc that Proofpoint has dubbed LEMPO, establishes persistence, it can perform reconnaissance on the infected machine, save the reconnaissance details to the host, exfiltrate sensitive information to an actor-controlled email account via SMTPS, and then cover its tracks by deleting that day's host artifacts.
Information	<https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media>
AlienVault OTX	<https://otx.alienvault.com/browse/global/pulses?q=tag:LEMPO>

Last change to this tool card: 10 August 2021

Download this tool card in JSON format

All groups using tool LEMPO

Changed	Name	Country	Observed	
APT groups				
	Tortoiseshell, Imperial Kitten		2018-Oct 2023	

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