Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:39:41 UTC

Tool: BottomLoader

Names	BottomLoader
Category	Malware
Type	Downloader
Description	(Talos) Pivoting off the NineRAT samples, we discovered two additional malware families written in DLang by Lazarus. One of these is simply a downloader we track as “BottomLoader” meant to download and execute the next stage payload from a remote host such as HazyLoad.
Information	<https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bottomloader>

Last change to this tool card: 17 January 2024

Download this tool card in JSON format

All groups using tool BottomLoader

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=ad4c5c3e-7c81-4920-bea8-cee14ff7831f