Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:12:29 UTC

Tool: Godzilla

Names	Godzilla Godzilla Loader
Category	Malware
Type	Downloader, Worm, Botnet
Description	(Check Point) Enter Godzilla Loader, a malware being advertised on Dark Web forums, and being actively developed right now. Godzilla fills the “downloader” or “dropper” niche, offering a level of indirection such that the binary that first runs on the victim machine does not contain any of the actual payload, and instead downloads the payload from a remote server. Godzilla is actively maintained, with new features being added periodically, and retails for $500, around a quarter of the asking price of its better-established competitor, Emotet.
Information	<https://research.checkpoint.com/2018/godzilla-loader-and-the-long-tail-of-malware/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.godzilla_loader>

Last change to this tool card: 29 April 2020

Download this tool card in JSON format

All groups using tool Godzilla

Changed	Name	Country	Observed	
APT groups				
	Dalbit		2022	
	Earth Alux		2023	
	Operation Silent Skimmer	[Unknown]	2022	

Other groups

	TA554	[Unknown]	2017	

4 groups listed (3 APT, 1 other, 0 unknown)
