Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 12:09:39 UTC

Tool: GIMMICK

Names	GIMMICK
Category	Malware
Type	Backdoor, Downloader, Exfiltration
Description	(Volexity) GIMMICK is used in targeted attacks by Storm Cloud, a Chinese espionage threat actor known to attack organizations across Asia. It is a feature-rich, multi-platform malware family that uses public cloud hosting services (such as Google Drive) for command-and-control (C2) channels. The newly identified macOS variant is written primarily in Objective C, with Windows versions written in both .NET and Delphi. Despite core differences in programming languages used and operating systems targeted, Volexity tracks the malware under the same name due to shared C2 architecture, file paths, and behavioral patterns used by all variants.
Information	<https://www.volexity.com/blog/2022/03/22/storm-cloud-on-the-horizon-gimmick-malware-strikes-at-macos/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/osx.gimmick> <https://malpedia.caad.fkie.fraunhofer.de/details/win.gimmick>

Last change to this tool card: 27 August 2024

Download this tool card in JSON format

All groups using tool GIMMICK

Changed	Name	Country	Observed	
APT groups				
	Bronze Highland		2012-Jul 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=9243117d-7400-455a-a9cc-98413c1681d8