Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 12:37:16 UTC

Tool: Pantegana

Names	Pantegana
Category	Tools
Type	Backdoor
Description	(Recorded Future) Pantegana is an open-source malware family written in Go that features a cross-platform payload client Windows, Linux, OSX and uses HTTPS for C2 communications. It supports file upload and download, system fingerprinting, and direct command-line interaction with infected hosts. Pantegana also supports obfuscation using the open-source obfuscator Garble. Publicly reported use of Pantegana in the wild to date is minimal, other than a campaign exploiting a zero-day vulnerability in the Sophos Firewall appliance attributed by Volexity to the suspected Chinese state-sponsored threat activity group DriftingCloud.
Information	<https://go.recordedfuture.com/hubfs/reports/cta-2024-0716.pdf>

Last change to this tool card: 27 August 2024

Download this tool card in JSON format

All groups using tool Pantegana

Changed	Name	Country	Observed	
APT groups				
	TAG-100		2024	

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