Troll Stealer - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:11:33 UTC

Tool: Troll Stealer

Names	Troll Stealer TrollAgent
Category	Malware
Type	Info stealer
Description	(S2W Talon) S2W Talon has named the malware “Troll Stealer” because it contains the pathname “D:/~/repo/golang/src/root.go/s/troll/agent” within the malware. Troll Stealer can steal information from the infected system like SSH, FileZilla, C drive files/directories, browser, system information, screen captures and send it to the C&C server.
Information	<https://medium.com/s2wblog/kimsuky-disguised-as-a-korean-company-signed-with-a-valid-certificate-to-distribute-troll-stealer-cfa5d54314e2>
MITRE ATT&CK	<https://attack.mitre.org/software/S1196>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.troll_stealer>

Last change to this tool card: 28 June 2025

Download this tool card in JSON format

All groups using tool Troll Stealer

Changed	Name	Country	Observed	
APT groups				
	Kimsuky, Velvet Chollima		2012-Aug 2025	

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