Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:59:58 UTC

Tool: PoohMilk Loader

Names	PoohMilk Loader PoohMilk
Category	Malware
Type	Loader
Description	(Palo Alto) Our analysis shows that PoohMilk is the first stage loader. After a successful exploitation, it sets persistence in the registry with the appropriate command line argument to execute the second stage payload, in this case, Freenki Loader.
Information	<https://unit42.paloaltonetworks.com/unit42-freemilk-highly-targeted-spear-phishing-campaign/> <http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.poohmilk>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:poohmilk>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool PoohMilk Loader

Changed	Name	Country	Observed	
APT groups				
	Reaper, APT 37, Ricochet Chollima, ScarCruft		2012-Mar 2025	

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