Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:49:30 UTC

Tool: JuicyPotato

Names	JuicyPotato
Category	Exploits
Type	Backdoor
Description	A sugared version of RottenPotatoNG, with a bit of juice, i.e. another Local Privilege Escalation tool, from a Windows Service Accounts to NT AUTHORITY\SYSTEM.
Information	<https://github.com/ohpe> <https://lifars.com/wp-content/uploads/2020/06/Cryptocurrency-Miners-XMRig-Based-CoinMiner-by-Blue-Mockingbird-Group.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.juicy_potato>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool JuicyPotato

Changed	Name	Country	Observed	
APT groups				
	APT 33, Elfin, Magnallium		2013-Apr 2024	
	Dalbit		2022	
	Flax Typhoon		2021-Nov 2023	
	Gelsemium		2014-2023	
	Operation Silent Skimmer	[Unknown]	2022	

	Parisite, Fox Kitten, Pioneer Kitten		2017-Nov 2020	
	Sandworm Team, Iron Viking, Voodoo Bear		2009-Dec 2024	
	Volatile Cedar		2012-Early 2020	

8 groups listed (8 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=728448ac-d8dc-47bc-b5cc-8bfff10a6e88