Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:14:51 UTC

Tool: FlowCloud

Names	FlowCloud
Category	Malware
Type	Reconnaissance, Backdoor, Keylogger, Info stealer, Exfiltration
Description	(Proofpoint) While we found the ultimate execution method for both the LookBack GUP Proxy Tool and FlowCloud malware were the same across both macro versions, we found that the FlowCloud macro introduced a new method for the delivery of the malware. FlowCloud malware is capable of RAT functionalities based on its available commands including accessing the clipboard, installed applications, keyboard, mouse, screen, files, services, and processes with the ability to exfiltrate information via command and control. Additionally, the malware variants analyzed have several distinct characteristics that indicate the malware may have been active in the threat landscape since at least July 2016.
Information	<https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new> <https://www.proofpoint.com/us/blog/threat-insight/flowcloud-version-413-malware-analysis> <https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape> <https://nao-sec.org/2021/01/royal-road-redive.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.flowcloud>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:FlowCloud>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool FlowCloud

Changed	Name	Country	Observed

APT groups

	LookBack, TA410	[Unknown]	2019-Feb 2022	

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