Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:05:04 UTC

Tool: KopiLuwak

Names	KopiLuwak
Category	Malware
Type	Reconnaissance, Backdoor
Description	(Kaspersky) The KopiLuwak script is decoded by macro code very similar to that previously seen with IcedCoffee, but the resulting script is not the final step. This script is executed with a parameter used as a key to RC4 decrypt an additional layer of javascript that contains the system information collection and command and control beaconing functionality. KopiLuwak performs a more comprehensive system and network reconnaissance collection, and like IcedCoffee leaves very little on disk for investigators to discover other than the base script.
Information	<https://securelist.com/shedding-skin-turlas-fresh-faces/88069/> <https://securelist.com/blog/research/77429/kopiluwak-a-new-javascript-payload-from-turla/> <https://www.proofpoint.com/us/threat-insight/post/turla-apt-actor-refreshes-kopiluwak-javascript-backdoor-use-g20-themed-attack>
MITRE ATT&CK	<https://attack.mitre.org/software/S1075>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/js.kopiluwak>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool KopiLuwak

Changed	Name	Country	Observed	
APT groups				
	Tomiris	[Unknown]	2020	

	Turla, Waterbug, Venomous Bear		1996-2024	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=bf8419b4-0007-4045-bf5f-646e9bfbdc07