Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:54:13 UTC

Tool: LiteDuke

Names	LiteDuke
Category	Malware
Type	Backdoor
Description	(ESET) LiteDuke is a third-stage backdoor that was mainly used in 2014-2015. It is not directly linked to Operation Ghost, but we found it on some machines compromised by MiniDuke. We chose to document is mainly because we did not find it described elsewhere. We have dubbed it LiteDuke because it used SQLite to store information such as its configuration.
Information	<https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/> <https://norfolkinfosec.com/looking-back-at-liteduke/> <https://www.carbonblack.com/2020/03/26/the-dukes-of-moscow/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0513/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.liteduke>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool LiteDuke

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=99ff3fb6-edf3-4c07-b789-3ce1673cd753