Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:23:47 UTC

Tool: FatDuke

Names	FatDuke
Category	Malware
Type	Backdoor
Description	(ESET) FatDuke, the third stage. This sophisticated backdoor implements a lot of functionalities and has a very flexible configuration. Its code is also well obfuscated using manu opaque predicates. They re-comple it and modify the obfuscation frequently to bypass security product detections.
Information	<https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/> <https://www.secureworks.com/research/threat-profiles/iron-hemlock>
MITRE ATT&CK	<https://attack.mitre.org/software/S0512/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.fatduke>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool FatDuke

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

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