Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:27:40 UTC

Tool: Rook

Names	Rook
Category	Malware
Type	Ransomware
Description	According to PCrisk, Rook is ransomware (an updated variant of Babuk) that prevents victims from accessing/opening files by encryptir file/ransom note ('HowToRestoreYourFiles.txt'). Rook renames files by appending the '.Rook' extension. For example, it renames '1.jpg'
Information	<https://github.com/Dump-GUY/Malware-analysis-and-Reverse-engineering/blob/main/NightSky_Ransomware%E2%80%93just_a_Rook_RW_fork_in_VMProtect_suit/NightSky_Ransomware%E2% <https://chuongdong.com/reverse%20engineering/2022/01/06/RookRansomware/> <https://seguranca-informatica.pt/rook-ransomware-analysis/> <https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader> <https://blog.cyble.com/2022/03/15/deep-dive-analysis-pandora-ransomware/> <https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.rook>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool Rook

Changed	Name	Country	Observed	
APT groups				
	Bronze Starlight		2021-Mar 2023	

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

↑

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=c454ae0f-ae6d-4d20-a7dc-78665a109e37