Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:54:12 UTC

Tool: LOOKOVER

Names	LOOKOVER
Category	Malware
Type	Info stealer
Description	(Mandiant) The threat actor's first attempt to extend their access to the network appliances by targeting the TACACS server was the use of LOOKOVER. LOOKOVER is a sniffer written in C that processes TACACS+ authentication packets, performs decryption, and writes its contents to a specified file path. LOOKOVER uses the publicly available libpcap library to sniff TCP packets.
Information	<https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations>

Last change to this tool card: 26 August 2024

Download this tool card in JSON format

All groups using tool LOOKOVER

Changed	Name	Country	Observed	
APT groups				
	UNC3886		2021-Early 2025	

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