Threat Group Cards: A Threat Actor Encyclopedia

Tool: Lowkey

Names	Lowkey PortReuse
Category	Malware
Type	Backdoor, Rootkit
Description	(FireEye) LOWKEY is a passive backdoor that utilizes a user mode rootkit to provide covert communications with the backdoor component by forwarding packets in between a TCP Socket and a named pipe.
Information	<https://paper.bobylive.com/Security/APT_Report/APT-41.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.lowkey>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:LOWKEY>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Lowkey

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	

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