Threat Group Cards: A Threat Actor Encyclopedia

Tool: MoonPeak

Names	MoonPeak
Category	Malware
Type	Backdoor
Description	(Talos) This a XenoRAT-based malware, which is under active development by a North Korean nexus cluster we are calling “UAT-5394.” Our analysis of infrastructure used in the campaign reveals additional links to the UAT-5394 infrastructure and new tactics, techniques and procedures (TTPs) of the threat actor.
Information	<https://blog.talosintelligence.com/moonpeak-malware-infrastructure-north-korea/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.moonpeak>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool MoonPeak

Changed	Name	Country	Observed	
APT groups				
	Kimsuky, Velvet Chollima		2012-Aug 2025	

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