Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:53:00 UTC

Tool: RedAlpha

Names	RedAlpha
Category	Malware
Type	Reconnaissance, Backdoor
Description	(Recorded Future) The RedAlpha campaigns began in mid-2017 by targeting the Tibetan community in India. The latest campaign remains ongoing, with new subdomains registered in late April 2018. The threat actor utilized a careful combination of victim reconnaissance and fingerprinting, followed by selective targeting with multi-stage malware. The malware utilized changed from a reliable custom toolset in the 2017 campaign to a more cautious and spartan approach, ending with commodity malware in 2018. Observing these two campaigns in succession demonstrates the evolution of a relatively unknown threat actor.
Information	<https://www.recordedfuture.com/redalpha-cyber-campaigns/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.redalpha>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:RedAlpha>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool RedAlpha

Changed	Name	Country	Observed	
APT groups				
	RedAlpha		2015-2021	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=98c9d065-cb9a-42fd-8a76-1a28764a24d3