Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:06:24 UTC

Tool: TERA

Names	TERA
Category	Malware
Type	Backdoor
Description	(FireEye) TERA is a backdoor that uses legitimate services, such as Google Translate and Yahoo! Babel Fish, as proxies to download C&C configurations. It also uses a rootkit to mask network activity. After resolving the IP address of its C&C server, TERA will provide an input output control (IOCTL) code to its driver (rootkit component).
Information	<https://paper.bobylive.com/Security/APT_Report/APT-41.pdf>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool TERA

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

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