Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 01:07:28 UTC

Tool: TrailBlazer

Names	TrailBlazer
Category	Malware
Type	Backdoor
Description	(CrowdStrike) TrailBlazer is a sophisticated malware family that provides modular functionality and a very low prevalence. The malware shares high-level functionality with other malware families. In particular, the use of random identifier strings for C2 operations and result codes, and attempts to hide C2 communications in seemingly legitimate web traffic, were previously observed tactics, techniques and procedures (TTPs) in GoldMax and SUNBURST.
Information	<https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0682/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool TrailBlazer

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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