Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:34:48 UTC

Tool: AIRBREAK

Names	AIRBREAK Orz
Category	Malware
Type	Backdoor, Reconnaissance, Info stealer, Exfiltration
Description	(Recorded Future) AIRBREAK, also known as Orz, is a JavaScript-based backdoor that retrieves commands from hidden strings in compromised webpages and actor-controlled profiles on legitimate services.
Information	<https://go.recordedfuture.com/hubfs/reports/cta-2018-1113.pdf> <https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html> <https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets>
MITRE ATT&CK	<https://attack.mitre.org/software/S0229/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/js.airbreak>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:AIRBREAK>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool AIRBREAK

Changed	Name	Country	Observed	
APT groups				
	Leviathan, APT 40, TEMP.Periscope		2013-Jul 2021	

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