Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:07:12 UTC

Tool: RustBucket

Names	RustBucket
Category	Malware
Type	Backdoor
Description	(Sekoia) Since at least December 2022, Bluenoroff was observed leveraging RustBucket, a Rust and Objective-C written malware targeting macOS running systems. This recent Bluenoroff activity illustrates how intrusion sets turn to cross-platform language in their malware development efforts, further expanding their capabilities highly likely to broaden their victimology. While other DPRK-nexus intrusion sets, including Lazarus, Kimsuky and more recently Reaper were already reported targeting macOS, it is the first time Bluenoroff was observed targeting macOS users, to the best of our knowledge.
Information	<https://blog.sekoia.io/bluenoroffs-rustbucket-campaign/> <https://www.jamf.com/blog/bluenoroff-apt-targets-macos-rustbucket-malware/> <https://www.elastic.co/security-labs/DPRK-strikes-using-a-new-variant-of-rustbucket> <https://securelist.com/bluenoroff-new-macos-malware/111290/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/osx.rustbucket>

Last change to this tool card: 16 January 2024

Download this tool card in JSON format

All groups using tool RustBucket

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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