Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:25:34 UTC

Tool: JSPRAT

Names	JSPRAT
Category	Malware
Type	Backdoor
Description	(Mandiant) The usage of JSPRAT by FIN13 allows the actor to achieve local command execution, upload/download files, and proxy network traffic for additional pivoting during later stages of the intrusion. FIN13 has also historically used publicly available web shells coded in various languages including PHP, C# (ASP.NET), and Java.
Information	<https://www.mandiant.com/resources/fin13-cybercriminal-mexico> <https://www.secureworks.com/research/analysis-of-dhs-nccic-indicators>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/js.jsprat>

Last change to this tool card: 28 December 2021

Download this tool card in JSON format

All groups using tool JSPRAT

Changed	Name	Country	Observed	
APT groups				
	FIN13	[Unknown]	2016	

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