Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:59:57 UTC

Tool: BUSTEDPIPE

Names	BUSTEDPIPE
Category	Malware
Type	Remote command
Description	(Mandiant) In the same investigation where FIN13 has used wmiexec.vbs, Mandiant has also observed the actor use a custom JSP web shell tunneler named BUSTEDPIPE to facilitate lateral movement via web requests.
Information	<https://www.mandiant.com/resources/fin13-cybercriminal-mexico>

Last change to this tool card: 26 December 2021

Download this tool card in JSON format

All groups using tool BUSTEDPIPE

Changed	Name	Country	Observed	
APT groups				
	FIN13	[Unknown]	2016	

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