Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:36:19 UTC

Tool: BitterRAT

Names	BitterRAT Bitter RAT
Category	Malware
Type	Backdoor
Description	(Forcepoint) BITTER used free dynamic DNS (DDNS) and dedicated server hosting services in order to set up their C2s. The download site where the exploit documents download the RAT binaries are, in most cases, different from the actual RAT C2. However, both of them are typically registered using a Gmail email address and a spoofed identity purporting to be either from United Kingdom or Great Britain.
Information	<https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan> <https://ti.360.net/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bitter_rat>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool BitterRAT

Changed	Name	Country	Observed	
APT groups				
	Bitter	[South Asia]	2013-Nov 2024	

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