Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:59:58 UTC

Tool: BreachRAT

Names	BreachRAT
Category	Malware
Type	Backdoor
Description	(FireEye) The payload is a backdoor that we call the Breach Remote Administration Tool (BreachRAT) written in C++. We had not previously observed this payload used by these threat actors. The malware name is derived from the hardcoded PDB path found in the RAT: C:\Work\Breach Remote Administration Tool\Release\Client.pdb. This RAT communicates with 5.189.145.248, a command and control (C2) IP address that this group has used previously with other malware, including DarkComet and njRAT.
Information	<https://www.fireeye.com/blog/threat-research/2016/06/apt_group_sends_spea.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.breach_rat>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool BreachRAT

Changed	Name	Country	Observed	
APT groups				
	Transparent Tribe, APT 36		2013-Mar 2025	

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