Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:25:47 UTC

Tool: SierraCharlie

Names	SierraCharlie
Category	Malware
Type	Loader, Worm
Description	(Novetta) SierraCharlie is a spreader that appears to target RDP as its vector for propagation. Novetta has not spent a significant amount of time investigating the SierraCharlie family before publication, but the following characteristics of the malware family are known: 1. The random IP generation code found in both SierraJuliett-MikeOne and SierraBravo can be found within SierraCharlie 2. SierraCharlie, structurally speaking, is heavily object oriented (C++) 3. The suicide script within SierraCharlie is consistent with other Lazarus Group malware families 4. The propagation mechanism appears to focus on RDP 5. At least one sample identifies the malware's program name as "RDPBForce" 6. At least two samples have two distinct version information entries with in the resource section with one entry in English and the other in Korean.
Information	<https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-RAT-and-Staging-Report.pdf>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool SierraCharlie

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

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