Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:24:35 UTC

Tool: BLUEHAZE

Names	BLUEHAZE
Category	Malware
Type	Loader
Description	(Mandiant) BLUEHAZE is a launcher written in C/C++ that launches a copy of NCAT to create a reverse shell to a hardcoded command and control (C2).
Information	<https://www.mandiant.com/resources/blog/china-nexus-espionage-southeast-asia>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bluehaze>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool BLUEHAZE

Changed	Name	Country	Observed	
APT groups				
	UNC4191		2022	

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