Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:57:26 UTC

Tool: CEELOADER

Names	CEELOADER
Category	Malware
Type	Loader
Description	(Mandiant) The threat actor used native Windows tools to perform initial reconnaissance, credential theft and deploy Cobalt Strike BEACON to devices via PowerShell. The actor then used this BEACON implant to persistently install CEELOADER as a Scheduled Task that ran on login as SYSTEM on specific systems. CEELOADER is [a] downloader that decrypts a shellcode payload to execute in memory on the victim device.
Information	<https://www.mandiant.com/resources/russian-targeting-gov-business>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ceeloader>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool CEELOADER

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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