Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:16:59 UTC

Tool: RAINDROP

Names	RAINDROP
Category	Malware
Type	Backdoor, Dropper, Loader, Remote command
Description	(Symantec) Raindrop (Backdoor.Raindrop) is a loader which delivers a payload of Cobalt Strike. Raindrop is very similar to the already documented TEARDROP tool, but there are some key differences between the two. While Teardrop was delivered by the initial SUNBURST backdoor (Backdoor.Sunburst), Raindrop appears to have been used for spreading across the victim's network. Symantec has seen no evidence to date of Raindrop being delivered directly by Sunburst. Instead, it appears elsewhere on networks where at least one computer has already been compromised by Sunburst.
Information	<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware>
MITRE ATT&CK	<https://attack.mitre.org/software/S0565/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.raindrop>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool RAINDROP

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

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=122be2b4-0bc3-41f3-8154-b21db01f7a01