Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:48:25 UTC

Tool: P8RAT

Names	P8RAT GreetCake
Category	Malware
Type	Backdoor, Loader
Description	(Kaspersky) One of Ecipekac's payloads is a new fileless malware which we call P8RAT (a.k.a GreetCake). P8RAT has the following unique data structure used to store the C2 communication configuration. We collected several samples of P8RAT during our research and found no C2 address of P8RAT that was used more than once. In total we found 10 backdoor commands in all the collected P8RAT samples. The most recent P8RAT sample, with the compilation timestamp of December 14, 2020, shows a new backdoor command with the code number of "309" implemented. The command "304", which was present in earlier samples and carries similar functionality, was removed.
Information	<https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0626/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool P8RAT

Changed	Name	Country	Observed	
APT groups				
	Stone Panda, APT 10, menuPass		2006-Mar 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b5cb59ac-bfd5-400f-91ba-57472c375fd3