Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:01:01 UTC

Tool: RARSTONE

Names	RARSTONE
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Trend Micro) The new sample detected by Trend Micro as BKDR_RARSTONE.A is similar (but not) PlugX, as it directly loads a backdoor “file” in memory without dropping any “file”. However, as we proceeded with our analysis, we found that BKDR_RARSTONE has some tricks of its own.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/bkdr_rarstone-new-rat-to-watch-out-for/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0055/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:rarstone>

Last change to this tool card: 13 June 2020

Download this tool card in JSON format

All groups using tool RARSTONE

Changed	Name	Country	Observed	
APT groups				
	Naikon, Lotus Panda		2010-Apr 2022	

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