Deed RAT - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:45:44 UTC

Tool: Deed RAT

Names	Deed RAT SnappyBee
Category	Malware
Type	Reconnaissance, Backdoor, Loader
Description	(BleepingComputer) Deed RAT's functions depend on which plugins are fetched and loaded. For example, PT has seen eight plugins for startup, C2 config, installation, code injection into processes, network interactions, connection management, registry editing, registry monitoring, and proxy sniffing. The supported protocols for C2 communication include TCP, TLS, HTTP, HTTPS, UDP, and DNS, so there's generally a high level of versatility. The commands supported by Deed RAT are the following: • Collect system information • Create a separate communication channel for a plugin • Self-remove • Ping • Deactivate connection • Update the shellcode for an injection stored in the registry • Update the main shellcode on disk and delete all plugins
Information	<https://www.bleepingcomputer.com/news/security/chinese-space-pirates-are-hacking-russian-aerospace-firms/> <https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/space-pirates-tools-and-connections/>

Last change to this tool card: 26 December 2024

Download this tool card in JSON format

All groups using tool Deed RAT

Changed	Name	Country	Observed	
APT groups				
	Salt Typhoon, GhostEmperor		2020-Feb 2025	
	Space Pirates		2017-Nov 2024	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=53fff35a-7a4a-466a-8baa-02ffb46929ec