

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:30:59 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool FunnyDream


↪ Tool: FunnyDream

Names	FunnyDream
Category	Malware
Type	Backdoor , Dropper , Loader , Exfiltration
Description	(Bitdefender) The attackers used the backdoor prevalently as DLL files, but we observed an executable to be used as well. The files we found implement many persistence mechanisms, their droppers and loaders use many different file names for the payload, all of that suggesting that the backdoor is custom made.
Information	<p><https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf></p> <p><https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf></p> <p><https://nao-sec.org/2021/01/royal-road-rediscover.html></p> <p><https://insight-jp.nttsecurity.com/post/102glv5/pandas-new-arsenal-part-3-smanager></p>
MITRE ATT&CK	< https://attack.mitre.org/software/S1044/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.funny_dream >

Last change to this tool card: 30 December 2022

Download this tool card in [JSON](#) format

All groups using tool FunnyDream

Changed	Name	Country	Observed
APT groups			
	FunnyDream		2018

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

Source: <https://apt.eta-da.or.th/cgi-bin/listgroups.cgi?u=332c984a-acae-4a4f-98af-8e6f808942c7>