Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:26:19 UTC

APT group: FunnyDream

Names	FunnyDream *(Kaspersky)* Red Hariasa *(PWC)* Bronze Edgewood *(SecureWorks)* TAG-16 *(Recorded Future)*
Country	China
Motivation	Information theft and espionage
First seen	2018
Description	In early 2020 Kaspersky published a report based on its investigation of an ongoing attack campaign called “FunnyDream”. This Chinese-speaking actor has been active for at least a few years and possesses different implants with various capabilities. Since mid-2018, researchers at Kaspersky saw continuing high activity from this threat actor and among their targets were a number of high-level government organisations as well as some political parties from various Asian countries including the Philippines, Thailand, Vietnam, and Malaysia. The campaign comprises a number of cyber espionage tools with various capabilities. As of the latest monitoring of the global cybersecurity company, FunnyDream's espionage attacks are still ongoing.
Observed	Sectors: Government. Countries: Indonesia, Malaysia, Philippines, Taiwan, Thailand, Vietnam.
Tools used	ccf32, Chinoxy, Filepak, FilepakMonitor, FunnyDream, Keyrecord, Md_client, PCShare, ScreenCap, TcpBridge, Tcp_transfer, Living off the Land.
Information	<https://www.digitalnewsasia.com/business/kaspersky-2019-apt-report-cyberspying-groups-hunt-intelligence-sea> <https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf> <https://go.recordedfuture.com/hubfs/reports/cta-2021-1208.pdf>

Last change to this card: 27 December 2021

Download this actor card in PDF or JSON format
