Mysterious Elephant - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:26:59 UTC

APT group: Mysterious Elephant

Names	Mysterious Elephant *(Kaspersk)* APT-K-47 *(Knownsec 404)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2023
Description	(Knownsec 404) Recently, in the course of daily APT tracking,the Knownsec 404 Advanced Threat Intelligence team discovered an attack campaign by the APT-K-47 organization using the topic of “Hajj”, and the attackers used a CHM file to execute a malicious payload in the same directory. The final payload is relatively simple, supporting only the cmd shell, and is implemented using asynchronous programming, which is very similar to the “Asynshell” that was used by the organization several times during Our team’s tracking cycle from 2023 to the first half of 2024. Based on our tracking observations, the previously captured Asynshell has been updated in several versions, and based on the logic and functionality of the code, we have reason to suspect that this sample is an upgraded version of Asynshell.
Observed	Countries: Pakistan.
Tools used	ORPCBackdoor.
Information	<https://medium.com/@knownsec404team/unveiling-the-past-and-present-of-apt-k-47-weapon-asyncshell-5a98f75c2d68> <https://medium.com/@knownsec404team/apt-k-47-mysterious-elephant-a-new-apt-organization-in-south-asia-5c66f954477>

Last change to this card: 26 December 2024

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=7a5bd493-2c51-4878-bc60-7639d7e9da21