

# Awaken Likho - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:07:14 UTC

## APT group: Awaken Likho

Names	Awaken Likho ( <i>Kaspersky</i> ) Core Werewolf ( <i>BI.ZONE</i> )
Country	[Unknown]
Motivation	<a href="#">Information theft and espionage</a>
First seen	2021
Description	<p>(<a href="#">Kaspersky</a>) In July 2021, a campaign was launched primarily targeting Russian government agencies and industrial enterprises. Shortly after the campaign started, we began tracking it, and published three reports in August and September 2024 through our threat research subscription on the threat actor we named Awaken Likho (also named by other vendors as Core Werewolf).</p> <p>While investigating the activity of this APT group, we discovered a new campaign that began in June 2024 and continued at least until August. Analysis of the campaign revealed that the attackers had significantly changed the software they used in their attacks. The attackers now prefer using the agent for the legitimate MeshCentral platform instead of the UltraVNC module, which they had previously used to gain remote access to systems. The group remains focused on targeting Russian government organizations and enterprises.</p>
Observed	Sectors: <a href="#">Government</a> . Countries: <a href="#">Russia</a> .
Tools used	
Information	<p>&lt;<a href="https://securelist.com/awaken-likho-apt-new-implant-campaign/114101/">https://securelist.com/awaken-likho-apt-new-implant-campaign/114101/</a>&gt; &lt;<a href="https://bi.zone/eng/expertise/blog/core-werewolf-protiv-opk-i-kriticheskoy-infrastruktury/">https://bi.zone/eng/expertise/blog/core-werewolf-protiv-opk-i-kriticheskoy-infrastruktury/</a>&gt; &lt;<a href="https://bi.zone/eng/expertise/blog/ne-budi-likho-core-werewolf-sovershenstvuet-ataki-na-rossijskie-gosorganizatsii/">https://bi.zone/eng/expertise/blog/ne-budi-likho-core-werewolf-sovershenstvuet-ataki-na-rossijskie-gosorganizatsii/</a>&gt;</p>

Last change to this card: 24 October 2024

Download this actor card in [PDF](#) or [JSON](#) format

---

Source: <https://apt.eta.or.th/cgi-bin/showcard.cgi?u=f3c3beeb-ae74-411b-8a9a-110533a0b28d>