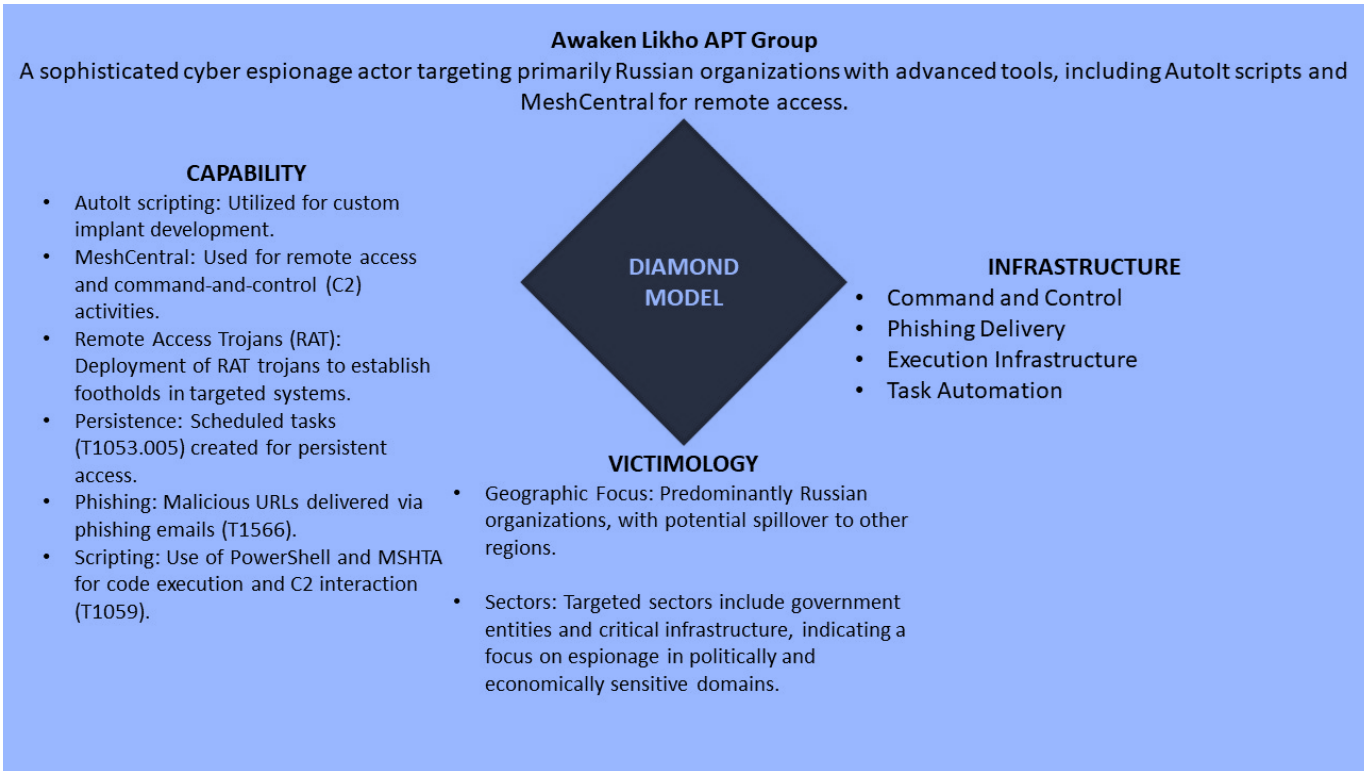
Awaken Likho

The Awaken Likho APT group has been identified as a sophisticated threat actor using advanced tools and techniques to conduct cyber espionage operations. Kaspersky researchers recently analyzed new implants used by the group, which rely heavily on the AutoIt scripting language and the MeshCentral platform. These implants were discovered targeting Russian organizations, but the group's operations may extend beyond this region.



Awaken Likho APT Group

A sophisticated cyber espionage actor targeting primarily Russian organizations with advanced tools, including AutoIt scripts and MeshCentral for remote access.

DIAMOND MODEL

CAPABILITY

- AutoIt scripting: Utilized for custom implant development.
- MeshCentral: Used for remote access and command-and-control (C2) activities.
- Remote Access Trojans (RAT): Deployment of RAT trojans to establish footholds in targeted systems.
- Persistence: Scheduled tasks (T1053.005) created for persistent access.
- Phishing: Malicious URLs delivered via phishing emails (T1566).
- Scripting: Use of PowerShell and MSHTA for code execution and C2 interaction (T1059).

INFRASTRUCTURE

- Command and Control
- Phishing Delivery
- Execution Infrastructure
- Task Automation

VICTIMOLOGY

- Geographic Focus: Predominantly Russian organizations, with potential spillover to other regions.
- Sectors: Targeted sectors include government entities and critical infrastructure, indicating a focus on espionage in politically and economically sensitive domains.

Blue Team Focus

- DFIR: Focus on incident response related to scheduled task creation, PowerShell execution, and RAT implants. Investigate connections to known IOCs, such as hashes and the C2 domain/IP.
- SecOps: Implement detections for malicious PowerShell, MeshCentral activity, and UltraVNC usage via SIEM rules. Monitor network traffic for suspicious HTTP/HTTPS communications tied to the identified domain/IP.
- Purple Team: Use the model to simulate phishing and remote access techniques leveraging MeshCentral, as well as credential harvesting efforts observed in this campaign.

Attacks Vectors

- Delivery (Phishing Email) ➔ Malicious URL Link (MSHTA, PowerShell, Drive-by Download) ➔ Download of Self-Extracting Archive (.exe) ➔ Execution of Self-Extracting Archive (.exe) ➔ Dropper Execution (.exe) ➔ MeshAgent Execution (.exe) ➔ Network Communication to C2 Server

Indicators of Compromise (IOCs) – source: Kaspersky

Hashes

- 603eead3a4dd56a796ea26b1e507a1a3
- deae4a955e1c38aae41bec5e5098f96f
- 892c55202ce3beb1c82183c1ad81c7a0
- 63302bc6c9aebe8f0cdafdd2ecc2198a
- 912ebcf7da25c56e0a2bd0dfb0c9adff
- c495321edebe32ce6731f7382e474a0e

Domain

- kwazindernuren.com

IP address

- 38.180.101.12

Malicious Task Name

- MicrosoftEdgeUpdateTaskMachineMS