Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Awaken Likho Adopts New Tactics to Spy on Russian Government

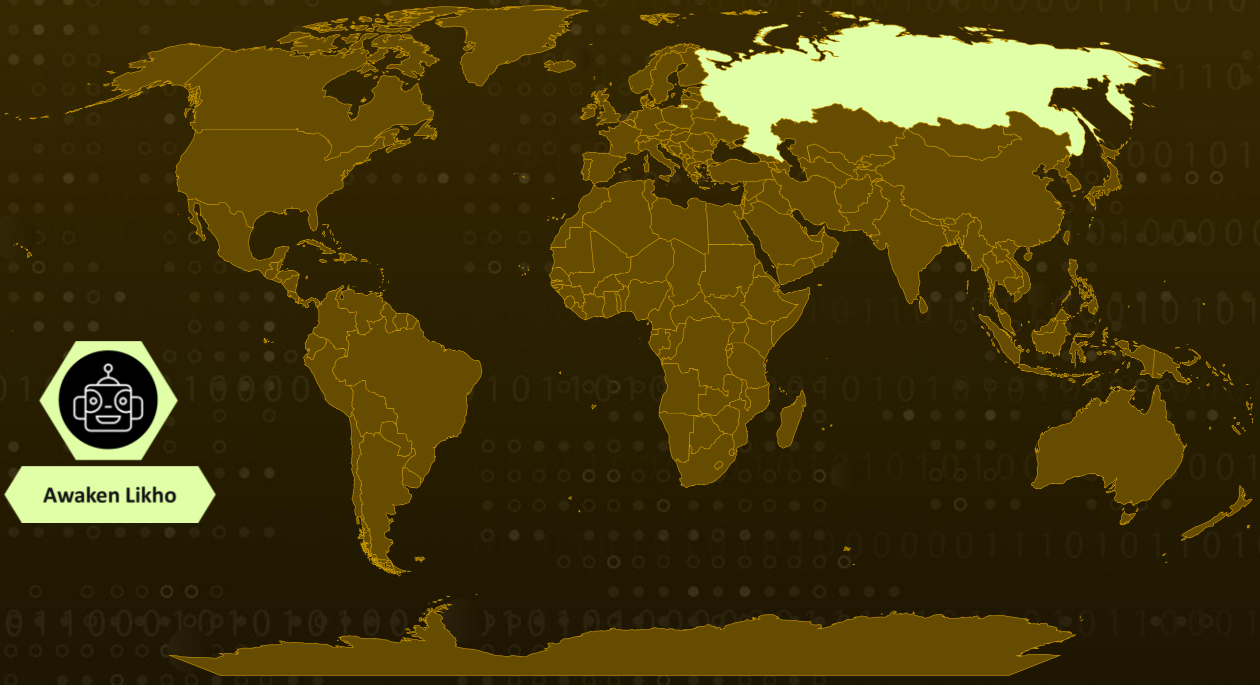
Date of Publication	Admiralty Code	TA Number
October 11, 2024	A1	TA2024389

Summary

Attack Commenced: June 2024
Threat Actor: Awaken Likho (aka Core Werewolf, PseudoGamaredon)
Targeted Country: Russia
Targeted Industries: Enterprises, Government

Attack: Awaken Likho, an advanced cyber espionage group active since 2021, saw increased activity after the Russo-Ukrainian conflict. Previously using UltraVNC for remote access, they shifted to MeshAgent in June 2024, enhancing their attack capabilities. Targeting government and industrial networks by exploiting legitimate tools like MeshAgent, Awaken Likho presents a growing threat, highlighting the need for vigilance against evolving cyber risks.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 Awaken Likho, also known as Core Werewolf or PseudoGamaredon, has been active since at least 2021. Their activity, however, surged following the onset of the Russo-Ukrainian conflict. For years, the group relied on the UltraVNC module for remote system access.

#2 In a new campaign that began in June 2024 and continued through August 2024, the attackers switched to MeshAgent, a component of the MeshCentral platform. This campaign focused on cyberespionage and device control, specifically targeting government and industrial organizations in Russia and their contractors.

#3 Awaken Likho operators typically gather intelligence on their victims using search engines. The attack chain begins with phishing emails containing 7-Zip self-extracting archives (SFX) that masquerade as Microsoft Word or PDF documents through the use of double extensions.

#4 These archives covertly deploy an AutoIt script to install the MeshAgent tool. The archives contain five files, four of which are disguised as legitimate system services and command files. MeshCentral, a legitimate open-source remote management tool, was exploited by the attackers for remote desktop access, device control, file transfers, and real-time monitoring. This tactic mirrors the approach of other adversaries like Lace Tempest and LilacSquid, who have also adopted the use of MeshAgent for similar purposes.

Recommendations

Enhanced Task Scheduler Monitoring: Set up automated monitoring and alerting systems to flag any suspicious tasks named "MicrosoftEdgeUpdateTaskMachineMS" or similar variants. Since Awaken Likho disguises malicious activities under trusted names, detecting anomalies in task creation or execution can reveal ongoing attacks.

Implement a Zero Trust Architecture: Adopt a Zero Trust security model that operates on the principle of "never trust, always verify." This approach requires strict identity verification for every person and device trying to access resources on your network, regardless of whether they are inside or outside the network perimeter.

Deploy Advanced Email Filtering: Use advanced email filtering solutions to detect and block phishing attempts before they reach users. Implement sandboxing techniques to analyze attachments and links in emails for malicious content.

Heighten Awareness: Familiarize yourself with common social engineering tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	T1593 Search Open Websites/Domains
T1593.002 Search Engines	T1566 Phishing	T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1059.003 Windows Command Shell	T1053 Scheduled Task/Job	T1053.005 Scheduled Task
T1204 User Execution	T1204.002 Malicious File	T1543 Create or Modify System Process	T1055 Process Injection
T1036 Masquerading	T1036.005 Match Legitimate Name or Location	T1036.007 Double File Extension	T1083 File and Directory Discovery

T1057 Process Discovery	**T1005** Data from Local System	**T1070** Indicator Removal	**T1027** Obfuscated Files or Information
T1027.002 Software Packing	**T1133** External Remote Services	**T1564.003** Hidden Window	**T1059.010** AutoHotKey & AutoIT

Indicators of Compromise (IOCs)

TYPE	VALUE
File Name	MicrosoftStores.exe, NetworkDrivers.exe, nKka9a82kjn8KJHA9.cmd, EdgeBrowser.cmd
Domain	kwazindernuren[.]com
IPv4	38[.]180[.]101[.]12
MD5	603eead3a4dd56a796ea26b1e507a1a3, deae4a955e1c38aae41bec5e5098f96f, 892c55202ce3beb1c82183c1ad81c7a0, 63302bc6c9aebe8f0cdafdd2ecc2198a, 912ebcf7da25c56e0a2bd0dfb0c9adff, c495321edebe32ce6731f7382e474a0e
SHA1	56d6ef744adbc484b15697b320fd69c5c0264f89, a45d8d99b6bc53fa392a9dc374c4153a62a11e2a, 976b5bc7aafc32450f0b59126f50855074805f28, f4e2c56e1e5e73aa356a68da0ae986103c9a7bad, a76601fc29c523a3039ed9e7a1fc679b963db617, bcd91cad490d0555853f289f084033062fa1ffaa
SHA256	7491991dd42dabb123b46e33850a89bed0a2790f892d16a592e787d3fee8c0d5, f11423a3c0f3f30d718b45f2dcab394cb8bdcd473c47a56544e706b9780f1495, f3421e5392e3fce07476b3c34153a7db0f6c8f873bd8887373f7821bd0281dcc, 37895c19d608aba8223e7aa289267faea735c8ee13676780a1a0247ad371b9b8, c31faf696c44e6b1aeab4624e5330dc748633e2d8a25d624fc66fed384797f69, 82415a52885b2731214ebd5b33ceef379208478baeb2a09bc985c9ce8c62e003

References

https://securelist.com/awaken-likho-apt-new-implant-campaign/114101/

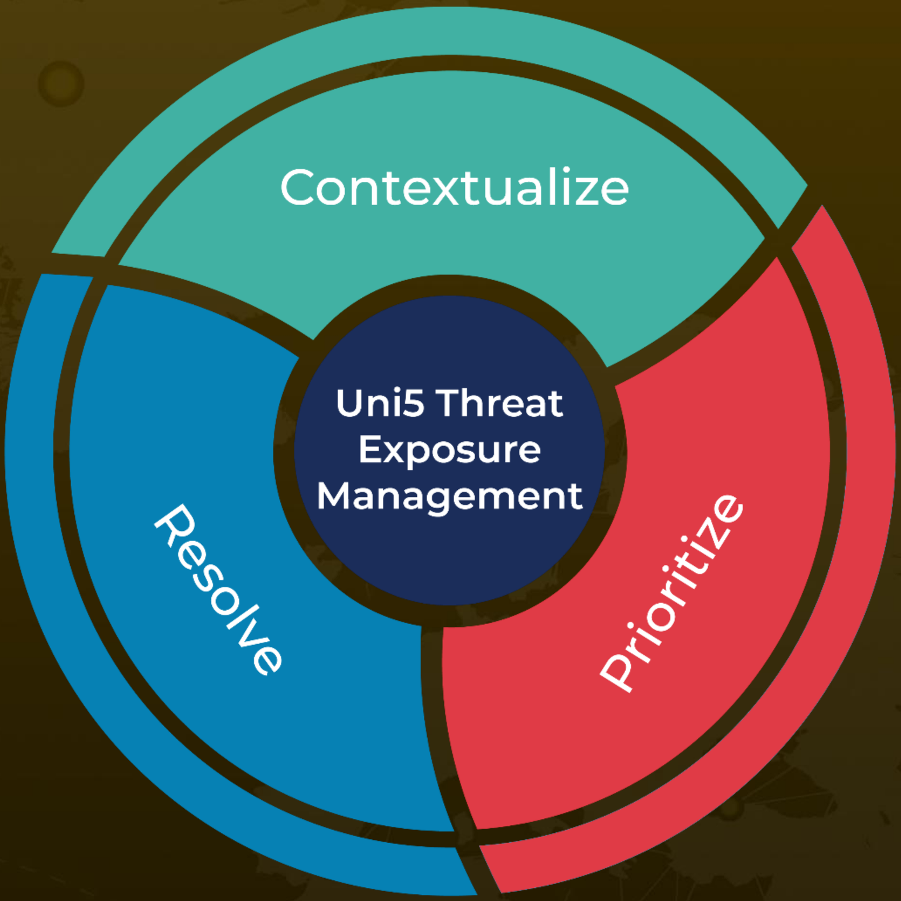
https://hivepro.com/threat-advisory/lace-tempest-exploits-zero-day-in-a-strategic-strike-on-sysaid/

https://hivepro.com/threat-advisory/deciphering-lilacsquids-strategies-for-long-term-data-theft/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 11, 2024 • 6:00 AM

More at www.hivepro.com