KPMG Cyber Threat Intelligence Platform

UAT-8302 - China-Nexus Advanced Persistent Threat Cluster

TLP : Clear

KPMG. Make the Difference.

UAT-8302 is a China-aligned advanced persistent threat group identified in late 2024, with strong tactical and tooling overlap with known Chinese state-sponsored clusters. Its operations aim to achieve long-term espionage access and collect sensitive organizational and geopolitical intelligence. UAT-8302 primarily targets government and state-affiliated entities, with activity observed across agencies in South America and Southeastern Europe.

Initial access is likely achieved by exploiting internet-facing vulnerabilities, including zero-day and n-day flaws. Post-compromise, network and Active Directory (AD) reconnaissance is performed using Impacket, WMI, PowerShell, native Windows tools, and AD utilities (e.g., SharpGetUserLoginIPRP and AD Explorer) to enumerate hosts, users, SMB shares, domain objects, login activity, and services. Credential harvesting targets AD and Entra ID environments, including login data, event logs, and stored credentials, enabling privilege escalation and lateral movement. Propagation occurs via SMB-/WMI-based execution, stolen credentials, and scripted deployments, with tool usage varying by environment and campaign. UAT-8302 deploys various combinations of China-nexus-associated malware and loaders, such as NetDraft, VSHELL, SNOWLIGHT, Draculoader, CloudSorcerer, and other RAT frameworks, delivered via multi-stage DLL sideloading, reflecting adaptable, ecosystem-wide tool reuse. Observed malware capabilities include command execution, in-memory execution, persistence via scheduled tasks or injected processes, and credential theft. For command and control, the group uses both dedicated infrastructure and legitimate services (Microsoft Graph API, OneDrive, GitHub), alongside proxy/tunneling tools like Stowaway and SoftEther VPN to maintain persistence and enable covert data exfiltration.

UAT-8302's multi-stage attack chain and reliance on legitimate cloud services highlight the need for timely patching, continuous endpoint monitoring, and strong identity access controls.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Patch your Windows environment with the latest version asper the OEM and secure it with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context.

The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

Atul Gupta
Partner
Head of Cyber Security
T: +91 98100 81050
E: atulgupta@kpmg.com

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

UAT-8302 - China-Nexus Advanced Persistent Threat Cluster

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses

85.209.156[.]3	185.238.189[.]41
38.54.32[.]244	156.238.224[.]82
103.27.108[.]55	45.135.135[.]100
45.140.168[.]62	88.151.195[.]133

Indicators of Compromise: Domains

msiidentity[.]com	trafficmanagerupdate[.]com
drivelivelime[.]com	update-kaspersky[.]workers[.]dev

Indicators of Compromise: Hashes

efc71bd23572eec985a6d1bbf61308fd
b0467b78bf67cf703b1ce2ad38d3664c
fc9c1ba5f1a804b93558b7213adc24bd
99911fce9e0d697c99421b81e8fe2a04
cf1a8c083143995dc6fffaeb5d21edc8
3d00e34594dbaba266f301ca37246e06
111e8abb4b8592172d597926f47f018c
97f04361758d4242428f9e6801a02583
4c71357de3c0b12094693ca6eff94cad
23b7908c6bde98456e653c1d0b2e6962
f694401d8e80bb0f672b1b30fd7b153a
76f4a223ba57db108fd7ede89bd61301
efc71bd23572eec985a6d1bbf61308fd
99911fce9e0d697c99421b81e8fe2a04
3d00e34594dbaba266f301ca37246e06

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

UAT-8302 - China-Nexus Advanced Persistent Threat Cluster

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
111e8abb4b8592172d597926f47f018c
4c71357de3c0b12094693ca6eff94cad
f694401d8e80bb0f672b1b30fd7b153a
efc71bd23572eec985a6d1bbf61308fd
99911fce9e0d697c99421b81e8fe2a04
3d00e34594dbaba266f301ca37246e06
111e8abb4b8592172d597926f47f018c
4c71357de3c0b12094693ca6eff94cad
f694401d8e80bb0f672b1b30fd7b153a
7b6e094d98eb3f695e5856db4d8d22e11898cec9
45550a47bca6dac8347d3c770d52eb780d614908
6bf0b85ac5bd117595cb38697e3e8da9e8f1eef2
f1551d3e5d144eef4e70a29dd3dc52fb22459d1f
5a82cdd226eea96615d3364ba9260a65f7e5e67a
a1c3520282c81afabdefa4834b96563edf95c3c7
738d4398e7d11427051093ba8a6f37e51470795c
75c88fd77024dce3931911d6630fccf93460ea9f
c46bac27b5ca151afabd22c5546f78ae2ae3a20d
0481e87d4d0cb3ba9d5c53c726c9c37bd802114c
3ddd90b99ee7ac3ec39e1d22b67c257d273a0970
495aafc32f8f3eddd3da6a48ef5694330473a79e
7b6e094d98eb3f695e5856db4d8d22e11898cec9
f1551d3e5d144eef4e70a29dd3dc52fb22459d1f
a1c3520282c81afabdefa4834b96563edf95c3c7
738d4398e7d11427051093ba8a6f37e51470795c

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

UAT-8302 - China-Nexus Advanced Persistent Threat Cluster

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
c46bac27b5ca151afabd22c5546f78ae2ae3a20d
3ddd90b99ee7ac3ec39e1d22b67c257d273a0970
7b6e094d98eb3f695e5856db4d8d22e11898cec9
f1551d3e5d144eef4e70a29dd3dc52fb22459d1f
a1c3520282c81afabdefa4834b96563edf95c3c7
738d4398e7d11427051093ba8a6f37e51470795c
c46bac27b5ca151afabd22c5546f78ae2ae3a20d
3ddd90b99ee7ac3ec39e1d22b67c257d273a0970
3dec6703b2cbc6157eb67e80061d27f9190c8301c9dd60eb0be1e8b096482d7e
199bd156c81b2ef4fb259467a20eacaa9d861eeb2002f1570727c2f9ff1d5dab
2b627f6afe1364a7d0d832ccba87ef33a8a39f30a70a5f395e2a3cb0e2161cb3
45cd169bf9cd7298d972425ad0d4e98512f29de4560a155101ab7427e4f4123f
f859a67ceebc52f0770a222b85a5002195089ee442eac4bea761c29be994e2ea
343105919aa6df8a75ecb8b06b74f23a7d3e221fca56c67b728c50ea141314bc
7d9c70fc36143eb33583c30430dcb40cf9d306067594cc30ffd113063acd6292
1bb59491f7289b94ab0130d7065d74d2459a802a7550ebf8cd0828f0a09c4d38
843f8aea7842126e906cadbad8d81fa456c184fb5372c6946978a4fe115edb1c
35b2a5260b21ddb145486771ec2b1e4dc1f5b7f2275309e139e4abc1da0c614b
7c593ca40725765a0747cc3100b43a29b88ad1708ef77e915ab02686c0153001
e74098b17d5d95e0014cf9c7f41f2a4e4be8baefc2b0eb42d39ae05a95b08ea5
3dec6703b2cbc6157eb67e80061d27f9190c8301c9dd60eb0be1e8b096482d7e
45cd169bf9cd7298d972425ad0d4e98512f29de4560a155101ab7427e4f4123f
343105919aa6df8a75ecb8b06b74f23a7d3e221fca56c67b728c50ea141314bc
7d9c70fc36143eb33583c30430dcb40cf9d306067594cc30ffd113063acd6292
843f8aea7842126e906cadbad8d81fa456c184fb5372c6946978a4fe115edb1c

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

UAT-8302 - China-Nexus Advanced Persistent Threat Cluster

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
7c593ca40725765a0747cc3100b43a29b88ad1708ef77e915ab02686c0153001
3dec6703b2cbc6157eb67e80061d27f9190c8301c9dd60eb0be1e8b096482d7e
45cd169bf9cd7298d972425ad0d4e98512f29de4560a155101ab7427e4f4123f
343105919aa6df8a75ecb8b06b74f23a7d3e221fca56c67b728c50ea141314bc
7d9c70fc36143eb33583c30430dcb40cf9d306067594cc30ffd113063acd6292
843f8aea7842126e906cadbad8d81fa456c184fb5372c6946978a4fe115edb1c
7c593ca40725765a0747cc3100b43a29b88ad1708ef77e915ab02686c0153001