KPMG Cyber Threat Intelligence Platform

Amaranth Dragon - Targeted Espionage via WinRAR Exploitation

TLP : Clear

KPMG. Make the Difference.

Amaranth Dragon is a China-nexus cyberespionage threat actor first identified in 2025 and is assessed to maintain substantive links to APT41. The group relies on custom tooling, including the Amaranth Loader, TGAmaranth RAT, and in-memory execution of the Havoc Framework. They primarily target government and law-enforcement entities across Southeast Asian countries including Thailand, Laos, Cambodia, Indonesia, Singapore, and the Philippines.

Initial access is assessed to have likely occurred via spear-phishing emails delivering weaponized ZIP archives containing .LNK and .BAT files, hosted on legitimate cloud platforms (e.g., Dropbox) or attacker-controlled infrastructure. Subsequently, RAR archives are used to deliver malicious files and exploit the Windows WinRAR vulnerability 'CVE-2025-8088', that enables arbitrary code execution upon victim interaction, allowing persistence and payload deployment. Once executed, the malicious archive typically deploys the Amaranth Loader, a 64-bit DLL, sideloaded through a legitimate signed executable. The loader retrieves an AES key from a hardcoded URL, decrypts an encrypted payload in memory, and executes the Havoc C2 Framework entirely in memory, for remote execution, system reconnaissance, and exfiltration capabilities. In some operations, the RAR archive delivers a password-protected TGAmaranth RAT instead of the loader. This RAT communicates with a hard-coded Telegram bot for C2 and supports commands for process listing, screenshots, shell execution, and file transfer. The C2 infrastructure is Cloudflare-protected and geo-fenced to accept traffic solely from target-country IP ranges. This configuration, combined with the staged AES keys and payload hosting, ensures precise targeting while minimizing operational exposure.

Amaranth Dragon's rapid vulnerability exploitation and controlled C2 ecosystem highlights the urgency to enforce rapid patching, monitor suspicious archives, and strengthen layered defenses.

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

Amaranth Dragon - Targeted Espionage via WinRAR Exploitation

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
92.223.76[.]20	92.38.170[.]6
92.223.124[.]45	93.123.17[.]151
92.223.120[.]10	

Indicators of Compromise: Domains	
todaynewsfetch[.]com	dns.annasoft.gcdn[.]co

Indicators of Compromise: Hashes
92167258a558bf4d4a570d475c8e9133
16e6deda398135c8fe41c9aeccf4c58e
5fd48646b12103d50637cfc886de7a06
17973ba65de5e5dd434535c996041d32
7023c5b541d7a8baea45a06ce95e1435
8cabacf23f59ea73929fd4cd6ae256ac
8f4b39160c88f1611761e7b44374ce8f
a3475c575496de5ad018074c092c5a18
c128c55977d85e80888dd9c0b39e538e
a1203d34eb4d146bf2c799b5ac628404
8e130c2604516ccd4bcba72cc6549649
54341c0ab41639779b304325409fa1dca1e11b09
259819d1ae6421c2871f2ba0d128089036a0b29b
9afadca9b2dad54004bd376dbee7e98c38dbdf50
B4dc300031edf5dd4968028146b0d608bdd975c5
c54a68d6bcc6d04ff08ad9619706e54923a20248

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Amaranth Dragon - Targeted Espionage via WinRAR Exploitation

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
92b8fa4d3e7f42036fc297a3b765e365e27cdce5
e34d7e8ba4bb949aa5c491b950ab30688d5dbadc
19abb00922f4fb3d4b28713bc866a033a11c1567
3a647d54f0866496d6d71c7b8e9f928759d535fd
44ac2785b0352113ed12b856ec4507fa0b897adf
53641ae0acb0fd986b30bdb1766086140abdc625
a80c9e1b3116f882d4f25e1934a2e890706ba44c
b0b95528f5df65140540e473a5ac477d7f4dff87
d70bad36a4060f93a3c5c9092bbf299c463a1451
d80edb2d04670d304713b148d6a721498f842376
1c1d53cb0f2a2d9b6d7ddb4ed55ed18880ae45e6
3823415ce9d1408a6595035e1cb634b2e261e005
40550c3696581a00b976adddbbef145f2531770e
5670d4688b2ec8b414a96aa795d81b78580ae20b
582d275c4f10c8632294cadcf56df13729612de2
78066f82804410625f6cd02a913464e163c5613e
85a31476dd35ff67439a2cbb4dea40e3223f8eaf
b93db4606ab2233a6d48b9658ab7ca432ba93985
c582718d37e9563f019e3ef78e736a0282203371
e739b3cffbb94357390a0f451d8f4171fdb9200b
ed0232814fe9adb9fe62e04c8982cebf5c5e79ab
ff4e717f9fa54cbaadadf145433df4f8292c56c1
00351add8e0bca838e8dac40875b8ad5195805bd
481d50d5ab7c0a41a7c4fabb01b5c50c8f4fabf2
718c5846d3b903e3e9e2df9281f5e25b371465f2

KPMG

KPMG Cyber Threat Intelligence Platform

Amaranth Dragon - Targeted Espionage via WinRAR Exploitation

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
cd949663598c49141a98b438cf408113602e5c19
4b27e1b2261e10f0ff47426a6603b9e8a0b0a98ad81df18a77b54c4c455d91f1
6526752857c307284d38654e1417b8aac5991a328226355e1b9221b34cd151d0
6a44c7bc52fef3e70f7e60e01d8808cb2fe6e6565b095628554979a89a36ed28
c4bd5154a8d11b0659d8251070a0adc14a7fb98f0a4fc5d54ca9d0ac940dc8d0
c9f7605fce64721206f19ccf4002db7edb1b747383f5a48608909755699bdd09
ce940f04eeb4c2b92056d2a966318058c5971cb12ffe523a3c6b32f530a2c5f0
d7711333c34a27aed5d38755f30d14591c147680e2b05eaa0484c958ddaae3b6
e8ef0265c48925be7bb16e8051021889ff7b98337e327fa260595b5db3336895
a2c128fc040ed2db7634134f0577b3267164b71f692fc9b37c08e48b168d89e6
6a44c7bc52fef3e70f7e60e01d8808cb2fe6e6565b095628554979a89a36ed28
7e0da1399ff99e41493db489159668db566b6b00cd367e770619b774ec515809
98d9745f52f9c8805d05a3f2c18bfedeb342e438085840d3611d063af9b80720
79cc492a51fd0be594317c79b0ac0e7967f03744888d7024381b535b19e15e0c
d7711333c34a27aed5d38755f30d14591c147680e2b05eaa0484c958ddaae3b6