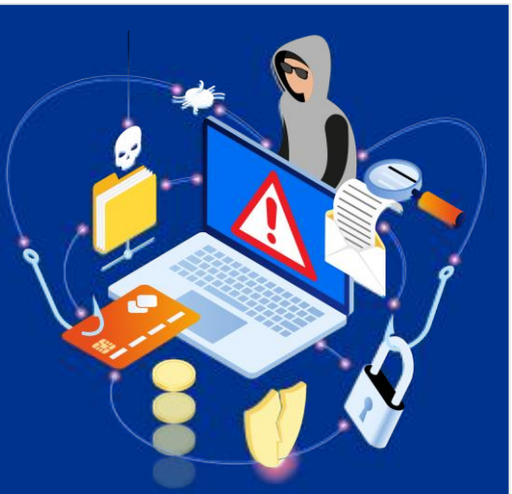
KPMG Cyber Threat Intelligence Platform



Noodle RAT - The Cross-Platform Menace

TLP : Clear

Noodle RAT (aka ANGRYREBEL & Nood RAT) is a complex cross-platform remote access trojan (RAT) used by Chinese-speaking threat actors for espionage and cybercrime. Identified in 2022, it has been active since at least 2016 but was misclassified as variants of Gh0st RAT or Rekoobe. It is notable for its ability to function on both Windows and Linux systems and was observed in various campaigns across countries such as - Thailand, India, Japan, Malaysia, and Taiwan.

Initial access is achieved by delivering loaders via social engineering, and by exploiting vulnerabilities for remote access. For Windows, the payload is deployed using MULTIDROP or MICROLOAD; MULTIDROP delivers the payload directly and MICROLOAD uses Oleview.exe for injection. For Linux, the payload is deployed as an exploit against public-facing applications, copied to /tmp/CCCCCCCC, and process names are modified. For persistence, Windows uses scheduled tasks or registry modifications, while Linux uses process name spoofing by overwriting argv and cron jobs. Communication with C2 for Windows is done by TCP, SSL, and HTTP with RC4 combined with XOR and AND encryption, while for Linux, it uses TCP and HTTP with RC4 and XOR and AND for command processing, and HMAC_SHA1 with AES128-CBC for reverse shell sessions. Commands are executed such as file management, in-memory module execution, and TCP proxying for Windows, and reverse shell, file management, scheduling, and SOCKS tunneling for Linux. Data is exfiltrated using a C2 server and payloads are downloaded for further functionality. Evasion is performed using self-deletion and anti-detection methods on Windows, and process name spoofing on Linux to hide and remove traces of the malware.

NoodleRat's modular design make it a formidable threat, but its impact can be curtailed by vigilant monitoring for unusual network behavior.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The 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

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

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

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

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

KPMG

KPMG Cyber Threat Intelligence Platform

Noodle RAT - The Cross-Platform Menace

TLP : Clear

Indicators of Compromise: IP Addresses	
42.51.40[.]184	1.117.165[.]141
101.42.139[.]110	

Indicators of Compromise: Hashes
cb131b05dc3e42fad5caeadccbee378b
ecac141c99e8cef83389203b862b24fd
67c8235ac0861c8622ac2ddb1f5c4a18
c1eebf2d4f441226770276110d1e5cf2
0a35e06f53c17ab1c8e18e7e0c0821d8
b42018c5fba4758ac46eb2c39344a020
f9eece34b6574236f067fa1a1782cdc0
7d631e5b0c78805dd5d440cce788d25b
35743db3dc333245ef5b69100721ced9
7038782f110e67d001b2cf466e13e391
8457f71c6a5fe83bb513d1dfba99271a
905c2158fadfe31850766f010e149a0f
256a871f1f968650291eef92428ee9de
f61a68097d5cf8cf74a9c97c33e5e626
e8007e15550a69ad8fd60d06c6d36385
5c2ccc619d798792761ef68a395aae70
b2082e3f5e6197d414a2462c5fb13baa
af93633c61e209de7f9029deac21ff5a
3477735428e24922b3301eefc1063039
fc85419f3b2afc89154700dd8cf37576
d312073a10e8d1fede43cfd18c6f3517
5b380c95f25b76ccd55eb791c6558abe
c440bd814be37fac669567131c4ba996
7d3ea628fce3146fccb722acc95544c4
fc931bb1973782c4be015ef6e169edea
a15ebd19cac42b0297858018da62b1be
4f3afdcfff8f7994b7d3d3fbaa6858b4
4961fcc2e3cc23c340aa0af9c4046131
6b1b7e89c6e566de97cadcf3323ae77f

KPMG

KPMG Cyber Threat Intelligence Platform

Noodle RAT - The Cross-Platform Menace

TLP : Clear

Indicators of Compromise: Hashes
4f5297c564c8f0064e7db65864198025
025a32835eb8647147ed1bbf64c37fa5
6728b74d5b30d2db8436f0c9f64684f1
8d9530b52744e681b1ca0de5580d065083cf9e44
b3a027f3bdb8ce87ea5eacc65e803d89b5f3dc35
6920cf39875fb1be1a01471c3041ece615ee4e4e
8965d8da52af8379704b09226252e185ae1b0f6f
2f4ee1c39f78ecde5a84233233d02b355022aa50
6aa0b6bfe059354782febd4fa665dbacd726b488
9249b61b2d23546097ad2d5042d3f2f21ccbd11a
14fd16e6465b74c5ac4dc895f4c15bccb447af31
f366f2730d481059a5153590ef3cab5d7658a3ef
54670aaf6212eeec04e2cb1bf9cff984393f29ec
1be33241473015788c11571ad3ab13ac82805da2
fa681933eccc1b3cae4cce6ab6f16db08c2f2a87
73c05da7efcc15de593bb4542bf8de6a9aab74a6
7316b5cc2aac0390890f6819d90b7cd36359ca62
4d4bc836641840ad8b0873b07d31ce38732c4a28
4b149222830a3df927a42b72d7f07e9198947f01
d30ef99a3da490b15b7fc098cec813f6acfb3ebe
bf191c7545dc2d69bbcde1fe857add49f599ea20
c4c612dcb2741246214946e2acda3cafcfe68f1c
ea82fceb2dc65bf0cc62762dd2df8853dbdac686
902f8dd913cf912021e5a33c48a9b3c7d530b0a7
c0ed451166cce58edc94cab17c8223393e252adc
b266e95d8d05db94573cf1d9144a4396f5248eb1
6ea1b572c8d5bca49ef085dcba453148641c362e
cfe8b990d32fa91ad556dedb73a616fc14bff9ae
0c8842054e9aba008f964f395de64464115b8ba1
faeba91ce8a10d237c7f3fdc4c9f86fc09c2ac0c
ea65bcf3561e17551774b4b8cb9a1c4469a2b778
2897abd5ca0913756263a94462b0391ce092c2be
fcf631e940f33641748f51cfaad1e5cc073e31f0
ea05decae3c710ac9b1fe01bf6d5d0735de1c479

KPMG

KPMG Cyber Threat Intelligence Platform

Noodle RAT - The Cross-Platform Menace

TLP : Clear

Indicators of Compromise: Hashes
4408b0f0149342e64c4a977d3c1f5ae56e7d1944
53277642a2ac0f7bb12d5464f4d7474ff4985674
51fda2b39009a71376a4a50e935186be0b5a6792
1ba5ec3a040f79fb38b0a1554938d6dbb2418eb7
809da3ec7734fdd21121d0c25504754e067aaae4
4c0a92f24482cbc60781e09db31f1d5abbddb7fa
b32d188412809a5d89979a1d2f016ea1b6f6094c
ce212a63bd3f823667f3907c333c459ba6f63719
107b35cc025f09d7e7412f681c159190459a2289
3e282386e85e1f13b097254928917667b1894b27
1afd03b91e73db0de7685af473530503bc9257ff
244e4e3f88c67ab4ad62bfbb75741e901f758828
49481dd3c7316c8e924150798e87eee884193f3c
04a0bbae3e3fe7ba167bc2d6317d0a3936286272
2b9f64e451c8b2a1983d81438b9cdd150062586b
3033d9ea417db05c1177e9c7bfb3db792c823eeb
8318c6e8ad58518349a2efd3fbcb372f81478798
7cfda35ec1576c6d169a67a00155a95c693830d4
c830a233f716416e3754e46aa70e049d10989a48028f3879d425c3851c4dd761
cf543c6d4fb03ebc0a00a8ebe89511af713817878351a2bccfc62a1cc4ac0b3f
cde4ca499282045eecd4fc15ac80a232294556a59b3c8c8a7a593e8333cfd3c7
479e3ef28d3c70b110ff993086e4518f4a5a6fb8285b530350ad2bcd6d0bb192
53338d643052bb2082f1370c21a21ff41ee1e6f43b3bd937519d7c9a491aeb13
c49371cd8dd33f725a780ea179e6281f5cb7f42e84a00836c8fe3350b7b9b2d0
a8db92a8f34caa5084a3fdb8a683a1854bff84612dfd25a965bc12a454a38556
678edc2ea9473b02a13e9fc7557f6c7172f0f00f4237e2da91a6766c53db1d3d
275d63587f3ac511d7cca5ff85af2914e74d8b68edd5a7a8a1609426d5b7f6a9
5cda94180b245de8421f226eb516d0aa1d3fd8167ebed4fa06070dd38344cec0
61f34459815eb403ec841246a4277d825dcd25700baad867b61ec3166d034825
67e60fca3d28dcae09b74ffd62f5efe462700b6d2b3334d519e4caac55820df0
3bff2c5bfc24fc99d925126ec6beb95d395a85bc736a395aaf4719c301cbbfd4
88b4904a582522d9a91fb4ad616adbd432c556b17427cfb177c8205f484792ba
bf5ea570bf4d18e60dd758a2461fbdf73a500dbd179e458aca81d65b5d9155e1
7440a7b56d3670d4204a57974fa76ae76ca78168bb181640f565976d192cc159

KPMG

KPMG Cyber Threat Intelligence Platform

Noodle RAT - The Cross-Platform Menace

TLP : Clear

Indicators of Compromise: Hashes
1e9add97a289de7f5679aceace7a3a39437a33254ac9c217d9a530e9369f60be
cac63e105d73d59c7f83779005ada0a4d3f7fb072cfc2c9590b64fe3896d2e3e
5b4c421edb3571dbc7d581596a9ac952e453394b30132dec8e390ec561cd4abb
3893f8a44a2d1fef45354984f3c6906ae8627c6f0c489f6f14e8da03197312ae
0153c9e22428f08597fe87cb8bd6664f6481e05bbf4e3d4174f44d2524446bdb
c4fb9757ed6db6ab2bd4253cb8a1542a590443654260f2b947c288d5717487d6
70b19172b743973a45f5d707d4eec4f8508d41aa684516f1fb8c75bec59d02bb
96231be4cc6cf256eebd828af4338588272ea478c609a7f16a03bdf1a61dd431
bf553e82119e2483d36eff51cf152861938c584749ebc005d4d612876277b787
7b07b722091d9658fe106448b6e1c6b7484d7b7d163ddeb19132174973b62759
b21f4039707eb4fc40ad1a7ed10be753ab3922c4a60bde819dcd74d44fef991d
4c4d51b377faebf61f95663765e622eb652866ab9cc7e9964a5d02f4dc0b53d3
b24e160843d96c6d75452d6f4e379b73a417fc821b26ca85d740ca0a499615ab
e5fb5a3b8663fbb2686caf88fdb3362115dc0f0bf9cc5d32d1e42c00aa6660b4
d17d964cacb063a6fe685d6e5e7dbc02c597de51b46c994f0aadb56c3bf96f13
ba45dfa8e6b86140e526959c8568824ddd743d418231440d48740e76a33610ea
1c2bbab6c496b66b108dc810649c19319655a2246f7fc6cf2a0911f5d73f2f3a
14f9a20356fc0e1806524057e8366d994831e3568cf438694a5c4d5463c25010
7e7bfe7e83867defa9280c8bce98cabcd0e6410cac7cc9a1baa88131b4a263b1
45b3d192ed79541a9711c16c7d73bd4d0a74598ecb7b56416f8754fb5d6feb56
53cebf50348e4507e92d23cfe3bbc87d6bf50e06962462d036542c37a50a23c1
a27d133f6a1bd72285f021403082dc8e47180fe56e88b274f474459088857603
4198efb00840f440d96987518bd80dbc90cde3023bc8c2b0aae456af07875405
abdbbc10467421b93fe1df6da0de70a4d454adcced1bfc6c1cebf1207fba93db
bcac1d42c39932fb20f571655cd1bbe507c3fddda63d4f0ea8986a3dd5265f41
68389b48c6f15b6da7f2d78c0864d6b9b9135f6ace3564d29b26f5dc9b5d6313
bf1b88385aebb37182421e967749f057fbefb4e4386bb47b5098abac7c70c476
1a9ff06ac18f57a6382fdae54bf8735a6ad7d9c9f1f9aa0dfff0e3e828f1820b
15f3536ac33588444cf6a632f17c74ee0ee8777d0d2166206222b4d5f66de715
ca2200ef6ce1abc37e5778b40e9b14031b81014560dae9c6a16fd7ba948c7656
bbcfc826f614433ff1b7c8031349cf5b411d868b07259eca9c19cd5af772b85e
6933a01980378c2160740e5cecaba29530555e3d65bd89ef80db49419a419f8d
5dac572374cb40561ea5dbc0dfc963d863f08862a0bd33fdac6ac8d0aa180ada
24a827336a1f942925fd57e763109e3a83b1a5762c077c1e80bd057bb1b15bad