Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Noodle RAT: Understanding the Full Scope of this Cross-Platform Malware

Date of Publication	Admiralty Code	TA Number
June 20, 2024	A1	TA2024237

Summary

First Seen: July 2016
Malware: Noodle RAT (aka ANGRYREBEL, Nood RAT)
Attack Region: Asia-Pacific region
Attack: Noodle RAT, also known as ANGRYREBEL and Nood RAT, has been associated with Chinese-speaking espionage groups since at least July 2016. Initially mistaken for variants of Gh0st RAT and Rekoobe, it has only recently been recognized as a distinct type of malware.

Attack Timeline

Attack Regions

Attack Details

#1 Noodle RAT, also known as ANGRYREBEL and Nood RAT, has been linked to Chinese-speaking espionage groups since at least July 2016. Initially mistaken for variants of Gh0st RAT and Rekoobe, it has only recently been recognized as a distinct type of malware.

#2 Noodle RAT is available for both Windows and Linux systems, with numerous targeted attacks reported in the Asia-Pacific region. It is employed by groups such as Iron Tiger, Calypso, Rocke, and Cloud Snooper, all of which have ties to China.

#3 This malware has been active in various campaigns, utilizing shellcode foundations and loaders like MULTIDROP and MICROLOAD, specifically targeting areas such as Thailand and India.

#4 The Windows variant of Noodle RAT is an in-memory modular backdoor, deployed via a loader due to its shellcode foundation. It supports commands for downloading/uploading files, running additional malware, functioning as a TCP proxy, and even self-deletion.

#5 The Linux variant, an ELF version of Noodle RAT, has a different design. It can launch a reverse shell, download/upload files, schedule tasks, and initiate SOCKS tunneling. Both versions share identical code for command-and-control (C2) communications and utilize similar configuration formats.

#6 Noodle RAT has shown a consistent pattern of attacks over the years, with initial detections on Windows in mid-2016, followed by Linux in late 2016 to early 2017. The malware has since been used in targeted campaigns across various countries in Asia, demonstrating its evolving and persistent threat nature. The discovery of Noodle RAT highlights the sophistication and commercial nature of China's cyber espionage operations.

Recommendations

Adopt Zero-Trust Security Model: Implement a zero-trust security model that enforces strict access controls and requires continuous verification of user and device legitimacy.

Hardening Endpoints: Apply security hardening measures to endpoints, servers, and other critical systems, including disabling unnecessary services, applying least privilege access controls, and enforcing strong password policies.

Application Whitelisting: Use application whitelisting to ensure that only approved and trusted applications can run on your systems, preventing unauthorized software from executing.

Monitoring and Logging: Implement robust monitoring and logging mechanisms to detect suspicious activity or unauthorized access to your accounts. Regularly review access logs and audit trails for unusual patterns or login locations.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	T1189 Drive-by Compromise	T1190 Exploit Public-Facing Application
T1566 Phishing	T1059 Command and Scripting Interpreter	T1053 Scheduled Task/Job	T1027 Obfuscated Files or Information
T1505.003 Web Shell	T1090 Proxy	T1584.004 Server	T1588 Obtain Capabilities
T1588.002 Tool	T1543 Create or Modify System Process	T1562 Impair Defenses	T1056 Input Capture
T1083 File and Directory Discovery	T1105 Ingress Tool Transfer	T1041 Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	4f5297c564c8f0064e7db65864198025, 025a32835eb8647147ed1bbf64c37fa5, 6728b74d5b30d2db8436f0c9f64684f1, cb131b05dc3e42fad5caeadccbee378b, ecac141c99e8cef83389203b862b24fd, 67c8235ac0861c8622ac2ddb1f5c4a18, c1eebf2d4f441226770276110d1e5cf2, 0a35e06f53c17ab1c8e18e7e0c0821d8, b42018c5fba4758ac46eb2c39344a020, f9eece34b6574236f067fa1a1782cdc0, 7d631e5b0c78805dd5d440cce788d25b, 35743db3dc333245ef5b69100721ced9
SHA1	8d9530b52744e681b1ca0de5580d065083cf9e44, b3a027f3bdb8ce87ea5eacc65e803d89b5f3dc35, 6920cf39875fb1be1a01471c3041ece615ee4e4e, 8965d8da52af8379704b09226252e185ae1b0f6f, 2f4ee1c39f78ecde5a84233233d02b355022aa50, 6aa0b6bfe059354782febd4fa665dbacd726b488, 9249b61b2d23546097ad2d5042d3f2f21ccbd11a, 14fd16e6465b74c5ac4dc895f4c15bccb447af31, f366f2730d481059a5153590ef3cab5d7658a3ef, 54670aaf6212eeec04e2cb1bf9cff984393f29ec, 1be33241473015788c11571ad3ab13ac82805da2, fa681933eccc1b3cae4cce6ab6f16db08c2f2a87
SHA256	cf543c6d4fb03ebc0a00a8ebe89511af713817878351a2bccfc62a1cc4ac0b3f, cde4ca499282045eecd4fc15ac80a232294556a59b3c8c8a7a593e8333cfd3c7, 479e3ef28d3c70b110ff993086e4518f4a5a6fb8285b530350ad2bcd6d0bb192, 53338d643052bb2082f1370c21a21ff41ee1e6f43b3bd937519d7c9a491aeb13, c49371cd8dd33f725a780ea179e6281f5cb7f42e84a00836c8fe3350b7b9b2d0, a8db92a8f34caa5084a3fdb8a683a1854bff84612dfd25a965bc12a454a38556, 678edc2ea9473b02a13e9fc7557f6c7172f0f00f4237e2da91a6766c53db1d3d, 275d63587f3ac511d7cca5ff85af2914e74d8b68edd5a7a8a1609426d5b7f6a9, 5cda94180b245de8421f226eb516d0aa1d3fd8167ebed4fa06070dd38344cec0,

TYPE	VALUE
SHA256	61f34459815eb403ec841246a4277d825dcd25700baad867b61ec3166d034825, 67e60fca3d28dcae09b74ffd62f5efe462700b6d2b3334d519e4caac55820df0, 3bff2c5bfc24fc99d925126ec6beb95d395a85bc736a395aaf4719c301cbbfd4, 88b4904a582522d9a91fb4ad616adbd432c556b17427cfb177c8205f484792ba, bf5ea570bf4d18e60dd758a2461fbdf73a500dbd179e458aca81d65b5d9155e1, 7440a7b56d3670d4204a57974fa76ae76ca78168bb181640f565976d192cc159, 1e9add97a289de7f5679aceace7a3a39437a33254ac9c217d9a530e9369f60be, cac63e105d73d59c7f83779005ada0a4d3f7fb072cfc2c9590b64fe3896d2e3e, 5b4c421edb3571dbc7d581596a9ac952e453394b30132dec8e390ec561cd4abb, 3893f8a44a2d1fef45354984f3c6906ae8627c6f0c489f6f14e8da03197312ae, 0153c9e22428f08597fe87cb8bd6664f6481e05bbf4e3d4174f44d2524446bdb, c4fb9757ed6db6ab2bd4253cb8a1542a590443654260f2b947c288d5717487d6, 70b19172b743973a45f5d707d4eec4f8508d41aa684516f1fb8c75bec59d02bb, 96231be4cc6cf256eebd828af4338588272ea478c609a7f16a03bdf1a61dd431, bf553e82119e2483d36eff51cf152861938c584749ebc005d4d612876277b787, 7b07b722091d9658fe106448b6e1c6b7484d7b7d163ddeb19132174973b62759, b21f4039707eb4fc40ad1a7ed10be753ab3922c4a60bde819dcd74d44fef991d, 4c4d51b377faebf61f95663765e622eb652866ab9cc7e9964a5d02f4dc0b53d3, b24e160843d96c6d75452d6f4e379b73a417fc821b26ca85d740ca0a499615ab, e5fb5a3b8663fbb2686caf88fdb3362115dc0f0bf9cc5d32d1e42c00aa6660b4, d17d964cacb063a6fe685d6e5e7dbc02c597de51b46c994f0aadb56c3bf96f13, ba45dfa8e6b86140e526959c8568824ddd743d418231440d48740e76a33610ea, 1c2bbab6c496b66b108dc810649c19319655a2246f7fc6cf2a0911f5d73f2f3a,

TYPE	VALUE
SHA256	14f9a20356fc0e1806524057e8366d994831e3568cf438694a5c4d5463c25010, 7e7bfe7e83867defa9280c8bce98cabcd0e6410cac7cc9a1baa88131b4a263b1, 45b3d192ed79541a9711c16c7d73bd4d0a74598ecb7b56416f8754fb5d6feb56, 53cebf50348e4507e92d23cfe3bbc87d6bf50e06962462d036542c37a50a23c1, a27d133f6a1bd72285f021403082dc8e47180fe56e88b274f474459088857603, 4198efb00840f440d96987518bd80dbc90cde3023bc8c2b0aae456af07875405, abdbbc10467421b93fe1df6da0de70a4d454adcced1bfc6c1cebf1207fba93db, bcac1d42c39932fb20f571655cd1bbe507c3fddda63d4f0ea8986a3dd5265f41, 68389b48c6f15b6da7f2d78c0864d6b9b9135f6ace3564d29b26f5dc9b5d6313, bf1b88385aebb37182421e967749f057fbefb4e4386bb47b5098abac7c70c476, 1a9ff06ac18f57a6382fdae54bf8735a6ad7d9c9f1f9aa0dfff0e3e828f1820b, 15f3536ac33588444cf6a632f17c74ee0ee8777d0d2166206222b4d5f66de715, ca2200ef6ce1abc37e5778b40e9b14031b81014560dae9c6a16fd7ba948c7656, bbcfc826f614433ff1b7c8031349cf5b411d868b07259eca9c19cd5af772b85e, 6933a01980378c2160740e5cecaba29530555e3d65bd89ef80db49419a419f8d, 5dac572374cb40561ea5dbc0dfc963d863f08862a0bd33fdac6ac8d0aa180ada, 24a827336a1f942925fd57e763109e3a83b1a5762c077c1e80bd057bb1b15bad

References

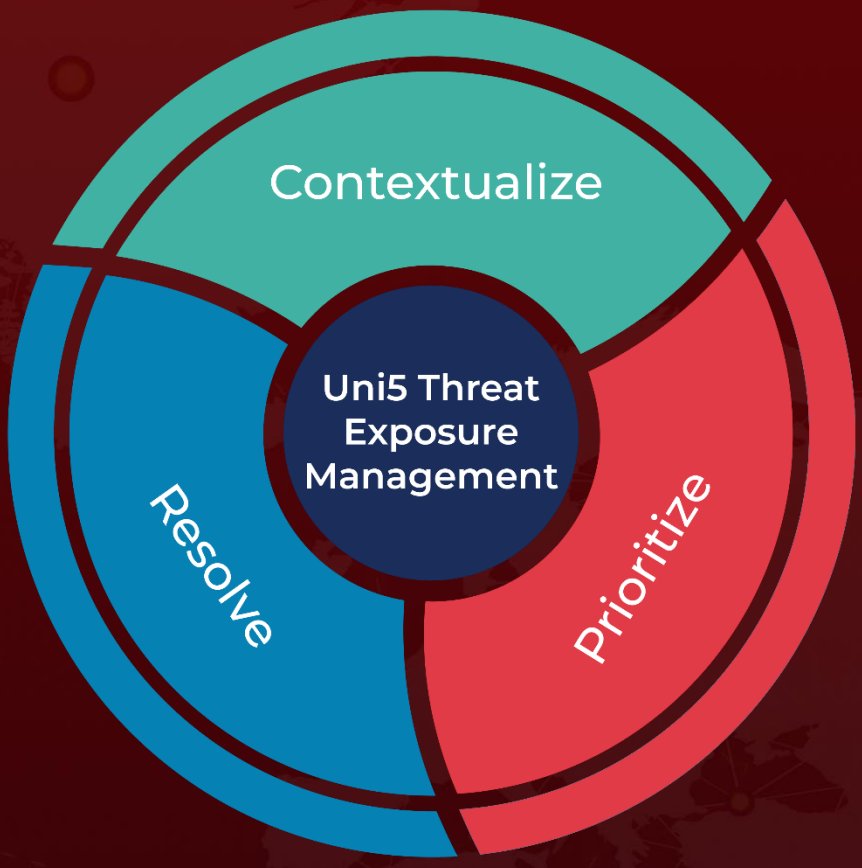
https://www.trendmicro.com/en_us/research/24/f/noodle-rat-reviewing-the-new-backdoor-used-by-chinese-speaking-g.html

https://www.rewterz.com/threat-advisory/new-malware-noodle-rat-targets-linux-and-windows-users-active-iocs

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

June 20, 2024 • 6:00 AM

More at www.hivepro.com