KPMG

KPMG Cyber Threat Intelligence Platform

NJRAT - A Persistent Threat Affecting Critical Industries

TLP : Clear

NJRAT (aka Bladabindi or Lime-Worm) is a sophisticated Remote Access Trojan (RAT) created in 2012 by the hacking group "M38dHhM." The latest variants, NJRAT 0.7NC and 0.6.4, feature new enhancements improving its functionality and evasion capabilities. NJRAT has been observed in numerous high-profile campaigns targeting key sectors such as government, finance, manufacturing, energy, and oil and gas, in regions including the Middle East, North America, and Latin America.

Initial access is gained via spear-phishing email with an obfuscated VBS file in a seemingly legitimate document. The VBS file executes PowerShell to decode base64 data, which loads a malicious DLL, containing the njRAT payload. This payload activates a method called "VAI" to secure the exploit and mutate the system. njRAT maintains persistence by copying itself to the Windows startup folder, modifying the registry, and setting environment variables. It performs a range of operations, including logging keystrokes, capturing screenshots, extracting credentials and sensitive data, and enabling remote control of the compromised computer. Connection to a C2 server is established using a custom protocol to receive and execute commands, send data, and maintain control. Stolen data (e.g. screenshots, keystroke logs) is sent to the C2 server via the established channel. If instructed by the C2, njRAT performs self-removal operations which includes deleting itself, cleaning up registry entries, removing its firewall whitelist, and deleting persistence mechanisms. To avoid detection, njRAT employs .NET obfuscation techniques, disguises itself as a critical process, and detects virtual machines or sandbox environments to evade analysis.

NJRAT's extensive capabilities, including advanced evasion and versatile functions, make it a highly adaptive threat, necessitating a comprehensive and multifaceted detection and response strategy.

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2024 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG Cyber Threat Intelligence Platform

NJRAT - A Persistent Threat Affecting Critical Industries

TLP : Clear

Indicators of Compromise: IP Addresses	
107.2.6[.]1	109.197.74[.]13
1.227.134[.]55	101.132.25[.]152
103.70.5[.]250	103.147.184[.]73
103.70.6[.]159	103.212.81[.]159
1.243.157[.]185	103.22.181[.]199
103.1.184[.]108	103.91.207[.]190
103.149.13[.]61	103.91.207[.]235
103.82.249[.]74	104.234.10[.]114
103.91.204[.]40	107.167.244[.]67
103.97.209[.]13	107.175.38[.]101
104.168.7[.]110	108.158.147[.]14
104.20.68[.]143	109.206.243[.]59
104.22.32[.]240	103.125.234[.]199
109.197.74[.]13	103.151.125[.]186
101.132.25[.]152	103.212.180[.]233

Indicators of Compromise: Domains	
cynorix[.]com	bitcoincoin[.]xyz
fucklgbt[.]lol	fortdelgres[.]com
542199235l[.]com	file-coin-coin-10[.]com

Indicators of Compromise: Hashes
8fe42fdad7d7d33f91dae15b35dd1a30
2add405f7dd20dc3fff8ffa82d3caa39
256ac8fe73c61f22a1c479606e1508ea
c4ef301caf49a38ffd5a95ff9245ed80
c69db7b6cbe628572359bbdbdda07177
09f93cc4aab59e8304e022b0d2179260
935b4f91cd79ec1d023f6071bcf5b584
2b6de935b211af1badfd58ee09e1f343
c6cbe0c2fef6507a9a7f828a4a59cfb6
185318b82fe99e78d51cf9b9e132e9a0
40590d26405803eebe8b0aa66d086b60

Indicators of Compromise: Hashes
6175e14e465756c626ccc0f398fcdcb0
4b7d118b20d8854372129f53365d529f
edf8f50f318c20bccb889743172d9fd2
83719e7f59fb51e605fd66a16ac4dae0
c0785717b43c81b30106a530f8880860
2cbace9fe745d6b698953a1286eaacc7
b4a8a6d4cd9c4e2f530fe3bd8c3e3fd3
d708dafd133a13e84c5db6ad23eecfa6
de296b6955dda4d05cb9090b583712b0
5a58b504897a518e9f719bb8da20a681
dcc0946afc440b8b0a0c4ec24ac30db8
ec53ca8c607f9c76345c7e2aa95f7074
f39d9edcb7db7838b0f7948f118b96ac
7b2de084cecce4991fedefa673b71cdf
fffa70b03be37289d22501472d2a2840
3a46a2a92ccf023b0149d791bc79899c
6d2ff29ae225dd5d9472053c4f804890
a892edfe5c99e03acba96225afb0a1e0
0ea77f8ba4ca83bfbbc2bc429653a831
0616222604d7b733cbc9251fe6fcaac4
e81425657414d958a7d4eed978e58338
06573d2a17de5eda5ec8fe95fc49eab2
9a64c26c15d374046a6bec8c889bb5d0
a01b1742a6fd16667a0aae71cb6636b9
219149012db021f4135e38bda99693e6
41e990ab2c6582fa78eec4de2c4d731d
bf7cbb2ac60406fe0c339fb89a6d610b61f7e6b2
33155ce05f51507912b032e608dd68bef8897723
561374deac4562846aae126b59ff07f0748dd12d
c0e0e1626fb8895177db8dc7fe446eecfa65df45
b46beacb407b24d9c9c5cf98eec30ca777d0285f
18ae42c6fd7fdb44e81e9b4cd93d547e7e81fc99
7b46f6976e30df63f23a53b65b6ac15fc58f1b16
1e7030c9bce0bb2c720980d6c62272149d1f040e

Indicators of Compromise: Hashes
2631afe67cc6f6a10d97c59e258ee74c1a84a303
b5e9a852f6fa1aabcc6314dc4229908aea82ca3e
76d85bb70f6339622a8208f427c02034798bf8e8
287ac3fd146079096b0ebdbf79c59acdc61db090
d54cef9c9fef834a61413ee816ff2464a9b6bc36
5f88c8fd69c2457bd37442b7a03b17f4d1964199
d97b6a238bd9cb96e48e6bbf951606722276fd18
8d907d8a043f66a5300dbdc7b75ebd5da8963dfb
72a48d1c49640a6623fc5add0dd04f30c89349c2
8520bedfc884c3b98b99b0b75608b625f45c2c9c
a09b41ac539fd3f362b2ecfe5f07caabfcf7a28b
bc86587c8ecd8157fed12690890318fda1ff90df
40c19b465bba365ef8ffe3d2fc1e0bff32b1dabb
43c4e2185c07b2f1bf7caf926276b1cd824a2f4b
6fff251b09868c598e4a11fc533a5ad8a11a1422
9844fe4ae19c282635b2c5cfc7106b42ff9a7146
c23dd17842334c85e65908e571043b7f841b5ff5
f9889efc1a5cbb619ddc957ca8b01899259476b9
835c1241aeb2593de39203eed3cb40d9ffdf38ad
3f3d16ec658f869d90b2126f51e0c6a5756d7c88
6339617042b563fb88bbeac577b8dfaf6c5cca9f
30fdf184938a9d92efec22515fd88dacadea61eb
59a3fa9cd560a8fc750fcc045a779c09cea4c41a
1e9e92d2fe26843ad45fc8fe9a656ea68bf57b56
cf159cd756afd8709bd2d2d76274a6fabb926f20
801410d19aa4b4d5dee2fff1c5644184125eb77c
97557e262dfef14906a9f3b665a884934dd08c92
60a49e3aa221e08efd166dd4c195946c1059c052
b8c6b8c81b541d35fdb4b318b3ac999c885fceb8
0225156af50ee95f9fdbfca0c0fe652d81bae15ce2f0b41e68ef857536c140fc
021dc00726385f75bafcd0ae02fa6c9aa369f2b6e02571c22e3510d726e0c9cf
01602f727c84ee7e11e3684c0886fc03f4c45980ecfbfbd361a7023aafc1330d
0164c3cf00850e242bba50acf83d8247308477c24cc47c4f35b7100006f73823
0174841d3dc6ff63135c23732a8dd375e4c86b8025050b47b515a92373ec445a

KPMG Cyber Threat Intelligence Platform

NJRAT - A Persistent Threat Affecting Critical Industries

TLP : Clear

Indicators of Compromise: Hashes
cefa4ebf82b3d077a68ce1933be3dc6e9cadce8bc27671a5fcd76ee2f4d04977
0ab64bf67f37f11a4681e26df984b1c402c6f8b7180de9a176527721004108fd
51378096fae4ca961c717dd6c793210e532c0aad42a68fb42d38a136df28c994
00106cd75add92ad18167e93eeba2876a2409e8c86ba2587e99ecebf8c6fa7f9
001872a8a1fe6a61f749c8741d9f6e7b76ef8e86c3509c638681dbf15aee24af
001b2f473864a2324818c19768fecf53adb6614fb6f9d84360875b48bd0f212b
0029f3ad8f965207b3dd5173e11a82c970369c564ac2501d9be7e63a02ef27af
002bb2f17508a37c2e66b04e53ca1fb98328306886d7db8328ddef04a0e0b5c5
0052ac6031eefb69fc5f5cd780bcb5fff2a0728c5f0c57b01493a64d7004b7e4
00584b2ffe8284a1e024c424dcaf0decd18da1562bef1e1ea409487aeb655d53
0088d42558db8697390fe888cc6bbb230fdcaf726069a11cc28a44595eb38f18
009e23ca30cf77e3bf43f57becd4b1ae85ce8cddafcbeb4b8618d5374fe23ff9
00be3df100019a015209e3ee4d2d8aa68d787ba0492e69a85da681d80635cc72
00f1708c72b9a382d958d057049877ab58ee7039cdaab81fe419067b13d75223
0138a1985fe1f6cc49d5b61d477e9c7b677434a3cd8fc48bbee3a1aea1a8de97
014984b4b81ac3aee22523fc6a79030159f63a0f79ba6028dde7dd8795b1c325
0153b54df5c746be46830624f1b44dc2525cf48a9a3535eca21e0aa44cccc206
015b1b8ab3a1a9cd872b490ff5c2330d65d37ceba0d1784c295b4a4e1f173898
015c8775ff5e46f8ac053936d1652d82db5c1aaa5a275aa1b957f723e8ec9b23
01897bed0d01dbedd642a788244be6e178b5f049600aa6241572a2a19f7b4781
0198efc9aafc205a769a41760a1787050b45507f8edbde5ded906e1a59a14cda
01b7c4f2fd331fa3b60509d40f17e18622cc4e2e0d51d2da642a8a169b4099b3
01b3b58616ebeab846c36612f7e1dc250f4860edd3aafd90478b44a82b92fa93
01ef01c7d774edd368244257d4294850f2c4f0678b0938c8eee818a3a6ebcaf0
01e8c52df1c70cc30a8b6fd42c385b292bcb0ee5d3cc7c5b86371827d31a12e2
01e3c4e657ab9990d03eabcb3fe1fee29fe6d00611e2c0c51d632f6043a2d6ab
01d3c6c77d0c71f1a8aa55a7ad0dc6b8f7427760906a028f11259aa43f96d282
020a9a702d9da62a44d23ed68f50d49df2e06aef54da60ee2440c21e8158bbfd
02097aa971c13f51e9640e58ac8c4b90c29f7b7ac760a95b12169a6989b78b3f
023a41305bae352e2bab9686ab8efdde111585a6e357b6245b59bb3459142b38
0231c4a5cd7e1a07cdbaf84df4f635fd6c4acbadf14f817b4004ecbcc3fbd3f2
022a1b5715fb0f998d764baa57a9862bf3e766de274125860748772e9eecb3b2