KPMG

KPMG Cyber Threat Intelligence Platform

Raspberry Robin – Resurged with Advanced Evasion Tactics

Raspberry Robin, aka QNAP worm, was first reported in late 2021, and has emerged as a significant Windows worm targeting the technology and manufacturing sectors. Transitioning from USB to WSF distribution, it deploys intricate obfuscation and anti-analysis methods, complicating detection. It's not just a standalone threat but also facilitates other malicious activities by groups like EvilCorp and TA505. The malware delivers multiple payloads, including SocGholish, Cobalt Strike, and ransomware precursors like IcedID and Truebot.

Initial access, potentially via spam or malvertising, leads to malware spreading through malicious domains and subdomains, utilizing Windows Script Files (.wsf) for distribution. Upon execution, the malware uses techniques such as using unreadable characters, junk sequences, and unused code fragments to obfuscate the script, for defense evasion. Additionally, it employs anti-analysis and virtual machine (VM) detection techniques to ensure it is running on a real end-user device rather than in a sandbox environment. The malware accesses Windows Management Instrumentation (WMI) using a SWbemLocator object and interacts with the Windows OS via the WScript object, checking for virtualization by analyzing processor patterns, network card MAC addresses, and running processes. To maintain persistence, it manipulates Microsoft Defender and evades dynamic analysis by self-restarting with arguments and residing solely in memory. After validation, the malware downloads the Raspberry Robin DLL, renames it to ".dll," and executes it using msiexec for further malicious activities.

Raspberry Robin's agile tactics and evasion methods pose a persistent challenge, demanding continuous vigilance and proactive defense strategies to mitigate its impact effectively.

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
Associate 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.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

Indicators of Compromise: Domains	
1v[.]nz	dominieunflaming[.]sbs
7t[.]nz	ophthalmomyositis[.]sbs
9y[.]si	mammaterijekasumy[.]sbs
polyideism[.]sbs	halsalkalindivvies[.]sbs
quarrelers[.]sbs	metriconetimeagley[.]sbs
brittlebush[.]sbs	freamingrafttwoway[.]sbs
misalienate[.]sbs	dundeelieflydeflect[.]sbs
chroococcoid[.]sbs	hockersmixtecsquier[.]sbs
refractorily[.]sbs	nametagsweatseyelike[.]sbs
counterboring[.]sbs	rockerstalbertcerate[.]sbs
syllabication[.]sbs	biltongpumpsiecrumrod[.]sbs
annuelertimes[.]sbs	arctiidkwatumaindwelt[.]sbs
spendthriftiness[.]sbs	dechlorinatingdermatropic[.]sbs

Indicators of Compromise: Hashes
553b9eaa741adfb9073638e001d369441a802b406d3bca50436aea1df5b16da5
4c87daaa84c41706156d370603602147988262 29f5dedd6c46c821d879409509
4e93fb810189d3e1df1d0ef0f30642b8891e4140301a4aaaf5cb939555887 34d
0b369277901fff2ac52bf04e366318aa9018e7ea570779f476b2a0e676c9db83
ca6f46bdfd14021c102d4e4d95597a20bb9685628b4067b9ba85f18644ad6cdb
98ad6aad996e4005389ea7e4782a4a082c1e83a8a20ad07bb3a3eed4047b3603
9303b89abe2c0393e78991f74a90d9202a2f14dc267367277da7af705733eb32
229c6b0dc9298a6868a24aad6cf3c8b08feb97f809f2d67fb6dc2e71ebee876b
78ae67f650400ef6db9a85aa3d10ab7684f789e587ef33420a352a9b53916364
dd576545834e9c439491d62a8a6d9578a58693cef9f5cd2783fc80f49275dac8
fbdbe211e66792f3cefc50da6b3b88d82d497be1cd25f4654d4d122c0ed10a42
a3de553cae9671bd94aae75f76f8de2dd9abb41780d25f012debf7761a579ea9
479d1cb582c03c679cb23ccb6b5dd1611822f59f311a6cdc82bd6eef5f53da14
d5dd3f1dd787746403843100c8dec9c70c20d8098071aafc5bfeef20b95fd93f
b4566c3cbfa193ad6dc7173d8b5d93734f06d940085110f6a2c781252 4c2c236
752ccebfcf2d63d44bf3073b2f30e83758aa0ae26d3bdca59de6e53e6d33b19e
a81176e32b8d73fbbd11d1a1da32789c8b18cf6aa79e1b4cae8ed031b7e9dbbf
99d1e9839922063d3655583d541ac6908000222cd847c95c919a27c9d2b01301

KPMG

KPMG Cyber Threat Intelligence Platform

Raspberry Robin – Resurged with Advanced Evasion Tactics

Indicators of Compromise: Hashes
07b19580d9c5febb2b7d1da395022ca790372104bc99b35a8b18d506dfa2f9c0
8921a869a93b4e9cec50b66b81793af67c2664aec5028c48738bae03f7026560
981e56f56ab9c3dc81deed819ad3cd7367b8d44449a1ebbf1aad5033f2bd4547
068f7a941ca655d71dd894c1564a24bbe9d67a6aa9e60b0692f558512e28c3a4
f2e1130b4baf1dc611fdde8029234348b4df69d5ebe32edc540e6fe1caaadd0a
de877115545a14417593fcf21d0ebf9b252940155e8fcdf152e5c6af54ffc84f
4a0af8b333065d245b094964de709bb832fa630799106e711b38357236780924
812f646f94d6b6766698ce11de68bf49e9478272ad48113c4fe227735a0248a6
2fc1750ac3ed97630a6088d1c4007065beaf44f50dfec1a068cea33537a53160
08beb3900bbd4b4860e41b08b8585b7f3021676db3c07d9615d1a0aa92d3f0ce
64c5b1ccc4023e0cdb1e7c880f00832b2a98bb9ce18f832e0c664b16726ea6fa
28bc455cf1feeb0d9de0680ca8726bcf723b47bef43d3cb4180972aba7d30fa8
b55e88c542c9a90b4cba403d029f0c21aca5d3f001c47af7650269a227d9a982
3f0fed4651179173f88b6be99eab1ab4f04f5eebe0f7eecdaff59b1e0c9fd6f6
63ed9258e33164ee82be7d933377484b7ec7dc211a1119e4def4ac64d8d75c1f
2dc987eb9844063e824ff6c27d64176c9fa8fcf974e835d5a06f6f022a05ea2b
8fe220f1d81857cdd9d72d85a6d44d6e6e8bab59d6454877b27e6104bc3a2b01
040a7f7f0304b486f82beac718abe7628fd1c514c22afa49d5540e652db9aabd
0d35c51a0214117f1ad94428ccf789c8dd2376177192a86c4e7af9bd106affae
83af28eb822624aa7d2434697ae1857ff7d5a27b8b1cbfbccc7ddabc4d6299e9
c2d4c676886a94f26fcadd5c381183ec93583b63b6acd43d48cff90c6a308bb2
02e951d3e6644d21dd5b1d99f0a3b3111985bfe798a99a5b884419282c9c18c7
ff927726e3ef1a8d621696ec9f28925406f40d2eaa2580a8585bd8b1ab48a53e
f88fd72addccd83abeb8e1a946d6912d52a4a1c79452836a6b3bfe466e918ca4
369053a465556ac48558b1d1fb44b4b8a99df362a0633bcce8215a54f3cf265b
c39f842302c80f925f47f35f0a033229e554a2e0128b2f98d93e1094ee32c074
59e701743d78bcedc8ee825348c4fce930af88179ae22b34b6ec6fa4091059b5
577277dee893b1a0fd6c84a0d52708dd198704b43ca25c6d8d62750f212db71e
3c888db21bfb820731e08607497c3692bca4ccf396b91b11770fe1eccbc69e8a
db7b3ff26af8a6ea7d986c21db50c55e7b5a2f9ad3264f9f8b6a2c24044d5640
8d033a8d7987e9bd533054762d8c314a1e650df28cefe1d4d01b6516407c13f4
1e45021c137a2a09002aa063c8b976ddc3b18a18aebb5847e80ee2c3799b92e9
a982ce60ad2a680ec6dba4e8eacaf9ddd5e6222731299ada6a8a5883465d865e
2d83ee0241906ea366a01be95daaa243c164ff2c8de8adf8ba488ab770017ddc

Indicators of Compromise: Hashes
3a175d0703fabecc2a3b275319ea0121ab72f65791e1cb19e95271e6c886d2d9
5ca87d09d855d5f5f4776215eb032d3db6f9a9be5cacc281f9e54442673e359c
6d7ed6fc5f5fd62ed943c32d6f0fc6d80d3dec66c8d39baa8f6a67f124b15c82
a0da83719bda577f7117245a99f8b1c93bb3d7f26e01fe541caa8cf76c1305d3
664e43cc1f05272b106449a4bf1e46268b16953bf13bd5c7895c0cf14c2acf37
57dd92e059d73f3355b02d76d23f37ea907e377b81586bf9ca106a9f5874f985
c434c46e740fb0945be98edd46ade19fdae9ba22c97fbf0c05d1dfd78ef29931
2b39d3cfe9454bd711039b6fe7c06357ca6857232b39160c3f87181677ed1d94
02a3d4501ee318d2f32dc8710c30193078e4ed6cfd1d8e739d25a7cecbe721d8
9901bd03f879abb46fd40844395cfcd3db7aad2d8f39fc4036daf80142d5c424
2b8985171132bc3b6c935ff0384b89b66c8c4b0d94f2f3635c1929e6f25d4df7
8452b8172f60b7faf9a451dd60bce5a1e05d0cec23a2b9feb63352af2c3c09aa
95a7ee7dc15a92ac73ebafbd3c434923a8a4ff452b899c0ffb0300c6234cae00
2de6c465cf01530a5a8a665ca7070b251f6268748fc600868f66dba7b8831ff8
c1a0cae08c40f4a6f4a08b166a9958d6b5a34597dba4c065e99f0bc35ef92bcf
c8461e1600a9bfdf7bef67f8b042f9d0889970564a9afa46695b154b1558802d
eb93af5de2db5695d0aad2cdb4fab9722699c96baa2fb939423d56efa9fffbc5
976cb19ba871775be49ffa665f9e6e40e117b8234f1b62157919179c96cffc1d
bbee400083f1252c67f2aee49c4ddc0ca91eb1d43cef2adfb2efc5fec8c4507e
98798ff8d95b4c85e55ccbfe5954bbad215533d30ef2706c7c20acb53c34cebb
6291634df63495aab81eba750b6bae61b4e344788585dddaf30489eb56b270b
b08b277ef09ada4b393824c58c6966670feef4edf5f2687ea7f73057f4a9ba74
b089ebdd7415083553a72694ae1eb063ec71e219ece5319fa53aede32b878e95
0944f760ea0b471225 3059dae86c4c229edcadbb24087a3a09d59d5f36bcd4ef
6b01ee1a9c9082907b46e788ca6707c95d5aec272790007810eff52bfaabff99
46dfc1ccf5b9e443835f3f10933a064cee32054331279f86070516588e26ae3e
67001013750b2c9e9a7f3b240531fd563ab406753f5634e6d7343fa203f08ac2
35943c73bed9e5c1852d9fa3bbac1360cfe302aed11ee512fe9c54a1263fd10c
e907b6cb8977f8eb0e41569969c3f228fdcee5c6aaf45871c74b7d7b62c31320
7b2c39ab0b027d2c842fd1be41116b5e07b63e1aa644d84a9d09a5b57f040b51
e77ada0a635f6b656c03cb12208f54cbcad1dbe39e89f5b73003d55dcba7e64a
c34f4c38cefe4d786703866fec85c2a1ce620f4ba8e8bef0ccbfd4b33519c6b6
87ea33dc761eb16768f98453e55130796c48da574ff810f33a4d0c6f974ff4e2
39f891a7c958361777e7afac705c1b8d72e81c2f2f0407c3748087c3c8f840bc