KPMG Cyber Threat Intelligence Platform

Raspberry Robin – The new popular worm

Raspberry Robin, first observed in September 2021 as a mere worm spread by USB drives has evolved into a popular malware distribution tool used by many threat actors including DEV-0243, DEV-0950 to name a few. It targets companies of strategic importance in manufacturing, technology, oil and gas and transportation sectors. Within the past month, it has spread to nearly 3,000 systems that are connected to almost 1,000 different businesses.

Raspberry Robin infection starts with USB drives which contains malicious .LNK file disguised as a folder. The '.lnk' file contains a link to invoke "cmd.exe" that reads and executes another malicious file from the infected USB. Further, "cmd.exe" is used to launch "msiexec.exe" with mixed case letters to download malicious payload hosted on compromised QNAP NAS devices which serve as their C2. Further, "Msiexec.exe" used to launch a legitimate system binary 'Fodhelper.exe' to handle UAC bypass which in-turn spawns native signed binaries to run malicious code with higher privileges. Persistence is established by adding itself to RunOnce registry key every time the payload is launched. C2 connection is established by utilizing native processes like regsvr32 & dllhost32 processes without any command line arguments to initiate outbound connections to TOR nodes. Raspberry Robin has found its demand within threat groups deploying Clop, Evil Corp, IceID, Bumblebee, Dridex, etc.

It is imperative for organizations to monitor USB device connections and disable autorun feature on Windows. Also, policies around use of USB drives on endpoints should be developed and enforced. A sound awareness program and red team simulation to aid in overall training and protection from such threats must be adopted.

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

KPMG

KPMG Cyber Threat Intelligence Platform

Raspberry Robin – The new popular worm

Indicators of Compromise: IP Addresses	
77.3.29[.]5	95.112.26[.]67
46.11.6[.]104	95.112.99[.]68
47.62.21[.]60	95.88.31[.]182
77.0.14[.]225	37.223.74[.]108
77.0.54[.]234	77.102.161[.]76
77.0.76[.]210	77.222.169[.]40
77.28.25[.]25	77.227.156[.]97
77.28.30[.]58	77.237.29[.]198
77.28.30[.]92	77.92.212[.]109
77.33.92[.]10	77.99.129[.]181
77.49.34[.]67	78.10.163[.]208
77.56.224[.]7	84.221.210[.]56
77.6.65[.]115	89.103.155[.]86
46.11.83[.]236	95.116.202[.]95
46.11.88[.]157	95.116.84[.]233
46.11.88[.]251	95.88.112[.]237
46.217.252[.]5	179.60.150[.]120
47.62.80[.]170	185.55.243[.]109
77.10.57[.]142	195.158.67[.]252
77.134.1[.]180	46.217.252[.]172
77.162.19[.]47	46.246.235[.]240
77.253.40[.]31	62.117.214[.]168
77.28.19[.]243	77.163.246[.]172
77.28.20[.]241	78.120.231[.]242
77.28.21[.]107	78.127.108[.]253
77.28.22[.]149	80.174.244[.]147
77.28.24[.]132	88.141.193[.]140
77.28.26[.]122	95.112.118[.]167
77.8.158[.]118	95.112.128[.]167
77.8.173[.]243	195.158.67[.]252

KPMG

KPMG Cyber Threat Intelligence Platform

Raspberry Robin – The new popular worm

Indicators of Compromise: Domains	
t7[.]nz	krrz[.]pm
c4z[.]pl	l9b[.]org
f0[.]tel	kjaj[.]top
p9[.]tel	uoej[.]net
nzm[.]one	cnsbi[.]mh
lwip[.]re	qmpo[.]art
bpyo[.]in	kglo[.]link
glnj[.]nl	

Indicators of Compromise: Hashes
e8f0d33109448f877a0e532b1a27131a
22531e030b05dbaafe9932b8779c73f6
6f5ea8383bc3bd07668a7d24fe9b0828
90e00d255fc9162080c02510e7e10ffa6b6ed995
bfcfa72ba5095fba108314c1c4deb5faed82ef4d
f2590890dee40225c5727f2ee50e8e8c8283a0f1
f0be02c32a05a653b75bfec845306bd7555042fa
b490bad317e2a5b14c143393f221829825b52fd0
98a9366ddc8a411bcedd6934322ef50e2f203215
7f157d69f981637e1275a670862c2ffa6b3571b3
0a290e597ec33194f95fbccda632b106c93dc28d
1a5fcb209b5af4c620453a70653263109716f277150f0d389810df85ec0beac1
f89b5ef68b23921fffd500edd254c2d44264e9f20eb682dc97ecdd97ed5fe6f6
05c771c6ab0fb3b75dcaa748750ec31de621e61a23e42b52431d67b1025a1e56
09600477ff392293e3fbef40b3ecdb489819f6f0c74c3c8ec90efa58a0e8bd6f
0b5860e7a380623920a2426dd72fe5981ec1f21600b381e414eb54b0b2dffcc6
0f2fefe08d185e1a03d065ff45840b5bd3b9c0492b3b8434fc785e96eb981a23
105a6bfbc28c85c95411468c6e45ca66ceddfd16e04049c076160b689d0421a1
1073d38346b39fb3d92f4cd814ea13d32ecf5b16c07c87560802343bd1605dfd
1308405ad1cacc637c888a93028962c0638d3a09f8042e9d51fa269d9af5be75
181303c131c604ca92454680d988782230aa9d424ff7b1aae8eac172adcc63f5
1d0191c5dc6cd12bc3718fbc1c7bff5dc037d79f6e0aa29441a9d2c717a81005
2011a4d44868c7ae5888e002e560bdefaee80fb1ebc475ab27cc087ceaba3421

KPMG

KPMG Cyber Threat Intelligence Platform

Raspberry Robin – The new popular worm

Indicators of Compromise: Hashes
273f8a8e3f1f7aebebb62cd85ccde99f31c97cfb690bf1d82137dc907d8b46c8
2b58155372b12666d1ffd2b868200c6d4708bce810cda5de1df4d027878bee50
2d09627f1e18e10a84ee46a39393a475f2221646845619d0e91c53e55b6ced78
3258221c3cfe43e436dcdcd861094958fb3b2a0c6e6fbd480340a617bd6c6372
325e69483cabd38079c34b6aac5f7ecb6bd971e2ad050009569fbf5f87e5b4e5
3456982084e2ba7e9bf2640d6635aad3b73daa0e6d4b5d2fadc8231234a8fefb
3e97d7208c0b4d30bd9e2df8128d149bc63678e6bb4de1c856652ff1771e399d
41a872cfc4d45bebd449c1f07df957003ce9e2b70f61723c87a11c9d3ad18a5c
4bdc63acbbdc6f332d710327cae95825e517e5023c8c3d708433d4adbd905565
4ec325580b1b5df51c1ce739795ba0bd791b87eb46b30d01f1720f1a4a4855f4
4f7d0d590e1beed28c106c4dfb0484621fceea018b9f655987b42a623e58b18e
6198efa6bec2d0ecf4eace023570538289e8160866caee151bda35be7736c1b6
6265d6edfbf0dc8e475bb1ad50d211963302e3ee6fb3ffa1554995fc132e7288
634688f7b8f7b1cdc1103fdf1d27a2f0a9d944eca3561949b6638325905d9523
641e899d788a5a12aaa9ce95a3b136ef69746ea41075364c545131b44a671150
64aa54501ee346360ef487938058dc6987a2217928eb3bd097bae24a3b1f33af
667e9bd9ae498dcfb9948f7a77c188fb26df9eb2fcc51bbe41ab7c2a3ddff230
6966cf4fdf8d2903e6592dbe33d9c384ecab2a04c52f7ceb4443fdd76d4243ea
6f179213ad18db6dc9e85159af8224f1aafde8db534cb7d1e6400eeafc4650f8
70dbb7409aa5bf237f0463da8a26e2c0ea12d7f2c35e9bce89a9b2e820ac638d
7752fc97466c4d70051d078cfe0741655a0671881b04de7880baa6bd23a1aea7
825c881dd6061a1b181bdecd74da45a894e9ab6c5674f019172e4926d1e19b6e
8b9ea540f76c84460a5457b060489341b3374e0b17c24895b3df68e73bc12011
8c6eb7b3590a221d6e5dde90c1b3c1a46cc37ab5e0becf0c2fb96358856760d3
8d35efd658a4c648f1f0bda743b235ea298ba427aa9c24fe7d37b34f65029636
8ff280e6e5ce3d38fb92c687cfe7ad39538b041632ed018815eb126b24e5d491
9239c45b08079866ad61b0f35709bf0502af35e0661439b886bf085b0242bdee
92491497b83a8ad213c15c3f43fc34358a6d7e5ccf3cfbc7e93bb3f436a96456
9254db5b18f53f25d68ab5a1e973a46590965403cb3b38ce0a0c171653e810b7
99c0c2111241b8ab416a7405a0453b77b3e5749bfd1fb182848b903d1adae15f
9c362e16e56723885d4c3ad88ce36d57713f24d01f23d52b0c465d5d4767dd8f
a14f14c7b468c40f865db7512d632b7268ba958786ad2b6e3c8cae85eaec9fae
a19a4037df70ff896bbbf923b250098d78933af9ad77d1017d4f5b85e5a8b8fb
a1b2435d7cc11d738419b0d1b9a2c7d6b8c071f17ac08f6dce5eb85771dc624c

KPMG

KPMG Cyber Threat Intelligence Platform

Raspberry Robin – The new popular worm

Indicators of Compromise: Hashes
a43a2e2351b2087f48c52d33b18e6278bd50d8e64c18462335988300c27febb9
a5b7f672907cc9716d3ccc20f2c783fef110dd1a92f0c03acf1e6b7cab121e76
b09ed3931a6fbfa3a2bf701c92302e80f716f0c29384046b34b78429a5274c7d
b0b16fcec7631b087f7cd5965676a3ff39b9e29b3696454cbec489623da922de
b13823805b534d14f88fa2c017c469517e81d6aa19994ba432f683b1dc304d58
b4cb7640d4ecacaf554744229f5dd5d07fba70b72cc19d268b3fb70a7e4914a4
b59cbd494a290e3c98db577558c97071d2667ad414e77495e56132c4c5b81313
bad38e743708ea746930e8f4b6663a162add4503821d998a6049961e82c48250
bd6ddcecebe506a720c12191c0b06fc928cb04252b18c7ec27b0cd163cd5866f
c158550e9871f0337417ab19111f233fb4fa653f63ac184922d3eb6e3eb720f9
c45cb46b5b052459a4e8d93377f22c482eafe2930a18571c92b4970d7f31da23
c64878de9c1f1114988726b990e51e76a63d09773b67ac000918c7befd9fba9b
cc945f11956cb1c4a5c0cc80e4f49409976138816326bb13a2e65bf9e38c0d7c
cdb1485fc915ccc5359389f27780c8dce6e44e9c2623cf7ecf362d1ea13dd01d
d0e4b91971520c3aa4b92af5203627666cd83261f41dfb02f29371069d25de52
d41af31a3d833b8470bd2fac52c258ada62819cdf212bee1ae4168e100c9438d
d4bfc8c52f58dabc6c25d28142af9386f4b70f79dcc42518e00b114696ca57fb
e8ebd9b7bcf8bb42b910c9fd5b94f9ffa98399fe3d6a09c1490dacf2ae680270
edea13bf957e4c450c1028a1071fdbd9efeec94717c172260912eaf022d32621
f0a7fc685747beb21d9339aed02eb9f7ee85996d79d226858fea8c2f83af36cc
fc2fdacbbb116992dcd444cbc4c65179a33277ca588f02f9c696129ffe341b9e
fd843db504171aab5fbbc2955fda9471f726a4d006c28ad25174f729f4c8b874
c0a13af59e578b77e82fe0bc87301f93fc2ccf0adce450087121cb32f218092c