KPMG Cyber Threat Intelligence Platform

Remcos RAT - A Deceptive Remote Access Threat

Remcos RAT, initially marketed as a legitimate remote access tool since 2016, gained prominence during the COVID-19 pandemic, offering full remote access to compromised systems. The UAC-0050 threat group deployed Remcos RAT in their recent cyber intelligence operations against Ukrainian government agencies and has also been associated with a campaign targeting South Korean users through the Webhards, a popular online storage system, disguised as adult themed games.

Initial access is achieved through phishing emails containing a LNK (.lnk) file. The LNK file conceals an obfuscated URL string that, when de-obfuscated, is executed using MSHTA, directing to new-tech-savvy[.]com. The executed URL leads to 6.hta file, containing VBScripts with obfuscated content, which upon de-obfuscation initiates a PowerShell script that initializes Base64-encoded strings, creates an AES decryption object, decrypts and decompresses the payload, executing it as a new PowerShell process. The decrypted payload results in another PowerShell script, involving file path creation, file existence verification, and downloading additional payloads (word_update.exe, ofer.docx) from new-tech-savvy[.]com. Payloads are placed in the %appdata% directory and to establish persistence word_update.exe creates a self-copy file and a startup entry. Unusual resource data in the LNK file undergoes decryption through XOR operations. Post decryption, WriteFile API initiates transfer of data to an unnamed pipe, facilitating data exchange between word_update.exe and cmd.exe. The data in cmd.exe memory is decrypted during runtime, triggering the execution of the Remcos RAT.

The intricate chain showcases a comprehensive infiltration strategy with layers of obfuscation and payload deployment, emphasizing the need of enhanced cybersecurity protocols.

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 josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Remcos RAT - A Deceptive Remote Access Threat

Indicators of Compromise: IP Addresses	
5.42.92[.]31	45.87.154[.]153
141.95.84[.]40	141.95.16[.]111
139.28.36[.]84	74.119.194[.]217
45.87.155[.]41	103.169.35[.]140
46.249.58[.]40	94.131.102[.]119
101.99.75[.]16	94.131.102[.]115
103.110.32[.]7	94.131.102[.]124
194.87.31[.]229	94.131.102[.]122
101.99.75[.]145	94.131.102[.]117

Indicators of Compromise: Domains	
con-ip[.]com	generem.camdvr[.]org
new-tech-savvy[.]com	henderson1.camdvr[.]org

Indicators of Compromise: Hashes
56154fedaa70a3e58b7262b7c344d30a
9b777d69b018701ec5ad19ae3f06553f
74865c6c290488bd5552aa905c02666c
7c05cfed156f152139a6b1f0d48b5cc1
0b2d0eb5af93a3355244e1319e3de9da
b1f8484ee01a7730938210ea6e851888
7f87d36c989a11edf0de9af392891d89
f5ee6aa31c950dfe55972e50e02201d3
5c734bb1e41fab9c7b2dabd06e27bc7b
1c3e1e0319dc6aa24166d5e2aaaec675
818beece85ecd90d413782dd51d939b1
8158b43f745e0e7a519458b0150e1b61
f71ef85824f906856cb3d2205058bdd2
8bebea01d914a3c3a2d876417f7d1d54
4388789c81afd593c5fc2f0249502153
b28167faf2bcf0150d5e816346abb42d
450b6105389abfcbc35ca57cb1887c3e

KPMG

KPMG Cyber Threat Intelligence Platform

Remcos RAT - A Deceptive Remote Access Threat

Indicators of Compromise: Hashes
25fca21c810a8ffabf4fdf3b1755c73c
791545e6e3c5eb61dd12ccfbae1b9982
5379d703170770355efdbce86dcdb1d3
c54fea66c5150e6d924ca83f504c1aa4
0f085b3b449de9e8956360d83573e176
5f3e358fd5eb5839e4bb7a4d5e2f62af
94cf9d252151df6a337597bd01f02b92
4e7f8e9c3f6abff4f54007081b10aca5
1b1a1d6e59dd41e8854ce4ea80eb022f
c31f87fdf4a631180ed1bf137b6a2704
31ba4f7a41dda57b4d10ebbc020db9c17012f17c
f2d8bce46e8df36013b89e4de8bca66e3cf0de3e
1a05d4945350d06389a00f16fe72a0c149dd2bc4
a9bc862f7143a3e34ba420d624f81a9efd1516fc
8fc2d03837836d6a2e6d2bd0a18bbb9a1d65ba0c
4ab9c910cfc9690b7f54eba83e30bc1fe6984297
e644bc7774cfd1beecea50fb47b8ffd32b092c30
502bbd516526e579b2b0d0a5aaef0a66659e7fbb
1bee4d678beb8928377fbc112eade1af5ec30295
db3c330fcd97e0a983a13456e22f1b7f4982e5d6
757320c803fa55e7b44ac647fb340e1180ea6d93
09f678acd0ecb99e22e069661edf4fda8457e496
f20d2dcdd6303ed23bfe9dcffe3736a6de660a74
5089adac80acd2d36ad9cb1cce0e4a544474269e
ce1ce088c6bf640734870e9c318a4da58931a34a
3afff628e1bb841c4bb2fd04b6cdcb400c221736
225f3bc7017ce5e5464862ec9c864a11fedf1145
85afc4d1e65359e0a682878d55f4afcc51b070c2
7fdd801486d701ef0f97b4c91bcdd58ee294c593
c7aa25f2a1640e475be91e4bcb42ec7da6babfa6
93ac12eb3d7c3233e16e7862db99cfef00f17345
1a8a0e8c437d2110f12c5a51956154c41d6f6d6c
cdf707e2fa81364e6ba39da254ba52d4aa8c9468
18823a708aff6400ca742a5afab46dcf3cb5c0b4

KPMG

KPMG Cyber Threat Intelligence Platform

Remcos RAT - A Deceptive Remote Access Threat

Indicators of Compromise: Hashes
bd8af44e09a69fd3c4337d15baec09727a56c5fd
02b68e1f2b57c6f37e86dfa6aeaed9235514bf27
e54dbad1ea5d660ea2cff2610e7f623f482b8f11
f650a9f1930e55e405d7121c56b90a996ab213a05b772a8f02ceb1cdbeb91165
8963e1c87200d0b900f558c1968428dc3a1f05748ddeff0150297aa33d14ff88
fe128f5efc9be2d0b42653ed49937b18fca277b69d7c471cd351db37f8a8567d
e4615b74d62f384d23e58bc467c615b17779e4f8084c8a0134db97a5e642027f
88f0722c907100ef09049c82032a0ac66afa153d03fb89d378ae65f6e5890a3f
c5452b859922b9633839e092f09f0ce4818b6085043360c90c0b0f2bfad9fca1
5fff1cd29bb6e6cfe9516b70f9f44755098392c2e2a0f4784486182c309b2c99
bd871a2ccd6d7c4f89f9f5087e60cfdcc7ab35b670cfda7ddfd6dbbab8c8560c
8f157186dca8c21aeebd31a7253155728c51b239129768ee91df34dc693783f5
2daca1cab168a535027d3b08c5e1273bfd0fceddcbdf68cc7f5f62fd144aa1a6
378c219332e74786b5ce562d15a99fe021e47f1480be09b779db78ae87da9c26
3b78e6564c4774a6d3cd88c62e56c6705c2428e53cacb3a95713b8c399a7d7ad
ab310316f34881a67c6df912e646203adc676d1f53a5bf43873014dfdb0d68cf
4fa02ec602055dfbdb1d639b3d265d8f7b20d6cd328fdb62dd77b7a1aad5829a
c416d6ca4ee95a6647cc4357ba51a5e04a956b5a4ceaa74ad768fe544d706f48
2eecf5e7f48a7d84c212695f157295d060963470e4e0afab14eb2e491ae0f1d6
b7edc54e6b42ca1cda290ce8cacfecaac6dbcc8c14631bc20fb184a6309c1824
9d8282d54901d4e795f0469a5191242b2e7b3b0c51f810f71c739bfff52de8d5
aec8c11151af856a99824c579838163204c0519470a370a29fcddd5e21150223
e2c60159ad9908ac2a1ab446c1866dfe5a59b1535ca29f111ae56833996d82b8
9c579392d600eb07e19d7d4c7b0c485d5a9c0cdabdc66518ad4b10db7fca1eee
26cce78de160996f29caef74246d3ade256b1fe76e08d65ff726705e8bf3ec2b
d935d16b1603eb83d9c8587e3fe36ba247341adb572bac99a291f35bd13d7292
16bb974c71635d85ce58284f8e17291ac46bf7c2972e3235fcf60c1a1c0ed681
b765ff113cf1373281b31bc7ee1ad75af9607e7efe5b60af2fcc160f5b4344fd
5d57faeaf1e302117cf4121fd6a6f9e3391748f3afc8feabcb7b444c434b85e9
2f497ff3f27048054b345c0e177fc2365ad2b093490e1e980e7f475116cad26c
61ebcf7f2ea90a057a46e3fd4d9212063639b01b6e5e4c90ae3447b76f52e323
cb531e7d7523dcbf63b5307abcbca3fa5404defd476773af41e45200c7804035
7c680aa4e0b230ef2521b77ed67a20a3fb297fe36401f31d639258ec47eb77cc
6ecf9fda65dc1a4a9c7610510ac9f78a6663e75d736a8444c72e11a0cc8d8d46