

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 (.Ink) file. The LNK file conceals an obfuscated URL string that, when de-obfuscated, is executed using MSHTA, directing to new-techsavvy[.]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

Sony Anthony

Partner, KPMG in India T: +91 98455 65222 E: santhony@kpmg.com

Manish Tembhurkar Associate Partner,

KPMG in India T: +91 98181 99432 E: mtembhurkar@kpmg.com B V, Raghavendra Partner, KPMG in India T: +91 98455 45202 E: raghavendrabv@kpmg.com

Chandra Prakash

Partner, KPMG in India T: +91 99000 20190 E: chandraprakash@kpmg.com

#KPMG josh

home.kpma/in

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 ro 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 IL P, 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.







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	
<pre>con-ip[.]com</pre>	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





Remcos RAT - A Deceptive Remote Access Threat

25fca21c810a8ffabf4fdf3b1755c73c 7915456e63c5kb61d12ccfbae1b9982 5379d7031707703556fdbcc86dcdb1d3 5379d7031707703556fdbcc86dcdb1d3 6468c515b6c6d224ca83f59dc1aa4 96785358fd5bb839dbb73dd52cf52af 94cf9d252151df6a337597d01f02b92 94cf9d252151df6a337597b01f02b92 94cf9d252151df6a337597b01f02b92 94cf9d252151df6a337597b01f02b92 94cf9d252151df6a337597b01f02b92 94cf9d252151df6a337597b01f02b92 94cf9d252151df6a337597b01f02b92 94cf9d252151df6a337597bd01f02b92 94cf9d252151df6a337597bd01f02b92 94cf9d25451df6a37597bd01f02b92 91badf7a41da57bd01f02b92d9d52f 91badf7a41da57bd10ebbc92d9b9c17912f17c 92dbbc451652e617bd398e4d9f61f5f2a0c149dd2bc4 9abc862f7143383d8a26d2bd0a18bb59a1d65baac 94b9c90cfc690b7f54eba8283bc1fe6984297 6e44bc7774cf11beccea56f147b8ffd32b092c30 952bbd516526e579b2bd0d5aaef0a6659e7fbb 1bec4d678be1b9828377fbc112ca61af5ec30295 db3c330fcd97e0a983313456221b1b7f49825d6 75732c683fr4557b44ac647f3346ec64974 9689adc880c6bf647f358c64d6669a7d 5689adc880c6bf6487445898 9889adc80ac2d23b6edcf4fa358313a4a	Indicators of Compromise: Hashes
791545e6e3c5eb61dd12ccfbae1b982 53794783178778355e7dbce86dc4b1d3 c54fea66c5150e6d924ca83f50e4c1aa4 67883b3443de9e8955630ed33573c176 5f3e358fd5be58399e4bb7a4d5e2f62af 94cf9d252151df6a337597bd01f02b92 4e7f8e9c3f6abf4ff54007881b10aca5 1b1a1d6e59dd11e8854ce4ea80eb927f c31f87fdf4a631180ed1bf137b6a2704 31ba47ra41dda57bd10ebbc620db9c17012f17c f2d8bce46e8df36013b89edde8bca663cf0de3e a9bc862f7143a3e34b420d24f81a9efd1516fc 8fc208337385d6a3280e0f16fc72a0c119dd2bc4 a9bc862f7143a3e34b420d24f81a9efd1516fc 8fc2083837385d6a3280ef16fc72a0c149dd2bc4 a9bc862f7143a3e34b420d24f81a9efd1516fc 8fc208337385d6a3280ef16fc72a0c149dd2bc4 a9bc302fcf9090b7f54eba83e30bc1fe6984297 6c44bc777xfcfd1becce36fb47b8fc032b092c30 502bbd516526e579b2b0d0a5aaef0a6659e7fbb 1bee4d678beb8928377bc112eade1af5ec30295 db3c330fcd97e0a983a13456221h7f4982e5d6 57322c883635b2b14ac647fb34e923866 25732bc7017ce5e5464862ce9c864a11fedf1145 2688cbffc407a87ce9c31384d58391334a 3affff28e1bb841c4bb2fd04b6ccb40e221736 225f3bc7017ce5e5464862ce9c864a11fedf1145 858afc41e65359ea62878035ffa4cc51b07ec2	25fca21c810a8ffabf4fdf3b1755c73c
5379d703170770355efdbce86dcdb1d3 c54fea66c5150e6d924ca83f59dc1aa4 0f085b3b449e9e8956360d83573e176 5782358fd5eb5339e4bb7ad52cf2af 94cf9d252151df6a337597bd01f02b92 4z7f8e9c3f6abff4f54007081b10aca5 1b1ald6e59dd1e8854ce4ea80e022f c31f87fdf4a631180edbf137b6a2704 1abadf7a41da57bd10ebbc202db9c17012f17c f2d8bc468df36013b89edde8bca66e3cf0de3e 1ab6259dd1e8854ce4e30e022f f2d8bc4545350d60389a9df16fc72a0c149ddbc4 a9bc862f7143a384ba20d624f81a9ef1d516fc 8fc2d9a3738bc6a2ecdb20d9a18bb9a1d65ba8c 4ab9c910cfc9690b7f54eba83a9bc1fe6984297 e644bc777cfd1beecea59fb47b8ffd32b992c30 502bb51652ec579b2b00da5aaef0a6659e7fbb 1beedd678be8928377fbc112eade1affsc30295 1bead678be8928377fbc112eade1affsc30295 1bead678be8928377fbc12eade1affsc30295 1bead623bfe9dcffe3736ad6e60947 502bbc51652ec579b2b0da5aaef0a6659e7fbb 1bead623bfe9dcffe3736ad6e60947 502bbc51652ec579b2b0da5aaef0a6659e7fbb 1bead623bfe9dcffe3736ad6e6074 502bbc1652ec579b2b0da5aaef0a6659e7fbb 1ae5dc4d6a83dc2d36ad9cbc1ce0e4a544474269 ce1ce088c56f640734870ec213fad4a58313a3 225fbc70	791545e6e3c5eb61dd12ccfbae1b9982
c54fea66c5150e6d924ca83f504c1aa4 0f6853b1449dep885560d83573e176 5f3a538fd5eb53894bb7add5e2f62af 9dcf9d252151df6a337597bd1f62b92 4drf9de52151df6a337597bd1f62b92 1b1a1d6e59dd1e8854ce4ea80eb022f c31f87fdf4a631180ed1bf137b6a2704 31baf7a41dda57bd1febbc20db9c17012f17c f2d8bce46e8d736013b89ed4e8bca66e3cf0de3e aabc495350d6389a0bf16fe22ac149dd2bc4 a9bc862f7143a3e34ba420dc24f81a9efd1516fc 8fc2d8337836d6a2e6d2bd0a18bb9a1d65ba0c e644bc777dcf1becce36bf47b8ffd3b092230 502bd516526e579b2b0d0a5aaefa66659e7bb 1beedd678beb8928377bc112eade1af5ec30295 db3c330fcd97e0a983a13456e22f1b7f4982e5d6 757320c891555c9t4ac647b304e1180ead603 09f678acd0ecb99e22e60961edf4fda857e496 f2d02dcdd303ac23bfe0dcffe373a6de660a74 5089adac80acd2d36advb1cce0e4a54447269e ce1ce088c6bf640734870e9c318ada58931a34a 3afffd28e1bb8a1c4bb2fd4bdcdcbd0a0c21736 225f3bc7017ce5e54da68c53d555fafcc51b702C 7fdd8014e673b901e4db4b2e7da6b6c6ba7d 5089adac80acd2d36advb1cce0e4a54447269e ce1ce088c6bf640734870e9c318ada58931a34a 3afffc28e1bb841cdb2bd94bcdcbda0e221736 225f3bc7017ce5e54da68c631f6cf1145	5379d703170770355efdbce86dcdb1d3
0f085b3b449de9e8956360d83573e176 5f3e358fdseb5839e4bb7ad5e2f62af 94cf9d25151df6a337597bd01f02b92 4e7f8e9c3f6abff4f54007081b10aca5 1b1a1d6e590d41e8854ce4ea80eb02f c31f87fdf4a631180ed1bf137b6a2704 31ba47ra4td0a57b4d10eb0c20d0bsc17012f17c f2d8bce46e8d136013889a0ef16fe72a0c149dd2bc4 a9bc69c77143a2e3dba420d624f81a9efd1516fc 8fc2d03837836d6a2e6d2bd0a18bbb9a1d65ba0c 4a9bc910efc69609b7f54eba83e30bc1fe6984297 e644bc7774cfd1beceas0fb47b8ffd32b09c30 9b2bb3165266579b2b0d0a5aaef0a66659c7fbb 1bee4d678beb822837fbc112eade1af5ec30295 db3c330fcd97e0a983a1345se22f1b7f4982e5d6 757320c803fa5s5rb44ac6d7fb30e1180ea6d93 09f678ac0decb99e22e6096fb14f4a8457e496 c2e1ce088c6bf640734870e9c318a4da58931a34a 3afff628e1bb841c4bb2fd4b4bcc4b40e221736 22sfbc7017ce5e544462ec9c86a411fc1145 85afc4d1e63359e0a682878d55fafcc51b070c2 7fdd801486d701ef6f75Ac91bcdb8e292c93 c1ce088c6bf640734870e9c318a4da58931a34a 3afff628e1bb841-c4b2b7db4bccdb400c21736 22sfbc7017ce5e5446462ec9c86a411fc51b070c2 7fdd801486d701ef6f75Ac91bcd58e294553 c1ce088c6bf640734870e9c318a4da58931a34a 3afff628e1bb8	c54fea66c5150e6d924ca83f504c1aa4
5f3e358fdseb5839e4bb7a4d5e2f62af 94cf9d252151df6a337597bd01f02b92 4e7f8e9c3f6abff4f54007081b10aca5 1b1a1d659dd41e8854ce4e380eb022f c31f87fdf4a631180ed1bf137b6a2704 31ba4f7a41da57bd10ebbc020db9c17012f17c f2d8bce46e8df36013b89e4de8bca66e3cf0de3e 1ao5d3943538d63289a0ef16fc72aoc149dd2bc4 a9bc62f7143a3e3dba2ded281a9efd15l5fc 8fc2d93837836d6a2e6d2bd0a18bbb91d65ba0c e644bc7774cfd1beecea50fb47b8ffd32b092c30 9b2bd516526e579b2b0d0a5aaef0a66659e7fbb 1bee4d678be8928377bc112eade1af5ec30295 db3c39fcd97e0a983a13456e22f1b7f948e25d6 757320c803fa55e7b44ac647fb340e1180ea6d33 09f678ac.d0ecb99e22e609661edf4fda8457e496 f2d02dcd6303ed23bfe9dcffe37366de660a74 5089badc 80ecd2d36ad9cb1cce0e4a544474269e ce1ce088cbf640734870e9c318a4da5893134a 3afffc828e1b841c4bb2fd04b6ccb400c221736 235f3c7017ce5e5464862e9246538134a 235f3c7017ce5e5464862e924c519870e2 7fdd801486d701ef077bc21bcd58e294c593 c7aa25f2a1640e475be91e4bcd2e7da6baf66 7ja22f2a1640e475be91e4bcd2e7da6baf66 7ja22f2a1640e475be91e4bcd2e7da6baf66 7ja22f2a1640e475be91e4bcd2e7da6baf66 7ja22f2a1640e475be91e4bcd2e7da6	0f085b3b449de9e8956360d83573e176
94cf9d252151df6a337597bd01f92b92 4c7f8e9c3f6abff4f54007081b10aca5 1b1a1d6e59dd188854ce4ea80eb022f c31f87fdf4a631180ed1bf137b6a2704 31ba4f7a41dd357bd10ebbc020db9c7012f17c f2d8bce4e8df36013809e4de8bca6663cf0de3e 1ao5d4945350d6389a0ef16fe72ac149dd2bc4 a9bc862f7143a3e34ba420d24f81a9efd1516fc 8fc2d03837836d6a2e6d2bd0a18bb9a1d65ba0c 4ab9c910cfc9690b7f54eba83e30bc1fe6984297 e644bc7774cfd1beceas0fb47b8ffd32b09c30 9b2bb616526579bb20d0a5aer60a6659e7fbb 1bee4d678beb8928377bc112eade1af5ec3025 db3c339fcd97ea093813456e221b7f4982e5d6 757320c803fa55e7b44ac647fb340e1180ea6d93 09f678acd0ecb99e22e069661edf4fd8457e496 f2d02dcd383eacd23bfe9dcfe69331a3a 3afffc28eb882837fbc112eade1af5ec30275 264bc77417ce5e5464862ec9c84a11edf1145 858afc4d1e65359e0a682878d55fa4cc51b070c2 7frd8801486d701ef6f97b4c91bcd38ee294c593 c1ce088c6bf40733810e9c1ef600f17345 203c2b1632a642c303e1e2e7dc3be3e24de3bfa6 7jac12e3d7c323a1e6786cb99cfe00f17345 13a80e8c437d2110f12c53155614d16f66c c1cr088c6457d2112e12c5155614d16f66c c1d770z2fa81564e0a32da254ba52d4aa8c9468 1a8a0e8c437d2110ef12c5315565	5f3e358fd5eb5839e4bb7a4d5e2f62af
4e7f8e9c3f6abff4f54007081b10aca5 1b1a1d6e59dd41e8854ce4ea80e022f c31f87fdf4a631180ed1bf137b6a2704 31ba47a41dda57b4d10ebbc020db9c17012f17c f2d8bce46e8df36013b89edde8bca6663cf0de3e 1a05d4943550d063389a00f16fe72a0c149dd2bc4 a9bc862f7143a3e34ba420d624f81a9efd1516fc 8fc2d0337836d6a2e6d2bd0a18bb9a1d65ba0c 4ab9c910cfc9699b7f54eba83e30bc1fe6984297 e644bc7774cfd1beece369fb47b8ffd32b092c30 502bb516526e579b2b0d0a5aaef0a6659e7fbb 1bee4d678be8923377fbc112eade1af5cc30295 db3c339fcd97e0a983313456e22f1b7f4982e5d6 757320c803fa55e7b44ac647 fb340e1180ea6d93 09f678acd0ecb99e22e069661edf4fda8457e496 f2d02dcd5a30ed2bte9dcffe3736a6de60a74 508badac80acd2306ed9ct1cce0e4a54474269e ce1ce088c6ff640734870e9c318a4d58931334a 225f3bc7017ce5e546482ce2c8de411fedf1145 825afc4d1e65359e0a682878d55fa4cc51b070c2 7fdd801486d701ef0f7b4c91bcd58ee294c593 cfaa25f2a1640e475be91e4bc42e7da6baffa6 93ac12eb3d7c3231e16e786c4099ceff00f17345 1a8a0e8c437d2110f12c531596154c41d6f6d6c cd7707c2fa18a164e6b33da254ba52d4a82468 1a8a0e8c437d2110f12c531596154c416f6d6c cd7707c2fa18a164e6c33ba2a54ba52d4a82468	94cf9d252151df6a337597bd01f02b92
1b1a1d6e59dd41e8854ce4ea80eb022f c31f87fdf4a631180ed1bf137b6a2704 31ba4f7a41dda57b4d10ebbc020db9c17012f17c f2d8bce46e8df36013b89ed4e8bca66e3cf0de3e 1a05d4945350d06389.a00f16fe72a0c149dd2bc4 a9bc862f7143a3e3dba2d2d2df81a9efd1516fc 86c2d03837836Ga2e6d2bd0a18bb9a1d65ba0c 4ab9c910cfc969007f54eba33e30bc1fe6984297 e644bc7774cfd1becea50fb47b8ffd32b092c30 502bbd516526e579b2bd0d5aaef0a6659e7fbb 1bee4d678beb8928377fbc112eade1af5ec30295 db3c330fcd97e0a983a13456e22f1b744982e5d6 757320c803fa55rb44ac647fb340e1180ea6d33 09f678acd0ecb9922e069661edf4fda8457e496 celce088c6bf640734870e9c318ad43893134a 3afff628e1bb841c4bb2fd04b6cdcb400c221736 225f3bc7017ce5e5464862e9c864a11fedf1145 883afc4d1e65359e0a682878d55f4afcc51b070c2 7fda801486d701ef6795Acc91bcdd58ec294c593 c7aa25f2a1640e475be91e4bc4b2c7da6bafa6 93ac12eb3d7c323216e78620b99c1ef00f17345 1a8a0e8c43720110f12c5a51956154c41def66dc c4770rc2r481354e6ba39d2254a824548 1a88028a7708aff6400cr342a5af20468 1a8282a708aff6400cr342a5af20456	4e7f8e9c3f6abff4f54007081b10aca5
c31f87fdf4a631180ed1bf137b6a2704 31ba4f7a41dda57b4d10ebbc020db9c17012f17c f2d8bce46e8df36013b89ed48bca66e3cf0de3e 1a05d4945350d06389a00f16f72a0c149dd2bc4 a9bc862f7143a3e3dba420d624f81a9efd1516fc 8fc2d03837836d6a2e6d2bd0a18bb9a1d65ba0c 4ab9c910cfc969007f54eba83e30bc1fe6984297 e644bc7774cfd1beccea50fb47b8ffd32b09230 502bbd516526e579b2b0d0a5aaef0a6659e7fbb 1bee4d678beb8928377fbc112eade1af5ec30295 db3c330fcd97e0a983a13456e22f1b7f4982e5d6 757320c803fa55c7b44ac647fb340e1180ead93 09f678acd0ecb9922e069661edf4fda845re496 6989adc80acd236ad9cb1cce0e4a544474269e ce1ce088c6bf640734870e9c38ada4589313a4a 3afff628e1bb841c4bb2fd04b6cdcb400c221736 225f3bc7017cc5s464862e9c864a11fedf1145 85afc4d1e65359e0a682878d55f4afcc51b070c2 7fdd801486d701ef697b4c31bcdd58e294c593 c7aa2sf2a1640e475be91e4bc4b2c7da6babfa6 93ac12eb3d7c32331e6c7862d99cfef00f17345 1a8a0e8c437d2110f12c5a51596154c41d6f6d6c c47707c2fa131364ec5ba39c24ba52daa8c9468 1a8823a708aff6400cr34za5a4ba52daa8c9468	1b1a1d6e59dd41e8854ce4ea80eb022f
31ba4f7a41dda57b4d10ebbc020db9c17012f17c f2d8bce46e8df36013b89e4de8bca66e3cf0de3e 1a05d4945350d06389a00f16fe72a0c149dd2bc4 a9bc862f7143a3e34ba420d624f81a9efd1516fc 8fc2d03837836d6a2e6d2bd0a18bbb9a1d65ba0c 4ab9c910cfc9690b7f54eba83e30bc1fe6984297 e644bc7774cfd1becea50fb47b8ffd32b092c30 502bb516526e579b2b0d0a5aaef0a66659e7fbb 1bee4d678beb8928377fbc112eade1af5ec30295 db3c330fcd97e0a98a13456e22f1b7f4982e5d6 75732c803fa55e7b44ac647fb340e1180ea6d93 09f678acd0ecb99e22e069661edf4fda8457e496 f20d2dcdd6303ed23bfe9dcffe3736a6de660a74 5089adac80acd2d36ad9cb1cce0e4a544474269e ce1ce088c6bf640734870e9c318a4da58931a34a 3afff628e1bb841c4bb2fddb4bcdcb400c221736 225f3bc7017ce5e5464862ec9c864a11fedf1145 85arc4d1e6539e0a682878d55f4afcc51b070c2 7fdd801486d701ef0f97bc491bcd58ee294c593 c7aa25f2a1640e475be91e4bc42c7da6babfa6 93ac12eb3d7c3233e16e7862db99ccfe600f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707c2fa81364e6ba39da254ba52d4a829468 18823a708aff6400ca742a5afab46cf3cb5c0b4	c31f87fdf4a631180ed1bf137b6a2704
f2d8bce46e8df36013b89e4de8bca66e3cf0de3e la05d4945350d06389a00f16fe72a0c149dd2bc4 a9bc862f7143a3e3dba420d624f81a9efd1516fc B#c2d03837836d6a2e6d2bd0a18bbb9a1d65ba0c 4ab9c910cfc9690b7f54eba83e30bc1fe6984297 e644bc7774cfd1beecea50fb47b8ffd32b092c30 502bbd516526e579b2b0d0a5aaef0a66659e7fbb 1bee4d678beb8928377bc112eade1af5ec30295 db3c330fcd97e0a983a13456e22f1b7f4982e5d6 75732c803fa55e7b44ac647fb340e1180ea6d33 09f678acd0ecb99e22e069661edf4fda8457e496 f20d2dcdd630aed23bfe9dcffe3736a6de66074 5089adac80acd2d36ad9cb1cce0e4a544474269 ce1ce088c6bf640734870e9c318a4da58931a34a 3afff628e1bb841c4bb2fddb4b6cdcb400c221736 225f3bc7017ce5e5464862ec9c864a11fedf1145 85arc4d1e65359e0a682878d55f4afcc51b070c2 7fd801486d701ef0f97bc91bcd58e294c593 c7aa25f2a1640e475be91e4bc42c7a66bafa6 93ac12e337c3233e16a7862db99cfef00f17345 1a8a0e8c4372d110f12c5a51956154c41def6d6c cdf707c2fa81364e6ba39ad23bab22daa829468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	31ba4f7a41dda57b4d10ebbc020db9c17012f17c
1a05d4945350d06389.a00f16fe72a0c149dd2bc4 a9bc862f7143a3e34ba420d624f81a9efd1516fc 8fc2d03837836d6a2e6d2bd0a18bb99a1d65ba0c 4ab9c910cfc9690b7f54eba83e30bc1fe6984297 e644bc7774cfd1beecea50fb47b8ffd32b092c30 582bbd516526e579b2b0d0a5aaef0a66659e7fbb 1bee4d678beb8928377fbc112eade1af5ec30295 db3c330fcd97e0a983a13456e22f1b7f4982e5d6 757320c803fa55e7b44ac647fb340e1180ea6d93 09f678acd0ecb99e22e069661edf4fd3457e496 f20ddcdd630aec03b fe9dcffe3736ade660a74 5089adac80acd236ad9cb1cce0e4a544474269e ce1ce088c6bf640734870e9c318a4da58931a34a 3afff628e1bb841c4bb2fd04b6ccb400c221736 225f3bc7017ce5e5464862ec9c864a11fedf1145 85afc4d1e65359e0a682878d55fa4cfc1b070c2 7fd801486d701ef0f97b4c91bcd58ee294c593 cfaa25f2a1640e475be91e4bcb42ec7da6babfa6 93ac12e3047c323e16e7862db99cfef00f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707c2fa81364e6ba39da254ba52d4aa8c9468	f2d8bce46e8df36013b89e4de8bca66e3cf0de3e
a9bc862f7143a3e34ba420d624f81a9efd1516fc 8fc2d03837836d6a2e6d2bd0a18bbb9a1d65ba0c 4abpc910cfc9690b7f54eba83e30bc1fe6984297 e644bc7774cfd1beecea50fb47b8ffd32b092c30 502bbd516526e579b2b0d0a5aaef0a66659e7fbb 1bee4d678beb8928377fbc112eade1af5ec30295 db3c330fcd97e0a983a13456e22f1b7f4982e5d6 757320c803fa55e7b44ac647fb340e1180ea6d93 09f678acd0ecb99e22e069661edf4fda8457e496 f20d2dcdd630ad23bfe9dcffe37366de660a74 508badac80acd236ad9cb1cce0e4a544474269e ce1ce088c6bf640734870e9c318a4da58931a34a 3afff628e1bb841c4bb2fd04b6dcb400c221736 22553bc7017ce5e5464862ec9c864a11fedf1145 85afc4d1e65359e0a682878d55f4afcc51b070c2 7fd8041486d701ef697b4c91bcd58ee294c593 cfaa25f2a1640e475be91e4bcb42ec7da6bafa6 93ac12eb3d7c3233e1ee7862db99cfef00f17345 18828ec437d2110f12c5s1956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4a8c9468 18823a708aff6400ca742a5afab46cdf3cb5c0b4	1a05d4945350d06389a00f16fe72a0c149dd2bc4
8fc2d03837836d6a2e6d2bd0a18bbb9a1d65ba0c 4ab9c910cfc9690b7f54eba83e30bc1fe6984297 e644bc7774cfd1beccea50fb47b8ffd32b092c30 502bbd516526e579b2b0d0a5aaef0a6659e7fbb 1bee4d678beb8928377fbc112eade1af5ec30295 db3c330fcd97e0a983a13456e22f1b7f4982e5d6 757320c803fa55e7b44ac647fb340e1180ea6d93 09f678acd0ecb99e22e069661edf4fda8457e496 f20d2dcdd6303ed23bfe9dcffe3736a6de660a74 5089adac80acd2d36ad9cb1cce0e4a544474269e ce1ce088c6bf640734870e9c318a4da58931a34a 3afff628e1bb841c4bb2fd04b6cdcb400c221736 225f3bc7017ce5e5464862ec9c864a11fedf1145 85afc4d1e653590a682878d55f4afcc51b070c2 7fdd801486d701ef0f97b4c91bcd58ee294c593 c7aa25f2a1640e475be91e4bcb42ec7da6babfa6 93ac12eb3d7c3233e16e7862db99cfef00f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6dcc cdf707e2fa81364ecba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	a9bc862f7143a3e34ba420d624f81a9efd1516fc
4abbc910cfc9690b7f54eba83e30bc1fe6984297 e644bc7774cfd1becce369fb47b8ffd32b092c30 502bbd516526e579b2b0d0a5aaef0a666997fbb 1bee4d678beb8928377fbc112eade1af5cc30295 db3c330fcd97e0a983a13456e22f1b7f4982e5d6 757320c803fa55e7b44ac647fb340e1180ea6d93 09f678acd0ecb99e22e069661edf4fda8457e496 f20d2dcdd630aed23bfe9dcffe3736a6de660a74 5089adac80acd2d36ad9cb1cce0e4a544474269e ce1ce088c6bf640734870e9c318a4da58931a34a 3afff628e1bb841c4bb2fd04b6cdcb400c221736 225f3bc7017ce5e5464862ec9c864a11fedf1145 85afc4d1e65359e0a682878d55fa4fcc51b070c2 7fdd801486d701ef0f97b4c91bcdd58ee294c593 c7aa25f2a1640e475be91e4bcb42ec7da6babfa6 93ac12eb3d7c3233e16e7862db99cfef00f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	8fc2d03837836d6a2e6d2bd0a18bbb9a1d65ba0c
e644bc7774cfd1beecea50fb47b8ffd32b092c30 502bbd516526e579b2b0d0a5aaef0a66659e7fbb 1bee4d678beb8928377fbc112eade1af5ec30295 db3c330fcd97e0a983a13456e22f1b7f4982e5d6 757320c803fa55e7b44ac647fb340e1180ea6d93 09f678acd0ecb99e22e069661edf4fda8457e496 f20d2dcdd6303ed23bfe9dcffe3736a6de660a74 5089adac80acd2d36ad9cb1cce0e4a544474269e ce1ce088c6bf640734870e9c318a4da58931a34a 3afff628e1bb841c4bb2fd04b6cdcb400c221736 225f3bc7017ce5e5464862ec9c864a11fedf1145 85afc4d1e65359e0a682878d55f4afcc51b070c2 7fdd801486d701ef6f97b4c91bcdd58ee294c593 c7aa25f2a1640e475be91e4bcb42ec7da6babfa6 93ac12eb3d7c3233e16e7862db99cfef00f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	4ab9c910cfc9690b7f54eba83e30bc1fe6984297
502bbd516526e579b2b0d0a5aaef0a66659e7fbb 1bee4d678beb8928377fbc112eade1af5ec30295 db3c330fcd97e0a983a13456e22f1b7f4982e5d6 757320c803fa55e7b44ac647fb340e1180ea6d93 09f678acd0ecb99e22e069661edf4fda8457e496 f20d2dcdd6303ed23bfe9dcffe3736a6de660a74 5089adac80acd2d36ad9cb1cce0e4a544474269e ce1ce088c6bf640734870e9c318a4da58931a34a 3afff628e1bb841c4bb2fd04b6cdcb400c221736 225f3bc7017ce5e5464862ec9c864a11fedf1145 85afc4d1e65339e0a682878d55f4afcc51b070c2 7fdd801486d701ef097b4c91bcdd58e294c593 c7aa25f2a1640e475be91e4bc42ec7da6babfa6 93ac12eb3d7c3233e16e7862db99cfef00f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	e644bc7774cfd1beecea50fb47b8ffd32b092c30
1bee4d678beb8928377fbc112eade1af5ec30295 db3c330fcd97e0a983a13456e22f1b7f4982e5d6 757320c803fa55e7b44ac647fb340e1180ea6d93 09f678acd0ecb99e22e069661edf4fda8457e496 f20d2dcdd630aed23bfe9dcffe3736a6de660a74 5089adac80acd236ad9cb1cce0e4a544474269e ce1ce088c6bf640734870e9c318a4da58931a34a 3afff628e1bb841c4bb2fd04b6cdcb400c221736 225f3bc7017ce5e5464862ec9c864a11fedf1145 85afc4d1e65359e0a682878d55f4afcc51b070c2 7fdd801486d701ef0f97b4c91bcdd58ee294c593 c7aa25f2a1640e475be91e4bcb42ec7da6babfa6 93ac12eb3d7c3233e16e7862db99cfef00f17345 1880e8c437d2110f12c5a51956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	502bbd516526e579b2b0d0a5aaef0a66659e7fbb
db3c330fcd97e0a983a13456e22f1b7f4982e5d6 757320c803fa55c7b44ac647fb340e1180ea6d93 09f678acd0ecb99e22e069661edf4fda8457e496 f20d2dcdd630aed23bfe9dcffe3736a6de660a74 5089adac80acd2d36ad9cb1cce0e4a544474269e ce1ce088c6bf640734870e9c318a4da58931a34a 3afff628e1bb841c4bb2fd04b6cdcb400c221736 225f3bc7017ce5e5464862e9c864a11fedf1145 85afc4d1e65359e0a682878d55f4afcc51b070c2 7fdd801486d701ef6f97b4c91bcdd58ee294c593 c7aa25f2a1640e475be91e4bcb42ec7da6babfa6 93ac12eb3d7c3233e16e7862db99cfef00f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab4dcf3cb5c0b4	1bee4d678beb8928377fbc112eade1af5ec30295
757320c803fa55e7b44ac647fb340e1180ea6d93 09f678acd0ecb99e22e069661edf4fda8457e496 f20d2dcd6303ed23bfe9dcffe3736a6de660a74 5089adac80acd2d36ad9cb1cce0e4a544474269e ce1ce088c6bf640734870e9c318a4da58931a34a 3afff628e1bb841c4bb2fd04b6cdcb400c221736 225f3bc7017ce5e5464862ec9c864a11fedf1145 85afc4d1e65359e0a682878d55f4afcc51b070c2 7fdd801486d701ef0f97b4c91bcdd58ee294c593 c7aa25f2a1640e475be91e4bcb42ec7da6babfa6 93ac12eb3d7c3233e16e7862db99cfef00f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	db3c330fcd97e0a983a13456e22f1b7f4982e5d6
09f678ac d0ecb99e22 e06966 1edf4 fda8457e496 f20d2dcdd6303 ed23b fe9dcffe3736a6de 660a74 5089adac 80acd2d36ad9cb1c ce0e4a544474269e ce1ce088 c6bf640734870e9c 318a4da58931a34a 3afff628 e1bb841c4bb2fd04b6cdcb400c 221736 225f3bc7017ce5e5464862ec9c864a11fedf1145 85afc4d1e65359e0a682878d55f4afcc51b070c2 7fdd801486d701ef6f97b4c91bcdd58ee294c593 c7aa25f2a1640e475be91e4bcb42ec7da6babfa6 93ac12eb3d7c3233e16e7862db99c fef00f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	757320c803fa55e7b44ac647fb340e1180ea6d93
f20d2dcdd6303ed23bfe9dcffe3736a6de660a745089adac80acd2d36ad9cb1cce0e4a544474269ece1ce088c6bf640734870e9c318a4da58931a34a3afff628e1bb841c4bb2fd04b6cdcb400c221736225f3bc7017ce5e5464862ec9c864a11fedf114585afc4d1e65359e0a682878d55f4afcc51b070c27fdd801486d701ef0f97b4c91bcdd58ee294c593c7aa25f2a1640e475be91e4bcb42ec7da6babfa693ac12eb3d7c3233e16e7862db99cfef00f173451a8a0e8c437d2110f12c5a51956154c41d6f6d6ccdf707e2fa81364e6ba39da254ba52d4aa8c946818823a708aff6400ca742a5afab46dcf3cb5c0b4	09f678acd0ecb99e22e069661edf4fda8457e496
5089adac 80acd 2d36a d9cb1c ce0e4a 544474269e ce1ce088 c6bf640734870e9c 318a4da58931a34a 3afff628 e1bb841c4bb2fd04b6cdcb400c 221736 225f3bc7017ce5e5464862ec 9c864a11fedf1145 85afc4d1e65359e0a682878d55f4afcc51b070c2 7fdd801486d701ef0f97b4c91bcdd58ec294c593 c7aa25f2a1640e475be91e4bcb42ec7da6babfa6 93ac12eb3d7c3233e16e7862db99cfef00f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	f20d2dcdd6303ed23bfe9dcffe3736a6de660a74
ce1ce088c6bf640734870e9c318a4da58931a34a 3afff628e1bb841c4bb2fd04b6cdcb400c221736 225f3bc7017ce5e5464862ec9c864a11fedf1145 85afc4d1e65359e0a682878d55f4afcc51b070c2 7fdd801486d701ef0f97b4c91bcdd58ee294c593 c7aa25f2a1640e475be91e4bcb42ec7da6babfa6 93ac12eb3d7c3233e16e7862db99cfef00f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	5089adac80acd2d36ad9cb1cce0e4a544474269e
3afff628e1bb841c4bb2fd04b6cdcb400c221736 225f3bc7017ce5e5464862ec9c864a11fedf1145 85afc4d1e65359e0a682878d55f4afcc51b070c2 7fdd801486d701ef0f97b4c91bcdd58ee294c593 c7aa25f2a1640e475be91e4bcb42ec7da6babfa6 93ac12eb3d7c3233e16e7862db99cfef00f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	ce1ce088c6bf640734870e9c318a4da58931a34a
225f3bc7017ce5e5464862ec9c864a11fedf1145 85afc4d1e65359e0a682878d55f4afcc51b070c2 7fdd801486d701ef0f97b4c91bcdd58ee294c593 c7aa25f2a1640e475be91e4bcb42ec7da6babfa6 93ac12eb3d7c3233e16e7862db99cfef00f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	3afff628e1bb841c4bb2fd04b6cdcb400c221736
85afc4d1e65359e0a682878d55f4afcc51b070c2 7fdd801486d701ef0f97b4c91bcdd58ee294c593 c7aa25f2a1640e475be91e4bcb42ec7da6babfa6 93ac12eb3d7c3233e16e7862db99cfef00f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	225f3bc7017ce5e5464862ec9c864a11fedf1145
7fdd801486d701ef0f97b4c91bcdd58ee294c593 c7aa25f2a1640e475be91e4bcb42ec7da6babfa6 93ac12eb3d7c3233e16e7862db99cfef00f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	85afc4d1e65359e0a682878d55f4afcc51b070c2
c7aa25f2a1640e475be91e4bcb42ec7da6babfa6 93ac12eb3d7c3233e16e7862db99cfef00f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	7fdd801486d701ef0f97b4c91bcdd58ee294c593
93ac12eb3d7c3233e16e7862db99cfef00f17345 1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	c7aa25f2a1640e475be91e4bcb42ec7da6babfa6
1a8a0e8c437d2110f12c5a51956154c41d6f6d6c cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	93ac12eb3d7c3233e16e7862db99cfef00f17345
cdf707e2fa81364e6ba39da254ba52d4aa8c9468 18823a708aff6400ca742a5afab46dcf3cb5c0b4	1a8a0e8c437d2110f12c5a51956154c41d6f6d6c
18823a708aff6400ca742a5afab46dcf3cb5c0b4	cdf707e2fa81364e6ba39da254ba52d4aa8c9468
	18823a708aff6400ca742a5afab46dcf3cb5c0b4



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