KPMG Cyber Threat Intelligence Platform

DragonRank Group - Disrupting IIS Servers and SEO Integrity

TLP : Clear

KPMG. Make the Difference.

DragonRank is a newly identified Chinese-origin threat actor that targets web application services and IIS servers to manipulate search engine rankings. Unlike typical black hat SEO groups, DragonRank focuses on lateral movement and privilege escalation to sustain control over various servers within a target's network. They target sectors such as jewelry, media, healthcare, manufacturing, and IT services across countries in Asia and Europe.

Initial access is achieved through vulnerabilities in web applications like phpMyAdmin and WordPress, deploying the ASPXspy web shell on compromised servers for initial control. Web shells collect system details and map networks, using tools like Mimikatz, PrintNotifyPotato, BadPotato, and GodPotato for credential harvesting. Lateral movement within the network exploits compromised credentials via RDP, targeting additional Windows IIS servers, deploying web shells, and installing malware like PlugX and BadIIS. Administrator permissions are cloned to guest accounts for elevation to admin levels, creating hidden admin accounts like "admin$" for persistence, which are later deleted. Compromised servers are re-engaged to verify operational status and maintain access, re-downloading web shells and managing admin accounts. File concealment techniques hide malware by placing BadIIS in directories like Kaspersky SDK, using PDB strings to disguise it, and modifying file attributes to evade detection. PlugX and other tools are utilized for C2 communication and RDP is disabled and re-enabled to maintain access and cover signs of tampering. Search engine algorithms are manipulated to improve website rankings, using BadIIS to alter HTTP responses, perform SEO fraud, and proxy malicious communications.

DragonRank poses a serious threat by compromising IIS servers, necessitating strong security measures to mitigate their impact on SEO rankings and companies' online presence.

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.

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

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

Atul Gupta
Partner
Head of Cyber Security
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

DragonRank Group - Disrupting IIS Servers and SEO Integrity

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses

154.23.179[.]133	202.162.108[.]48

Indicators of Compromise: Domains

ig26[.]com	googie[.]pw
yx52[.]pw	tttseo[.]com

Indicators of Compromise: Hashes

e9194bd20e9bd6f6f5e572796514b285
7d8c5f7d684971923fc11d0033bef90d
7968fb0f54637e2fa745ed5410fc6886
39cf482fd20594170458a58b97f1e37c
12d03e7790a534a20984ffcef967b261
07b2dd4a339e7ba579362de606dc9411
a17ea49b998508ef9be7a087c33784bc
8dc8cd05a1a8edc53b6ef7779751bfc2
4d0e8e3c38d77f80519e4a46a5a6c389
7eb4d7409446cc974ab4a62bc9a5fdf7
b5848af3dae4370928e3adc091facbc2
405f2150c05814ffbcf6f2308263707d
9d56ce6db4868af796fd82f01b3fe6ef
fae95f61b4970c3769b7d8dffcc1b8dd
f9b7a389f995c7f01c37351afc457fa4
fd24ad0498a206d322bf7605d13be1bf
8f862493f30b97f2c7af34bf50f9ef90
b779d9efc1e00e2626e9942d9a065666

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

DragonRank Group - Disrupting IIS Servers and SEO Integrity

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
a043443af3021d1f6b58ce87ba264f4d
7a47f695a09ff82968144858f228cd67
9363fa01a791889ec72655717edee6c2
43e00adbbc09e4b65f09e81e5bd2b716579a6a61
ab7ebc82930e69621d9bccb6698928f4a3719d29
8b921434de690d153c4c4cdf21d390fc85f0d4f0
4fcb63093b555fe8d4cec443918d54eca3e01e60
76f71a7c14efaa957d945aeeea130e64ef31390e
1ea91cb532dcfc55e1c4c62a62c0ccb97627d924
2d0051751af7992778e0c3cac90b1e6bea9272ca
9eccf2e0ab48f799aecd5ebe227d86a7723dcca3
695ed42d15d7bb33a5f4f7c0f93908f97be14d0a
06b817c357b92d16a73882c58d8aaa8d7a138407
b45bdcb0d520ffcf2b00771f2c2494cb769d8dba
2e920b393414bfa4f7b25dc5e6ab002e4d3dd770
277ebe24bdba5cd7e4fd5e769c4c858b14bc3ab5
44ad2555303af3184d956333dca10bd389476a6e
9c99eb8a248166fe119fb290d29987c7cc7648ca
b0e9138bb825e8cc77e36ea80d103821dd2d4c3f
e07de140c0d0fd67fca697484f80c2ae9934884b
d2d18a6944fc74830e10fe4d14738d360c882d4d
cc6ce468c8eb8e272a5a7b2c1a15c7b910f36c74
8e4e562f67c66ca2497604cee8938070039c5ac7
261efa49c5f2252ea206d3ceea1bd773528066b0
620ea476fef24d51e0f47acaec4cf2084203cfcf
01829f674d3dabcb8fcaedaa61eafcbba7f42afa

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

DragonRank Group - Disrupting IIS Servers and SEO Integrity

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
31dff8d7ec666b24bc953cacfa32d751c7469387
322d9277f54f1b82ac616bfc1432848db1fd2d9c
3807a5c7d938b50b8542d2700a62d289079e7bbf
cc5498e6558af137d85e91acea2a72ef59e8a00c
b792e6758eb45c4fb9db163c8f406aa46257139c
5e80353459a921bfbf5a77488e43eb45fd1e7ea1
c574a9ab7ce1eb160ae160c6bd8c4d16d3da7183
72fc4ba4d8e9a7b11fa0b76611e85b7aaf3558ac08dc8e9628fad48d72fb8190
9277f848a5348e447e02cf94beae392815a235264443fdd69a3ff6eb48f040a8
614920f1a8550070a983f2ad22d6358c6742a9e02802b025eeea8db8c3d41fb7
6422684371fabf8a2ceaf06146d0a11d2c3c79647700c61f55e4af095a8360a4
3f17c66aab154212fb02fc7e329296c233aebe4abd9248204fa99c490c113a6e
8251189e8b596743683f2ab2d731eb19efe3e4e28ac5c100ea88cfdc36aeeac8
875239000f22cff75f62f9a1aa9924a8c3fea72124b0c4b31c7b3814f9dc0601
c41587c393741e78b678f1fc3d7934859a306c4cc4c0b02ca08d596289caeff4
cdc9f18de75991e7b289ab26b32dca9f4de6f95f88a6d3d32c87a111c4dc4d18
6e5eb43b81f103e4926be92d6bef9048bfa042bddb95a1ad3245230df0e04d22
7dd1307fd65599600a5056ae867c373333ae265f6fa29dc02ec697916159ed84
373d95685d0fd184aa4d5e47f7b1eb1848badef4fc9db46415f858f37eb20eee
839b8532681df355271cd5fdbf0c0d09bef9c8cbbfa98d3fe9727afa670c30e7
74063aeff534b824ad3f505431e56875c1fd73dfd95be7972defaf0719120406
8714970129d26b5967552190c540f3f7579a818c60cc4f587ebfe51d833a1a06
c8cfb43414cd425eede08a6267a0cdf3789175dfba95a903ee9dfa0ae2e94a8b
e3db221308873ae75ef124484688f303c7eb6af1ac1ed5f7fbbdcfcda7d8cf80
e9a9f3c7321d83e781c00eed712f9ecffc2024fd41ee1e45bc77d2ff8b1264d1
dcbe7748ceaec2ff72e9d8afa568973658534695527bd6762c05d8b9ed596f16

KPMG

KPMG Cyber Threat Intelligence Platform

DragonRank Group - Disrupting IIS Servers and SEO Integrity

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
42e99d6292f5e32592769735fc7736855a4167a40243bde671af7d47cd59003d
6430651ce3d7ab9771bdd2701d2ab953929ba8099d272f390bb263a136f8f815
0cd5e57662df74165fcdf8b668d23c654064c51a9d75c228b3a2b0e74bff58ed
c747d509ecfed834d147bdf7390903e0670e6624b7921ffcb5c73390af615850
b3aa822a7349d95c2210598b95fa8e85c1ce0f22acdf10611a31e3e82c84ed33
3cacf83c74a3be04a2fc7f9d19564b219949e941fd9b4aa183ee25f87c2816a0
45f21f20af0482092cdcc9d00c0657f000fac3c31fc3aeebe78ee1a397b914b3
9a8e9d587b570d4074f1c8317b163aa8d0c566efd88f294d9d85bc7776352a28
99ab43bf8a9934d01ba9ec6203c95e3c16e6c0dfc633538ab29795ba979b4adf
8627cc34ab2c713ecf5d4d171a32325eb69b140542cdd36d7eca46c19e310253
30080323573618d9463351c471b1bb577de8ee40cdd5fc915daf14a25737a67f
ad7773cb9e55e4c37bed2bb34a9e695c8965cc12c75b3da5e12f868fc1c78a52
f2c5c7d65752a2fdf94466d36fbeee720f060aa140a89530322732d3385fb3db
b9faf82542bbaca124ef80f58ee55a866ee10481fa30419c89f112d7bb4a9815
2c635e82f71944444b8dcc08949ff7c0ac5f04f78cfcb86410d9f61c63accf4d
1749b814522ba5dc141b399ee8f04616d72bfdfdd8ab8ebab6c9d494a378cbfc
d802ac7ad043e24db3c640b1364da79973eac2025f647654972a544d5a2740dd
f3f95debb843d6faf41c6884e1e7541dcff5fe1c47014914d895aaad757e0159
b24b47faa11b18a4e67fcffc05265b51bab2cf7732c66f6695ce10e89d61fcb7
96d5f775fca96cfe092e94bd1b978be215fd3d52e0fe1cc15bc61d787c122c85
3424b3c334bc28a2996177397644587 33bb38132e1403ef69985e4beb0dc40f2
94b323eaf06ea503bf0157c575128e46083257b8ee71d4e5faa7ca4d38e50f8c
b76ef88a61f6cb0189358a0b4268a6828054bdcd6e0bf7dff2af491d7542beaf
0ab7e992aa85a0e23d9a7ee1e3928eb2015c0733d7fb324bf8b0c0e3c65d500b
206c9e66f337fbf0611e172217b550b9f8f25cc807e478910c872856c32eb741
fd0dd6c05be458e18640db3eaaa9f6d259c1224f244110595b0a634fffacadf9

Follow us on:
kpmg.com/in/socialmedia