Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

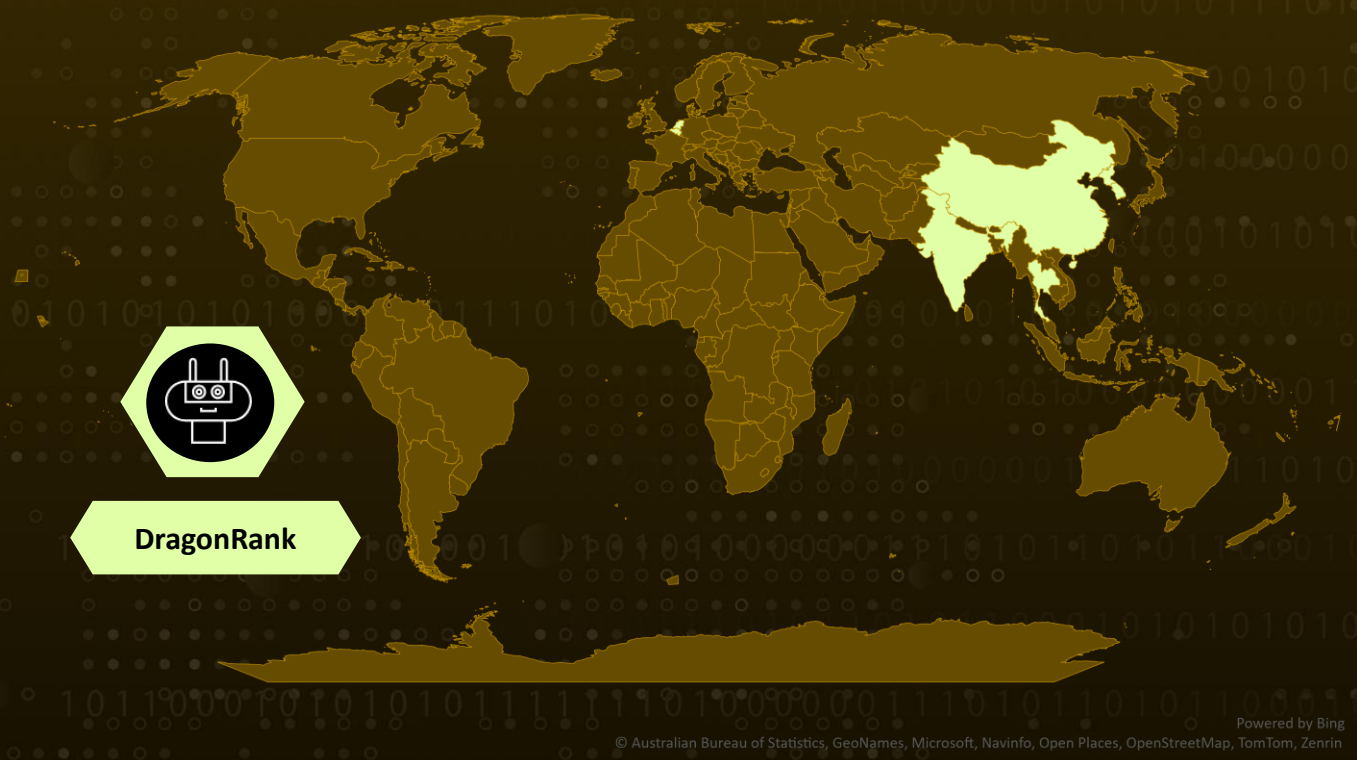
DragonRank: The SEO Hackers Manipulating Search Results

Date of Publication	Admiralty Code	TA Number
September 13, 2024	A1	TA2024355

Summary

First Seen: 2024
Targeted Countries: Thailand, India, Korea, Belgium, Netherlands and China
Malware: PlugX and BadIIS
Threat Actor: DragonRank
Targeted Industries: Jewelry, media, research services, healthcare, video and television production, manufacturing, transportation, religious and spiritual organizations, IT services, international affairs, agriculture, sports, and even niche markets
Affected Platforms: Windows
Attack: DragonRank is a newly identified hacking group that primarily targets countries in Asia and Europe. They exploit vulnerabilities in web applications to deploy web shells and malware like PlugX and BadIIS, allowing them to gather system information and establish persistent control. Their main goal is to manipulate search engine optimization (SEO) rankings for third-party scam websites hosted on compromised servers, thereby increasing the visibility of these malicious sites.

Attack Regions



Attack Details

#1 DragonRank is a newly identified hacking group that primarily targets servers across Asia and Europe. This group engages in SEO (Search Engine Optimization) poisoning campaigns to manipulate search engine results, thereby drawing unsuspecting users to malicious websites. These compromised sites often feature fraudulent content, including malware and credential-stealing tools.

#2 The group is known for exploiting vulnerabilities in web applications like WordPress or phpMyAdmin and using tools such as web shells to gain control of Microsoft Internet Information Services (IIS) servers. After taking over these servers, DragonRank deploys malware like PlugX and BadIIS, which help them steal information, move laterally through networks, and evade detection. One of their notable techniques is using Windows Structured Exception Handling (SEH) to disguise malware activity.

#3 The group offers unethical SEO services to clients via platforms like Telegram and QQ, suggesting they are financially motivated. Their attacks have spanned industries ranging from healthcare to media, agriculture, and more, with confirmed victims in countries like China, India, Thailand, Belgium, and the Netherlands.

#4 The hacking group appears to be linked to Chinese-speaking actors Overall, this campaign highlights a sophisticated blend of cybercrime tactics aimed at exploiting vulnerabilities for financial gain through SEO manipulation.

Recommendations

Regularly Update and Patch Systems: Ensure that all web applications, including content management systems (CMS) like WordPress and phpMyAdmin, are regularly updated to the latest versions. Conduct routine vulnerability assessments to identify and remediate weaknesses in your systems.

Implement Web Application Firewalls (WAF): Deploy a WAF to monitor and filter incoming traffic to your web applications, blocking malicious requests and preventing exploitation of known vulnerabilities. Configure custom rules to detect and mitigate specific threats associated with the DragonRank campaign.

Enhance Authentication Mechanisms: Enforce strong password policies and encourage the use of multi-factor authentication (MFA) for all administrative accounts. Regularly monitor account activity for unusual login attempts or privilege escalations.

Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with BadIIS and PlugX, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	**TA0008** Lateral Movement	**TA0042** Resource Development	**TA0003** Persistence
TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0040** Impact
TA0011 Command and Control	**TA0009** Collection	**T1588.006** Vulnerabilities	**T1588** Obtain Capabilities
T1016 System Network Configuration Discovery	**T1057** Process Discovery	**T1033** System Owner/User Discovery	**T1069.001** Local Groups
T1082 System Information Discovery	**T1555** Credentials from Password Stores	**T1505.003** Web Shell	**T1505** Server Software Component
T1021.001 Remote Desktop Protocol	**T1021** Remote Services	**T1574.002** DLL Side-Loading	**T1574** Hijack Execution Flow
T1027 Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information	**T1055** Process Injection	**T1608.006** SEO Poisoning

T1608 Stage Capabilities	T1547 Boot or Logon Autostart Execution	T1090 Proxy	T1584.004 Server
T1584 Compromise Infrastructure	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1059 Command and Scripting Interpreter
T1218.011 Rundll32	T1218.007 Msiexec	T1218 System Binary Proxy Execution	T1547.001 Registry Run Keys / Startup Folder
T1113 Screen Capture			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	72fc4ba4d8e9a7b11fa0b76611e85b7aaf3558ac08dc8e9628fad48d72fb8190, 9277f848a5348e447e02cf94beae392815a235264443fdd69a3ff6eb48f040a8, ffa94d76d4423e43a42c7944c512e1a71827a89ad513d565f82eb8fe374ef74d, 3503d6ccb9f49e1b1cb83844d1b05ae3cf7621dfec8dc115a40abb9ec61b00bb, 614920f1a8550070a983f2ad22d6358c6742a9e02802b025eeea8db8c3d41fb7, 6422684371fabf8a2ceaf06146d0a11d2c3c79647700c61f55e4af095a8360a4, 6430651ce3d7ab9771bdd2701d2ab953929ba8099d272f390bb263a136f8f815, 0cd5e57662df74165fcdf8b668d23c654064c51a9d75c228b3a2b0e74bff58ed, 3f17c66aab154212fb02fc7e329296c233aebe4abd9248204fa99c490c113a6e, 8251189e8b596743683f2ab2d731eb19efe3e4e28ac5c100ea88cfdc36aeeac8, 875239000f22cff75f62f9a1aa9924a8c3fea72124b0c4b31c7b3814f9dc0601, c41587c393741e78b678f1fc3d7934859a306c4cc4c0b02ca08d596289caeff4, cdc9f18de75991e7b289ab26b32dca9f4de6f95f88a6d3d32c87a111c4dc4d18,

TYPE	VALUE
SHA256	c747d509ecfed834d147bdf7390903e0670e6624b7921ffcb5c73390af615850, 6e5eb43b81f103e4926be92d6bef9048bfa042bddb95a1ad3245230df0e04d22, 7dd1307fd65599600a5056ae867c373333ae265f6fa29dc02ec697916159ed84, 373d95685d0fd184aa4d5e47f7b1eb1848badef4fc9db46415f858f37eb20eee, 839b8532681df355271cd5fdbf0c0d09bef9c8cbbfa98d3fe9727afa670c30e7, 74063aeff534b824ad3f505431e56875c1fd73dfd95be7972defaf0719120406, 8714970129d26b5967552190c540f3f7579a818c60cc4f587ebfe51d833a1a06, c8cfb43414cd425eede08a6267a0cdf3789175dfba95a903ee9dfa0ae2e94a8b, e3db221308873ae75ef124484688f303c7eb6af1ac1ed5f7fbbdcfcda7d8cf80, e9a9f3c7321d83e781c00eed712f9ecffc2024fd41ee1e45bc77d2ff8b1264d1, dcbe7748ceaec2ff72e9d8afa568973658534695527bd6762c05d8b9ed596f16, b3aa822a7349d95c2210598b95fa8e85c1ce0f22acdf10611a31e3e82c84ed33, 3cacf83c74a3be04a2fc7f9d19564b219949e941fd9b4aa183ee25f87c2816a0, 45f21f20af0482092cdcc9d00c0657f000fac3c31fc3aeebe78ee1a397b914b3, 9a8e9d587b570d4074f1c8317b163aa8d0c566efd88f294d9d85bc7776352a28, 99ab43bf8a9934d01ba9ec6203c95e3c16e6c0dfc633538ab29795ba979b4adf, 8627cc34ab2c713ecf5d4d171a32325eb69b140542cdd36d7eca46c19e310253, 42e99d6292f5e32592769735fc7736855a4167a40243bde671af7d47cd59003d, 30080323573618d9463351c471b1bb577de8ee40cdd5fc915daf14a25737a67f, ad7773cb9e55e4c37bed2bb34a9e695c8965cc12c75b3da5e12f868fc1c78a52, f2c5c7d65752a2fdf94466d36fbeee720f060aa140a89530322732d3385fb3db, b9faf82542bbaca124ef80f58ee55a866ee10481fa30419c89f112d7bb4a9815, 2c635e82f71944444b8dcc08949ff7c0ac5f04f78cfcb86410d9f61c63accf4d,

TYPE	VALUE
SHA256	1749b814522ba5dc141b399ee8f04616d72bfdfdd8ab8ebab6c9d494a378cbfc, d802ac7ad043e24db3c640b1364da79973eac2025f647654972a544d5a2740dd, f3f95debb843d6faf41c6884e1e7541dcff5fe1c47014914d895aaad757e0159, b24b47faa11b18a4e67fcffc05265b51bab2cf7732c66f6695ce10e89d61fcb7, 96d5f775fca96cfe092e94bd1b978be215fd3d52e0fe1cc15bc61d787c122c85, 3424b3c334bc28a299617739764458733bb38132e1403ef69985e4beb0dc40f2, 94b323eaf06ea503bf0157c575128e46083257b8ee71d4e5faa7ca4d38e50f8c, b76ef88a61f6cb0189358a0b4268a6828054bdcd6e0bf7dff2af491d7542beaf, 0ab7e992aa85a0e23d9a7ee1e3928eb2015c0733d7fb324bf8b0c0e3c65d500b, 206c9e66f337fbf0611e172217b550b9f8f25cc807e478910c872856c32eb741, fd0dd6c05be458e18640db3eaaa9f6d259c1224f244110595b0a634fffacadf9
URLs	hxxp[:]//35[.]247[.]175[.]184[:]443/1[.]aspx, hxxps[:]//admin1[.]tttseo[.]com/ht[.]zip, hxxp[:]//ddos[.]tttseo[.]com/ddos/ddos[.]zip, hxxp[:]//a[.]googie[.]pw/xx1[.]php, hxxp[:]//a[.]googie[.]pw/zz1[.]php, hxxp[:]//b[.]googie[.]pw/xx1[.]php, hxxp[:]//b[.]googie[.]pw/zz1[.]php, hxxp[:]//web[.]googie[.]pw/xx1[.]php, hxxp[:]//web[.]googie[.]pw/zz1[.]php, hxxp[:]//www[.]ig26[.]com/xx1[.]php, hxxp[:]//www[.]ig26[.]com/zz1[.]php, hxxp[:]//www[.]googie[.]pw/xx1[.]php, hxxp[:]//www[.]googie[.]pw/zz1[.]php, hxxp[:]//www[.]yx52[.]pw/xx1[.]php, hxxp[:]//www[.]yx52[.]pw/zz1[.]php
Domain	mail[.]tttseo[.]com
IPv4:Port	202[.]162[.]108[.]48[:]443, 154[.]23[.]179[.]133[:]888, 154[.]23[.]179[.]133[:]443

References

https://blog.talosintelligence.com/dragon-rank-seo-poisoning/

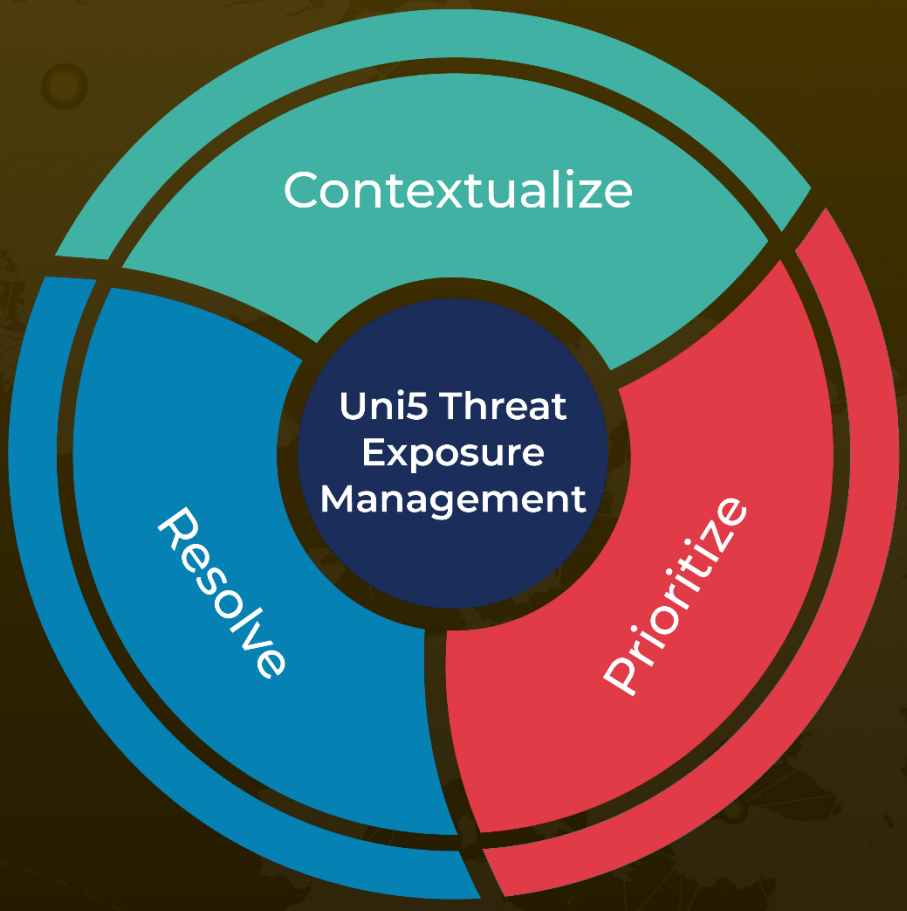
https://github.com/Cisco-Talos/IOCs/blob/main/2024/09/DragonRank%2C%20a%20Chinese-speaking%20SEO%20manipulator%20service%20provider.txt

https://www.hivepro.com/threat-advisory/malicious-google-ads-target-chinese-users-covertly-delivering-rats/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 13, 2024 • 5:30 AM

More at www.hivepro.com