Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

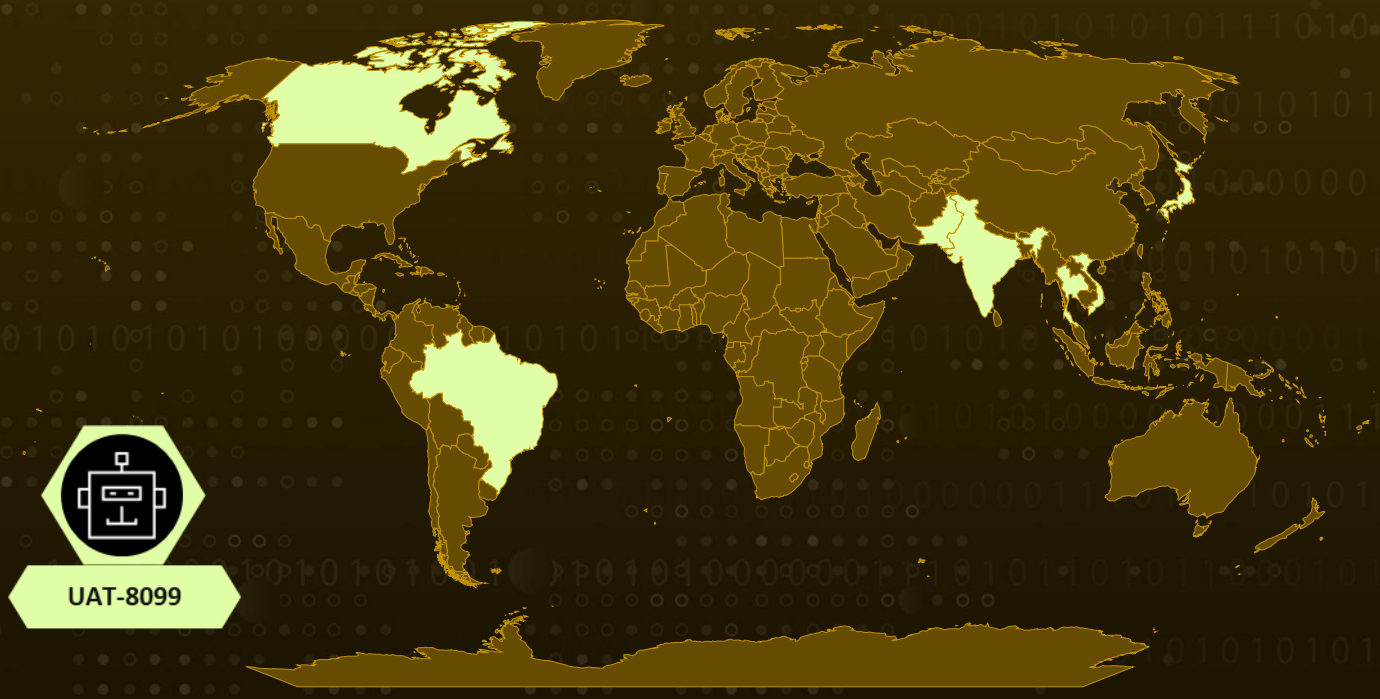
UAT-8099 Cybercrime Group Leverages BadIIS

Date of Publication	Admiralty Code	TA Number
February 2, 2026	A1	TA2026031

Summary

First Seen: April 2025
Targeted Regions: India, Thailand, Vietnam, Canada, Brazil, Pakistan, Japan
Targeted Platforms: Microsoft Windows Server, Linux
Targeted Product: Microsoft Internet Information Services (IIS)
Targeted Industries: Education, Technology, Telecommunications
Threat Actor: UAT-8099
Malware: BadIIS
Attack: UAT-8099 is a cybercrime group that compromises vulnerable IIS servers to conduct search engine optimization (SEO) fraud and steal high-value credentials, configuration files, and certificate data. The group exploits weak file upload configurations to deploy web shells and the BadIIS malware, which manipulates search engine rankings by injecting malicious content when Googlebot crawlers visit compromised servers.

Attack Regions



Attack Details

#1

UAT-8099 targets Microsoft Internet Information Services (IIS) servers with insecure file upload controls. After identifying a vulnerable host, the group uploads ASP.NET web shells to gain entry and perform initial reconnaissance. They exploit weak content management systems and misconfigured upload features to collect system details and map further attack paths within the environment.

#2

After securing access, the attackers enable the guest account, elevate it to administrator privileges, and activate Remote Desktop Protocol (RDP) for persistent control. They create concealed administrator accounts, commonly using names such as admin$ or mysql$, to maintain long-term access. Cobalt Strike beacons are then deployed through DLL sideloading with inetinfo.exe, using a multi-stage loader that ends with a custom reflective loader. To disguise command-and-control traffic, the group relies on SoftEther VPN, EasyTier decentralized VPN, and Fast Reverse Proxy (FRP).

#3

The group installs **BadIIS** malware on compromised servers, using it for proxying traffic, injecting malicious content, and conducting SEO fraud. In proxy mode, the malware relays traffic to secondary command-and-control servers. In injector mode, it modifies web responses from Google search traffic to insert malicious JavaScript that redirects users to gambling and advertising sites. In SEO fraud mode, it serves keyword-rich pages to search engine crawlers, manipulating search rankings for gambling-related terms.

#4

In parallel, UAT-8099 carries out large-scale data theft. Using RDP, the attackers search for sensitive files such as logs, credentials, configuration data, and certificates with the Everything file search tool. They review the data locally, bundle it into hidden directories, compress it with WinRAR, and exfiltrate it for resale or further abuse.

Recommendations

Restrict IIS File Upload Configurations: Immediately review and harden all IIS server file upload settings to restrict allowed file types and prevent unauthorized uploads of executable scripts and web shells.

Deploy StaticFile Handler for Upload Directories: Configure IIS to prevent execution of uploaded scripts or files by adding a StaticFile handler to upload folders, effectively blocking web shell execution.

Monitor for Hidden Administrator Accounts: Regularly audit user accounts for unauthorized or hidden administrator accounts such as "admin$" or "mysql$" that may indicate compromise and persistence by UAT-8099.

Disable or Restrict External RDP Access: Disable Remote Desktop Protocol access from external networks or implement strict network segmentation and multi-factor authentication for remote administrative access.

Scan for Web Shells and BadIIS Modules: Conduct regular scans of IIS servers for unauthorized web shells, BadIIS modules, and anomalous files using threat intelligence feeds containing indicators of compromise specific to this campaign.

Implement Certificate Management Best Practices: Monitor for unauthorized certificate issuance or usage, as threat actors specifically target and exfiltrate certificate data for potential resale or impersonation attacks.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.005: Visual Basic
Persistence	T1505: Server Software Component	T1505.003: Web Shell
		T1505.004: IIS Components
	T1136: Create Account	T1136.001: Local Account
Privilege Escalation	T1078: Valid Accounts	T1078.003: Local Accounts
Defense Evasion	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1027: Obfuscated Files or Information	
Credential Access	T1552: Unsecured Credentials	T1552.001: Credentials In Files
Discovery	T1083: File and Directory Discovery	
Collection	T1560: Archive Collected Data	T1560.001: Archive via Utility
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1572: Protocol Tunneling	
Impact	T1491: Defacement	T1491.002: External Defacement

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	tdk[.]hunanduodao[.]com/jump/fql[.]js, tdk[.]hunanduodao[.]com/jump/ov[.]js, tdkfsdfa[.]cnmseo[.]com/jump/fql[.]js, tdkfsdfa[.]cnmseo[.]com/jump/ll[.]js, tz[.]jmfwy[.]com/jump/json[.]js, tz[.]jmfwy[.]com/jump/mage[.]js, tz[.]jmfwy[.]com/jump/tiger[.]js, tz[.]ohtcm[.]com/jump/fql[.]js, tz[.]ohtcm[.]com/jump/json[.]js, tz[.]ohtcm[.]com/jump/ll[.]js, tz[.]ohtcm[.]com/jump/ov[.]js, tz[.]suucx[.]com/jump/ov[.]js, google[.]sneaws[.]com, w3c[.]sneaws[.]com, aspx2[.]ggseocdn[.]com, th1[.]ggseocdn[.]com, bxphp[.]ggseocdn[.]com, bx[.]ggseocdn[.]com, list[.]ggseocdn[.]com, ar[.]ggseocdn[.]com, x2[.]ggseocdn[.]com, x3[.]ggseocdn[.]com, alex[.]rootggseo[.]com, modll[.]win123888[.]com, mo2dll[.]win123888[.]com, cheng[.]win123888.com, th1[.]win123888[.]com, x5[.]westooo[.]com, joydphp[.]westooo[.]com, joyddll[.]westooo[.]com, bx[.]westooo[.]com, ar[.]mnnoxzmq[.]com, iis[.]ihack[.]one, mejsc1[.]com, ceshi[.]mejsc4[.]com, link[.]mejsc4[.]com, mulu[.]ihack[.]one, tdk[.]ihack[.]one, xl[.]luodixijin[.]com,

TYPE	VALUE
Domains	xldll[.]xijingdafa[.]com, meindi11[.]com, google[.]dfbdfwrthgef[.]top, buvmfuwecndskmkvhndfjk[.]dfbdfwrthgef[.]top, suidcbdewjskbcsdjvbwehcsdj[.]dfbdfwrthgef[.]top
SHA256	1ab98783a02ad9f127e776c435ef4e24a18ab93c4b4ee5ede722817d4b20771a, 1ece4d8603f5e28a7b0f6a8c83963a57cf23e5d2fadfc138419c3a051a75c93a, 2cc87bd2ae25a5119cb950618850eddeb578954fa780b125c1f51d234fb405e3, 4bc189af91779582a1d29cfe187aa233e7ba50d223261fb9fbe31df5b06dff96, 6be5c8882bc02cf4e86d2ab9d20aa3446b71dd12c73f9c6bf0faf9412d7d23ba, 9a2fd34e22c5f3d3d5fb96e3cd514dad7b03ed7bf53a87e7d8d9b73987d02ece, 11ea6aa2b31677f8a36627d4af709e70cff4a033b0975f63c19b28945e6226b7, 29ffb1d28f98582e81e78e6b2d5502da50c8ebdee0d40005a86b0dadece2923b, 56be91643dd8b86f347cc8d743c568f2d0169781ba999a2f708e503b59ecff76, 70d6bc89451e36889c045f30de22bc02e032788c8938baa0d5802e8f747c3e79, 91e1f4fc92f104ec8b29bb56df87f8e7d8b518c63997e2ea162d3f1cac3fcac1, 416ef6da8a27a99cbce6517d31857c8b8b55f02e9c8118510dc33814fb6f57be, 660ccb6dcfad97bfaddc667c61b1904e99a06eab981d44119092624d42912d68, 9458a75c1e24add9a48e0425e514a5f0cb46a826bff30ea7ea34e69099345f29, 265336511db98a4c40476455e2ae93aaf926abecd8f9b9d741f8d253abb80357, a781581baf6e1e335f22c9ffbb2656a2d9c8e51f463e3a48068210425df1c205, ab03a7caed279fc6411ec19386faff3b65be34c91c3f0550eaef84a663720d0d, bcc393c1686a0f5d493041e98dcafe0098d952d5e93eb4d2ebdb63c0efd2de33, c7a22f5c55ac1373a5964a6598da2a9afd8a61b9d729b9bf52a93c967a7f0eda, cdf454173bac13266e0f7db5de386439f197e2c480e1cc303dd7e806484645da,

TYPE	VALUE
SHA256	e84a16c8e25a4e40926cbb4cc210a09830298b6f99d532035f5136d05ffc008c, e448557d26cf2917efded8e30c67db8094ce1f6db78801742988ea21f3429d7c, 5d320b60d2f40c200e81eaeb67a86a04782bff84582c73e726255dba2dcb821e, 99f2c4773560eb515cfcb0ad45cf8e47c46580ab19494463160f885e048ce830, 565502d2454e4b65d3bd810fccf4b429264562fefa5cfff24c905b76b3b860a6, a34ea8fb565ac6f57eefc987c61159c1e6f1af6a8717ffb42f4b745db3bf9e31, 187e1417fd9d4f4a44e4f7b7172aef056e9d0ab5d7a7addf61c2cfa893f74fd1, 6b60b6df8a1a95f51ffe57255c05d26eb9e113857efac3b29d6ef080b8d414f3, 672ffdf1e9d4848015d29a68111266ef55fc6702dfe7b2053ce677882648dd5d, ebeef831c52b7e930a6456caedf7849814b8d4def2bc0e70a0e7a357621ef6bc, 230b84398e873938bbcc7e4a1a358bde4345385d58eb45c1726cee22028026e9, 48ec6530470b295db455bf2c72dc4fbd18672725f45821304f966d436b428865, 33d3ccf82279d94a8e8e772a0c4963d65a1f3576dbd6ed7b4ab8a0ee4869f97f, d8c0ef6dbf7d4572f92d3a492f32061ab8f3dd46beb9ff5a0bf9bf550935458c, 762db01f0dc61a3f4aa1695cb24a92fa21d236d8c5577926337ac1799d6569a5, 7276bc5fe4d29daf7a23a9a68022330290be45cc3a5a1d76e82063135b85ce5c, 046417685ad2eb075f33a0f757391df84750d2395fa6f82b1f05359710b7c9b6, f7cc8cf5a8e565c1aa8b7bd524f4f9fac392387de749657cb9d1cf4d694c4ad2, b3d08508b1e8962e56da007408450e2a40fae8cac1ee7d526914be80e31f6854, 8b2a61f29fdeda908d299515975a4dd3abd1a7508dbe8487bcb2a56fad2ec16f, e042f1a9b0a1d69311a5a1bd4eea37cc1a8a02cffe3f9ad5eb0c78fa79f326e2, 5a6dd4bb2db005adee56732b96fa6f4ceed47fc42298daf7bb3e6db32b59eac6, f659c4cfe4517a07b9c944cb7818be4022fdc42187766808ad02987a4152a875,

TYPE	VALUE
SHA256	7ddf475abc6e01a1e703f4c54e5a2c8601fef4767b3b1859b78cfdc18b173004, 0afa8830d2c664a192af94b638ab6b1c096d13e41a7f1886b71ff020e0d9bd93, 088fa3063c3015978955b572d5ddcff0838a945ce25665f24cca83d33e039cb9, c85a942a0d17c7accbabbf68ce04635327b757a662687c798e998c983c2a744c, e1342bca7bc4f3ff9453c68cd16532f4e6567a1ada37b6e2635cbc1c1ba325ac, 0c532a4a9f398fa2f5e12c2eac00c81ff4a70ac6746cf462c3f2206ed910693f, 94d8eaef036231cd604d0c769f0918e826501644a149876c09e967811c104860, 5284d5e034aa8c077469d3ef8fb2c09aa041c475703ea99c87855cf6eecf9564, fee057cee9da92d3d29078e7c30da7472ce99cc2ecaf4e13e8b3d6f266a6d35f, 299aabc6b9b03d92a6aed9d12eed45a669e5795763092693ac98322107cf8217, 85cf3c802a97facb5ae4c1e945c5042915017f35bdf1a570754b88710facf3f3, 0c364717dea76cbff870a2dbf2099213615a4caacaa5de61f7271c7eec73759f, 2eedd804c1fa4578485b55f4872145b7f891016510fe88fa760b61b8248dec82, 704ce326c380e4a35594df2b7d9bd17517709378451f3d9788728d01df36d0f6, b8626f0c45c68f6176540a64e2f8c6d5ac8b942a5ec030b590870a6eaffb931f, cbb4a9172f4b0185d3aecbaa60b8e04d8910889da8905e5089df3efdec0a38dd, ee6288fa8e5f111571475211b15522bc987da8421e9687a8089d1edef1df14a2, 74eb8d245d5571f3ee9a4e5417fb919034662681ff26a298a3526032307f16a4, cd86344937c7e7c9895fde8eecc682eb347c583e1ded491075aef548a8e255a4, 49740a5785f0d6790ee7f82915d2a95866332fc3eaf6fb0da59645404e4aed0c, 0511345f452e8c5ff2ca903553ba72f4fcb4f029f72b12e27f6a33e33977e5d2, 1149c50a049dca8ada30247532d0b2f18b94c199b45fd5dc129b5a9fda0991e9, 78f813c4474dcb4a1be9354d341bedcae6ef8689828a150c5936c308a0490777

TYPE	VALUE
URLs	hxxps[:]//7070-ppxcx-a1-3gg5ufwp666ee644-1300076834[.]tcb[.]qcloud[.]la/test/zcgo/go[.]exe, hxxps[:]//7070-ppxcx-a1-3gg5ufwp666ee644-1300076834[.]tcb[.]qcloud[.]la/test/zcgo/zcgo1[.]vbs, hxxp[:]//go1[.]kmm5tn[.]ceye[.]io, hxxp[:]//404[.]imxzq[.]com/tdks[.]php?domain=%s&path=%s, hxxp[:]//tdk[.]hunanduodao[.]com/tdk[.]php?domain=%s&path=%s, hxxps[:]//404[.]imxzq[.]com/tdks[.]php?domain=%s&path=%s, hxxps[:]//404[.]jmfwy[.]com/tdks[.]php?domain=%s&path=%s, hxxps[:]//799[.]cors5[.]vip/1018[.]php?domain=%s&path=%s, hxxps[:]//fql[.]jmfwy[.]com/tdks[.]php?domain=%s&path=%s, hxxps[:]//tdk[.]jmfwy[.]com/tdk[.]php?domain=%s&path=%s, hxxps[:]//th[.]gtwql[.]com/1018[.]php?domain=%s&path=%s, hxxps[:]//thov[.]hunanduodao[.]com/tdks[.]php?domain=%s&path=%s, hxxps[:]//bxphp[.]westooo[.]com/?xhost=%s&url=%s&ua=Googlespider&f=bd, hxxps[:]//bxphp[.]westooo[.]com/58z[.]js, hxxps[:]//bxphp[.]westooo[.]com/u[.]php, hxxps[:]//cdn[.]windowserrorapis[.]com[:]8443/v5/owa/rYpKZYehSa0sW1gFbbaVg4KB1m[.]cab

References

https://blog.talosintelligence.com/uat-8099-new-persistence-mechanisms-and-regional-focus/

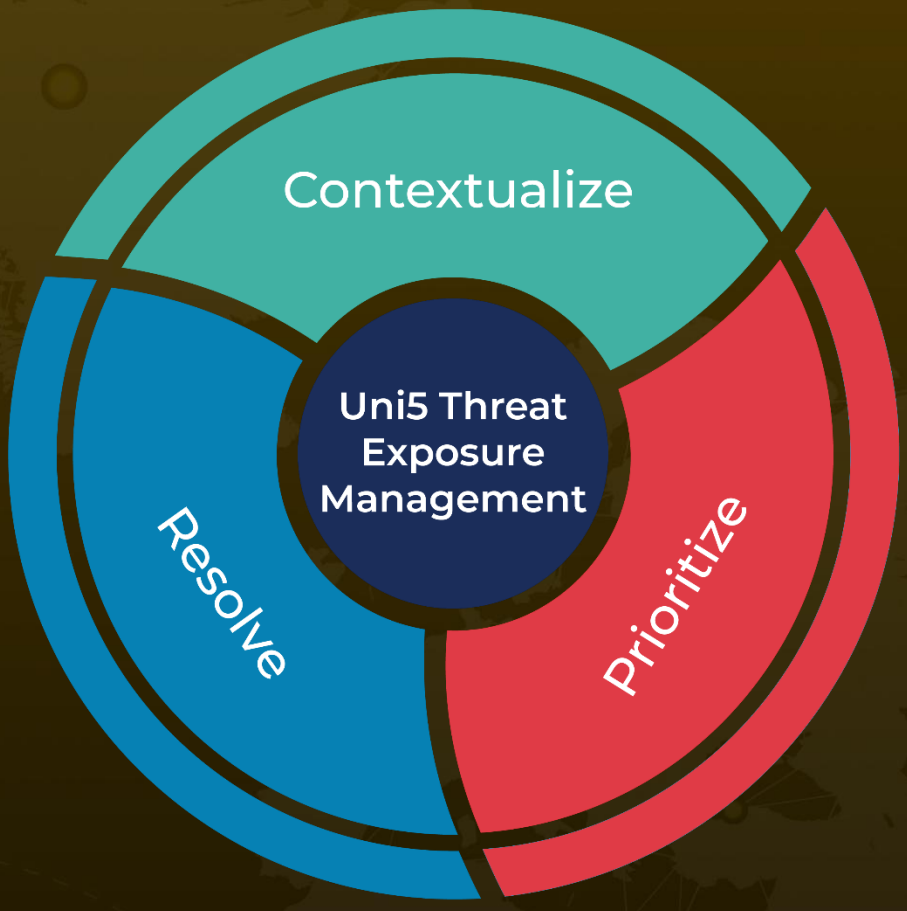
https://blog.talosintelligence.com/uat-8099-chinese-speaking-cybercrime-group-seo-fraud/

https://hivepro.com/threat-advisory/operation-rewrite-how-badiis-rewired-the-web-for-seo-poisoning/

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

February 2, 2026 • 01:00 AM

More at www.hivepro.com