Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

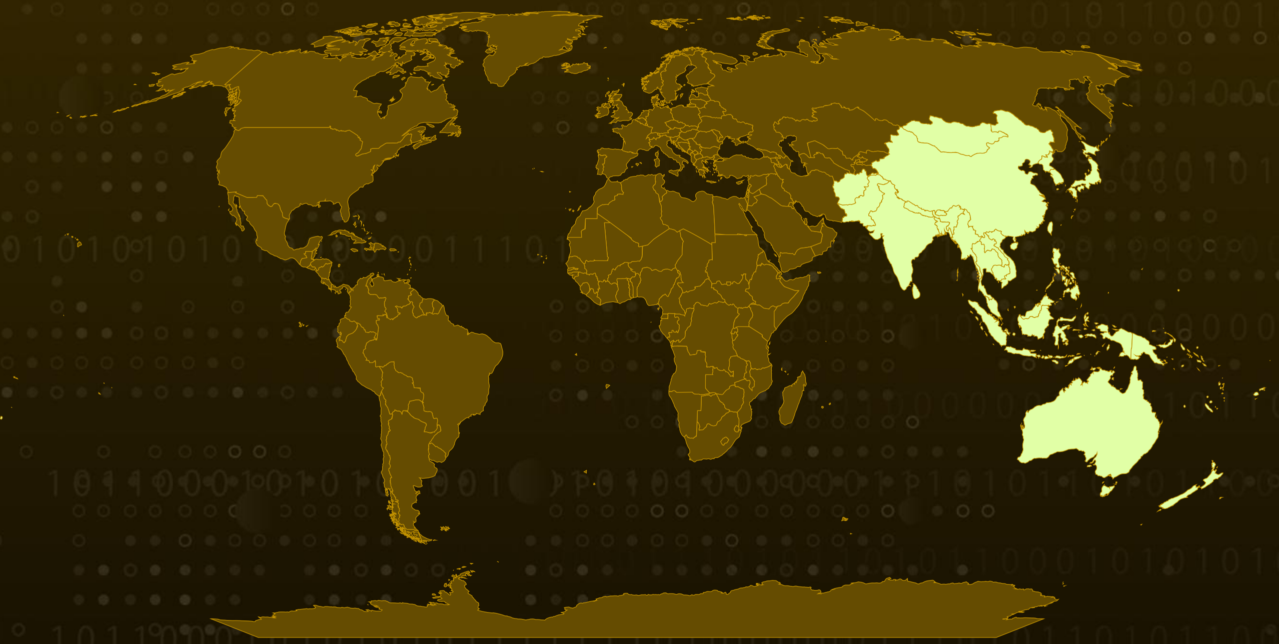
FatalRAT Malware Targets APAC Industries via Chinese Cloud Services

Date of Publication	Admiralty Code	TA Number
February 25, 2025	A1	TA2025058

Summary

Attack Discovered: 2025
Targeted Countries: Asia-Pacific region
Affected Industries: Industrial Organizations, Government Agencies, Manufacturing, Construction, Information Technology, Telecommunications, Healthcare, Power and Energy, and Large-scale Logistics and Transportation, Finance
Malware: FatalRAT
Attack: A highly sophisticated cyberespionage campaign is actively targeting various organizations across the Asia-Pacific (APAC) region, deploying the FatalRAT remote access trojan (RAT) to gain persistent access. The attackers are leveraging legitimate Chinese cloud services, including the myqcloud content delivery network (CDN) and Youdao Cloud Notes, to support their infrastructure and evade detection. Using a multi-stage payload delivery framework, they stealthily deploy malware while bypassing security defenses. FatalRAT grants attackers extensive control over infected systems, enabling keystroke logging, data theft, and remote command execution. While data exfiltration appears to be the primary goal, the malware's capabilities suggest the potential for further disruptive or damaging actions.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Details

#1 A sophisticated cyberattack targeting various organizations in the Asia-Pacific (APAC) region leveraged Chinese cloud content delivery networks (CDNs) such as MyQcloud and Youdao Cloud Notes. Attackers used an advanced payload delivery framework that relied on native file hosting services, encrypted sample packers, dynamic command-and-control (C2) address changes, CDN-based hosting, and DLL sideloading to evade detection. The campaign primarily deployed FatalRAT, a backdoor capable of remote administration, data exfiltration, and system manipulation.

#2 The attack was executed through a phishing campaign that targeted government agencies and industrial organizations, delivering multi-stage malware via ZIP archives disguised as invoices and tax filing applications. These ZIP files contained first-stage loaders for FatalRAT, making detection challenging. Instead of relying on fake phishing websites, the attackers embedded malicious file attachments that initiated the infection process. The malware retrieved dynamically updated configuration files and second-stage loaders from Youdao Cloud Notes, allowing it to adjust its behavior in real time.

#3 Once installed, the malware executed a complex infection chain involving DLL sideloading, process injection, and registry manipulation. The second-stage loader, Fangao.dll, retrieved configuration details and submitted system information to a predefined server endpoint. It performed system checks, created mutexes to prevent duplicate infections, and decrypted the final FatalRAT payload using an XOR key. The malware also leveraged Windows Group Policy settings to establish persistence, using the PureCodec application as a disguise. To evade detection, it simulated legitimate processes and displayed fake error messages while extracting its components.

#4 FatalRAT incorporated multiple anti-analysis techniques, including 17 checks for sandbox environments and virtual machines. If a security tool was detected, the malware immediately terminated itself. It also blocked workstation locking and launched a keylogger to capture keystrokes, storing them locally for later exfiltration. The malware's configuration, decrypted from an XOR-encrypted file, allowed it to modify registry keys, install itself as a service, and maintain persistence across reboots. Its network communications relied on dynamically retrieved URLs, preventing static analysis and takedown efforts.

#5 The campaign specifically targeted government agencies and industrial enterprises. The attack's use of Chinese-language cloud services, social engineering tactics, and industrial sector targeting suggests the involvement of a Chinese-speaking threat actor. While no specific group has been definitively linked to the attack, the attackers' infrastructure and techniques indicate a well-organized and persistent cyber-espionage operation.

Recommendations

Stay Alert with Unfamiliar Emails: Be wary of emails from unknown senders, especially if they contain attachments or links. Before clicking or downloading anything, take a moment to verify the sender's legitimacy to avoid potential threats.

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Limit Unapproved Cloud Services: Keep a close watch on cloud storage usage and restrict access to unapproved platforms like Youdao Cloud Notes to prevent attackers from using them to deliver malicious payloads.

Strengthen Security and Access Controls: Deploy advanced Endpoint Detection and Response (EDR) solutions to detect and block suspicious activities like DLL sideloading and unauthorized script execution. Additionally, enforce Multi-Factor Authentication (MFA) for all critical accounts and remote access services to reduce the risk of unauthorized privilege escalation.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0010 Exfiltration
TA0011 Command and Control	T1190 Exploit Public-Facing Application	T1566 Phishing	T1566.001 Spearphishing Attachment
T1036 Masquerading	T1036.008 Masquerade File Type	T1083 File and Directory Discovery	T1059 Command and Scripting Interpreter

T1059.005 Visual Basic	**T1574** Hijack Execution Flow	**T1574.002** DLL Side-Loading	**T1547** Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	**T1548** Abuse Elevation Control Mechanism	**T1548.002** Bypass User Account Control	**T1497** Virtualization/Sandbox Evasion
T1056 Input Capture	**T1056.001** Keylogging	**T1057** Process Discovery	**T1055** Process Injection
T1112 Modify Registry	**T1021** Remote Services	**T1027** Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	02fb1958a901d7d1c8b60ecc0e59207c, 033a8d6ec5a738a1a90dd4a86c7259c8, 04aa425d86f4ef8dc4fc1509b195838a, 096c34df242562d278fc1578dc31df92, 09a50edb49cbb59a34828a37e63be846, 0a49345c77da210ab0cd031fda6bc962, 0a70ea6596c92fbfb461909ed57503fa, 0b20f0ff1aaff4068f99f4db69ba9c1e, 0c33792c6ed37452f44ca94ce7385250, 142eb5106fcc2f95b7daf37dca970595, 15b7990bd006d857ee02c529b45783ac, 1c79abe9f52cbe92f042615a9f6b6f10, 1e80a8b3f4efb4bb27771d729f5ced85, 2026ead0c2366d049ecd5e42ac1b1b07, 24ecb197ee73e5b1eef2ded592640cf2, 26f0806932dfd029f0fe12e49bb4c799, 28231ce260ce66388d58ce536d7ed201, 2aa41ae3d3ae789147218652e6593161, 2bccd50322afb7a349c163ce9b76bb66, 357534f6a2bffa77b83501715e382a94, 362fc5799ecef8e9e328cfbf6272c48f, 3843ef98a4c7ee88f10078e6a38f15ee, 3883957530482a399abb5e1f06e4581f, 3b32fc9115c224653f5afba793c0bbef, 3ca82fd8d12967c32388ad18e9727fac,

TYPE	VALUE
MD5	44b47fdab8ca3375fe5a875deefa265c, 4fc6dbb9beeecb2d60f3fef356c6df01, 502054d938a18172a3657aaf2326bcf4, 50a5c5a3c07f04d96f5f1968996cfb74, 50d29ee29b54685bd10b8d2917696413, 58a8daae643a84c112ddc6e79c750271, 58e44c4d797cecfed42c1fdf18c2d5f9, 58fe500e022ea1aeebbe72c4ce694531, 5b730131c3271820c03d711f2549b894, 5c1de870ea1e08b25e7ce4397372f5a6, 5d7fba23a44683c0b471d9a7cc7f5042, 632c0808e4d0c7b293642e4c4ae8e2a2, 6356234720271 5eff0e7f2d6ad07a2aa, 63c600434def54157204765619838372, 64013e613a0130cb1b7845139537bc5e, 64d72e8d0539e6a0b74fb1c6e5127c05, 64fdeed776cfd5e260444ae2e4a5b1a4, 699ad2a5b6d9b9b59df79e9265ebd47a, 6a5e3776c3bfdadd899704589f28e9fd, 6a73f3bab8fb205ed46e57cf076b6f6d, 7081b6781e66bdceb2b119a783b6c7fd, 771a5d8fc6829618f15abe49796d1c44, 790cf080abb18af471d465998b37fd1b, 797d111244805e897db5c21010ee8e12, 7ba376f5a71ffa21a92c7b35c3b000eb, 82394a97458094b1cb22c4e243f4e9db, 8c0599c0a6b7ffaff93762d0c3ea2569, 8da2c4796c439f4a57536bd5c5d3f811, 8e474f9321fc341770c9100853eb41eb, 9037ccfcd3d3d1542089d30d3041db1c, 936c16a64432348176f9183cd1524cef, 93f12cbfb9ba1a66d3a050a74bab690b, 949f086c40cfc5144243a24688961414, 9636309c41e8a33507c349b8e9053c49, 991cb5f8476edbc73223d1331704a9fd, 9bb22b91b5ad59972130a3a428f7b5bb, 9bf2e34511619b7c4573c3974bdbaa39, 9e8a08fcddb10db8d58e17b544d81bff, a009b341aa6f5bda61300dc5e7822480, a7b20338dd9ed5462ddff312b67556e9, ab5f57681299933c1f70b938caa526d3, ac3fbdbfbc08f41e4ad1c004180093f1, ad216eaf11500eb73c6cdafc18cb49d8, ae735b1d9b7e9dd496d22409ceaeda66, b0c315c5dcda6e4442280c07b11d1ba5,

TYPE	VALUE
MD5	b1ad89be2632933350683b91011a4aee, b37917ea3849607d02d330130a823567, b3f8f1272813bff80630b9caab6e5089, b5c46f829fed11b4ddc2e155dc5cf974, bc36b1be438f92fe5f9a47f13244503e, bd6b8574738c7589887b61d4fad68fce, bdd68e7733c09fad48d4642689741ea4, be15a198f05eb39277720defa9188f62, c4579aa972d32e946752357ca56ee501, c555cc05f9d16b9e9222693e523e0ba5, c89a4a106619c67b8410efa695d78ef3, ca7dc49e80b2a77677718c72f3cc6bc1, cbc36deadef17a4c315cbbff3f74439f, d35635e8d07b923d1e89f541d4f03b90, d413cf08ef7c6357dd0215b8b9ebe6f4, d494efc086447c543d0c3c7beecf2bc6, d6bda8be4ba9563844b3b9367b73bd2e, dc2676b0c54b31a017ada4f62693de54, dded5d108b6a9ee50d629148d8ed4ec5, df6f5f4b7b8ba3c2c0ddc00d47e33218, e0d5b46dffee56c337fdc172ce617850, e32020ab02e11a995effb7781aabd92f, e6ef56c91bd735542775dfef277e0cc7, e8204900e8acb502ca6e008f9532b35e, e91991304abf5d881545bc127e7fb324, eb9419aa5c6fee96defad140450a9633, ec0bdf52c113487e803028dbc52e8173, ed036740be0a8e3203a54edd4d4b735c, f9e461cc83076d5f597855165e89f0db, fdc35392af34ef43291b8f7f959ef501, feb8e6059a234ea689404d3d4336e8af, 4e40c9945cc8b62c123e5636155e96a7, 6bfe01cd9c038aa90bcd600d49657c21, 80c7667c14df5b92ab206b2ea9b42aff, eb53df9fe23d469350885164aa82215e, 32c105c5229843aaebf12621359195a9, 34b29454676e780d81d8bba066d7d94f, 8577438ecff5753ddcf427b93c5976c8, f481a67933055956e8dd77b4b2bde9ed, f8136c909fb35457fc963d87b50bc158, 02477e031f776539c8118b8e0e6663b0, 02d8c59e5e8a85a81ee75ce517609739, 05c528a2b8bb20aad901c733d146d595, 15962f79997a308ab3072c10e573e97c, 17278c3f4e8bf56d9c1054f67f19b82c, 172ee543d8a083177fc1832257f6d57d,

TYPE	VALUE
MD5	1fe3885dea6be2e1572d8c61e3910d19, 249f568f8b8709591e7afd934ebea299, 266bb19f9ceb1a4ccbf45577bbeaac1a, 3c583e01eddd0ea6fe59a89aea4503b4, 3ec20285d88906336bd4119a74d977a0, 43156787489e6aa3a853346cded3e67b, 46630065be23c229adff5e0ae5ca1f48, 577e1a301e91440b920f24e7f6603d45, 5be46b50cac057500ea3424be69bf73a, 60a92d76e96aaa0ec79b5081ddcc8a24, 60dbc3ef17a50ea7726bdb94e96a1614, 635f3617050e4c442f2cbd7f147c4dcf, 675a113cdbcce171e1ff172834b5f740, 68a27f7ccbfa7d3b958fad078d37e299, 73e49ddf4251924c66e3445a06250b10, 787f2819d905d3fe684460143e01825c, 7ac3ebac032c4afd09e18709d19358ed, 8f67a7220d36d5c233fc70d6ecf1ee33, 9b4d46177f24ca0a4881f0c7c83f5ef8, 9c3f469a5b54fb2ec29ac7831780ed6d, 9d34d83e4671aaf23ff3e61cb9daa115, a935ef1151d45c7860bfe799424bea4b, bcec6b78adb3cf966fab9025dacb0f05, d0d3efcff97ef59fe269c6ed5ebb06c9, ebc0809580940e384207aa1704e5cc8e, eca08239da3acaf0d389886a9b91612a, ed6837f0e351aff09db3c8ee93fbcf06, fb8dc76a0cb0a5d32e787a1bb21f92d2, feb49021233524bd64eb6ce37359c425
IPv4:Port	101[.]33[.]243[.]31[:]82, 43[.]154[.]238[.]130[:]6000, 134[.]122[.]137[.]252[:]6000, 43[.]154[.]238[.]130[:]8081, 111[.]230[.]93[.]174[:]8081, 43[.]159[.]192[.]196[:]6000, 43[.]138[.]199[.]241[:]6000, 175[.]178[.]166[.]216[:]6000, 43[.]139[.]35[.]42[:]6000, 43[.]139[.]101[.]11[:]6000, 81[.]71[.]1[.]107[:]6000, 175[.]178[.]89[.]24[:]6000, 106[.]52[.]216[.]112[:]6000, 43[.]154[.]68[.]193[:]6000, 107[.]148[.]54[.]105[:]6000, 47[.]106[.]224[.]107[:]6000, 154[.]39[.]238[.]101[:]6000,

TYPE	VALUE
IPv4:Port	206[.]233[.]130[.]141[:]6000, 107[.]148[.]50[.]116[:]6000, 103[.]144[.]29[.]211[:]6000, 107[.]148[.]52[.]241[:]6000, 107[.]148[.]50[.]112[:]6000, 107[.]148[.]52[.]242[:]6000, 111[.]230[.]10[.]93[:]6000, 111[.]230[.]32[.]52[:]6000, 107[.]148[.]50[.]113[:]6000, 111[.]230[.]108[.]14[:]6000, 175[.]178[.]96[.]9[:]8081, 1[.]12[.]37[.]113[:]8081, 111[.]230[.]15[.]48[:]8081, 111[.]230[.]91[.]145[:]8081, 111[.]230[.]45[.]217[:]8081, 154[.]91[.]227[.]32[:]6000, 82[.]156[.]145[.]216[:]6000, 122[.]152[.]231[.]146[:]6000, 154[.]206[.]236[.]9[:]6000, 119[.]29[.]219[.]211[:]6000, 107[.]148[.]52[.]176[:]6000, 120[.]78[.]173[.]89[:]6000, 120[.]79[.]91[.]168[:]6000, 114[.]132[.]46[.]48[:]6000, 123[.]207[.]35[.]145[:]6000, 8[.]217[.]0[.]16[:]6000, 123[.]207[.]1[.]145[:]6000, 114[.]132[.]56[.]175[:]6000, 119[.]29[.]235[.]38[:]6000, 123[.]207[.]79[.]195[:]6000, 139[.]199[.]168[.]63[:]6000, 123[.]207[.]55[.]60[:]6000, 43[.]138[.]176[.]5[:]6000, 123[.]207[.]16[.]43[:]6000, 123[.]207[.]58[.]147[:]6000, 103[.]144[.]29[.]123[:]6000, 156[.]236[.]67[.]181[:]6000, 123[.]207[.]44[.]193[:]6000, 123[.]207[.]8[.]204[:]6000, 114[.]132[.]121[.]130[:]6000, 154[.]197[.]6[.]103[:]6000, 42[.]193[.]242[.]180[:]6000, 47[.]57[.]68[.]157[:]8080, 101[.]33[.]243[.]31[:]82, 43[.]154[.]238[.]130[:]6000, 134[.]122[.]137[.]252[:]6000,

TYPE	VALUE
IPv4:Port	43[.]154[.]238[.]130[:]8081, 111[.]230[.]93[.]174[:]8081, 43[.]159[.]192[.]196[:]6000, 43[.]138[.]199[.]241[:]6000, 175[.]178[.]166[.]216[:]6000, 43[.]139[.]35[.]42[:]6000, 43[.]139[.]101[.]11[:]6000, 81[.]71[.]1[.]107[:]6000, 175[.]178[.]89[.]24[:]6000, 106[.]52[.]216[.]112[:]6000, 43[.]154[.]68[.]193[:]6000, 107[.]148[.]54[.]105[:]6000, 47[.]106[.]224[.]107[:]6000, 154[.]39[.]238[.]101[:]6000, 206[.]233[.]130[.]141[:]6000, 107[.]148[.]50[.]116[:]6000, 103[.]144[.]29[.]211[:]6000, 107[.]148[.]52[.]241[:]6000, 107[.]148[.]50[.]112[:]6000, 107[.]148[.]52[.]242[:]6000, 111[.]230[.]10[.]93[:]6000, 111[.]230[.]32[.]52[:]6000, 107[.]148[.]50[.]113[:]6000, 111[.]230[.]108[.]14[:]6000, 175[.]178[.]96[.]9[:]8081, 1[.]12[.]37[.]113[:]8081, 111[.]230[.]15[.]48[:]8081, 111[.]230[.]91[.]145[:]8081, 111[.]230[.]45[.]217[:]8081, 154[.]91[.]227[.]32[:]6000, 82[.]156[.]145[.]216[:]6000, 122[.]152[.]231[.]146[:]6000, 154[.]206[.]236[.]9[:]6000, 119[.]29[.]219[.]211[:]6000, 107[.]148[.]52[.]176[:]6000, 120[.]78[.]173[.]89[:]6000, 120[.]79[.]91[.]168[:]6000, 114[.]132[.]46[.]48[:]6000, 123[.]207[.]35[.]145[:]6000, 8[.]217[.]0[.]16[:]6000, 123[.]207[.]1[.]145[:]6000, 114[.]132[.]56[.]175[:]6000, 119[.]29[.]235[.]38[:]6000, 123[.]207[.]79[.]195[:]6000, 139[.]199[.]168[.]63[:]6000, 123[.]207[.]55[.]60[:]6000,

TYPE	VALUE
IPv4:Port	43[.]138[.]176[.]5[:]6000, 123[.]207[.]16[.]43[:]6000, 123[.]207[.]58[.]147[:]6000, 103[.]144[.]29[.]123[:]6000, 156[.]236[.]67[.]181[:]6000, 123[.]207[.]44[.]193[:]6000, 123[.]207[.]8[.]204[:]6000, 114[.]132[.]121[.]130[:]6000, 154[.]197[.]6[.]103[:]6000, 42[.]193[.]242[.]180[:]6000, 47[.]57[.]68[.]157[:]8080
Domains	microsoftmiddlename[.]tk, cloudservicesdevc[.]tk, novadector[.]xyz, microsoftupdatesoftware[.]ga, 0a305ffb2a1d41f6870eac02f9afce89[.]xyz, xindajiema[.]info, Vip033324[.]xyz, microsoftmiddlename[.]tk, cloudservicesdevc[.]tk, novadector[.]xyz, microsoftupdatesoftware[.]ga, 101.kkftodesk101[.]top, 102.kkftodesk102[.]top, 104.kkftodesk104[.]top, 105.kkftodesk105[.]top, 106.kkftodesk106[.]top, 107.kkftodesk107[.]top, 108.kkftodesk108[.]top, 109.kkftodesk109[.]top, 110.kkftodesk110[.]top, 34.kosdage[.]asia
Registry key	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\SVP7
File Path	C:\ProgramData\KnGoe, C:\user0, C:\ProgramData\8877, C:\Windows\nw_elf[.]dll, C:\Windows\Fatal[.]key, C:\ProgramData\jy[.]lnk

References

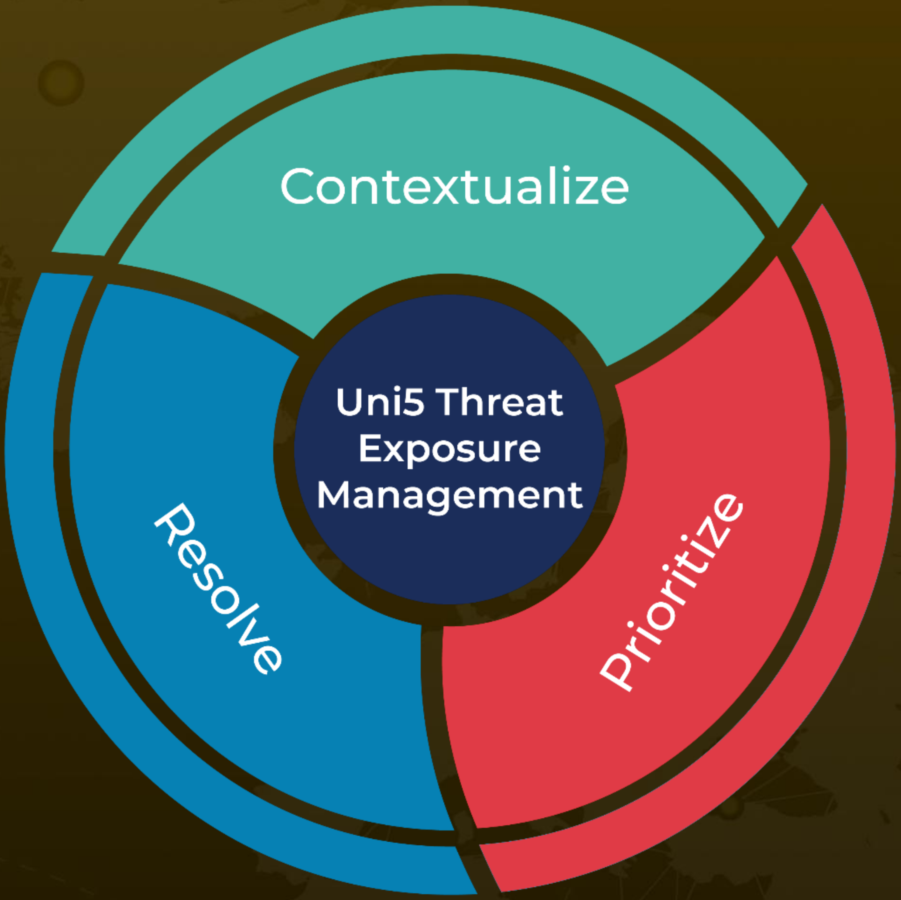
https://ics-cert.kaspersky.com/publications/reports/2025/02/24/fatalrat-attacks-in-apac-backdoor-delivered-via-an-overly-long-infection-chain-to-chinese-speaking-targets/

https://www.hivepro.com/threat-advisory/fatalrats-calculated-cryptocurrency-carnage/

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 25, 2025 • 3:50 AM

More at www.hivepro.com