KPMG Cyber Threat Intelligence Platform

FatalRAT - Leveraging Chinese Cloud Services to Target APAC Industries

TLP : Clear

KPMG. Make the Difference.

FatalRAT is a sophisticated malware linked to cyber espionage campaigns targeting critical infrastructure across the Asia-Pacific (APAC) region. It uses legitimate Chinese cloud services like Youdao Cloud Notes and Tencent Cloud to deliver its payloads through a multi-stage infection. The primary targets include sectors such as manufacturing, energy, IT, and logistics, affecting countries like Taiwan, Malaysia, China, Japan, Thailand, South Korea, Singapore, the Philippines, Vietnam, and Hong Kong.

Initial Access is gained through a phishing email containing a ZIP archive with a Chinese-language filename, containing a first-stage loader. The first-stage loader contacts Youdao Cloud Notes (a cloud service) to retrieve a list of configurators and second-stage loaders, dynamically changing C2 addresses to avoid tracking. The configurator module collects system information, sends it to the attacker's server, and downloads encrypted configuration data from another cloud hosted note, which is used by the second-stage loader to download and execute the FatalRAT payload. To maintain persistence, FatalRAT exploits legitimate software like PureCodec and DriverAssistant, using DLL sideloading to hide in legitimate process memory and evade detection. Once activated, FatalRAT executes keylogging, Master Boot Record (MBR) corruption, data deletion, and installs remote access tools like AnyDesk and UltraViewer, while also manipulating network connections (starting/stopping proxy servers) to enable further attacks. Evasion techniques include detecting VMs or sandboxes, terminating itself to avoid analysis in virtual environments. C2 communication occurs via legitimate cloud services, masking the attack infrastructure and making detection more difficult.

FatalRAT's use of cloud services for cyber intrusions highlights its sophisticated tactics, necessitating robust cybersecurity measures and monitoring to prevent potential threats.

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

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

FatalRAT - Leveraging Chinese Cloud Services to Target APAC Industries

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses

154.39.238[.]101	123.207.79[.]195
107.148.50[.]116	139.199.168[.]63
103.144.29[.]211	123.207.58[.]147
107.148.52[.]241	103.144.29[.]123
107.148.50[.]112	156.236.67[.]181
107.148.52[.]242	123.207.44[.]193
107.148.50[.]113	42.193.242[.]180
111.230.108[.]14	134.122.137[.]252
111.230.91[.]145	175.178.166[.]216
111.230.45[.]217	206.233.130[.]141
82.156.145[.]216	122.152.231[.]146
119.29.219[.]211	114.132.121[.]130

Indicators of Compromise: Domains

novadector[.]xyz	107.kkftodesk107[.]top
xindajiema[.]info	108.kkftodesk108[.]top
34.kosdage[.]asia	109.kkftodesk109[.]top
cloudservicesdevc[.]tk	110.kkftodesk110[.]top
101.kkftodesk101[.]top	microsoftmiddlename[.]tk
102.kkftodesk102[.]top	microsoftupdatesoftware[.]ga

Indicators of Compromise: Hashes

02fb1958a901d7d1c8b60ecc0e59207c
033a8d6ec5a738a1a90dd4a86c7259c8
04aa425d86f4ef8dc4fc1509b195838a

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

FatalRAT - Leveraging Chinese Cloud Services to Target APAC Industries

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
096c34df242562d278fc1578dc31df92
09a50edb49cbb59a34828a37e63be846
0a49345c77da210ab0cd031fda6bc962
0a70ea6596c92fbfb461909ed57503fa
0b20f0ff1aaff4068f99f4db69ba9c1e
0c33792c6ed37452f44ca94ce7385250
142eb5106fcc2f95b7daf37dca970595
15b7990bd006d857ee02c529b45783ac
1c79abe9f52cbe92f042615a9f6b6f10
1e80a8b3f4efb4bb27771d729f5ced85
2026ead0c2366d049ecd5e42ac1b1b07
24ecb197ee73e5b1eef2ded592640cf2
26f0806932dfd029f0fe12e49bb4c799
28231ce260ce66388d58ce536d7ed201
2aa41ae3d3ae789147218652e6593161
2bccd50322afb7a349c163ce9b76bb66
357534f6a2bffa77b83501715e382a94
362fc5799ecef8e9e328cfbf6272c48f
3843ef98a4c7ee88f10078e6a38f15ee
3883957530482a399abb5e1f06e4581f
3b32fc9115c224653f5afba793c0bbef
3ca82fd8d12967c32388ad18e9727fac
44b47fdab8ca3375fe5a875deefa265c
4fc6dbb9beeecb2d60f3fef356c6df01
502054d938a18172a3657aaf2326bcf4
50a5c5a3c07f04d96f5f1968996cfb74

KPMG

KPMG Cyber Threat Intelligence Platform

FatalRAT - Leveraging Chinese Cloud Services to Target APAC Industries

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
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

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

FatalRAT - Leveraging Chinese Cloud Services to Target APAC Industries

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
e0d5b46dffee56c337fdc172ce617850
e32020ab02e11a995effb7781aabd92f
e6ef56c91bd735542775dfef277e0cc7
e8204900e8acb502ca6e008f9532b35e
e91991304abf5d881545bc127e7fb324
eb9419aa5c6fee96defad140450a9633
ec0bdf52c113487e803028dbc52e8173
ed036740be0a8e3203a54edd4d4b735c
f9e461cc83076d5f597855165e89f0db
fdc35392af34ef43291b8f7f959ef501
feb8e6059a234ea689404d3d4336e8af
f80f8a725028bcc09639f7b1ff9439436d974f0bf92871048092eaec5d7458f0
d56471adbfd095d1be1d4b8288d14283efbf6414912064a97423751a69c1427f
8b0fde6e42ba17b0b475bb8dd54b8554cc6682d81b9e632f8890daa9ceefd48d
715138e6cb30bd18cc6afad6322e35f6f1a3d40ac135a1a9bc76cb884508c686
a5ca7b8af70d6e483007c6c9c60b0a2002e150b0f479744989fdd58ad2fc62d3
03e8610b95753eee43179b1ccc3fb72c8595a7d76e9b0290ea765f8e6372d4f9
0555ba582ffdb07a3e93a4d936d2d0d2bd506040f12e5b55e042e82d4bc169ad
fba1b353b063a068bd8a191ce699d335158028a6c94282a27f86b784cd4e94e5
b3c47e48facfb1d6e4f93b1e9b91c1a931f5e491c5ab4aa0fc5c10ed077674b4
149271557eec7f5b17cd046d1f9936dca1654be1edd7835f005fbba145d65b8c
1b6ab4d69332a041109c9a8b7bc1d12dd28566a0614363f7887d9044e4345a2e
e1368e893c44b29acfe7e9e190bbe448deda18d1847ed697b01c17a373207053
efc27a42e520918f83b041f81975e8dbca9916d159dfc41380112c20b43bcd39
c03a524b4e0561141012a6dc17f09bc8d0bf772cf2c94731971a50d67dccb2f4
47835bbb98d4660ffa225000797e22c3cfd48ae43af8ccf0999a760b8c3a92ba