KPMG Cyber Threat Intelligence Platform

FamousSparrow - Expands Operations with SparroWocky Backdoor

TLP : Clear

KPMG. Make the Difference.



FamousSparrow is a China-aligned cyberespionage group active since at least 2019. The group is known for using custom malware and has recently expanded its malware arsenal with the SparroWocky backdoor. FamousSparrow targets government entities, law firms, engineering companies, and the oil and gas sector across the United States, Mexico, Honduras, Azerbaijan, Peru, Panama, Guatemala, Ecuador, Venezuela, and Argentina.

Initial access is gained by exploiting Microsoft Exchange servers, including ProxyNotShell exploit chain, to execute commands and deploy ASPX web shells. Following compromise, the group uses web shells and PowerShell for host and Active Directory discovery, privilege escalation via BadPotato, and additional malware deployment. Multiple backdoors are deployed through DLL side-loading and specialized loaders, including the Trident loader for SparrowDoor and SparroWocky, LogMeIn Hamachi for Deed RAT, and Mofu Loader for Terndoor. For defense evasion, Deed RAT uses two-stage DLL side-loading and in-memory payload decryption, while SparroWocky employs PE header stripping, API hashing, MinHook-based ‘CreateThread’ hooking, call-stack spoofing, and reflective execution with Beacon Object File (BOF) support. Persistence is established via Windows services and Registry Run keys, with Deed RAT masquerading as a LogMeIn Hamachi service, SparroWocky supporting both methods, and Terndoor using a service-based kernel-driver mechanism. For lateral movement, they reuse compromised domain-administrator credentials to access systems via RDP and use Impacket utilities for remote execution. SparroWocky collects system and network information, screenshots, and files for exfiltration, communicating via TLS over TCP with RC4 encryption, HTTP/SOCKS5 proxies, and BOF support.

FamousSparrow’s Exchange server exploitation and backdoor deployment enable persistent access and data exfiltration, but endpoint monitoring and anomaly detection can reduce impact.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Enforce browser extension approval policies through enterprise controls.
- 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

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

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

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

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

KPMG

KPMG Cyber Threat Intelligence Platform

FamousSparrow - Expands Operations with SparroWocky Backdoor

TLP : Clear

KPMG. Make the Difference.



Indicators of Compromise: IP Addresses

38.54.57[.]17	130.94.101[.]82
216.238.92[.]2	27.102.113[.]240
38.60.197[.]55	43.254.216[.]195
38.60.224[.]51	91.148.134[.]115
38.60.241[.]65	140.99.164[.]199
45.131.179[.]24	149.104.87[.]228
77.111.101[.]40	149.104.90[.]203
38.60.209[.]106	216.238.105[.]53
38.60.224[.]235	216.238.106[.]150
38.60.241[.]127	216.238.110[.]120
38.60.241[.]193	216.238.121[.]164
103.85.25[.]166	

Indicators of Compromise: Domain

credits.offices-analytics[.]com

Indicators of Compromise: Hashes

006f22e5e419d349e6459d0d5610105f
59f241ae36899c9283a898bbaec7de5e
357b0ec0fbd81e25f68cbb81444f01f6
54b419c2cac1a08605936e016d460697
fdf677939cb36c29a6b4b139fad5acde
badc4892e4220f8bcf245881347102f1
2a0378d98ca30965157eb7306aeeb494
922c1edb47fba94b548edca863165fb1

Follow us on:
kpmg.com/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

KPMG

KPMG Cyber Threat Intelligence Platform

FamousSparrow - Expands Operations with SparroWocky Backdoor

TLP : Clear

KPMG. Make the Difference.



Indicators of Compromise: Hashes
c40a2f5f25157e6a434602017531d608
8037d1d022ccc182d75b12b1c533df7d
b162026b29d75a870543ad9c044c28c2
fdc44057e87d7c350e6df84bb72541236a770ba2
b9601e60f87545441bf8579b2f62668c56507f4a
cc350ba25947b7f9ec5d11ea8269407c0fd74095
1b06e877c2c12d74336e7532bc0ecf761e5fa5d4
e2b0851e2e281cc7bca3d6d9b2fa0c4b7ac5a02b
23e228d5603b4802398b2e7419187aef71ff9dd5
873f98caf234c3a8a9db18343dad7b42117e85d4
44f0a22b143b79fa760bf31e14c8fff714c8a2a1
76c430b55f180a85f4e1a1e40e4a2ea37db97599
c26f04790c6fb7950d89ab1b08207ace01efb536
bb2f5b573ac7a761015daad0b7ff03b294dc60f6
e0ff727c5feb3352f0bb6df91bcf2b3100203e5777c8b49b3913fcec0dbbd260
03241adc63e5a204dcec26915f4df076a8121fa7827edfdc36b75e4803c2f019
0e74d57f572e384ad179ad8aa094cbdc92a6abbcc77eeb658fc05743ffd94e68
d53346b5c8c6c76e7bc0407410a58328a1e214a4d359e558380963d29a35f71b
222d68c03d96d230bc3829e86be8821f32960375b70388028a705a4986b8d9c6
90af57e976aea91030579b9761e5265251986b707550ca1b793191e2818bad92
67d7962eaec2c785d7a6db8502c74e6ccd95445d366e370fa9fe6743d68cb42c
e0b6f8535e19f0a4938e3317de0c4493ecea17aa906fd0454805ba2086cbf3a8
773635768e738bec776dfd7504164b3596e5eee344757dd1ac9a1ad19b452c86
d057034675befc1b4c2ae4132c4d169201c9abfbae79181185d45ca6721e43cc
8dfaa1f579de14bca8bb27c54a57dd87646a835969766ca9ddb81ecd9329f4e4

Follow us on:
kpmg.com/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.