KPMG Cyber Threat Intelligence Platform

FOG Ransomware: The Silent Storm of Cybercrime

TLP : Clear

KPMG. Make the Difference.

The FOG ransomware group, first seen in May 2024, primarily targets education, recreation, travel and manufacturing sectors in USA. It has variants for both Windows and Linux, including specialized versions for virtual environments. The group exploits known vulnerabilities in applications and purchase compromised credentials from Initial Access Brokers to gain entry. Using a double extortion method, they pressure victims into paying the ransom.

Access to victim networks is gained through the exploitation of compromised VPN credentials and by using 'pass-the-hash' techniques on admin accounts. Custom PowerShell scripts are deployed to extract browser passwords, thereby enabling privilege escalation. RDP is used to connect to Windows servers, and tools such as FileZilla and reverse SSH Shell are employed to maintain persistence within the network. Security measures, including Windows Defender and other processes, are disabled on compromised machines. Additionally, Windows API calls are utilized to gather system information and terminate further processes. Internal connection attempts are initiated on common ports for network scanning with tools like Nmap. Additionally, SMB enumeration tools such as SharpShares and SoftPerfect Network Scanner are employed to gather detailed network information. Multiple RDP connections are established to new clients, using devices as pivots to propagate deeper into the networks. High read and write activity is observed, with internal drive files being changed to the ".flocked" extension upon encryption. Legitimate remote access tools, including AnyDesk and SplashTop, are repurposed for C2 communication. Tools like 7-Zip and WinRAR, along with third-party cloud services such as MEGA, are used to facilitate the exfiltration of stolen data.

Fog ransomware's exploitation of VPN credentials and admin accounts emphasizes the importance of securing access points and constant threat surveillance.

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

Chandra Prakash
Partner
T: +91 99000 20190
E: chandraprakash@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

FOG Ransomware: The Silent Storm of Cybercrime

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
5.230.33[.]176	85.209.11[.]254
85.209.11[.]27	77.247.126[.]200
85.209.11[.]227	

Indicators of Compromise: Hashes
617d79c02ebac68b613d5b7cdbf001fd
07c6b4756715d73304ec0ebc951dddad
4fdabe571b66ceec3448939bfb3ffcd1
6a58b52b184715583cda792b56a0a1ed
4b69e562609d08ce8dfe703b9077e33b
04d3e794624a82228a7e683fdf22e182
16659ae52ce03889ad19db1f5710c6aa
24f6faa5d2e9c8fb15ae0c936bfa4545
46c17c999744470b689331f41eab7df1
4ebeb72c7da644a296a0026c061db51d
5c336de3b3d794322ad9e5915e3a509f
6eeefcb85673c14201d024b6e6ac6258
76ea3b599daf05d19ca7bfb94497347d
1a638556de77369151839bf7a570d972410360e3
7c680a87233ff7e75866657e9c1acf97d69f6579
f7c8c60172f9ae4dab9f61c28ccae7084da90a06
507b26054319ff31f275ba44ddc9d2b5037bd295
e1fb7d15408988df39a80b8939972f7843f0e785
83f00af43df650fda2c5b4a04a7b31790a8ad4cf
44a76b9546427627a8d88a650c1bed3f1cc0278c
eeafa71946e81d8fe5ebf6be53e83a84dcca50ba

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

FOG Ransomware: The Silent Storm of Cybercrime

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
763499b37aacd317e7d2f512872f9ed719aacae1
3477a173e2c1005a81d042802ab0f22cc12a4d55
90be89524b72f330e49017a11e7b8a257f975e9a
114b74e926913bb0a588e671025f9eb38e8b854b
66b814fe3be64229e2cc19f0a4460e123ba74971
17f85d25f0f0c15a164eb11a34f498268677dcb0
b8a63127df6a87d333061c622220d6d70ed80f7c
6f94ea0eae2664c8341265d62ff7d871da702a76
5256262a417e9a29fe23e8cca09782c7a3532fc9
dd3bbad1b014f8d8e9f981ac0deb9f2f343c5cf4
4b0f18a0acc434df0907dab5be2de1ca70e3560a
b83a105dda4806f7ac5e9f3b6546829b37d42d85911d1c4487b1e95bfea91e9d
46f533007fb231d0b0af058a0997ab5e6b44a1b02ae327621f04fdc4b2e18964
e672608045263234 84f564eebeb6c99ed021b960b899ff788aed85bb7a9d75c3
9d00158489f0a399fc0bc3ce1e8fc309d29a327f6ea0097e34e0f49b72a85079
8b9c7d2554fe315199fae656448dc193accbec162d4afff3f204ce2346507a8a
d0c1662ce239e4d288048c0e3324ec52962f6ddda77da0cb7af9c1d9c2f1e2eb
e11e7db705a11f8ca250d8d6826371e550b3214757f5bb9b648c7b0fad09294b
db3d0484228ed14ad8d3763f4880d36024fb27b189c91720ff147b92d46bcb5a
0b1866b627d8078d296e7d39583c9f856117be79c1d226b8c9378fe075369118
bd3f01e7c100422a6faae60d76da16158f6d8b3868d474e81fd657ec3c0127ef
c5b5def1c8882b702b6b25cbd94461c737bc151366d2d9eba5006c04886bfc9a
de451e233072b0d34acecf04ddc38bcad61b56a1e0218041ca0a80ad752baccf
bce29ef3b95306cb7b304fb8c3039be7157356d9f9d4e7e1c6bfbf02a117f48f
b75fdee208d2834ab147dacb51f4e7d70e44457c8b639048fe67b252b8d61f1f
8990ae8c5d6bdc7dd63162d50eb8f2789957a4aa72d908e6107f36d7b1486441