KPMG Cyber Threat Intelligence Platform

Gentlemen Ransomware - Rapidly Expanding Global Cyber Threat

TLP : Clear

KPMG. Make the Difference.

The Gentlemen ransomware group, identified in August 2025, has rapidly emerged as a sophisticated and adaptable threat actor. Within a short timeframe, it claimed over 30 attacks across 17 countries, primarily targeting manufacturing, healthcare, insurance, aviation, and consumer services. The most affected regions include Thailand, the United States, India, Mexico, and Colombia.

Initial access is obtained by exploiting internet-facing services and abusing compromised FortiGate administrative accounts. For reconnaissance, the group scans networks using tools such as Advanced IP Scanner and Nmap and executes enumeration scripts to identify domain user accounts. Lateral movement and remote execution are facilitated through legitimate administrative utilities like PsExec, PowerRun, and PuTTY to transfer and execute payloads across systems. Privilege escalation is achieved by running components with elevated privileges, granting full control over the compromised environment. To evade detection and maintain persistence, the threat actor deploys kernel-level anti-AV utilities, disable Microsoft Defender's real-time protection, configure exclusions, neutralize EDR, and clear telemetry data and event logs. For propagation, Group Policy Objects are modified to distribute a password-protected payload via NETLOGON/SYSVOL directories, ensuring domain-wide deployment. Sensitive data is staged and exfiltrated over encrypted SFTP using WinSCP, while remote tools such as AnyDesk are abused as persistent, encrypted command-and-control channels. Finally, they disable critical services, delete shadow copies and forensic traces, encrypt files with the ".7mtzhh" extension, and drop ransom notes titled README-GENTLEMEN.txt to maximize operational impact.

With a clear focus on compromising Windows-based environments the group employs a blend of custom-built anti-antivirus tools and advanced evasion techniques.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Patch your Windows environment with the latest version asper the OEM and secure it 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

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

Gentlemen Ransomware - Rapidly Expanding Global Cyber Threat

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Address

104.86.182[.]8

Indicators of Compromise: Hashes

a88daa62751c212b7579a57f1f4ae8f8
408dd6ade80f2ebbc2e5470a1fb506f1
df249727c12741ca176d5f1ccba3ce188a546d28
c12c4d58541cc4f75ae19b65295a52c559570054
c0979ec20b87084317d1bfa50405f7149c3b5c5f
e00293ce0eb534874efd615ae590cf6aa3858ba4
7a311b584497e8133cd85950fec6132904dd5b02388a9feed3f5e057fb891d09
4c82fbafef9bab484a2fbe23e4ec8aac06e8e296d6c9e496f4a589f97fd4ab71
0002acdcbce29a01357d13dd7025b7b0d656763428b1297b950394fdd068a096
0008aaa853001623ba1e2084afbe27fed8faebad8755cb9584ce9f75b73c5a53
0019ee55db44a45c1d221e50e55d660eaeb24e1b1072087e1346903921cd8229
003381c91e50f1a2b8be7dc1a6bfaa5af12ffe4d617e4c43897f3e0d2800d0ef
0043a98418e2588dbb2a410574b6dec54a52608e83c7d4e08ea06d683f2c9913
005e8301b497a75484acfbc10a49d2e45b0bb090310972afc86d052dd3d1a339
00694fdee131bb692add8f02da2ee2fc147ab2c09ecf7321fad3207976494939
006ac1771aaacf02c44cdcde5a2913a07a6c82f30e84b94eceb2100cc0ca0298
00a93232fb64496ab7c8b3b1a250a61e3ca936a7b797b0f2c7dc16d1c78a54bb
00b6a47efb9049283473fe8296ee2488b790a3ba8133c4a7586aeaf9e685a9a7
00ce99391bba9ffeb9ae3baf206eea3be99d2e0cc433a9ce8a37e9f4e4f2bc5b
00e47ef59e8ce07ae591bb87f693f97955a8e2a52c32668153303943859aaaf6
00ed5f41cc3b8812c2c2cc7e3b733e19a3809076b14e4bb30c0b9f0668a1c1b1
00fd5303503ef3d91496fb14441061929fcc8651ba2abecacde86ff54ef06d07
010d6d3854182d0dfea4293eca8849906bf08718bb8781238af657f1fbde2f0a

KPMG

KPMG Cyber Threat Intelligence Platform

Gentlemen Ransomware - Rapidly Expanding Global Cyber Threat

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
019d420f4cc961d6a7c632e8be5f158eed94c84906dc61923e50c18724dba8af
01bfc830626191cffe8b35a2e61b8545c38203674a4f8bf6805d89a50434ecf5
01ee929fefc2c4fc999d231c7342996d228dce5e514a16a56abd81d3c533a8b8
0208ef60699014a57b58eac363973dbe333b94aa430c1b1443f91615a941bfce
0238e0341dc7818d1a61f7f1017b659b7bc82f02e7945eaf9d0ab7889677b559
023bbab9e147bbfad6e19b76f3f35bf44081c69c3c91e3d1587d3e639f7847c3
023cc6b05dd940ed3faabfa2fc1c1f6b49fc2a122a59ca2593ebf0884aea7017
0255f7d0611bdf9ae573628007a427931f8f8d04fdc857689785e63180a13fc6
026f058fe290063a612c44cac98ca9d4a2ebc6ed06e1d4c16c52d1169407f0dd
0272a75a97e742b13715a8fc69aa292760390822578500dcb73fcd5ca2b7c7e7
02ce33e0afb75d2fc969c555722d71487ce5b23a058845c94861e45866bc2f20
03391a28d58fe8a2eda9fd9302197ff086822a78cd717532962aa686844f3729
03437abbfa60bc0e268ea8098a5e80585ee8b7842b470092471bc6434d39666c
048cbd8e760a23edb4535193dcd1216cdc9ae223a9883a30ef07b9b346a07ea9
0a0cf5fdc45897e0905d0e13d2eac30e1c2804b41e2fc736df0a324e88d34746
0121141e055dc5d174d2d3079ff957db4d8b17f969134bb8ca61a491dd41b58d
0152552c9656b47fdb05dd30b8f535a7232884ee4c599780d3ee194d5c7fb923