# KPMG Cyber Threat Intelligence Platform

**Medusa Ransomware – Global Cyber Threat Exploiting Vulnerabilities**

**TLP :** Clear

**KPMG. Make the Difference.**

**Medusa ransomware, identified in 2023, is a sophisticated ransomware-as-a-service operation that primarily targets Windows environments. With its advanced evasion and encryption techniques, Medusa poses a formidable threat to various sectors, including high technology, education, manufacturing, healthcare, and retail. This opportunistic group has a global reach, impacting organizations in countries such as the U.S., U.K., France, Italy, Spain, India, and many others worldwide.**

Medusa often gains access by exploiting known vulnerabilities in public-facing assets or applications, such as the Fortinet EMS SQL injection vulnerability (CVE-2023-48788). This allows the attacker to manipulate queries, execute remote code, and create a webshell for payload exchange. PowerShell scripts are used to run commands, exfiltrate data, and deploy ransomware. The script terminates services, uses TOR links for data exfiltration, and performs encryption. Persistence is established through compromised RMM tools such as ConnectWise, PDQDeploy, and AnyDesk, and registry keys are modified for startup execution. Discovery processes validate legitimate programs to mask compromised iterations, and transfers are done via bitsadmin. Credentials are obtained from LSASS, and tools like bitsadmin and PSExec are used for transferring malicious files between hosts. Kernel drivers protected by Safengine Shielden are dropped to target and terminate security products, and techniques such as WMI are employed to delete backups. Asymmetric RSA encryption is used to encode targeted files and directories, and files are renamed with extensions like .medusa or .mylock, excluding crucial system files to ensure some utilities remain functional.

Medusa's advanced encryption techniques, combined with its comprehensive attack strategies, underscore the need for robust security measures and proactive threat management.

### 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

## Medusa Ransomware – Global Cyber Threat Exploiting Vulnerabilities

**TLP :** Clear

**KPMG. Make the Difference.**

| Indicators of Compromise: IP Addresses | |
|---|---|
| 176.123.9[.]68 | 198.54.123[.]60 |
| 194.28.50[.]70 | 103.131.70[.]228 |
| 45.61.185[.]34 | 193.178.169[.]19 |
| 207.188.6[.]17 | 91.219.236[.]204 |
| 103.217.41[.]10 | 172.64.154[.]227 |

| Indicators of Compromise: Hashes |
|---|
| 5d5027305deb2cb2fd263fea9a6011af |
| 35dfc1fcb06fe31264a3fc7ff307e166 |
| 8cd11f34d817a99e4972641caf07951e |
| 47386ee20a6a94830ee4fa38b419a6f7 |
| e4b7fdabef67a0550877e6439beb093d |
| a57f84e3848ab36fd59c94d32284a41e |
| 08278e867322735de9e75f59b539426e |
| 120e36c2428a4bfe9f37b977f698fa39 |
| 217b5b689dca5aa0026401bffc8d3079 |
| 3030943c7e5f2c7b710c416f7d979c25 |
| 30e71d452761fbe75d9c8648b61249c3 |
| 312e41aa5901f6e00811de343627d418 |
| 38b1cdb61aff9b5096cc971cbb3159e0 |
| 412568f078ec521bdba6ae14b9f36823 |
| 4293f5b9957dc9e61247e6e1149e4c0f |
| 4536297338323c00783fdceabf8d36bf |
| 47d222dd2ac5741433451c8acaac75bd |
| 4984d9af56c39a161b627e019ed2604d |
| 6701070c21d3c6487c3e6291f2f0f1c9 |

**Follow us on:**
**kpmg.com/in/socialmedia**

KPMG

# KPMG Cyber Threat Intelligence Platform

## Medusa Ransomware – Global Cyber Threat Exploiting Vulnerabilities

**TLP :** Clear

**KPMG. Make the Difference.**

| Indicators of Compromise: Hashes |
|---|
| 7405efcdd3e931cde430317df1c00131 |
| 7b9dbd1a611dc4d378607e5f50b23654 |
| 7ecc2ed7db7bbb6dc794f29feb477c8c |
| 82143033173cbeee7f559002fb8ab8c5 |
| 84b88ac81e4872ff3bf15c72f431d101 |
| 858ffbe870a7454c4a59f889d8d49169 |
| 9353a3fa46ce13ea133cfab51c8cbd7a |
| 99a1f6e096dc79b1bc1adbefaa0cd9c5 |
| acb0fde71fa3d57261e8eac9c3da88ab |
| ad182ac22ee9e8075a324fcee2038108 |
| d82b27fdcc3a63f2ab0c46c5a3caef0a |
| d8550fb34f73ccc47b02c51b138b11dd |
| db5e29c0729486ba3833426093652451c5fca9b5 |
| ee4575cf9818636781677d63236d3dc65652deab |
| 042ce9ab1afe035e0924753f076fcb20de0d1a1d |
| 4d5992de4601c4306885c71b0ba197184bb69221 |
| 0fe01b51818c6c7c1556bffb43976a5264b3cc43 |
| 1bbda98348f0d8d58c6afccd50a76321d02919f9 |
| 86d92fc3ba2b3536893b8e753da9cbae70063a50 |
| 9f5a9707ba0fcd5b695be131dedfdfe3b2d359d9 |
| a35dd292647db3cb7bf60449732fc5f12162f39e |
| 0c1ce8017cfcc24927fff1b00606e8c83c4ebfa7 |
| 78bcffb9ee6a7d29e18f66c0138aa3fd3a9225fa |
| 3e5a80fe286834f6d5f0aaf014a420ec40ebad7d |
| c87cd85d434e358b85f94cad098aa1f653d9cdbf |
| f968e5c2314e198f4c0c2a4596d13ee1b6482330 |

KPMG

# KPMG Cyber Threat Intelligence Platform

## Medusa Ransomware – Global Cyber Threat Exploiting Vulnerabilities

**TLP :** Clear

**KPMG. Make the Difference.**

| Indicators of Compromise: Hashes |
|---|
| 7ad1bf03b480ebd2b85b2bc5be4b9140b0ce6d4d |
| 02a0ea73ccc55c0236aa1b4ab590f11787e3586e |
| eef59fd5b71487448bfd44270d909b1441cd537b |
| 7219f91bd5fb94128159d18956e1bd9132bf10e0 |
| 69c1527fbd840eee87821328ecf1453984ddc73e |
| e5162ede86712df1e602cbf1ca8b205ab113a931 |
| 855b8aeb4160641ecea5710174086ee74d3e42c1 |
| e03aedb8b9770f899a29f1939636db43825e95cf |
| 0823d067541de16325e5454a91b57262365a0705 |
| fc31989737dcf21b73bc0956220852dfab2cb549 |
| f3e66237577a690ee907deac9ffbf6074a85e7a5 |
| 0bcf20885b50d64a876e7b46497b22689cb93d33 |
| da237c7bad052c9cb99cbab75b8bc2bdb23b3f65 |
| 212e3254099967712c6690be11ae9d65a8966ffa |
| 4bc8175c5fbe088297ec4eb3fa26acd8927530e2 |
| 657c0cce98d6e73e53b4001eeea51ed91fdcf3d47a18712b6ba9c66d59677980 |
| 736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270 |
| 7d68da8aa78929bb467682ddb080e750ed07cd21b1ee7a9f38cf2810eeb9cb95 |
| 9144a60ac86d4c91f7553768d9bef848acd3bd9fe3e599b7ea2024a8a3115669 |
| f30d2204814204a2295cd5c703591e81cdfe63ee04b0e45d7ed76fe0db4a711b |
| 7593b85e66e49f39feb3141b0d390ed9c660a227042686485131f4956e1f69ff |
| fb07649497b39eee0a93598ff66f14a1f7625f2b6d4c30d8bb5c48de848cd4f2 |
| 50a334ff766b053dee01ee1e410eebc5a24144517c59f9317ec47be9b70f6c48 |
| e70a261143213e70ffa10643e17b5890443bd2b159527cd2c408dea989a17cfc |
| 746c79b5b6030091c37251939690eee31d023de5303544b46032bf89580806e5 |
| 81ca80c8275b0fdfeef2a816a7bf567f8e9a145b03ab96138c527af5c79bbec2 |

KPMG

# KPMG Cyber Threat Intelligence Platform

## Medusa Ransomware – Global Cyber Threat Exploiting Vulnerabilities

**TLP :** Clear

**KPMG. Make the Difference.**

| Indicators of Compromise: Hashes |
|---|
| bae48fe24d140f4c1c118edbfaee4ab6446c173a0d0b849585a88db3f38f01b8 |
| b1e97cd1ae60622ae83c56c9d15895a24405f949e4bb337e86159bcdd93e138e |
| e2c2a80cb4ecc511f30d72b3487cb9023b40a25f6bbe07a92f47230fb76544f4 |
| a8b84ab6489fde1fab987df27508abd7d4b30d06ab854b5fda37a277e89a2558 |
| 9814f9d8a8b129d745d74d3069da69aaf4187146327cb615108e9ed1b5d3c58e |
| ed139beb506a17843c6f4b631afdf5a41ec93121da66d142b412333e628b9db8 |
| fd24ff7e838fea836079c4554254768abdce32c4f46148c609a5a676c9e71103 |
| 104ffe0cc10413b8c3dd04fdc921f07c3cc55efba9a63ccdccf45e4012151c5f |
| fc12de55f162cd0645e6f7299f6160d1a3b4c3a665efaf4f8bd891d8139d159e |
| 40fbb2f6850213af595dd27231b06c498f87e62b50e8b883976900cc1afa75e1 |
| abe330ec7e157293afee2d96489165d3aa0ed9a59252ecf4f3acfa3205ca9d15 |
| 4ae110bb89ddcc45bb2c4e980794195ee5eb85b5261799caedef7334f0f57cc4 |
| 4d4df87cf8d8551d836f67fbde4337863bac3ff6b5cb324675054ea023b12ab6 |
| 8597f458f1dcc5ecdf209d9c98b1f72c2fce2486236a3ae73adbe26fb6f9c671 |
| 8b9bdc5cf5534d377a6201d1803a5aa0915b93c9df524307118fd61f361bdba2 |
| aae247b1fe640f2c96cbfa508d18d475f3e4c8b29fa117a31d17ba0c4e5caa48 |
| b1672fd7ef5f4419f5c74a0829645087e92437f766042bfa3325a2a96610f271 |
| d33b09ddee82c5c439cb0c66e5c1dee9ad5259e912a3979b31c66622fb9d47ea |