# KPMG Cyber Threat Intelligence Platform

## Rhysida Ransomware - Infecting Healthcare Organizations

Rhysida, a relatively new Ransomware-as-a-Service (RaaS) group emerged in late May 2023, gained notoriety by targeting the Chilean Army, signaling a trend of Latin American government institutions being in the crosshairs of ransomware groups. The group verified its claims by leaking stolen files. Initially focused on Education, Government, Manufacturing, and Technology sectors, Rhysida has since expanded to include Healthcare and Public Health, prompting a warning from the U.S. Department of Health and Human Services in August 2023, highlighting its growing significance in the ransomware landscape.

Initial access to a victim's network is achieved through phishing emails. Post access, it deploys a second-stage payload as Cobalt Strike or SystemBC to assist in Discovery & Lateral Movement within the network. To ensure persistence, SystemBC installs a registry key named 'socks' to execute on startup & set up a firewall rule to allow outbound traffic to another server. They utilize 'NTDSUtil' to create a backup of 'NTDS.dit' in a folder named temp_l0gs. Later, they enumerate domain admin accounts to seek privilege escalation. To evade detection and hinder recovery efforts, they use a PowerShell script called SILENTKILL to disable security software, alter local settings, modify the local Firewall, and delete system backups. They employ various techniques for lateral movement, including PsExec, RDP, and Windows Remote Management (WinRM), with the goal of deploying the ransomware payload. Upon deployment, Rhysida scans, lists all local drive files on compromised system & then proceeds with encryption using a 4096-bit RSA key and ChaCha20 algorithm.

Rhysida's unique tactics highlight ransomware innovation. Proactive defense strategies, such as network segmentation, strong authentication and continuous monitoring are essential for mitigation.

### 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.

### The 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 |

## Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471


**Atul Gupta**
Partner, Head of Cyber Security,
KPMG in India
**T:** +91 98100 81050
**E:** atulgupta@kpmg.com

**B V, Raghavendra**
Partner, KPMG in India
**T:** +91 98455 45202
**E:** raghavendrabv@kpmg.com

**Sony Anthony**
Partner, KPMG in India
**T:** +91 98455 65222
**E:** santhony@kpmg.com

**Chandra Prakash**
Partner, KPMG in India
**T:** +91 99000 20190
**E:** chandraprakash@kpmg.com

**Manish Tembhurkar**
Associate Partner,
KPMG in India
**T:** +91 98181 99432
**E:** mtembhurkar@kpmg.com

KPMG

# KPMG Cyber Threat Intelligence Platform

## Rhysida Ransomware - Infecting Healthcare Organizations

| Indicators of Compromise: IP Addresses |
|---|
| 209.197.3[.]8 |
| 23.216.147[.]64 |
| 23.216.147[.]76 |

| Indicators of Compromise: Hashes |
|---|
| 0c8e88877383ccd23a755f429006b437 |
| 1e256229b58061860be8dbf0dc4fe67e |
| 41948cd77a6cf817b77be426968a6ad3 |
| 59a9ca795b59161f767b94fc2dece71a |
| 4ef0160b3eb114a94aeedd0bb5716058 |
| 44c7d18633b5741db270a6bd378b6f3c |
| c9a5e675dbb1f0ce61623f24757a1c72 |
| fbbb2685cb612b25c50c59c1ffa6e654 |
| 599aa41fade39e06daf4cdc87bb78bd7 |
| db50086280878a064a1b5ccc61888bcd |
| 67edfff8250487d97f403c74fed85388 |
| fac561bb0f072d29fe6f8ee6072c905a |
| 7dd4de113a97c638518f01760ff4f03c |
| 2b825ea77e240d2ab6b6695a602cb07c |
| 26f41a46d0addde100bb9512a130de5e |
| 69b3d913a3967153d1e91ba1a31ebed839b297ed |
| 338d4f4ec714359d589918cee1adad12ef231907 |
| 7abc07e7f56fc27130f84d1c7935a0961bd58cb9 |
| b07f6a5f61834a57304ad4d885bd37d8e1badba8 |
| 10cb9fa20dec34fa7ceab8248a0deef8ecb7bcef |
| c1d41db1662289870d9b0172c53612b8a346a0e3 |
| 560a64721d5a647ffae76febdb6f99bf356dae79 |
| 134c25e1b864f14d25e06d29cce0ca0b90968b44 |
| 2543857b275ea5c6d332ab279498a5b772bd2bd4 |
| eda3a5b8ec86dd5741786ed791d43698bb92a262 |
| f20bc8af34dd292e017caf4d42dd95d0cdc08792 |
| da29dc6bd9ba38d11d46665e42bed7d5c35f48fc |
| 39649fa040a3c6894758016a65afec7b6acd4017 |

KPMG

# KPMG Cyber Threat Intelligence Platform

## Rhysida Ransomware - Infecting Healthcare Organizations

| Indicators of Compromise: Hashes |
| --- |
| ae6eb3cce06f666934e03dd46269526e56aff3b1 |
| bef7719a8a98131b8bdf885895b5d1c3f9d089ad |
| a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6 |
| d5c2f87033a5baeeb1b5b681f2c4a156ff1c05ccd1bfdaf6eae019fc4d5320ee |
| 2a3942d213548573af8cb07c13547c0d52d1c3d72365276d6623b3951bd6d1b2 |
| 250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738546c2ab1 |
| 1a9c27e5be8c58da1c02fc4245a07831d5d431cdd1a91cd35d2dd0ad62da71cd |
| 258ddd78655ac0587f64d7146e52549115b67465302c0cbd15a0cba746f05595 |
| 0bb0e1fcff8ccf54c6f9ecfd4bbb6757f6a25cb0e7a173d12cf0f402a3ae706f |
| f6f74e05e24dd2e4e60e5fb50f73fc720ee826a43f2f0056e5b88724fa06fbab |
| 6903b00a15eff9b494947896f222bd5b093a63aa1f340815823645fd57bd61de |
| 3bc0340007f3a9831cb35766f2eb42de81d13aeb99b3a8c07dee0bb8b000cb96 |
| 67a78b39e760e3460a135a7e4fa096ab6ce6b013658103890c866d9401928ba5 |
| 3d2013c2ba0aa1c0475cab186ddf3d9005133fe5f88b5d8604b46673b96a40d8 |
| 2c5d3fea7ad3c9c49e9c1a154370229c86c48fbaf7044213fd85d31efcebf7f6 |
| 3518195c256aa940c607f8534c91b5a9cd453c7417810de3cd4d262e2906d24f |
| 0050a69d6e93eddcd1ea4b7e951945f8970e5700d9436238bde7f63d757988ae |
| 00d0d67877a78891d2b70d20450bca5c52b4911c852c458b80991d5bd472a82c |
| 02a3ff008c61f77a3f626016beb1bb527a9940b19a020bfa50bbe3488bd052f9 |
| 05ae37ff06562e9c318a8553987fa5ab65506189d9a2f8ffe4ebef4a71b3d6c8 |
| 06b7c353b14dda458dc0f34a53aa4a124d77a37432d2f280bc206d0505f8d013 |
| 08c8ba824eedb463270667ab4dcce7bdfdc661ec101fd27162cebc19611c20f1 |
| 0b321c2cf9df8de0752e05e75d77ba90ef21c45a980d23d9f51ab57d4f020daa |
| 0bb5a96296d9e27d072ee5654be8b2deed6a61e42672847c2f7d07fd1e7ede4b |
| 0dc3b4ce6a5cc67459d2eb0e914bfd030aa26598b8d6ee3869dee5f59cf7d09b |
| 0f503ea8dde3d74efc87fbf8ee3470d12bf265ea764d834498987f8d4aee7a48 |
| 10315b3804adb9d143db079d6c7d2266dc2f2a6bf89e9e5706cd0ff7b64bf561 |
| 10f35ede1a006aa64d4d427aeea6520096acf83878fae4a29effcf3b7f4bcb3b |
| 11a675db46e1db74841eac1b9a94c955efa17787946af6888ffa7acecf9e5f25 |
| 12f332269f09dbb76e451bde9d2b1a9658f0a4b07dd6dc76a3c269ee5af3cf62 |