



# KPMG Cyber Threat Intelligence Platform

## Royal Ransomware – Stopping at Nothing



Royal Ransomware, formerly known as Zeon, is a highly advanced malware strain that emerged in early 2022 that is operated by Dev-0569 group. From using Blackcat’s encryptor, Royal has evolved to use its own ‘Zeon’ encryptor having major resemblance with tools of Conti. The group has been targeting multiple countries around the globe, across sectors spanning transportation, critical manufacturing industries, technology, education, healthcare, and government sectors.

Royal gains initial access through techniques like callback phishing, malvertising, exploiting vulnerabilities of vSphere & other public facing services and exposed RDP. Tools like PCHunter, Process Hacker, GMER, or PowerTool are then used to kill security solutions. Remote access software such as AnyDesk, LogMeIn, and Atera are leveraged to maintain persist access to the victim’s network. Network and system discovery tools allow Royal to collect information about Active Directory and other systems. Cobalt Strike and Qakbot are used as C2 to deliver malware, payloads, other additional tools including dual use agents. Connectwise, Splashtop, etc were leveraged for lateral movement and to execute malicious processes. Rclone cloud web service is used to exfiltrate data before proceeding to file encryption over SMB. Execution requires a 32-character “id” argument along with “path” & “ep” arguments for target encryption path and encryption percentage. Finally, volume shadow copies are deleted via “vssadmin” tool to hamper recovery.

Royal ransomware is on a massive hacking spree, getting ranked among the most active and dangerous ransomware campaigns of 2022. Further, with Royal expanding its scope of attack to target ESXi servers by abusing multiple CVEs, organizations must ensure that latest patches are applied and secure exposed systems and services.

### 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: raghavendrabbv@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

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 endeavor 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.

© 2023 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.

#KPMGjosh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia





# KPMG Cyber Threat Intelligence Platform

Royal Ransomware – Stopping at Nothing



## Indicators of Compromise: IP Addresses

5.44.42[.]20	45.8.158[.]104
186.64.67[.]6	105.69.155[.]85
41.97.65[.]51	181.141.3[.]126
134.35.9[.]209	197.158.89[.]85
196.70.77[.]11	197.204.247[.]7

## Indicators of Compromise: Domains

sombrat[.]com	parkerpublic[.]com
gororama[.]com	softeruplive[.]com
ciborkumari[.]xyz	altocloudzone[.]live
myappearinc[.]com	tumbleproperty[.]com

## Indicators of Compromise: Hashes

df0b88dafe7a65295f99e69a67db9e1b
b93fa14627f73de3274ba15503c916b0
2f5d60c2475b723526fbdadef55c3c7
9fb7d7a1f50541917972115b7d8265b4
60bf4ae8cc40b0e3e28613657ed2eed8
fb8535e2bd80cc8044c52a3ed82d390d
7cf4b655453d28f246c815a953f48936
4f926252e22afa85e5da7f83158db20f
5a24676210bd317520fe30d048c9a106
cb8a14388e1da3956849d638af50fe9d
bd1c7369830ebd781ed5eade64f8f9e4
5cae01aea8ed390ce9bec17b6c1237e4
50cc3a3bca96d7096c8118e838d9bc16
afd5d656a42a746e95926ef07933f054
219761770ad0a94ac9879a6028bd8e55
585b05b290d241a249af93b1896a9474128da969
41a79f83f8b00ac7a9dd06e1e225d64d95d29b1d
a84ed0f3c46b01d66510ccc9b1fc1e07af005c60
c96154690f60a8e1f2271242e458029014ffe30a
65dc04f3f75deb3b287cca3138d9d0ec36b8bea0



# KPMG Cyber Threat Intelligence Platform

Royal Ransomware – Stopping at Nothing



## Indicators of Compromise: Hashes

db3163a09eb33ff4370ad162a05f4b2584a20456
b286b58ed32b6df4ecdb5df86d7d7d177bb7bfaf
a0ee0761602470e24bcea5f403e8d1e8bfa29832
4f65118960bd8bcc744d62e6f464f8bc82c85a9e
3a80a49efaac5d839400e4fb8f803243fb39a513
04028a0a1d44f81709040c31af026785209d4343
554085b1fef4b90c8679a9d10a2c758f10563a79
8a983042278bc5897dbcd54d1d7e3143f8b7ead553b5a4713e30deffda16375
8a99353662ccae117d2bb22efd8c43d7169060450be413af763e8ad7522d2451
be030e685536eb38ba1fec1c90e90a4165f6641c8dc39291db1d23f4ee9fa0b1
b8c4aec31c134adbdb8aad65d2bcb21cfe62d299696a23add9aa1de082c6e20
4a9dde3979c2343c024c6eeeddf7639be301826dd637c006074e04a1e4e9fe7
4cd00234b18e04dcd745cc81bb928c8451f6601affb5fa45f20bb11bfb5383ce
08c6e20b1785d4ec4e3f9956931d992377963580b4b2c6579fd9930e08882b1c
f8cff7082a936912baf2124d42ed82403c75c87cb160553a7df862f8d81809ee
d47d4b52e75e8cf3b11ea171163a66c06d1792227c1cf7ca49d7df60804a1681
216047c048bf1dcbf031cf24bd5e0f263994a5df60b23089e393033d17257cb5
19896a23d7b054625c2f6b1ee1551a0da68ad25cddb24510a3b74578418e618
82f1f72f4b1bfd7cc8afbe6d170686b1066049bc7e5863b51aa15ccc5c841f58
74d81ef0be02899a177d7ff6374d699b634c70275b3292dbc67e577b5f6a3f3c
342b398647073159dfa8a7d36510171f731b760089a546e96fbb8a292791efee
f484f919ba6e36ff33e4fb391b8859a94d89c172a465964f99d6113b55ced429
250bcbfa58da3e713b4ca12edef4dc06358e8986cad15928aa30c44fe4596488
9db958bc5b4a21340ceeeb8c36873aa6bd02a460e688de56ccbba945384b1926
c24c59c8f4e7a581a5d45ee181151ec0a3f0b59af987eac9b363577087c9746
5fda381a9884f7be2d57b8a290f389578a9d2f63e2ecb98bd773248a7eb99fa2
312f34ee8c7b2199a3e78b4a52bd87700cc8f3aa01aa641e5d899501cb720775
7cbfea0bff4b373a175327d6cc395f6c176dab1cedf9075e7130508bec4d5393
2598e8adb87976abe48f0eba4bbb9a7cb69439e0c133b21aee3845dfccf3fb8f
dce73c3c9c2f0033ea90e6eaf3b43eb037f29c78d2d35a8d0db9e46e30883626
e710e902507ad63e1d2ce1220212b1a751b70504259457234103bb22845a9424
b8c2b7d4f6d70fe91399fd810ab8458ba462b9f5b9f1c10a4a8936c70ca6ddc8
3434271f2038afaddad4caad8000e390b3573b2b53e02841653a4ee0dfd73674
094d1476331d6f693f1d546b53f1c1a42863e6cde014e2ed655f3cbe63e5ecde



# KPMG Cyber Threat Intelligence Platform

Royal Ransomware – Stopping at Nothing



## Indicators of Compromise: Hashes

0b3001a9237264d1b4091bd575bd42d897afbbf51ab96f3e631ee1deeed334cb

572d88c419c6ae75aeb784ceab327d040cb589903d6285bbffa77338111af14b

e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173

bd2c2cf0631d881ed382817afcce2b093f4e412ffb170a719e2762f250abfea4

d1aa0ceb01cca76a88f9ee0c5817d24e7a15ad40768430373ae3009a619e2691