KPMG Cyber Threat Intelligence Platform

Chaos Ransomware – Disguised Utility Enabling Data Encryption

TLP : Clear

KPMG. Make the Difference.

Chaos is a highly destructive ransomware strain that recently evolved into a faster, more aggressive C++ variant. Active since 2021, its modern iterations surfaced in 2025. Its methodology combines rapid file encryption and irreversible data wiping for large files, alongside clipboard hijacking to silently redirect cryptocurrency payments to attacker-controlled wallets. Chaos broadly targets enterprise sectors, predominantly impacting organizations in the United States, United Kingdom, New Zealand, and India.

Initial access is gained through a trojanized downloader, masquerading as a legitimate system utility, previously observed as “System Optimizer v2.1.” Upon execution, the payload disguises itself as svchost.exe, including manipulation of the console window title to mimic legitimate system processes, and prevents multiple instances from running. A deliberate delay is introduced to evade automated sandbox analysis before initiating malicious activity. The malware verifies administrative privileges by attempting to create a file in the Windows system directory. If successful, it executes recovery suppression to delete shadow copies, disable recovery options, and remove backup catalogs. File processing is performed using size-based logic where files under 50 MB are encrypted using AES-256-CFB via Windows CryptoAPI with XOR as a fallback, files between 50 MB and 1.3 GB are bypassed, and files exceeding 1.3 GB are irreversibly deleted while critical system directories are excluded. All encrypted files are rewritten in place and appended with the .chaos extension. The malware also deploys a clipboard hijacking module that monitors for cryptocurrency wallet patterns and replaces them with attacker-controlled addresses using Windows Clipboard APIs. Unlike typical ransomware, it remains active post-encryption in a persistent monitoring state. Finally, it drops a ransom note in %AppData% and displays a MessageBoxW alert directing victims to payment instructions.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the latest versions as per the OEM 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

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

Chaos Ransomware – Disguised Utility Enabling Data Encryption

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
45.61.134[.]36	185.215.113[.]75
185.156.73[.]73	185.215.113[.]43
107.170.35[.]225	170.178.168[.]203
185.215.113[.]16	185.215.113[.]209
144.172.103[.]42	

Indicators of Compromise: Domains	
pivqmane[.]com	almondtradingltd[.]com

Indicators of Compromise: Hashes
87fd821b67a1f329548f222d81a55be7
9113f4b245da32c75d61b467ee89e0b7
160f60dc3fc9920cfc3847de4de2ef09
cf888b19415661e4ec5714d470639aa4
062b199b84a6d5b51afd786e3ef860b0
dac27123cbf245b20cfd0334dca3ed57
edad71dba3bcab9750acde4e8f599642
deb70602c2aaee8245874ef50151d4fe
4e7dc2106473ce85e565cabd9e0cf108
e04a724de7604718d62b6a97ba2280ad
2f61d025d30fcf3a278673164043ce15
1de3e96ce1fd5929ac75a6868fb3a75b
22892b8303fa56f4b584a04c09d508d8

Follow us on:
kpmg.com/in/socialmedia

KPMG Cyber Threat Intelligence Platform

Chaos Ransomware – Disguised Utility Enabling Data Encryption

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
dd3fa6ae969ccdf3d221bd95ffef5a7b
176c3de6c4a1ac5c34b6d6be54fca774
e72e6f28b3fc6bfe087a7bdffb068443
21f974f224cef8bcaa194bed75f25ee28e1ca8d4
34a45f4172a355bf532185a83d0dd55df9794e91
bb73d57a43b27c11baf6f221ad17c0a83a08f752
10f24f275347760c5ea59a06372f8ec784014989
2dd84d5c0380c8c987261a9f4363c654679d49c3
bf33f741ac20632dee2d02a7d4ae92d931487d4b
14797717a888b0bd860368074423442 33fa512c4
80689beabfec1c7dba6a4f6dfedcf9f5eaaf612e
9bfab09f1333bf7ce5f89b7881513bd30cb56698
0f87cc0601a2dec4f847e8a75cb1d4141a3961c7
fbcde7674e8e7cba389824f213dbc3ebd609691b
bca8e8c81139a944b3aad4fcb7ab3c6dc2918701
e1d65daaf338663006014f7d86eea5aebf142134
8975046c5cdbab0e36aa9ccad61b05a898810079
73efc19941b9341f7735a616888b4f306b4815eb
50c5d24005f477410c633af5d2dd90e6bcb8f116
1d846592ffcc19ed03a34316520aa31369218a88afa4e17ac547686d0348aa5b
11cfea4100ba3731d859148d2011c7225d337db22797f7e111c0f2876e986490
7c4b465159e1c7dbbe67f0eeb3f58de1caba293999a49843a0818480f05be14e
19f5999948a4dcc9b5956e797d1194f9498b214479d2a6da8cb8d5a1c0ce3267
2fb01284cb8496ce32e57d921070acd54c64cab5bb3e37fa5750ece54f88b2a4
5d3fcf6532c9ee5778753c3f13e71d1e3b157b49e56133bdff5d04d6e6d6c8be

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Chaos Ransomware – Disguised Utility Enabling Data Encryption

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
76fde847037ca79c8e897fac9d80567efc4ec3a193ec3d8ae9c9fcd9e1ac4939
9521a154b06743fcb3a24b6b61ae0b4cbd1f1ba74d3d9cd9110042082d0b1d5c
bbf9ebbfd93306108299e54ecbfb59bb9433eeb34f89cef61864f4e87640eaf0
f200ea7ccc5c9b0eaada74046551ed18a3a9d11c9e87999b25e6b8ee55857359
f4b5b1166c1267fc5a565a861295a20cf357c17d75418f40b4f14b094409d431
fe717bab60f1b03012b1e6287e3f3725f1ad5163897041b824024aedabb7c46d
87618787e1032bbf6a6ca8b3388ea3803be20a49e4afaba1df38a6116085062f
21cf7da02e01b3c2317178395eff873e50ab9b8f27a23ffed37b2efff8fd6b90
35c1eb5ff8913c4ca4feb712e05354772146247bdb4b337868c687730f201023
0334cd1b8ab17203179da1ae77c1fad97ddf794cc63a6048aca664956d10b2ca