KPMG Cyber Threat Intelligence Platform

Kryptina Ransomware – Resurfaces with Mallox Variant Targeting Enterprises

TLP : Clear

KPMG. Make the Difference.

Kryptina is a C-based Linux ransomware that first surfaced on dark web forums as a Ransomware-as-a-Service (RaaS) in December 2023. It is a fast and lightweight ransomware that offers granular control. After its source code was leaked, it was revealed that Mallox ransomware was using it as its Linux variant, with minor modifications. The ransomware has since been observed in campaigns against SMBs and enterprises in industries, including energy, food, automotive, and construction, across countries such as India, China, Singapore, the UK, Saudi Arabia, Turkey, Portugal, Japan, and Malaysia.

Initial access is gained through various means, such as phishing emails, exploiting software vulnerabilities like MSSQL Server, or brute force attacks. Once access is secured, attackers deploy the ransomware executable manually or via automated scripts, exploiting system vulnerabilities to escalate privileges. The ransomware scans the network for connected devices and services, prioritizing valuable files for encryption. Kryptina uses AES-256 in CBC mode for file encryption appending a specific file extension (e.g., .locked or .lmallox). It processes files by initializing OpenSSL contexts, transforming file data, and applying XOR obfuscation to key configuration data. Uses Python scripts for the payload builder and web server components, requiring dependencies like pycrypto, termcolor, flask, and others for proper functionality. Allows customization of target names, encryption keys, extensions, threads, and file size, and includes a secure delete option that overwrites files with random bytes. After encryption, a ransom note is generated, with some variants involving data theft to pressure victims, who are contacted via channels like Tox for negotiations.

The adoption of Kryptina by Mallox affiliates highlights the evolving complexity and commoditization of ransomware, necessitating enhanced cybersecurity measures.

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

Kryptina Ransomware – Resurfaces with Mallox Variant Targeting Enterprises

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses

185.73.125[.]6

Indicators of Compromise: Hashes

255796e447b92ece07f2a44f80bd75a6
5b0c1958a875c205951b88fd1c885900
71efe7a21da183c407682261612afc0f
51d51696c7f3a0e3fba4b8ceab210bac
6bb2752ea73b4d6a5c33f543b5c29461
1448ce8abc2f0184ec898d55f9c338b4
120c6ddfc24274b6e2e3a1ba7dc519ab
4825f3a92780be4a285583b0f24fed99
d201bd19e60d500963aff0c235b07727
7db34438395f64fb19060aa76f4a3163
b0770b7f24a436d256f2d58fc8581a18
4532803225b8b1a8a7811a44f3f2e2e6
7f099845d8e6849d6ab4d64b546477d6
779aa15cd6a8d416e7f722331d87f47b
8d0fd41d35df82d3e7e2ff5c1747b87c
231478ff24055d5cdb5fbec36060c8ff
68785d476573955d50a3908dc18bf73b
b5b20e03ae941e9f21c444bd50225c41
4cdddec7f4bc26dbedeca6d4acb1c4dc
66bb9363e23c7ef2d16c89cd654b491e
be08c3e95df5992903a69e04cbab22e3
193d2c42fea21defedbce498b5039272
e9e087c52b97c7a3e343642379829e0a

KPMG

KPMG Cyber Threat Intelligence Platform

Kryptina Ransomware – Resurfaces with Mallox Variant Targeting Enterprises

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
af1d24091758f1e02d51dc5f5297c932
fabcc64299ec88bcf2815b6c328bdf5e
1b4bbc6a2cfe628395c5d670d5ef470d
63580c4b49d350cf1701fb906c94318a683ae668
63ff8359da29c3ba8352ceb4939f2a3e64987ab6
dd495839a4f4db0331c72a4483071a1cef8da17e
0b9d2895d29f7d553e5613266c2319e10afdda78
e3e8ed6ac01e6edb8d8848b1472882afb0b36f0b
f84ffe172f9d6db18320ad69fc9eade46c41e9da
355d70ffe98e6f22b6c3ad8d045e025a5ff78260
0f632f8e59b8c8b99241d0fd5ff802f31a3650cd
1379a1b08f938f9a53082150d53efadb2ad37ae5
21bacf8daa45717e87a39842ec33ad61d9d79cfe
262497702d6b7f7d4af73a90cb7d0e930f9ec355
29936b1aa952a89905bf0f7b7053515fd72d8c5c
2b3fc20c4521848f33edcf55ed3d508811c42861
341552a8650d2bdad5f3ec12e333e3153172ee66
43377911601247920dc15e9b22eda4c57cb9e743
58552820ba2271e5c3a76b30bd3a07144232b9b3
5cf67c0a1fa06101232437bee5111fefcd8e2df4
88a039be03abc7305db724079e1a85810088f900
9050419cbecc88be7a06ea823e270db16f47c1ea
93ef3578f9c3db304a979b0d9d36234396ec6ac9
a1a8922702ffa8c74aba9782cca90c939dfb15bf
b07c725edb65a879d392cd961b4cb6a876e40e2d
b27d291596cc890d283e0d3a3e08907c47e3d1cc

KPMG Cyber Threat Intelligence Platform

Kryptina Ransomware – Resurfaces with Mallox Variant Targeting Enterprises

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
b768ba3e6e03a77004539ae999bb2ae7b1f12c62
C20e8d536804cf97584eec93d9a89c09541155bc
C4d988135e960e88e7acfae79a45c20e100984b6
d46fbc4a57dce813574ee312001eaad0aa4e52de
d618a9655985c33e69a4713ebe39d473a4d58cde
dc3f98dded6c1f1e363db6752c512e01ac9433f3
ee3cd3a749f5146cf6d4b36ee87913c51b9bfe93
ef2565c789316612d8103056cec25f77674d78d1
f17d9b3cd2ba1dea125d2e1a4aeafc6d4d8f12dc
03bbfdbad1d1fd93d6c76de9a61e9cfc49e7e319
095538ff7643b0c142335c978bfe83d32a68cdac
1f08d9d0fe90d572a1bb0488ffe60e9f20c11002
226aea1e37bc2d809115ceb6ac5ea99e62d759c9
2aa6a1019c16f4142888278098f0c3263e95e446
33306b854770f95d0a164932d72bec1f78de54bf
51acdb8f29726fe7d5b6207f106e7138b564fd39
5413adf32129d50c4984e406d5a3804435d1cfc1
60b5beffaf738f5112233ed9b36975822c1f7bfc
6f3c3129fc2ac56b61fa4df21e723f3dd2aceb70
8ec866aa48a9bb8d6df7fbbe1a073390f4b0098c
d0231ce29ea7a63bea7451c42d69e93c83babb48
d41b8a7bc9bc444372e06e67585a8086d6ae8cfc
ddcf4a6bc32afe94e3ea955eead9db179d5394c2
e9b9f425fa818899070f69d09d3a35d7ccc88de6ac98b2c8b02116f1b314bc78
3528c95d5ed79e231a5243e01d455ae18e063e2346aa1c4296be5515c3e88482
616db74f35a6d9c8ba99ac589099971648c6a2290bc36cb6fec705f5238a6c4e

KPMG

KPMG Cyber Threat Intelligence Platform

Kryptina Ransomware – Resurfaces with Mallox Variant Targeting Enterprises

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
4f7f19b42226c59faad9f6f8a7c041731f5a8cf0c13915b4908feec312f47c3f
B7776fc59166d0fdafa0ff7ab867049512226b0d7302a3acd9532ab05e58d44b
45a236e7aa80515aafb6c656c758faad6e77fb435b35bfa407aef3918212078d
cd0f87f7df534b0e29b2ffa5d02cdef0d7db29a67a316e143554eb1945d75e6c
c23c25621872ef6a5f6a04dc1caf283a5efb3e046f6f721e96f661d28e3e6280
ff5e8c23e622bdaf6fd608691e6c3da298b0bfe867b0d8d84d37d991b75a237c
2289706f678585059502a24283e0f55d56cf477524753c606f64825bba66fca8
175e20a7c8d54bfa6271de9d550c25c21e1c91aaf39aaa80779389fc8600d53f
d6629a9b618ede05e9e75a2cebfb69bc7b1a34fe00a42ff60d88828a307c0d08
522c3dc47bb192400c4c3117159ed67082516eceb8d2e94bbdc1a8ae00adb95c
e6d4e65c45700dcedd2b5ed73734328500b5f5a016d79440d3611092475b9e6e
e0b6c83aa3aeff6d7d5fb4b5863cc94ca6158e12fd049d6863322bafb244a41d
2fdaee89b426fa3ee00f3e8d10ebf23f1de1562746e5ba2ee606443572190610
23ba8078df63ebb313f2f2a2f24dab840e068ddd5cc54bb661db7d010954d2fc
f4b64976d7dcb04466f0a89d81cd2eb158158c752c042ec248549415799965bf
9f4c40c0d52291334d90455a64106f920ede3bda5c3f7d00b0933032b0f208d8
9195ad1b5c2d4b20b12958224c6913b6a7929c3c4d2648a552aa7dc92da9143b
c714df0154f2b6fc8a82aa35281836c664bd3fbf4be3efc7e8b5b94ac87fc0a6
74c3cff306919e944ba1502bd3b014b111d06ded4119e9e8544e84749a07d24e
61f36c5ae038faa2b58a9a17b464d01414b4265e46634f353319c471d0a35789
ec1b3e6440b0fe1523295479fb18660aaac2f9f13a72145feebe07d60c2d9197
3b1b1beacd0925dcb27675c45f50574921181c097ab8004d18bc116e5a99bde0
694eeec46cfe1b7acd54cf95b307416be984a5238b3059cc3af446e74e28d889
e52a8d0337bae656b01cb76c03975ac3d75ac4984c028ba2a6531396dea6dddd
f67f3acfbf23d37c7c81d890a2b56d38d468d3fde37b3934d77a1cb3f5ac342b
0f8de2a116f590ace3a818302d2531af9f3c972816638c92773048c640807acc