KPMG Cyber Threat Intelligence Platform

LARVA-208 - Web3 Intrusions via AI-themed Social Engineering

TLP : Clear

KPMG. Make the Difference.

LARVA-208 (aka Water Gamayun and EncryptHub) is a technically skilled cybercriminal group first identified in June 2024. They have been associated with ransomware operations involving RansomHub and BlackSuit and are believed to have compromised over 600 organizations globally, driven primarily by financial motives. They operate on a global scale, showing no regional limitations, and tend to target industries that handle sensitive or high-value data, like finance, enterprise IT, and critical infrastructure.

LARVA 208 has shifted its focus to Web3 developers by impersonating AI startups on platforms like X, Telegram, and Remote3, distributing fake job or portfolio review invites. This marks a departure from its earlier smishing and vishing tactics targeting VPN users. Users are redirected to fraudulent domains (e.g., norlax[.]ai, mimicking Teampilot[.]ai) and asked to enter an email and invitation code, similar to their previous techniques that spoofed VPN login portals. Users are prompted to join a “meeting” where a simulated audio check falsely reports a missing or outdated Realtek HD Audio Driver, which upon clicking downloads a disguised executable that silently runs embedded PowerShell commands. The PowerShell script fetches the Fickle stealer from actor-controlled infrastructure (SilentPrism), hosted on bulletproof services linked to Luminous Mantis, echoing past use of custom loaders for malware like StealC and Rhadamanthys. The Fickle stealer collects extensive telemetry including OS and hardware details, installed software, geolocation and IP data, developer credentials, browser cookies, password vaults, and crypto wallet contents. Stolen data is exfiltrated to SilentPrism via bulletproof-hosted C2 domains, enabling real-time access or resale.

LARVA-208’s use of AI-themed lures and trusted platforms highlights the need to strengthen threat intelligence with phishing domains and IoCs, as traditional defenses may fall short.

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

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

LARVA-208 - Web3 Intrusions via AI-themed Social Engineering

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Address

82.115.223[.]182

Indicators of Compromise: Domains

b8-crypt0x[.]com	malwarehunterteam[.]net
global-protect[.]us	

Indicators of Compromise: Hashes

005277fccc94e59bcc80b2c0908e7651
37bf5aac3ee38ea97e2855e931d47b3c
a94d7d111993bfcc4bbc3fbe197a9edb
e7d864fcd7d14faf0724aad0829ff484
64d0c82b7365b1938c4507b06a2160dc
ba3fc03734e30d87fe4dfe96ac3ea03c
239e8a3ee1fafe452d0b59eadb32247b
6dade10533881d86c1a4762ccddb449f
59fc531c4c9545c0d888b47ec924745b
f617d2bbd6f372158831497db89f19e8
765354be128a6295a1fb35c4f0ddc128
894d8b4a721fd1931318e475f7872b9c
e2d005af8f840f371ab2cef870dacbcf
a0ad194a5aca632f0c71f3939665f229
660698dbe0a658de9cbe74f86f3ad1f0
5e2bf2978e3c3d2a5b1b0a745dac39af
210de49b640b9d06985f882404dc49fa
54238273f549f59cd28aedfe98fb32e5
adffd4d8ba3af7ea2bf6ca7a89a6c79a

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

LARVA-208 - Web3 Intrusions via AI-themed Social Engineering

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
56b1fb146753add245fb21df3f63ad3eb1110c46
2863c350f685f71b800ffd7cfb8df5e03497274e
9726cb6f9a5a3c24364741f36d2d52a24a26551c
4aea97c6ecbd3de68791cc2591c930965962d6e7
631705a952626a37e87e0f66ff11ed82636d4746
d63a8c0a00fb1c68450da7cc19a08a6ed96791dc
40ea19eca66a4a91b113fcce9ea6ecafa1bc3970
833cdf5a77811fbbf0c822f3edea4235eee0da51
31a9e8a27590a0555e6b198738a07b105cec757b
34ce94dcec5e6f02e49d64792d56c5511f347f60
4f177c65dce913506dc8b7ee281b47d2c5cfefb6
7d61ffb8d0be4dbf2867e1f08a17792bb2554da4
db2efdff7983b2f13e22d36ee2515a3604f93224
65a2dee3cd9aaaf18d7e1fbaf8fd8359f547873a
86cdd56775d65fd2ae79a64f13e8a49fa45c2faa
b873e5d9c519debf753e21f0fc0a27d439e3d112
57ab6bdbb41289f3c8983d5b48fc98c08782ed1f
32810768905876e9a738e867d23e69155135aa24
1f72030aa638c2e99340b7ccfa07ee5c46dfc46b
b94895044b45e115371ea744580c82e34f37e233
3fce08f14b875e52d1c1fea6f9a0fa3de0f65b9a
f18e909ff0990ece02ae83b5f9436c4676767c1e
d0276cd254c337dc3aee1a076361724d45e31734
a225bee48074feac53c7cb2f3929a41f7b4a71d3
e399091d6e1ae22ddc73afa7687d1cbfdb58d71d
336f07620c35d0760e0877f2941d36c07a737b8d

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

LARVA-208 - Web3 Intrusions via AI-themed Social Engineering

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
7a51a25c1d451a37a28b08290149bed05d82ffa305a5c9a86576046a324a25dd
7d9b41d7600c79b79e01f4e5100673bb134d5b4ea84ed8fcc9a2be6ccc1df4f7
7f8bd2d63bb95d61fcbdb22827c3a3e46655f556da769d3880c62865e6fde820
86e4115111e88bbaf09fe73cfc8255a4aac64f7ffed4a3229bbc8d626566f0c8
8833f2a6e84c91e31ae65e5ab269b362f7d4c2a2af63d760fe5b6452b9ecba96
90b7b711f56f00a1fa08a7a29f2cd8602b8aa1a0d78986dbfc9f64e38ac6cecd
94ee2227696da3049ff67592834b4b6f98186f91e6d1cd1eeec44f24b9df754b
95768bc40bb040d0c07c23f566cc20df0651fc14714e617b3f4b7ed3c6b7e5dd
9637506691705b2ffa90ff6b46fb71f11125dffabb19f3e89fd1bfb1f4caa223
969c7ee8709a519c4a4878b230d4ba7f81fb9563320b5983f8f1f95d4d215ece
97a766db470c44347b65a0bc282582f96a47d96ed8d7946f4da33775d384033a
97b6dc6f61b1eebb32a1e62a62680ad9814e535e40d8cd3d01583e7b1db127e8
983506186590f7118cb507d29f12f163afb536a03e6d0f4fb441df8afe49ede1
9854322760307c04aacd78f136e4d1496950811ee2f24978915d7cd322ecb36c
9b830c2979cbce45573aa21d765adda76f52db254155ae49648ef5050ceaf774
9d2aaa8672d583af4c03c23127d6cac509799a49ff9293ed63628d5b710b7528
9e9ca325f44eeff4087bb67052536ba565da18e70e5b29c79ed77c14c5548131
a04365c2804ed63ea0cadba4fa4ffc2e0541a09059abc0e046ee57ef1645ab64
ad95786b2402c6a2cc36a513937a10503aff74e180ea1213cbfe40ca820d3b13
af4d26b987093be6b442e655ffdafa8e1542e80f6a47a6895aa523f2f180025c
b1b3d27deb35dd8c8fed75e878adae3f262475c8e8951d59e5df091562c2779b
b1fa0ded2f0cc42a70b7a0c051f772cd6db76b15d50ec119307027e670998728
b29e630b9c70b0daaba4f83489494444c04c7a470b9c24eb4ddffb6cd7cf05ff
b3ed3f2bc5334e54ca8d6020d37da0764f123fa5717638229422bd95a028097b
b4f66a5e2876e04db93aae029049a07efed2d6dca05c89c393fe5aba03b949a7
b7b72d141ed56c8e5a924dfa959771548883b88e84646150447f85eb97f88e62

KPMG

KPMG Cyber Threat Intelligence Platform

LARVA-208 - Web3 Intrusions via AI-themed Social Engineering

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
b9ea588642ea77d39ccafab329c2f10718f2c7771e2ee77a0c6deda285a48de8
ba195a227fb76e8820d6db36cd00c89095b88faf01471fcdd9c0c7de61a63a5d
bad43a1c8ba1dacf3daf82bc30a0673f9bc2675ea6cdedd34624ffc933b959f4
badb915188b5292cb1a22624aa386ab0ad8279d5bd2678926123560ecffe0e0c
bb563180196989dcee91417aa56d6f1bfc9320b2427536c200dffcd784774906
bbaba3d086a38405ef816d97c76a98fefb0e49d899f61de53c44f38142356f3a
bf3e01de4c7af551c4f39aaac09763a71d4bac03126ac9de426f0d51dc970eec
c13fb67beec7f1737234483ad8d333ff77dfce804ec5c945b45fed448f272074
ca22e7b954277659a308ef321a67516689a24c51aea7ac3c5f2d76a583b11530
cbb84155467087c4da2ec411463e4af379582bb742ce7009156756482868859c
cd301bdc07518027567a5ed242ae2075f9f0bdf73315e99d4d949280f151fefe
cedf4589428ae05d3d2dca1d1bd7fa28f6cafe54a077a6090f873053e04fd5ce
cfafc9b2d6cbc65769074bab296c5fbacc676d298f7391a3ff787307eb1cbce0
cff9c5a87b3fb5961ddf59dfa0558c5b63503f89905e2a81ccd405e333408e72
d150d8d8bfa651c0e08a10323ecb0bccf346a35bd1bad19f89a5338acd8a88b3
d56afa4e4c8adb6232d0ebab0527b9fbc6b2619ebe1f39d06952877eeb2d195c
d76c25e2761210783055b43349370253d794e94ee913a2be7596b9554eacf107
db3fe436f4eeb9c20dc206af3dfdff8454460ad80ef4bab03291528e3e0754ad
e0ae6b6cfd6544a02517e91b74bda9d5cb98674dc04609743de012354c2cdf22
e2f5b088daeca178bf05464d05d33b365e315b53704655042847cf6db048f2d2
e31ce5803bb68222eeac117614ddb92ed3c137bcf129f873d44960ab9d8bab33
e71e6b81c46aab4760840369e3ffe6ac80a9e6a2e62fc7e563265ed37efd695a
e77423214cfc184f3b41bdd539024d466bd5a94c91cfaa65d4e831410a8a8f94
ecb7ee118b68b178e62b68a7e2aaee85bafc8b721cb9cee30d009a0c96e59cef
ecc8e7e5353c814ff7f66c278a19723b5769d53c49f69c3487d495fbc882a8b9
ee07759184ecaf4e0ef0a2981dccfc5b6c4da43a14a7beb002ae06c95a145dcc