KPMG Cyber Threat Intelligence Platform

JSCEAL – Compiled JavaScript Malware Targeting Crypto Platforms

TLP : Clear

KPMG. Make the Difference.

JSCEAL is a sophisticated malware, active since at least March 2024, primarily targeting users of cryptocurrency trading applications. It employs compiled JavaScript (JSC) files, a lesser-known feature of the V8 JavaScript engine to obfuscate code and evade static analysis, resulting in extremely low detection rates. The operation has demonstrated significant scale and reach, particularly across Europe, with thousands of malicious ads generating millions of views.

Initial access is achieved via social media malvertising, often themed around cryptocurrency or financial services, redirecting users to fake websites that prompt installation of a malicious MSI installer. The MSI unpacks several DLLs, sets up a local HTTP server on localhost:30303, and the website's JavaScript communicates via POST requests to monitor the process. If either component fails, the infection halts. To disguise its activity, the installer launches a legitimate-looking website using msedge_proxy.exe, reducing user suspicion. The DLL modules parse incoming POST data, perform system fingerprinting, and activate a PowerShell backdoor that exfiltrates system information and victim metadata to the attacker's command-and-control (C2) server. If the system is deemed valuable, the final payload 'JSCEAL' is deployed and executed using Node[.]js and build[.]zip, enabling a wide range of post-exploitation capabilities. JSCEAL establishes a local proxy to intercept and manipulate the victim's web traffic, enabling real-time adversary-in-the-middle (AitM) attacks. JSCEAL steals credentials, cookies, saved passwords, Telegram sessions, keystrokes, screenshots, and crypto wallet data, while maintaining persistent access as a full-featured Remote Access Trojan (RAT).

JSCEAL's use of JSC payloads and masquerading techniques signals a growing threat, reinforcing the need for advanced runtime analysis to counter increasingly evasive attack methods.

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

JSCEAL – Compiled JavaScript Malware Targeting Crypto Platforms

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Domains	
app-pc[.]com	desktop-apps[.]com
pc-app[.]com	pc-downloads[.]com
87-899[.]help	supercharming[.]com
foo-foo[.]bar	downloads-app[.]com
pffffer[.]icu	app-pc-windows[.]com
twisted[.]mom	desktop-app-pc[.]com
ggr-lach[.]com	downloads-apps[.]com
18-22-59[.]com	pc-download-app[.]com
grpc-test[.]me	vertical-scaling[.]com
supernegro[.]mom	app-pc-downloads[.]com

Indicators of Compromise: Hashes
198dc3be72e02fec93786467dcaf8358
a51e6afb9496ce3736749009cb36beed
46755708d4ff4b8d60f73d3db0def566
bfe676093c739cb731a1a905f89601ee
22f58e139275eb9597519bc4646aa4d1
f7fdabf872ba1dce7bdddb3c0cfce426
3d48a83fd884ae23fae1627ef1a20de6
8441871cc3df3d5f6fdef9e8ac7eee8d
7541883920c15131776d01ec8be2b66e
c04c6e6fc1fdb960ca876ed25da851ad
eee8a5e9db7a0ed13331c1f308b84f6f
35d90e4ca391f47371d12345180bf932
dcf5e2a6f5a92fcef05556665fda950c

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

JSCEAL – Compiled JavaScript Malware Targeting Crypto Platforms

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
332e200f7c0e4693417a38923979994f
9875429d727e366a10774afdad5e9c13
f74b292aab603c4c448039c30f2f7145
a393a50ea7b095e86b3693112813f93e
e02646146fdfac9c1c8577602dd8fd84
56f49d402fcfc53b16c54fa449a2101e
b34ad854c6d07361f1fcaceacf0e7b7fc542da24
ae2996abc671e04e218466bd4e18a4f620415d71
850aea15433d04b2904e4a0200b52b2d9ff264c9
d59660e0675097db16364c1085b2f150719d10f9
c63e04f8268e67cd4c6d5a5434ea440b30d0c405
cb5c716d815f44fe1df7fcfcff397ed42f7d1585
b019643ecda36a4c84eabaf1fd89dc9824d7c0d4
de64e818e5a4a94d0a1da64a823fb2da8e6bb119
f1b310f65a509ce86b3e71b76006d94c3c666320
50c9353b102d076df42dbc9450642dd062e26e38
8d223490583310867c9d0d4067d0f3ed474e82bf
f5243d96e333c10e0df45e9816870d7eea168173
4ccee6eef0fe182c9e61e6ed2cc29ab78fea509e
78fd29a9b3b820814917b421b103e89e60f86aa3
33cf8ca6dded4fd664525a5cb3d0e33a953a1108
ef341d6f7e6739d274d9a6474697cf42afa0ac58
c6b58fca13429a752f6909fa135ace4d92899dd9
e62b052245cae279f7b655be95e40e4276304764
0b8f426c645c80e50a1ea9d50d490f488d46e749
f312464d947e0add1ff14e6ad96c7944385af462

KPMG

KPMG Cyber Threat Intelligence Platform

JSCEAL – Compiled JavaScript Malware Targeting Crypto Platforms

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
dc8e0a7cd9779823b9310db81ba283ff5fe8dbed
00e8b839d235cd853c1d49da1dd600b8b0954ceb
0be5f2861003ac5857d89d7ba593c7cd7b85aa51
2fff514f9496afc14d61b6e71deeeb6d1217ff33
0207f65982931abbd6984c61dc0ae183de6ecd3a2142899bc6df37a1b21c591e
0f6357f4dbc36dcf73b4e83f9af5a796e81742a1aab11c2c2ecdc0ea2691df41
a9528e99a5b0a288855fca1d3a03975fe99ad6c5b8702a27d12e94c9a7a5367d
d8ebbee135dba28a08fd975366ddf62d3ab2ed10f2b339b867ba6800cbb9321e
6a3cd43d6ee7744631efb49d40ed38dcd88f8801f85992c703e2a44f13291243
a22d15afdeeb983d73255e274a8b62b76d267ca1cf943228d17992ceb6fd1643
680da0b4d9f0c553dcdacdbbf516f59fcedd3a87f24aa1b59e9858b089d14329
74c9175036bcaa239f433a98606df3a3be60ab9246f2067f500cea4b2be09a8f
cd6785e9690349d95ce34d30befe8b472f304e7c1129a0824c6e7a909aab7805
012c29675f4680830380c13ab008d8275e7b767d99cf1bde6f07048f8af60753
01c3b49ff55dfbe738b6c9370681b1985abd34641a75803fea1468e102b726c9
e7945eee02f90a9a03eb82e64fcc8ed07fd1d6d528afe0f8f948699b0497c5f0
3545b3debcfc385f169c92edca55dc5c9d394580fac1482a8394af5806b996b8
b1b608c7f0d943b48102237347754e593ac09715f0deda6a4a61730ece03a942
2b647bde846907c875504a3bf9df1ad12bf3a904130dd481ee8cac2effc9aa3c
d4bd8ba1ca7643016e324cdee81f46b2c5a49508fdc9011d71abeeea672e35fa
7a6beb95d6c5c790cdfe04d4634f5ebf24707f80ed75ba20c09b1b78e4f448a5
c7eedf31cf9e456cc9eb419edf30573f9ba03e80faccce9e86373e935f6c1b93
86610f1a2c87b80c898ec485681193f0788c017f2d0f73fad26b259655c6a8a5
044e8525eff98c030632fb52cd145c404f7f1fe22c99f74afd3f9b14e38f2375
c65fdb27d1b478a4926c2e283f8c50e827d522c13ba56da67e1fb436548a4454
abcbbaf9e5b34d59c9caa015a0276a457e0de2b403a5a8aff37617f141f1bb96

KPMG

KPMG Cyber Threat Intelligence Platform

JSCEAL – Compiled JavaScript Malware Targeting Crypto Platforms

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
4ff0bb65fb61bd59ab3fce204686a9e144989c65a1b92849bba5a144f9a23e77
03f3b378e78df66df0ffdaa37e286c71b8ae0da7893112125c3fee29b76b1db9
f8d598d28dbb8294a5c709ab23d51e29e652ab47d5a317aa31f6302481159458
a5b97ec3fee224213eebd1c762e0f874481af46bfcd521cbf3baba4b1c1b6037
2ba5fdec63b23d7578bbb5c0a07bcae7fdcbb339acfff4fb4b2edd6e48a1ba62
4889dda77ff5e7871e261d74b2ed83d987d3066471937b496e3b45101d3ddb93
bc5d17555db59898dd15f43c8362d4f3c4013d80d64442d25d05f50caca00655
dce4294fb041c22de81d3eb4c4a178b5bdf6d9fb48b348556a51582553b3fb52
8a9b2c59cfa1f332c12b430e0e7f367ea812871bb6825e172b85bb479068010d
c50fe7a338e7e2edb430688c87c65f92a0efd2115a8fab2e4e9776893d28db86
6e885af1b4b884c264f29253b80bfa47b29af7ac0757e5148e8cb3c342cd3183
9ce4d4e97956c190d384837d42274d8db33ae6073ab318f1e55f3e03da62507d
209639849f74bf2736ede28b0a90a8f5799a14fb6a3fc79833ccc2144aa49b2d
75e03884bf2f630c41ca04148cb28b7163945e146287fd1d2aafb10d3dd9b9d9
1d9945ac1a06f5ecef58d75452c898f39c6fa71f91274baf70404104bea63f36
1b757be18092f64e50127d80dff35d0da3d4e2d99ed199a6df134a86461a727f
c320e4d29fb661273e0cda16c756d962a62b2ad3d76ab13c4d1aa7dcb6168449
a05f029c644f8ad912994a364aa4a6c1d64da0a894f7856bc9be251e598404f9
7ee0db8bade12d9861ccf8f43334a217c587d97bc0828238a98a325aaff75f8e
521e82117dc6d8d1a086f6094a31b3714677bdf5b8b27a40235e2d0d2ece3487
e51855ae6e8e69f66c2af6d939769385f53e57445b9734b1b4811c09bfc80c97
4188868248e8f74ecd2f2868605a77f1986dbbf74d3bf741135c69931673ad38
54c0ef7cca1112e75bff0ebca5da91a1ca66c531e0b6a47b1e85907e21cc8623
ed6746a55f2160c586fdc66cd2c1db69f7fd0a73e6c2f1d83dd240c43828ba58
111fc7d7dd1f4ba3a87927b1754a9b67d2c60d58feb1cd6cc28d6c0b4057184f
d7cbdc2b5c57b1f61c771be74e56aefc05ebd8faeb0d9a7b02daff6946248dbb