KPMG Cyber Threat Intelligence Platform

Lumma Stealer – Social Engineering Info Stealer

TLP : Clear

KPMG. Make the Difference.

Lumma Stealet (aka LummaC2, Lummac, and Lumma), is a highly sophisticated information-stealing Malware-as-a-Service (MaaS) of Russian origin, active since 2022. Engineered in C++, it leverages advanced obfuscation and anti-analysis techniques, which contribute to its effectiveness and potency. This malware is adept at stealing sensitive information, including cryptocurrency wallets, browser cookies and extensions, login credentials, credit card details, and two-factor authentication (2FA) data, targeting organizations across many industries globally.

Lumma Stealer is delivered via phishing emails, malicious advertisements, exploit kits, compromised YouTube videos promoting cracked software, and recently, via fake CAPTCHA pages. These CAPTCHA pages trick users into clicking them, running a Base64-encoded PowerShell script that downloads the malware. The PowerShell script utilizes mshta.exe, a trusted Windows utility, to download and execute obfuscated JavaScript containing the Lumma payload. The payload is executed through obfuscated scripts, downloaded archive files, and process hollowing, injecting malicious code into legitimate apps. To evade antivirus detection, scripts like 'Killing.bat' are used to identify and disable security software by scanning for antivirus processes. During data theft, browser-stored credentials, cookies, cryptocurrency wallet information, 2FA tokens, and files with keywords like "seed," "pass," or "wallet" are targeted. Stolen data is transferred to attacker-controlled servers via encrypted HTTPS connections for C2 communication, typically hosted on ".shop" domains or CDNs. Stealth tactics include scanning for VMs & debugging tools, hiding malicious activities in background processes, and using trusted system tools to avoid detection.

Lumma Stealer's exploitation of legitimate services and use of obfuscated payloads to steal sensitive information underscores the need for robust security measures to combat such threats.

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

Lumma Stealer – Social Engineering Info Stealer

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
89.187.169[.]3	146.19.128[.]68

Indicators of Compromise: Domains	
priooozekw[.]shop	writerospzm[.]shop
outpointsozp[.]shop	abortinoiwiam[.]shop
surroundeocw[.]shop	racedsuitreow[.]shop
pumpkinkwquo[.]shop	deallyharvenw[.]shop
upknittsoappz[.]shop	mennyudosirso[.]shop
candleduseiwo[.]shop	quialitsuzoxm[.]shop
lariatedzugspd[.]shop	bassizcellskz[.]shop
shepherdlyopzc[.]shop	languagedscie[.]shop
unseaffarignsk[.]shop	celebratioopz[.]shop
warrantelespsz[.]shop	defenddsouneuw[.]shop
callosallsaospz[.]shop	covvercilverow[.]shop
liernessfornicsa[.]shop	deallerospfosu[.]shop
indexterityszcoxp[.]shop	futureddospzmvq[.]shop
crowdstrike-office365[.]com	complaintsipzzx[.]shop

Indicators of Compromise: Hashes
e74b1e485e42e8ba7a65ab6927e872a5
fe8d434116b9e721f0d470587d08422e
5777ab1c9225c53b8e5206d446b2a871
76c8017fa040092c2731f18279d2193b
2790cd100709e77c3f055c9fc58b0c67

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Lumma Stealer – Social Engineering Info Stealer

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
902f8f6c48da2b1e2e666dd2d4fbdf51
f95336c88ee7f8b6275fac1a458dad53
62d09f076e6e0240548c2f837536a46a
eb1cda71eeb15f7d529f68e15d5fff84
689e01a34a731c6f051e39cd55fb71ad
53fe090954a3b44ec96679000c9c65cb
b2f6bdff62150ea6f88c81dcb199d41b
8a9baf0bf2ffabd39007a630a430a29b
6ee7ddebff0a2b78c7ac30f6e00d1d11
03be9681aad7c7724b70f4057486ff7c
13adfb572724dcb1caa16bb5bdd52af3
3b48c90d4a283982ced898df9570894b
560573d7a40739736f13ddc595192d4f
42c06594d0b4e652c5c39b531912087f
c42e7842a08143f56d20dd918e84e85d
d15a13fe445a1ca38371c5c7c10d3b4b
26bdbc63af8abae9a8fb6ec0913a307ef6614cf2
36b6b48e868e65575533dc15326422754b67bb1e
79fea0be5521f44c6b3fd621fb4c95167ec7542f
7b90b7605bb124e28cc264cf93eccccc0f77a19c4
39cefe4883fb9ad1c37463d59c414084ab9410ef
d03a028fe7f428e5996b9f83861b047fbf58fc80
c98eee5919b9ebe871a116027d40f42f9bf267f8
f2f57024c7cc3f9ff5f999ee20c4f5c38bfc20a2
a71780b3a97632bf623b63f14ff9976401468121
c0bb747f2049624b38f8e46f600c9a5f9af043e8

KPMG

KPMG Cyber Threat Intelligence Platform

Lumma Stealer – Social Engineering Info Stealer

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
afdefcd9eb251202665388635c0109b5f7b4c0a5
e264ba0e9987b0ad0812e5dd4dd3075531cfe269
128a085b84667420359bfd5b7bad0a431ca89e35
99b8464e2aabff3f35899ead95dfac83f5edac51
9f3651ad5725848c880c24f8e749205a7e1e78c1
a01fa9facf3a13c5a9c079d79974842abff2a3f2
f2c37ad5ca8877186c846b6dfb2cb761f5353305
f89f91e33bf59d0a07dfb1c4d7246d74a05dd67d
594d61532fb2aea88f2e3245473b600d351ee398
bfc1422d1c5351561087bd3e6d82ffbad5221dae
c07e49c362f0c21513507726994a9bd040c0d4eb
ed07663c40d54fff42af99c2969971a3493f1bf7
437b343933eb768094463656c287a1713fd3187a
475ea9bbb950841c13e83fd3d7ad14a0fc9fcfda
4bf5b1654cc920c0f31756075c3b500a0ade3c26
7f7c9e1b1bfe9b5893202aa8a80559faf3c9858f
1da298cab4d537b0b7b5dabf09bff6a212b9e45731e0cc772f99026005fb9e48
c28c1d76b1937373be1b5d5455e2accf3698c41cb3815d01209b232e82b6dae0
2468e5bb596fa4543dba2adfe8fd795073486193b77108319e073b9924709a8a
bbf7154f14d736f0c8491fb9fb44d2f179cdb02d34ab54c04466fa0702ea7d55
1c2ec4c72c2f31a327b6ba4dfe27a607d311578e25d96cf34c54845eea986f36
f4f1c01264eb138c80a8deab4463951acf3222fcaa2141e6b0cc12405191a219
72fb604d44bf49245173ca6736d904ded5e75db7d972527c4bf98283d6207f38
0aee99eb37a16f57b8221f8014853e81000fb823ebd30a81c0030e9730a59570
a0655c7b163fd4a8f60e106a5e393ca4c50d47e84bf698cb4cf7090d6d28beca
2c968c23e15be37cd5d0feee0c15b4f4bc172594e67035f9f3ed9da46751ddf5

KPMG

KPMG Cyber Threat Intelligence Platform

Lumma Stealer – Social Engineering Info Stealer

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
aca54f9f5398342566e02470854aff48c53659be0c0cb83d3ce1fd05430375f8
865347471135bb5459ad0e647e75a14ad91424b6f13a5c05d9ecd9183a8a1cf4
1e06ef09d9e487fd54dbb70784898bff5c3ee25d87f468c9c5d0dfb8948fb45c
280900902df7bb855b27614884b369e5e0da25ff22efacc59443a4f593ccd145
2856b7d3948dfb5231056e5243725775783988073284 9c2e2a35de3103c64768
3ed535bbcd9d4980ec8bc60cd64804e9c9617b7d88723d3b05e6ad35821c3fe7
50f9c384443a40d15a6e74960f1ba75dcf741eabdb5713bd2eba453a6aad81e5
56f2aedb86d26da157b178203cec09faff26e659f6f2be916597c9dd4825d69f
6217436a326d1abcd78a838d60ab5de1fee8a62cda9f0d49116f9c36dc29d6fa
66ad1c04ebb970f2494f2f30b45d6a83c2f3a2bb663565899f57bb5422851518
6ec39c6eee15805ef3098af7ae172517a279b042fc6c323ebf1aef8f8f2b21be
922b1f00115dfac831078bb5e5571640e95dbd0d6d4022186e5aa4165082c6b2
a992cee863a4668698af92b4f9bd427d7a827996bf09824b89beff21578b49bd
b5c0610bc01cfc3dafc9c976cb00fe7240430f0d03ec5e112a0b3f153f93b49a
bb7a19963b422ed31b0b942eeaad7388421bc270a8513337f8ec043a84a4f11c
c1e27b2e7db4fba9f011317ff86b0d638fe720b945e933b286bb3cf6cdb60b6f
c3e50ca693f88678d1a6e05c870f605d18ad2ce5cfec6064b7b2fe81716d40b0
d669078a7cdcf71fb3f2c077d43f7f9c9fdbdb9af6f4d454d23a718c6286302a
e6b00ee585b008f110829df68c01a62d3bfac1ffe7d65298c8a4e4109b8a7319
e9cd2429628e3955dd1f7c714fbaa3e3b85bfaac0bc31582cf9c5232cb8fc352
1300262a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49
033bb18add8e31e4006a462c018af04886f323b9a4dd84214509338dc287ced0
32bbfe4da12bbb86950764df952ed4492f6431dfe598eb7721aab4ffcb545813
602e246378c8aa60cbb29ebcfdda38b0b6567c5d3910478da3143a0af5372d87
690a310c17587bc7efdf9455fed0af66a457ea678e3b4ff73ba3aa14f8dfb489
3aa011528c4d261a82a0698a5be19d47c4114e2443b93617978fe7f34957930f

Follow us on:
kpmg.com/in/socialmedia