KPMG Cyber Threat Intelligence Platform

PEAKLIGHT - Advanced Memory-Only Malware Targeting Windows

TLP : Clear

KPMG. Make the Difference.

PEAKLIGHT is a newly identified, sophisticated memory-only dropper and PowerShell-based downloader designed to target Windows systems. Discovered recently, PEAKLIGHT represents a novel threat due to its highly obfuscated and multi-stage infection process that operates entirely in memory, evading traditional detection methods. It employs a complex chain to deliver various payloads, including information stealers and loaders.

Initial Access is achieved by tricking victims into downloading malicious ZIP files disguised as pirated movie files, often distributed via peer-to-peer networks or malicious websites. Inside the ZIP, an LNK file masquerades as a media file. When opened, this LNK file executes an embedded PowerShell script, initiating the attack. The PowerShell script connects to a Content Delivery Network (CDN) to download and execute an obfuscated, memory-only JavaScript dropper. The PEAKLIGHT PowerShell downloader contacts a C2 server to fetch additional malicious payloads. Two LNK file variations are identified: Variation 1 uses forfiles.exe to search for win.ini and execute a PowerShell script, while Variation 2 leverages asterisks (*) as wildcards to launch mshta.exe and run the dropper code from a remote server. The JavaScript dropper includes hex-encoded and Base64-encoded PowerShell payloads that are unpacked in memory to execute PEAKLIGHT and download a legitimate movie trailer as a distraction. PEAKLIGHT delivers various malware strains, including LUMMAC.V2, SHADOWLADDER, and CRYPTBOT—each with its own capabilities for stealing sensitive information from the victim. PEAKLIGHT runs entirely in memory, evading detection by not writing files to disk, making it harder for antivirus software to spot.

PEAKLIGHT's diverse versions, each with unique capabilities and advanced obfuscation techniques, highlight the urgent need to enhance cyber resilience and reduce infection risks.

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

PEAKLIGHT - Advanced Memory-Only Malware Targeting Windows

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses

62.133.61[.]56

Indicators of Compromise: Domains

gceight8vt[.]top	deprivedrinkyfaiir[.]shop
brewdogebar[.]com	detailbaconroollyws[.]shop
forikabrof[.]click	messtimetabledkolvk[.]shop
patternapplauderw[.]shop	considerrycurrentyws[.]shop
horsedwollfedrwos[.]shop	understanndtytonyguw[.]shop
relaxtionflouwerwi[.]shop	tropicalironexpressiw[.]shop

Indicators of Compromise: Hashes

d6ea5dcdb2f88a65399f87809f43f83c
307f40ebc6d8a207455c96d34759f1f3
d8e21ac76b228ec144217d1e85df2693
43939986a671821203bf9b6ba52a51b4
58c4ba9385139785e9700898cb097538
95361f5f264e58d6ca4538e7b436ab67
47eee41b822d953c47434377006e01fe
b15bac961f62448c872e1dc6d3931016
e7c43dc3ec4360374043b872f934ec9e
b6b8164feca728db02e6b636162a2960
bb9641e3035ae8c0ab6117ecc82b65a1
236c709bbcb92aa30b7e67705ef7f55a
d7aff07e7cd20a5419f2411f6330f530
a6c4d2072961e9a8c98712c46be588f8
059d94e8944eca4056e92d60f7044f14

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

PEAKLIGHT - Advanced Memory-Only Malware Targeting Windows

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
b716a1d24c05c6adee11ca7388b728d3
dfdc331e575dae6660d6ed3c03d214bd
62f20122a70c0f86a98ff14e84bcc999
91423dd4f34f759aaf82aa73fa202120
f98e0d9599d40ed032ff16de242987ca
6f24be390aa63e8365eeab5b23e077e3f835e59d
8067947f973d2e0e2416dacdf9f3b2464838825a
39a190c8b7dc589c85476f3fdb27d165207cfca7
09d96d5804628eadb5dba5c37e9a22ca5312a3a4
77b238dd8af8ea6555f367476cdb34d520bef34b
32a0713812274d04ce726b014ac80623a6f9acda
ad42e88bbcce1640aeda1397f82c826ba764d08e
1dcb61babb08fe5db711e379cb67335357a5db82
6514933e53c6eb9594786a773f75595b0eafeaf7
f89472f876829593646a5c93f22bf1209fff5d0d
923fb0545fad9bab123fd6f43e4b04c5c555eb4a
d7647d4dab58e6a205ee73e9afca054e5e24b532
dff4996b6e6b74be72ee6f526fac590a82946db1
65bdb4f383e87f7455f29b2c6ead301076cabac2
46a491abbbb434b6a1a2a1b1a793d24acd1d6c4b
7e1a5db6e9c56ec3cd462dcb872a904aa77456f6
473d413a209280848b7a1cbb510766dc0d77a77b
33bba2befa35d92f68fb62fb6c066f597ef11c81
e3bf61f6f96d1a121a1f7f47188cd36fc51f4565ca8cd8fc07207e56a038e7ca
d9158d0fd577687321a7b29c5df3712a44e7aa13f03207a158147e9e4b253b53
11e72df66c5673a99696cf302f1ea3aa35877b668474900e5272f0e33eb73348

KPMG Cyber Threat Intelligence Platform

PEAKLIGHT - Advanced Memory-Only Malware Targeting Windows

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
34dcc780d2a2357c52019d87a0720802a92f358d15320247c80cc21060fb6f57
d6b2e83093cdaa1c59777b91a68ebd801161cf0e8f6499ca41fd2f99dfb2d839
31fa6a32b73ceef86560bdad24f0b69c50bf035cb1b18ccbf7a97857a39deb64
3f86ca59335214a918870d86a47b21cc77f941dfcb32b7ba97620021621e7444
e63d29cda8af6ad95286c11996f0ac32a70ac24c1c2baa78d22593babd826a41
07061f3fd8c15bdd484b55baa44191aa9d045c9889234550939f46c063e6211c
218106e2f5ee44e8ae3ecf62e5c2cb1c3db50e5825f4737c9d13bbd48114ed0b
bf1a0c67b433f52ebd304553f022baa34bfbca258c932d2b4b8b956b1467bfa5
658ac17f4047ccc594edfd7c038701fe2c72ec2edf4aefe6f3c2dd28ab3dd471
8235bd354b95a117a50922b994732cba101815a26a502ab9dc039a533329e2a5
ead01fc10a3a7c5bef4f37a8137724c290716d07f4f032d5057f2a198834d5d7
a1010375ee640ecb61d0912243ff7ca8ea56f3ad3eeacb0f109bff56f519c1fb
98a93c1e0708be18eea76134a5d49a052373c38458c8fb434339ca4c3e37a5ab
973bbef82c2feecd5e3fbf75eac3e14fdce767cde712281ca2fbefc9eac218d2
9fa7cacb5730faacc2b17d735c45ee1370130d863c3366d08ec013afe648bfa6

Follow us on:
kpmg.com/in/socialmedia