KPMG Cyber Threat Intelligence Platform

MedusaLocker Ransomware: In-force and Compact !

Initially targeting and encrypting windows-based machines, MedusaLocker first surfaced in September 2019. This threat actor primarily targets medical and pharmaceutical based companies. To avoid the execution of several security tools, the threat actor displayed an extremely intriguing behavior by restarting the machines in safe mode before execution. MedusaLocker is a typical ransomware which uses single extortion model and demands for ransom in Bitcoin. Lately, this threat actor has mainly relied on remote desktop protocol (RDP) based vulnerabilities to gain access to the victim's network.

For gaining an initial access to victim's network, the threat actor primarily targets vulnerable RDP configuration, leverages phishing mails or brute force password guessing on RDP services. Following this, the ransomware runs a PowerShell script through a batch file. Before encrypting the contents for privacy, the threat actor kills all security processes. The machine is then restarted in safe mode by MedusaLocker to avoid being detected by various security tools. A ransom letter is subsequently added to each folder containing the victim's encrypted data. For maintaining the persistence, the threat actor copies an executable to the directory and schedule a task to run ransomware in every 15 minutes.

MedusaLocker ensures that maximum amount of data is captured, both locally and remotely, so that victims are unable to take any recovery measures. Thus, it is important to ensure that organizations have Disaster Recovery (BCP/DRP) plans and procedures in place. In addition to these plans, companies should perform regular system backups and maintain efficient network segmentation.

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.

The 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

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

KPMG

KPMG Cyber Threat Intelligence Platform

MedusaLocker Ransomware: In-force and Compact !

Indicators of Compromise: IP Addresses	
159.223.0[.]9	194.5.250[.]124
198.0.198[.]5	194.5.220[.]124
84.38.189[.]52	45.146.164[.]141
94.232.43[.]63	185.220.101[.]35
194.61.55[.]94	198.50.233[.]202
87.251.75[.]71	195.123.246[.]138
50.80.219[.]149	138.124.186[.]221
179.60.150[.]97	185.220.100[.]249
108.11.30[.]103	185.220.101[.]146
188.68.216[.]23	185.220.101[.]252
196.240.57[.]20	

Indicators of Compromise: Hashes
47d222dd2ac5741433451c8acaac75bd
4293f5b9957dc9e61247e6e1149e4c0f
82143033173cbeee7f559002fb8ab8c5
a35dd292647db3cb7bf60449732fc5f12162f39e
86d92fc3ba2b3536893b8e753da9cbae70063a50
02a0ea73ccc55c0236aa1b4ab590f11787e3586e
c87cd85d434e358b85f94cad098aa1f653d9cdbf
e03aedb8b9770f899a29f1939636db43825e95cf
1bbda98348f0d8d58c6afccd50a76321d02919f9
0c1ce8017cfcc24927fff1b00606e8c83c4ebfa7
6abac524387a106f73d9ddb5d8a84cb72dad1cdd
212e3254099967712c6690be11ae9d65a8966ffa
4bc8175c5fbe088297ec4eb3fa26acd8927530e2
2ac4359a7db288f07ed39f696e528cb379d2d979
820d3dfe29368e3f16f2818e318805d78a6b7d3d
7219f91bd5fb94128159d18956e1bd9132bf10e0
855b8aeb4160641ecea5710174086ee74d3e42c1
e5162ede86712df1e602cbf1ca8b205ab113a931
7ad1bf03b480ebd2b85b2bc5be4b9140b0ce6d4d
eef59fd5b71487448bfd44270d909b1441cd537b

KPMG

KPMG Cyber Threat Intelligence Platform

MedusaLocker Ransomware: In-force and Compact !

Indicators of Compromise: Hashes
69c1527fbd840eee87821328ecf1453984ddc73e
0fe01b51818c6c7c1556bffb43976a5264b3cc43
f3e66237577a690ee907deac9ffbf6074a85e7a5
0bcf20885b50d64a876e7b46497b22689cb93d33
78bcffb9ee6a7d29e18f66c0138aa3fd3a9225fa
fc31989737dcf21b73bc0956220852dfab2cb549
b209dcdfdd030ae1944507fcd9ef0eaeabe22f21
e70a261143213e70ffa10643e17b5890443bd2b159527cd2c408dea989a17cfc
fb07649497b39eee0a93598ff66f14a1f7625f2b6d4c30d8bb5c48de848cd4f2
ed139beb506a17843c6f4b631afdf5a41ec93121da66d142b412333e628b9db8
a8b84ab6489fde1fab987df27508abd7d4b30d06ab854b5fda37a277e89a2558
4ae110bb89ddcc45bb2c4e980794195ee5eb85b5261799caedef7334f0f57cc4
00ebd55a9de1fcdd57550d97463b6bc417184730e3f4646253ba53c4b473b7c0
02f250a3df59dec575f26679ebd25de7c1d5b4d9d08016685f87a3628a393f92
0a82724cfb44769e69d75318b0868cd6de4aa789951362b3e86199e6c7922610
0bad6382f3e3c8bf90f4a141b344154f8f70e31a98f354b8ac813b9fcdaf48f7
0c840606112df18bfa06d58195a0ed43715c56899445d55f55bc3789fde14ed9
124c65d01c6ba01dead43e246ae4c300d7345c8f46ae71ebf101bef5510f35aa
1d1e8e2bd3f8276f629e315b2ac838deaac37f3b61ceb780a58f7db611cf9669
21c644438a00fb75fabb577076933a99119e9f07e71eaab3f7dc6c629860c4c0
2c64f5f2bde51f7c650078aeee22a4b73e6b859a7327d0e3dd0d88a17e13dbb4
316a5895965fdea58de100355ba1b3a14c0515a40156fc7ab64bdb5d14379888
3592c9268f515efe1275760a21046a03a3067872fcb3da7b53477527123c09a7
3a5b015655f3aad4b4fd647aa34fda4ce784d75a20d12a73f8dc0e0d866e7e01
3f7cbfe8c40ec4b599ba7dea95321c377c1d9f08c56c62b6809157f73774bde8
461f427d71d6e2e2320ed5f8e6160d6bee23a98ff929d8d8b7567dcc6118d937
4ccc3a7c6b18db6f7251c447e19e24c9dde30a45e78d283ed367f6f0165c2fb1
4cf090e3ae23ea6cbe76df697bf7143bcc95acfc1521fbe5af77cb5033fae87a
590ea5fa2db24715d72c276c59434b38d21678d6dcabb41f0e370f6dc56ab26b
5aa810e4891538670cc0db6274b7276abe84e8ccbbaef1d3b1208b9ad419a9fa
6b9ca4cbb68f23e164625614d9d074b7bb9e2c5aeb429034ed4d6440594ce64e
6e3b77a1131912156c3f65f3b7e8572bd2e02b8bb7180104e8bf36e2e1451d43
6eeb8de811f707ec3b77e212d415f0d79dca77b564d7738ae36612c457f451cc
7b7cce10967d657b7ad0a66270dfee7000dac8aca2e39199c9713a4ee42279c2

KPMG

KPMG Cyber Threat Intelligence Platform

MedusaLocker Ransomware: In-force and Compact !

Indicators of Compromise: Hashes
897737252ce8e474774548b99c9bb5fc52484fe51df8e5d87945186adf7a5dd5
8b80a84b2a0a5a5f9670a951492749c3798c9f4d41589872224d57d41913fb46
8c2dce63957579f99a0e8c71755bd8a69298a4621d7b8984b06b69ed874f8d26
a0ff2c622c32e05aef8e7fb2e36b693aecc8cc04e049d3b47c0e0cb50d3ab575
a6cc8bd23bbafd0b356404eb24b50236815a03abdfcf8d280dbedd5c45bf6282
a9787581be4c667438a07a060137d6a83abcc2d1e33eef1086622dece56bb48f
a9ce91a9a1bcbe2cd2ec023cdf2f302c8ac4f6bfe04e83a9c4edd1c47b53618e
b561a5d5bb5cf659f7f23fd833244a61031bc5c5e69972b22f4ff5c495a44203
c01323aae6c62466bda8e6347e64266c725e6a754b06d4fc4aad1c323d3e21ed
c7ba33d4ef49b5dd0e6ad4a17bb04733db4832c5ef6bc07da51a0a4ffd7d831f
c7e71eb5d99cb54f83d3617682805bdf2991cb8fd0b4d34ecc0cf7624aaed6c8
ddb4776992155b9c5a26b47b53df2fed780c67b45eca5cbdf573e0dc3c20c371
ddca9b2f9b4c20faad500e19ba74c8d478c5be02596e9b1ff5a26ef4396bcd59
dde3c98b6a370fb8d1785f3134a76cb465cd663db20dffe011da57a4de37aa95
e2148660af56e9fde27e26ae3db205ca2d68ef1caf968e21f498fa94d8b56ef9
e71a4e701874c1a8e6bbdda79038b08b2fd36015a575fe167632eb629060b416
e86234c97b85a388f5df0a4900c1902f402210a9f73c26c3f856e25ae61bb80f
ea4285821c6292cc0ac5b740d3bc77484858432e29843a729434d48248793d82
f7fac370ff01836fd82e68a9b95372f612785087821ebd8fb89fe1dcf7122b22
fda65c171b36dbeb6eee6912ce85da045d06f780bf74a1000c57f0c6fb8ad415
7593b85e66e49f39feb3141b0d390ed9c660a227042686485131f4956e1f69ff
bae48fe24d140f4c1c118edbfaee4ab6446c173a0d0b849585a88db3f38f01b8
d90573cdf776f60a91dc57e8c77dd61adbdaaf205de29faf26afd138c520f487
d33b09ddee82c5c439cb0c66e5c1dee9ad5259e912a3979b31c66622fb9d47ea
678069f7847f4a839724fa8574b12619443bbfbc4d65d3d04c3f9aa1ba5fb37a
d74e297ac85652d1f9c43ca98ff649d7770c155556ba94cf9e665ca645aded0c
abe330ec7e157293afee2d96489165d3aa0ed9a59252ecf4f3acfa3205ca9d15
40fbb2f6850213af595dd27231b06c498f87e62b50e8b883976900cc1afa75e1
8b9bdc5cf5534d377a6201d1803a5aa0915b93c9df524307118fd61f361bdba2
aae247b1fe640f2c96cbfa508d18d475f3e4c8b29fa117a31d17ba0c4e5caa48
8597f458f1dcc5ecdf209d9c98b1f72c2fce2486236a3ae73adbe26fb6f9c671
7af23ee3ad9d4822c371936037ff823a719c9ab877973e32690b0dadceb55792