KPMG Cyber Threat Intelligence Platform

Loki Locker – A Painfully Mischievous RaaS

Named after the Norse trickster God, Loki has been creating quite some chaos on its target infrastructure. Making rounds since August 2021, Loki is in the bandwagon of Ransomware-as-a-Service (Raas) and is sold to carefully vetted affiliates. Targeting Windows systems in English speaking countries, the country of origin of the Loki is still quite obscure. Although attributed to be of Iranian origin based on tools that aided in its initial distribution, it might as well be a trick to divert blame.

The '.NET' written Loki Locker comes with a heavy obfuscation leveraging a virtualization package that works on C# based obfuscator ConfuserEx, making it hard to reverse/analyze. On execution, Loki sets up persistence by creating a scheduled task to execute the binary on every logon & copies itself to the Startup folder. Before it can proceed to encryption phase, Loki does extensive preparation like loading configuration from a config file, kill processed if specified, disable Windows Defender, task manager and deletes backup and shadow copies. It goes a step further and changes the user's login note to display ransom note. C2 URL is hard coded, and Loki sends a POST request along with hardcoded 'chat-id' parameter unique to each victim. It also drops tools like 'ns.exe' to scan the network for shared drives. As the final act, Loki begins encrypting each file with a randomly generated AES-256 key. The key is further encrypted with victim's RSA public key. Along with the ransom note, Loki drops 'cpriv.loki' file which contains victim's full key pair encrypted with attacker's public key encoded in base64.

Loki's ultimate mischief involves setting a timer value which on expiry wipes the system clean & attempts to overwrite Master Boot Record to create carnage if the ransom isn't paid. Having a regular offline backup is thus crucial for firms to recover critical system data.

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

Loki Locker – A Painfully Mischievous RaaS

Indicators of Compromise: IP Addresses	
91.223.82[.]6	194.226.139[.]3

Indicators of Compromise: Domains
loki-locker[.]one

Indicators of Compromise: Hashes
e7c4b46eb8854da31bc98e604ce77704
351a999d84f24e916cb1bbdfc993e132
8aea251877cb4f5ee6cf357831f8620c
2ffc2446a2a6cf04c06a85deb43b9fb8
bc60a6c03e8f86b2196fd515583c4827
1ce419f381c6614143af50d6bf5c9d13
c9854160ae23ca269f909c0bd3661e8e
a9707f640bd55e8bd5b90b2c1c61a3a7
12c3254f0e01f3596dda380718394fb1
b8400afd1787cfefae5eb262ab3335e4
4243af93241f7b07f670a46a579441aa
ad81961ccc571e985d35e6f30d396859
ed64744fcc9dbade6d03b40b2542e492
16b4d928126efc786f370d6da015f5d9
3b97edb736c6a7b8278aa72f519ce38c
6280f2bf535f144fd816d5924bb27c6f0f108f09
4ddeb9b3fc1f6898649a4bb2b25a64e089333906
3081bbd117a6b69c74b41215703b90bcb7187232
270049aa93ba2f8df6d6402e52a519cf9f187ad0
614585d4314bd9a61bbab2ee5b3037426ebbd5e5
614585d4314bd9a61bbab2ee5b3037426ebbd5e5
d396de116dff4fac6c78b0826ad43ebb6e041f3d
ae5bebbe24779ff984b6ab3f1c842d05cc61cd0e
03915f700402fec04c6c3ef38e827e0093d1c533
4b1e7937b89a491bf105e1242a1b84c3ba9e9e66
0605bf2a926d41e330dfa16036d968cbdb230601

KPMG

KPMG Cyber Threat Intelligence Platform

Loki Locker – A Painfully Mischievous RaaS

Indicators of Compromise: Hashes
6410f56102aa43a8815c13bdd94e1f55df3fe7cb
90df5483fdf14af13edf56b74289550dae79693c
1aa34a09f89e6b0750962e3ff8030e0cd5f6bf61
c710f732fd6f8ca4cb6d65d86a248b5d7c74f70a
2ee4b6c746b4f2a4ea832a53109531152ed324f6
69338159672de3bcdcc18d8e434380b679b88101
675f7b9185ccc3241650ff2fd96f5e1a0bbf63ee
7b73993fb07c0b16171bad449e49c9344ca87d6a
5eaa4b404bcec536af8c9089e54b45bc9829c380
d4941479fab7aeca3903c0d93a03123c834f71ef
a54627ea2a555d4842817d2fa578fe28ca0d7645
7de6ae598de91e85d247d341f829f0bc16f341a0
851cbce081d2b694985d349ecc92b144da527327
2eaa65c565248b2784583e1d1512d4fe0bc35219
185311e52a66a79237b304cbc808157cb2bdb300
a5c3f87720eab5bbb73eea208f9c3d8b0b7fa0c7
78d0be807ae945a68e50901623d9602e6f38e960
081936642b65b5164ab4a3de3b565beaf3ff7823
42088f0e3e9c70b7d1d238f7e3b03a3ca177748ba2568adba9104bbed2827734
6d1ecc48069eae14a831af05d29d2d25c0fa9f7c62f1f51c44d0d70fb014a590
84d9ef8cb92d57b178cce655f3f7808c6f5cf42f15c468f741b253f37ffc39fc
bb382bbc0756832748b33f0d7f7ec218d570afa031937259e69237df4945d074
ca478cb334360bef31d394438cba1449dfe0b8d751cc8eb679f09e12e5068d1a
e9e80fd3fe71d133609f5bc75081b13123e4f9a5ed1920050727955185f3ce52
fe40e5c6244c7e0a256689b6ea0881998fef897cece79a2add3ba8f7a23f4f2b
8cb1e9c99ad716a2541697a6d4ada32433b56e11dfe6aa1cb7c4fbc72b4bad2e
c1e8c720da2297aa4432364441b341ec85e6f7f571cf6348ffdc51f4ae96418a
0684437b17ae4c28129fbb2cfe75b83cc8424ba119b9ca716ad001a284d62ead
15d7342be36d20ce615647fac9c2277f46b6d19aa54f3cf3d99e49d6ce0486d0
1a4a3bfb72f3a80e4b499ecebe99f53a2b7785eace7f612b3e219409d1e1ffc7
2a7f01d924a4fc38c9fad586634eccbc28de07d97531c4a02eb6085359093a45
37702b94f9fc14a406312a2a392ad9553cf05c4b6870d94b5cf4781c02c29414
4215b5ce91deb97011cba2dd94d5bac1a745d6d55f6938b86e209eaaf8e655df
52c045b57e24585467be13454c5db551987fd23bfa931a7f6ab41e6f11b8a7ec

KPMG

KPMG Cyber Threat Intelligence Platform

Loki Locker – A Painfully Mischievous RaaS

Indicators of Compromise: Hashes
55da12a82c8e0b9fda5dbba6612627c0ee5d13d55e3bcc1df2ca9785c97caf64
5ccee068daf8a672d0e63e334e00985aa7fe56aa26b6c036d562728fdf968237
6205056cd92c75579f56bd0ce7159fae9f360d4c183beb10743330952bf22056
630e24cc1c4c95321965ad967e77e1888c48c4b1f653d800c7df08e879814787
75a5d27c77cf8515cff84d789f0e8f849b37e15b9b5f1c0801bab414061048a6
78a530f35d1cc89fc757b7661cbd57b2e9e46aeed53e2e66247db66c214a2ba0
7f23ea1e5ab087ba2c4e0ea251d680ef5190d49181efcc222702075b276d5990
8630df622ee773c3d9c934fe9d925c019b43232e8f2810ee651dcf5f3ec79893
88acae18f2cf7de7bb76784d45d9612561c8890872ea3629f0608577928745a5
8de5b9332556da8f401c5cbf3cea1dbc1e1ba277c0efa85dce8cd36310c2936c
8f78555f0f62b4f280a77109dbaa4aeb5c347d1ea38b521f98c57a7acea8087e
8f8cf6b8cd0c789d3f67f6291bb7c0c5416e27320631c852152a63513185941e
a1e30ea263ba21d656717f7f7824ecb2dc90896f55eae134afaf7691209979fd
ac1b326f23e17726a2b90ce8a9d29c6e44a2cb37b431e2b94734bdd17618ae26
adacbc5402326f87c76cc7737ad924ce5bd7394400ef86a48fa754af9d22da66
b01a96892f3efdaa6682078339b23d8954d571c27ee15a4ce9ef8ad6c415f06d
b8996e435ba229837d13f9837f6c0451f50a5767b0d1f1bb715670c802a1d564
c3fe7ee5451108c16d7730d0bf589f70b841f3846908c1761d827a70f3462ef0
c80513aaff11a2a2914d3a674737f63fbc04c6d5de7fda6f8b6e07df580664cf
c8e8599e8d86ff7daf02ea9c01d31f4cdcf829314c76b84d1b1b8a982d1299c5
cb17673f3cde6e542db3ff5facee2a01fdec462be275e9274c512038470009d1
da0a82d322502cd6d156649dee1e0a45348df0dce272b6ae2dd81af25f774c62
df24b04f6ff0ac50fbf1c01ee02f809c1c3f9fbe9d14eefc3306b1b586bf943e
e28b0a93649010788bbeda883a08254fefe3710700fc2c5a8dea94ec39402ec3
f2da3d1410c5058720a4307acf5fec7fc2b54285be9dd89eae108cce368dcde7
fe930861d5eec95a3ea1239e7a8f4182a2cf5b094ac3a48c4cb2f0ef39facd05
fffcf4be17e732aa3a5387e747290236d0f75ff3a24cb43eca793668d7772ddd
4e6471c4574152d0eb2d2c608e540e505f3db41b50997d1f06c47e587a355d80
7c890018d49fe085cd8b78efd1f921cc01936c190284a50e3c2a0b36917c9e10
9ab1694c978f11521c6bca73d40256e4b433f3279792db8ae1fecc5e0ad174c9
ebc955f12b0a2b588efca6de0af144dd00e33ead80185a887bf7c97329b28ec6
1e6ecdb54224eea50476be03d5a48083deae15301f26ba3519e0c0a5eb77b1f4
268c2924d45c0c7be9b67b85f03ddf5df97f2bc8963faefe1bec244e0cb95225
36b5fe49cd81393f8c60c70c941a1e6aaf181775b0614f1c4a142f38c7af1a81