KPMG Cyber Threat Intelligence Platform

LuoYu - A near impossible man on the side Attacker !

The savvy, Chinese speaking APT – LuoYu has been suspected to be in the trail since 2008 and is seen primarily targeting Chinese foreign diplomatic organizations, defense, and telecommunication sectors alongside occasional global attacks in Korea, Japan, Germany, India and Russia. The infamously known group has now drawn attention following the discovery of their new payload delivery strategy of using man-on-the-side technique.

LouYu group has established themselves as a cross-platform threat known to target Windows, Linux, Android and macOS devices with its wide range of malwares prominently ReverseWindow, SpyDealer, ShadowPad, PlugX and WinDealer. The threat actor has been known to employ the watering-hole strategy wherein they target local news websites in order to compromise their victims who visit the targeted sites. Further, the group is known to be well versed in impersonating popular Asian social messaging platforms and distributing trojanized versions of the same in the wild. Their sophisticated man-on-the-side distribution tactic for malwares leverages rogue servers to listen through the network traffic followed by insertion of the malicious payload and strategically timing the response to deliver the same to victims before the actual response. The bewildering features include the ability for the payload to pick any random IP out of extensive range of 48,000 IPs of a specific ASN as C2 and the malicious actor's aptness to interact with non-existent domains as C2.

Suspectedly the nature of threat actor's operations means there exists no specific defense against such detrimental threat. In order to fortify the risk organizations should follow a holistic security plan inclusive of antivirus scans, analysis of entire traffic and detailed logging and anomaly detection.

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

Indicator of Compromise

Indicators of Compromise: IP Addresses	
113.62.0[.]0	113.63.255[.]255
111.120.0[.]0	101.226.26[.]203
58.56.199[.]53	101.226.26[.]204
113.62.198[.]99	101.226.28[.]202
113.62.61[.]126	101.226.28[.]201
113.62.45[.]102	58.215.136[.]251
113.62.225[.]17	58.215.136[.]250
221.195.68[.]71	101.226.26[.]201
23.253.126[.]58	101.226.28[.]199
101.226.27[.]225	101.226.27[.]226
101.226.26[.]202	117.135.161[.]105
122.112.245[.]55	111.123.255[.]255
101.226.28[.]200	

Indicators of Compromise: Domains	
0fr04.veriblockpool[.]com	download.pplive[.]com
ossapp.suning[.]com	

Indicators of Compromise: Hashes
0c8663bf912ef4d69a1473597925feeb
1bd4911ea9eba86f7745f2c1a45bc01b
5a7a90ceb6e7137c753d8de226fc7947
73695fc3868f541995b3d1cc4dfc1350
76ba5272a17fdab7521ea21a57d23591
8410893f1f88c5d9ab327bc139ff295d
cc7207f09a6fe41c71626ad4d3f127ce
e01b393e8897ed116ba9e0e87a4b1da1
ef25d934d12684b371a17c76daf3662c
faa8eaed63c4e9f212ef81e2365dd9e8
ce65092fe9959cc0ee5a8408987e3cd4
d9a6725b6a2b38f96974518ec9e361ab
270902c6bb6844dc25ffaec801393245
4e07a477039b37790f7a8e976024eb66

KPMG

KPMG Cyber Threat Intelligence Platform

Indicator of Compromise

Indicators of Compromise: Hashes
f756083b62ba45dcc6a4d2d2727780e4
03a2f95e1c1d28d89f0475520b16e8ac
6102f77c85541d00b4c3bc95f100febc
46c1b81d2cc911a9dd1923b74f434d59
d45e50d0cc6c1342e40ea254edae091a
6f5a8bb0a3e47db08b679da0167ae5f7
90fe0a9946d49cda2c979a4f03c71c43
1f737f7e9c18faa39d222806e05448fe
9becb385c52c422a93a5d626e8072780
158c7382c88e10ab0208c9a3c72d5f579b614947
64a1785683858d8b6f4e7e2b2fac213fb752bae0
84e749c37978f9387e16fab29c7b1b291be93a63
313b231491408bd107cecf0207868336f26d79ba
b062773bdd9f8433cbd6e7642226221972ecd4e1
0d3a5725b6f740929b51f9a8611b4f843e2e07b1
87635d7632568c98c0091d4a53680fd920096327
09ce87f436e23234b713fa3975b279987c3fe1f2
436a726f735b2cc057f007a852de030aec3dc5d4
a45ceda6d23cd0c4fe9f53aa43e6f0c36e1b4467
4093e5dfc182297c1d0e0c9e8fc47e942c971d61
19d259f8396868a3106c22ce72e8126495e11505
b28606b9feb83d2d51d8253767b53e23abb406f7
6b831413932a394bd9fb25e2bbdc06533821378c
78294dfc4874b54c870b8daf7c43cfb5d8c211d0
f64c63f6e17f082ea254f0e56a69b389e35857fd
204a603c409e559b65c35208200a169a232da94c
ecd001aeb6bcbafb3e2fda74d76eea3c0ddad4e6e7ff1f43cd7709d4b4580261
318c431c56252f9421c755c281db7bd99dc1efa28c44a8d6db4708289725c318
28df5c75a2f78120ff96d4a72a3c23cee97c9b46c96410cf591af38cb4aed0fa
4a9b37ca2f90bfa90b0b8db8cc80fe01d154ba88e3bc25b00a7f8ff6c509a76f
08530e8280a93b8a1d51c20647e6be73795ef161e3b16e22e5e23d88ead4e226
b9f526eea625eec1ddab25a0fc9bd847f37c9189750499c446471b7a52204d5a
27c51026b89c124a002589c24cd99a0c116afd73c4dc37f013791f757ced7b7e
7b024deda9a285ce08cdea266a351c5714ca61e6799cf12aa474ccdf04363a68

KPMG

KPMG Cyber Threat Intelligence Platform

Indicator of Compromise

Indicators of Compromise: Hashes
6a4dbc5011708c030c7f4a36abbc0e2a26228f7a0e6d799b2f6a77998f1168c2
6b4d133ed7b4686c04a502e597e90e8dd2486c44d317b805fca72d671eec404c
b4fda51b2259c17f82833890474f21b06a534dbf782f0f0c898631c8c10b9818
0c365d9730a10f1a3680d24214682f79f88aa2a2a602d3d80ef4c1712210ab07
2eef273af0c768b514db6159d7772054d27a6fa8bc3d862df74de75741dbfb9c
db034aeb3c72b75d955c02458ba2991c99033ada444ebed4e2a1ed4c9326c400
25cbfb26265889754ccc5598bf5f21885e50792ca0686e3ff3029b7dc4452f4d
1e9fc7f32bd5522dd0222932eb9f1d8bd0a2e132c7b46cfcc622ad97831e6128
ea4561607c00687ea82b3365de26959f1adb98b6a9ba64fa6d47a6c19f22daa4