KPMG Cyber Threat Intelligence Platform

APT 42 – A con artist with phony tricks

Active since 2015, APT 42 is an Iranian cyber espionage group that primarily targets Middle Eastern countries along with USA and Australia owing to the nation state's strategic interest. The group targets its victims by establishing trust, gaining access to personal and business emails, and deploying Android and Windows info-stealers, spyware and even ransomware in few cases. They have been extensively targeting think-tanks, researchers and journalists across various sectors like non-profits, education, healthcare, legal, manufacturing and media.

Threat actor starts their operation with a spear phishing campaign containing fake Google book pages or Gmail account sign-in pages which aid in harvesting credentials and 2FA codes. Further, the stolen credentials are used for targeting other victims. In the second phase, the threat actors build rapport & confidence with victims through benign conversations by impersonating journalists or researchers. Post establishing trust, a PDF attachment containing a shortened URL of a credential harvesting page impersonating popular university or Google or Yahoo login page is sent via previously compromised email accounts. APT42 then hides its trail by deleting the sent mail from the sent box of the compromised email account. APT42 also sets up SMS-based OTP capturing service to bypass MFA and accesses files & documents through the M365 environment in search of any data of interest to Iran. In addition to spear phishing, APT42 involves in surveillance activities by infecting mobile devices of the victims with Android malware such as VINETHORN and PINEFLOWER which are dropped via text messages.

With nation-backed interests, patience and perseverance, APT42 is expected to continue operations. Hence it is imperative for organizations to keep their guards up in all forums to not fall prey.

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

APT 42 – A con artist with phony tricks

Indicators of Compromise: Hashes
da7d37bfb899a0094995944d4c5e2f21
df02a8a7cb2afb80cc2b789d96f02715
3d67ce57aab4f7f917cf87c724ed7dab
04a6997f0a8021b773ebb49977bc625f
34d37f64613f3fe00086ac8d5972db89
8e0eb3ceb1bbe736beaf64353dda1908
63cd07e805bcd4135a8e3a29fa3ceebd
0a3f454f94ef0f723ac6a4ad3f5bdf01
ae797446710e375f0fc9a33432d64256
60e6523d29e8a9b83f4503f2e7fd7e1d
00b5d45433391146ce98cd70a91bef08
335849d8fb13a4a189ba92af9bdf5d1d
9d0e761f3803889dc83c180901dc7b22
f3d25b1cedf39beee751eb9b2d8d2376
a04c2c3388da643ef67504ef8c6907fb
96444ed552ea5588dffca6a5a05298e9
afb5760c05db35a34c5dc41108ba72c2
d30abec551b0fb512dc2c327eeca3c43
9dd30569aaf57d6115e1d181b78df6b5
bdf188b3d0939ec837987b4936b19570
651d72776c0394693c25b1e3c9ec55d0
b7bc6a853f160df2cc64371467ed866d
88df70a0e21fb48e0f881fb91a2eaade
9a1e09b7ce904eefb83dc8d7571826f9
9bd1caf6b79f6a69981a15d649a04c19
3c6302fb6bdb953e2073a54b928fad9c
bdf188b3d0939ec837987b4936b19570
651d72776c0394693c25b1e3c9ec55d0
b7bc6a853f160df2cc64371467ed866d
8a847b0f466b3174741aac734989aa73
9624d9613fe8cdc6833888b9e68892565e3a5d11
03d7ffd758e98c9a2c8c4716c93f09687000e22e
470b850363677d3d54629a92ac8b5143f4584a09
3b9a2e34f5d603b55cf7fd223d4e5c784b805242

KPMG

KPMG Cyber Threat Intelligence Platform

APT 42 – A con artist with phony tricks

Indicators of Compromise: Hashes
66d36d0b170cf1a0001cca16357961a2f28cba60
08d2aea84d6c148ff2ad4653856fb080eb99abf2
2374f5a9278b209563e8193847a76c25c12eec8f
d08982960d71a101b87b1896fd841433b66c7262
29175a0015909186f69f827630ef3fe2c1c5302c
6303907ec7d1d591efffe876720a0ab051bfd429
7649c554e87f6ea21ba86bb26ea39521d5d18151
08270b049ae33f0bcd1d207ed77f999d51a09d94
ecf9b7283fda023fa37ad7fdb15be4eadded4e06
dbb64b0202bb4da6796279b5fa88262a6e31787e
b66ae149bbdfc7ec6875f59ec9f4a5ae1756f8ba
1504da49f6fe8638c7e39d4bcb547fbb15376462
8f2bc0d6adfb4cad43fdda9f3d732c859eb79e35
280b64c0156f101eaad3f31dbe91f0c1137627dc
aba938bf8dc5445df3d5b77a42db4d6643db4383
e45aeccb798f5cf6cb5d877821d1f4aa7f55cf6f
e3712e3d818e63060e30aec2a6db3598cbf0db92
e8f50ecea1a986b4f8b00836f7f00968a6ecba4f
448e6d519a340845a55b4b1809488427c0d79cdd
75b7db0597f234838e7c8431b57870411842775d
186f07279ac0f15cc7be5caf68addabb2091bc84
aba938bf8dc5445df3d5b77a42db4d6643db4383
e45aeccb798f5cf6cb5d877821d1f4aa7f55cf6f
e3712e3d818e63060e30aec2a6db3598cbf0db92
03eadb4ab93a1a0232cb40b7d2ef179a1cd0174d
b9b783ad3bc523a031cdf799dd9739a7bcbcf184e7e64a0f3cc2170be4d4526f
7a650d3b1e511a05d0441484c7c7df59a63003ce77cd4eb7081323fd79d2b9a3
a37a290863fe29b9812e819e4c5b047c44e7a7d7c40e33da6f5662e1957862ab
7eb564f0afc23cc8186e67f8c0d7e6c80215b75c9f0c4b35f558a9e35743ca41
003676e6240421426e5c0919eb40bdde52b383eb1c54596deb77218c3885cdc5
2c33b1dd793ad5e59180719d078301ee7ebb6cf7465286c19b042accca6ac749
a485ef522a00edc7eb141f4ef982dd52b3e784ea8d8f1bb0ca044a61ce642eac
6618051ea0c45d667c9d9594d676bc1f4adadd8cb30e0138489fee05ce91a9cb
734d9639fcfffef1a3c360269ccc1cda4f1d0e9dc857fa438f945e807b022c21

KPMG

KPMG Cyber Threat Intelligence Platform

APT 42 – A con artist with phony tricks

Indicators of Compromise: Hashes
3cad59c65ee1e261658c2489dc45a7c6875d8ccb917d291d282e48bca1b74752
2c92da2721466bfbdaff7fedd9f3e8334b688a88ee54d7cab491e1a9df41258f
971c5b5396ee37827635badea90d26d395b08d17cbe9e8027dc87b120f8bc0a2
d4375a22c0f3fb36ab788c0a9d6e0479bd19f48349f6e192b10d83047a74c9d7
90e5fa3f382c5b15a85484c17c15338a6c8dbc2b0ca4fb73c521892bd853f226
c2c1d804aeed1913f858df48bf89a58b1f9819d7276a70b50785cf91c9d34083
9410963ede9702e7b74b4057fee952250ded09f85a4bb477d45a64f2352ec811
4bcc2ad5b577954a6bd23aff16566ce0784a71f9526a5ae849347ae766f4033f
21c5661eb5e54d537c6c9394d7bd4accf53e06851978a36c94b649c4f404a42e
9f2bc9aebb3ee87cfbdef1716b5f67834db305cf400b41b278d5458800c5eeeb
28de2ccff30a4f198670b66b6f9a0ce5f5f9b7f889c2f5e6a4e365dea1c89d53
c0d5043b57a96ec00debd3f24e09612bcbc38a7fb5255ff905411459e70a6bb4
a8c062846411d3fb8ceb0b2fe34389c4910a4887cd39552d30e6a03a02f4cc78
c1664df788f690fd061994ed3eb9d767e2f293448ce9d7ff5bff37549e9e4dab
afd06652b24811d7e03d5525b292293dbdf49b8c0e450d748cab0289aecdbc02
5ee98a677f58b897df3287448e63a1a781d312d2a951f438e1d7e4ab658fa4a0
110c77f66a8d4d8ccc9dc468744302cf368efd071e3e4af39338b699f6bc7808
28de2ccff30a4f198670b66b6f9a0ce5f5f9b7f889c2f5e6a4e365dea1c89d53
c0d5043b57a96ec00debd3f24e09612bcbc38a7fb5255ff905411459e70a6bb4
a8c062846411d3fb8ceb0b2fe34389c4910a4887cd39552d30e6a03a02f4cc78
5d3ff202f20af915863eee45916412a271bae1ea3a0e20988309c16723ce4da5