KPMG

KPMG Cyber Threat Intelligence Platform

APT41 – Deploying Sophisticated Tools for Cyber Espionage

APT41 (aka Double Dragon, Earth Baku) is a sophisticated Chinese threat actor engaged in state-sponsored espionage and financially motivated activities. Active since 2007, APT41 has recently enhanced its operations by deploying advanced tools. Their latest focus involves targeting the video game industry through tactics like source code theft and virtual currency manipulation. They have impacted sectors like healthcare, high-tech, shipping, and telecommunications, affecting countries such as Italy, Spain, UK, Taiwan, Thailand, and Turkey.

Initial access is gained by exploiting known vulnerabilities or phishing emails with malicious attachments. This leads to deployment of ANTSWORD and BLUEBEAM webshells to download and execute the DUSTPAN dropper for persistence. DUSTPAN decrypts and loads the chacha20 encrypted Cobalt Strike BEACON backdoor, masquerading as a valid Windows binary. The BEACON then establishes communication by either using a self-managed infrastructure hosted behind Cloudflare or it utilizes Cloudflare Workers as its C2 channels. Upon establishment of C2, DUSTTRAP dropper is deployed which decrypts and loads an AES-128-CFB encrypted PE file into the memory for decrypting configuration data and plugins DLLs. The plugins manage network setup, encryption, and additional plugin downloads. Plugin loading is performed by trojanizing a legitimate DLL, injecting the malicious plugin code in it's .text section to call "ZwCreateSection", then restoring it to evade detection. Finally, the group leverages SQLULDR2 to export data from Oracle Databases, and PINEGROVE to exfiltrate large volumes of sensitive data and upload it to OneDrive.

APT41's evolution to advanced malware and software supply chain attacks shows a significant increase in sophistication, highlighting the need of enhanced security measures.

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

APT41 – Deploying Sophisticated Tools for Cyber Espionage

Indicators of Compromise: IP Addresses	
45.84.1[.]181	185.118.167[.]40
45.153.231[.]31	107.172.210[.]69
149.28.15[.]152	172.104.206[.]48
194.156.98[.]12	67.205.132[.]162
182.239.92[.]31	103.238.225[.]37
95.164.16[.]231	194.195.125[.]121
152.89.244[.]185	

Indicators of Compromise: Domains	
macfee[.]ga	agegamepay[.]com
notped[.]com	ageofwuxia[.]com
paniesx[.]com	ageofwuxia[.]net
dnsgogle[.]com	ageofwuxia[.]org
ns2.akacur[.]tk	gxxservice[.]com
ns1.akacur[.]tk	win7update[.]net
byeserver[.]com	ageofwuxia[.]info
gamewushu[.]com	linux-update[.]net
ibmupdate[.]com	operatingbox[.]com
infestexe[.]com	symanteclabs[.]com
kasparsky[.]net	microsoftfile[.]com
micros0ff[.]com	techniciantext[.]com
micros0tf[.]com	xigncodeservice[.]com
serverbye[.]com	sexyjapan.ddns[.]info

Indicators of Compromise: Hashes
ac125aea0b703de37980779599438b4a
17d0ada8f5610ff29f2e8eaf0e3bb578
9991ce9d2746313f505dbf0487337082
c33247bc3e7e8cb72133e47930e6ddad
cfce85548436fb89a83bf34dc17f325d
e98b9e21928252332edf934f3d18ac21
8222352a61eacca3a1c6517956aa0b55
dc725f5e9b1ae062fbec86ee4d816b45

KPMG

KPMG Cyber Threat Intelligence Platform

APT41 – Deploying Sophisticated Tools for Cyber Espionage

Indicators of Compromise: Hashes
46a557fbdce734a6794b228df0195474
77c60e5d2d99c3f63f2aea1773ed4653
849ab91e93116ae420d2fe2136d24a87
36711896cfeb67f599305b590f195aec
7d51ea0230d4692eeedc2d5a4cd66d2d
a0a96138b57ee24eed31b652ddf60d4e
ba08b593250c3ca5c13f56e2ca97d85e
223e4cc4cf5ce049f300671697a17a01
37e100dd8b2ad8b301b130c2bca3f1ea
557ff68798c71652db8a85596a4bab72
830a09ff05eac9a5f42897ba5176a36a
b0877494d36fab1f9f4219c3defbfb19
c8403fabda4d036a55d0353520e765c9
ff8d92dfbcda572ef97c142017eec658
ffd0f34739c1568797891b9961111464
72584d6b7dd10c82d9118567b548b2b1
97363d50a279492fda14cbab53429e75
a6c7db170bc7a4ee2cdb192247b59cd6
5e87b09f9a3f1b728c9797560a38764b
8c6cceae2eea92deb6f7632f949293f0
03f2f030182fe2f3d90a4b2584da798b36f35979
f94225fe2c835cf1afe7ca35bef3e9f99735ebf0
c5292d299094d778e6c1e7f3424b6d75b2245b30
2fce25afb8a29fcd526f61ba30f14dcc7ecfad3e
df2ebd205e1ad722a6255badbca2496583764507
00d2512b5596b4f1150cd13c284727a4fcb1d73e
f751fd089a2a9b5f5ed8aef52c24d82689c171b1
87c0d042d98345f967ac03d0a67199ae9fac3641
2cc76a0434a1d489c1547c7021a3dd68499141c3
c3874d5cc7e82ad373b67a3650b0dfee7c219f8f
56b0dec07b2c7f39e6f21af1fd172c6b86016f62
2ed5a7067b23b243b4998a09a6d925a3b4737b67
5e08fc83cd4bdc38a4fe374559d2c15550c079cf
d44ee36435344eca49aea84ec28370cde7ca2332

KPMG Cyber Threat Intelligence Platform

APT41 – Deploying Sophisticated Tools for Cyber Espionage

Indicators of Compromise: Hashes
d0429abec299ddfee7e1d9ccff1766afd4c0992b
6f065eea36e28403d4d518b8e24bb7a915b612c3
82072cb53416c89bfee95b239f9a90677a0848df
f067443c2c4d99dc6577006a2f105e51af731659
f1a181d29b38dfe60d8ea487e8ed0ef30f064763
5a85d1e19e0414fc59e454ccbaef0a3c6bb41268
67c957c268c1e56cc8eb34b02e5c09eae62680f5
b193ff40a98cd086f92893784d8896065faa3ee3
c40db0438a906eb0bec55093f1a0f2cc4cdc38104af0b4b4b3f18200a635c443
c3efcb6efad675613721910a783389a646b2d138c7721df9849b28952d25bcfc
069ca8ae8a3909aa4717832d911d646c536fed4c907866724f74daf4d740f41a
22a50cea6ad67a7e8582d2cd4cdc3eaaf57c0fbe8cd062a9b15710166e255a86
073b35ecbd1833575fbfb1307654fc532fd938482e09426cfb0541ad87a04f75
7586e58a569c2a07d0b3a710616f48833a040bf3fc57628bbdec7fcb462d565a
c7dce6c950735bfcf2125be8eb1f3dd468eeb56a1c615c34f95bf38cb58b7d3a
6b37e0e0b0586769bc7b32ae3e0bc2f29e8ad2a1d3de07d50bb3e5489e2dd136
c6a3a1ea84251aed908702a1f2a565496d583239c5f467f5dcd0cfc5bfb1a6db
33fd050760e251ab932e5ca4311b494ef72cee157b20537ce773420845302e49
8407defe0cc29d04b8d0f519b5008d30c09783fe0c63aad5ccb0950fc9a98406
cdc619734f4e2aba0137b5fe9faf36896b85dff7cd4a93de562de770777d181a
e5c7089eb3297b204aaabdb4a660d125a948ba869d2a7cf3cf7c0098125b5ef5
bd058a6fd20347f21c38115490aef858d06f26b49b9d7be357297e60bd2934cc
b0890685b25c6736827573e9536b2bf8c42dbaf36760fc947d461efdb6309aec
3a7dfc0850136c59104d362b11183a5a61511d056ef393f6a6a63fdba9bbb804
bc92e8e964e0492b3595d9470e59941bded90082040ac436583b9f3269e1e550
ed606d718874c29b9a1101775069d694b67eb5a4492404ddd98ebfcdcfcce205
c02accc26a389397fb172f83258baa8a974986ffd706ba708a3b0a679f61be56
166b6dcdac31f4bf51e4b20a7c3f7d4f7017ca0c30fa123d5591e25c3fa66107
e5f1360d4c299bb32e33e081115f2b520251a983af2ebc649b4b9b70308246fe
ab56501167fe689fe55f6e6ddc3bb91952299bd5c3ef004b02bf1c3b4061c7cf
0faddbe1713455e3fc9777ec45adf07b28e24f4c3ddca37586c2aa6b539898c0
1c88150ec85a07c3db5f18c5eedcb0b653467b897af01d690ed996e5e07ba8e3
e024ccc4c72eb5813cc2b6db7975e4750337a1cc619d7339b21fdbb32d93fd85
d7e8cc6c19ceebf0e125c9f18b50167c0ee65294b3fce179fdab560e3e8e0192

Indicators of Compromise: Hashes
ebf28e56ae5873102b51da2cc49cbbe43192ca2f318c4dfc874448d9b85ebd00
062a7399100454c7a523a938293bef7ddb0bc10636ed402be5f9797d8cc3c57e
a4647fcb35c79f26354c34452e4a03a1e4e338a80b2c29db97bba4088a208ad0
993d14d00b1463519fea78ca65d8529663f487cd76b67b3fd35440bcdf7a8e31
049a2d4d54c511b16f8bc33dae670736bf938c3542f2342192ad877ab38a7b5d
d00b3edc3fe688fa035f1b919ef6e8f451a9c2197ef83d9bac3fa3af5e752243
7096f1fdefa15065283a0b7928d1ab97923688c7974f98a33c94de214c675567
c667c9b2b9741247a56fcf0deebb4dc52b9ab4c0da6d9cdaba5461a5e2c86e0c
7e0c95fc64357f12e837112987333cdaf8c1208ef8c100649eba71f1ea90c1db
4aa6970cac04ace4a930de67d4c18106cf4004ba66670cfcdaa77a4c4821a213
42d138d0938494fd64e1e919707e7201e6675b1122bf30ab51b1ae26adaec921
7566558469ede04efc665212b45786a730055770f6ea8f924d8c1e324cae8691
7cd17fc948eb5fa398b8554fea036bdb3c0045880e03acbe532f4082c271e3c5
490c3e4af829e85751a44d21b25de1781cfe4961afdef6bb5759d9451f530994
63e8ed9692810d562adb80f27bb1aeaf48849e468bf5fd157bc83ca83139b6d7
79190925bd1c3fae65b0d11db40ac8e61fb9326ccfed9b7e09084b891089602d
c51c5bbc6f59407286276ce07f0f7ea994e76216e0abe34cbf20f1b1cbd9446d
e65d39fa659f64a57ee13e8a638abd9031fa1486311d2782f32e979d5dee1ca5
2eea29d83f485897e2bac9501ef000cc266ffe10019d8c529555a3435ac4aabd
5d971ed3947597fbb7e51d806647b37d64d9fe915b35c7c9eaf79a37b82dab90
70c03ce5c80aca2d35a5555b0532eedede24d4cc6bdb32a2c8f7e630bba5f26e
3e6c4e97cc09d0432fbbbf3f3e424d4aa967d3073b6002305cd6573c47f0341f
9283703dfbc642dd70c8c7667528552690e998bcb3f3374273c0b5c90c0d1366
f4d57acde4bc546a10cd199c70cdad09f576fdfe66a36b08a00c19ff6ae19661
0055dfaccc952c99b1171ce431a02abfce5c6f8fb5dc39e4019b624a7d03bfcb
faedf9fef6edac2f0565882112b2eae14edda024239d3218a9fe9ac7e0b12db6
462a02a8094e833fd456baf0a6d4e18bb7dab1a9f74d5f163a8334921a4ffde8
92cb362ae8d24c05f368d13036534fe014344994d46031a0a8636a7ca0b792c6
354c174e583e968f0ecf86cc20d59ecd6e0f9d21800428453b8db63f344f0f22
bae8f4f5fc959bff980d6a6d12797b0d647e97cc811c5b9e827d0b985d87f68f