Geopolitical nation-state threat actor overview June 2021

anchorednarratives.substack.com/p/geopolitical-nation-state-threat-794

RJM

Tracking nation-state apt actors, like Desert Viper, OceanLotus, APT34, APT41, and TransparentTribe in areas with high geopolitical tensions via Twitter threat intelligence

RJM

Jul 2, 2021

Disclaimer: The views, methods, and opinions expressed at Anchored Narratives are those of the author and do not necessarily reflect the official policy or position of my employer.

Cover: Indian power companies are targeted by the ReverseRat threat actor

Introduction

June ended as the month of #PrintNightmare, and the critical vulnerability impacts many organizations. Many of the (nation-state) threat actors will likely abuse this flaw if they were not already abusing it. Like last month, an overview of this month's observed cyber operations was shared by security researchers via Twitter. Where applicable, I will briefly describe the geopolitical tension between states. In this month's overview, IOC's from nation-state threat actors were selected that presumably originate from actors from Vietnam, China, India, and Pakistan, by basically searching for the keywords "***apt***" and "***c2:***" or "**c2**" over the

collected Twitter data from June 2021. The reported IOC's have not been examined yet and are therefore weakly anchored with evidence. But let's see what has been shared by security researchers for June 2021.

Middle East

Figure 1:Middle East

Gaza

In June, the following campaign was shared via Twitter by the alleged Palestinian threat actor dubbed APT-C-23 or Desert Viper.

```
"New #APT #APT-C-23 #micropsia sample md5 : 8c560cf2281320736e03f126d978ba28
filename:Experience or leadership skills experience or leadership skills.exe
C2:howard-maria[.]me
Drops generic CV template as decoy (cb142b1fe66cd3720b7d2cb054d50f82)"
```

Some other malware samples were also shared on Twitter:

```
"#APT-C-23 #AirdViper #CTI #APT e38c06f83a5c1b0a4f82c965a4c78654
15398d1f1280c5b40deae7f91cc06b36
5ea012cc4aca5eb4ff4211ae32dabb9d
8bd5dd1fe94bf55a3fcf16d669a90686
https://t.co/fSzwFdHV9M"
```

Some researchers on Twitter refer that the above samples might indicate that EgyptAir might be a target of the actor.

```
"New sample seems used by #APT-C-23. Once it gets executed, a document relating to
infomation about #EgyptAir is shown to confuse the victim and meanwhile  #RAT is
executed to perform remote control.
https://t.co/vm1moMOxIW
https://t.co/7NrAFW5duH
823bf27b1e559d6607f5224ab99de1c83bb5d36e2ed0e6644d551e94ec45d248

"#APT-C-23 #AirdViper #CTI #APT
335e604a7c3866b3fad6e8ee6989ddb9
The position of the president and the leadership on the elections and the
corresponding proposals for the decrees https://t.co/KQ6yiTslm2"
```

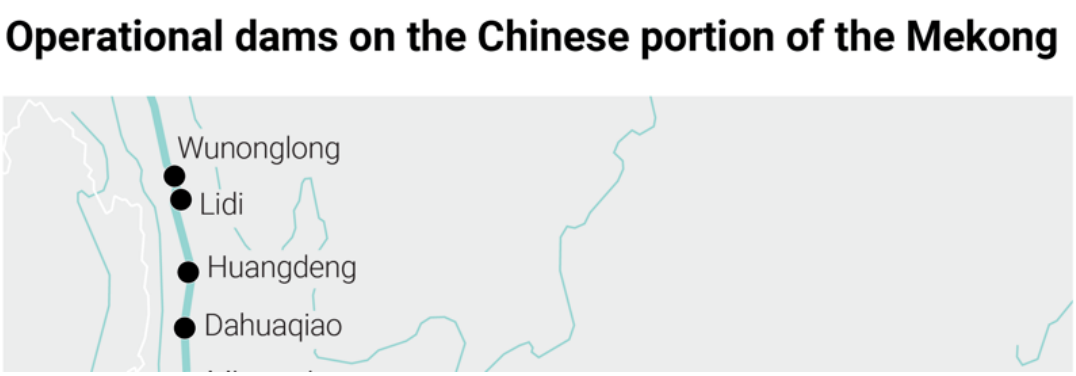
Iran

I will not go into disputes with other countries because there are many tensions between Iran's neighbors or the United States. Iran as a country is protected by mountains that are natural borders and is one of the highly populated and educated countries in the region. Therefore also a force to reckon with. There a multiple alleged nation-state actor groups that originate from Iran. For an overview of actors, visit the threat actor card maintained by the Thai Cert. This month the following activity was observed of APT34 or Oilrig. One of the actor groups which is held responsible for the Shamoon attacks in 2012.

```
"#APT
Sample from #APT34 Group:1858b880e23f1df3735f00719c2c28a3
We also spot an attack where DNS tunneling was used, suspected belong to #APT34, here
are the captured samples:
a90ae3747764127decae5a0d7856ef95
e2919dea773eb0796e46e126dbce17b1"

"#APT34
#oilrig
63ff31ede9713c10ba6b6f965167cbbd
ab25014c3d6f77ec5880c8f9728be968
e7737a2e170459905216622f2d43e4da
host:\"https://t.co/G6RQLX1vlH[.]lb\"
username:\"sig.dir.logistic\"
password:\"P@ssw0rdSigL0g\"
to:\"masters.michelle@protonmail.com\""
```

Asia




Miaowei
Gongguoqiao
Xiaowan
Manwan
Dachaoshan
Nuozhadu
Jinghong
CHINA
VIETNAM
MYANMAR
LAOS
Vientiane
Mekong River
THAILAND
Bangkok
CAMBODIA
Phnom Penh
Gulf of Thailand
Mekong Delta
100km

Source: The Stimson Centre SCMP / Mapcreator

Figure 2: Dam tensions in Laos, Thailand, and Vietnam

Vietnam

China is building multiple dams on the Mekong river. This also impacts the water flow downstream and impacts the irrigation of Myanmar, Thailand, Cambodia, and Vietnam. Since the building of the damns by China, geopolitical tensions are growing. Water is the new oil, and whoever controls it gains power. This, among other disputes, brings tensions in the South China Sea. Multiple threat actors are tracked from this region. One of them originates from Vietnam and is dubbed OceanLotus or APT32.

The following samples of APT32 were collected during June via Twitter.

```
"Today our researchers have found #RotaJakiro #ELF implant which maybe copy from
#Oceanlotus #APT group
ITW:1242ae39377b855f10fee9d61188dba9"

"Today our researchers have found #RotaJakiro #ELF implant which maybe copy from
#Oceanlotus #APT group
ITW:b3771f1b343c575392b261cc9bbe5675
34596914beb5d8a615662a4b21e5c1f7"

"#APT #APT32 #OceanLotus Sample
MD5:3aac297222bd691edb2b9c3ccb5b7e4c"

"#APT#OceanLotus
MD5:92da5c6a3212a1b806d0729a07d0f1db
CobaltStrike payload
C2:sjbingdu[.]info
IP:185[.]225[.]19[.]100"
```

China

Mustang Panda

China has a tremendous amount of nation-state actor groups. One of them has been dubbed by Crowdstrike as Mustang Panda and targets aviation, Government, NGOs, Think Tanks worldwide.

```
"#MustangPanda #APT
1854b3dcd60b46e6039972824faea889435a19c3
Bing Malleable
C2 176.118.167.36
Usual campaign with DLL side load
(C:\\Users\\Public\\Libraries\\Touch\\AcroRd32.dll)"
```

```
"#MustangPanda #PlugX variant
Encrypted: https://t.co/UmLYbRPe2l
Decryption Key: 6f 41 68 53 4f 70 69 6b 56 Config:185.239.226[.]17:965
185.239.226[.]17:110
103.200.97[.]189:965
103.200.97[.]189:110 https://t.co/sERztfYgVk"
```

APT41

Although no direct indicators were shared on Twitter, AirIndia was compromised by an actor called APT41, according to threat intelligence company Group-IB. According to FireEye, APT41 is a prolific cyber threat group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control. The group targets the following sectors worldwide: Construction, Defense, Education, Energy, Financial, Government, Healthcare, High-Tech, Hospitality, Manufacturing, Media, Oil and Gas, Petrochemical, Pharmaceutical, Retail, Telecommunications, Transportation, Online video game companies.

The analysis of Group-IB was called the "Big Airline Heist." Their report contains many indicators of compromise. Their tweet is shared below.

```
"New Group-IB #ThreatIntelligence blog is live!
Group-IB team attributed #AirIndia incident with moderate confidence to Chinese
nation-state TA #APT41.
The campaign was codenamed #ColunmTK ⬇️
https://t.co/V3zgDuTsHS
https://t.co/ssAjD9ec24"
```

Pakistan

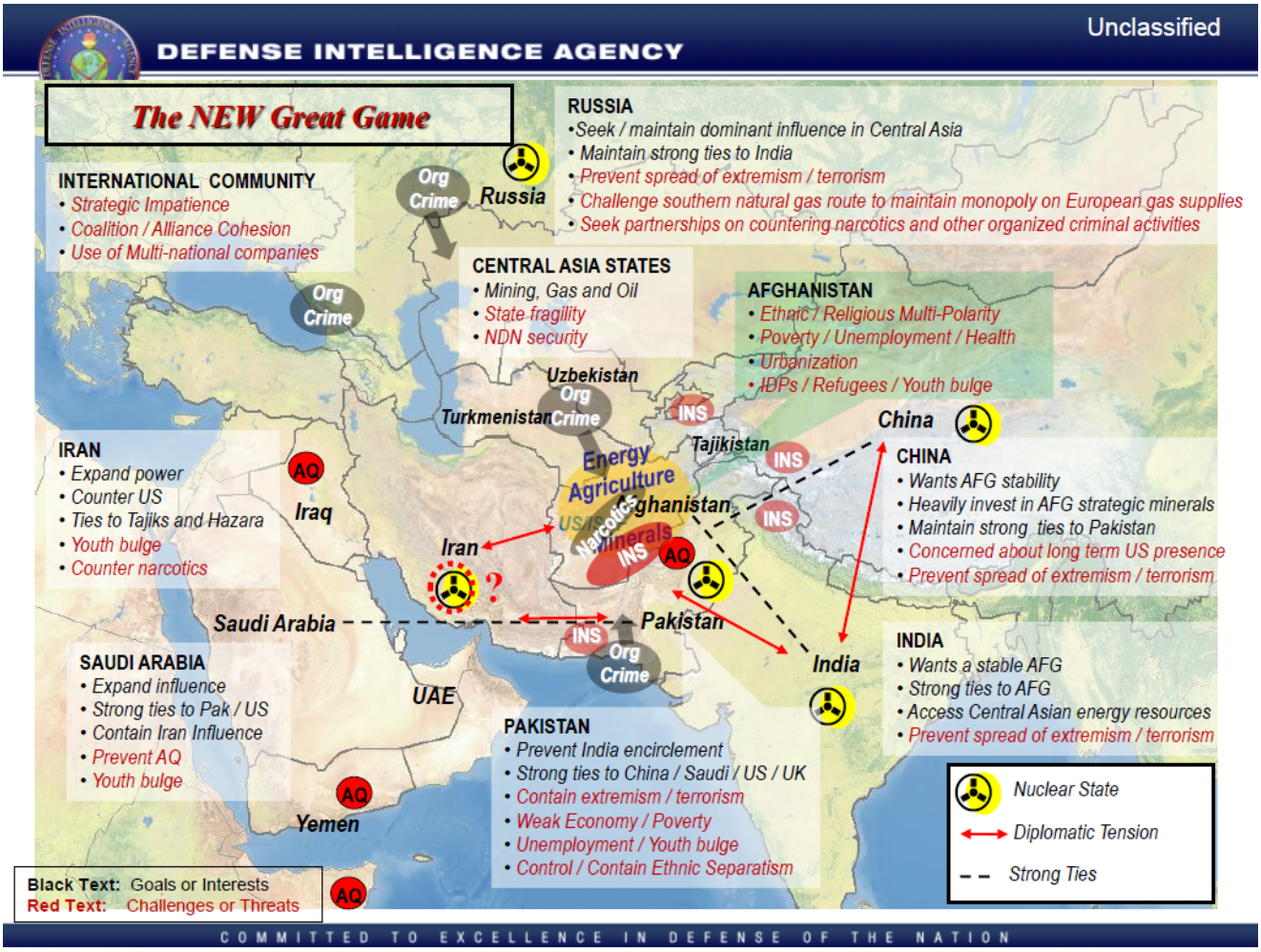


Figure 3: Pakistan and its neighbors (graphic courtesy Publicintelligence)

Also, in June, the alleged nation-state actor that belongs to Pakistan Transparent Tribe or APT36 has been very active.

For example, in June 2021, the following campaigns were shared on Twitter.

```
"Today our researchers have found sample which belongs to #TranSparentTribe #APT
group
ITW:4a7ff92e0ea13b41a5e3410c3becfb2e
filename:i.docm
C2:198.23.210.211:4898(8786)
https://t.co/WPoFbbR7MO"

"#TransparentTribe #APT:
Maldoc:Defence and security Agenda Point.ppt 54d5743efcc5511368c6c04bf6840a59
#Crimson Rat:6d88dcb578cef59d3d0244d1e93b0f57
trbgertrnion.exe
C2:167.160.166.80
Debug path:e:\\core-
projects\\adii\\trbgertrnion\\trbgertrnion\\obj\\Debug\\trbgertrnion.pdb
https://t.co/3Qc08jhvyN"
```

```
"This might be #TransparentTribe #APT maldoc:5cbcc3485f4286098b3a111ceec8ce54 Dropped
payload:c08e1509f379755df710d5a8fd4ff175
C2:5.189.170.84
Some other samples associated to this APT are using this
C2:b03e0568a5f26addc51c8a3e32baeb7f 9dadf9ce41994f869e8c35e1917b8238
https://t.co/tfw1uUrdfh"
```

Lastly, a new Pakistani APT, dubbed ReverseRat, was reported by Lumen in June, targeting medical and energy corporations in India. Indicators are listed below.


Ashish Kunwar @D0rkerDevil
Pakistani APTs targeting medical and energy corps in India . IOCs available . github.com/blacklotuslabs… #reverserat #IOC #Threat #ThreatHunting

blacklotuslabs/IOCsIOCs published by Black Lotus Labs. Contribute to blacklotuslabs/IOCs development by creating an account on GitHub.github.com
June 28th 2021

9 Retweets17 Likes

Conclusion

Twitter continues to be a valuable source to share threat intelligence on ongoing nation-state operations. In June 2021, many potential campaigns from different nation-state actors were reported on Twitter by security researchers or threat hunters in areas with high geopolitical tensions. A brief overview of some of these actors for June was outlined. Further research needs to be conducted if these IOCs can indeed be anchored to these aforementioned nation-states and understand more about their operations and victims. In the next article, I will further assess one or two potential interesting TransparentTribe malware samples

covered in this article to determine if tracking for such an actor can be improved or to gain a better understanding of their operations. Until next time and sharing is caring!
#TogetherWeAreStronger