Geopolitical nation-state threat actor overview May 2021

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

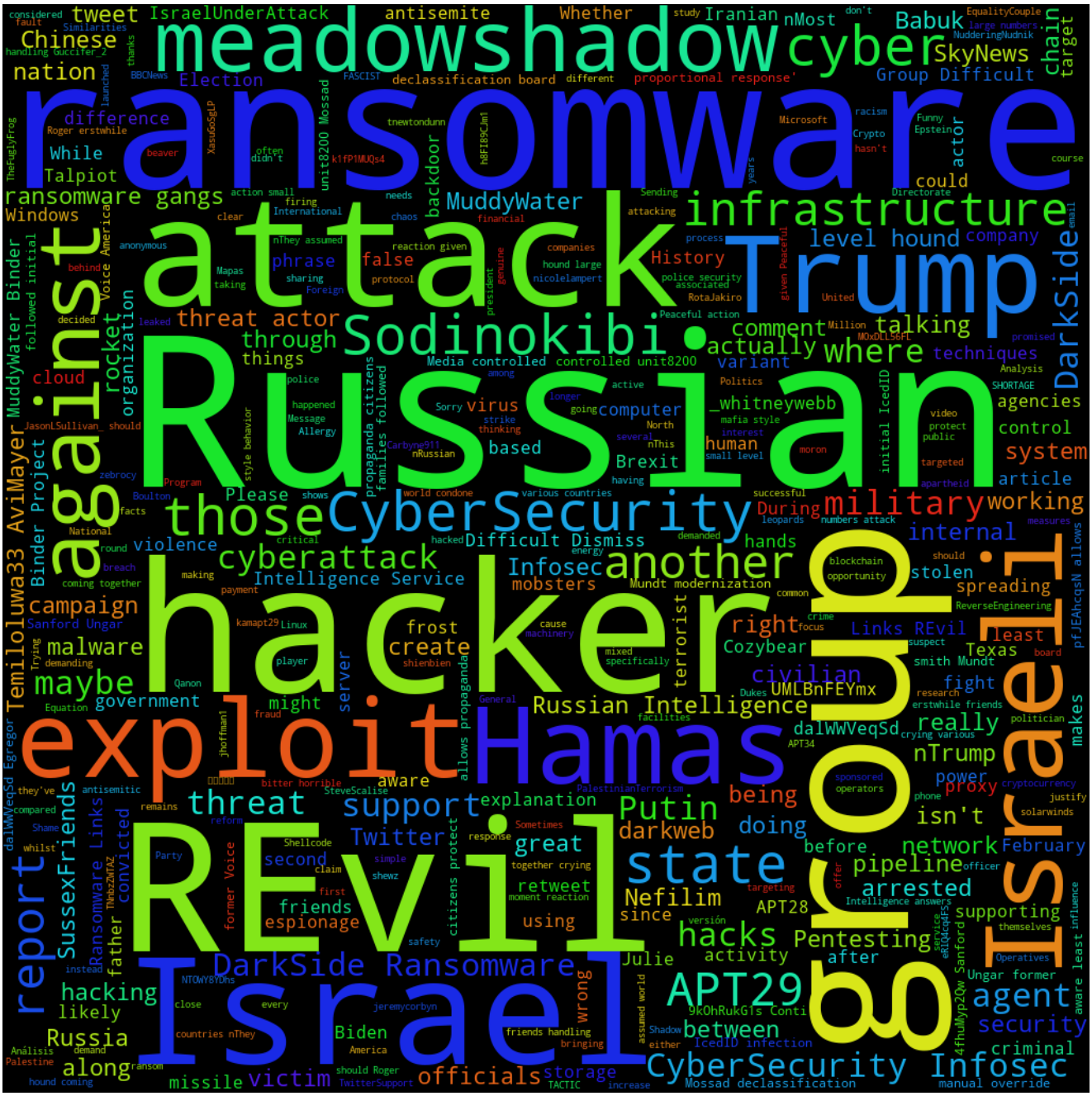
RJM

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

RJM

Jun 5, 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: Word cloud on the Twitter threat actor feed May 12, 2021 (Israel/Hamas)

Introduction

As I have previously described in the article about hunting for geopolitical tensions, the time has come to provide you a small overview of some interesting cyber operations observed and shared by security researchers via Twitter during May 2021. In this monthly overview, I will briefly describe the geopolitical tension between states and the reported cyber campaigns by the alleged nation-states by sharing actionable indicators of compromise (IOC's). In this month's overview, IOC's from nation-state threat actors were selected that originate from Palestine, India, and Pakistan, by basically searching for the keywords "***apt***"

and "***c2:***" over the collected Twitter data from May 2021. The reported IOC's have not been examined yet and are therefore weakly anchored with evidence. But let's explore the Twitter threat intelligence a bit further.

Middle East

Figure 1: Israel and its direct neighbors

At the beginning of May 2021, escalations between Israel and Palestine (Hamas) resulted in more than 3,440 rockets were fired towards Israeli cities. The dispute resulted in multiple casualties on both sides. The Israeli Defence Force (IDF) reported that it also disrupted Hamas cyber capabilities. As every physical dispute also has its cyber counterpart, the following campaign was observed by the alleged Palestinian threat actor dubbed APT-C-23 or Desert Viper by Kaspersky.

```
"#APT #APT-C-23 #micropsia 2021_05_30 About the Palestine-Israel Conflict in May
hash : d82e23359a756affdadc194b0a4271bf8a05c1a5755185567a4595bed6bd8106
filename:The unity of the people, the cause and the land docx.exe
C2:haleymartinez[.]me
https://t.co/8FQwjt4UHw"
```

Some other samples were also shared on Twitter:

```
filename:Questions about the study of freedoms 78639846 docx.exe
hash: 7833c0f413c1611f7281ac303bcef4b3
filename:The Palestinian Charter of Honor the Palestinian labor sector - docx.exe
hash: 6af6b474f627e8fff757060d3e39a2b6
filename:Biden assures US allies he will reverse Trump docx.exe hash:
b774dae8ebaa3b952dacaafa91871be3
```

India

Figure 2: India and China clash at the border June 15, 2020 (graphic NYT)

Since last year the geopolitical border escalations between India and China resulted in high tensions with many trade issues and banning certain Chinese apps in India. As India is also a growing power in the Asia-Pacific region, they have also matured their cyber operations in the past years. The following nation-state cyber actor groups are alleged to be Indian and have been detected by security researchers in May 2021.

Sidewinder APT group

The Sidewinder APT group has been observed since 2012 and targets mainly military targets.

```
"Today our researchers have found new rtf sample which belongs to #SideWinder #APT
group
ITW:344b7370c6e61812eeb1cf1d737f27f3
Topic: Building Port Resilience Against Pandemics C2:pmaesa[.]bahariafoundation[.]org
https://t.co/WUlmCTFGL7"
```

The lure document was taken from the following website.

```
"Today our researchers have found old #SideWinder #APT group sample which target at
China ITW:9016ed3c0fef18cfef81f71953e77572
filename:poly pending orders.doc
C2:cdn-gov[.]net
https://t.co/WwYarEWWce"
```

Bitter APT Group

The Bitter APT group leveraged a zero-day exploit this year and targeted China, Pakistan, and Saudi Arabia in different market sectors.

```
"#APT #BITTER #Malwarename:rftg.msi md5:72ff5729200a86d7d0e83dbfca87721b
download url:hxxp://sbss.com.pk/img/rftg.msi C2:http://helpdesk.autodefragapp[.]com
C2 url:http://helpdesk.autodefragapp[.]com/dFFrt3856ByutTs/xnb/data1.php?
id=WORK&amp;&amp;user=adminZxxZWindows7Professional"
```

Pakistan

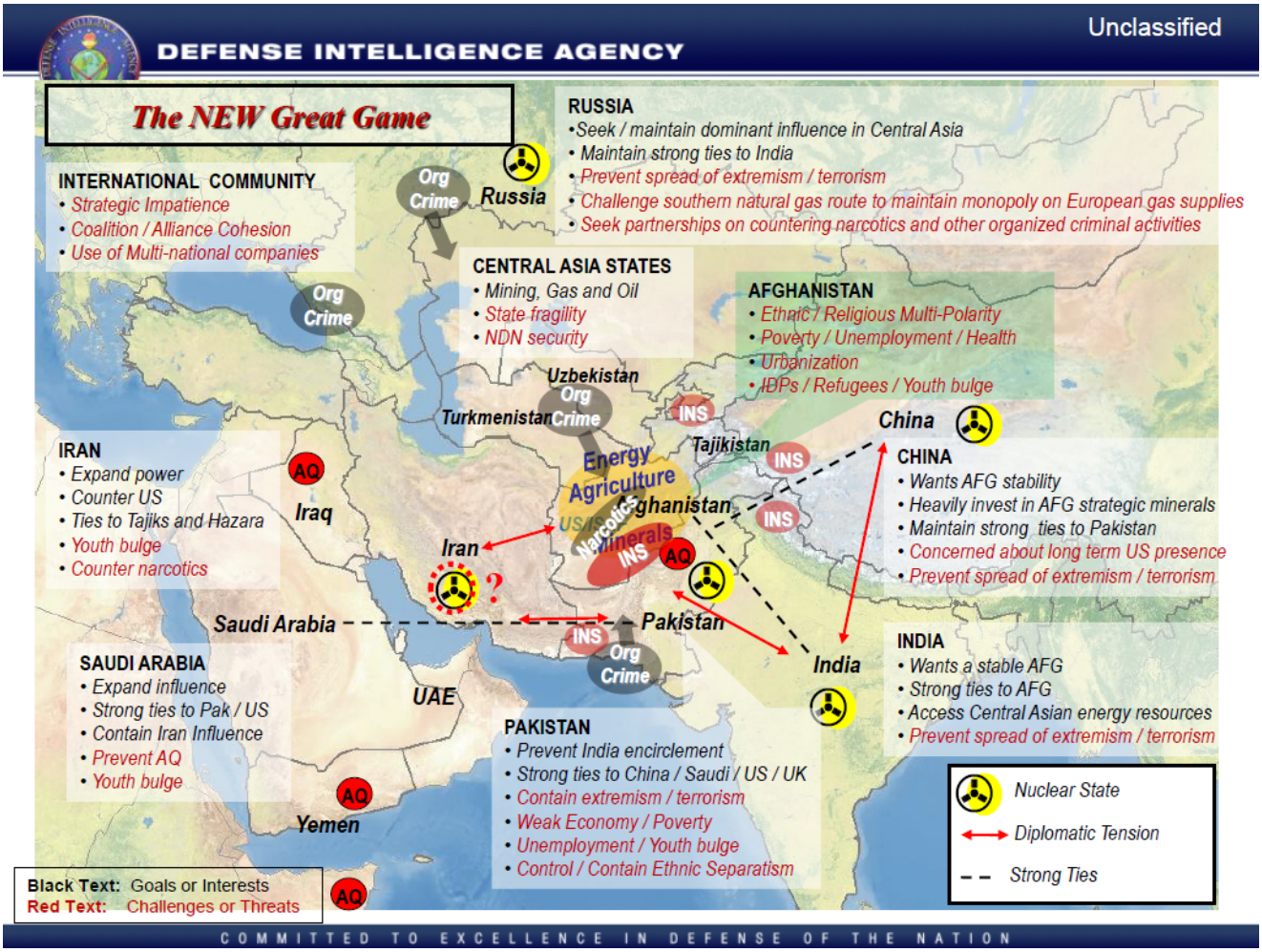


Figure 3: Pakistan and its neighbors (graphic courtesy Publicintelligence)

Pakistan and India have many geopolitical issues together, many also originating from the disputed region of Kashmir or the known Mumbai terrorist attack from 2008. From a cyber perspective, the alleged nation-state actor that belongs to Pakistan is dubbed Transparent Tribe or APT36. The group has been observed in campaigns against Indian diplomatic and

military resources. Cisco's Talos threat intelligence unit also shared an in-depth analysis of the TransParentTribe group in May. They shared that the group leveraged a new malware capability called ObligueRat, besides the already known CrimsonRat malware.

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

```
"Today our researchers have found sample which belongs to #TranSparentTribe #APT
group ITW:cb27d0bd9a97e053f3fbfcf4bba8b8fc
filename:Ultimate-File.docm
C2:134.119.181.142:6672
https://t.co/Ubnge6ThhR"

"Today our reseachers have found #oblique implant which belongs to #TransparentTribe
#APT group
Upload:NL
ITW:e98510e1252e7dd99012b23a400bb00b
filename: program.exe
C2:185.117.73.222:3344
https://t.co/xcraPu8HvQ"
```

Conclusion

Twitter seems a valuable source leveraged by security researchers to share threat intelligence on ongoing nation-state operations. In May 2021, many potential campaigns from different nation-state actors were reported on Twitter by security researchers or threat hunters in areas with geopolitical tensions. A brief overview of some of these actors for May 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 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!