Trouble in Asia and the Middle East. Tracking the TransparentTribe threat actor.

By RJM

Published: 2022-02-12 · Archived: 2026-04-05 23:40:32 UTC

Cover: Chabahar Port Iran, photo credit:www.tehrantimes.com

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

Welcome to the new subscribers of the Anchored Narratives mailing list. For those new to the list, I regularly pick an exciting tweet that matched my intelligence requirements and generated *anchored* stories on geopolitical (cyber) threats, digital forensics, and crime from that. Usually, I pick a story that I have no real in-depth or prior knowledge about. The goal is to understand a particular topic better, improve my investigation or writing skills, and generate a reliable story anchored with evidence that can be verified or challenged.

I have not been writing any stories lately as I started a great new job in September. I'm also working in incident response (IR) again with a lot of memory forensics! Awesome how Volexity has taken that field to the next level with a robust memory acquisition capability called Surge and a Volcano's memory analysis platform. I participated with the great George Garner Jr1., who unfortunately passed away in 2017, in a memory forensics challenge in 2005 where no software existed to analyze memory dumps.

But unbelievable how Volexity improved the acquisition and analysis piece with their products. However, they are commercial tools. I can only recommend them as they will provide you valuable insights into the *State* of a machine (integrity) in a certain period and decrease your root cause analysis time for breaches. The amount of forensic reconstruction from a collected memory sample the software can do is just something I have not

experienced before. We are even able to recover the entire exploit chains and backdoors executed by threat actors from memory. Just awesome.

But now, back to a new anchored narrative about a threat actor covered in the earlier monthly threat actor overviews of June and September, namely TransparentTribe.

With the revival of the Taliban in Afghanistan also geopolitical tensions in the neighboring countries changed drastically. What does this revival mean for China, India, and Pakistan? In this article, the nation-state actor, TransparentTribe matched my Twitter threat intelligence requirements 71 times since the beginning of this year. The threat-actor is likely originating from Pakistan and also linked to attacks on the critical infrastructure of India. Here we go!

In 2016 Proofpoint released a report “Operation TransparentTribe’ of a nation-state threat actor targeting India’s embassy staff in Saudi Arabia and Kazakstan via phishing attacks. Their research also unraveled attacks against Indian diplomatic and military resources via so-called watering holes attacks. A watering hole attack is a technique that hackers employ to compromise a popular website and infect its visitors with malware once they visit that infected website. Proofpoint then dubbed their malware as “MSIL/Crimson”, which later became known as CrimsonRat.

By 2017 CysInfo, shared an in-depth story about a threat actor who was impersonating the identity of an Indian Think Tank to Target the Central Bureau of Investigation (CBI) and Possibly Indian Army Officials. The registration information of the domains was traced back to a Pakistani telephone number and an IP address from Pakistan. The story’s author, known malware researcher, Monnappa K A, did not attribute it to TransparentTribe. However, his analysis was referenced in the Threat Actor Encyclopedia and attributed to the same group there.

In 2020 Kaspersky shared interesting research about the CrimsonRat Server component they detected and that the actor group targeted victims in Afghanistan and India.

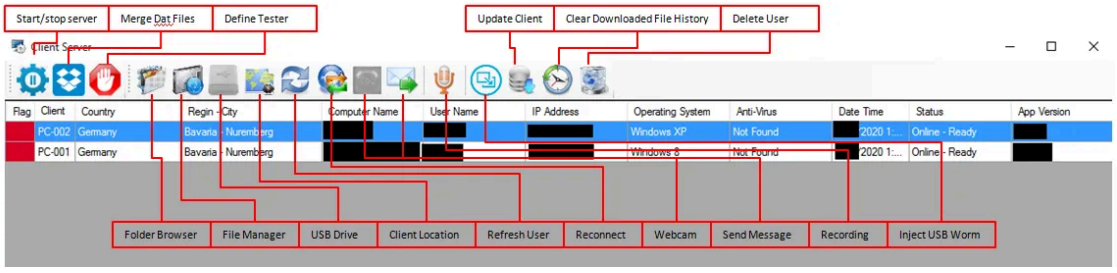

Figure 1: .Net Server component of CrimsonRat, reported by Kaspersky

CrimsonRat provides the espionage group with the following capabilities on the infected systems:

- manage remote filesystems
- upload or download files
- capture screenshots
- perform audio surveillance using microphones

- record video streams from webcam devices
- capture screenshots
- steal files from removable media
- execute arbitrary commands
- record keystrokes
- steal passwords saved in browsers
- spread across systems by infecting removable media

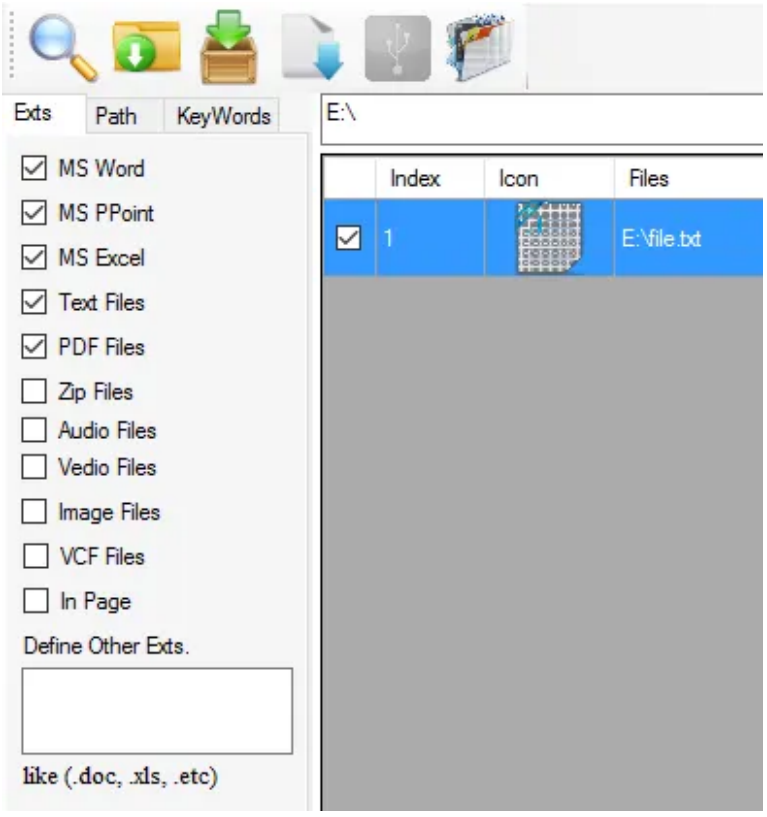

Figure 2: Collection of relevant files on infected systems via USB worm

Kaspersky detected hundreds of victims, but infection also occurred through a USB-Worm component of CrimsonRat. Kaspersky found an Android piece of malware to spy on mobile phones and a link between ObliqueRAT and Transparent Tribe in their second part. The group mimicked a known COVID tracking app.

In April 2021 and July 2021, Team Cymru released part 1 and part 2 of their analysis that focused on the infrastructure leveraged by the TransparentTribe group. It highlighted the following findings:

1. C2s are hosted with several VPS providers – most commonly Contabo, ColoCrossing, Pi Net, and QuadraNet.
2. Port 3389 was observed open on 83% of the CrimsonRAT C2 servers.

3. An RDP certificate serves as a key indicator for CrimsonRAT and has been observed on 17 C2 servers in total.

4. Analysis of C2 servers showed beaconing from victims who were primarily located in the Kashmir region.

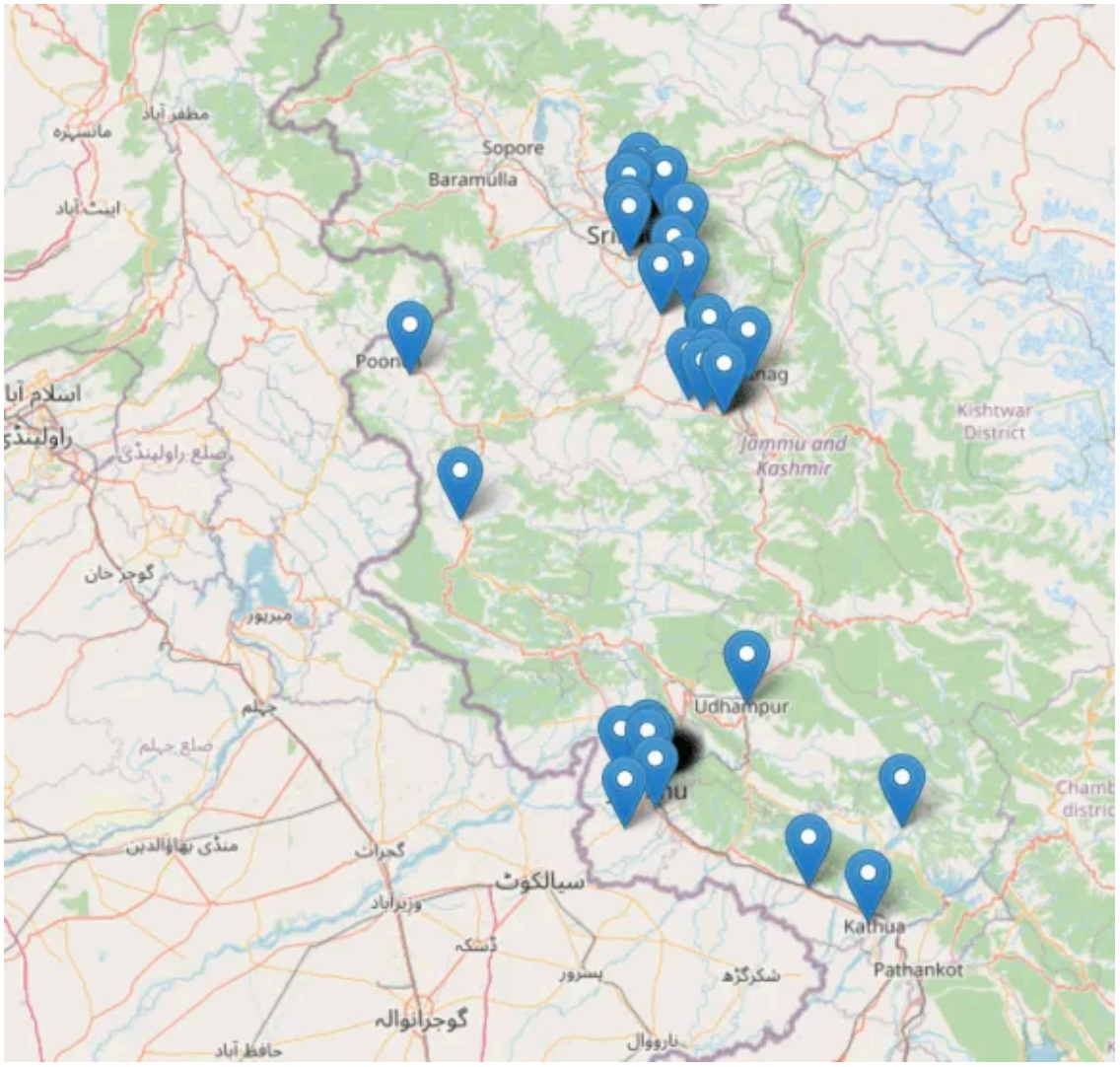

Figure 3: Clustering victims from a known TransparentTribe C2 server

In July 2021, the Hindu media outlet reported that TransparentTribe was targeting critical Indian infrastructure of public enterprises, according to a report by Seqrite. In their report, Seqrite mentions the group was “targeting critical Indian organizations”. The report explains that TransparentTribe mimicked the behavior of an Indian nation-state actor group named Sidewinder. Their analysis demonstrates that VPS provider Contabo in Germany hosts the CrimsonRat infrastructure. In addition, some of the domains used for their operations were registered to someone in Pakistan with the e-mail address “kingsmanfisher@gmail.com”.

In September 2021, Cyble shared research finding TransparentTribe malware that targeted the Indian Armed forces staff. Additionally, they found an icon loaded by the malicious app, which is the logo of the Canteen Store Department (CSD).

Figure 4: Icon of the CSD of the Indian Armed Forces

Lastly, in September 2021, Weibu online shared their insights in a threat intelligence report with relevant indicators of compromise (translated) called “Trilateral operations: years of cyber espionage against many countries in South Asia and the Middle East”. They captured several APT attacks against Iran, Afghanistan, and India, all parties that signed the “Chabahar Port Agreement”. In the report, Weibu lists a malicious document called “Chabahar Port Agreement (Trilateral) in Iran.doc”, which they observed in the attack uploaded to VirusTotal March 2021. The victims were targeted via phishing, watering holes or backdoored software, or malicious Android packages.

Weibu further explains the geopolitical significance of the Chabahar port. *“Chabahar Port is the global oil and gas center on the coast of the Persian Gulf to the west, and leads to the oil-rich Central Asian countries to the north. It is right at the intersection of West Asia, South Asia, Central Asia and the Indian Ocean. Geographical transportation is extremely important. “*

The agreement is crucial to India as this will provide them strategic access to Iran, and it can bypass Pakistan in transporting goods to Afghanistan. Still, it is also vital to counter the Chinese (naval) presence in the Arabian Sea, where China supports Pakistan to develop the Gwadar Port, which is nearby, namely 100 kilometers by sea.

The city of Chabahar is also an important military site for Iran’s navy and air force. In addition, Iran has many large iron mines, giant copper mines, and rich oil and gas resources. The threat actor responsible for the attack overlaps to a certain degree with the TransparentTribe group, and they are likely to have a Pakistani background, claimed by Weibu.

On the 24th of September 2021 malware researcher, at Malwarebytes Jazi (@h2jazi) shared the following TransparentTribe intelligence. Interestingly, the actors mimicked the original Iranian website “https://www.tasnimnews.com” website as their C2 server.

Jazi@h2jazi

#TransparentTribe #APT maldoc: 59ed41388826fed419cc3b18d28707491a4fa51309935c4fa016e53c6f2f94bc Nakul Kumar.doc #Crimson Rat: afd21ef5712ffcbe4e338a5eb347f742d3c786f985ba003434568146adedb290 C2: tasnimnewstehran[.]club

1:35 PM · Sep 24, 2021

11 Reposts · 31 Likes

I will briefly assess the malicious document and CrimsonRat backdoor to determine if new developments can be spotted. Let's start with the malicious document.

```
Nakul Kumar.doc 59ed41388826fed419cc3b18d28707491a4fa51309935c4fa016e53c6f2f94bc
```

First, the file type was determined with the *file* command. This revealed the following information:

```
59ed41388826fed419cc3b18d28707491a4fa51309935c4fa016e53c6f2f94bc: Composite Document File V2 Document, Little E
```

The *file* command revealed some interesting metadata. The next step was to inspect the documents for the presence of malicious macros. With the famous oletools, it was possible to retrieve all the Visual Basic for Application (VBA) macro's in the document.

```
 askfjlskdjflkjsdrkljskd = Split(UserForm1.TextBox1.Text & UserForm1.TextBox2.Text & UserForm1.TextBox3.Text & U
Dim lskjfjiogjnvdfgljwlfjfsf As Double
lskjfjiogjnvdfgljwlfjfsf = 0
For Each tiogjvelrrkjf In askfjlskdjflkjsdrkljskd
        ReDim Preserve alksdjweoijgskljsl_____(lskjfjiogjnvdfgljwlfjfsf)
        alksdjweoijgskljsl_____(lskjfjiogjnvdfgljwlfjfsf) = CByte(tiogjvelrrkjf)
        lskjfjiogjnvdfgljwlfjfsf = lskjfjiogjnvdfgljwlfjfsf + 1
```

```
 VBA FORM STRING IN '59ed41388826fed419cc3b18d28707491a4fa51309935c4fa016e53c6f2f94bc' - OLE stream: 'Macros/Use
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
20!163!163!232!71!161!103!90!143!154!72!231!144!84!104!72!25!253!146!69!107!219!79!95!58!0
```

Being familiar with their malicious documents, it appears that the actor is starting to use random names for variables and functions, but take note that the actor is still using the Split(UserForm1.Textbox1) where the decimal content is separated by "!". The same technique has been observed in the analysis of Monnappa K A in 2017 and displayed in the screenshot below.

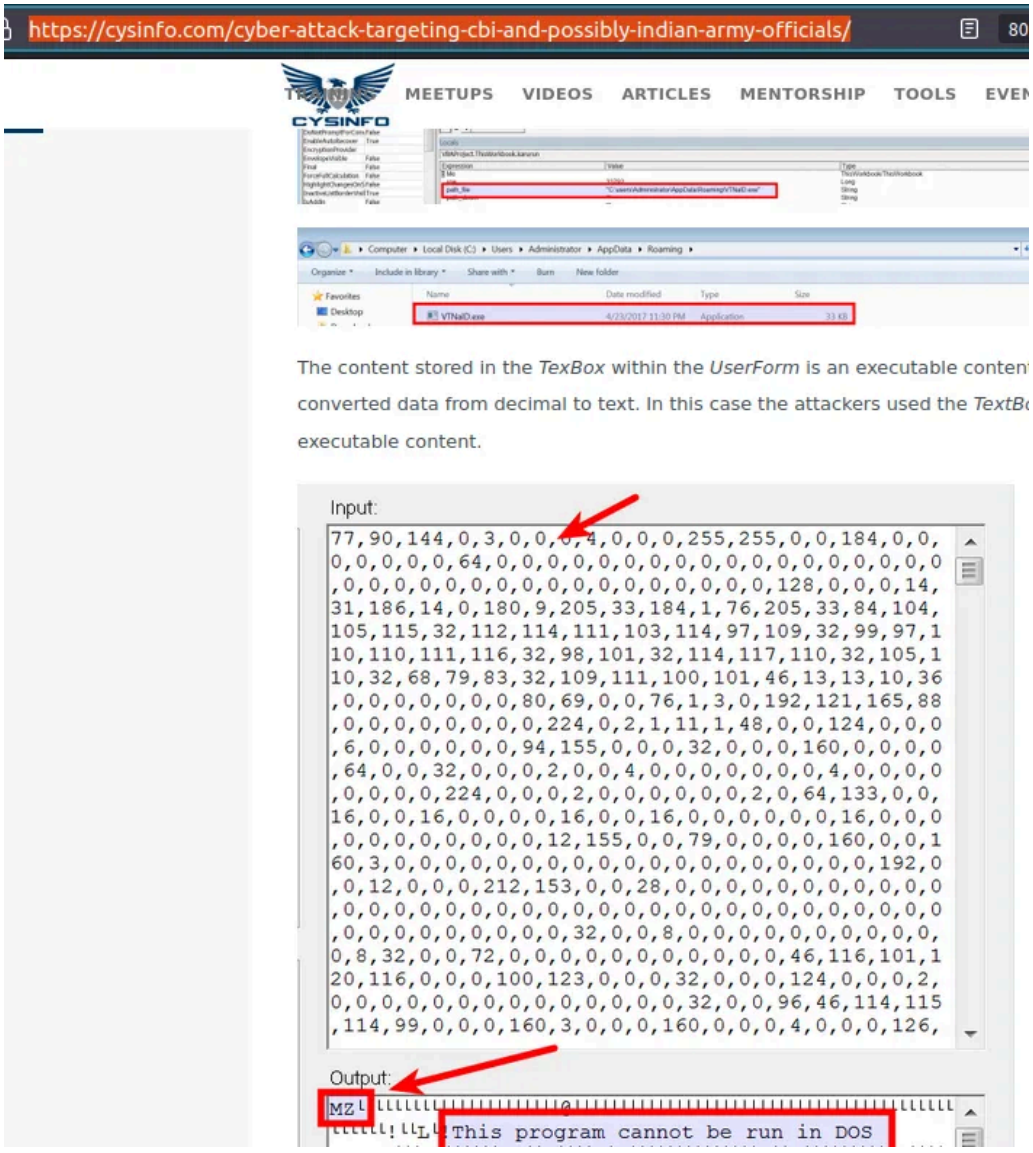

Figure 5: Similar methods observed in research from 2017

By extracting the decimal content from the malicious document and storing it in a text file, the CrimsonRat backdoor named “winword.exe” could be extracted by the following Python program. I could not enter the program in the code section of Substack as this produced an error, hence the screenshot.

Figure 6: Sample program to convert the decimal content into binary

To determine if the data has been converted correctly, the executable is calculated with *sha256sum.*

```
 $ sha256sum winword.exe
afd21ef5712ffcbe4e338a5eb347f742d3c786f985ba003434568146adedb290
```

The value corresponds with the data that Jazi, the malware researcher, shared. The file command was used again to determine if the executable is indeed a .Net piece of malware.

```
 $ file winword.exe
winword.exe: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
```

The *file* command provides insights that the malware is a .Net executable with loads in DnSpy, but first, the executable was investigated with ClamAV, the open-source anti-virus scanner. I'm a massive fan of that project as it is fast, and you can build your custom signatures with it. I have used it in the past to detect malicious backdoors on forensic images of multiple servers that were part of a significant forensic investigation.

```
 $ clamscan winword.exe
winword.exe: Win.Trojan.CrimsonRAT-7591455-0 FOUND

----------- SCAN SUMMARY -----------
Known viruses: 17106785
Engine version: 0.103.2
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 1.66 MB
Data read: 1.56 MB (ratio 1.07:1)
Time: 559.328 sec (9 m 19 s)
Start Date: 2021:10:10 11:15:17
End Date:   2021:10:10 11:24:37
```

ClamAV still detects this latest CrimsonRat. If you want to understand which patterns the malware got detected, you could leverage the power of *sigtool*. With the *sigtool,* you can display the signatures and decode the decimal and compressed values stored in the ClamAV databases. This method can also get a better insight into how actors develop their malware and obtain better intelligence on them.

```
 $ sigtool --find-sigs Win.Trojan.CrimsonRAT-7591455-0
[daily.ldb] Win.Trojan.CrimsonRAT-7591455-0;Engine:51-255,Target:1;(0|((1|2|3|4|5|6)>3,3));74686e61766977615c74
```

The -decode-sigs argument can decode the signatures of ClamAV.

```
 $ sigtool --find-sigs Win.Trojan.CrimsonRAT-7591455-0 |sigtool --decode-sigs
VIRUS NAME: Win.Trojan.CrimsonRAT-7591455-0

<cut for brevity>

thnaviwa\thnaviwa\obj\Debug\thnaviwa.pdb
pull_data
do_process
```

```
IPSConfig
_responce>b__
see_responce
funStarter

<cut for brevity>
```

I have removed other information for readability, but ClamAV detected the CrimsonRat sample as it encountered more than 3 of the strings like “pull_data” or “do_process” in the sample. This can be verified by executing the *strings* and *grep* on the “winword.exe” sample.

```
 $ strings -a winword.exe |grep -iE "(pull_data|do_process|_responce>b__|see_responce|funStarter|thnaviwa.pdb)"
gitfunStarter
gitsee_responce
gitpull_data
gitdo_process
```

The sample contained four matches with the signatures stored in the ClamAV database’ daily.ldb’. By loading the CrimsonRat (winword.exe) in dnSpy, you can view the code of the CrimsonRat, but also see some of the matching strings on the left. From this sample is also appears that the author of the CrimsonRat is obfuscating the code better than observed in earlier samples.

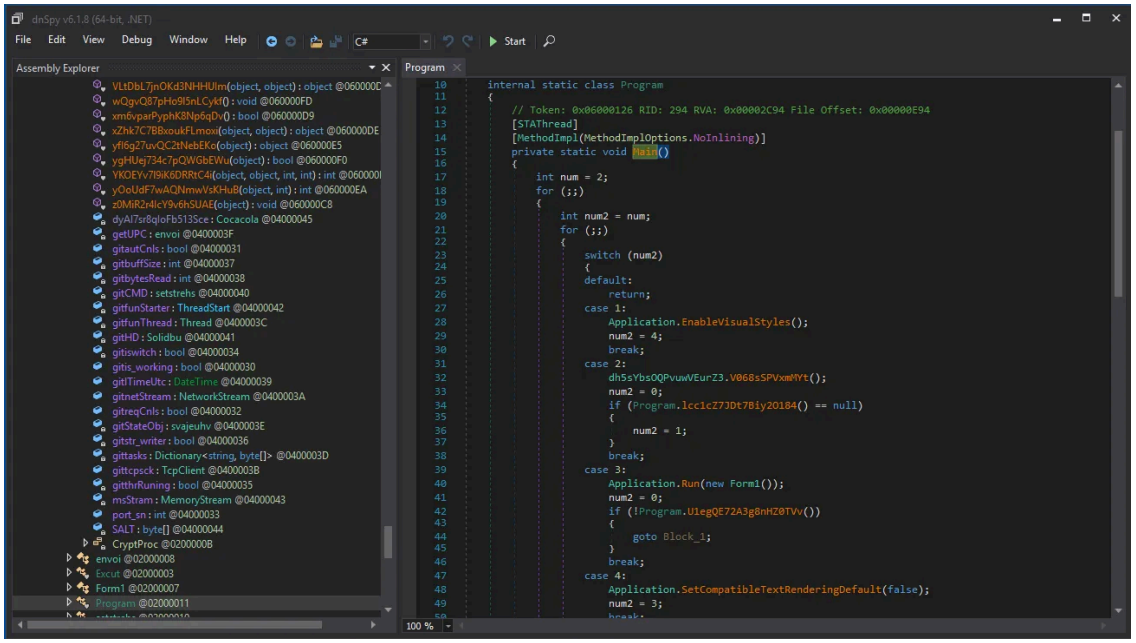

Figure 6: dnSpy displays randomized functions and routines in the latest CrimsonRat

The TransparentTribe actor seems very busy, is not stealthy, and anti-virus solutions have proper detections. The actor is observed in different regions in Asia and attacking multiple countries in the area, but primarily India and Afghanistan. The main attack vectors that the group employs are still phishing, watering hole attacks, or backdoored downloads. There appears to be a broad consensus among malware security researchers that the nation-state actor originates from Pakistan. The latest samples demonstrate that the actor is trying to obfuscate the

malware by applying random names to functions and variables in the malicious documents and the CrimsonRat, thus far not with a lot of success. The actor also has capabilities the target victims on the Android platform.

Although mentioned in some research, I could not observe that TransperentTribe was attacking critical infrastructure in India. Still, from a nation-state perspective, you likely want to gain a strategic foothold in the crucial infrastructure networks of your enemy.

Many security companies have shared research on TransparentTribe. Still, Weibo shared the fascinating geopolitical angle that I was unfamiliar with, namely one of significant strategic importance towards countering China's Belt and Road Initiative in the Middle East and Asia by India. They reported an attack on Iran, India, and Afghanistan with a theme of the trilateral agreement of the port of Chahabar in Iran. Until next time, where the indicators will direct me in writing the subsequent anchored narrative. Likely on another nation-state operating in the South Asia region.

The following IOC's were shared on Twitter by many malware researchers since the beginning of January 2021. Sharing is caring. Keep doing that! The list below matched my intelligence requirements multiple times but is not complete. The format of sharing that is the most used by security researchers is the following:

```
 #APT #APTGroupname
MD5 Maldoc:MD5 Value
Filename:Filename
Backdoor Name:MD5 value
ITW:MD5 value
Filename:Filename
Download from:Second stage payload location
C2: IP-address
Domain name: DNS name
Any other interesting artifacts: DBG path
```

Based upon the above information, the data listed below matched the search criteria. Of course, I have not reviewed all samples or confirmed them to belong to that the TransparentTribe group definitely, but it is very likely.

```
 MD5: c7a3276763a5c1b13f93028aab5a6e73
Filename:Nisha Doc.doc
CrimsonRat:938770e6e69e6feadb1b9f63af9969f4
Filename:ravidhtirad.exe
C2:151.106.14.125
```

```
 MD5:1F1082F170381D1CBA07EAE5F750FE7B
Filename:National Conference 2021.xlam
CrimsonRat:050EC7C999666E94840D559B4EBE2BE
C2:23.254.119.118
```

```
 MD5:7f1f7c5c4b6b486e5ba9340944036285
MD5:77c29d464efcae961424ae050453ef11
MD5:3c2b45a6d878cc9f30a5dc10abf400a1
```

```
 MD5:66558073be686a57514dbc72e56fd41c
Filename:RAKESH JAYKRISHNA.xls
C2:167.86.105.43:6588
```

```
 MD5:039c162d7fcd8640b337173e323f94d8
Filename:CSD_AppLaunch.exe
Download from:hxxps://secure256.net/ver4.mp3 = IntelWifi.exe
Filename:IntelWifi.exe
C2: 45.147.228.195:5434
```

```
 ITW:54a86a284932a893a80fb760f9231283
Filename:Weekly trg prog.doc
C2:64.188.25.143:4586
```

```
 Fake Wechat.exe
MD5:1DEFE1EAC1D87D6A7808E4471080388B
MD5:571E6B675E7E9AA3E5A1EF3A19C25909
```

```
 #Netwire RAT suspected to be dropped by #APT-C-56 #TransparentTribe
MD5:c2a38018cf336685e3c760c614bbf4c3
MD5:f0b43a3f4821a4cf4b514144b496e4d7
```

```
 "Today our researchers have found new #Tahorse sample which belongs to #TransparentTribe #APT group
ITW/MD5:cf937b817a81db6521a64229625fbc1b
C2:178.132.3.230
```

```
 C2: 5.189.134.216
```

```
 MD5/ITW:e98510e1252e7dd99012b23a400bb00b
Filename: program.exe
C2:185.117.73.222:3344
```

```
 MD5/ITW:4a7ff92e0ea13b41a5e3410c3becfb2e
Filename:i.docm
```

C2:198.23.210.211:4898(8786)

MD5:54d5743efcc5511368c6c04bf6840a59
Filename:Defence and security Agenda Point.ppt
#Crimson Rat:
MD5:6d88dcb578cef59d3d0244d1e93b0f57
Filename: trbgertrnion.exe
Debug path:e:\\core-projects\\adii\\trbgertrnion\\trbgertrnion\\obj\\Debug\\trbgertrnion.pdb
C2:167.160.166.80

"Today our researchers have found new #Tahorse sample which belongs to #TransparentTribe #APT group
ITW/MD5:7d5eea5905af0b091f3ed37b20b7d847
C2:178.132.3.230

MD5:8057dacaf42319cde2b979b5cdfff034
Filename:Criteria_of_Armed_forces_Offrs_docm
#Crimson Rat:
Filename:railthnsrqn.exe
MD5:3a64279863fa16be74abdc8c20ceecb0
C2:167.160.166.177

"Today our researchers have found #Tahorse APK Implant which belongs to #TransparentTribe #APT group
ITW:0fd1530fa9d78a579af960d57151a431
filename:whatsapplite.apk
C2:109.236.85.16:5987
myabcxyz1[.]ddns[.]net:5987

MD5:5cbcc3485f4286098b3a111ceec8ce54 #"This might be #TransparentTribe #APT maldoc:
MD5 c08e1509f379755df710d5a8fd4ff175 #Dropped payload
C2:5.189.170.84

MD5:66870a4045126c2744d86d92d564e1a4
C2: 167.86.118.69
Port: 443,7834
Domain: speedytech[.]work
JA3(ssl fingerprint): 54328bd36c14bd82ddaa0c04b25ed9ad

ITW/MD5:2f71caebb2842f4afd6c262f742d3b2b
Filename: Sunita Singh.exe
C2:151.106.14.125:6818

```
 MD5:6917d9ca4f9604ee09d08d5c33e93955
C2: 64.188.13.46
hxxp://64.188.13.46/deliveryyyyyyyyy/adwc.exe
```

```
 59ed41388826fed419cc3b18d28707491a4fa51309935c4fa016e53c6f2f94bc
Nakul Kumar.doc
Crimson Rat:
afd21ef5712ffcbe4e338a5eb347f742d3c786f985ba003434568146adedb290
C2:tasnimnewstehran[.]club
```

```
 ITW:643b11c3f6a6ccc41cfd37544b71c0dc  467e17b8d44626b7456716680e3d043d 0061d17ff54d214c5ea6867cb815caea
C2:66.154.103[.]106 Port :13374
```

```
 ITW:cb27d0bd9a97e053f3fbfcf4bba8b8fc
Filename:Ultimate-File.docm
C2:134.119.181.142:6672
```

```
 MD5 : 28dc287cc78e195386dc33564dfe449a
```

George M. Garner Jr. was the author of kntdd and kntlist. Kntdd was used to acquire memory on Windows systems, and kntlist was used to interpret structures in memory to detect rootkits. George, unfortunately, passed away in 2017.

Source: https://anchorednarratives.substack.com/p/trouble-in-asia-and-the-middle-east