Transparent Tribe: Evolution analysis, part 2

securelist.com/transparent-tribe-part-2/98233

Giampaolo Dedola

Background + Key findings

Transparent Tribe, also known as PROJECTM or MYTHIC LEOPARD, is a highly prolific group whose activities can be traced as far back as 2013. In the last four years, this APT group has never taken time off. They continue to hit their targets, which typically are Indian military and government personnel.

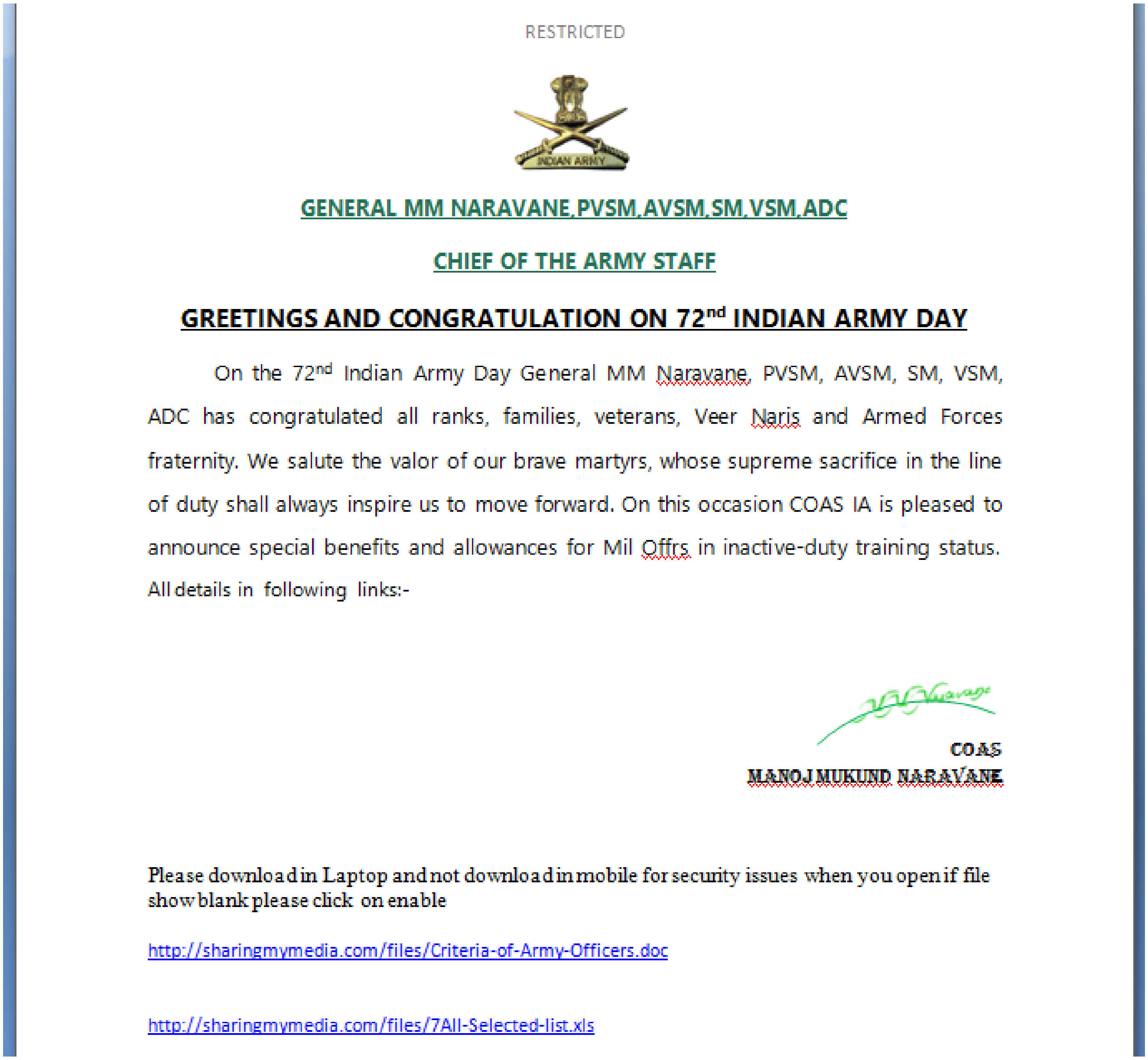
This is the second of two articles written to share the results of our recent investigations into Transparent Tribe. In the previous article, we described the various Crimson RAT components and provided an overview of impacted users. Here are some of the key insights that will be described in this part:

- We found a new Android implant used by Transparent Tribe for spying on mobile devices. It was distributed in India disguised as a porn-related app and a fake national COVID-19 tracking app.
- New evidence confirms a link between ObliqueRAT and Transparent Tribe.

Android implant

During our analysis, we found an interesting sample, which follows a variant of the previously described attack scheme. Specifically, the attack starts with a simple document, which is not malicious by itself, does not contain any macro and does not try to download other malicious components, but it uses social engineering tricks to lure the victim into downloading other documents from the following external URLs:

hxxp://sharingmymedia[.]com/files/Criteria-of-Army-Officers.doc hxxp://sharingmymedia[.]com/files/7All-Selected-list.xls



RESTRICTED

GENERAL MM NARAVANE,PVSM,AVSM,SM,VSM,ADC

CHIEF OF THE ARMY STAFF

GREETINGS AND CONGRATULATION ON 72nd INDIAN ARMY DAY

On the 72nd Indian Army Day General MM Naravane, PVSM, AVSM, SM, VSM, ADC has congratulated all ranks, families, veterans, Veer Naris and Armed Forces fraternity. We salute the valor of our brave martyrs, whose supreme sacrifice in the line of duty shall always inspire us to move forward. On this occasion COAS IA is pleased to announce special benefits and allowances for Mil Offrs in inactive-duty training status. All details in following links:-

COAS
MANOJ MUKUND NARAVANE

Please download in Laptop and not download in mobile for security issues when you open if file show blank please click on enable

http://sharingmymedia.com/files/Criteria-of-Army-Officers.doc

http://sharingmymedia.com/files/7All-Selected-list.xls

15DA10765B7BECFCCA3325A91D90DB37 – Special Benefits.docx

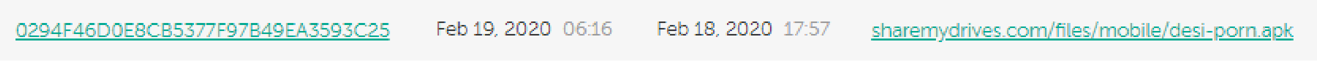
The remote files are two Microsoft Office documents with an embedded malicious VBA, which behaves similarly to those described in the previous article and drops the Crimson "Thin Client". The domain sharingmymedia[.]com was even more interesting: it was resolved with the IP 89.45.67[.]160 and was registered on 2020-01-10 using Namesilo and the following information:

Registrant Name: bluff hunnter
Registrant Organization:
Registrant Street: India Dehli
Registrant City: Dehli
Registrant State/Province: Delhi

Registrant Postal Code: 110001
Registrant Country: IN
Registrant Phone: +91.4214521212
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: hunterbluff007@gmail.com

The same information was used to register another domain, sharemydrives[.]com, which was registered seven days before, on 2020-01-03, using Namesilo. DNS resolution points to the same IP address: 89.45.67[.]160.

Using our Kaspersky Threat Intelligence Portal, we found the following related URL:



0294F46D0E8CB5377F97B49EA3593C25	Feb 19, 2020 06:16	Feb 18, 2020 17:57	sharemydrives.com/files/mobile/desi-porn.apk

Information in Kaspersky Threat Intelligence Portal

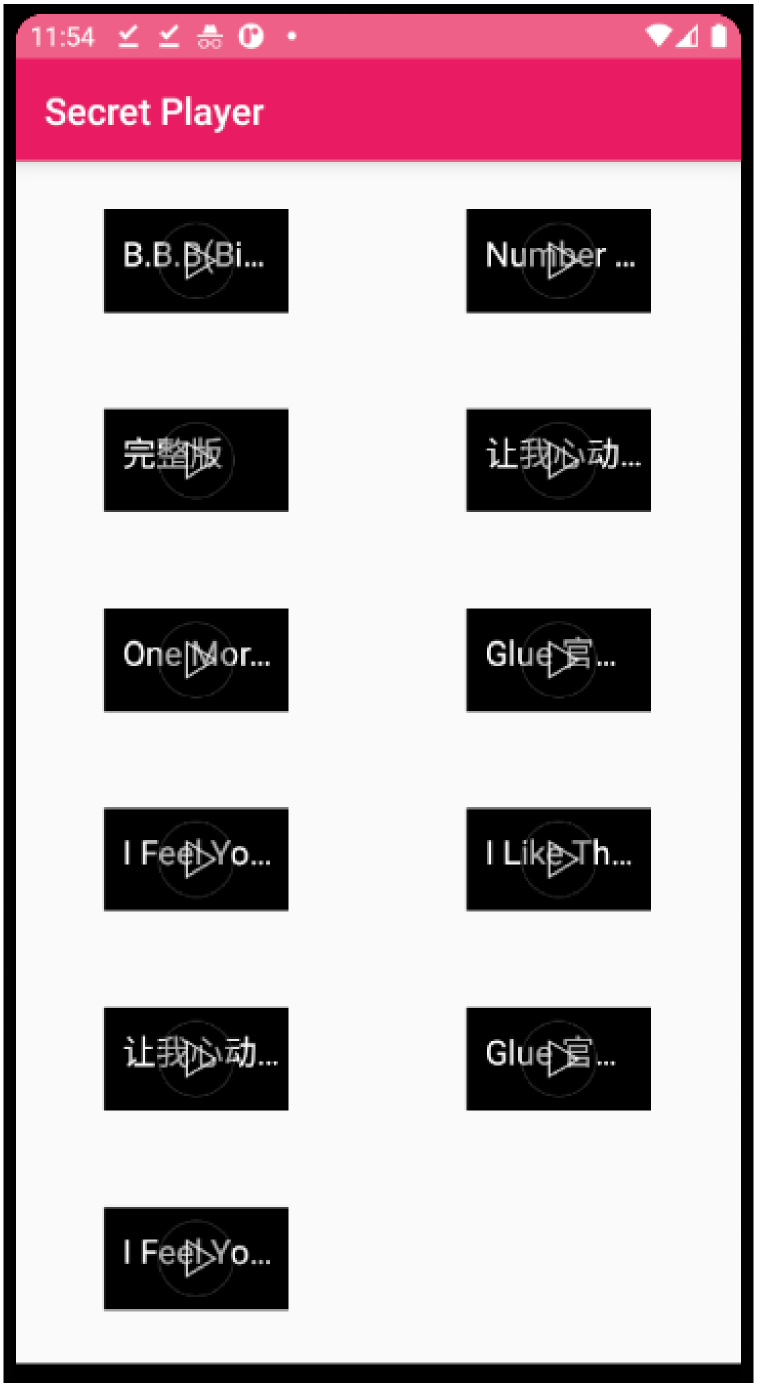
The file is a modified version of MxVideoPlayer, a simple open-source video player for Android, downloadable from GitHub and used by Transparent Tribe to drop and execute their Android RAT.

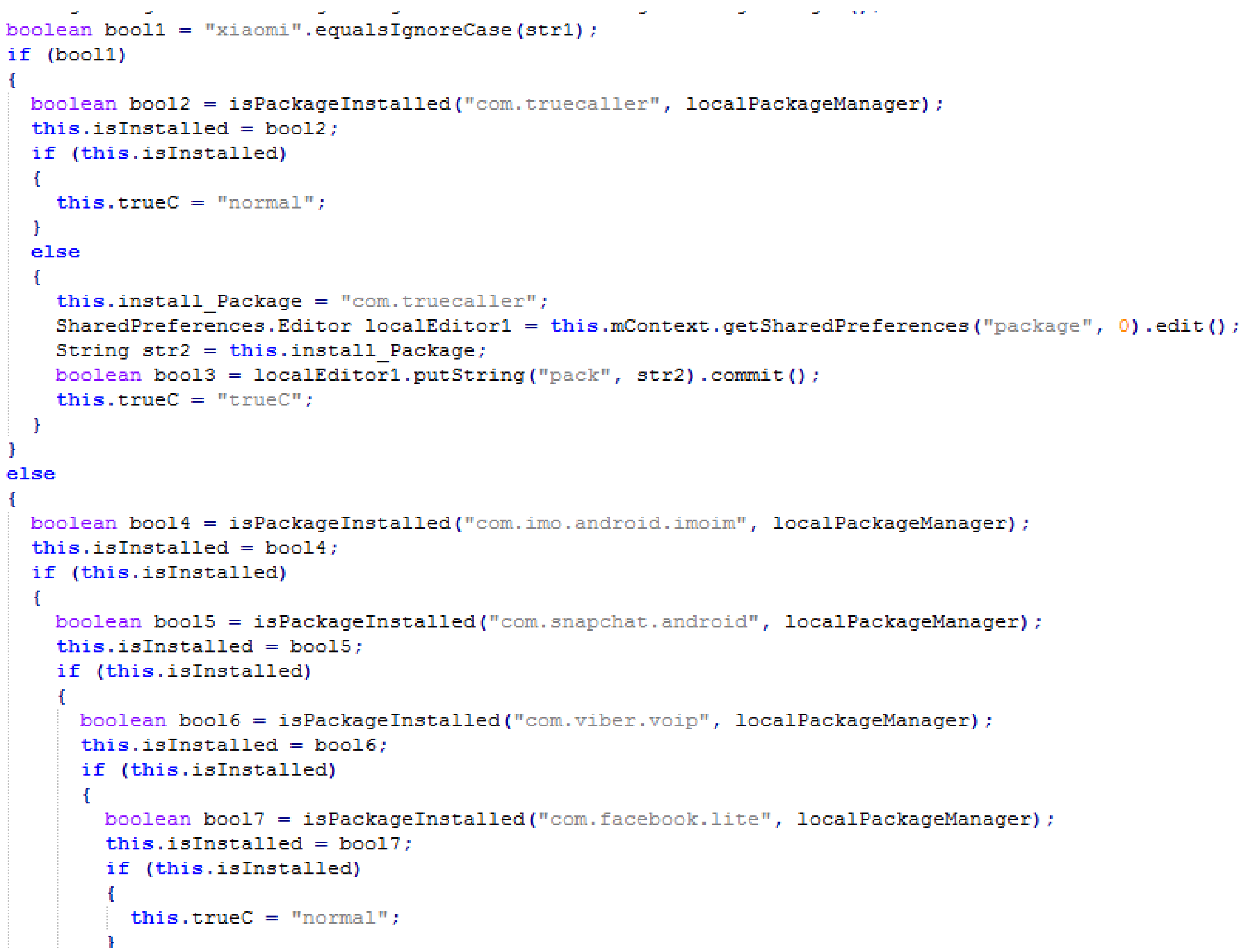
Desi-porn.apk screenshot

The dropper tries to find a list of legitimate packages on the system:

- imo.android.imoim
- snapchat.android
- viber.voip
- facebook.lite

If the device was produced by Xiaomi, it also checks if the com.truecaller package is present.





```
boolean bool1 = "xiaomi".equalsIgnoreCase(str1);
if (bool1)
{
  boolean bool2 = isPackageInstalled("com.truecaller", localPackageManager);
  this.isInstalled = bool2;
  if (this.isInstalled)
  {
    this.trueC = "normal";
  }
  else
  {
    this.install_Package = "com.truecaller";
    SharedPreferences.Editor localEditor1 = this.mContext.getSharedPreferences("package", 0).edit();
    String str2 = this.install_Package;
    boolean bool3 = localEditor1.putString("pack", str2).commit();
    this.trueC = "trueC";
  }
}
else
{
  boolean bool4 = isPackageInstalled("com.imo.android.imoim", localPackageManager);
  this.isInstalled = bool4;
  if (this.isInstalled)
  {
    boolean bool5 = isPackageInstalled("com.snapchat.android", localPackageManager);
    this.isInstalled = bool5;
    if (this.isInstalled)
    {
      boolean bool6 = isPackageInstalled("com.viber.voip", localPackageManager);
      this.isInstalled = bool6;
      if (this.isInstalled)
      {
        boolean bool7 = isPackageInstalled("com.facebook.lite", localPackageManager);
        this.isInstalled = bool7;
        if (this.isInstalled)
        {
          this.trueC = "normal";
        }
```

The code used to check if legitimate packages are installed

The first application on the list that is not installed on the system will be selected as the target application. The malware embeds multiple APK files, which are stored in a directory named "assets". The analyzed sample includes the following packages:

- apk a20fc273a49c3b882845ac8d6cc5beac
- apk 53cd72147b0ef6bf6e64d266bf3ccafe
- apk bae69f2ce9f002a11238dcf29101c14f
- apk b8006e986453a6f25fd94db6b7114ac2
- apk 4556ccecbf24b2e3e07d3856f42c7072
- apk 6c3308cd8a060327d841626a677a0549

The selected APK is copied to /.System/APK/. By default, the application tries to save the file to external storage, otherwise it saves it to the data directory.

Finally, the application tries to install the copied APK. The final malware is a modified version of the AhMyth Android RAT, open-source malware downloadable from GitHub, which is built by binding the malicious payload inside other legitimate applications.

The original AhMyth RAT includes support for the following commands:

Commands	Additional fields	Value	Description
x0000ca	extra	camlist	get a camera list
	extra	1	get a photo from the camera with the id 1
	extra	0	get a photo from the camera with the id 0
x0000fm	extra path	ls %dirpath%	get a list of files in the directory specified in the “path” variable.
	extra path	dl %filepath%	upload the specified file to the C2
x0000sm	extra	ls	get a list of text messages
	extra to sms	sendSMS %number% %message%	send a new text to another number
x0000cl			get the call log
x0000cn			get contacts
x0000mc	sec	%seconds%	record audio from the microphone for the specified number of seconds and upload the resulting file to the C2.
x0000lm			get the device location

Basically, it provides the following features:

- camera manager (list devices and steal screenshots)
- file manager (enumerate files and upload these to the C2)
- SMS manager (get a list of text messages or send a text)
- get the call log
- get the contact list
- microphone manager
- location manager (track the device location)

The RAT that we analyzed is slightly different from the original. It includes new features added by the attackers to improve data exfiltration, whereas some of the core features, such as the ability to steal pictures from the camera, are missing.

The operators added the following commands:

- x000upd – download a new APK from the URL specified in the “path” field.
- x000adm – autodownloader: not implemented in the version we analyzed, but available in other samples.

Moreover, the creators of the RAT also improved its audio surveillance capabilities and included a command to delete text messages with specific contents.

Commands	Additional fields	Value	Description
x000upd	path	%url%	download a new APK from the URL specified in the “path” field
x000adm			not implemented in the analyzed version. Other samples use this to start a class named “autodownloader”.
x0000mc	extra sec	au %seconds%	record audio for x seconds and upload the resulting file to the C2. Duration is specified in the “sec” value.
	extra	mu	stop recording and upload the resulting file to the C2
	extra	muS	start recording continuously. This generates MP3 files stored in the “/.System/Records/” directory.
x0000fm	extra path	ls %dirpath%	get a list of files in the directory specified in the “path” variable
	extra path	dl %filepath%	upload the specified file to hxxp://212.8.240[.]221:80/server/upload.php
sms	extra	ls	get a list of text messages
	extra to sms	sendSMS %number% %message%	Send a new text to another number.

	extra to sms	deleteSMS %message%	Delete a text that contains the string specified in the “sms” value. The “to” value is ignored.
x0000cl			get the call log
x0000cn			get contacts
x0000lm			get the device location

The “autodownloader” is a method used for performing the following actions:

- upload a contact list
- upload a text message list
- upload files stored in the following directories:
  - /.System/Records/
  - /Download/
  - /DCIM/Camera/
  - /Documents/
  - /WhatsApp/Media/WhatsApp Images/
  - /WhatsApp/Media/WhatsApp Documents/

The attacker uses the method to collect contacts and text messages automatically. In addition, the method collects the following: audio files created with the “x0000mc” command and stored in /.System/Records/, downloaded files, photos, images and documents shared via WhatsApp and other documents stored on the device.

Another interesting difference between the original AhMyth and the one modified by Transparent Tribe is the technique used for getting the C2 address. The original version stores the C2 server as a string directly embedded in the code, whereas the modified version uses a different approach. It embeds another URL encoded with Base64 and used for getting a configuration file, which contains the real C2 address.

In our sample, the URL was as follows:

hxxp://tryanotherhorse[.]com/config.txt

It provided the following content:

212.8.240.221:5987

http://www.tryanotherhorse.com

The first value is the real C2, which seems to be a server hosted in the Netherlands.

The modified version communicates via a different URL scheme, which includes more information:

- Original URL scheme: http://%server%:%port?model=%val%&manf=%val%&release=%val%&id=%val%
- Modified URL scheme http://%server%:%port?mac=%val%&battery=%val%&model=%val%&manf=%val%&release=%val%&id=%val%

Covid-19 tracking app

We found evidence of Transparent Tribe taking advantage of pandemic-tracking applications to distribute trojanized code. Specifically, we found an APK file imitating Aarogya Setu, a COVID-19 tracking mobile application developed by the National Informatics Centre under the Ministry of Electronics and Information Technology, Government of India. It allows users to connect to essential health services in India.

The discovered application tries to connect to the same malicious URL to get the C2 IP address:
hxxp://tryanotherhorse[.]com/config.txt

It uses the same URL scheme described earlier and it embeds the following APK packages:

- apk CF71BA878434605A3506203829C63B9D
- apk 627AA2F8A8FC2787B783E64C8C57B0ED
- apk 62FAD3AC69DB0E8E541EFA2F479618CE
- apk A912E5967261656457FD076986BB327C
- apk 3EB36A9853C9C68524DBE8C44734EC35
- apk 931435CB8A5B2542F8E5F29FD369E010

Interestingly enough, at the end of April, the Indian Army issued a warning to its personnel against Pakistani agencies' nefarious designs to hack the phones of Indian military personnel through a malicious application similar to Aarogya Setu.

According to some Indian online news sites, these applications were found to be sent by Pakistani Intelligence Operatives to WhatsApp groups of Indian Army personnel. It also mentioned that these applications later deployed additional packages:

According to some Indian online news sites, these applications were found to be sent by Pakistani Intelligence Operatives to WhatsApp groups of Indian Army personnel. It also mentioned that these applications later deployed additional packages:

- face.apk
- imo.apk
- normal.apk

- trueC.apk
- snap.apk
- viber.apk

Based on public information, the application may have been distributed by sending a malicious link via WhatsApp, SMS, phishing email or social media.

ObliqueRAT connection

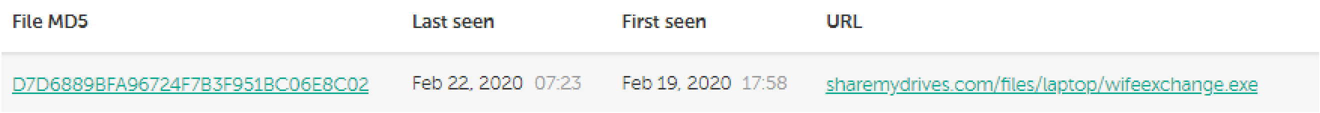
ObliqueRAT is another malicious program, described by Cisco Talos in an interesting article published in February. It was attributed to Transparent Tribe because some samples were distributed through malicious documents forged with macros that resembled those used for distributing Crimson RAT.

The report described two ObliqueRAT variants, one distributed via a malicious document as the infection vector and another one, named "Variant #0" and distributed with a dropper.

4a25e48b8cf515f4cdd6711a69ccc875429dcc32007adb133fb25d63e53e2ac6

Unfortunately, as reported by Talos, "The initial distribution vector of this dropper is currently unknown".

At this time, we do not have the full infection chain, but we can add another piece to the puzzle, because sharemydrives[.]com also hosted another file:

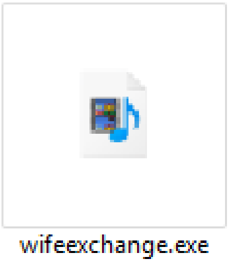


File MD5	Last seen	First seen	URL
D7D6889BFA96724F7B3F951BC06E8C02	Feb 22, 2020 07:23	Feb 19, 2020 17:58	sharemydrives.com/files/laptop/wifeexchange.exe

Information in Kaspersky Threat Intelligence Portal

The wifeexchange.exe sample is another dropper, which disguises itself as a porn clip.

Specifically, the executable file uses the same icon used by Windows for multimedia files.



Dropper icon

Once executed, the process tries to find a specific marker ("*#@") inside its file image, then drops and opens the following files:

- frame.exe –

  4a25e48b8cf515f4cdd6711a69ccc875429dcc32007adb133fb25d63e53e2ac6

- movie.mp4

Frame.exe is the dropper described by Talos, while movie.mp4 is a small porn clip.

Conclusions

Transparent Tribe members are trying to add new tools to extend their operations and infect mobile devices. They are also developing new custom .NET tools like ObliqueRAT, and as observed in the first report, we do not expect this group to slow down any time soon. We will keep monitoring their activities.

IoC

The followings IoC list is not complete. If you want more information about the APT discussed here, a full IoC list and YARA rules are available to customers of Kaspersky Threat Intelligence Reports. Contact: intelreports@kaspersky.com

15DA10765B7BECFCCA3325A91D90DB37 – Special Benefits.docx
48476DA4403243B342A166D8A6BE7A3F – 7All_Selected_list.xls
B3F8EEE133AE385D9C7655AAE033CA3E – Criteria of Army Officers.doc
D7D6889BFA96724F7B3F951BC06E8C02 – wifeexchange.exe

0294F46D0E8CB5377F97B49EA3593C25 – Android Dropper – Desi-porn.apk
5F563A38E3B98A7BC6C65555D0AD5CFD – Android Dropper – Aarogya Setu.apk
A20FC273A49C3B882845AC8D6CC5BEAC – Android RAT – face.apk
53CD72147B0EF6BF6E64D266BF3CCAFE – Android RAT – imo.apk
BAE69F2CE9F002A11238DCF29101C14F – Android RAT – normal.apk
B8006E986453A6F25FD94DB6B7114AC2 – Android RAT – snap.apk
4556CCECBF24B2E3E07D3856F42C7072 – Android RAT – trueC.apk
6C3308CD8A060327D841626A677A0549 – Android RAT – viber.apk
CF71BA878434605A3506203829C63B9D – Android RAT – face.apk
627AA2F8A8FC2787B783E64C8C57B0ED – Android RAT – imo.apk
62FAD3AC69DB0E8E541EFA2F479618CE – Android RAT – normal.apk
A912E5967261656457FD076986BB327C – Android RAT – snap.apk
3EB36A9853C9C68524DBE8C44734EC35 – Android RAT – trueC.apk
931435CB8A5B2542F8E5F29FD369E010 – Android RAT – viber.apk

hxxp://sharingmymedia[.]com/files/Criteria-of-Army-Officers.doc
hxxp://sharingmymedia[.]com/files/7All-Selected-list.xls
hxxp://sharemydrives[.]com/files/Laptop/wifeexchange.exe
hxxp://sharemydrives[.]com/files/Mobile/Desi-Porn.apk

hxxp://tryanotherhorse[.]com/config.txt – APK URL
212.8.240[.]221:5987 – Android RAT C2
hxxp://212.8.240[.]221:80/server/upload.php – URL used by Android RAT to upload files