Drinik Malware Returns With Advanced Capabilities Targeting Indian Taxpayers

By cybleinc

Published: 2022-10-27 · Archived: 2026-04-05 22:38:11 UTC

Android Banking Trojan Stealing User's Data Via Screen Recording and Keylogging

In September 2021, the Indian Computer Emergency Response Team (CERT-In) issued a warning about a new malware strain targeting Indian taxpayers and mentioned that customers of around 27 banks were at risk of this attack.

The Threat Actors (TA) behind this campaign were suspected of using Drinik malware. An early variant of Drinik malware was first spotted in 2016 as an SMS stealer. Around August 2021, the malware was observed to be active again, this time evolving into an Android banking trojan.

Cyble Research & Intelligence Labs (CRIL) has constantly been monitoring the different variants of Drinik Android malware. In September 2021, CRIL released a blog on a masquerading income tax application that targeted Indian taxpayers to steal Personally Identifiable Information (PII) and banking credentials through phishing attacks.

Recently, CRIL identified an upgraded version of Drinik impersonating the Income Tax Department of India and targeting 18 Indian banks (bank names are explicitly mentioned in the malicious APK file).

The TA uses the same campaign theme to lure the victim, but the malware has been upgraded with advanced capabilities. We have listed the main features implemented in the new variant, making the malware an advanced threat:

- Screen Recording to harvest credentials
- Keylogging
- Abusing CallScreeningService to manage incoming calls
- Receiving commands via FirebaseCloudMessaging

The malware variant is communicating with Command & Control (C&C) server *hxxp://gia[.]3utilities.com*, which is hosted on IP *198[.]12.107[.]13*. Our investigation confirmed that the previous campaign also used the same IP for its C&C communication, indicating that the Threat Actor (TA) behind both campaigns is the same.

The below figure shows the details of the C&C IP address and its connection with the previous campaign.

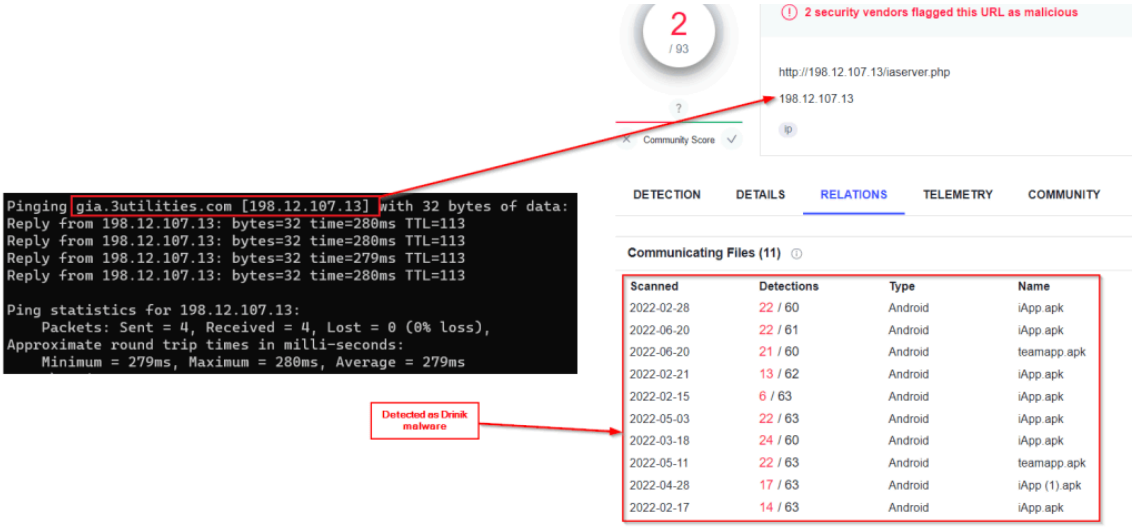

Figure 1 – IP address of C&C server associated with old Drinik variant

Evolution of Drinik:

CRIL observed 3 different variants of this malware since last year. The first variant was observed in September 2021, when the malware used phishing pages to steal credentials. In 2022, two new variants have been identified in the wild, introducing Screen Recording and Keylogging features.

The figure below shows the timeline of Drinik malware and its features.

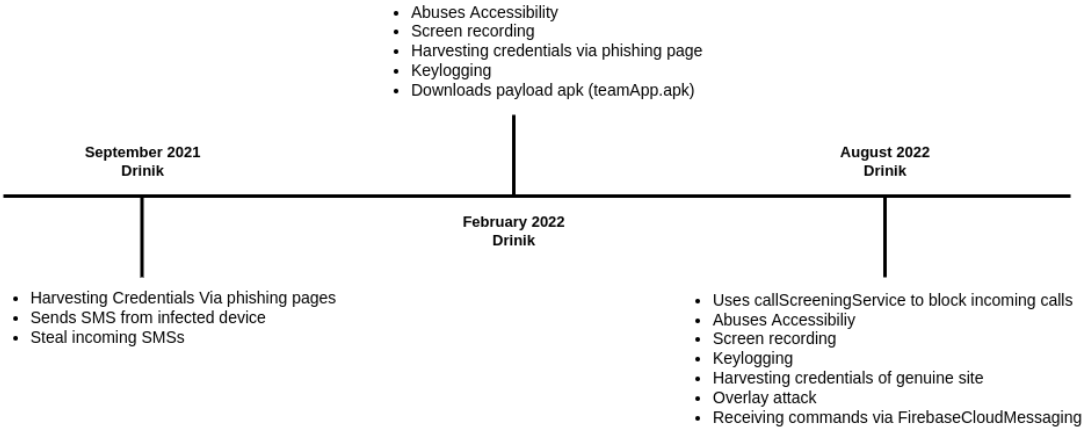

Figure 2 – Evolution of Drinik Banking Trojan

During our investigation, we found that the first version uses a simple phishing page to steal banking credentials, whereas the second version uses screen recording alongside the phishing technique.

Finally, the third and latest version loads the genuine income tax department site and uses screen recording along with a keylogging functionality to steal the login credentials. The below figure shows the login page of three different versions.

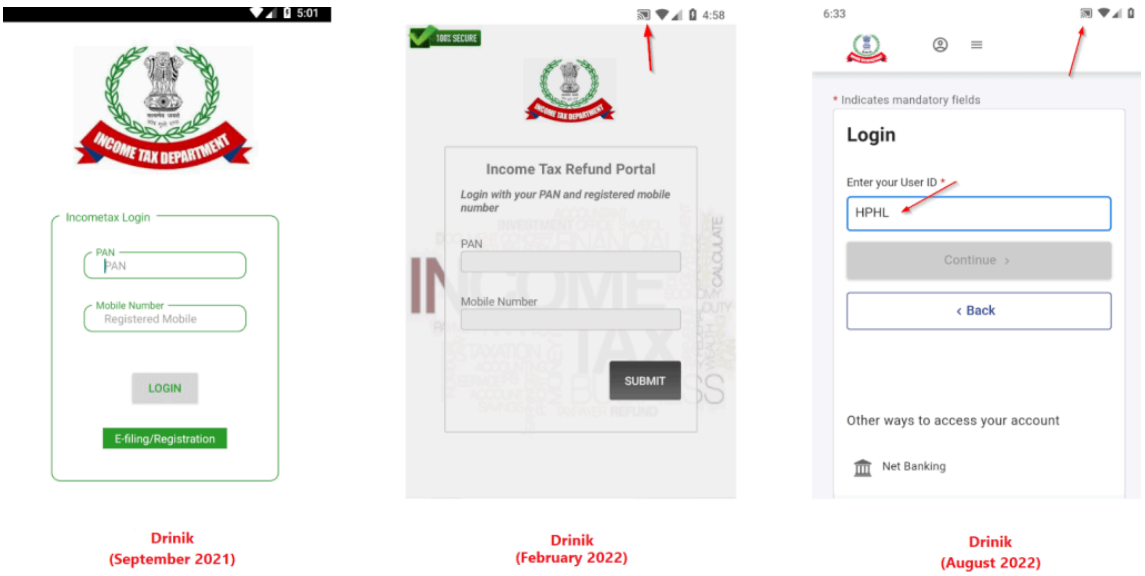

Figure 3 – Login pages of Drinik malware versions

In this analysis, we take a look at the latest sample "iAssist.apk (86acaac2a95d0b7ebf60e56bca3ce400ef2f9080dbc463d6b408314c265cb523)" of Drinik malware observed on October 18, 2022, which has additional code for abusing the CallScreeningService.

By abusing this service, the malware can disallow incoming calls without the user's knowledge. Additionally, the strings present in the file are encrypted to evade detection by antivirus products, and the malware decrypts them during run time using a custom decryption logic. The figure below shows the code snippet used by the malware to decrypt the encrypted strings.

```
static String bhx(int p0,String p1){
    String[] ssplit = p1.split(" 5-");
    StringBuilder stringBuilde = new StringBuilder();
    if (p0 > ssplit.length) {
        return "";
    }
    int len = ssplit.length;
    for (int i = 0; i < len; i = i+1) {
        stringBuilde = stringBuilde+(char)(Integer.parseInt(ssplit[i])+7);
    }
    return stringBuilde;
}
```

Figure 4 – Code to decrypt strings

Technical Analysis

APK Metadata Information

- App Name: **iAssist**
- Package Name: **lincoln.auy.iAssist**
- SHA256 Hash: **86acaac2a95d0b7ebf60e56bca3ce400ef2f9080dbc463d6b408314c265cb523**

The metadata information of the application is shown below.

Figure 5 – App Metadata Information

Manifest Description

The harmful permissions requested by the malware are:

Permission	Description
RECEIVE_SMS	Allows an application to receive SMS messages
READ_SMS	Access phone messages
SEND_SMS	Allows the application to send SMS messages
READ_CALL_LOG	Allows an app to read the user's call log
READ_EXTERNAL_STORAGE	Allows an application to read from external storage.
WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage.

Source Code Review

Like many other banking trojans, the new variant of Drinik relies on the Accessibility Service. After launching, the malware prompts the victim to grant permissions, followed by a request to enable Accessibility Service.

It then starts abusing the service to obtain the necessary permissions to start screen recording, disable Google Play Protect, execute auto-gestures, and capture key logs.

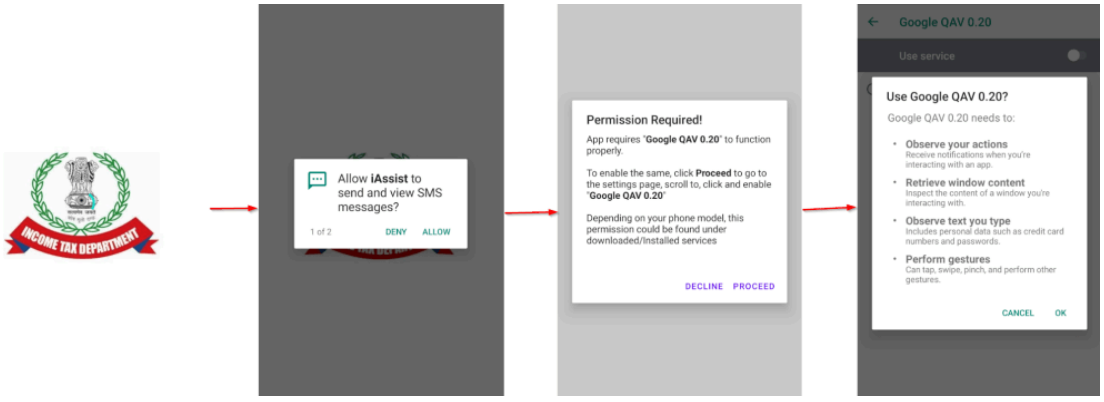

Figure 6 – Malware prompting users to grant Accessibility Service permissions

The latest Drinik variant loads the genuine Indian income tax site *hxxps://eportal[.]incometax.gov.in* using WebView instead of displaying fake phishing pages.

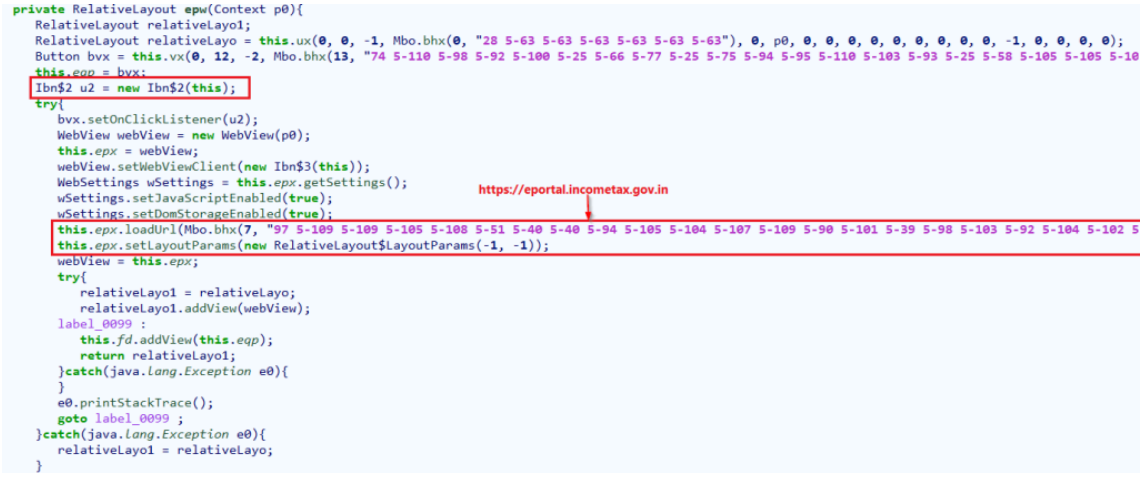

Figure 7 – Malware loading genuine Indian income tax portal using Webview

Before showing the login page to the victim, the malware displays an authentication screen for biometric verification. When the victim enters a PIN, the malware steals the biometric PIN by recording the screen using MediaProjection and also captures keystrokes.

The malware now sends the stolen details to the C&C server, as shown below.

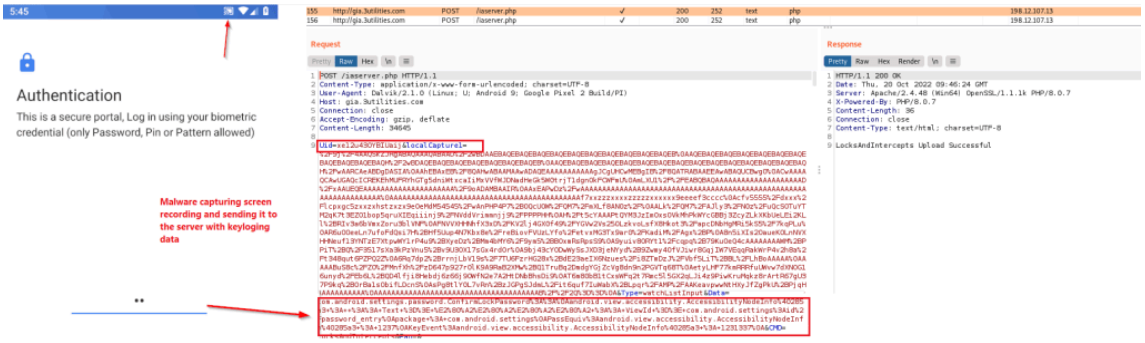

Figure 8 – Malware sending Biometric PIN to C&C Server

After authentication, the malware displays the genuine site loaded into a Webview. Drinik starts screen recording as soon as the victim enters the User ID (such as PAN/AADHAR/Other valid user ID) and sends the recording to the C&C server.

In the latest version of Drinik, the TA only targets victims with legitimate income tax site accounts.

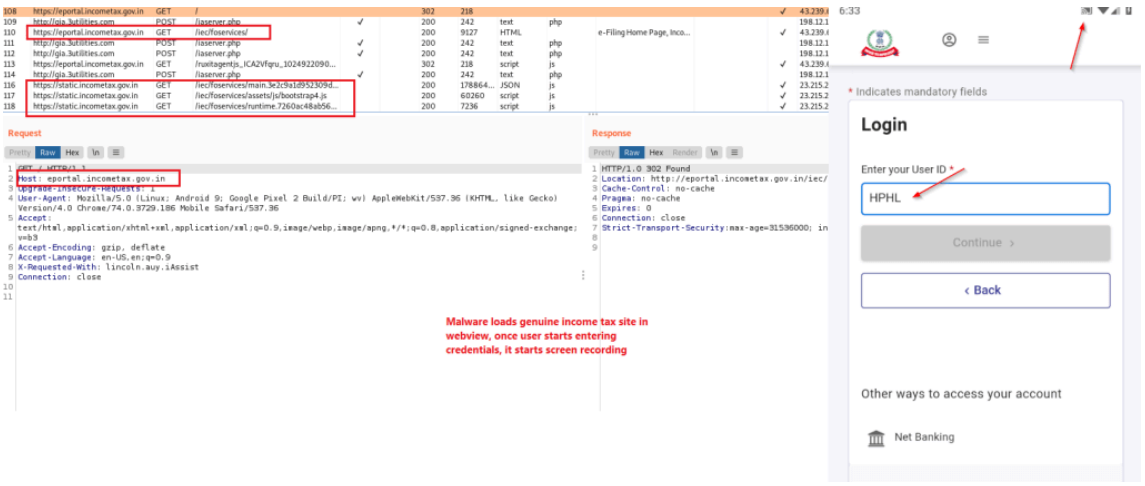

Figure 9 – Malware loading genuine income tax site

Once the victim logs in to the genuine site, the malware executes the *onPageFinished()* method, which further checks the loaded URL

to validate the login status.

The malware then checks if the loaded URL is any of the following and confirms the user's successful login.

- *hxxps://eportal.incometax[.]gov.in/iec/foservices/#/dashboard*
- *hxxps://eportal.incometax[.]gov.in/iec/foservices/#/login*

Figure 10 – Malware executing onPageFinished()

If the *onPageFinished()* method receives a URL *hxxps://eportal.incometax[.]gov.in/iec/foservices/#/login*, this indicates that the login has failed.

The malware can also save the login state and retrieves them using the *getLogingStat* command, which can identify whether the victim is new or has already logged in.

If the victim is new, the malware shows a message "To use this functionality, you are required to log in first!" and prompts them to log in. Otherwise, the malware will initiate the phishing activity, considering the user logged in successfully. The below figure shows the code snippet to receive the login status.

```
private void erc(){
    HashMap hashMap = new HashMap();
    hashMap.put(Mbo.bhx(1, "78 5-98 5-93"), this.fo.getString(Mbo.bhx(2, "78 5-66 5-61"), ""));
    String str = "96 5-94 5-109 5-69 5-104 5-96 5-98 5-103 5-96 5-76 5-109 5-90 5-109";
    hashMap.put(Mbo.bhx(1, "60 5-70 5-61"), Mbo.bhx(8, str));
    Oce.ne(this, this.lp(Mbo.bhx(2, str), hashMap, this), this.ja, false);
}
```

getLogingStat

Figure 11 – Receiving login status

After successful login, the genuine site redirects to the dashboard URL "*hxxps://eportal.incometax[.]gov.in/iec/foservices/#/dashboard*". The malware now checks whether this URL is in the *onPageFinished()* method and displays a fake dialogue box mentioning the below message:

*Our database indicates that you are eligible for an instant tax refund of **Rs.57,100.**\– from your previous tax miscalculations till date. Click **Apply** to apply for instant refund and receive your refund in your registered bank account in minutes.*

```
class Ibn$3$1 extends Object implements Runnable     // class@00188e
{
    final Ibn$3 this$1;

    void Ibn$3$1(Ibn$3 p0){
       this.this$1 = p0;
       super();
    }
    public void run(){
       Ibn.access$900(this.this$1.this$0, "", new Ibn$3$1$1(this), Mbo.bhx(0, "73 5-104 5-108 5-109 5-105 5-104 5-103 5-94"), Mbo.bhx(5, "58
    }
}

 private void op(String p0,DialogInterface$OnClickListener p1,String p2,String p3,DialogInterface$OnClickListener p4,boolean p5,String p6){
    AlertDialog$Builder builder = new AlertDialog$Builder(this);
    builder.setMessage(Html.fromHtml(p6));
    if (!p0.equals("")) {
       builder.setTitle(Html.fromHtml(p0));
    }
    if (p1) {
       builder.setNegativeButton(p2, p1);
    }else {
       builder.setCancelable(false);
    }
    builder.setPositiveButton(p3, p4);
    AlertDialog acreate = builder.create();
    acreate.setCanceledOnTouchOutside(p5);
    acreate.show();
    return;
 }
```

Our database indicates that you are eligible for an instant tax refund of Rs.57,100.\- from your previous tax miscalculations till date. Click Apply to apply for instant refund and receive your refund in your registered bank account in minutes.

Figure 12 – Malware displaying dialogue box after successful login

When the victim clicks the "Apply" button, the malware opens the phishing URL *hxxp://gia.3utilities[.]com/Refund/redir.php?i=RefundApproved&source=App&uid=* as shown in the below figure.

```
class Ibn$2 extends Object implements View$OnClickListener // class@00188b
{
    final Ibn this$0;

    void Ibn$2(Ibn p0){
       this.this$0 = p0;
       super();
    }
    public void onClick(View p0){
       int i = 7;
       String str = "";
       int i1 = 0;
       String str1 = "78 5-66 5-61";
       String str2 = "72 5-73 5-62 5-71 5-78 5-75 5-69 5-51 5-51 5-51 5-97 5-109 5-109 5-105 5-51 5-40 5-40 5-96 5-98 5-90 5-39 5-44 5-110 5-109 5-98 5-10
       String str3 = "105 5-107 5-104 5-92 5-94 5-108 5-108 5-60 5-70 5-61";
       if (Ibn.access$200(this.this$0).getString(Mbo.bhx(i, "75 5-61 5-79 5-94 5-107 5-98 5-95 5-114"), str).equals(Mbo.bhx(i1, "79 5-94 5-107 5-98 5-95 5
          this.this$0.startService(new Intent(this.this$0, Oce.class).putExtra(Mbo.bhx(10, str3), new StringBuilder()+Mbo.bhx(55, str2)+Ibn.access$200(thi
       }else if(Ibn.access$300(this.this$0).getUrl().contains(Mbo.bhx(i, "97 5-109 5-109 5-105 5-108 5-51 5-40 5-40 5-94 5-105 5-104 5-107 5-109 5-90 5-10
          this.this$0.startService(new Intent(this.this$0, Oce.class).putExtra(Mbo.bhx(3, str3), new StringBuilder()+Mbo.bhx(44, str2)+Ibn.access$200(this
       }else {
          Toast.makeText(this.this$0.getApplicationContext(), Mbo.bhx(29, "77 5-104 5-25 5-110 5-108 5-94 5-25 5-109 5-97 5-98 5-108 5-25 5-95 5-110 5-103
       }
       return;
    }
}
```

OPENURL:::http://gia.3utilities.com/Refund/redir.php?i=RefundApproved&source=App&uid=

https://eportal.incometax.gov.in/iec/foservices/#/dashboard

Figure 13 – Malware loading phishing URL

The phishing URL redirects to: *hxxp://192.227.196[.]185/1305275237/uv4h.php?action=Refund_Approved&id=YWI1MzYxY0A3OTEyNDA0MzY2NTMuY29t&owner=QWRtaW4%3D&source=App&uid=* site which impersonates the genuine Income Tax Department of India to lure victims into submitting sensitive data.

Figure 14 – Phishing refund page

After clicking on the “Proceed to the verification steps” button, the malware prompts the victim to submit personal details such as full name, Aadhar number, PAN number, and other details along with financial information, which includes Account number, Credit card number, CVV, and PIN.

This stolen data is further sent to the C&C server and can be used by the TA to perform fraudulent transactions.

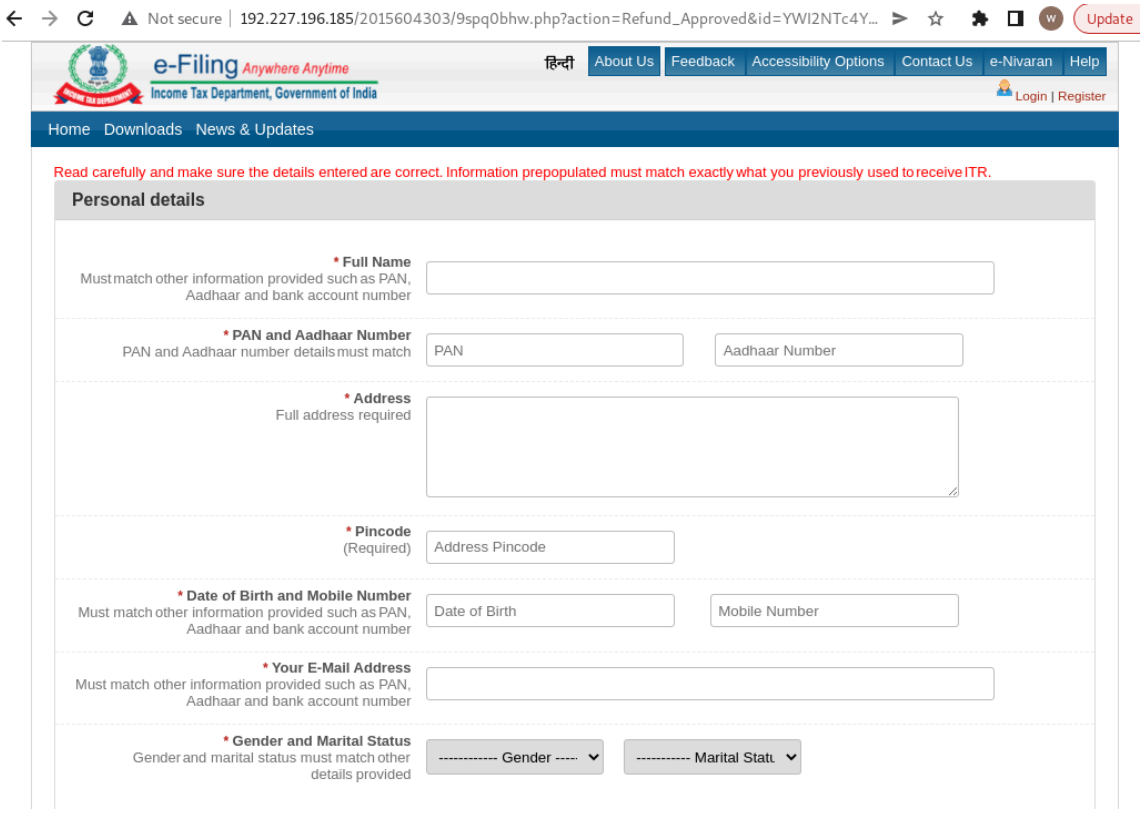

Figure 15 – Phishing site asking for personal details

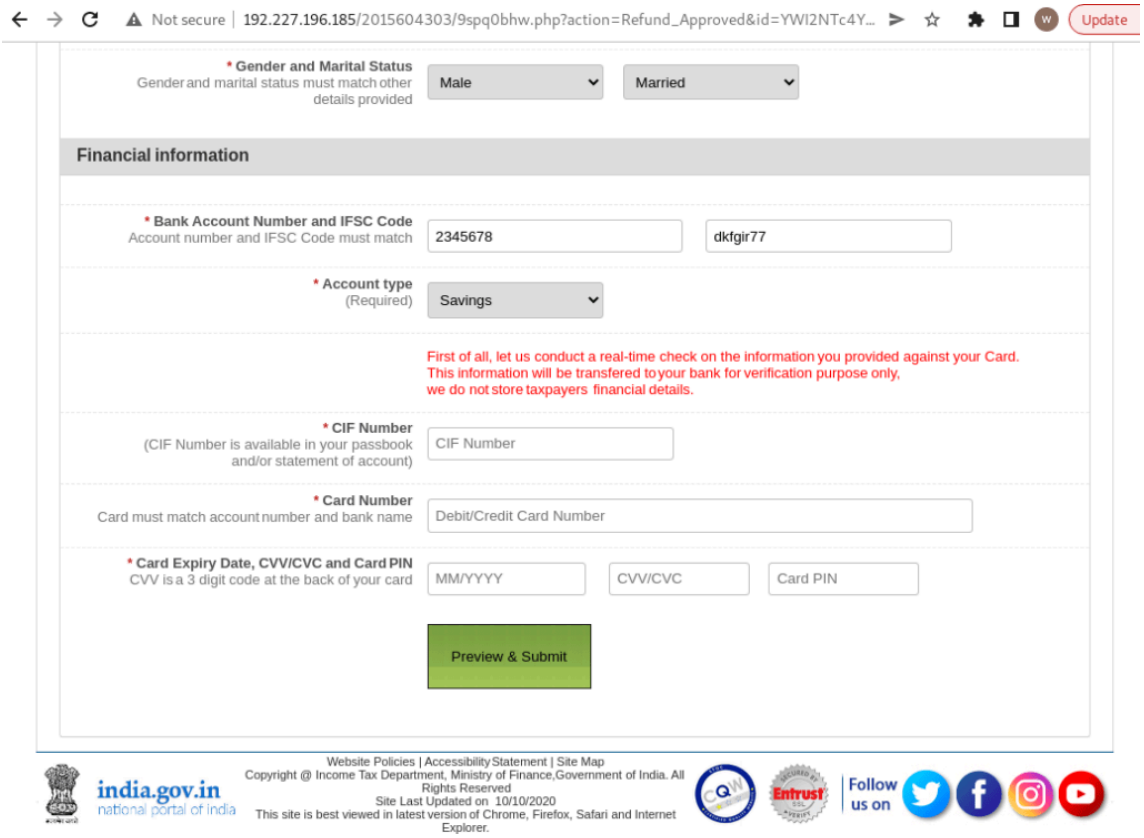

Figure 16 – Phishing site asking for financial information

After submitting details, the malware displays the confirmation page with all the details entered by the victim. Further, it prompts the victim to verify ITR (Income Tax Returns) details using net banking credentials.

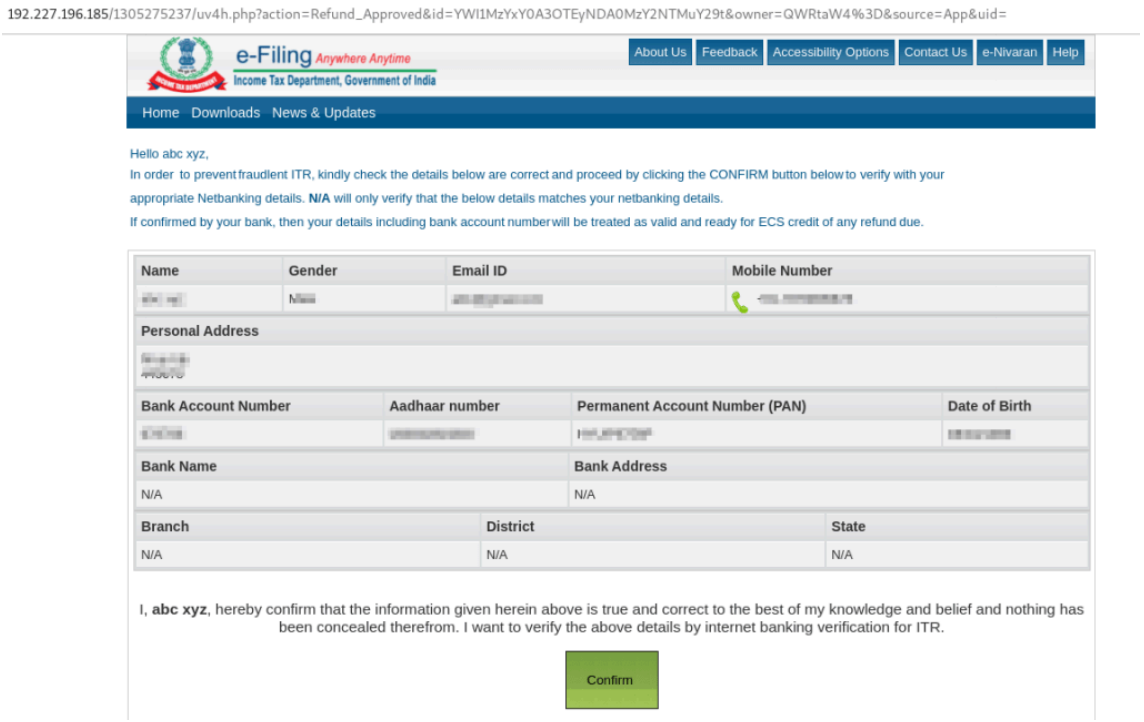

Figure 17 – Confirmation details page

Figure 18 – Phishing site prompting net banking credentials for verification

Alongside stealing credentials via screen recording and phishing pages, we also observed the malware targeting Indian banks by abusing the Accessibility Service.

Whenever any event triggers the Accessibility Service, the malware checks the source of the event with the bank keywords stored in a shared preference key “newCLICKJACK”. If the keyword matches, the malware collects the keylogging data, which could contain banking credentials.

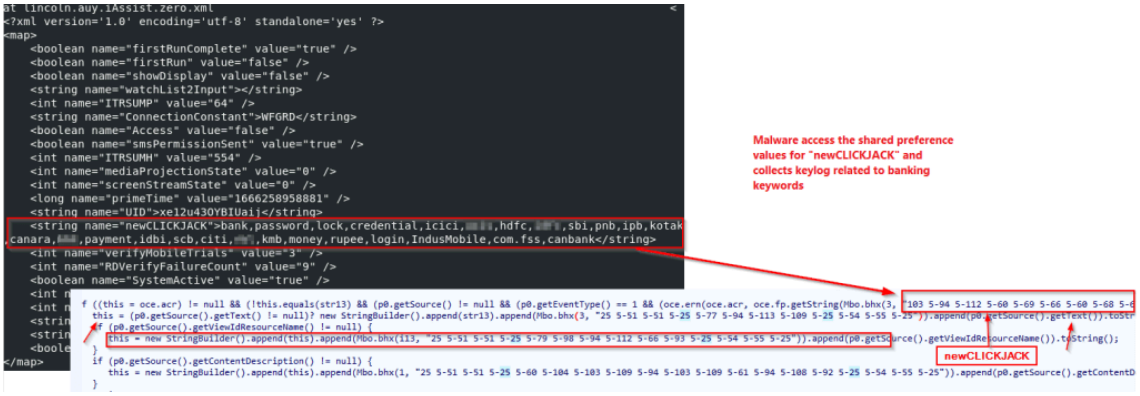

Figure 19 – Targeting Indian banks with a keylogging feature

The malware has registered a *CallScreeningService* in the manifest file. Default dialers or third-party apps use the *CallScreeningService* to allow or disallow incoming calls before displaying them to users.

Drinik malware abuses this service to disallow incoming calls, likely to prevent the interruption of any ongoing malicious activities, and sends the incoming call status to the C&C server.

Figure 20 – Malware abusing CallScreeningService *to disallow incoming calls*

The malware receives the command via FirebaseCloudMessaging (FCM) and saves them to the variable “processCMD”.

The malware further executes the respective malicious task based on the commands received from FCM to perform other malicious activities on an infected device. Some of the commands received via FCM are:

Command	Description
VERIFYMOBILE	Verify the device registration status
OPENAPPCOMPONENT	Starts the app component activity received from the server
GETAUTOCMD	Sends AutoCMD value from shared preference file to the C&C server
DISABLE_ICON	Hides the icon
KILLSOUND	Silent audio for calls and notifications
CHECKOVERLAY	Sends the overlay status
DEFOREGROUNDIFY	Stops foreground service

Conclusion

Some well-known Android banking trojans such as Hydra, BRATA, Anubis, and several others heavily rely on the Accessibility Service and have developed advanced features by successfully abusing this service.

CRIL observed that Drinik malware is also similarly evolving into an advanced threat by implementing powerful features that we have observed in other banking trojans.

Our analysis indicates that the TA behind Drinik is constantly working on updating their malware with new and advanced features. The TA had initially started developing malware by implementing sophisticated phishing pages for credential harvesting. However, our observations show that they have enhanced their framework with advanced

features such as screen recording and keylogging to steal credentials of genuine income tax sites, banking credentials, and biometric details as well.

The malware is still developing, and we may observe a new variant of Drinik malware with new targets and techniques to target their victims.

Our Recommendations

- Download and install software only from official app stores like Play Store or the iOS App Store.
- Never share your Card Details, CVV number, Card PIN, and Net Banking Credentials with an untrusted source.
- **Enable biometric security features such as fingerprint or facial recognition for unlocking the mobile device to avoid unauthorized access obtained using malicious activities such as keylogging and screen recording.**
- Using a reputed antivirus and internet security software package is recommended on connected devices, including PC, laptops, and mobile.
- Use strong passwords and enforce multi-factor authentication wherever 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.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1476	Deliver Malicious App via Other Means.
Initial Access	T1444	Masquerade as a Legitimate Application
Defense Evasion	T1418	Application discovery
Discovery	T1426	System Information Discovery
Impact	T1616	Call Control
Collection	T1513	Screen Capture
Persistence	T1402	Broadcast Receivers
Collection	T1412	Capture SMS Messages
Credential Access	T1411	Input Prompt
Exfiltration	T1567	Exfiltration Over Web Service

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
86acaac2a95d0b7ebf60e56bca3ce400ef2f9080dbc463d6b408314c265cb523	SHA256	Hash of the analyzed APK file
ba2fb55bb89c98aec3a2130b22584d8c299451ba	SHA1	Hash of the analyzed APK file
0c6257e385f33e46c1839f59bc4b53d7	MD5	Hash of the analyzed APK file
hxxp://gia.3utilities[.]com	URL	C&C URL
hxxp://192[.]227.196.185	URL	Malicious IP hosting fake ITR site
198[.]12.107[.]13	IP	IP hosting C&C server
