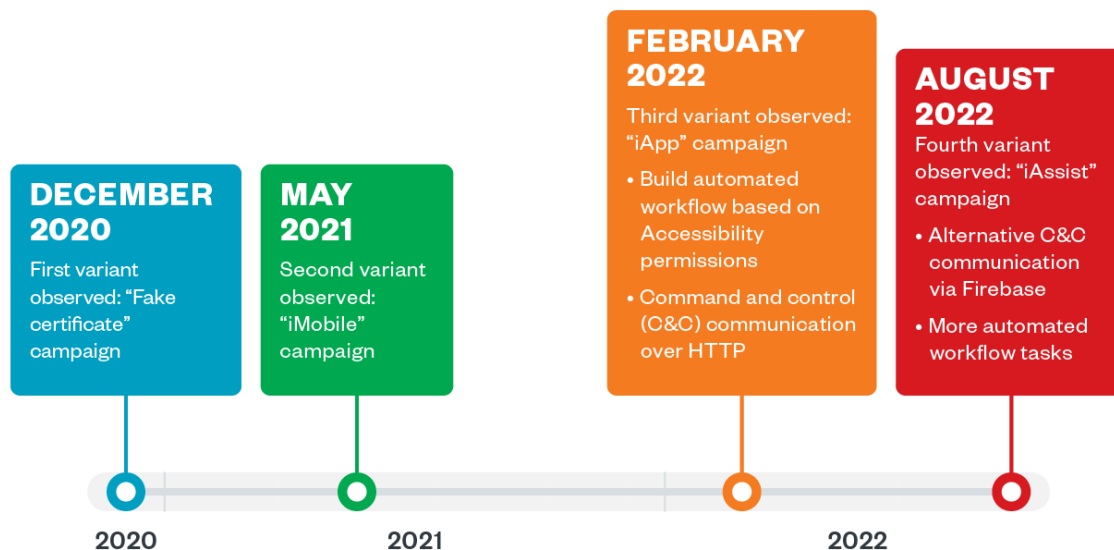


Massive Phishing Campaigns Target India Banks' Clients



©2022 TREND MICRO

Figure 1. Timeline of Elibomi variants deployed

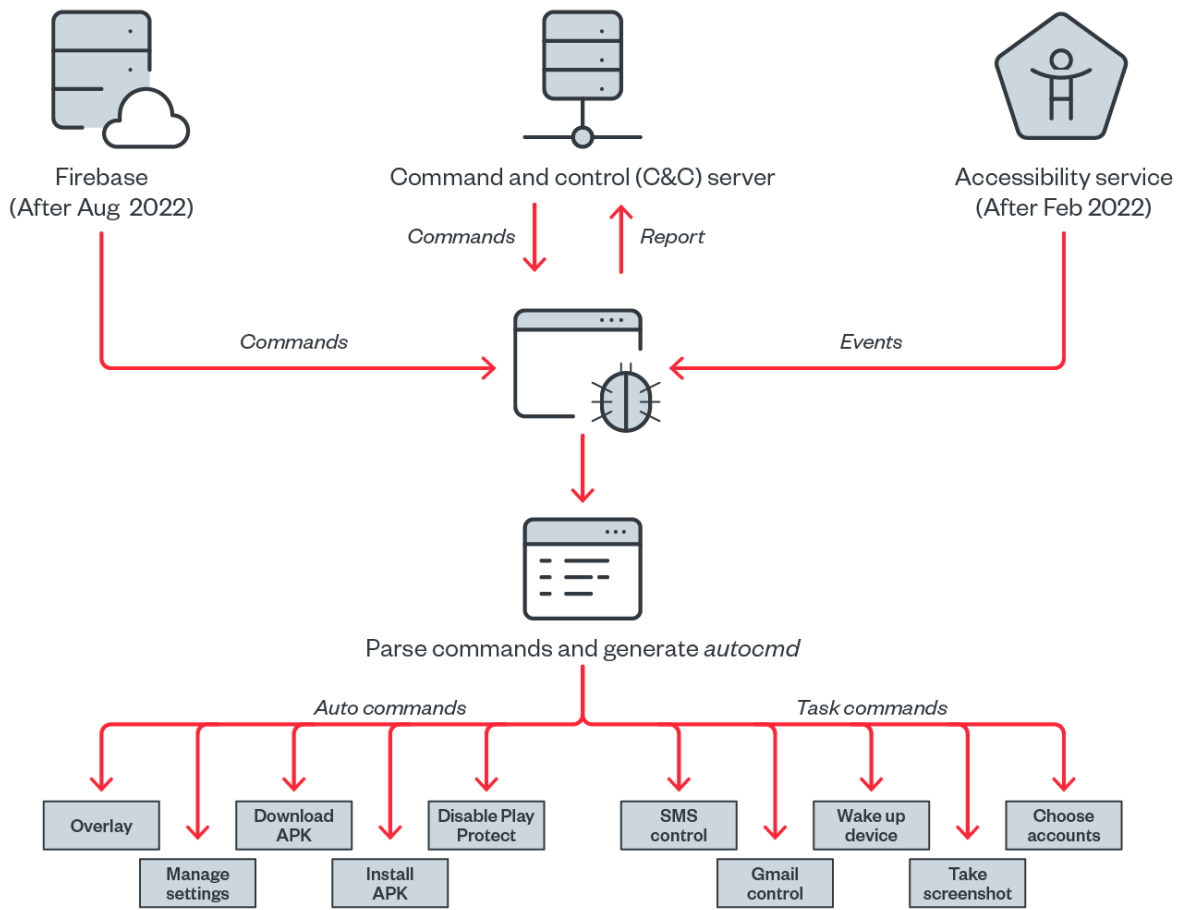
By Trend Micro Mobile Team

We observed an uptick in attacks targeting bank customers in India, the common entry point being a text message with a phishing link. The SMS content urges the victims to open the embedded phishing link or malicious app download page and follow the instructions: To fill in their personally identifiable information (PII) and credit card details to allegedly get a tax refund or credit card reward points. As of this writing, we observed five banking malware families involved in these attacks, namely Elibomi, FakeReward, AxBanker, IcRAT, and IcSpy.

We analyzed that the bank customers targeted include account subscribers of seven banks, including some of the most well-known banks located in the country and potentially affecting millions of customers. Common among these routines include the abuse of the legitimate banks' logos, names, and affiliated brands and services to convince victims that their respective phishing sites are affiliated. This blog entry will discuss three of the identified banking malware families and their latest changes (as IcRAT and IcSpy have been documented): Elibomi is an old malware that has evolved into a fully equipped banking trojan, while FakeReward and AxBanker are newly discovered banking trojans. Bank clients are advised to remain vigilant against these kinds of threats, and to protect their information and devices from malware infections.

Elibomi returns with more functions

Elibomi's first and second variants, "fake certificates" and "iMobile" campaigns, appeared towards the end of 2020 and remained active in 2021, designed to steal victims' PII and credit card information. During the early months of 2022, we observed a phishing campaign dropping a new variant of Elibomi with a package name that ended with "iApp." From this variant on, the routine changed drastically: the threat actors added automation to workflow tasks via Accessibility permissions such as automated clicking, granting of permissions, and capturing screenshots.



©2022 TREND MICRO

Figure 2. Elibomi's latest variants' functions

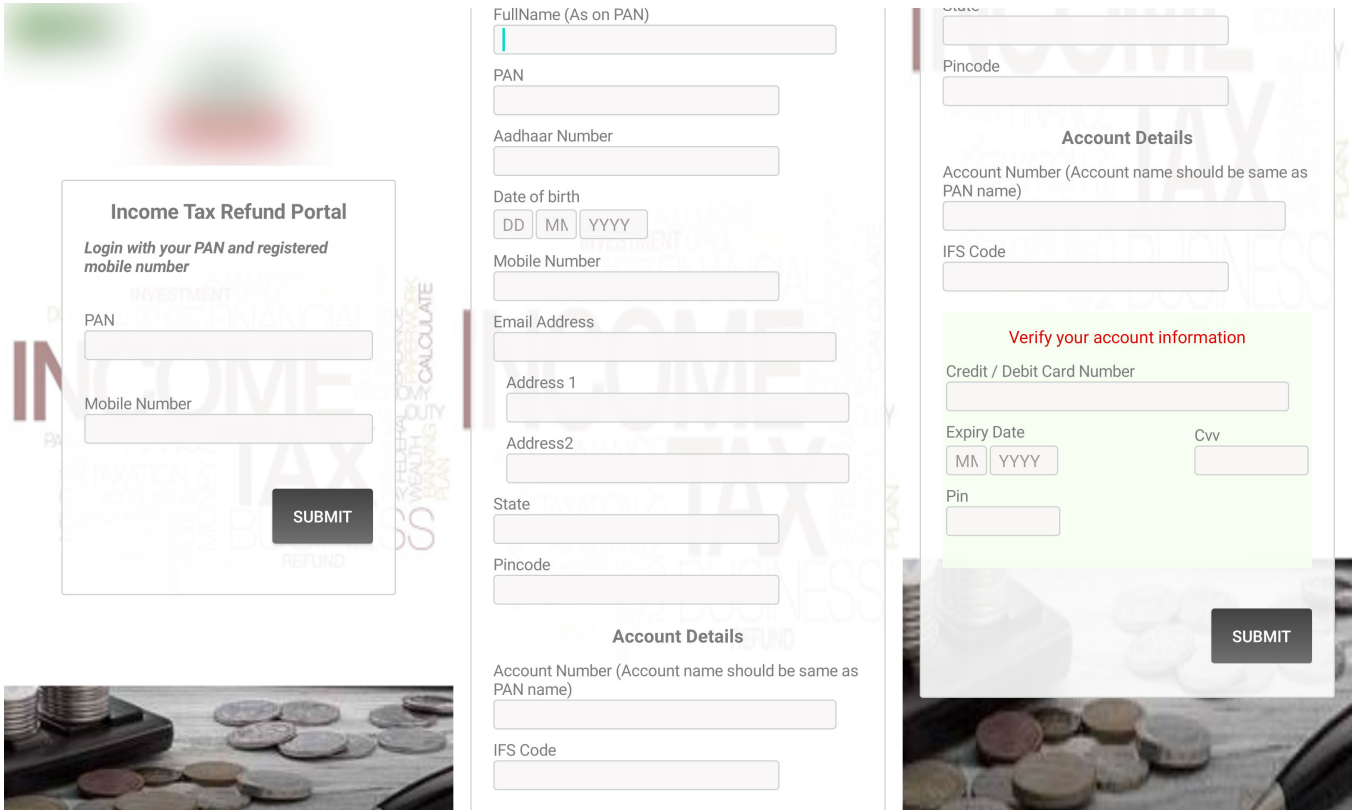


Figure 3. Elibomi’s phishing page harvests the victim’s PII and credit card information

More recently, we found a fourth variant of Elibomi delivered from the same phishing site with a package name ending with “iAssist.” This variant added the cloud-hosted real-time database Firebase as an alternative command and control (C&C) server and an environment check tool called RDVerify for detection evasion. In the next sections, we detail the different commands and functions that the third and fourth variants of Elibomi are capable of, as well as the implications of these updates. It is also worth noting that an update has again been observed in October on the latest iterations, as documented by security researchers from [Cyble](#).

Overview: Elibomi’s automated variants

Due to the automated workflow framework of the latest variants, we called the third (“iApp” campaign) and fourth (“iAssist” campaign) automated variants and break down the commands and functions we found from their respective routines.

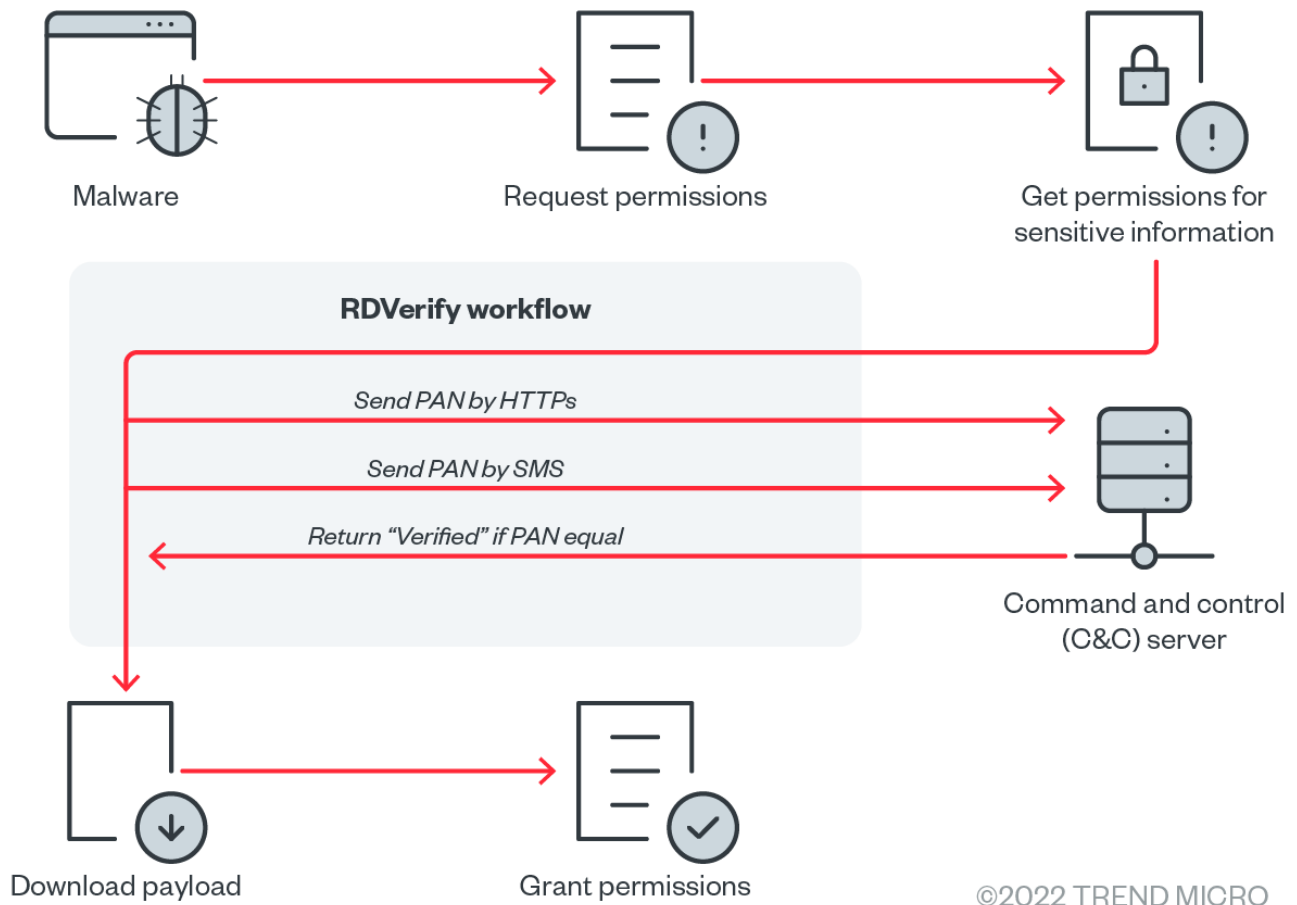


Figure 4. RDVerify workflow

Sophisticated command format

Looking into the routines of the third and fourth variants, Elibomi implements a sophisticated and lengthy command list and has three types of commands to conduct malicious activities: Task command, server command, and auto command. The succeeding section breaks down the three commands we found.

Task command

We found that the task command was the main command among the three, enumerating the specific malicious activities needed in the routine. It is capable of being a recursive command for complex tasks, or a non-recursive command function:

1. As a non-recursive command: A single command that contains the command name and corresponding operands. This can be split by “...” to get the sub-terms.
2. As a recursive command: A combination of non-recursive commands that can be split by “,” or “-” to get non-recursive commands.

As an example, should a specific aspect of Elibomi’s routine require unlocking the device without the user becoming aware of it, the malware can use this recursive command to accomplish three tasks: wakeup, remove the screen overlay, and make the gesture combination for the unlock screen pin or pattern.

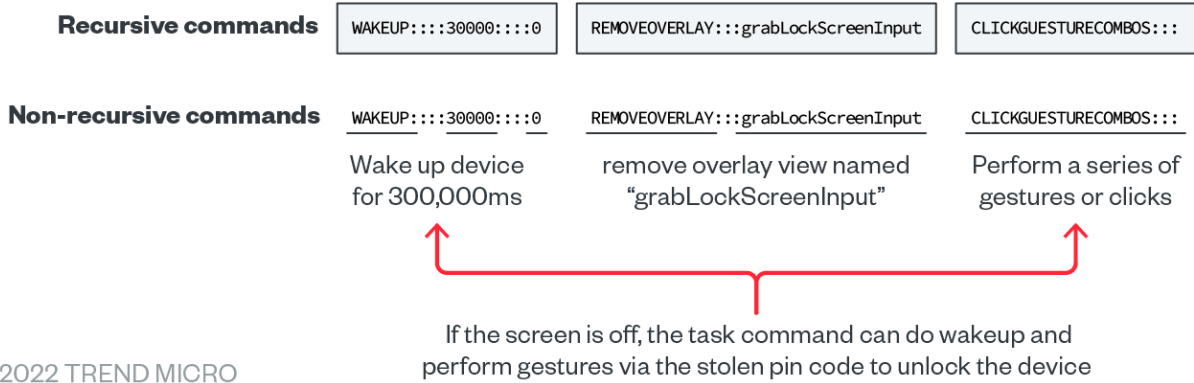


Figure 5. Elibomi task command

Server command

This command returns the execution result to the backend server. For example, "D:::Unlock has been executed - ##-##" shows and communicates with the server that the task command was able to unlock the device successfully.

Auto command

The auto command plays a vital role in Elibomi's automated workflow, describing how Elibomi uses *Accessibility* to conduct the malicious behaviors step by step. For example, auto command is responsible for how Elibomi enables the Media Projection automatically. When the attackers get the Accessibility permissions granted and receive the task command *MEDIAPROJECTION*, Elibomi will generate the auto command <SCREENCLICK:Button:start now|ok|accept|allow> to click on "START NOW" in the MediaProjection dialog box.

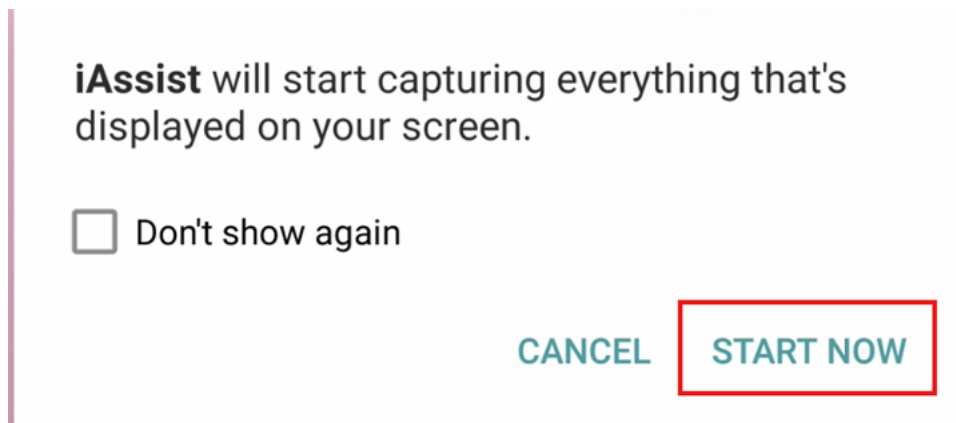


Figure 6. Taking screenshots of the victim's window

A fully automated malware

Analyzing the routines that the two latest variants of Elibomi are capable of, this malware can interact with the device's user interface (UI) automatically without the user knowing. To become a "fully automated malware," Elibomi will show a message upon launch that pushes the user to enable Accessibility permissions by disguising itself as a Google application. It then proceeds to show a dialog box upon launch as if there is an urgent need to grant Accessibility permissions to push the user to allow the said request.

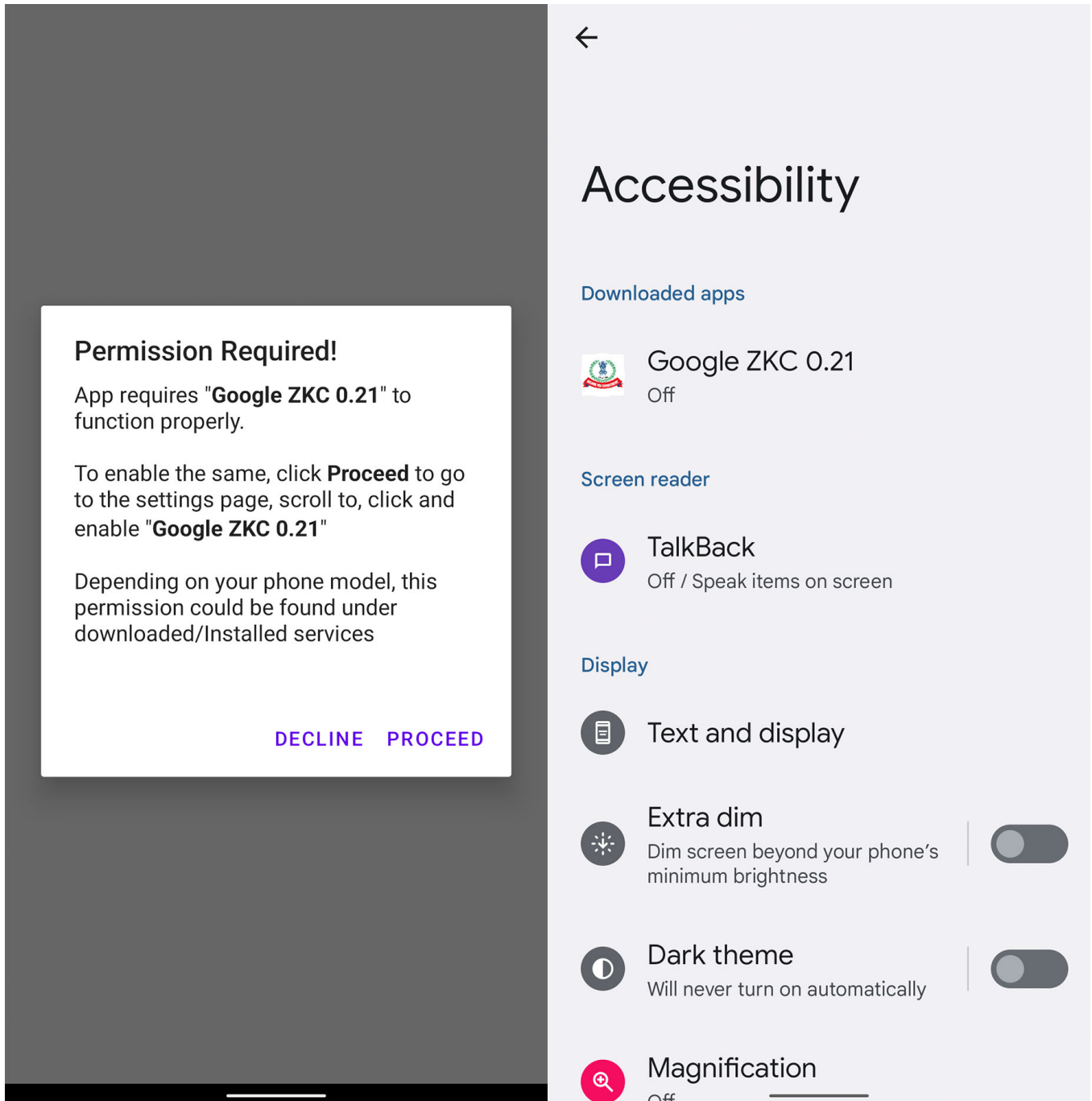


Figure 7. Elibomi requests for the Accessibility permission to proceed with the automated tasks

The following is the full list of malicious tasks that have been added to Elibomi's automation workflow in the latest automated variants:

Task	Related Task Command	Related Auto Command
Get MediaProjection permission	EXECUTORSEQUENCE::: PERMISSIONFOLLOWUP#222#MEDIAPROJECTIONPERMISSION	CLICK:Button:start now ok accept allow:-::-:5
Allow Write settings	EnableSettingsSequence	fullforwardswipe:Switch:-::-:fullforwardswipe
Get SMS-related permissions	EXECUTORSEQUENCE::: PERMISSIONFOLLOWUP#222# SMSPERMISSION	CLICK:Button:ok accept allow:-::-:CLICK:But

Set itself as default SMS app	PERMISSIONS:::REVOKEDFAULTSMS STARTSMSSEQUENCE	CLICK:Button:yes ok accept allow:-::-:SCRE
Allow Install App from Unkown Source	REQUESTINSTALLPERMISSION	CLICK:Button:ok accept allow:-::-:CLICK:But
Disable battery optimization	IGNORE_BATTERY_OPTIMIZATIONS	CLICK:Button:ok accept allow:-::-:SCREENC
Install additional APK and grant permission for the payload	DOWNLOADAPK EXECUTORSEQUENCE:::INSTALLAPK EXECUTORSEQUENCE:::OPENAPPCOMPONENTandGRANTPERMISSIONS	CLICK:Button:ok accept allow:-::-:CLICK:But
Get all accounts	SCREENSHOT GLOBAL_ACTION_BACK	N/A
Disable Google Play Protect	DISABLEPLAYPROTECT	N/A
Read or delete emails from Gmail	GMAILSEQUENCE	click:android.widget.Button:Empty:-:-
Prevent disable Accessibility	GLOBAL_ACTION_BACK	N/A
Prevent Uninstall	GLOBAL_ACTION_BACK	N/A
Prevent enabling of Google Play Protect	GLOBAL_ACTION_BACK	N/A
Unlock device	WAKEUP	N/A

Table 1. List of malicious tasks added to the two latest variants of Elibomi

Elibomi affects Android 12 and lower, and can automatically grant the attackers sensitive permissions, enable/disable sensitive settings such as enable installation of apps from unknown sources, and disable GooglePlay protect. Android 13 is not affected as Google restricts the Accessibility permission in the latest version.

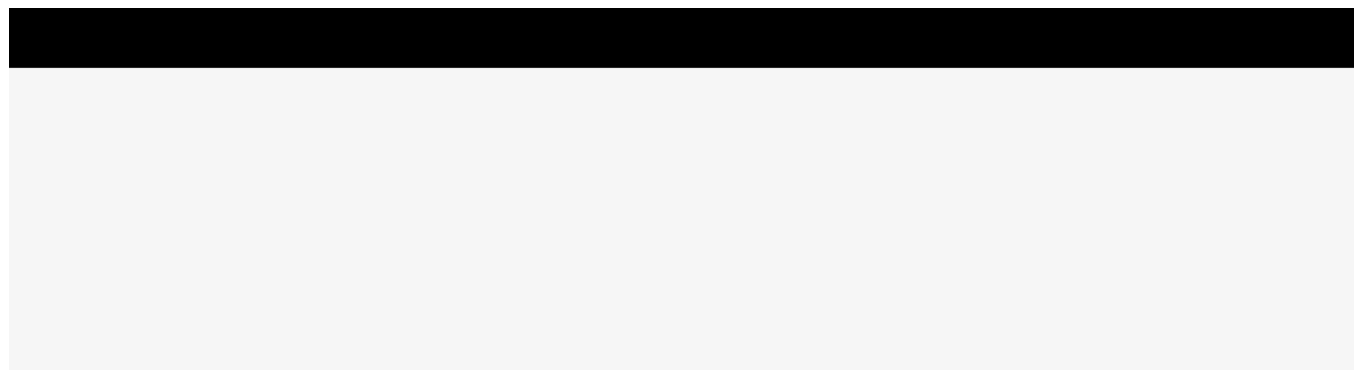
Video 1. How Elibomi's latest campaign operates in the user's mobile device

Overlay mechanisms

For both iApp and iAssist campaigns, Elibomi implements an overlay by adding a view to the current window as an evasion technique from users, instead of having an overlay on other apps such as bank applications to steal users' credentials.

Wait screen overlay

In order to evade visual detection from users, Elibomi will show a waiting screen after gaining Accessibility permissions for service. However, it already executes an automated workflow in the background to grant sensitive permissions to the attacker.





Setting up, please wait..

Remaining 12 seconds

Figure 8. Wait screen overlay to hide malicious activities in the background

Elibomi uses another window type called “TYPE_ACCESSIBILITY_OVERLAY” instead of request “SYSTEM_ALERT_WINDOW” permission to add an additional view to the current window.

```
WindowManager.LayoutParams v1 = new WindowManager.LayoutParams(0x7F0, v5, arg4);
v1.dimAmount = arg3;
return v1;
}
```

Figure 9. Create layout with type “TYPE_ACCESSIBILITY_OVERLAY”

Fake pin overlay

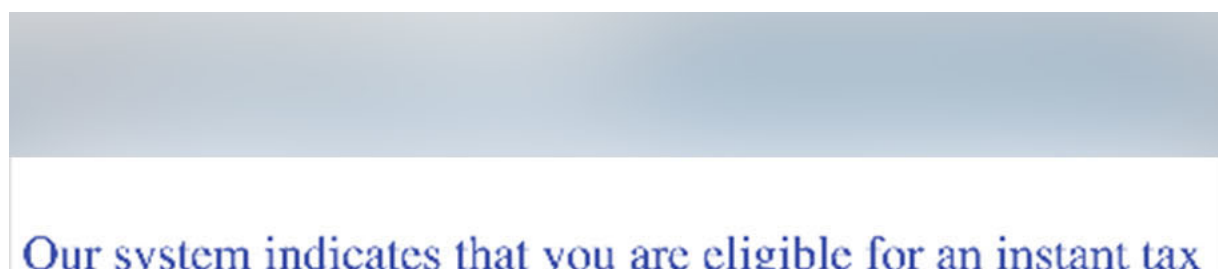
To unlock the device automatically, Elibomi is capable of stealing the pin code or pattern saved by the user by showing an overlay screen to the victim and “listening” for the user’s actions to record their gestures and clicks.

```
View.OnTouchListener avb(String arg2, String arg3) {
return new View.OnTouchListener() {
@Override // android.view.View$OnTouchListener
public boolean onTouch(View arg16, MotionEvent arg17) {
land.bkz.iApp.AcsService.20 v1 = this;
MotionEvent v0 = arg17;
try {
int v3 = arg17.getAction();
if(v3 == 2 && (AcsService.this.apz == v0.getPointerId(0) && ((AcsService.this.art.equals("ACTION_DOWN")) || (AcsService.this.art.equals("ACTION_MOVE"))
float v4 = AcsService.this.arf;
AcsService.this.ara = v4;
long v11 = AcsService.this.arl;
AcsService.this.aro = v11;
float v4_1 = AcsService.this.ari;
AcsService.this.arc = v4_1;
String v4_2 = AcsService.this.art;
AcsService.this.arr = v4_2;
AcsService.this.art = "ACTION_MOVE";
float v4_3 = arg17.getRawX();
AcsService.this.ari = v4_3;
long v11_1 = AcsService.this.aro;
long v3_1 = AcsService.this.arl - v11_1;
float v12 = arg17.getRawX();
AcsService.this.arf = v12;
long v12_1 = System.currentTimeMillis();
AcsService.this.arl = v12_1;
AcsService.this.arx = AcsService.this.arx.equalsIgnoreCase("") ? AcsService.this.ara + "," + AcsService.this.arc + "," + AcsService.this.arf + ","
}
}
```

Figure 10. Touch Listener code to record the victim’s actions observed from Elibomi’s third variant

Not just Android

From our scanning online, we [found](#) the cybercriminals extending their phishing campaign not only on Android but have also ventured to other platforms such as email. Comparing [previous](#) phishing sites, it appears that they have created different themes to induce victims to fill in their sensitive information. The type of stolen data is nearly the same as what they require users to put on the Android platform.



refund of **Rs.57,100.-** from your previous tax miscalculations till date. In line with our mandate, this category is qualified for an instant tax refund. Click the link below to download the new Incometax Refund Assistant app **iAssist** now to receive your refunds in minutes.

Incometax Refund is now easier, faster and better with the new **iAssist**, you can now apply for an instant tax refunds from your dashboard. All applications are fasttracked to enable you receive your refund at the earliest. and you will receive updates on the progress of your application. You can start in 3 easy steps

- 1.** Download and install **iAssist** from the link below. (Grant app permission during install).
- 2.** Click on the 'Quick Refund Application' button at the bottom of your screen to submit instant refund application. On successful application, it usually takes minutes for refunds to be received in your bank account. This could as well take longer if we can not verify your details or you have submitted incorrect details.
- 3.** Login with your PAN/AADHAAR/OTHER USERID and your credentials from [REDACTED] to check the progress of your application. Click Register if you are not registered on [REDACTED] to register instantly and then log into your account.

(kindly note that old app has been discontinued).

[Download iAssist Now.](#)



Figure 11. More recent phishing websites urging victims to download the iAssist app

“iAssist” campaign as a fast-evolving Elibomi variant for more profit

In the fourth variant, we noted one interesting task added to their automated workflow. While the Accessibility permission detects the *payment risk* notification string that sends the message “continuing to pay may cause loss of money” to appear on the UI, it will click on “Ignore risk” to dismiss the alert dialog. This warning usually appears if there is a risk of payments or transfers occurring while using a bank app, and can indicate that the cybercriminals behind this malware can consistently update or enhance Elibomi to automatically conduct money transfers from the victim’s device without them noticing.

```
label_508:
v26 = v6;
if(!v7.toLowerCase().contains("payment risk") && (v7.toLowerCase().contains("continuing to pay may cause loss of money")) && (v7.toLowerCase().contains("ignore risk")) &&
AccessibilityNodeInfo v38_1 = Uch.this.getRootInActiveWindow();
Uch.access$2000(Uch.this, // arg0:education.awn.iAssist.Uch
true, // arg1:boolean
"SCREENCLICK", // arg2:java.lang.String
"Ignore risks", // arg3:java.lang.String
"-_", // arg4:java.lang.String
0, // arg5:int
"-_", // arg6:java.lang.String
false, // arg7:boolean
"-_", // arg8:java.lang.String
v38_1, // arg9:android.view.accessibility.AccessibilityNodeInfo
"android.widget.Button" // arg10:java.lang.String
);
}
}
```

Figure 12. Elibomi capable of clicking “Ignore risks” button automatically

FakeReward: Targeting three banks’ customers in India

In August, we found a campaign we named FakeReward targeting customers of three of the largest banks in India wherein the threat actors registered several domains similar to the legitimate domains to confuse victims. These phishing websites were pretending to be the official websites of these three banks, even abusing the companies’ names and logos to complete their look.



Get Instant Reward Points Just by downloading the app and filling Few Details. Get 10% Extra Cashback Coupon Code for your Next Purchase on your Email Id.

Congratulations Your Card has Been Approved
[Download link](#)



loading the app and filling Few Details. Get 10% Extra Cashback Coupon Code for your Next Purchase on your Email Id.

Congratulations Your Card has Been Approved
[Download link](#)

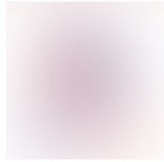


Get Instant Reward Points Just by downloading the app and filling Few Details. Get 10% Extra Cashback Coupon Code for your Next Purchase on your Email Id.

Congratulations Your Card has Been Approved
[Download link](#)

Figure 13. FakeReward's phishing websites target customers of three specific banks in India

The FakeReward banking trojan shows a page to request SMS permissions upon launching. Once granted, the malware will collect all text messages to the device and upload it to a remote server, then set up a monitor to listen to incoming SMS messages and sync it to the remote server. We released an initial [social media thread](#) on the said campaign to warn security teams and their respective bank customers to be vigilant against this malware.



Hey there,

For quick approval and medical loan disbursal at the earliest we require your permission to access.



User Personal Information

Our app collects user account data like name, financial information. This information is required as a part of the registration process to access our service. Our app also collects mobile number for verification to check the active SIM status on the device, uniquely identify you and prevent frauds & unauthorised access.



SMS Permission

Our application requires access to your SMS-upload KYC documents and make your journey with us seamless and smooth.

Deny

Allow

Name

Enter Name

Mobile Number

Mobile Number

Email

Enter Email

Date of Birth

Year

Month

Day

CARD Number

Valid Card Number

Expiry Date

Year

Month

CVV Code

CVV

CARD Holder Name

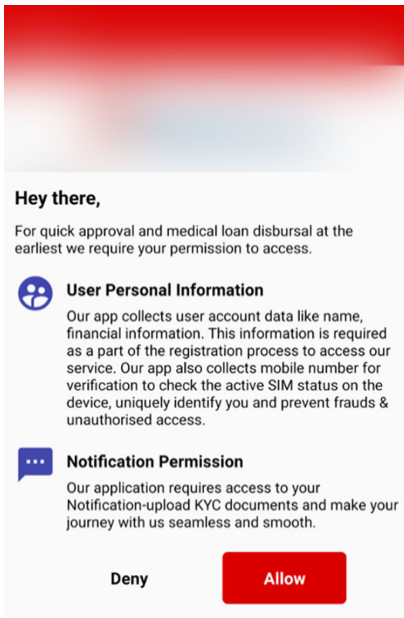
Card holder name

SUBMIT

Figure 14. Requests SMS permissions and collects PII and credit card information

Latest changes

In its recent update, FakeReward malware tries to request a notification permission to extract text messages instead of directly requesting access for SMS permissions.



```

if(this.LOG_TEXT) {
    int v3 = 0;
    this.appName = Util.getAppnameFromPackage(this.context, this.packageName, false);
    this.tickerText = Util.nullToEmptyString(this.n.tickerText);
    if(v0_1 != null) {
        this.title = Util.nullToEmptyString(v0_1.getCharSequence("android.title"));
        this.titleBig = Util.nullToEmptyString(v0_1.getCharSequence("android.title.big"));
        this.text = Util.nullToEmptyString(v0_1.getCharSequence("android.text"));
        this.textBig = Util.nullToEmptyString(v0_1.getCharSequence("android.bigText"));
        this.textInfo = Util.nullToEmptyString(v0_1.getCharSequence("android.infoText"));
        this.textSub = Util.nullToEmptyString(v0_1.getCharSequence("android.subText"));
        this.textSummary = Util.nullToEmptyString(v0_1.getCharSequence("android.summaryText"));
        CharSequence[] v1_2 = v0_1.getCharSequenceArray("android.textLines");
        if(v1_2 != null) {
            this.textLines = "";
            while(v3 < v1_2.length) {
                this.textLines = this.textLines + v1_2[v3] + "\n";
                ++v3;
            }
            this.textLines = this.textLines.trim();
        }
    }
}
}

```

Figure 15. Request notification permission as seen by the user (left), and the code to parse the notification (right)

Security researchers from [K7 Security Labs](#) and [MalwareHunterTeam](#) have also found samples of at least five other FakeReward variants. We noted the increase in the number of families and variants of FakeReward malware targeting users in India that appear the same when examined using tactics, techniques, and procedures (TTPs) but show differences in codes. Trend Micro customers are protected from all these emerging phishing families and variants.

Potential connection between FakeReward and IcRAT

During our investigation, we found an interesting coincidence: FakeReward and IcRAT started targeting the customers of one bank nearly at the same time. Moreover, we also found the phishing websites of these two malware families to be nearly similar, making us believe that the cybercriminals behind these two malware families are connected.

FILES 2		Detections	Size	Sort by	Export	Tools	Help
		First seen	Last seen	Submitters			
2DA210623178F90801E53394DB438098D23674063C538F341EF5094EBDE61131	FakeReward	0 / 65	7.00 MB	2022-09-23 14:35:20	2022-09-24 06:13:57	2	
8325398082C110E9219CF8D963C91587753F1080DD109CEEFC47E8C7EF978FE9	IcRat	5 / 65	3.78 MB	2022-09-22 14:26:09	2022-09-22 14:26:09	1	

Figure 16. Tracking FakeReward and IcRAT (Screenshot taken from VirusTotal)

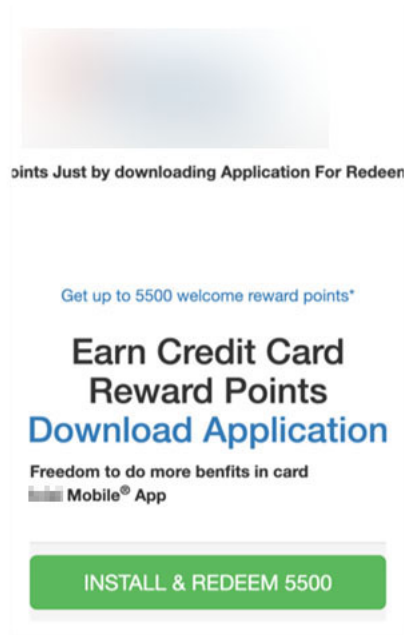


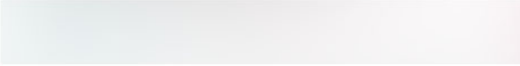
Figure 17. Phishing site of IcRAT

AxBanker: Fake app targeting bank's customers

In addition to FakeReward banking malware targeting the customers of two banks, we also found another [banking trojan](#) targeting the customers of another major Indian bank that has been active since late August. The website has a similar phishing theme wherein customers "Get Reward Points" to attract victims to download and install the app.

Up to **10X**  **REWARD Points**
on **100+** brand gift cards

With your Credit & Debit Cards.





Buy Now



T&C apply.

Progress with REWARDS

REWARDS is a carefully crafted loyalty programme by  that allows customers to earn points for every relationship they have with the Bank - Savings and Current Account, credit and Debit Cards and across all other retail products like  Direct, Forex and NRI.

Burgundy Private

Earn points on Burgundy transactions, and redeem them for **500+** options.

Download App

Copyright © 2022 

Figure 18. AxBanker phishing website pretending to be an offer from a major bank

Once the malware is installed and launched, it will request SMS permissions in order to capture and upload incoming SMS to a remote server. The malware will then show several fake pages to collect the victim's personal data and credit card information.

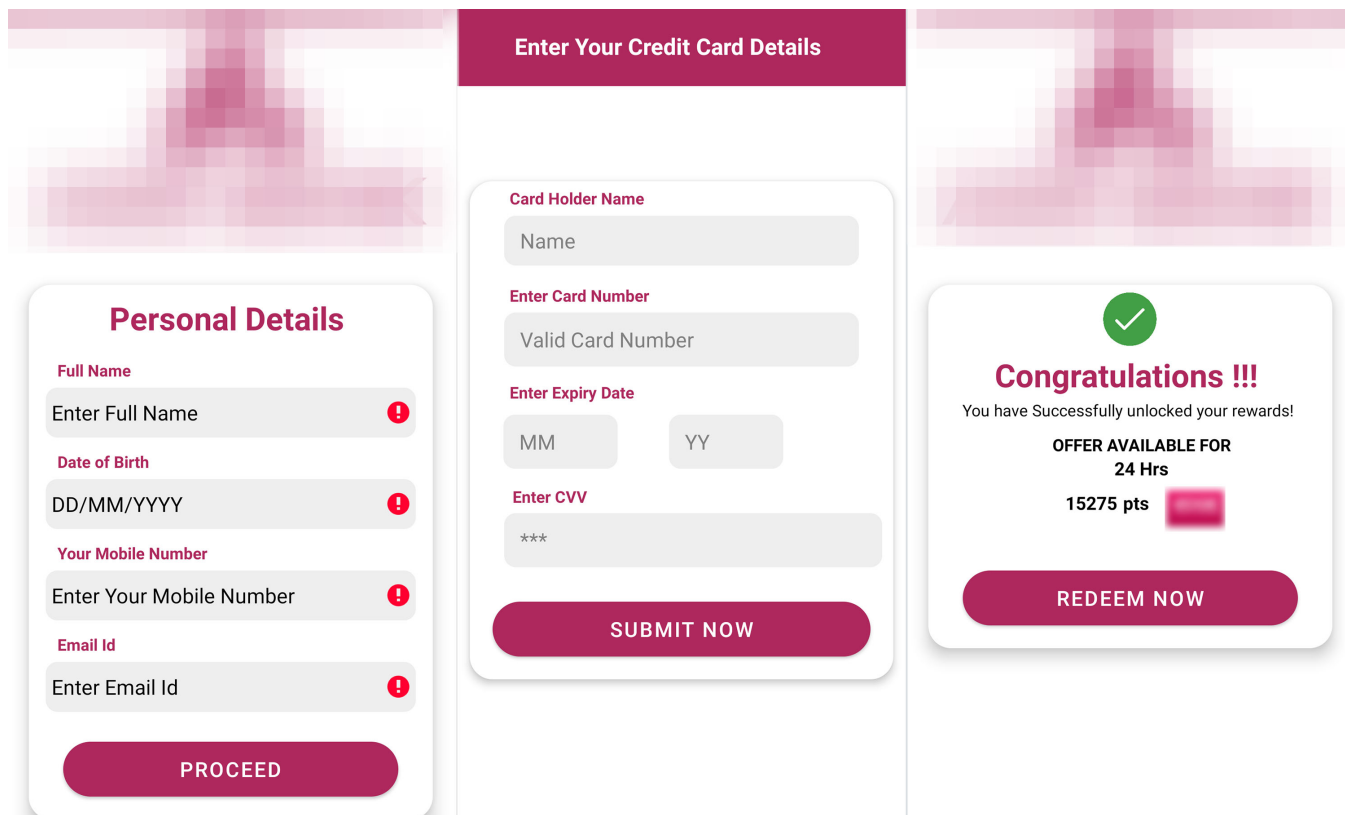


Figure 19. AxBanker malware harvests the victim's personal data and credit card information

Conclusion

While the types of stolen data and phishing themes are similar, we don't have enough evidence to conclude that the cybercriminals behind all of these banking malware families are connected but are aggressive in developing further. In the case of the threat actors behind Elibomi, these cybercriminals are likely knowledgeable and adept in Android development based on the automation of tasks pertaining to Accessibility permissions. Meanwhile, the threat actors behind FakeReward appear to have deployed phishing malware prior to this campaign based on their capability of hiding their tracks: the phishing domains used operate for only three to four days at a time before becoming inaccessible. In addition, a quick scan shows that only a few security engines have been able to pick up on its new variant.

Our monitoring also shows that while no other customers outside India have been targeted by these malware families, phishing campaigns in the country have significantly increased and are increasingly becoming adept at detection evasion. One possible reason for this uptick is the growing number of new threat actors entering the India underground market, bringing with them profitable business models, and interacting with other malicious players to learn, exchange ideas from, and establish connections. Users and bank customers are advised to remain vigilant and follow these best practices:

- Check the text message's sender. Legitimate companies and organizations have official contact channels from where they send notifications and promotions.
- Do not download and install applications from unknown sources. Choose to download the official bank apps from official platforms.
- Do not enter sensitive personal information in untrusted apps or websites. Contact banks and organizations through their known channels to ask if they have ongoing promotions or announcements like the message received.
- Double check the dialog boxes' requests and messages before granting sensitive permissions such as Accessibility to untrusted apps.

Trend Micro solutions

[Trend Micro Mobile Security Solutions](#) can scan mobile devices in real time and on demand to detect malicious apps, sites, or malware to block or delete them. These solutions are available on Android and iOS, and can protect users' devices and help them minimize the threats brought by these fraudulent applications and websites.

Indicators of Compromise (IOCs)

For a full list of the IOCs, find it [here](#).