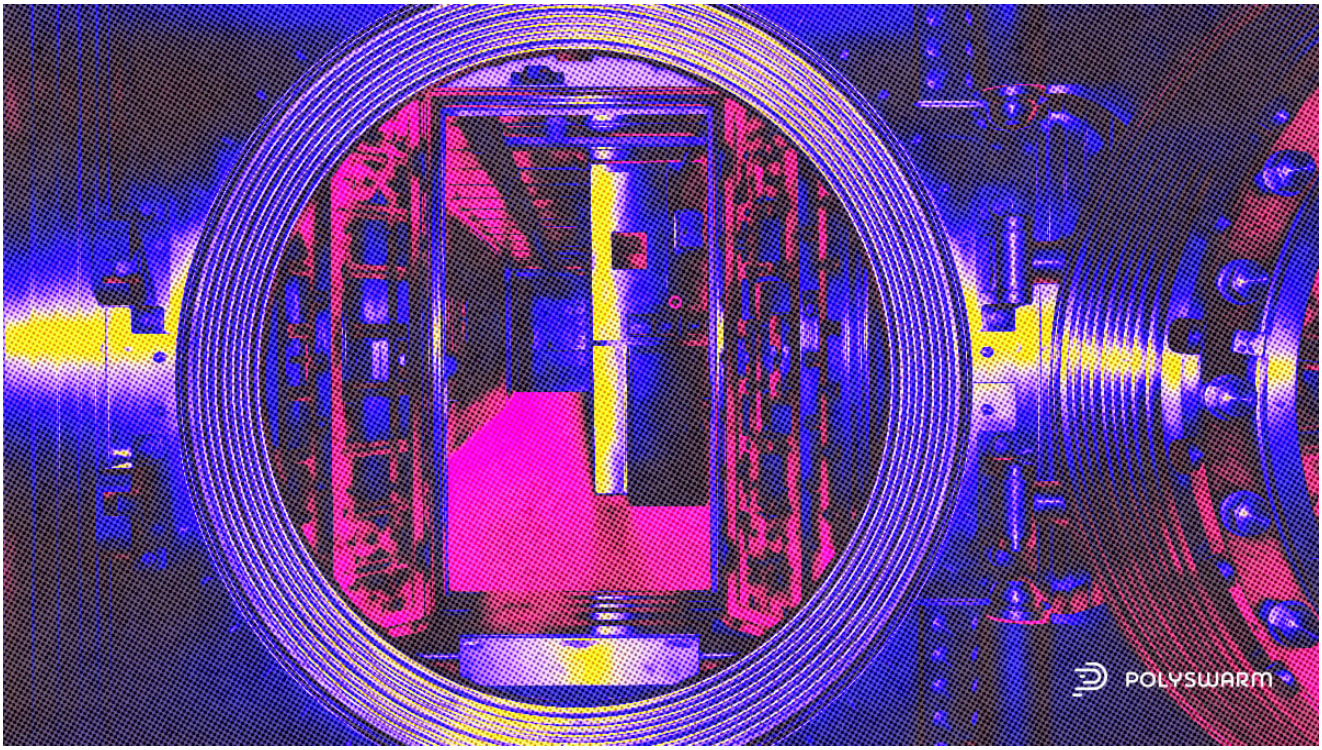
# Phishing and Android Malware Campaign Targets Indian Banks

blog.polyswarm.io/phishing-and-android-malware-campaign-targets-indian-banks




**Related Families:** Elibomi, FakeReward, AxBanker, IcRAT, IcSpy
**Verticals Targeted:**

Financial

### Executive Summary

Trend Micro recently reported on a phishing and Android malware campaign targeting clients of multiple banks in India. The campaign leverages multiple malware families, including Elibomi, FakeReward, AxBanker, IcRAT, and IcSpy.

### Key Takeaway

- A large-scale phishing campaign targeted customers of multiple Indian banks.
- The malware used in the campaign included Elibomi, FakeReward, AxBanker, IcRAT, and IcSpy.
- While the other malware families have been in the wild for some time, FakeReward and AxBanker are novel malware families.

## The Campaign

A large-scale phishing and Android malware campaign was recently observed targeting customers of seven financial institutions in India. One of the known attack vectors was an SMS message containing either a phishing link or a link to a malicious app download. Threat actors abused the logos, names, and affiliated brands and services of legitimate banks to create an elaborate phishing scheme.

## The Malware

The campaign leveraged at least five banking trojan malware families, including Elibomi, FakeReward, AxBanker, IcRAT, and IcSpy. While IcRAT, IcSpy, and Elibomi were previously active in the wild, FakeReward and AxBanker are newly discovered malware families.

### Elibomi

Elibomi is an Android malware that has been active in the wild since at least 2020. It is used to steal PII and credit card information. In early 2022, Trend Micro researchers observed it being used in a phishing campaign targeting Indian banks. The new variant used in this campaign had a package name ending in iApp. Threat actors added functionality, including automated clicking, permission granting, and screenshot captures. Another Elibomi variant had a package name ending in iAssist. This variant used Firebase for C2 and used RDVerify to evade detection. It affects Android 12 and lower.

### IcRAT

IcRAT is an Android banking malware. It was used to target customers of a particular bank at nearly the same time FakeReward was used to target the same bank. Trend Micro researchers also noticed an overlap of the phishing websites used by both malware families.

### IcSpy

IcSpy requests SMS permissions and enables a debug option to allow the threat actors to access application data and run arbitrary code on affected Android versions. IcSpy uploads SMS messages to the C2.

### FakeReward

FakeReward is an Android banking Trojan that requests SMS permissions upon launch. FakeReward collects all text messages sent to the device and sends them to the C2. It also sets up monitoring to listen to incoming SMS messages. Updated versions of FakeReward request notification permission to extract text messages. Multiple FakeReward variants were used in this campaign.

### AxBanker

AxBanker is a banking Trojan targeting Indian banking customers since at least August 2022. The phishing website associated with this malware entices customers with a reward points system to convince them to download the app. AxBanker also requests SMS permissions and uses phishing pages to collect the victim's personal data and credit card information.

### IOCs

PolySwarm has multiple samples associated with this campaign.

### Elibomi IOCs

12b47e5b7f6cc7371c7a243ae0d58cf7b7391e0a471a4365d03b7db9e45a5dd8
40b469c6e7176101abb3d114c689fe0b3cc244292bcbc0658174337596caf1a9

a389911dcba6afa54a1977657a17292ec1a8e3f49ee3726600725f4200ca7960

You can use the following CLI command to search for all Elibomi samples in our portal:

**$ polyswarm link list -f Elibomi**

### IcRAT IOCs

8325398d82c110e9219cfbd963c915b7753f108ddd109ceefc47e8c7ef978fe9

You can use the following CLI command to search for all IcRAT samples in our portal:

**$ polyswarm link list -f IcRAT**

**IcSpy IOCs**

F050abd03d3a58bb4f5b85cd831ccd176f3fa46d12deee35c541f6af3e491a34

You can use the following CLI command to search for all IcSpy samples in our portal:

**$ polyswarm link list -f IcSpy**

**FakeReward IOCs**

2da210623178f90801e53394db43809bd23674063c53bf341ef5d94ebde61131

b28b792b6a093481722dde813de98d163de325bbcc84c70a568499367d9a9418

237f30949ebf7c67a58a7a38c2464db28b722cd1f0f7aae45c469bd9db8b22c8

You can use the following CLI command to search for all FakeReward samples in our portal:

**$ polyswarm link list -f FakeReward**

**AxBanker IOCs**

34cdc6ef199b4c50ee80eb0efce13a63a9a0e6bee9c23610456e913bf78272a8

66c572dd6b68a1abc48241f6d7308fbc42b18470e1d8989190f515a6f621f0a1

You can use the following CLI command to search for all AxBanker samples in our portal:

**$ polyswarm link list -f AxBanker**

***Don’t have a PolySwarm account? Go here to sign up for a free Community plan or to subscribe.***

***Contact us at hivemind@polyswarm.io | Check out our blog | Subscribe to our reports***

Topics: Threat Bulletin, Financial, India, Android, Phishing, Elibomi, FakeReward, AxBanker, IcRA, IcSpy

**Written by PolySwarm Tech Team**

---