

2023

# Mobile Banking Heists Report

29 Malware Families Targeting 1,800 Mobile  
Banking Apps



# Index

---

<b>Introduction</b>	<b>2</b>
<b>Executive Summary</b>	<b>3</b>
New Banking Malware Families	3
New Capabilities in Emerging Banking Malware Families	4
Key Observations from Zimperium's Research	5
Malware is Evolving; Our Defenses Need to Advance	6
<b>Banking Trojans</b>	<b>6</b>
What Is a Banking Trojan?	6
What's the Story Behind the Name?	7
What Is a Banking Malware Family?	7
What Makes Trojans So Successful?	7
<b>Key Research Highlights</b>	<b>9</b>
Research Summary	9
How Last Year's Malware Evolved	10
Top Banking Malware Families	11
Countries Targeted In Each Region	12
Top Targeted Banking Organizations By App Download	13
Top Targeted Mobile Banking Apps By Malware Family	14
<b>New Malware Capabilities: Insights From Zimperium's Research</b>	<b>15</b>
MaaS (Malware-as-a-Service)	15
Automated Transfer System (ATS) Technique	16
TOAD (Telephone-Oriented Attack Delivery)	18
Screen Sharing Abuse	20
Media Reports Highlighting Successful Heists	22
<b>The Broader Economic Impact</b>	<b>24</b>
Impact on Financial Organizations	24
Impact on Consumers	24
<b>Best Practices: Protecting Apps from Malware</b>	<b>25</b>
<b>How Zimperium Can Help</b>	<b>26</b>
<b>How Consumers Can Better Protect Themselves</b>	<b>28</b>
<b>Conclusion: Adaptive Security Amid Evolving Threats</b>	<b>31</b>
<b>About Zimperium</b>	<b>32</b>
<b>Affiliations</b>	<b>33</b>
<b>Appendix</b>	<b>33</b>
GitHub Malware Samples	33
<b>References</b>	<b>33</b>
<b>Credits</b>	<b>34</b>

# Introduction

The mobile banking market is on a rapid ascent, **projected to hit the \$7 billion mark by 2032<sup>1</sup>**, fueled by consumer demands for seamless and personalized banking experiences. As indicated below, mobile banking is outpacing online banking across all age groups due to its convenience and our desire to have those apps at our fingertips.



Age group	% who primarily use online banking	% who primarily use mobile banking
15-24	6.3%	74.1%
25-34	12.9%	69.4%
35-44	18.4%	60.5%
45-54	22.8%	49.1%
55-64	27.3%	33.2%
65+	28.2%	15.3%

Fig: Mobile Banking Adoption Soars (Source)

However, this surge is accompanied by a dramatic growth in financial fraud. According to LexisNexis' 2022 True Cost of Fraud Study, in the US, mobile fraud accounted for 32% and 37% of all fraud, respectively, an increase of 5% and 12%. The UK witnessed a 17% rise in the last year alone and a 25% increase in fraud victims over two years.

Yet, amid these figures, a critical statistic stands out: **one in every 20 fraud attacks can be traced back to a rogue mobile application**, underscoring a pivotal front in the battle against financial fraud and emphasizing the acute need for stringent mobile app security measures.

The threat landscape, as detailed by Zimperium's threat intelligence, demonstrates the pressing nature of these risks. Zimperium's monitoring of millions of Android devices has unveiled that about 9% have been affected by malware, with banking trojans infecting a fifth of these devices, spanning 187 countries with over 24,000 unique samples identified. Such alarming statistics serve as a clarion call for an escalated defense, especially as mobile banking trojans have become a preferred tool for digital fraud, accounting for 16% of all such activities in the US.

This year, the Verizon Data Breach Investigations Report (DBIR) stated that 94% of breaches remain financially driven, making mobile banking a prime target for nefarious actors wielding sophisticated banking trojans. It further illuminates the situation, identifying stolen credentials, phishing, and vulnerability exploitation as the foremost tactics used by attackers—tactics at which banking malware excels.

In an era where mobile is the digital channel of choice for banking, understanding the anatomy, impact, and trends of mobile banking malware is essential to building secure mobile banking apps that garner customer trust and thrive in a hyper-competitive environment. This report aims to arm mobile security and product leaders with the knowledge to develop mobile app security strategies that align with the sophistication of today's malware. It is an essential read for those at the forefront of combating threats on the mobile platform.

## Reflections on 2022 Research

It's clear from [last year's report](#) that mobile banking trojans employed a multi-faceted approach to exploit vulnerabilities and evade detection. Zimperium found that 1400 mobile apps across 800 brands were targeted by 19 banking malware families.

Within the malware analyzed, Zimperium researchers observed the following key capabilities:

- **Distribution:** Via app stores and deceptive SMS
- **Exploitation:** Abuses accessibility services for credential access and keylogging
- **Command-and-Control:** For data exfiltration and remote control
- **Evasion:** Disables anti-malware and blocks uninstall attempts

## This Year's Objectives

This year Zimperium's research takes a deeper dive into malware within these banking trojans targeting Mobile Banking and FinServ/Trading mobile apps. Zimperium's Advanced Research and Exploitation team (zLabs) investigated several malware samples to understand their evolution, geographical dispersion, attack vectors, and capabilities.

Key questions the zLabs team addressed in this report include:











1. **What's Changed:** Malware evolution and concerning trends
2. **New Capabilities:** Which new capabilities are being integrated?
3. **Real-World Impact:** What is the impact on businesses and consumers?
4. **Guidelines:** What are some good practices to follow?
5. **How to Stay Ahead:** How can Zimperium help?

# Executive Summary

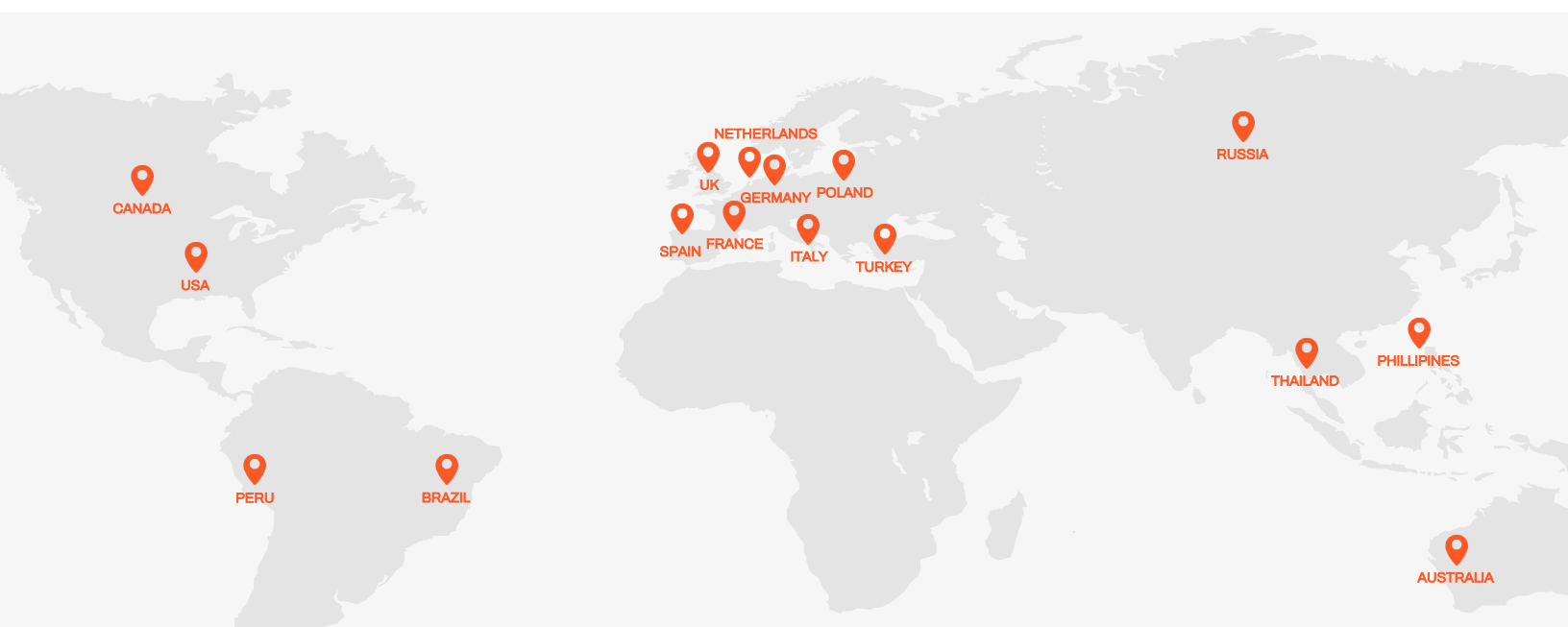
Zimperium's latest research explores a dynamic and expanding threat landscape by meticulously analyzing **29** banking malware families and associated trojan applications. This year alone, the research team identified **10** new active families, signifying the **continued investment** from threat actors in targeting mobile banking applications. The 19 adversaries who persist from last year reveal new capabilities that show a **relentless pursuit of financial exploitation**. Traditional banking applications remain the prime target, with a staggering 1103 apps—accounting for 61% of the targets—while the emerging FinTech and Trading apps are now in the crosshairs, making up the remaining 39%. It is undeniable that these sophisticated banking trojan threats have a global impact, with 61 countries grappling with them.

## New Banking Malware Families

Listed below are the ten new banking malware families Zimperium reviewed and some key characteristics.

Nexus	Godfather	Pixpirate	Saderat	Hook	PixBankBot	Xenomorph v3	Vultur	BrasDex	GoatRat
									
<b>498</b> Known Variants	<b>1,171</b> Known Variants	<b>123</b> Known Variants	<b>300</b> Known Variants	<b>14</b> Known Variants	<b>4</b> Known Variants	<b>6</b> Known Variants	<b>9</b> Known Variants	<b>1</b> Known Variants	<b>52</b> Known Variants
<b>39</b> Banking Apps Targeted	<b>237</b> Banking Apps Targeted	<b>10</b> Banking Apps Targeted	<b>8</b> Banking Apps Targeted	<b>468</b> Banking Apps Targeted	<b>4</b> Banking Apps Targeted	<b>83</b> Banking Apps Targeted	<b>122</b> Banking Apps Targeted	<b>8</b> Banking Apps Targeted	<b>6</b> Banking Apps Targeted
<b>9</b> Countries Targeted	<b>57</b> Countries Targeted	<b>1</b> Countries Targeted	<b>23</b> Countries Targeted	<b>43</b> Countries Targeted	<b>1</b> Countries Targeted	<b>14</b> Countries Targeted	<b>15</b> Countries Targeted	<b>1</b> Countries Targeted	<b>1</b> Countries Targeted
Offered as MaaS	Offered as MaaS	Not offered as MaaS	Not offered as MaaS	Offered as MaaS	Not offered as MaaS	Offered as MaaS	Not offered as MaaS	Not offered as MaaS	Not offered as MaaS
Stolen Data Exfiltrated to: USA Netherlands Turkey Spain	Stolen Data Exfiltrated to: USA Turkey Spain Canada France Germany UK Italy Poland	Stolen Data Exfiltrated to: Brazil	Stolen Data Exfiltrated to: Thailand Philippines Peru	Stolen Data Exfiltrated to: Russia	Stolen Data Exfiltrated to: Brazil	Stolen Data Exfiltrated to: USA	Stolen Data Exfiltrated to: USA	Stolen Data Exfiltrated to: Australia Poland	Stolen Data Exfiltrated to: Brazil

\*Zimperium customers using Zimperium Mobile Threat Defense and Zimperium Runtime SDK zDefend solutions are protected from these threats.





# New Capabilities in Emerging Banking Malware Families

Of the 29 banking malware families analyzed this year, several had new capabilities focussed on evading security, avoiding detection, and effortlessly stealing banking credentials and frictionless mobile banking fraud. Below are four notable capabilities that best represent their growing sophistication:



## Automated Transfer System (ATS Module)

This framework allows cybercriminals to automate fraud by extracting credentials and account balances, initiating unauthorized transactions, obtaining Multi-Factor Authentication (MFA) tokens, and authorizing fund transfers.



## Telephone-Based Attack Delivery (TOAD)

TOAD attacks involve cybercriminals posing as call center representatives and sweet-talking targets into downloading “security” software that **is actually a banking trojan**.



## Screen Sharing

The screen-sharing capability enables threat actors to remotely interact with and manipulate a device, **even without physical access**. This capability was developed to help product vendors provide remote customer support. However, threat actors are now repurposing it for malicious purposes.



## Malware-as-a-Service (MaaS)

MaaS platforms offer a range of features optimized for malware authors, including pre-coded attack vectors, customizable trojan templates, and evasion techniques like code obfuscation. These services allow for quick adaptations, making it easier for malware authors to circumvent new security protocols, sustaining the malware's effectiveness over time. Subscriptions to these platforms range from 3,000 - 7,000 USD per month, depending on the services offered.



# Key Observations from Zimperium's Research

## Looking Back

### Traditional Mobile App Security Measures Undermined

More than **50%** of the malware families researched already have advanced keylogging, screen overlay, accessibility, and SMS-stealing capabilities. The traditional security mechanisms employed by traditional mobile banking apps—such as Strong Passwords, Domain-Based Security, One-Time-Passwords (OTP), and Multi-Factor Authentication (MFA)—are increasingly being undermined on end-user mobile devices by banking malware.

### Malware Variants Outpace Signature-Based Security

Zimperium found over **2,100 variants** associated with just the ten new banking malware families researched. A combination of open-source malware and Malware-as-a-Service offerings has led to a proliferation of new variants. “Saderat,” a malware about which Zimperium recently reported, has over 28 malicious app variants that aren't fully detected by the industry. Security approaches that solely rely on signatures or require a new app version to be released when a new threat is discovered are not viable.

### App Security Standards Ignored, Making Trojans Easy

Most legitimate apps don't have a great degree of compliance with the Open Web Application Security Project (OWASP) Mobile Application Security Verification Standard (MASVS) standards. Apps lack adequate protection from reverse engineering and tampering as these security standards recommend, allowing threat actors to reverse them quickly, create clones with banking malware, and distribute them via social engineering.

## Looking Forward

### Regulatory Requirements Evolve and Become Prescriptive

Globally, mobile banking security regulatory frameworks are undergoing significant changes. New regional regulations will mirror those in countries like [Singapore](#), [India](#), and [Malaysia](#), where security requirements are prescriptive and **will mandate protections** such as code protection, cryptographic key protection, anti-malware, and other safeguards. As banking malware continues to increase globally, the zLabs team expects this regulatory trend to accelerate.

### Banking Apps are Just the Beginning

**50%** of the malware families analyzed already target Payment, NeoBanks, and Crypto wallets. Zimperium researcher expect more apps in these categories to be targeted in the future. In addition, **17%** of families have already begun using entertainment apps, government websites, messaging services, and social media sites.

### Ransomware Capabilities on the Rise

Last year's research showed that Anubis, LokiBot, and MysteryBot already profit from encrypting user data, which is the first step to becoming ransomware. In this year's research, Nexus is integrating ransomware capabilities as part of its Malware-as-a-Service offering. The Verizon DBIR reported this year that ransomware is present in **59%** of all incidents with a Financial motivation. Consumers should expect to see more ransomware capabilities within mobile banking malware, with the potential to disrupt customer access to banking services.

# Malware is Evolving; Our Defenses Need to Advance

Using advanced tactics, modern banking malware has outpaced and undermined traditional mobile app security measures. Today, mobile app security solutions must enable the following capabilities within mobile banking applications to keep up with today's evolving threat landscape:

- **Threat Visibility:** Provide real-time visibility into real-world threats across the install base
- **Zero-Day Defense:** Defend against known and zero-day threats detected on the device
- **On-device Mitigation:** Empower apps to respond immediately on-device to mitigate risk
- **Adaptive Security:** Receive real-time updates to threat detections and response without having to republish a new app

Zimperium stands at the forefront of mobile app security, offering businesses the expertise and advanced solutions needed to achieve a comprehensive, mobile-first security posture.

## Banking Trojans

### What Is a Banking Trojan?

Bank trojans are **seemingly legitimate apps** that contain **malicious software** (malware) that exploits banking apps installed on end-user mobile devices. It is designed to steal banking credentials, financial information, and personally identifiable information (PII) or facilitate unauthorized payment transactions.





## What's the Story Behind the Name?

A trojan is an app that appears legitimate but contains malicious code or malware. They take their name from the legendary Trojan War. Unable to breach the mighty walls of the city of Troy after ten long years of conflict, the Greeks devised a plan to trick Troy into breaching the walls for them. Much like a modern social engineering attack, the Greeks spread false information that they had given up and left, leaving outside the city walls a large wooden horse as an offering to the goddess of war, Athena, so that she would grant them safe passage home. The Trojans, seeing the horse as a sign of their victory, brought it inside the previously impenetrable city walls—unknowingly opening themselves up to attack.

## What Is a Banking Malware Family?

A banking malware family refers to a **group of related malicious software** variants designed specifically to target banking applications and steal financial information. These families are categorized based on their common codebase, behavioral traits, and attack methodologies. Each family may include multiple strains or versions of malware that have evolved over time to bypass security measures and exploit vulnerabilities in banking systems.

## What Makes Trojans so Successful?

### Phishing Vulnerability: The Risks of Falling Prey

Phishing often serves as a vector for trojan distribution by deceiving users into downloading malicious apps or clicking on compromised links that lead to trojan installations. The success in this case is largely attributed to users' susceptibility to phishing campaigns on mobile. They evolve quickly and bypass traditional static protection measures. Threat actors today use QR codes, SMS, Facebook Messenger, Twitter, or even secure messaging apps like Signal and WhatsApp to impersonate trusted brands and deliver phishing URLs. Phishing attempts are difficult to identify when mobile, social, and brand impersonation are combined.

Based on [Global Mobile Threat Report](#) data from Zimperium, as well as the Anti-Phishing Working Group (APWG), **financial services is the most targeted sector, accounting for 23% of documented phishing attacks. Financial services firms have been targeted 60% more than the next most targeted sector, Social Media.**

### Preconditioned Trust: The Bias in App Permissions

There are many trojan applications masquerading as legitimate applications in popular categories, such as those listed below.



Tools

Productivity

Entertainment

Photography

Gaming

Education

## What Makes These App Categories So Appealing?

- **Broad Appeal:** Malware can reach a very broad audience through categories like Entertainment, Productivity, and Education.
- **Extensive Permissions:** These apps often require extensive device, network, notification, camera, and accessibility permissions, allowing malware to install invasive features.
- **Trust Exploitation:** Education is generally considered safe, which makes it more likely that users will drop their guard and install trojan apps, even if the apps are new.

## Longevity: Trojans Persist on Devices

Trojans persist because they are built by copying legitimate features or apps. Trojans mimic trusted apps' advertised functions and stay on devices for a long time, undermining user skepticism. Threat actors can easily reverse-engineer legitimate apps, making this possible. In most cases, apps do not have anti-reversing or anti-tampering protections, especially those that are able to withstand today's advanced attacker techniques. A threat actor can create a near-identical clone of a legitimate app by analyzing its architecture and functionality and then proceeding to embed malicious features. This makes it extremely difficult for end users to suspect or remove these functional trojans because they're conditioned to judge apps by their performance.

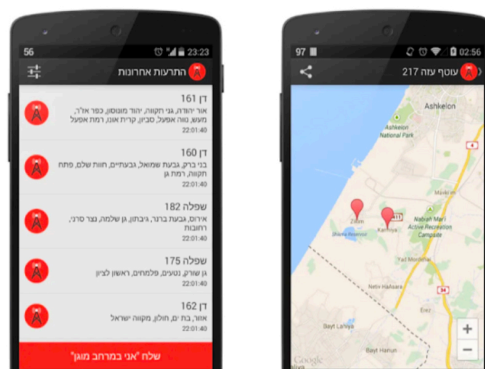
## Real-World Example of Legitimate App Abuse

Below is a recent example of app abuse. Attackers were spoofing a widely used open-source application that warns Israelis of incoming airstrikes, called RedAlert, to lure users into downloading a malicious version of the software that, instead of telling those under attack where to seek safety, collects their sensitive data.



### The fastest, most reliable rocket alert application

Over 450,000 downloads and a 4.7 star rating to prove it. The only rocket alert application with dedicated notification servers that drastically improve alert speed and reliability.





# Key Research Highlights

In the following section, the zLabs Advanced Research and Exploitation team presents a series of tables that distill the key findings from their extensive research. These tables have been curated to provide you with a clear and concise snapshot of the critical data and trends unearthed during their study.

## Research Summary



# Malware Families  
Researched

**29**



# Traditional Banking  
Apps Targeted

**1,103 (61%)**



# Evolved Malware  
Families from 2022

**19**



# FinTech/Trading  
Apps Targeted

**704 (39%)**



# New Malware  
Families in 2023

**10**



# Countries  
Impacted

**61**

# How Last Year's Malware Evolved

	In 2022	In 2023
<b>Novel Capabilities</b>	Spam Contacts Abuse Accessibility Services Intercept MFA tokens Screen Overlay Attacks Real Time Screen Sharing Disable Anti-Malware Apps Hide Trojan App Icons	Intercept Notifications Bypass One-Time Passwords Make Code Open Source Automatic Transfer System (ATS) Detect & Evade Emulators Domain Generation Algorithms(DGA)
<b>Predominant Targets</b>	Banking Payments	Banking Payments Cryptocurrency Social Media Messaging

Research conducted by the zLabs team clearly shows that the malware Zimperium highlighted in the 2022 Mobile Banking Heist report has evolved considerably in the last twelve months. Despite the high infection levels already achieved, malware authors are constantly adding new features. Let's take a look at how these new capabilities undermine traditional security measures.

1. **Intercepting Notifications:** Undermines secure notification systems, requiring secure channels for alerts.
2. **Bypassing One-Time Passwords:** Weakens the effectiveness of Multi-Factor Authentication (MFA).
3. **Making Code Open Source:** Accelerates malware evolution, making signature-based anti-malware solutions less effective.
4. **Leveraging Automated Transfer System (ATS):** The ability to perform unauthorized transactions with little to no user interaction.
5. **Detecting & Evading Emulators:** Challenges automated malware analysis systems and basic mobile security Software Development Kits (SDKs), requiring more advanced threat detection capabilities.
6. **Using Domain Generation Algorithms (DGA):** Makes denylisting domains ineffective, requiring advanced Domain Name System (DNS) filtering solutions.

# Top Banking Malware Families

Below are the top 10 malware families based on the number of banks targeted out of the 29 analyzed by the zLabs team this year.



**618**  
Banks Targeted

Hook



**105**  
Banks Targeted

Mysterybot



**419**  
Banks Targeted

Godfather



**76**  
Banks Targeted

Medusa



**414**  
Banks Targeted

Teabot



**53**  
Banks Targeted

Cabossous



**400**  
Banks Targeted

Xenomorph



**41**  
Banks Targeted

Anubis



**371**  
Banks Targeted

Exobot



**40**  
Banks Targeted

Coper



# Countries Targeted In Each Region

Listed below are the top countries targeted by the 29 malware families the zLabs team analyzed this year.

## AMERICAS



**United States**

109 Banks Targeted



**Canada**

17 Banks Targeted



**Brazil**

11 Banks Targeted

## EUROPE



**United Kingdom**

48 Banks Targeted



**Italy**

44 Banks Targeted



**France**

30 Banks Targeted



**Spain**

29 Banks Targeted



**Portugal**

27 Banks Targeted



**Germany**

23 Banks Targeted

## MIDDLE EAST



**Turkey**

32 Banks Targeted



**United Arab Emirates**

12 Banks Targeted



**Saudi Arabia**

8 Banks Targeted

## ASIA-PACIFIC



**Australia**

34 Banks Targeted



**New Zealand**

8 Banks Targeted



**ASEAN**

30 Banks Targeted



**Japan**

5 Banks Targeted

# Top Targeted Banking Organizations By App Download

The following is a list of some of the top banking organizations targeted by this year's malware families.



PhonePe

Country	# Downloads
India	100,000,000



Barclays

Country	# Downloads
United Kingdom	11,000,000



WeChat International Pte. Ltd.

Country	# Downloads
United States	100,000,000



Wells Fargo

Country	# Downloads
United States	10,500,000



Binance Inc.

Country	# Downloads
Malta	50,000,000



QNB Finansbank A.S.

Country	# Downloads
Turkey	11,100,000



Bank of America

Country	# Downloads
United States	11,200,000



CaixaBank

Country	# Downloads
Spain	11,000,000

\* Approximate Number of Downloads: This value indicates the total downloads of the legitimate Android mobile banking app from app stores.



# Top Targeted Mobile Banking Apps by Malware Family

The following are some of the top mobile banking applications that were targeted by the malware families Zimperium analyzed this year.



Caixa

16

Malware Families Targeting the App



EVO Banco móvil

12

Malware Families Targeting the App



Intesa Sanpaolo Mobile

13

Malware Families Targeting the App



Kutxabank

12

Malware Families Targeting the App



Bankinter Mobile

13

Malware Families Targeting the App



Bank of America

11

Malware Families Targeting the App



YouApp Banco BPM Mobile

12

Malware Families Targeting the App



Wells Fargo

11

Malware Families Targeting the App



Capital One Mobile

12

Malware Families Targeting the App

# New Malware Capabilities: Insights from Zimperium's Research

Zimperium's research into 29 banking malware families and their samples yielded valuable insights into new targets and capabilities. Among the findings, zLabs researchers identified four new capabilities that are not only significant on their own but also crucial when considering how the malware families are using them to achieve their fraud objectives. Based on Zimperium's analysis of malware samples, this section provides insight into how they operate.



## MaaS (Malware-as-a-Service)

### What is MaaS?

In recent years Zimperium researchers have seen some cybercriminals establish themselves as legitimate companies offering services to clients. The result was Malware-as-a-Service, where one-time purchases, subscriptions, and profit-sharing options were available. Consequently, new cybercriminals have had a much easier time entering the market. It enables easy deployment of advanced attacks on mobile banking applications and transactions by providing individuals with ready-made malicious toolkits for rent or subscription.



### How Nexus Uses MaaS for Fraud

[Nexus](#) is one of the banking malware families that is distributed under this progressive model. Zimperium has observed the following about this capability.

#### Distribution

Nexus makes itself available as MaaS by advertising its offerings on various hacking forums. Interested parties can subscribe or rent its services for a specific period of time, much like purchasing a software subscription. Its MaaS model democratizes access to its advanced capabilities, allowing even those with limited technical expertise to launch sophisticated cyber-attacks.

1



#### C2 Communication

Nexus possesses an autonomous updating mechanism. It communicates with its command-and-control (C2) server to check for updates on-demand, allowing it to adapt and evolve in real-time to match the banking app version currently installed on the device. This makes Nexus significantly more resilient to detection and countermeasures, sustaining its effectiveness over longer periods.

3



2

#### Account Takeover

One of Nexus' core capabilities is facilitating account takeover attacks. It leverages overlay attacks and keylogging to capture user credentials, in addition to stealing SMS messages to bypass two-factor authentication (2FA). It exploits Android's Accessibility Services to glean information from cryptocurrency wallets and disable 2FA modules. This makes Nexus not just a banking trojan but a multi-faceted tool that can target multiple types of secure accounts.



4

#### Control

A command-and-control server enables subscribers to access Nexus' functionalities via payment and access credentials. Using this MaaS setup, malware can be distributed and used more easily, increasing its impact and reach.





## Automated Transfer System (ATS) Technique

### What is ATS?

In this context, the ATS is not to be confused with the bank's Automated Transfer Service (ATS). The ATS technique is used by malware to transfer unauthorized funds from a victim's account without raising suspicions.

### How it works

The following is an explanation of how ATS works.

#### 1 Credential Harvesting

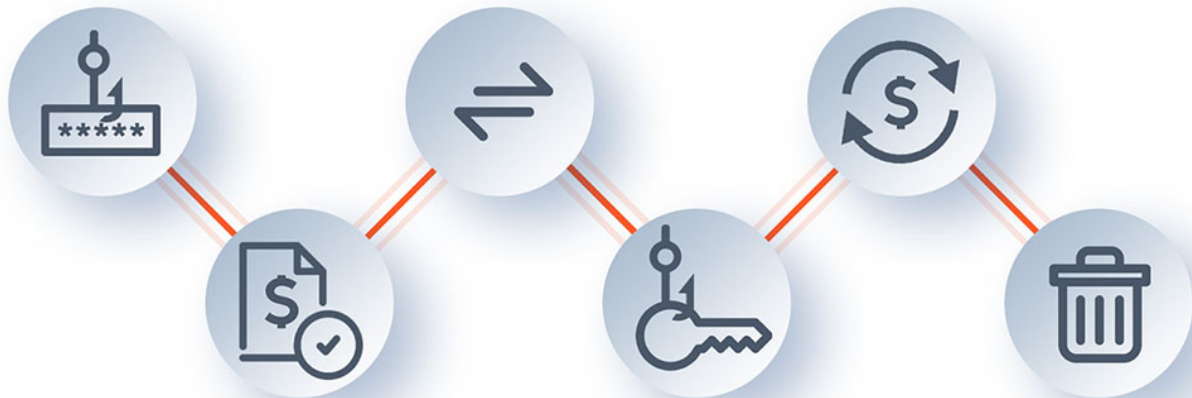
After successful infiltration, the ATS module remains idle, monitoring user activity in banking apps. When the user logs into a banking app, it captures login credentials, account numbers, and other sensitive information.

#### 3 Transaction Initiation

ATS either waits for the user to start a transaction before modifying recipient details or starts a transaction automatically. It locates User Interface (UI) components such as text fields for entering transfer amounts and account details and even buttons for initiating transactions, interacting with them as if they were real users.

#### 5 Transaction Execution

With all the necessary information, the ATS will finalize the transaction, sending funds to a predetermined account controlled by the attackers.



#### 2 Account Balance Checks

The ATS module automatically queries account balances to decide how much money to transfer without raising suspicion.

#### 4 MFA Token Capture

When a legitimate transaction is hijacked, the user will enter MFA to authorize the transaction. If an unauthorized transaction is initiated, an ATS module will trick the user into entering an OTP, or one time password, often by using a pop-up claiming session expiration and a OTP is needed.

#### 6 Evasion and Cleanup

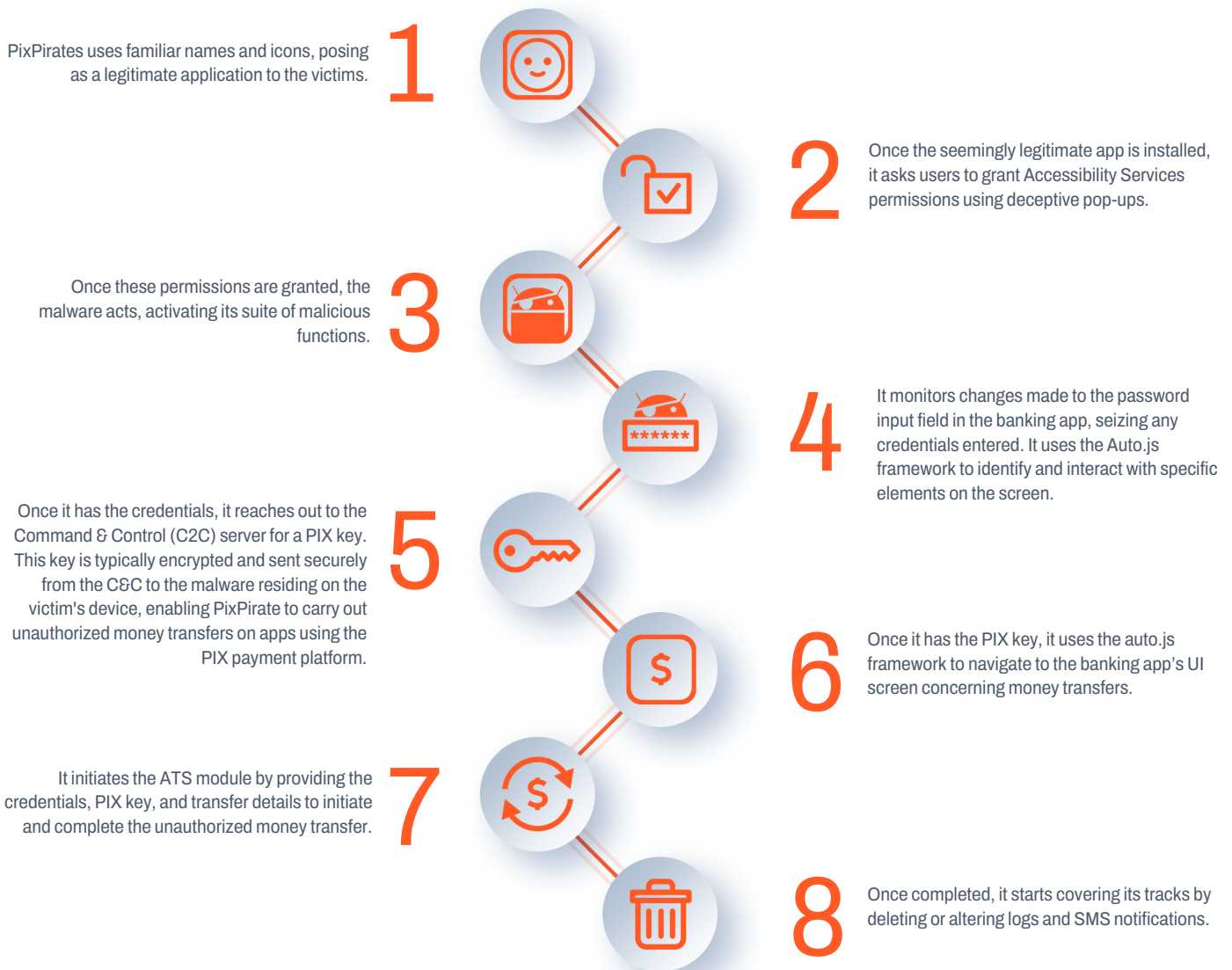
Finally, the ATS may delete transaction-related SMS alerts or app notifications, making it harder for the victim to detect the fraud immediately.



## How PixPirate Leverages ATS for Fraud

At the beginning of 2023, researchers at Cleafy documented a new Android banking malware called [PixPirate](#). This malware belongs to the newest generation that is capable of making unauthorized money transfers via mobile banking apps using the Instant Payment platform Pix.

Here's how zLabs researchers observed this ATS capability being used by PixPirate.



### Examples of Other Banking Trojans Using ATS Techniques:



GoatRat



PixBankBot



Xenomorph



# TOAD (Telephone-Oriented Attack Delivery)

## What is TOAD?

TOAD is a social engineering attack that involves tricking users into engaging in a phone conversation with an attacker (usually posing as a support agent). Afterward, the “support agent” takes the victim through a series of steps to download and install malware on the mobile device, which is capable of performing unauthorized fund transfers, data theft, or other forms of financial fraud.

## How it works

The following is an explanation of how TOAD works.

### 1 Phishing Stage

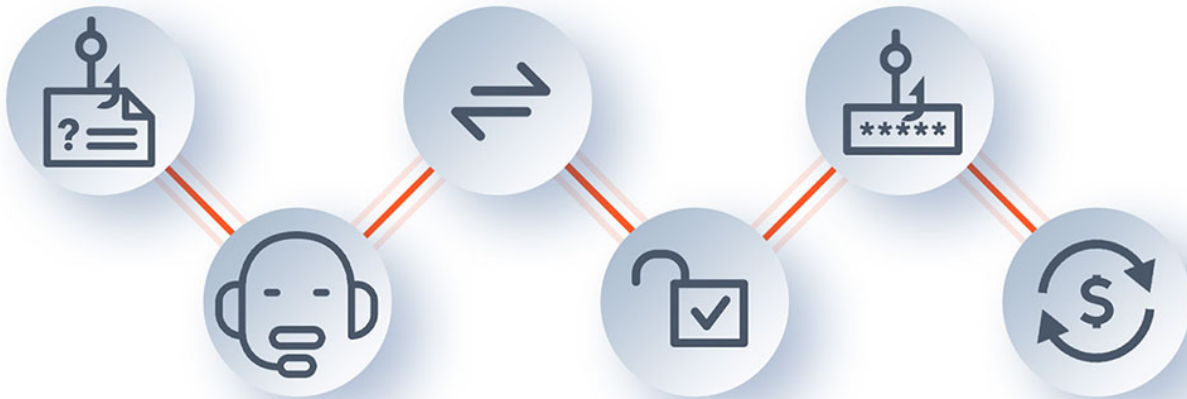
A victim is lured into inputting sensitive details into a phishing overlay screen disguised as a legitimate page, most often mimicking a banking application. In addition to the credentials, the screen asks the users to set up security questions and responses during account registration.

### 3 Malware Deployment

This seemingly benign software is the malware, often a trojan, designed to compromise the mobile device. It may even be a legitimate remote-access tool repurposed for malicious intent.

### 5 Data Harvesting

With elevated permissions, the malware can then access sensitive data like passwords, bank account details, and even MFA tokens, storing them or sending them to a remote server.



### 2 Attacker Calls the Victim

The cybercriminal then places a call to the victim, typically posing as a customer support agent. The cyber criminal persuades the victim to download what they describe as "essential" or "mandatory" software updates. But this app is essentially the trojan.

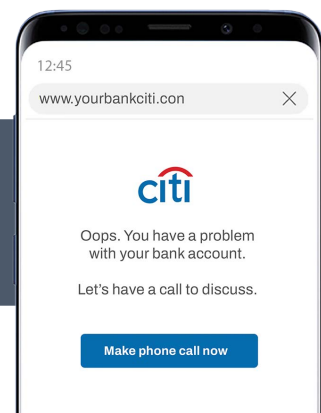
### 4 Elevated Privileges

Once installed, the malware may prompt the user to grant it elevated permissions, sometimes using other social engineering techniques over the phone to achieve this.

### 6 Remote Control

The fraudsters may now remotely operate the device to perform activities like unauthorized fund transfers, data theft, or other forms of financial fraud.

Alternatively, the attacker can trick the victim into calling them by setting up a deceptive website showing that the victim has some problem with their bank account or some other service.







## How Copybara Uses TOAD for Fraud

The emergence of [Copybara](#), a malware using a framework akin to BRATA, marks a shift towards hybrid fraud attacks that combine traditional phishing with telephone-oriented attack delivery (TOAD). Specifically targeting Italian banks, Copybara leverages Vishing (voice phishing) to complete its attack chain and acquire victim data.

Here's how zLabs researchers observed this capability being used by Copybara.



This vishing-aided multi-step process is quite novel because it leverages human trust via voice interaction, often bypassing suspicions that would typically arise from a text-based phishing attempt.



## Screen Sharing Abuse

### What is Screen Sharing?

Screen Sharing is a feature that allows for remote screen sharing and control of a device. In mobile banking trojans, the malware can remotely access and manipulate a user's device, including their banking app, to carry out unauthorized transactions or steal information. Screen Sharing is not a malicious capability per se; it's a tool with legitimate uses, and is sometimes used by application developers to support users having issues within the app. However, mobile banking trojans are using it for malicious purposes.

### How it works

The following is an explanation of how Screen Sharing works:

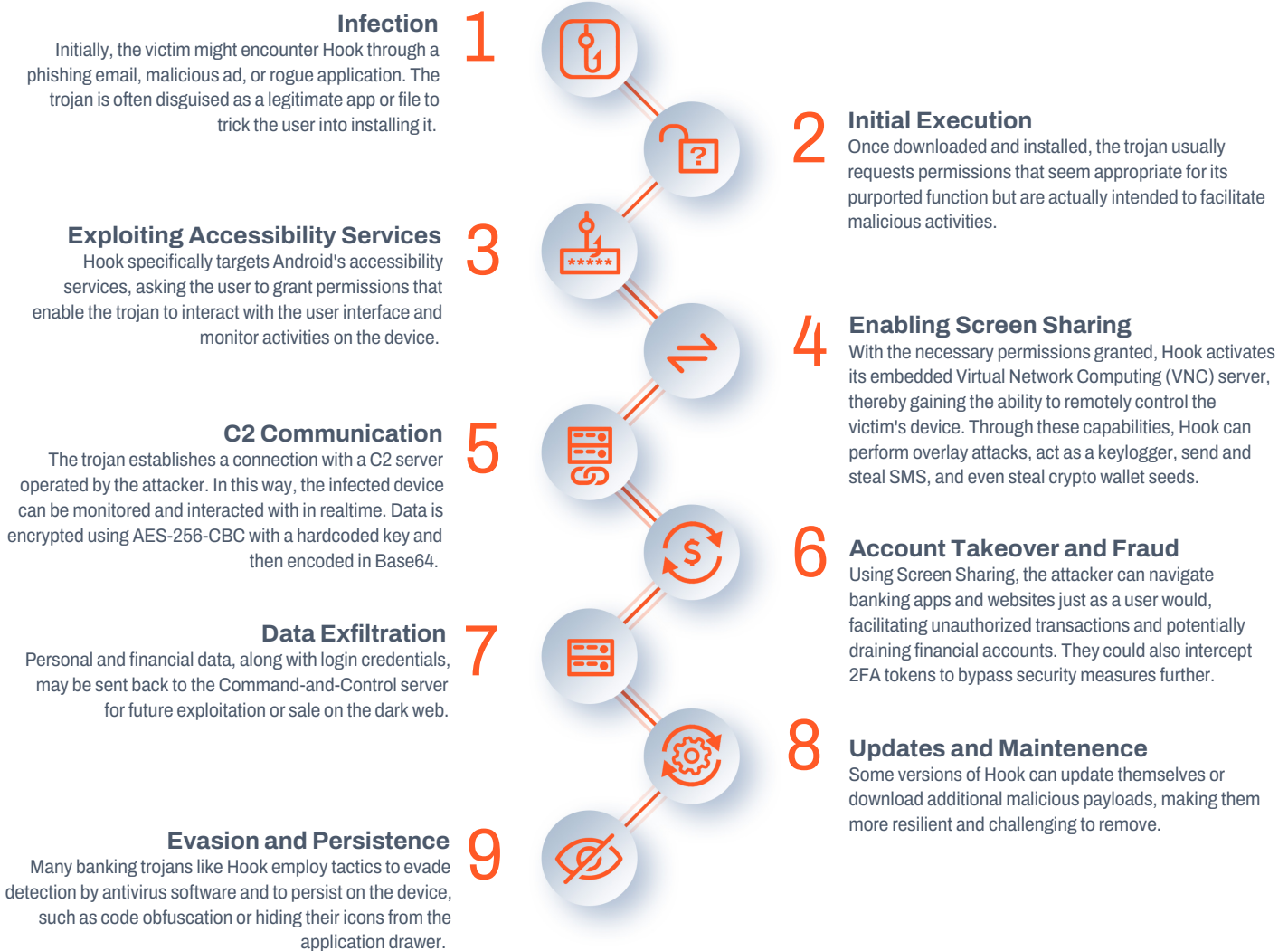




## How Hook Uses Screen Sharing for Fraud

[ThreatFabric](#) documented Hook in January 2023. The malware is an evolution of ERMAC known to be sold for \$7,000 per month. This malware was developed by a malware author called DukeEugene.

Here's how zLabs researchers observed this capability being used by Hook.



The combination of initial deception, exploitation of permissions, and use of advanced capabilities like Screen Sharing make Hook a particularly potent and malicious threat in the realm of mobile banking trojans.



### Examples of Banking Trojans using Screen Sharing



Nexus



Mailbot



Godfather



Hook

# Media Reports Highlighting Successful Mobile Banking Heists

The mobile banking landscape, while offering convenience and connectivity, also contains sophisticated malware threats that are far from theoretical. The stark reality is that malware scams have tangibly impacted lives, with substantial financial losses as a stark testament to their severity. The incidents highlighted below are not outliers but are indicative of a growing trend that exploits the intersection of technology and trust. The examples provided are sobering reminders of the real-world consequences of cyber threats in our increasingly interconnected lives.



## \$10 Million Has Been Lost in Malware Scams in 2023

Ever scroll through your social media feed and come across an advertisement for food or cleaning services? An innocent ad can turn risky when the seller asks you to download an app to place an order or book a service. Since the beginning of this year, approximately 750 people have lost a combined total of over \$10 million to malware app scams. In this episode of CNA Insider, host Steven Chia investigates how these scams work and attempts to bait a scammer himself.

[Watch the full episode here](#)



## Scan With Malware and Lose \$20,000

In May 2023, The Straight Times reported on how a woman from Singapore scanned a QR code in her local bubble tea shop. That night while she was sleeping, the malware she had unknowingly allowed on her phone removed \$20,000 from her bank account. In response to this story, the Singaporean police noted that since March, there have been at least 113 victims who lost at least \$445,000.

[Read the full article here](#)

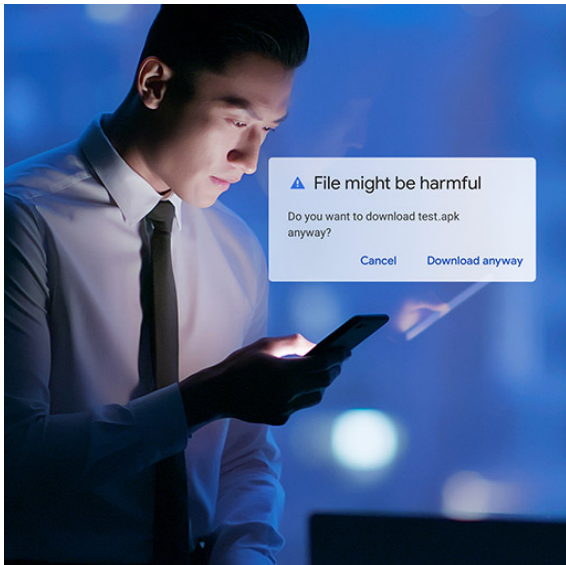




## Fraudsters Scam \$37,400 From a Woman's Life Savings

In May of this year, another Singaporean citizen lost her life savings after seeing an ad for cheap durians, a spicy fruit popular in Southeast Asia. She contacted the seller on Facebook Messenger, who then contacted her via phone. She was instructed to download an app and enter her personal details to create a membership. She was also instructed to enter a one-time password from her bank into the app. Of course, this was all the attackers with the discount fruit ads needed to empty her bank account. These examples cited in the media are hardly isolated incidents.

[Read the full article here](#)



## Malware-Related Scams Cost Users \$100,000

In June of this year, two Android users lost \$99,800 from their Central Provident Fund (CPF) due to malware scams. The victims were lured by social media ads for groceries, directing them to download an Android Package Kit (APK) for payment and ordering. These APK files were sourced from third-party platforms rather than the Google Play Store, making them susceptible to containing phishing malware. Unbeknownst to the victims, the downloaded apps granted scammers remote access to their devices, leading to the theft of sensitive data, including Singpass passcodes.

[Read the full article here](#)



# The Broader Economic Impact

## Impact on Financial Organizations

1. **Growing Fraud Losses:** Outseer reported that **59%**<sup>2</sup> of fraudulent banking transactions were initiated via the mobile banking app last year. Zimperium's current research clearly shows that banking malware continues to evolve to undermine traditional security measures and make fraud frictionless. These trends suggest that mobile app-enabled fraud will continue to rise for traditional banks.
2. **Increased Operational Costs:** Banks and FinTech companies face the burden of continually updating their security measures to combat evolving malware. This results in regulatory scrutiny and increased spending on cybersecurity infrastructure, threat detection, and incident response, affecting overall profitability. According to Lexis Nexus, the cost of fraud is highest among U.S. banks, where every **\$1** of fraud loss actually costs **\$4.36**. These fees include the legal, processing, investigation, and recovery expenses. Compliance costs will continue to rise as the regulatory environment evolves to deal with mobile banking malware.
3. **Consumer Confidence & Brand Impact:** Given that acquiring new customers is more costly than retaining existing ones, the repercussions of malware scams extend beyond the initial monetary damage to deeper, more enduring dents in customer loyalty. However, the restoration of trust, deemed more crucial than convenience by nearly 70% of consumers, hinges significantly on the bank's handling of the crisis. Banks must respond with transparency, speed, and a customer-first approach to salvage and potentially strengthen customer relationships, buffering the long-term financial consequences.

## Impact on Consumers

1. **Financial Loss:** These advanced malware variants steal banking credentials and carry out unauthorized money transfers. This not only leaves global consumers at an elevated risk of financial fraud but also places a burden on them to protect themselves on their mobile devices. To build better cyber hygiene, consumers must educate themselves about these risks and consider investing in mobile security solutions.
2. **Data Privacy Concerns:** Banking malware's ability to harvest a broad range of personal data—ranging from banking credentials to personally identifiable information (PII)—expands the scope of identity theft. Global consumers are not only vulnerable to immediate financial loss but also face long-term risks related to identity theft and personal privacy invasion. *The ITRC Aftermath report shows that 46% of identity theft victims are dissatisfied with how financial institutions and credit unions handle their cases.*

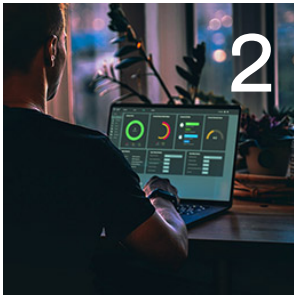


# Best Practices: Protecting Apps From Malware



## Best Practice: Ensure Protection Matches Threat Sophistication

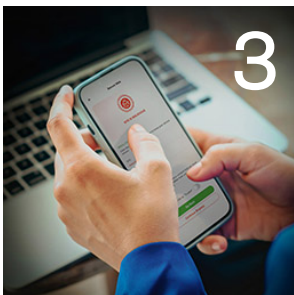
Given the rise in advanced tooling that enables threat actors to bypass rudimentary code protections, mobile application security teams must prioritize advanced code protection techniques. These protections should aim to impede the reverse engineering and tampering of mobile applications. Malicious actors have a much harder time dissecting an app when it combines multiple methods of app hardening and anti-tampering. This not only deters the creation of targeted malware but also reduces the likelihood of scalable fraud. The goal is to elevate the security posture to a point where the cost and effort of attacking the application outweighs the potential gains for the attacker.



## Best Practice: Implement Runtime Visibility for Comprehensive Threat Monitoring and Modeling

In a landscape where real-world threats often outpace standard security measures, the absence of runtime threat visibility is a significant security gap. Security and development teams frequently operate in the dark, constrained by a limited understanding of the mobile threats targeting their applications on end-user devices in real-time. In these cases, mobile app teams must rely exclusively on standards and best practices to implement security. Standards are a great starting point, but they aren't sufficient. In reality, Zimperium found that most apps are not compliant with OWASP and MASVS to a great extent. Attackers have an enormous attack surface and opportunity because of the gap between real-world threats and current protections.

To bridge this gap, it's imperative for mobile application security leaders to enable runtime visibility across various threat vectors, including device, network, application, and phishing. This real-time insight allows for active identification and reporting of risks, threats, and attacks. For security teams, it paves the way for continuous threat monitoring and rapid response. For development teams, it facilitates accurate threat modeling, allowing for the design of more resilient apps.



## Best Practice: Deploy On-Device Protection for Real-Time Threat Response

While threat visibility is crucial, the ability to respond effectively and in real-time is equally important. Mobile Application Security leaders should prioritize implementing **on-device protection** mechanisms that enable apps to take immediate actions upon threat detection. This ability to take action should be autonomous, requiring no dependency on network connectivity or back-end server communication. The response will depend on the severity and context of the threat; options include halting the application, changing its behavior dynamically, or redirecting the user to educational material.

By adopting an on-device protection strategy, threats are neutralized at the point of occurrence, all while maintaining a seamless user experience. This approach enhances both the resilience and adaptability of mobile banking applications in the face of evolving security threats.

# How Zimperium Can Help

Today, Zimperium enables over **135 global financial companies to realize** the full potential of mobile-powered businesses by activating a Mobile-First Security Strategy. Here are two solutions that directly help businesses build effective malware defenses for their mobile applications:

## Advanced Application Shielding with zShield

Zimperium's zShield is an advanced code protection solution that provides robust protection against reverse engineering and app tampering techniques. The solution prevents threat actors from examining the mobile banking app's code and finding ways to abuse it, even with sophisticated tooling. They also make it difficult for threat actors to clone or impersonate legitimate apps or steal their code to build highly effective and persistent Trojans.

zShield has a number of protection capabilities to prevent malware authors from reversing and understanding the app's inner workings.

1. **Code Obfuscation** - Protects the code from being reverse-engineered and analyzed.
2. **Integrity Protection** - A set of measures that make it challenging to modify apps and repackage them.
3. **Anti-Debug Protection** - Detects and defends against debugging and hooking tools.
4. **Root/Jailbreak Protection** - Prevents the app from running on devices that have been jailbroken or rooted.

zShield offers banks a flexible approach to security, providing two distinct application methods tailored to an app's specific security requirements. The 'Low Code' option gives banks precise control over protecting individual app functions. At the same time, the 'No Code' method simplifies the process, allowing banks to upload the app to the platform to enforce essential protections automatically.



With zShield, mobile app teams can create a hostile environment for threat actors.



## Comprehensive Device Attestation, Runtime Visibility, and Protection with zDefend

Zimperium zDefend is an in-app security SDK that enables mobile banking applications to detect and proactively protect themselves by taking actions on the end user's device, even without network connectivity. The SDK leverages z9, Zimperium's patented machine learning-based threat detection engine, which lies at the core of its multi-layered approach to detecting known and Zero-Day threats.

Here are some key detection capabilities that the solution has to prevent malware abuse:

Assess Device Risk Posture	Detect Phishing & Malware Abuse
<ul style="list-style-type: none"> <li>Jailbroken/Rooted Devices</li> <li>Emulators</li> <li>Compromised Devices</li> <li>Rooting Detection Evasion</li> <li>Vulnerable Devices</li> <li>Actively Exploited Android and iOS Versions</li> </ul>	<ul style="list-style-type: none"> <li>Phishing Detections</li> <li>Accessibility Permissions</li> <li>Screen Overlay Detections</li> <li>Screen Sharing Detections</li> <li>Hooking Frameworks</li> <li>System Tampering</li> <li>Privilege Escalation Detection</li> <li>Network Traffic Interception</li> <li>Unsafe Network</li> </ul>

The SDK sends runtime threat intelligence and forensics to a centralized console, giving security operations teams real-time visibility into risks and threats across all end-user devices. By integrating this data with traditional fraud data from Fraud Management Systems, banks can proactively prevent on-device fraud (ODF).

Additionally, mobile app development and security teams can model threats based on this extensive threat data to better align protections with actual threats.

On-device actions pre-configured within the mobile application enable proactive protection. These actions can be updated in real-time via the centralized console **without publishing a new version** making it practical and scalable across large install bases.

Zimperium's ability to deliver comprehensive runtime security without compromising the mobile banking experience is what sets it apart from its competitors.

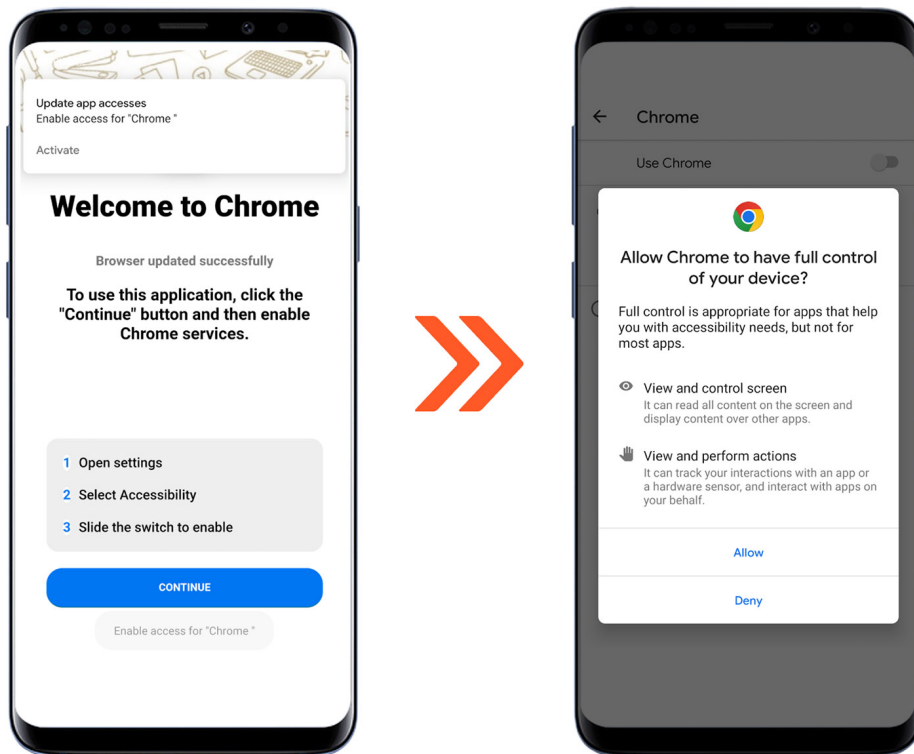


# How Consumers Can Better Protect Themselves

## Be Aware of Apps Asking For Accessibility Permissions

Accessibility permissions on Android are originally designed to assist users with disabilities, enhancing the usability of devices and apps. They allow apps to interact with the user interface, read screen content, automate touch and keystrokes, and perform other functions to make the device more accessible. Granting **accessibility permissions** can be risky because these permissions can give apps broad control over a device's functionalities. Banking trojans often ask for and then exploit accessibility features to automate transactions, capture sensitive data like passwords, or overlay fake login screens on legitimate banking apps. Being cautious about granting such permissions limits the potential attack surface for these malicious entities, thereby enhancing your device's security posture against banking trojans.

Below are images of a fake Google Chrome application distributed through third-party stores. Based on the images, it appears to be a legitimate application asking for accessibility permissions.



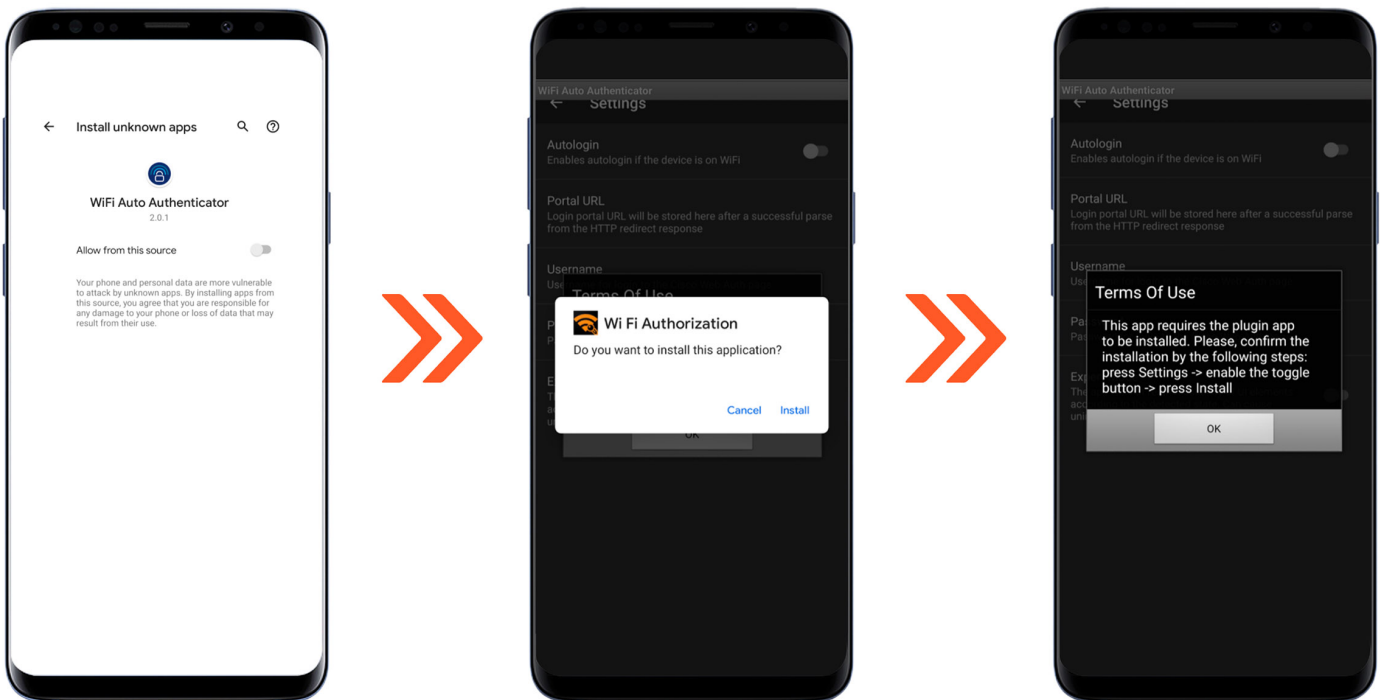
Fake Chrome App Asking for Accessibility Permissions

## Don't Download Apps From Unvetted Sources

Consumers should be cautious when downloading Android apps from third-party app stores, as these platforms often lack the rigorous security vetting found in official app stores. This lax security makes unvetted sources or third-party stores fertile ground for banking trojans disguised as legitimate apps.

Moreover, these third-party stores are frequently used in malware phishing campaigns that deploy droppers—initially benign-looking apps that later download malicious payloads. The absence of stringent security measures in third-party stores makes these droppers more easily distributed, making these platforms central to sophisticated banking trojan campaigns. Therefore, extra vigilance is advised when downloading apps from unofficial sources to minimize the risk of financial compromise.

The following images show a malware dropper impersonating WiFi Auto Authenticator. During download, the dropper asks permission to install from a third-party site. After installation, it asks for another malicious app called WiFi Authorization to be downloaded.



Example of a Malware Dropper installed from a third-party location



## Beware of Phishing Emails, SMSs, and URLs That Look Legitimate

Threat actors often reverse-engineer banking apps to steal logos, images, and user interface elements. This meticulous imitation creates rogue apps or phishing websites resembling authentic banking platforms. Coupled with using domains and URLs containing bank names, this increases the deception's credibility.

Consumers can adopt several measures to ascertain the legitimacy of an email suspected to be a phishing attempt:

- **Check the sender's email address:** Authentic emails from banks and other institutions will come from official domains. Be cautious of email addresses that look suspicious or are misspelled.
- **Scrutinize the language:** Phishing emails often contain typos, poor grammar, or overly urgent language urging immediate action.
- **Verify links and attachments:** Hover over any links without clicking to see where they lead. Be wary of unsolicited attachments.
- **Cross-reference information:** Contact the institution using verified channels to confirm the email's authenticity.
- **Invest in a mobile security solution:** Investing in a mobile security solution can add an extra layer of protection against phishing emails, malicious apps, and web-based threats.

By exercising these cautionary steps, consumers can significantly lower the risk of falling victim to phishing attacks.



Mobile-powered businesses can leverage Zimperium's Mobile Threat Defense (MTD) solution to secure Bring Your Own (BYO) and Corporate-owned mobile devices accessing enterprise data and infrastructure. With MTD's integration with Unified Endpoint Management (UEM) and Security Information and Event Management (SIEM) solutions, businesses are able to provide risk-based access and comprehensively protect their workforce from malware, network threats, and phishing attempts.

# Conclusion: Adaptive Security Amid Evolving Threats

In conclusion, the mobile malware landscape is transforming and challenging the core of traditional mobile app security measures deployed by financial institutions. The advent of Malware-as-a-Service (MaaS) platforms is disconcertingly democratizing cyber-attacks, enabling even less technically skilled individuals to compromise well-established security mechanisms. The ease with which these features can be replicated across other malware families amplifies the urgency to act.

Simultaneously, emerging regulatory frameworks, inspired by stringent measures adopted in countries like Singapore, India, and Malaysia, offer a double-edged sword. While setting new security baselines, they also impose a compliance burden on institutions, challenging the delicate balance between security and user experience.

The threat landscape is not confined to traditional banking alone; it is diversifying to include a variety of other sectors like cryptocurrency, payments, wallets, and even social media. Organizations across these sectors must recognize that the boundaries separating them from traditional financial institutions in terms of cyber risk are dissolving rapidly.

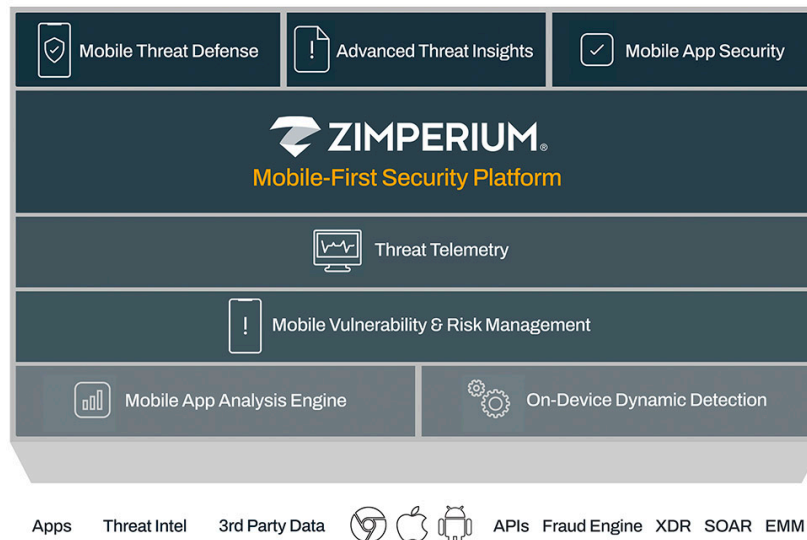
As we advance into an era marked by increasingly sophisticated malware, a proactive and adaptive security posture is no longer optional but essential. The need for real-time threat visibility and protection is critical, signifying a shift from a standards-based approach to one focused on combating genuine, evolving threats.

**This multidimensional escalation in the mobile threat landscape necessitates an equally multidimensional security strategy—one that is comprehensive, autonomous, and relentlessly focused on facing the threats of today and tomorrow.**



# About Zimperium

Zimperium enables global businesses to realize the full potential of mobile-powered businesses by activating a Mobile-First Security Strategy. Built for the demands of mobile business, Zimperium's Mobile-First Security Platform™ delivers unmatched security across both applications and devices. The Zimperium Mobile-First Security Platform unifies Zimperium Mobile Threat Defense (MTD) and Zimperium Mobile Application Protection Suite (MAPS), and provides centralized access to and management of Zimperium's mobile app and endpoint security solutions.



## Mobile Threat Defense Solution

Zimperium Mobile Threat Defense (MTD) is a privacy-first application that provides comprehensive mobile device security for enterprises. It is designed to provide security teams with mobile vulnerability risk assessments, valuable insights into the risk of mobile applications, and threat protection for protecting corporate-owned and/or BYO (bring-your-own) devices from advanced mobile threats across device, network, phishing, and app risks and malware vectors. [Learn more here.](#)

## Mobile Application Development Security Solutions

The Mobile Application Protection Suite (MAPS) from Zimperium provides four capabilities, including Mobile Application Security Testing (MAST), App Shielding, Key Protection, and Runtime Protection (RASP). The suite provides mobile app teams with centralized threat visibility and comprehensive in-app protection from development through runtime. It combines both inside-out and outside-in security approaches to help organizations build compliant, secure, and resilient mobile apps. [Learn more here.](#)

## Research Driven Innovation

Zimperium's research team, called zLabs conducts the malware research presented in this report. zLabs is an Advanced Research and Exploitation team and a leader in mobile security research, bringing together experts specializing exclusively in mobile ecosystems. The team's research-driven innovation shapes the development of sophisticated, layered security measures to safeguard mobile devices and applications. Leveraging unique threat insights, zLabs employs a multi-faceted approach using heuristic, behavioral, and machine learning techniques to provide robust in-app and on-device protection solutions. This focus on empirical research and cutting-edge methodologies places Zimperium at the forefront of mobile device and app security, making it an essential player in shaping the sector's best practices.



# Affiliations

Zimperium is a member of the App Defense Alliance and an active partner in the [malware mitigation program](#), which aims to quickly find Potentially Harmful Applications (PHAs) and stop them before they ever make it onto Google Play.

# Appendix

## Indicators of Compromise

You can find the IOCs for banking trojans in the GitHub repository link below.

<https://github.com/Zimperium/IOC/tree/master/2023-Banking-Heist>

# References

1. <https://www.alliedmarketresearch.com/mobile-banking-market>
2. <https://www.outseer.com/payment-security/outseer-report-fraudulent-banking/>
3. **Mobile Banking Statistics**  
<https://dataprot.net/statistics/mobile-banking-statistics/#:~:text=Mobile%20Banking%20Stats%20for%202023%2D%20Key%20Findings&text=In%20January%202023%2C%20there%20were,to%20%241.3%20billion%20by%202028.>
4. **Verizon DBIR**  
<https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/>
5. **2022 LexisNexis® True Cost of Fraud™ Study: Financial Services and Lending**  
<https://risk.lexisnexis.com/about-us/press-room/press-release/20221116-study-finds-fraud-costs#:~:text=Attacks%20and%20Costs%3A%20Fraud%20costs,every%20%241%20of%20fraud%20loss.>
6. **Outseer Fraud & Payments Report**  
<https://www.outseer.com/payment-security/outseer-report-fraudulent-banking/>
7. **APWG Phishing Activity Trends Report**  
[https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q4\\_2022.pdf](https://docs.apwg.org/reports/apwg_trends_report_q4_2022.pdf)  
\_ga=2.72190931.17624577.1698154516-97928637.1698154516&\_gl=1\*r2wloi\*\_ga\*OTc5Mjg2MzcuMTY5ODE1NDUxNg.\*\_ga\_55RF0RHXSr\*MTY5ODE1NDUxNi4xLjAuMTY5ODE1NDUxNi4wLjAuMA
8. <https://sifted.eu/articles/neobank-fraud-victims-revolut-monzo-starling>
8. <https://dataprot.net/statistics/mobile-banking-statistics/>
10. <https://www.pymnts.com/news/banking/2023/nearly-70-pct-consumers-prioritize-trust-over-convenience-choosing-bank/>

# Credits

---

**Researchers**

Aazim Bill SE Yaswant  
Francisco Bertona  
Gianluca Braga  
Nico Chiaraviglio  
Vishnu Pratapagiri

**Editors**

Lisa Bergamo

**Writers**

Krishna Vishnubhotla  
Nico Chiaraviglio

**Reviewers**

Jon Paterson  
Georgia Weidman  
Nico Chiaraviglio

**Graphic Design**

Tom Green

**Disclaimer**

Zimperium, Inc. makes this report available on an “as-is” basis with no guarantees of completeness, accuracy, usefulness or timeliness. The information contained in this report is general in nature. Opinions and conclusions presented reflect judgment at the time of publication and may change at any time. Zimperium, Inc. assumes no responsibility or liability for errors, omissions or for the results obtained from the use of the information. If you have specific mobile endpoint or application security concerns, please contact Zimperium, Inc. via <https://www.zimperium.com/contact-us/>.