



# 2023 Mobile Banking Heists Report

## Executive Summary

## Introduction

The mobile banking market is on a rapid ascent, **projected to hit the \$7 billion mark by 2032**, 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

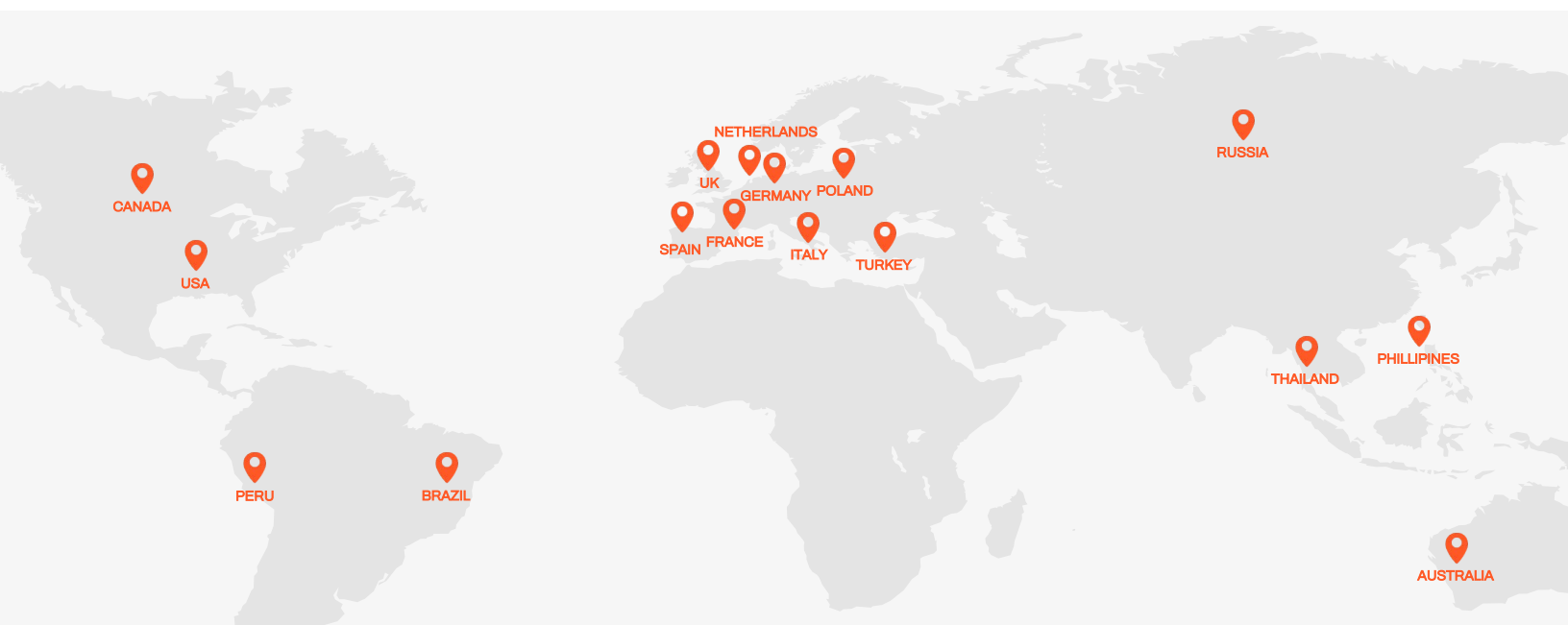
Zimperium's latest research explores a dynamic and expanding threat landscape by meticulously analyzing **29** banking malware families and associated trojan applications. This year alone, the research team identified **10** new active families, signifying the **continued investment** from threat actors 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.

## 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.

To learn more, **download** the full report at <https://get.zimperium.com/mobile-banking-heists-2023/>



Learn more at: [zimperium.com](https://www.zimperium.com)

Contact us at: 844.601.6760 | [info@zimperium.com](mailto:info@zimperium.com)

Zimperium, Inc  
4055 Valley View, Dallas, TX 75244