ZIMPERIUM

2023 Global Mobile Threat Report

With contributions by:

riscure

RSA

Trellix

Index

Executives Perspective

1.1: Mobile-Powered Business: Huge Opportunities…and Risks 2
1.2: 5 Security Principles of a Mobile-First Security Strategy 5
1.3: Artificial Intelligence and the Future of Mobile Security 9
1.4: The Way Forward for Unmanaged Devices 10

The Mobile Attack Surface

2.1: Zimperium zLabs: 2023 Research Highlights 12
2.2: 10 Mobile Attacks that Made Headlines in 2022 14
2.3: State of Mobile Endpoint Security in 2022 17
2.4: State of Mobile Application Security 2022 20

Mobile Endpoint Trends

3.1: The Continued Rise of Mobile-Specific Phishing 27
3.2: Mobile Malware: Evolving Attacks, Expanding Risks 35
3.3: Zimperium's Detection of Unknown Threats: Highlighting the Advantages of Machine Learning 40
3.4: Mobile Spyware: Increasing in Volume and Sophistication 42
3.5: Mobile Ransomware Is Now a Legitimate Threat 47
3.6: Exploited Mobile Vulnerabilities in 2022 49
3.7: Vulnerability Spotlight: A New Class of Vulnerabilities are Affecting Apple Devices 52
3.8: Mobile Platform and Ecosystem Risk in 2022 54
3.9: Mobile Threat Chains: The Anatomy of Multi-Phase Attacks 59
3.10: How Malicious Actors Are Attempting to Bypass Apple Safeguards 62

Mobile Application Trends

4.1: Trojans Jeopardize Mobile Banking, and More 66
4.2: Securing Mobile Payments in 2023 and Beyond 72
4.3: Mobile Apps and Insecure Cloud Storage: A Dangerous Mix 75
4.4: OWASP Mobile Top 10 and MASVS Standards: What They Say, How they Can Help Developers Create Secure Apps 77
4.5: Mobile Application Security: A Mobile Security Lab Perspective 81
4.6: Cryptographic Key Security: A Must for Mobile App Security 82

Summary

5:1: Conclusion 85
5.2: Sources 86
5.3: Glossary of Mobile Security Terms 87
5.4: Credits 89
5.5: About Zimperium 90

Mobile-Powered Business: Huge Opportunities...and Risks

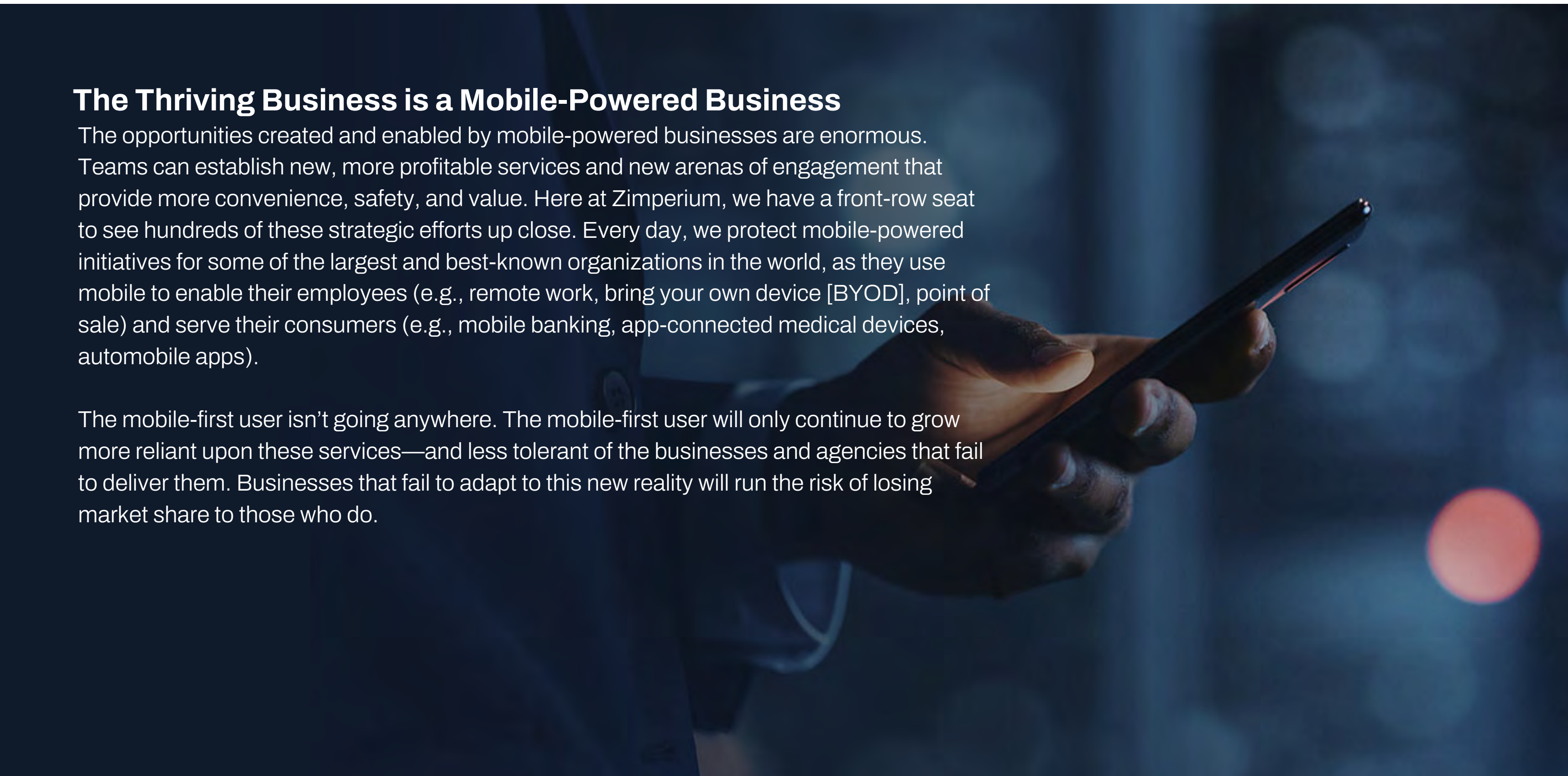
Shridhar Mittal, CEO at Zimperium

The Emergence of Mobile-First Users

In recent years, mobile devices have continued to proliferate around the globe and become increasingly woven into the fabric of our daily lives. As a result, we've become mobile-first users—where mobile devices are our first choice for how we communicate, navigate, bank, take photos, shop, and stay informed. In turn, the companies that support us have shifted into mobile-powered businesses. Mobile-powered businesses are those organizations that are harnessing the unique power of mobile devices and apps to improve profitability, productivity, and customer experiences.

Worldwide, there were 7.1 billion mobile device users in 2021, and that number is expected to grow to 7.5 billion by 2025.[1] Mobile app usage and purchases have also continued to grow and reach a massive scale. In 2022, revenue from mobile apps exceeded $400 billion.[2] Mobile apps now account for 60% of e-commerce purchases.[3] One survey found that 89% of respondents now use mobile banking apps. That number is even higher, at 97%, if we include millennials.[4]

Mobile devices are now also integral to the way we work. Last year's report revealed that 60% of the endpoints accessing enterprise assets were mobile devices. Employees are using mobile devices to interact with more apps, conduct more transactions, collaborate with more people, and access more data. And mobile devices are almost always the additional factor in multi-factor authentication (MFA) solutions that govern access to corporate resources, including desktops and laptops.



The Thriving Business is a Mobile-Powered Business

The opportunities created and enabled by mobile-powered businesses are enormous. Teams can establish new, more profitable services and new arenas of engagement that provide more convenience, safety, and value. Here at Zimperium, we have a front-row seat to see hundreds of these strategic efforts up close. Every day, we protect mobile-powered initiatives for some of the largest and best-known organizations in the world, as they use mobile to enable their employees (e.g., remote work, bring your own device [BYOD], point of sale) and serve their consumers (e.g., mobile banking, app-connected medical devices, automobile apps).

The mobile-first user isn't going anywhere. The mobile-first user will only continue to grow more reliant upon these services—and less tolerant of the businesses and agencies that fail to deliver them. Businesses that fail to adapt to this new reality will run the risk of losing market share to those who do.

Security Teams Need to Adapt to the Mobile-Powered Business, Fast

The rise of the mobile-powered business has fundamental implications for security teams. The explosive growth in mobile device and app usage has created an ever-growing attack surface—and increasing numbers of sophisticated cyber criminals and nation states continue to exploit these areas of vulnerability. Meanwhile, security budgets and staffing levels remain relatively flat. Consequently, today's teams are confronting large and rapidly growing vulnerability gaps.

The consequences of these vulnerability gaps have been devastating. For example, losses from online payment fraud cost e-commerce businesses $41 billion in 2022 and are expected to grow to $48 billion in 2023.[5] Another report found that 70% of digital fraud now occurs on mobile devices.[6]

In 2023, enterprise security teams will still contend with the aftermath of the COVID-19 pandemic and the rapid, massive shifts it precipitated. Telehealth, remote and hybrid work, cloud storage, short message service (SMS)-based multi-factor authentication, and QR codes are just a few examples of approaches that saw explosive growth in recent years—with each of these areas posing new security risks that teams haven't fully addressed. For example, one report revealed that 79% of respondents felt that recent changes to working practices had adversely affected their organization's cybersecurity. Nearly two-thirds (66%) of respondents indicated that they had previously come under pressure to sacrifice mobile-device security "to get the job done," and 52% said they succumbed to that pressure.[7]

The concerns expressed by security teams are well founded, with major attacks on the rise. The same report found that 45% of companies surveyed suffered a compromise in the past 12 months, up 22% over the prior year.[8]

45%

of companies surveyed suffered a compromise in the past 12 months, up 22% over the prior year

As mobile phones continue to be used for increasingly essential services, whether shopping, banking, or working, cybercriminals know there are growing opportunities to profit. For those tasked with countering these attacks, security must address a range of threats, including:

- **Device vulnerabilities**. Mobile devices of every form continue to be vulnerable. In recent months, significant vulnerabilities have been discovered in both Android and iOS devices.
- **Spyware**. Nation states continue to leverage spyware to pursue their objectives, and mobile devices continue to be targeted. U.S. ambassadors, Spain's Prime Minister, and the former Prime Minister of the UK have all fallen victim to spyware. However, spyware isn't just a threat to high-ranking government officials, and the public is increasingly aware of this fact. A Zimperium survey revealed that 85% of respondents felt spyware posed a threat to them and their organization.
- **Phishing**. Phishing has been and continues to be one of the most prevalent forms of cyberattacks on mobile. Our researchers found that 80% of phishing sites now either specifically target mobile devices or are built to function on both mobile devices and desktops. The average user is 6-10 times more likely to fall for an SMS phishing attack than an email-based one.

In response to these escalating threats, 85% of organizations now have a budget dedicated to mobile security.[9]

All these factors point to how critical it is to address mobile security comprehensively. Security teams need advanced, adaptive protections that safeguard against device, network, phishing, and app attacks. In addition, mobile apps must be effectively secured across the development lifecycle and post-deployment. What organizations truly need is a Mobile-First Security Strategy. Zimperium's CTO, Jon Paterson, explains what this is and how to begin executing this type of strategy in the next section of this report.

We Hope You Find Our 2023 Global Mobile Threat Report Useful

While these emerging trends can be sobering and downright scary for security teams, they don't have to be. This report is not intended to stoke fear but to provide an authoritative look at what is really happening in the global mobile threat landscape so teams will be able to make informed decisions about their risks and what to do about them.

In this report, we've compiled and distilled some of the most important trends and developments that shaped the mobile security landscape over the last year and those that are most critical to respond to in 2023. This report draws on the research of our internal experts and the insights of our partners and leading industry observers.

We sincerely hope you find these insights useful as you seek to strengthen security in our increasingly mobile-first world. If you ever need additional information to inform your strategies and plans, rest assured that the Zimperium team is here to help.

5 Security Principles of a Mobile-First Security Strategy

Jon Paterson, CTO at Zimperium

The Implications of Securing Mobile-Powered Business Initiatives

Mobile-powered initiatives are critical to profitability, productivity, and competitiveness. Mobile devices and apps are how customers interact with organizations and how employees access resources, collaborate, and work. In virtually every sphere of our lives, mobile devices are ubiquitous. This ubiquity has created several key implications for organizations:

- Diverse devices are accessing corporate data, including employee-owned mobile phones and other devices that aren’t managed by corporate IT teams.
- As this report will detail, threats to mobile apps and devices continue to rise in both volume and sophistication.
- The number of mobile apps an organization offers to employees continues to increase, and at the same time, the number and type of apps that are active on employee and customer devices is exploding.
- Sophistication of risks related to mobile are increasing, and businesses want to provide more direct access to mobile devices in zero trust environments, creating new challenges for CISOs and security organizations.
- Regulations and mandates related to application and user data continue to be more onerous, and more difficult to adhere to when addressing the global needs of an organization.

The Unique Security Challenges Posed by Mobile Devices and Apps

With the introduction of mobile devices and apps to the organization, security teams face a new set of challenges and need to be aware of new threat vectors and areas of risk:

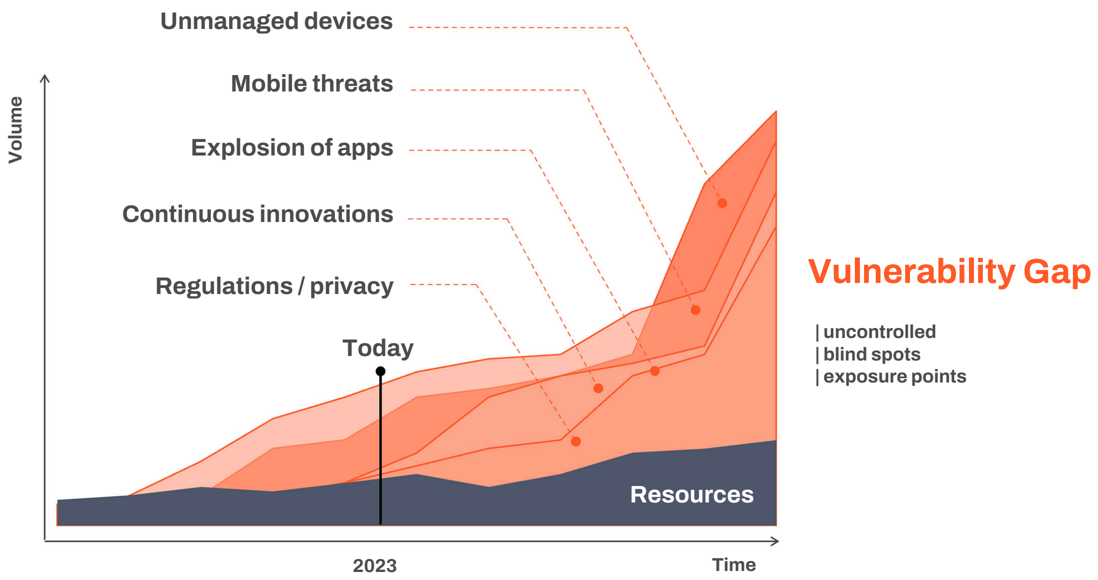
Devices: In a BYOD environment, mobile users are the “device administrators,” often with complete control over the apps they download, when (and whether) to install patches or updates, which permissions to grant, and more. Rather than operating in a relatively protected corporate environment, devices can be used anywhere, may be left anywhere, and are frequently connected to public Wi-Fi. Even in Unified Endpoint Management/ Mobile Device Management (UEM/MDM)-managed scenarios, the user continues to have override control for security decisions unless fully supervised. Many organizations allow mobile devices on corporate Wi-Fi without full security assurance. This practice opens the opportunity for a mobile device to be used as an entry -point to other corporate resources.

Apps for business: Traditional enterprise business applications run in a secure data center on servers organizations control. And mobile apps are deployed to app stores, where they are exposed to reverse engineering and tampered with by attackers, and ultimately run on end- user devices that are outside the control of the app owner with data primarily held in the cloud. Businesses often assess the cloud services they use and how they store data as part of a risk assessment, but the app itself is assumed secure. It’s imperative that organizations assess this potential risk on a continuous basis.

Apps for consumers: Consumer apps are making their way into the corporate world and pose potential security risks to the business. For example, employees access clipboard content and share resources and files on the device. As security professionals, how do we assess the potential risks of such applications, and have processes to assess and respond at scale?

The level and scope of risk continues to increase and evolve. At the same time, resources within organizations enabled to address mobile threats and complexities are in short supply. The result is a "Vulnerability Gap" that jeopardizes mobile-powered businesses with blind spots and an exponentially increasing number of exposure points.

The escalating Vulnerability Gap

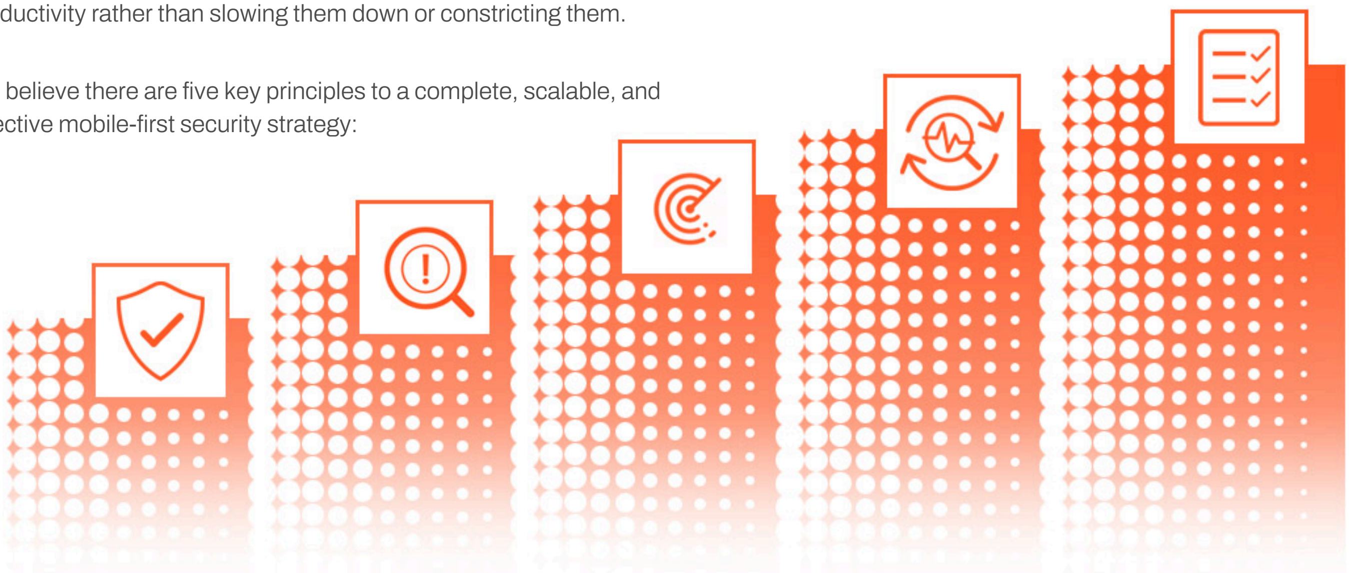


The fundamental question is this: ***"How do organizations realize the potential of mobile-powered initiatives without jeopardizing the integrity of the business?"*** (In other words, how do they solve the Vulnerability Gap?)

Five Key Principles of a Mobile-First Security Strategy

Zimperium has helped thousands of enterprises and government agencies around the world answer that important question of how to solve the Vulnerability Gap. From over a decade of experience, we know that the answer lies in having policies and controls addressing the challenges with a Mobile-First Security Strategy—a strategy that accounts for all of the complexities and realities of mobile devices, apps, users, and business models; one that supports and enables mobile-powered initiatives and enables users and productivity rather than slowing them down or constricting them.

We believe there are five key principles to a complete, scalable, and effective mobile-first security strategy:



1. **Prioritize and assess risk as close to the user or point of entry as possible**. Organizations need to prioritize securing mobile-powered business initiatives across all mobile devices and apps.
2. **Operate in a known state - visibility and vulnerability assessment for all your entry points**. Gain complete visibility of your mobile ecosystem and risk level. Automatically assess vulnerabilities and address them—without throttling productivity. Establish safeguards that are measurable, auditable, and insurable.
3. **Enhance your detection and response strategy for mobile**. Detect anomalies and prioritize remediations based on contextual intelligence—so the most critical gaps get addressed first. Embed security across the device and application lifecycle, provide risk-based response, and enable zero trust assessment of mobile endpoints.
4. **Start the autonomous journey**. Dynamically respond to ever-changing threats and mobile ecosystems. Automatically isolate compromised devices and untrusted environments. Establish a proactive, resilient, and scalable security posture.
5. **Minimize risk compliance failures**. Stay ahead of regulations, data sovereignty and privacy standards, while respecting employees' work/life boundaries.

A Real World Example

A great example of a well- considered Mobile-First Security Strategy is that of a major international organization who, prior to working with Zimperium, had a restrictive mobile security strategy where all devices, regardless of corporate- owned or BYOD, were required to be enrolled into UEM for device management. This caused friction with BYOD end users. Due to the lack of visibility to vulnerability and risk, they only supported a small subset of handset vendors that were approved for BYOD use.

By leveraging mobile threat defense (Key Principle #1), the organization gained better visibility into its risk posture and enabled the adoption of a broader range of device models & manufacturers. This allowed the organization to accelerate its BYOD strategy- while providing real-time insights into the risks on those devices (Key Principles #2 and #3). It also gave them the ability to provide and deliver automated response (Key Principle #4) without compromising security.

As a result, the bank has been able to achieve the vision of its mobile-powered initiative without security impacts. This is exactly how a Mobile-First Security Strategy should work in real life.

The same organization was able to leverage the Zimperium Mobile Application Protection Suite (MAPS) to provide runtime security insight to their mobile application (Key Principles #1, #2, and #3), as many of their customers were being targeted for scams/fraud via social engineering and malicious app installation. With the implementation of security telemetry inside their consumer banking app, they can now gain visibility to the risks, and automatically respond to them within the app (Key Principle #4). All of this can be accomplished while ensuring that they meet compliance and data sovereignty requirements (Key Principle #5).

As a result, the organization has been able to achieve its vision of its mobile-powered initiative, reducing risk- and providing visibility, actionable insights, and automated response.

Let's Get Practical

There's no turning back. The mobile-powered business is here to stay. Given that reality, what are some practical steps that security teams can take? Here are some key questions to consider:

Corporate Device and Application Usage Considerations

When developing your strategy to protect mobile devices and assessing the apps they contain, consider the following questions:

- How are you baselining your initial mobile device risk posture for both managed and unmanaged devices and responding dynamically to elevated risk?
- How many mobile devices are accessing your corporate assets that are unmanaged or without visibility?
- What is your strategy for BYO devices and unmanaged applications?
- What are your zero trust initiatives, and where does mobile fit?
- What is your vision for consolidating mobile security telemetry as part of your data lake and extended detection and response (XDR) strategies?
- Organizations often have a solid strategy for email phishing attacks - How do you reduce risk, measure, and respond to mobile phishing attacks?
- What is your strategy for mobile ransomware and spyware?
- How are you assessing the potential risk of publicly available applications on your managed and unmanaged devices?
- How are you addressing local privacy and data laws and compliance needs across your mobile assets (devices and apps)?

Mobile Application Development Considerations

When developing applications internally, or if applications are developed for your organization by third parties, consider the following questions:

- Often organizations are using external services for application review - typically, security flaws are assessed. Knowing that development teams release versions of apps one to four times a month, how do you deliver assurance of security at scale without impacting development performance?
- How are you assessing privacy and compliance issues of the applications you are releasing?
- Are your apps using code obfuscation or integrity checking? How are you attempting to thwart reverse engineering?
- How well do your app protection approaches score when compared against Open Worldwide Application Security Project (OWASP), Mobile Application Security Verification Standard (MASVS), National Information Assurance Partnership (NIAP), or Mobile Payments on COTS (MPoC) standards?
- How are you assessing the risk posture of the devices your app is running on (beyond using simplistic open- source jailbreak or root detection to “tick the box”)? What security logic do you have in place to make decisions around device attestation?
    - How do you keep up to date with new tool coverage?
- How are you giving security or SOC teams visibility into the attacks, and providing forensics to use as part of a greater security workflow?
- How will you attest the security mechanisms in place to auditors?
- An average mobile application has several externally developed software development kits (SDKs). Do you feel you have a robust workflow for identifying risks due to third-party SDK usage?

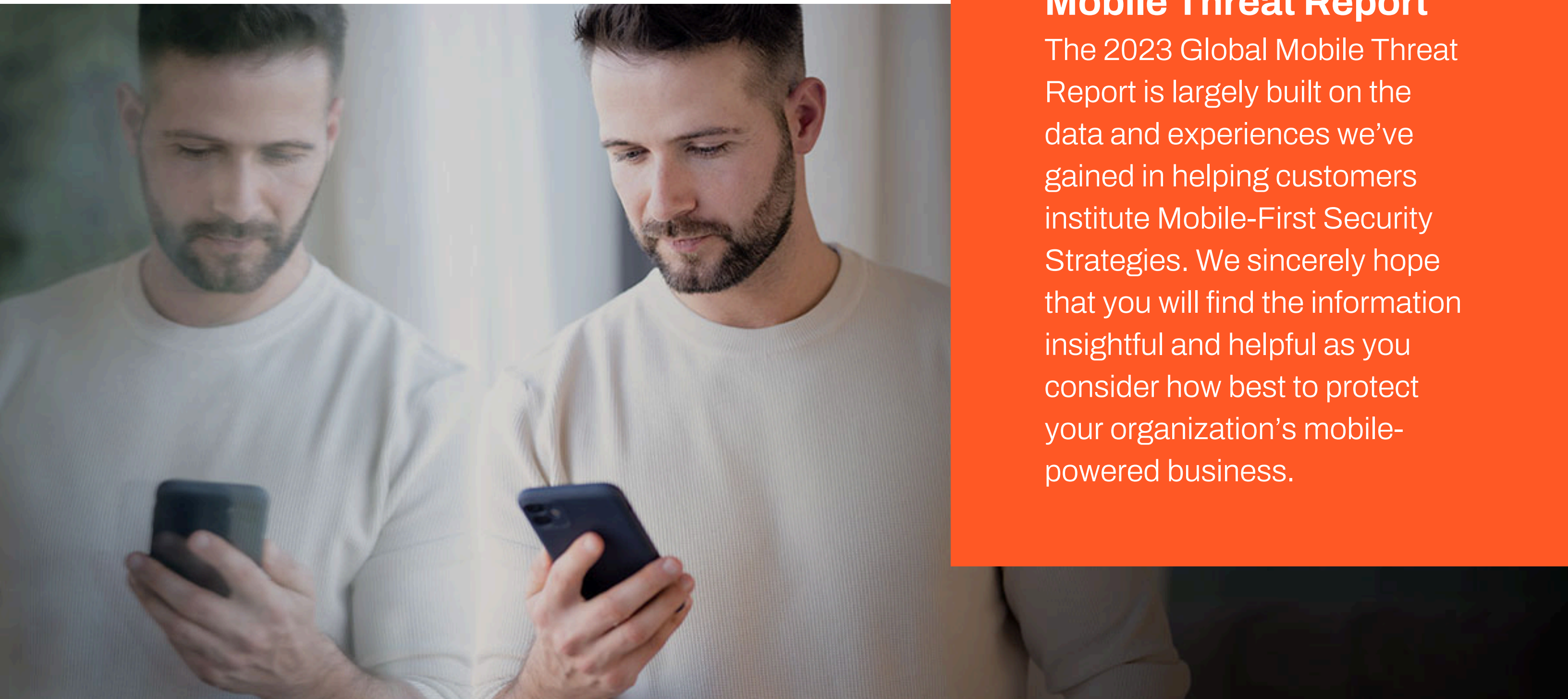
Security Considerations as a Mobile User and Consumer

As users of mobile devices, there are some key steps you can take that will help reduce risk for both your device and the data that you use:

- Apply security patches whenever available for your device.
- Disable developer configurations on the device unless actively developing. Keep a separate developer device for this use case.
- Prefer apps from known, approved stores over third-party ones.
- Ensure that operating systems and apps are automatically updating. Vulnerabilities are often addressed in updates as well as new features added.
- Check and consider permissions apps are requesting at download and when running.
- Read the reviews on apps before installing. If there are complaints of suspicious behaviors, be wary of installation.
- Leverage external app review services, if available, to provide risk or privacy visibility prior to downloading.
- Avoid public Wi-Fi usage. If you must use them, leverage a VPN to encrypt traffic.
- Leverage SMS and malicious URL and phishing protection solutions. As the report will highlight, this is a significant vector of attack that needs robust, immediate solutions.

The 2023 Global Mobile Threat Report

The 2023 Global Mobile Threat Report is largely built on the data and experiences we’ve gained in helping customers institute Mobile-First Security Strategies. We sincerely hope that you will find the information insightful and helpful as you consider how best to protect your organization’s mobile-powered business.



Artificial Intelligence and the Future of Mobile Security

Nico Chiaraviglio, Chief Scientist at Zimperium

In 1977, the first West Coast Computer Fair was held. During the fair, Ted Nelson gave an exposition titled, “Those unforgettable next two years,”, highlighting the explosion of personal computers that was about to occur. Thanks to artificial intelligence (AI), we are now experiencing a new version of those “unforgettable next two years.”. Unless you were living completely off the grid, you’ve probably heard of and perhaps even interacted with ChatGPT, the artificial intelligence-powered chatbot implementing a language model trained on the whole corpus of human knowledge. Early assessments show that ChatGPT is capable of solving almost any language-oriented task—unless that task is math related (just like for many actual people, math is AI’s least favorite subject). Furthermore, a recent paper from Microsoft claims that ChatGPT-4 is showing sparks of artificial general intelligence.

ChatGPT is only one of many AI milestones in recent years. Last year, there was a succession of milestones:

- Google’s LaMDA emerged as the first AI system to pass the Turing test.
- Several developments in scientific fields with DeepMind models for protein folding and matrix multiplication.
- Advances in text-to-image and text-to-video with OpenAI’s DALL-E and Meta’s Make-A-Video models.
- New successes in speech-to-speech translation, among several other fields.

Why AI is Such a Game-Changer in Cybersecurity

AI is also revolutionizing cybersecurity, demonstrating its facility as the most effective way for organizations to adapt to an evolving threat landscape. AI is such a great leap forward because it can automate and perform tasks such as threat detection, vulnerability management, and network monitoring, to name a few. While not always given due credit in the media, the value of AI has been evident for many years. Perhaps the best example of this is the email spam filter, which has existed since 1996.

Since Zimperium’s inception, AI has been at the core of its technology and innovation, being the only mobile threat defense (MTD) provider that can run machine learning models on device to perform a myriad of tasks such as detecting malware, phishing, system exploits, network reconnaissance, jailbreak/rooting, and system anomalies. Our models are constantly evolving to adapt to changing threats and are updated continuously to deliver peak performance.

Due to its high efficiency and privacy-centric approach, Zimperium’s detection capabilities are protecting residents of Los Angeles, New York, Dallas, and Michigan; students and educators at K-12 institutions; and devices of the U.S. Department of Defense and thousands of enterprise organizations around the world. At the same time, Zimperium has partnered with Google as part of its App Defense Alliance to keep malware out of the Play Store.

AI innovation won’t stop in 2023; it will accelerate, and Zimperium will be at the forefront of the process.

The Way Forward for Unmanaged Devices

Jim Taylor, Chief Product Officer, RSA

The best code you'll ever write is the code you write with your customers. That's what happened in 2022, when one of our customers—and one of the world's largest financial services organizations—told us they had a problem: they needed to secure users' unmanaged devices.

This need wasn't unique to this customer, or even to financial services generally. The global pandemic, financial headwinds, and remote work have all made unmanaged devices a fixture of the work-from-anywhere economy. Organizations don't want to pay for every cellphone, laptop, and tablet. Employees don't want their employers to install software on their phones.

While unmanaged devices may help an organization's bottom line, they still come at a high cost. By their very nature, unmanaged devices aren't as secure as managed hardware. And threat actors are taking notice: Verizon's 2022 Mobile Security Index found that mobile-related compromise had doubled from 2021 to 2022. About one-fifth of successful phishing emails come from mobile devices, per the 2022 Verizon Data Breach Investigations Report.

And it's not just that organizations are encountering more breaches—it's that those breaches have an even deeper impact: 73% of organizations that experienced a mobile-related compromise described it as a "major" breach. The 2022 IBM Cost of a Data Breach Report found that "costs where remote working was a factor in causing a breach" were roughly $1 million more than when employees were on site.

73% **of organizations that experienced a mobile-related compromise described it as a "major" breach.**

Have Cake, Eat it Too

Unmanaged devices expand the attack surface, are inherently less secure than managed hardware, and are still a necessary part of doing business. Our customer wanted to have their cybersecurity cake and eat the cost savings, too. At the same time, cybercriminals wanted to poison the cake, burn down the kitchen, and ransom the recipes.

We found a way forward by working with Zimperium to develop RSA Mobile Lock, which prevents risks and detects on-device threats.

Mobile Lock is automatically deployed as part of the RSA Authenticator App—it's not a second app that users need to manage. Once installed, Mobile Lock scans for critical risks like jailbroken devices, suspicious apps, elevation of privileges, man-in-the-middle attacks, and other threats. If it detects a threat, Mobile Lock restricts users from using the RSA Authenticator. When it detects a threat, Mobile Lock leaves all other systems on the device unaffected—a user can still call, text, connect to the Internet and, ideally, contact their IT department to resolve the issue.

Mobile Lock addressed our customer's problem—they can now establish trust in unmanaged mobile devices. Since launching the solution in October 2022, we're seeing early signs of massive uptake in the solution, with additional customers in healthcare, manufacturing and supply chain, and other financial services adopting Mobile Lock.

The *Right* Thing—Not *Everything*

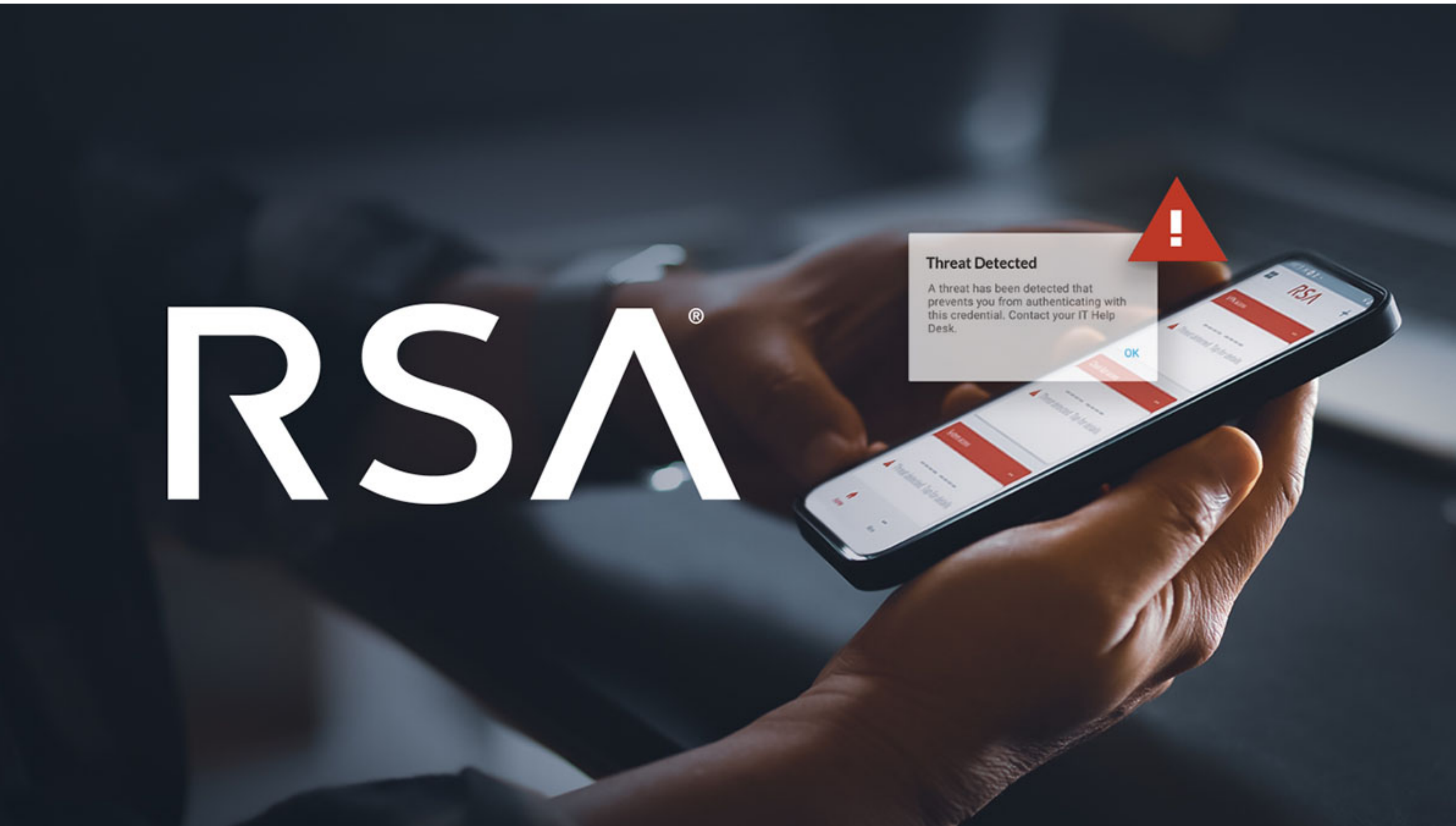
The growing number of unmanaged devices is a major accelerant driving explosive growth in the attack surface: increasing users, entitlements, and environments are making larger, more interconnected, and more vulnerable IT universes.

Zimperium's Global Mobile Threat Report and some of the highest-profile breaches in recent memory—including Colonial Pipeline, SolarWinds, and LAPSUS$—demonstrate how threat actors are successfully exploiting that growth. Zimperium's observation that the volume and sophistication of attacks are increasing significantly is absolutely correct.

If anything, that's putting it too lightly. There's simply too much spread across too many fragmented security solutions for humans to process at speed or scale. Today, I can't expect my security team to review *everything*—instead, I need them to prioritize the *right* thing. And the only way to do that is with automated intelligence solutions that find the signal in the noise, triage risks, and automate responses.

Our initial version of Mobile Lock was a great start at delivering those capabilities, but it was just a start. Cybersecurity's way forward demands a comprehensive approach that ingests signals, risks, and threats across the entire IT estate and at every stage of the identity lifecycle. The next version of Mobile Lock will do just that: it will review a broader array of signals, risks, and threats and build that intelligence into a broader security fabric.

Mobile Lock v1 solved the last problem—Mobile Lock v2 will get ahead of the *next* problem. That's right where our customers need us to be.



Threat Detected

A threat has been detected that prevents you from authenticating with this credential. Contact your IT Help Desk.

Zimperium zLabs: 2023 Research Highlights

The Zimperium zLabs Advanced Research Group continuously investigates mobile device and application threats targeting users worldwide.

The zLabs team detected an average of 77,000 unique malware samples every month in 2022. Between 2021 and 2022, the team saw the total number of malware samples rise by 51%, with more than 920,000 samples detected.

The following is an overview of some of the most high-profile discoveries made by the zLabs team.

Dirty RatMilad: Android Spyware

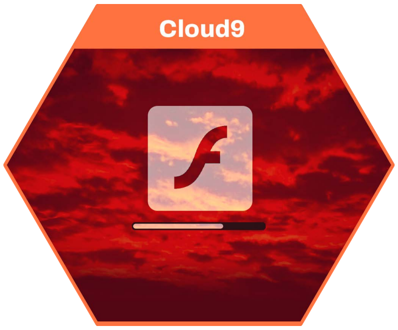
Mobile spyware is no longer just the domain of sophisticated government surveillance teams and nation states. RatMilad is just one example of how this type of spyware is being employed by smaller organizations. This malware (which has various spyware capabilities such as data exfiltration techniques) has taken various forms. The original variant of RatMilad was hidden within a phone number spoofing app called Text Me, an app that purported to help users verify a social media account by phone. In the fall of 2022, zLabs discovered a live sample of RatMilad hidden within an app called NumRent, which is a renamed, updated version of Text Me. These apps are distributed through links in messages and social media posts.

MoneyMonger: Malware Disguised by Flutter

Near the end of 2022, zLabs announced the discovery of MoneyMonger. Disguised as an app enabling individuals to get loans, this malware campaign enables malicious actors to steal private data. MoneyMonger was discovered in a Flutter app. Flutter is an open-source software kit for developing cross-platform apps. Through Flutter, teams can develop and maintain one codebase while delivering native mobile apps on multiple device platforms. By taking advantage of Flutter's framework, the threat actors behind MoneyMonger were able to obfuscate malicious features so they're not detected by legacy mobile security products.

Dark Herring: Scamware Exceeds 100 Million Installations

Last year's report featured an Android Trojan attack known as GriftHorse, outlining how it infected 10 million devices in over 70 countries. Unfortunately, since that time, the scamware threat only became more widespread. Early in 2022, zLabs discovered Dark Herring, another scamware campaign. Dark Herring has targeted more than 100 million victims globally. This campaign exploits direct carrier billing to scam money from unsuspecting users, with losses estimated to have reached hundreds of millions of dollars.



Cloud9: Chrome Extension Enables Remote Device Control

Late in the fall of 2022, the zLabs team discovered a malicious, potentially extremely dangerous extension to the Chrome browser. Dubbed Cloud9, this malware has the ability to steal information available during browser sessions. In addition, it can install malware that enables malicious actors to gain control over the infected device. This malware is distributed in a number of ways, including sideloading through fake executables and malicious websites purporting to provide users with Adobe Flash Player updates.

Schoolyard Bully: Trojan Credential Stealer Afflicts 300,000 Victims

Late in 2022, zLabs discovered a new Android threat campaign, the Schoolyard Bully Trojan. These trojans have been found in numerous apps that were downloaded from the Google Play Store and third-party app stores. The trojans are hidden within seemingly legitimate educational apps. Claiming more than 300,000 victims, the malware is focused on stealing an individual's Facebook credentials. While these malicious apps have been removed from the Google Play store, they remain on numerous third-party app sites.

The zLabs team detected an average of

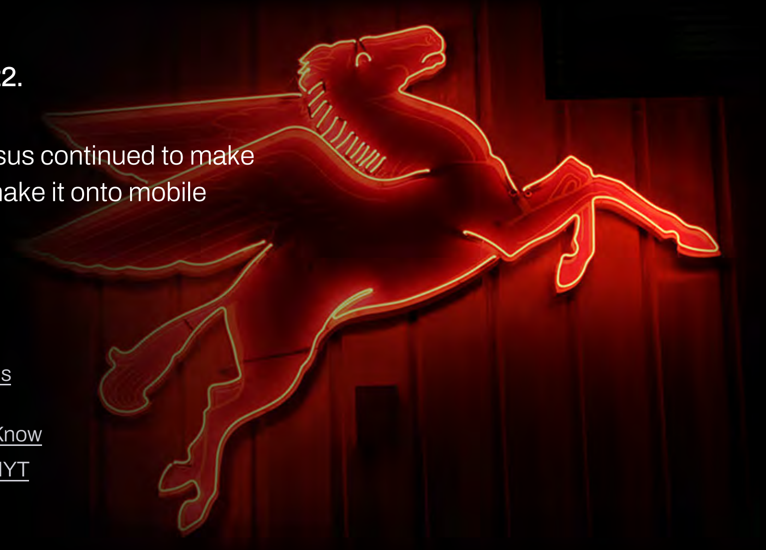
77,000

unique malware samples every month

10 Mobile Attacks that Made Headlines in 2022

Over the course of 2022, mobile threats continued to proliferate and generate news. The headlines from 2022 abundantly illustrate the persistent, dangerous nature of cyberattacks being waged around the world—and the porous nature of many of the mobile device and app safeguards that are in place today.

Here are the 10 mobile threats that generated the most news in 2022.

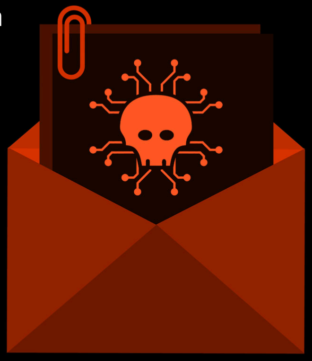


Pegasus Spyware: No stranger to the news in recent years, Pegasus continued to make waves in 2022. Developed by NSO Group, Pegasus continues to make it onto mobile devices and enable all manners of surveillance.

Notable Coverage:

- The Register: NSO claims 'more than 5' EU states use Pegasus spyware
- IT Brew: Pegasus spyware targets journalist's mobile devices, raising questions about state surveillance
- CNET: Pegasus Spyware and Citizen Surveillance: Here's What You Should Know
- FedScoop: FBI tested and almost deployed controversial Pegasus spyware: NYT

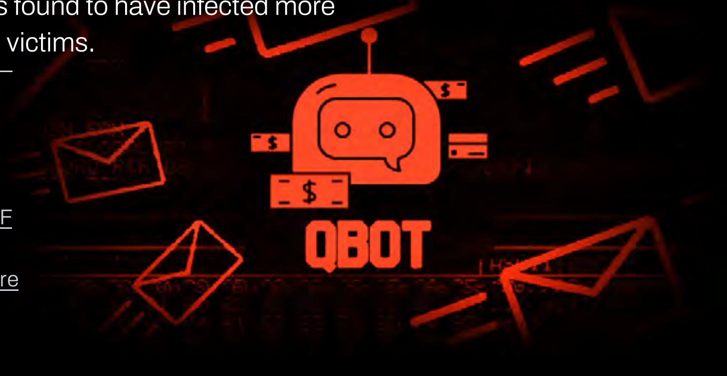
Emotet: Emotet is a malware-as-a-service offering that enables criminals to steal credit card data, install ransomware, and infiltrate networks. Taken down by law enforcement in 2021, new versions of Emotet reappeared in the fall of 2022, featuring more advanced evasion-detection capabilities.



Notable Coverage:

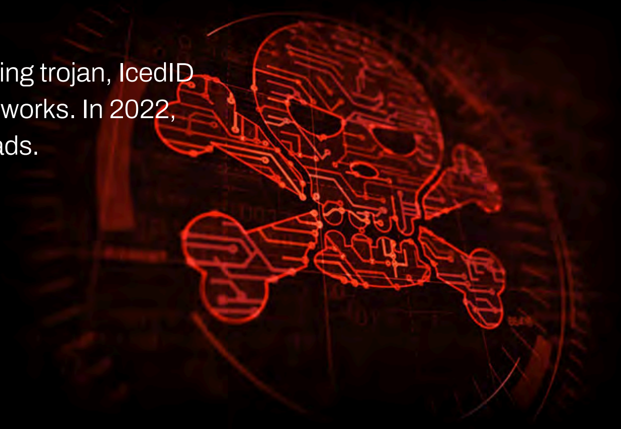
- Cybernews: Emotet is back from vacation
- Dark Reading: Emotet Rises Again With More Sophistication, Evasion
- Security Boulevard: VMware Research Uncovers Evolving Nature of Emotet Malware
- Bleeping Computer: Emotet malware attacks return after three-month break

QBot: First discovered back in 2009, QBot is a dangerous type of malware that's used to steal sensitive information, often banking details. In the fall of 2022, the malware was seen being delivered by attackers exploiting a zero-day exploit. In just over a week, QBot was found to have infected more than 1,800 users, with corporate users accounting for almost half of the victims.



Notable Coverage:

- Security Week: QBot Malware Infects Over 800 Corporate Users in New, Ongoing Campaign
- Dark Reading: QBot Expands Initial Access Malware Strategy With PDF-WSF Combo
- The Record: Hackers using Follina Windows zero-day to spread Qbot malware
- Infosecurity Magazine: Qbot Banking Trojan Increasingly Delivered Via Business Emails



IcedID (aka BokBot): IcedID got its start in 2017. Initially a modular banking trojan, IcedID is increasingly being used as a way to gain initial access into corporate networks. In 2022, attackers employed a range of new tactics to deliver their malicious payloads.

Notable Coverage:

- Bleeping Computer: Hackers behind IcedID malware attacks diversify delivery tactics
- Infosecurity Magazine: Three Variants of IcedID Malware Discovered
- TechTarget: Unit 42 finds polyglot files delivering IcedID malware
- MSSP Alert: New IcedID Malware Variants Broaden Attack Vectors

FluBot: Since its emergence in December 2020, FluBot has come to be considered the fastest growing Android botnet ever seen. In June 2022, an international law enforcement operation involving 11 countries took FluBot's infrastructure down.

Notable Coverage:

- The Hacker News: Widespread FluBot and TeaBot Malware Campaigns Targeting Android Devices
- Threatpost: International Authorities Take Down Flubot Malware Network
- Cyberscoop: Europol says it disabled FluBot botnet infecting 'huge' number of devices
- Bleeping Computer: FluBot Android malware targets Finland in new SMS campaigns

MaliBot: The successor of FluBot, MaliBot emerged—and received widespread recognition—in 2022. The malicious actors behind MaliBot initially targeted banking customers in Spain and Italy, though Android users around the world may be exposed.

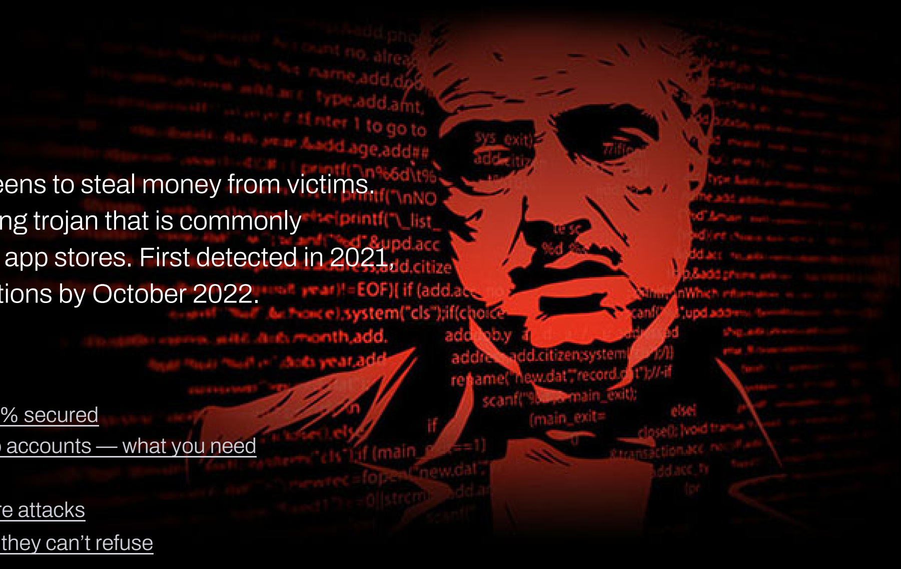
Notable Coverage:

- Computer Weekly: MaliBot Android malware spreading fast, says Check Point
- ZDNet: This new Android malware bypasses multi-factor authentication to steal your passwords
- Tech Republic: New Android banking malware disguises as crypto app to spread
- The Hacker News: MaliBot: A New Android Banking Trojan Spotted in the Wild

Hydra: Hydra is a banking trojan that targets Android devices. Through this malware, attackers trick users into granting dangerous permissions on their mobile devices. Once they've installed the malware, attackers can steal financial credentials. First discovered in 2019, Hydra grew to become the second-most common form of mobile malware by October 2022. (Source)

Notable Coverage:

- Bleeping Computer: Android malware on the Google Play Store gets 2 million downloads
- Krebs on Security: Actions Target Russian Govt. Botnet, Hydra Dark Market
- Computer Weekly: Hydra takedown merely shifts cyber criminal problem
- Bank Info Security: Hydra Aftermath: Where Do Criminals Lurk Now?



Godfather: Godfather malware employs fake login screens to steal money from victims. Godfather is the successor of Anubis, a malicious banking trojan that is commonly sideloaded, bypassing the security offered by legitimate app stores. First detected in 2021, Godfather had targeted more than 400 financial applications by October 2022.

Notable Coverage:

- Tech Wire Asia: Whether you use Android or iOS, no one is 100% secured
- Toms Guide: Godfather malware is draining banking and crypto accounts — what you need to know
- Reuters: German finance regulator warns of 'Godfather' malware attacks
- The Register: Godfather malware makes banking apps an offer they can’t refuse

Joker: Joker is stealthy malware that has been used to collect SMS messages and contact lists from infected devices. Additionally, Joker can conduct in-app purchases and subscribe to premium services without the victim’s knowledge. By June 2022, Joker had infected 50 Android applications, which received more than 300,000 downloads.

Notable Coverage:

- Laptop Mag: 'Joker' malware snuck into 50 Android apps — delete them before hackers cackle away with your data
- SC Magazine: Google removes Joker malware-infected apps
- Security Boulevard: Joker, Facestealer and Coper banking malwares on Google Play store
- Fast Company: These malware-infected apps for Android could secretly run up your phone bill

AgentTesla: AgentTesla is an advanced remote access trojan (RAT). Through this malware, attackers can collect a victim’s keystrokes, capture screenshots, and steal information. In the fall of 2022, AgentTesla was found to be one of the most widespread strains of malware, affecting 7% of organizations around the world. (Source)

Notable Coverage:

- Infosecurity Magazine: Advanced RAT AgentTesla Most Prolific Malware in October
- CSO Online: Malware builder uses fresh tactics to hit victims with Agent Tesla RAT
- Security Week: Three Nigerian Users of Agent Tesla RAT Arrested
- Digit.fyi: AgentTesla shakes education sector amid surge in malware attacks

State of Mobile Endpoint Security in 2023

Global Mobile Device Market

Worldwide, there were 7.1 billion mobile device users in 2021, and that number is expected to reach 7.5 billion by 2025.[10] Apple and Samsung continue to be the two smartphone vendors dominating the market. The number of unique mobile internet users increased to 5 billion, and over 60% of the global internet population uses a mobile device to go online.[11] Mobile internet traffic now accounts for nearly 60% of global web traffic, and the volume of data being consumed continues to grow.[12]

NUMBER OF GLOBAL SMARTPHONE USERS

7.1 BILLION

UNIQUE MOBILE INTERNET USERS

5 BILLION

MOBILE INTERNET TRAFFIC

60% OF GLOBAL WEB TRAFFIC

Mobile-powered Business Initiatives are Critical to Organizational Success

The surge in digital interactions has catapulted enterprises towards mobile-powered business models and the widespread move to support employees on their devices. With the continued proliferation of remote and hybrid workforces and BYOD policies, we have reached a tipping point for a new era of mobile ubiquity.

Enterprises had to adapt to a “get work done anytime and anywhere” mantra during the pandemic, which has made the need for mobile security more critical than ever. Mobile innovation has continued to make it easier for employees to collaborate, communicate, and access data, which is fueling increased productivity.

Mobile is the Modern Workplace

To get work done anywhere and anytime, employees are:

Adopting increasing volumes of mobile apps.
5.7 million apps are on the Google Play Store and Apple App Store combined. The average American has 80 apps downloaded on their phone.[13]

Collaborating with more people.
76% of respondents use smartphones for communicating, making it the top-rated response.

Seven in 10 individuals reported using mobile devices to send emails.[14]

Accessing a higher volume of data.
47% of web traffic in the US is from mobile devices.[15] 51% of smartphone users check their apps 1-10 times a day.[16]

For security teams, integrating mobile device telemetry into zero trust frameworks is critical to protect mobile-powered business models. Attacks are growing in volume and sophistication, as shown in this report. A zero trust approach has to be ingrained as a best practice throughout the modern workforce for both the user and the device. If a device that accesses critical business information isn't secured, one phishing link can lead to rogue access, or worse, ransomware for an enterprise.

Mobile Security Trends

Protecting mobile-powered businesses is difficult because mobile devices are an extension of people's lives, and apps are often the front door to risk. In the modern workforce, users are the administrators; therefore, vetting an app is easier said than done. An everyday user can't see beyond a privacy nutrition label. They do not know what countries or IP addresses are sharing their data or what third parties that data is being sold to.

Using unmanaged BYOD devices for work is continuing to trend upward.[17] This trend escalates the vulnerability gap because it leaves the door open for mobile threats, privacy concerns, and regulatory consequences. This is why there has been an ***upward trend in both private and public sector organizations banning social media and other apps*** that could potentially expose information for nefarious purpose. When an app is used for entertainment and yet exposes corporate data, something has to be done.

Device attestation is another approach that will continue to be at the forefront of mobile security as business and personal apps present increased risk. Mobile devices are being used more and more for authentication purposes, such as MFA, to validate users' identities. However, 2022's headline attacks, like the one that led to a breach at Uber,[18] amply demonstrate that MFA can be susceptible to compromise, which is why data attestation is critical for a mobile-first strategy. As RSA's Chief Product Officer, Jim Taylor explained earlier in this report, RSA has elevated data attestation with RSA Mobile Lock. It detects critical threats to a mobile device and restricts the user's ability to authenticate until the issue is resolved.

To say that mobile security is now critical is an understatement. That's why more extended detection and response (XDR) platform vendors are integrating mobile protection—mobile threat defense (MTD)—into their offerings. This integration offers visibility and orchestration. The enriched threat intelligence these integrated solutions provide enables security teams to improve threat hunting, logistics, and intelligence feeds. Further, it allows them to see new threats they could not detect with traditional endpoint detection tools.

Evolving Mobile Threat Landscape

Enterprise security teams are trying to protect the business' mobile-powered initiatives. This means they must contend with competing demands for securing mobile devices while ensuring users have frictionless, productive experiences. As cyberattacks are increasing in volume and sophistication, security teams around the globe must stay up to date with the latest threats to provide comprehensive protection to their offices, employees, network, and more. Below are just a few of the mobile threats that need to be addressed.

Ransomware Attacks Targeting Mobile Devices

Ransomware profits may be down by 40%, but the activity has not slowed down. Ransomware groups extorted nearly $456.8 million in 2022, which was a significant decrease from the prior year when criminals netted $766 million.[19] 2022 was the most active year in ransomware activity, with thousands of file-encrypting malware strains targeting companies of all sizes.[20] Interestingly, ransomware attacks targeting mobile devices have risen and continue to threaten mobile security. In 2022, Zimperium detected 17,000 unique ransomware samples and protected organizations against over 90,000 attacks.

Top 3 Sectors Hit By Ransomware[21]

Healthcare and Public Health
Critical Manufacturing
Government Facilities

Business email compromises accounted for an adjusted loss of over

$2.7 billion[24]

Phishing Targets Mobile Devices

According to the FBI Internet Crime Report 2022, phishing has remained the top internet crime for the past five years.[22] The increase in phishing scams targeting mobile devices is a significant security threat.

Last year's Zimperium Global Mobile Threat Report revealed that, between 2021 and 2022, the percentage of phishing sites targeting mobile devices increased from 75% to 80%. According to one report, phishing affected more than 300,000 individuals worldwide, and those were only the number of incidents that were reported.[23]

The Risks of Mobile Spyware

Mobile devices require an internet connection in order to obtain full productivity, making them the perfect host for spyware. Spyware can be used to secretly monitor a user's activity along with keystrokes, internet usage, and sensitive data and can take control of a device without the user's knowledge. This can be dangerous to the individual and risky for an employer. In 2022, Zimperium detected over 3,000 unique spyware samples.

The Need for Mobile-First Security

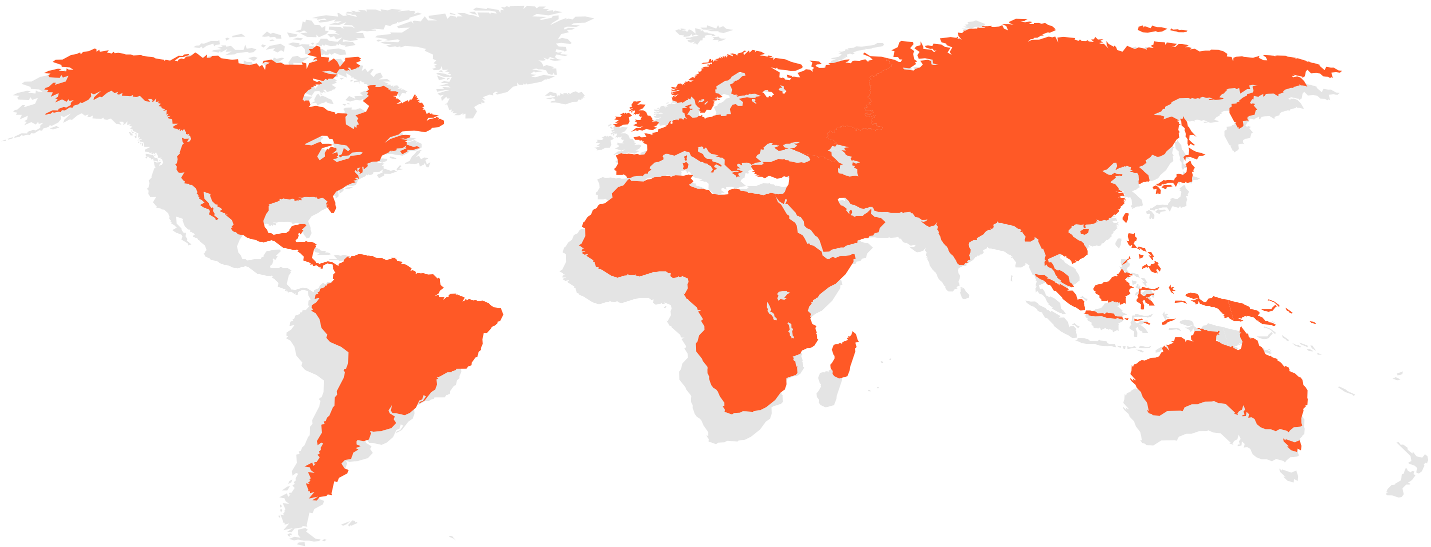
The increased number of attacks, combined with escalating usage of mobile devices and apps, has significantly elevated the need for mobile security. The data in this report demonstrates that mobile threats are increasing and becoming more sophisticated. As stated earlier, this report is not intended to create fear, but to offer instructive insights into the threats that Zimperium is seeing in the wild so security teams can better understand and adapt to the landscape. The goal is to provide helpful information to organizations as they attempt to build out a Mobile-First Security Strategy.

State of Mobile Application Security 2022

The use of mobile apps is becoming increasingly widespread within global businesses due to their ability to increase productivity and accelerate business growth. The proliferation of smartphones, improved internet connectivity, and the need for convenient access to information and services have contributed to the significant adoption of mobile apps by businesses.

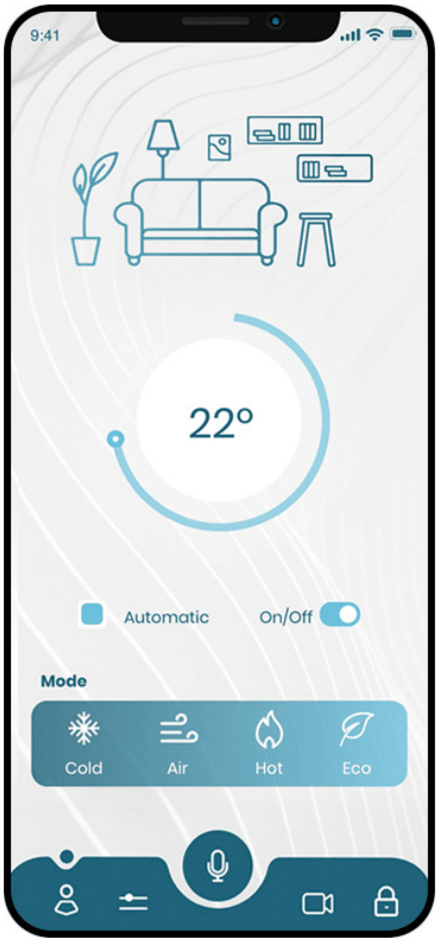
Mobile apps are widely used across various industries and regions worldwide. Among the areas and regions where mobile apps are most prevalent in global businesses are:

- **North America:** The North American mobile app ecosystem is highly developed in the United States and Canada. North American companies use mobile apps for customer engagement, e-commerce, enterprise mobility, and industry-specific apps.
- **Europe:** Global businesses have adopted mobile apps in many European countries, including the United Kingdom, Germany, France, and the Nordic countries. Apps are used for consumer-centric services such as digital banking, transportation, and healthcare.
- **Asia-Pacific:** Mobile app usage has seen exponential growth in the Asia-Pacific region, particularly in China, India, Japan, and South Korea. Social media, e-commerce, ride-sharing, and food delivery are all areas where mobile apps are prevalent.
- **Latin America:** Brazil, Mexico, Argentina, and Colombia have adopted mobile apps across various industries, including e-commerce, transportation, financial services, and communication. In the region, mobile apps allow businesses to reach large and growing consumer markets.
- **Middle East & Africa:** There is a rapid expansion of mobile app usage in the Middle East and Africa. Businesses in sectors such as e-commerce, fintech, transportation, and healthcare are leveraging mobile apps to capitalize on the region's growing digital economy.



Evolution of Mobile Applications

In recent years, mobile apps and mobile app development have continued to evolve and change rapidly, driven by advances in technology and changes in user behavior. Here are some of the notable trends and developments in this space:



Increased demand for mobile apps: During the pandemic, people started to rely on mobile apps for a range of activities, from remote work and learning, to socializing and entertainment. This pattern continues today, resulting in an increase in demand for mobile apps across different industries.

More emphasis on app security: As more mobile apps handle sensitive data, app security has become a top priority for developers. To prevent cyberattacks and data breaches, developers are implementing more robust security measures, such as two-factor authentication, encryption, and biometric authentication.

Rise of low-code and no-code app development: Low-code and no-code app development platforms have gained popularity, making it easier for non-technical individuals to create simple mobile apps without extensive coding knowledge. These platforms often include drag-and-drop interfaces, pre-built templates, and easy integration with other tools and services.

Continued dominance of Android and iOS: Android and iOS continue to dominate the mobile app market, with most mobile app development efforts focused on these platforms. However, other platforms, such as Flutter and React Native, have gained popularity as developers look for cross-platform development solutions.

How Mobile App Protection is Different

Securing mobile apps differs fundamentally from securing web and desktop apps. Here are some of the key differences between the two:

Easy access to app code: As soon as mobile apps are put in the app store, attackers have easy access to the code. Web apps run on corporate servers, so attackers cannot easily access the code.

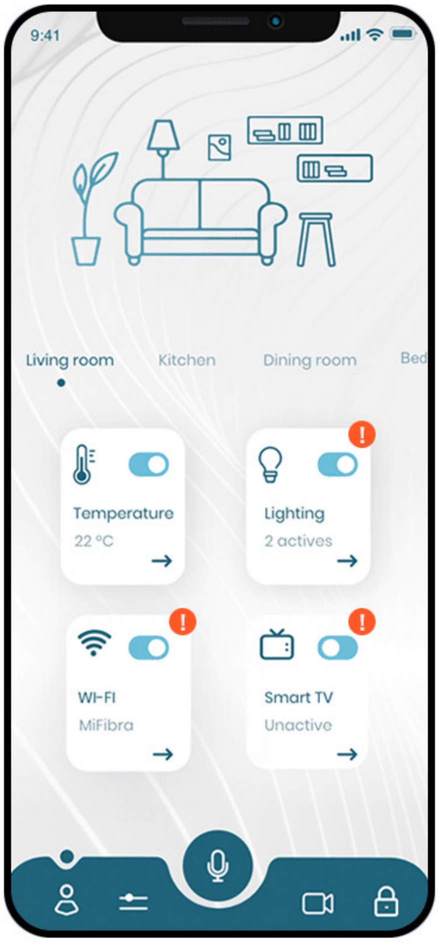
Run outside the perimeter: Most mobile apps run on devices that are outside the control of the enterprise that has produced them. As a result, the organization's risk is significantly higher since the app is exposed to several attack vectors on the device.

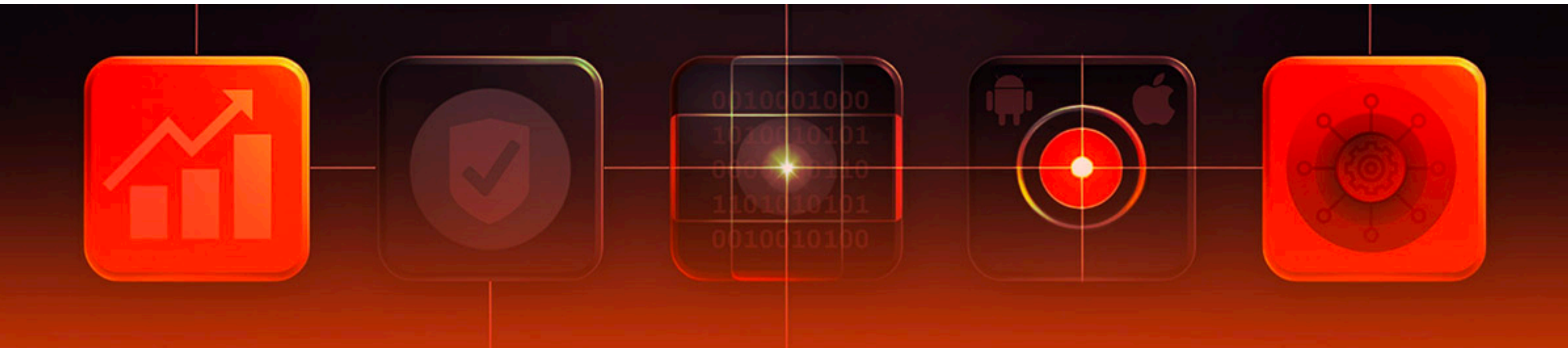
Different exposure points: Mobile apps are typically installed on devices and have access to device resources, such as cameras and GPS, while web apps run in a browser and have access to web resources, such as cookies and HTTP headers. The different exposure points associated with each type of application give rise to different security risks.

Platform-specific issues: Mobile apps are developed for different mobile operating systems, such as iOS and Android, each with their own unique security challenges. The OWASP Top 10 for Mobile, as well as MASVS, take these platform-specific issues into account.

Different programming languages: Mobile apps may be developed using different programming languages than web apps. For example, mobile apps may be developed using Java, Swift, or Kotlin, while web apps may be developed using JavaScript, PHP, or Python. This can create different vulnerabilities and risks.

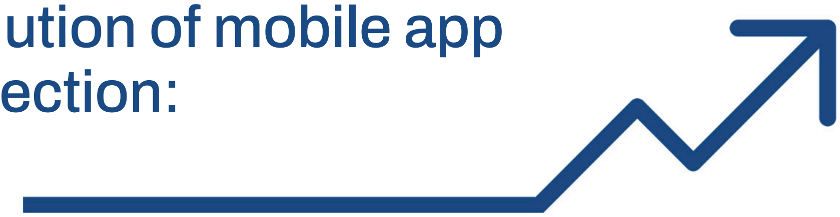
Differences in device security: Mobile devices may have different security mechanisms than web browsers, such as biometric authentication or secure enclaves. These differences can create unique security challenges for mobile apps.

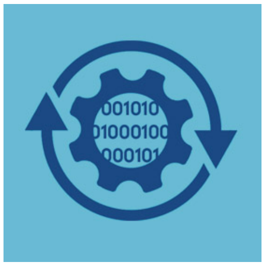




Mobile App Protection is Evolving

Here are the top 5 trends in the evolution of mobile app protection:

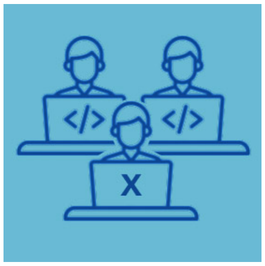




Constantly Evolving Reverse Engineering Technology

Reverse engineering via techniques like hooking, scripting, and hiding techniques remains a real concern for app developers. While the development of reversing technologies offers opportunities for innovation, it poses challenges for enterprises relying on security solutions. The cat-and-mouse game between attackers and security solutions often renders detecting and blocking techniques outdated by the time they are deployed, leaving enterprises vulnerable to sophisticated attacks.

To address this challenge, security solution providers need to conduct internal research and rapidly deploy fixes to stay ahead of evolving evasion techniques or deploy proactive tools which address the methodologies used by reversers. Ideally, these fixes should seamlessly integrate into existing solutions without requiring an enterprise to re-apply and redeploy apps.



Shortage of Security Engineers

The shortage of security engineers has significant implications for organizations. Due to the perception of reverse engineering as a concerning field associated with hackers, and the limited emphasis on low-level skills in universities, the security engineer shortage is often filled by individuals who develop a personal interest or evolve from amateurs. As a result, in-house security engineers, particularly during the design stage, may lack the necessary understanding of security needs, leading to the absence of security requirements in app designs. Moreover, the scarcity of skilled professionals leads to a heavy reliance on outsourcing security assurance, which can be expensive and is often neglected. App teams may resort to reactive security responses, addressing security issues only when they manifest rather than taking a proactive approach. Overall, the shortage of security engineers hampers the integration of security measures throughout the development lifecycle and may result in compromised security practices within organizations.

The Evolution of SecDevOps in Mobile Application Development

SecDevOps has evolved in mobile app development through the integration of mobile-specific security tools, increased adoption of mobile-focused security testing practices, incorporation of privacy and compliance considerations, implementation of secure continuous integration/continuous delivery/deployment (CI/CD) pipelines, utilization of mobile threat intelligence and monitoring, and emphasis on security education and awareness within development teams. These advancements have strengthened the overall security of mobile apps and enhanced the integration of security practices throughout the mobile SecDevOps workflow.

But SecDevOps in mobile app development still faces several challenges. These hurdles include a lack of mobile-specific security expertise, the fragmented mobile ecosystem with diverse platforms and device variations, balancing usability with security measures, managing third-party dependencies, limited availability of comprehensive security tools for mobile apps, and ensuring compliance with regulatory requirements. Achieving success requires investing in mobile-specific security tooling, expertise, testing methodologies, and security practices early in the development process and fostering collaboration between development, operations, and security.

The Proliferation of Supply Chain Attacks

Supply chain attacks in mobile apps are rampant across various areas within the mobile app ecosystem. Attack vectors include compromised third-party libraries and SDKs, malicious apps in official app stores, compromised ad networks, vulnerabilities in over-the-air (OTA) updates, tampered development tools, and many others.

These attacks are particularly effective in the realm of mobile apps due to several key reasons. First, there is a high level of trust and legitimacy associated with components within the mobile app supply chain, such as third-party libraries, app stores, and ad networks, making it easier for attackers to infiltrate and compromise them. Additionally, the widespread distribution of mobile apps increases the potential impact of supply chain attacks, as they can affect a large number of devices. The complex and interconnected nature of the mobile app ecosystem also makes it challenging to detect such attacks, as compromised components can appear genuine and evade automated security checks.

Supply chain attacks are made more effective by exploiting common development malpractices and the dynamic nature of mobile apps. It is essential to implement robust security measures, thoroughly vet third-party resources, and vigorously monitor the supply chain to mitigate these risks.

The Hybrid Applications

Hybrid apps have emerged in an attempt to address the challenge of building a single app for iOS and Android platforms using a single codebase. The goal of hybrid apps is to provide a cost-effective solution that abstracts the platform differences as much as possible. Previously, frameworks like Xamarin and React Native gained popularity for developing hybrid apps. However, the landscape has evolved, and now Flutter, with its Dart programming language, has gained significant traction. Their popularity has led to a larger pool of developers skilled in using these frameworks. They have extensive documentation, active communities, and resources available, making it easier for developers to learn and master hybrid app development techniques.

How Is The Mobile App Security Landscape Changing?

Mobile application security threats are constantly evolving due to advancements in technology, evolving attack techniques, and the expanding landscape of mobile apps. Here are some ways in which mobile application security threats are changing:

- **Sophisticated Malware:** Malicious apps targeting mobile devices have become increasingly sophisticated. Attackers use techniques like obfuscation, code injection, and encryption to hide malware within mobile apps. Advanced malware can bypass security measures, steal sensitive information, hijack devices, or gain unauthorized access to resources.
- **Application Vulnerabilities:** Vulnerabilities in mobile apps are a significant security concern. Attackers exploit coding errors, insecure data storage, weak authentication mechanisms, and inadequate encryption, to name a few, in order to gain unauthorized access or manipulate the app's functionality. Code scanners focus on syntax and semantics, which is a good start, but you need a mobile-focused security scanner that helps identify areas of abuse and exploitation.
- **Mobile Device Exploitation:** Mobile devices themselves can be vulnerable to security threats. Attackers may exploit device vulnerabilities, operating system weaknesses, or unpatched software to gain control over a device. This can lead to unauthorized access to data, device tampering, or the installation of malicious apps.
- **Poor Cloud Storage Configurations:** Improper cloud storage configurations in mobile apps can make them insecure. Inadequate access controls, misconfigured security settings, lack of data encryption, insecure data transfer, mismanagement of security credentials, and the failure to monitor and detect anomalies are some of the key issues.
- **Fake Mobile Apps:** Fake mobile apps are a real problem that can lead to malware distribution, financial fraud, data theft, brand impersonation, user safety risks, and challenges for app store ecosystems.
- **Third-Party App Stores:** Third-party app stores pose risks to mobile app security due to their lack of stringent security screening, increased likelihood of hosting malicious or counterfeit apps, limited app review and monitoring, slower security updates, and a lack of user awareness.

14%

of mobile apps using cloud storage were vulnerable due to unsecured configurations

Several of these will be covered in more depth in later sections of this report.

How Are Industry Standards and Regulations Adapting?

Regulation is evolving to adapt to the growing presence and impact of mobile apps. Here are some ways in which regulation is changing to address mobile apps:

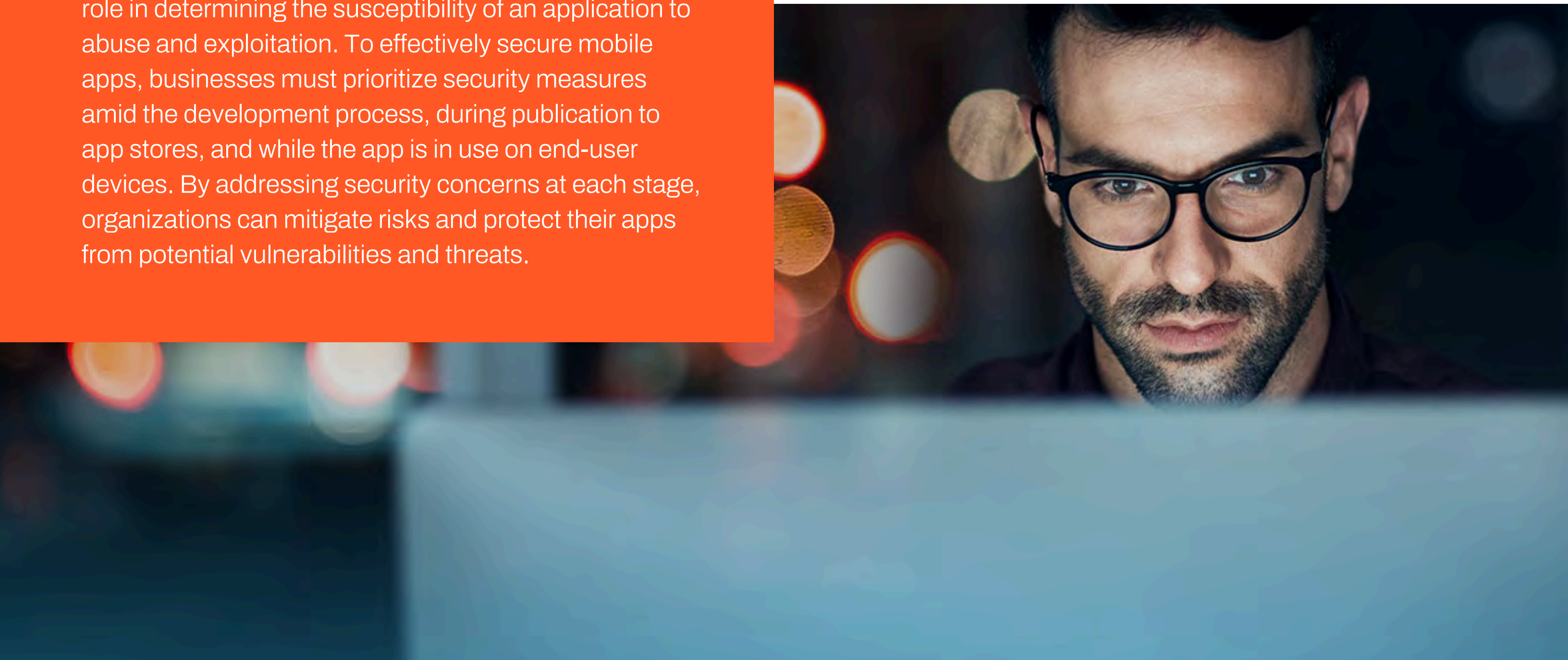
Privacy and Data Protection: With the increasing collection and processing of personal data by mobile apps, regulations like the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States have been enacted to protect user privacy. These regulations impose requirements on how personal data is collected, used, stored, and shared by mobile apps, as well as mandate transparency and user consent.

Mobile Payment Regulations: As mobile apps increasingly facilitate financial transactions and digital payments, regulatory bodies have developed frameworks specific to mobile payments. Standards like Mobile Payments on COTS (MPoC) aim to ensure the security, integrity, and transparency of mobile payment systems, protect consumer interests, and combat fraud and money laundering.

Government Directives: Governments and regulatory bodies are emphasizing the security of mobile apps to protect users and mitigate risks. Cybersecurity measures, such as secure data storage, encryption, authentication mechanisms, and vulnerability management, will soon become mandates under directives such as the NIS2 and the FDA's Consolidated Appropriations Act, 2023 (Omnibus).

Industry Standards: The National Institute of Standards and Technology (NIST) and the Open Worldwide Application Security Project (OWASP) play a crucial role in improving mobile app security. In order to enhance the security of mobile apps, NIST provides guidelines, standards, and best practices. The Mobile Top 10 and Mobile Application Security Verification Standard (MASVS) published by OWASP help mobile application developers build secure mobile apps. The OWASP compliance of mobile apps will be discussed in more detail in a later chapter.

The risks associated with mobile apps can be attributed to three key actors: developers, malicious actors, and end-users. Each of these stakeholders play a significant role in determining the susceptibility of an application to abuse and exploitation. To effectively secure mobile apps, businesses must prioritize security measures amid the development process, during publication to app stores, and while the app is in use on end-user devices. By addressing security concerns at each stage, organizations can mitigate risks and protect their apps from potential vulnerabilities and threats.



The Continued Rise of Mobile-Specific Phishing

The Scope of the Problem

Phishing is one of the most common forms of cyberattack. At some point, virtually anyone with a laptop or mobile device will be targeted. Here are just a few statistics that underscore the scope of the problem posed by phishing:

- The Anti-Phishing Working Group (APWG) reported more than 1.2 million phishing attacks during the third quarter of 2022 alone.[25]
- During 2022, a single employee in the retail industry received an average of 49 phishing emails.[26] (This doesn't include all the phishing messages an employee may receive via SMS.)
- 74% of all data breaches include some human element, such as social engineering, highlighting the persistent threats posed by phishing.[27]
- Phishing remains the top reported internet crime, according to the FBI Internet Crime Report 2022, for the past five years.
- Per the FBI crime report, it is estimated that in the US, there were over 300,000 people who have fallen victim to phishing attacks.[28]

As security controls and cyber defense techniques increasingly focus on detecting and mitigating email-based phishing risks, threat actors have devised new attack vectors to target mobile devices. These new attack vectors aim to exploit instant messaging apps, SMS, and even fake QR codes.

Key Takeaways

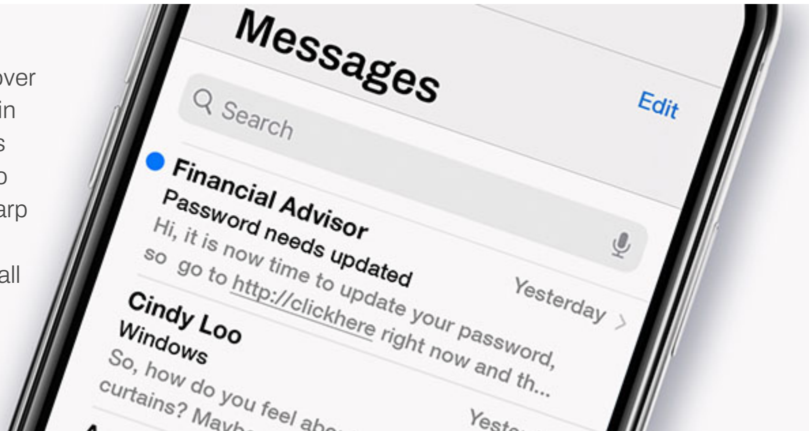
Here are the key takeaways associated with mobile phishing in the last year:

- The average user is 6-10 times more likely to fall for an SMS phishing attack than an email-based attack.
- 80% of phishing sites now either target mobile devices specifically or are designed to function on both mobile and desktops.
- The financial services sector accounts for the highest percentage of phishing attacks.
- Microsoft Office is one of the top productivity apps across several regions, underscoring the direct and significant risk phishing poses to businesses.

In the following sections, we examine these and other key findings in more detail.

For example, due to its convenience, ubiquity, and frequency of use, SMS is a rapidly growing attack vector for today's threat actors who are targeting mobile devices (via phishing or smishing) through the SMS protocol. While most users recognize the threat posed by email-based phishing, they often lack an understanding of mobile phishing via SMS and its associated dangers.

Mobile phishing using SMS gives threat actors significant advantages over the use of email phishing. Traditional anti-phishing solutions are in-line in corporate email and are blind to mobile phishing attacks. Data indicates that people are more likely to click links in SMS messages. According to **Constant Contact**,[29] emails have an average click rate of 1.33%. In sharp contrast, according to **Klaviyo**,[30] SMS click rates are between 8.9 to 14.5%. That means that the average user is 6-10 times more likely to fall for an SMS phishing attack than an email-based attack.

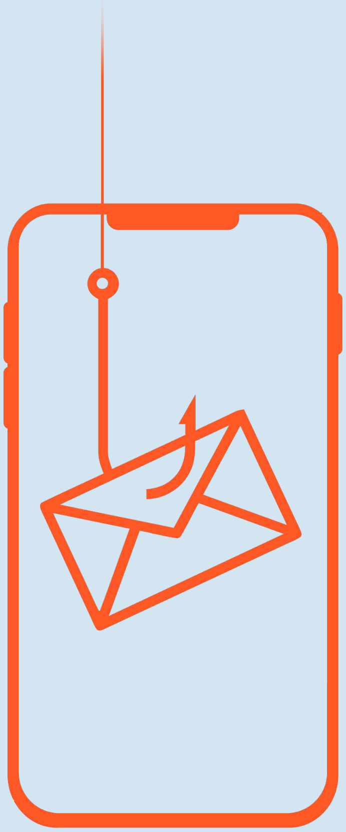


Financial Advisor
Password needs updated
Yesterday
Hi, it is now time to update your password, so go to http://clickhere right now and th...

Cindy Loo
Windows
So, how do you feel abo
curtains? Mayb
Yeste

Users Fall for Mobile Phishing… Period

Simply put, mobile phishing works. The average user will tell you that they receive many phishing texts and emails, but that they never fall for them. Zimperium data says otherwise. During 2022, Zimperium detected an average of four malicious/phishing links clicked for every device covered with its anti-phishing technology.



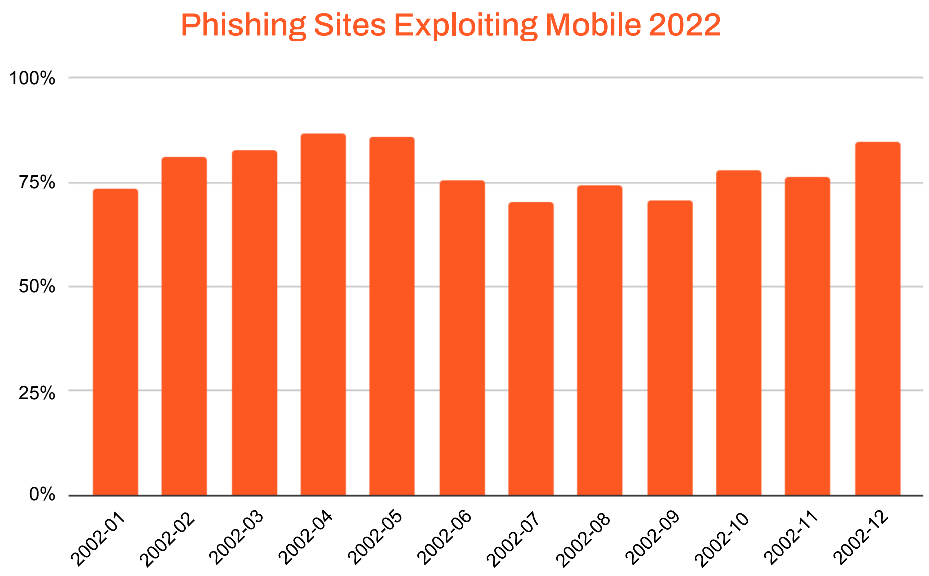
The Ubiquity of Mobile-Focused Attacks

Last year's report outlined how it was becoming increasingly common for phishing sites to employ code that could adapt to the functionality of specific mobile platforms. This trend of mobile-specific phishing continued in 2022. In 2021, 75% of the phishing sites Zimperium examined specifically targeted mobile devices and delivered content appropriate for the mobile format. In 2022, that number grew to 80%.

This move to mobile-focused attacks has been enabled by modern web development tools. These frameworks enable developers to produce a single website that can be rendered effectively on any platform.

In some cases, attackers aren't going after multiple platforms; they're focusing solely on mobile devices. For instance, many examples of malware have been uncovered that expressly don't function unless they are accessed by a mobile device. The assumption from Zimperium researchers is that attackers know traditional endpoints are more likely to have security safeguards. Further, the form factors and interfaces of mobile devices can make it more difficult for users to spot the signs of a phishing site.

The chart below depicts the number of phishing sites exploiting mobile devices.

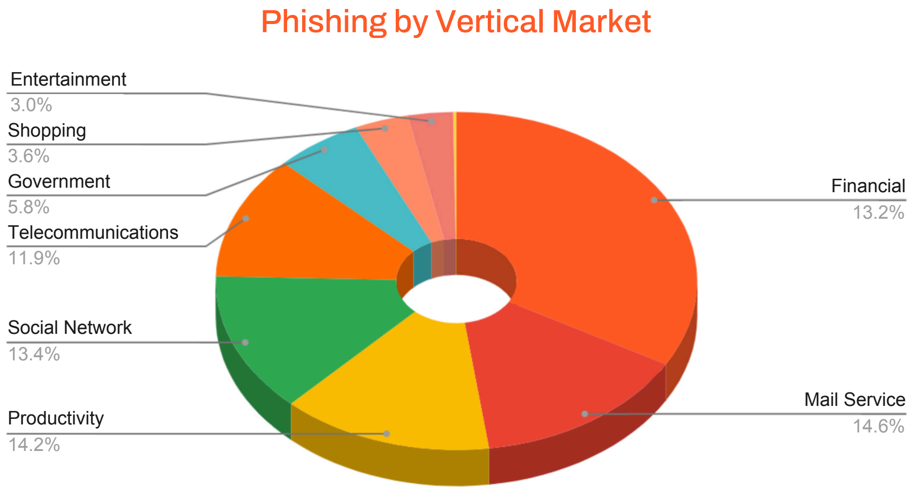


Phishing by Industry

Based on the Zimperium threat data, the single most targeted market is finance. When you consider most phishers are after money, it makes perfect sense that this remains an area of focus. Through a successful attack, phishers can quickly pursue tactics that can yield an immediate payoff. The data Zimperium has gathered is aligned with that of the Anti-Phishing Working Group (APWG), which also reported that financial services is the most targeted sector, accounting for 23% of all phishing attacks they documented.[31] In context, financial services firms have been targeted 60% more than the next most targeted sector.

Another common theme is the use of postal services and express shippers. While a subset of the population will work with any given bank, a majority of individuals use the postal service and express shippers. Targeting the everyday use of these common services allows phishers to cast a very broad net.

The rate of phishing in the financial service and mail service markets is followed closely by the productivity, social networks, and telecommunications markets.



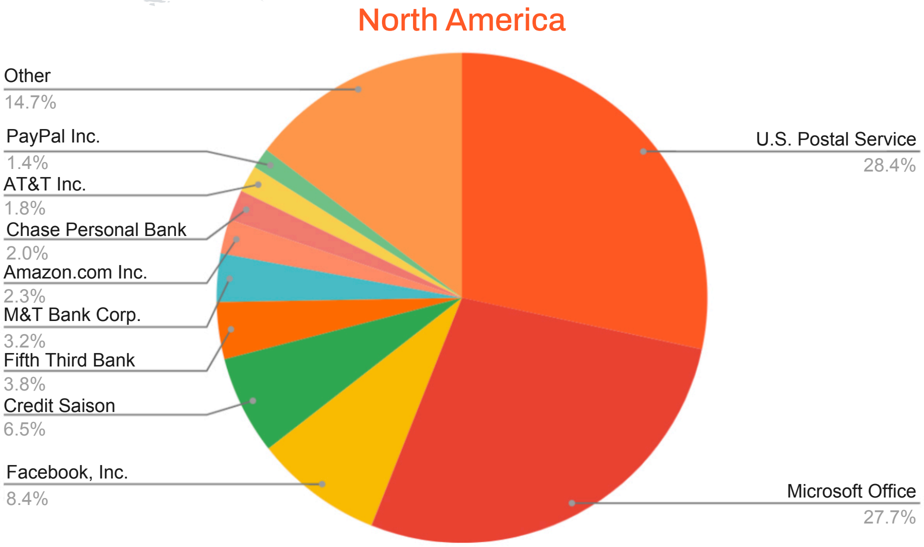
The Most Phished Brands, Globally

Zimperium continues to analyze phishing data by commonly targeted brand names across various regions. The most recognizable brands are targeted as phishers look to exploit the trust and familiarity consumers have with those organizations.

When you consider that some of these themes continue year-over-year, this data offers insights into what has been working well for phishers. Within this context, the continued frequency of Microsoft's appearance in this data should raise alarm bells for corporate security teams. For the past few years, Microsoft has consistently been featured, and for 2022, it's one of the top targeted brands in North America, EMEA (which includes Europe, the Middle East, and Africa), and APAC (Asia-Pacific). By duping victims into divulging credentials for corporate email services like Microsoft Outlook, phishers can pose a significant threat not only to employees but also to the corporations that employ them.

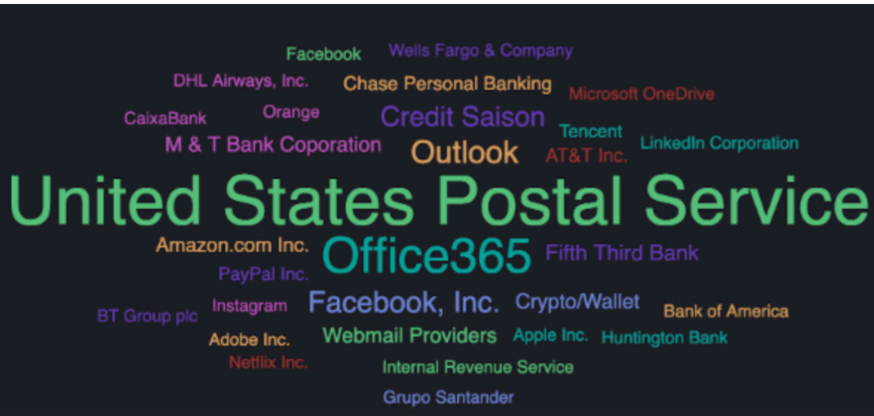
Those waging phishing attacks tailor their techniques to the region in which they're operating. That results in a very different makeup of brands being phished across different regions. The sections below offer a look at the targeted brands by region.

North America

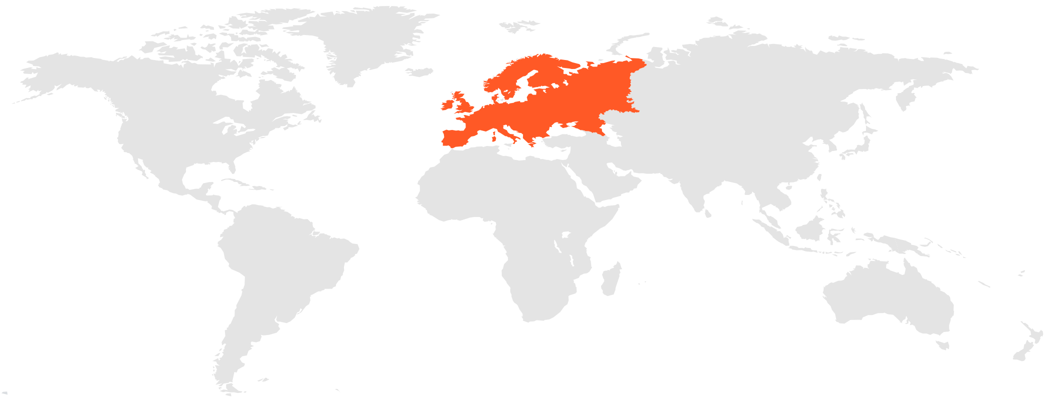


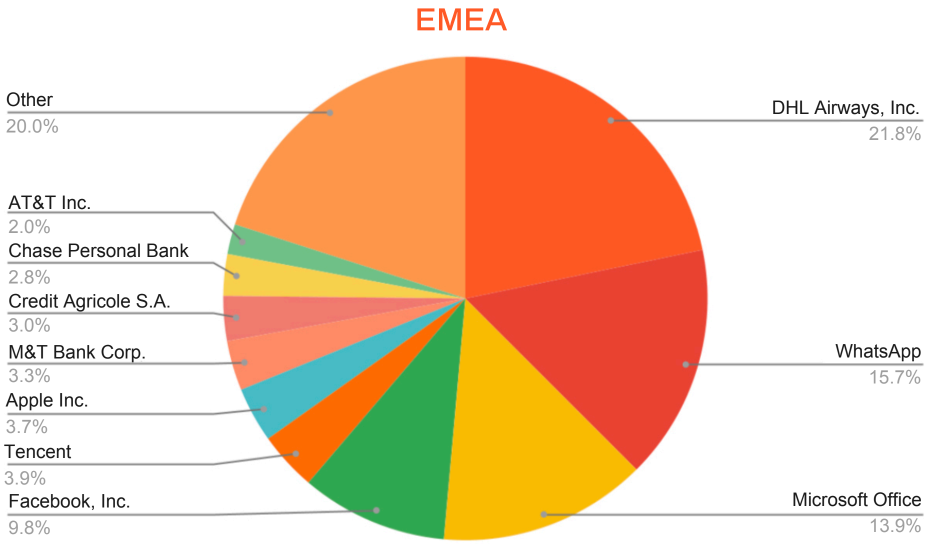
In 2021 and 2022, Microsoft appeared in almost one-third of phishing attacks (29% and 27.7%, respectively). In 2021, the U.S. Postal Service wasn't reflected in the top 10 brands targeted, but for 2022, it emerged as the most-targeted brand, taking over Microsoft's spot.

It's interesting to note the use of Facebook dropped from 20% to 8.4%. This is likely because of the large increase in the USPS sites and not a drop in those from Facebook. Familiar names from last year's report - including Amazon, AT&T, PayPal, and Chase - were also reflected in the data for 2022. New brands for this year are Credit Saison (6.5%), M&T Bank (3.2%), and Fifth Third Bank (3.8%). DHL Airways, Orange, and Tencent appeared in 2021 but dropped off this year's list.

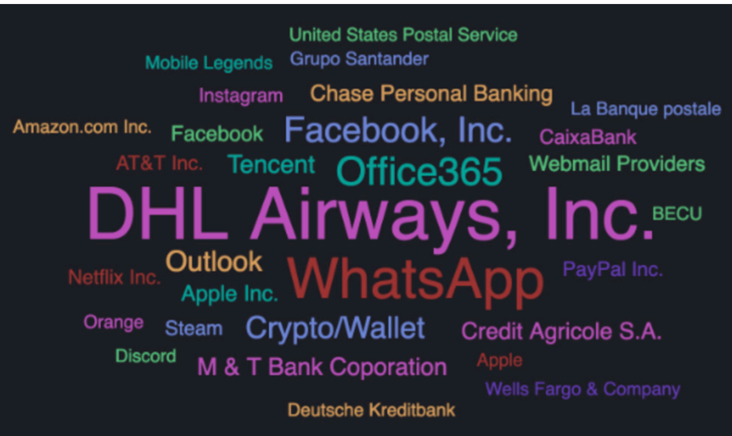


EMEA

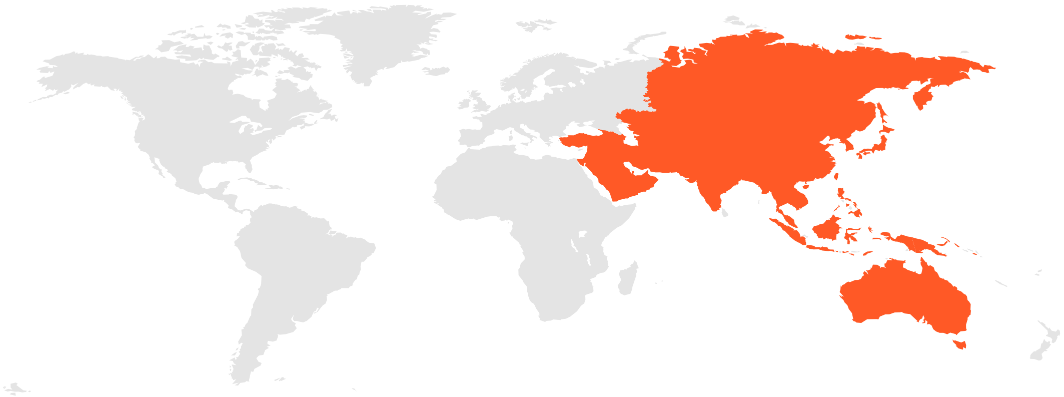


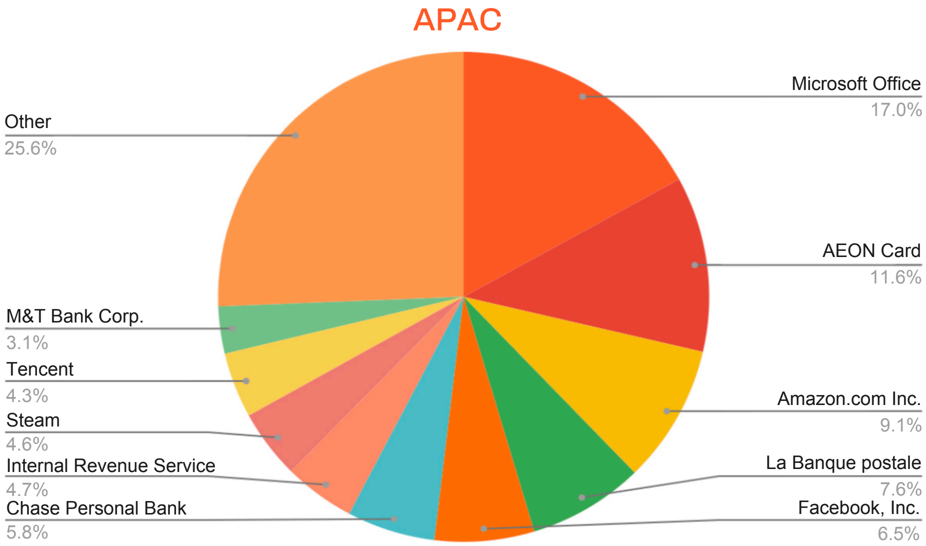


Between 2021 and 2022, Facebook dropped from the dominant spot. While it accounted for 45% of activity in 2021, that number fell to 9.8% in 2022. Microsoft was one of the top brands in both 2021 and 2022. While not featured in the top 10 last year, DHL Airways (21.8%) and WhatsApp (15.7%) brands were both used in a significant percentage of attacks. Also new to this year's top brands are AT&T, Credit Agricole, Apple, and Tencent.

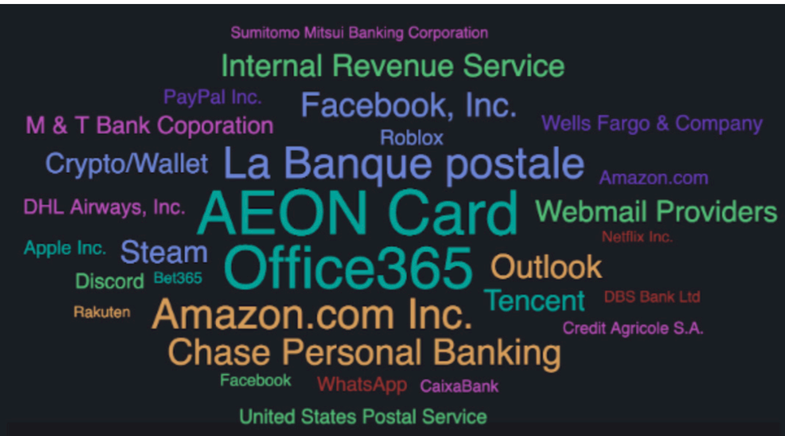


APAC

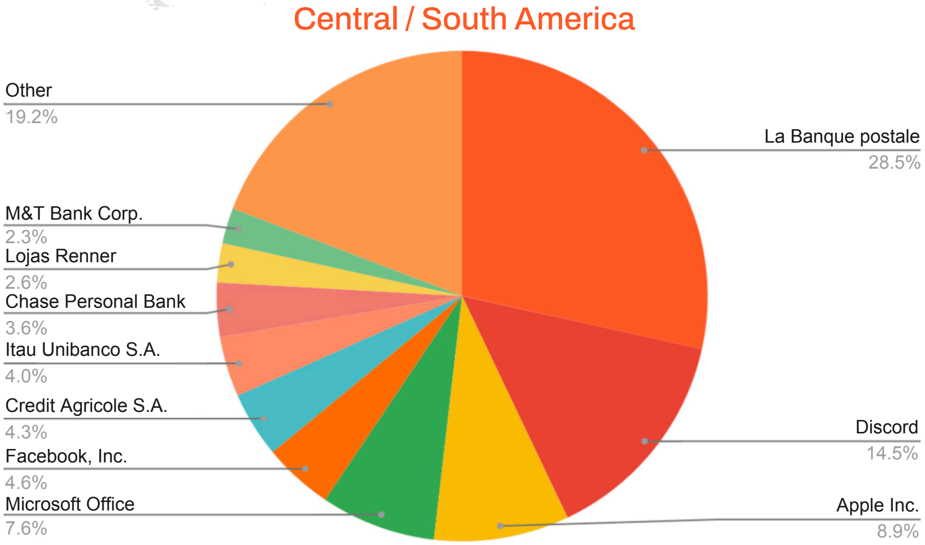




The Microsoft brand moved from third to first in usage, growing from 9.3% in 2021 to 17% in 2022. AEON Card (11.6%) and La Banque Postale (7.6%) are newly added and made up a significant percentage of attacks. Amazon, Chase, Facebook, and Steam were all brands that appeared in the top 10 for both years.

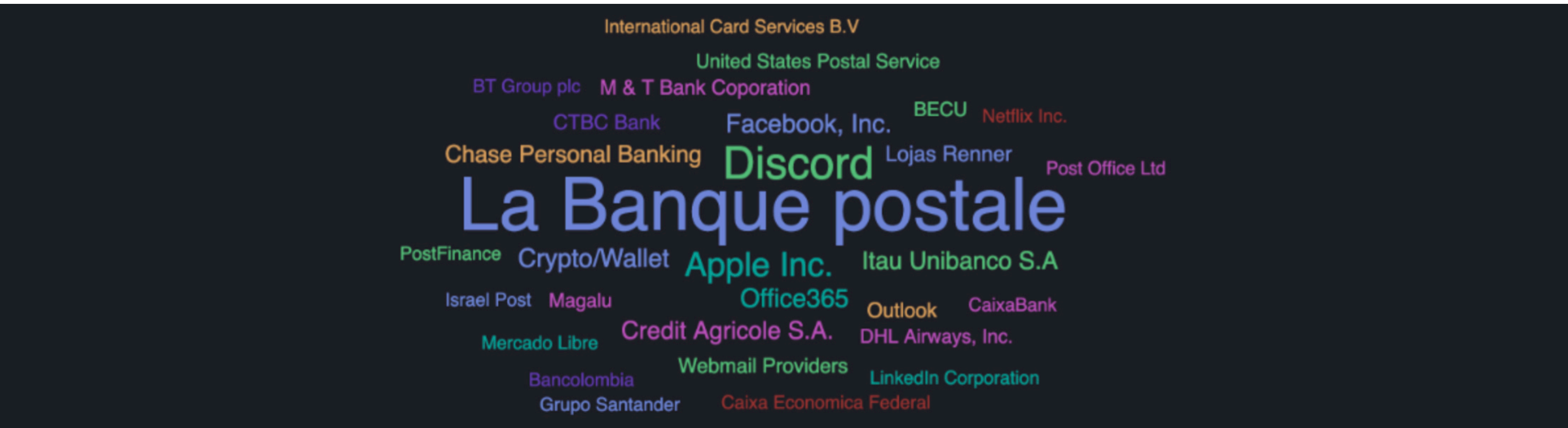


Central and South America



La Banque Postale grew from 10.7% in 2021 to the most attacked brand in 2022, accounting for almost one-third (28.5%) of phishing attacks. New on the list this year, Discord emerged in the second spot with 14.5%. Chase, Credit Agricole, and Itau Unibanco were among the names that appeared in the top 10 for both years. Between 2021 and 2022, Facebook dropped from 11.7% to 4.6%, and Microsoft dropped from 11% to 7.6%.

All of these findings reinforce the need to have proactive, dynamic detection of mobile phishing since the brands, campaigns, and techniques vary by region and over time.



Mobile Malware: Evolving Attacks, Expanding Risks

Key Takeaways

Here are the key takeaways associated with mobile malware in the last year:

- Between 2021 and 2022, the total number of malware samples detected increased by 51%.
- In 2021, Zimperium detected malware on 1 out of 50 Android devices. That number increased significantly in 2022 to 1 out of every 20 devices.
- Zimperium protected its customers from 2,000 samples each week that were not yet identified by the industry in general ("zero-day" malware).
- 23% of all Android samples and 24% of iOS samples submitted to public application repositories were malicious.
- Malware developers are constantly trying to find ways to avoid detection. The use of multi-platform development frameworks and tools by malware developers makes it increasingly difficult to determine the level of maliciousness, thereby presenting a more significant challenge for security analysts to detect and mitigate potential threats.

The following sections examine these and other key findings in more detail.

The Evolving, Expanding Threats Posed by Malware

Malware poses a significant risk to any organization regardless of geography or industry. Without strong, dynamic detection abilities, compromised mobile devices can leave sensitive services and assets exposed.

Whether a device is corporate-owned or personal (BYOD), the majority of mobile devices now contain both personal and corporate data and apps. As employees frequently use their phones for work purposes, the risks of a compromised device extend beyond the device itself. Malware today is specifically designed to evade detection and gain access to targeted assets, including controls and data on the device, as well as corporate assets accessed by those devices.

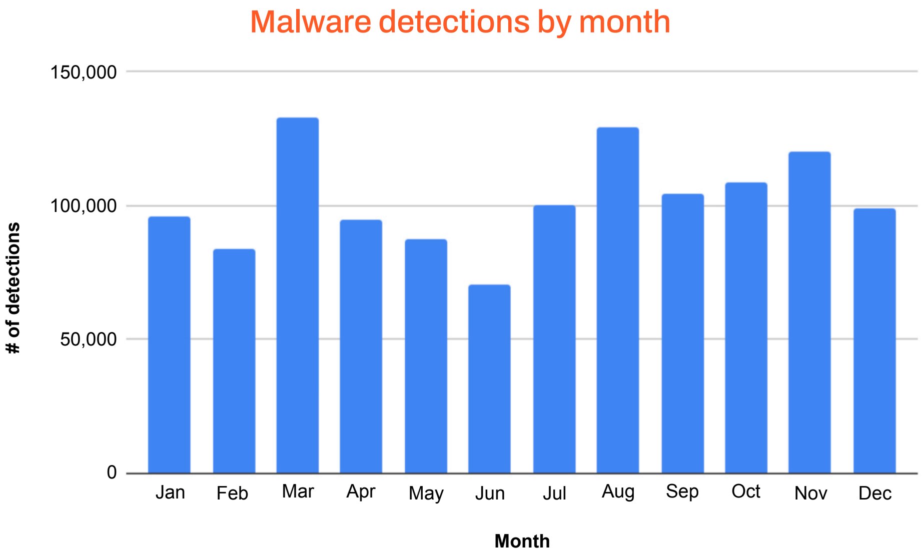
While enterprise security teams may institute VPNs, firewalls, multi-factor authentication, and more, the reality is that any security framework is reliant upon a number of elements. Ultimately, the security chain is only as strong as the weakest link. Often, that weak link is posed by users, who are susceptible to inadvertently taking risky actions such as clicking on malicious links. Additionally, users may not be aware of the potential risks both during and after an attack. Malicious actors are well aware of this reality, which is why they commonly focus on duping mobile device users into downloading a malicious app or divulging sensitive details like login credentials.

By targeting employees' mobile devices, malicious actors can gain access not only to personal and financial data on the device but also to multi-factor authentication mechanisms, business apps, corporate data stores, and more.

Volume of Malware Samples Discovered

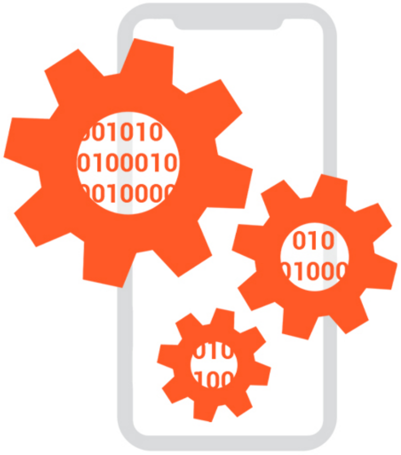
During 2022, an average of 77,000 unique malware samples were discovered each month. For the year, 925,000 unique malware samples were detected, up from 611,000 in 2021, which represents a jump of 51%. While these samples are often variants of known malware families, they are distinct in some way. This illustrates the level of persistence and effort being put forth by malware developers and how this activity keeps proliferating.

Given the increase in mobile malware detected, it should come as no surprise that more devices were impacted in 2022 than the previous year. In 2021, Zimperium detected malware on 1 out of 50 Android devices. That number increased significantly in 2022 to 1 out of every 20 devices.



In March 2022, Zimperium detected 132,000 samples, making it the highest-volume month. June represented the month with the fewest number of detections at 71,000.

In 2022, Zimperium protected its customers against 2,000 malware samples weekly that have not yet been identified by the industry in general. (This is not to suggest that other anti-malware tools are incapable of detecting these samples, but rather that they have not yet been discovered in public application repositories.)

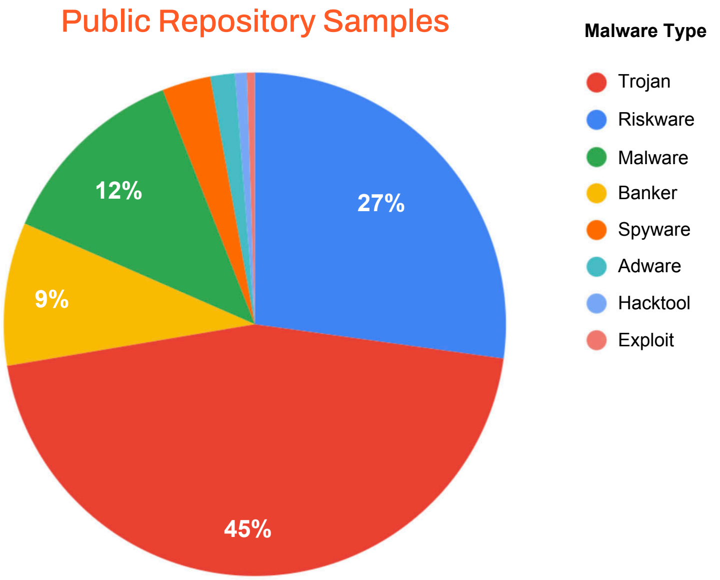


Machine learning-based solutions are necessary to provide the best and most comprehensive protection against malware for several reasons. First, the number of new malware variants being created is rapidly increasing, and traditional signature-based approaches to malware detection are becoming less effective. Machine learning algorithms can learn to identify patterns and behaviors that are indicative of malware without relying on known signatures. This enables them to detect new and previously unseen threats that have not yet been identified by the industry (like the 2,000 samples Zimperium discovers weekly).

Second, machine learning models can be trained on large datasets to continuously enhance their accuracy over time. They can adapt to new forms of malware and learn to identify subtle variations in attack patterns, allowing them to stay ahead of evolving threats and provide better protection for users.

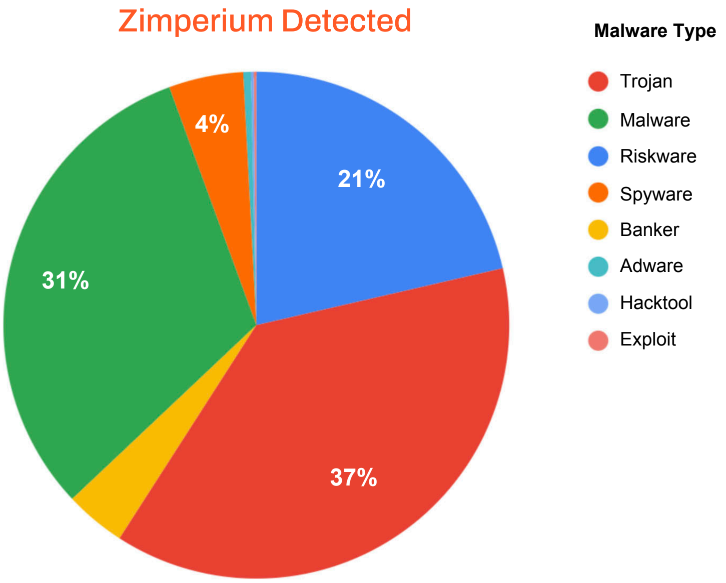
Breakdown of Malware Types

In examining malware types, Zimperium researchers have been able to leverage two data sources: the malware totals offered by public application repositories, and the data captured directly by Zimperium. The chart below offers a breakdown of malware types tracked by public application repositories, which offers a good picture of publicly known malware.



The chart above reveals that over 45% of all the mobile malware samples detected are trojans. Riskware and generic malware were the next two highest categories.

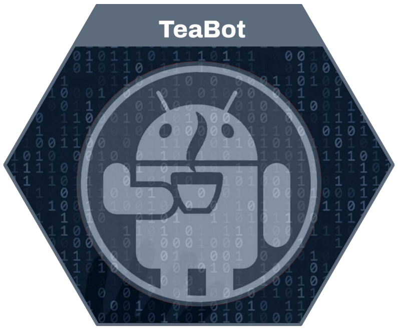
A similar breakdown based on Zimperium data from millions of corporate devices around the world is provided below.



While the descriptions and relative distributions are different, trojans are still the most common type of malware, accounting for 32% of all the samples. The data also shows that generic malware was found at a higher percentage on corporate devices than on the consumer side.

High-Profile Malware Campaigns

Following are examples of some of the more notorious malware campaigns that made the news in 2022:



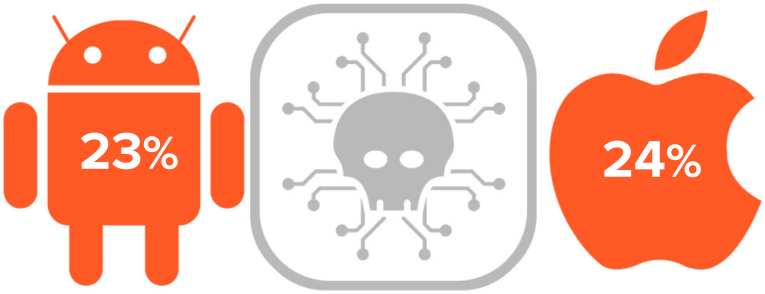
Dark Herring campaign. Early in 2022, Zimperium discovered this malware campaign which successfully targeted more than 105,000,000 victims around the world.[32] This campaign exploits direct carrier billing to scam money from unsuspecting users, and losses are estimated to have reached hundreds of millions of dollars.

TeaBot campaign. TeaBot is a banking trojan that was first detected by Cleafy in 2021.[33] This malware is designed to steal victims' credentials and SMS messages. In late 2021 and early 2022, the number of malware samples grew substantially. Ultimately, more than 400 malicious apps were detected.

RatMilad campaign. In the fall of 2022, the Zimperium zLabs team issued a warning about RatMilad, an Android spyware campaign targeting individuals in the Middle East.[34] The spyware was hidden within a phone number spoofing app and was distributed under the guise of enabling users to independently verify a social media account. Once users installed the app, malicious actors could gain control over their mobile devices, including the ability to view contacts, phone call logs, media, and files.

Malware Samples Detected, by Platform

By using publicly available malware repositories, the overall number of malicious apps can be gauged. According to the research conducted by Zimperium, approximately 23% of the 3.8 million Android samples submitted to one of the most popular repositories were identified as malicious. Similarly, Zimperium found that about 24% of all iOS samples submitted to it were also classified as malicious. It should be noted that this high percentage can be attributed in part to this repository being used by both security professionals and malicious actors who test whether their malware is detectable by anti-malware technologies. Nevertheless, this is currently the most comprehensive representation of the true malware landscape.



Development Techniques Employed to Help Evade Detection

Malware developers are constantly fighting to hide their code. Increasingly, they're employing development and delivery techniques that advance this objective. Below are two examples of these approaches:

- **Multi-platform development frameworks**. Malware developers have migrated to multi-platform development frameworks such as Flutter, Cordova, Unity, and Xamarin. For example, a predatory loan malware campaign was discovered that was developed via Flutter.[35] These frameworks are convenient, and they enable developers to create platform-independent code. Further, they can provide a form of code encapsulation which makes the code more challenging for conventional malware detection solutions to analyze.

- **Malware droppers**. Malicious actors are increasingly using malware droppers. Through this approach, they can deliver only minimal code initially. It is only at runtime that these droppers will download malicious code. Through this method, malicious actors can avoid detection by virtually all static code analysis techniques and even some dynamic analysis techniques.

3.3

Zimperium’s Detection of Unknown Threats: Highlighting the Advantages of Machine Learning

In the realm of cybersecurity, a lack of knowledge can be catastrophic. Establishing defenses against recognized threats is necessary, but it is even more vital to have mechanisms that can detect and safeguard against unknown threats that persistently appear. Simply put, prioritizing protection against unknown dangers should be a crucial concern, not just an optional benefit. In today’s complex, dynamic environments, it takes machine learning to achieve this key imperative.

When it comes to getting a picture of known threats, public application repositories are a valuable service. With public application repositories, a user can submit apps or files, and the service will employ over dozens of antivirus scanners to determine if the sample is malicious or not. (It is interesting to note that these services are widely used, not only by security teams looking to guard against threats, but also by malicious actors who are trying to determine whether a potential piece of malware will be detected.) Because they compile the findings of multiple tools, public application repositories provide a reasonable reflection of what’s known —revealing the body of knowledge available to security teams at a given point in time.

Zimperium MTD features a dynamic on-device detection engine. With its advanced detection capabilities, Zimperium MTD can detect previously documented threats and also unknown, zero-day attacks.

51% The increase in the total number of mobile malware samples detected by Zimperium year-over-year

By comparing the findings of public application repositories with those generated by Zimperium MTD, teams can get an effective illustration of the advantages of Zimperium MTD's dynamic on-device detection engine. The Zimperium zLabs team analyzed all the unique malicious samples that Zimperium MTD detected during Q4 2022. The team then analyzed which of those samples hadn't been detected previously and then looked at whether those newly detected samples were in public application repositories at the time of discovery. Here are the findings of this analysis:

- During Q4 2022, Zimperium detected 254,000 malware threats.
- Of the samples detected, 7,500 hadn't been detected by Zimperium previously.
- Of those newly identified samples, 63%, or 4,700, were not in public application repositories.
- This means that 63% of the new malware samples detected by Zimperium were completely unknown at the time of the detection.
- Many tools offer safeguards against what's known to be malicious. However, many are not equipped to defend against threats that have yet to be identified. This means that throughout the quarter, an organization relying solely on alternative solutions may have been exposed to 4,700 more new threats than an organization employing Zimperium solutions (not counting the "known" threats that many solutions fail to detect too).

Machine learning algorithms can process and analyze vast amounts of data and learn to identify patterns and behavior associated with malicious activity. Machine learning models can be trained to deliver high accuracy, scale to handle the largest volumes of data, and rapidly adapt to new types of threats as they emerge. This gives machine-learning based systems a definitive advantage in detecting new and unknown malware and zero-day threats that might be missed by signature-based systems.

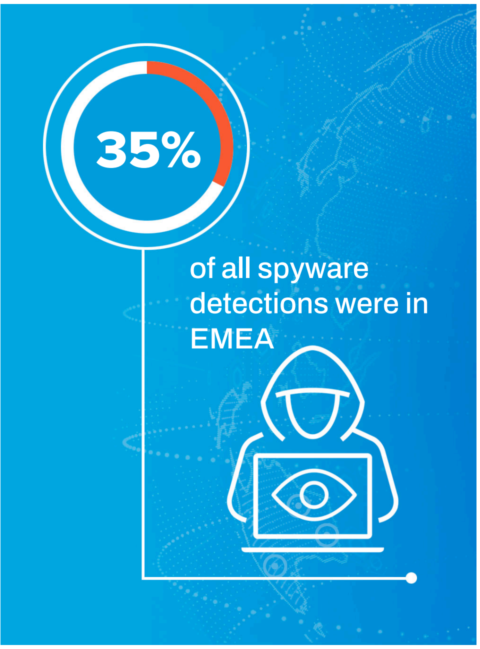
Mobile Spyware: Increasing in Volume and Sophistication

Introduction to Spyware

Spyware is a malicious software application that can secretly monitor a user's activity, including their internet usage, keystrokes, sensitive information like credit card numbers, and login credentials. It is frequently installed on mobile devices without the user's knowledge, often through mobile phishing or by exploiting software vulnerabilities.

Spyware has emerged as a byproduct of the convergence of technological, social, and political trends that have surfaced over the past decade.

Mobile devices are particularly vulnerable to spyware for several important reasons. First, they are always connected to the internet. This connectivity provides a long window of opportunity for surreptitious spyware-related activity. Second, the ease with which mobile devices can be customized allows unsuspecting users many opportunities to install malicious apps, perhaps disguised as legitimate apps. Third, while mobile operating systems have inherent security advantages over traditional endpoints (e.g., the OS kernel is locked down, and apps are in containers), mobile phones are less likely to have effective solutions to detect malware and device exploits.



Additionally, it is important to note that if spyware is installed on a desktop computer, it will only effectively be spying on user activity while the computer is in use. However, if spyware is installed on a mobile device, it becomes a powerful 24-hour tracker. This is particularly concerning considering how often mobile devices are with us. How many people leave their phones in the house when they leave? Or at their desk when they attend an important meeting? The ubiquity of mobile devices and their vulnerability to spyware underscores the importance of taking steps to secure these crucial endpoints.

Key Takeaways

Here are the key takeaways associated with mobile spyware in the last year:

- In 2022, Zimperium detected 3,200 unique spyware samples.
- While EMEA has the highest percentage of spyware detections when data is normalized (35%), North America is the region with the most spyware attacks detected.
- Spyware kits, services, and source code are commonly traded and shared on the dark web and on mainstream repositories like GitHub or online communities like Reddit.

In the following sections, we examine these and other key findings in more detail.

The Many Types of Spyware Offerings

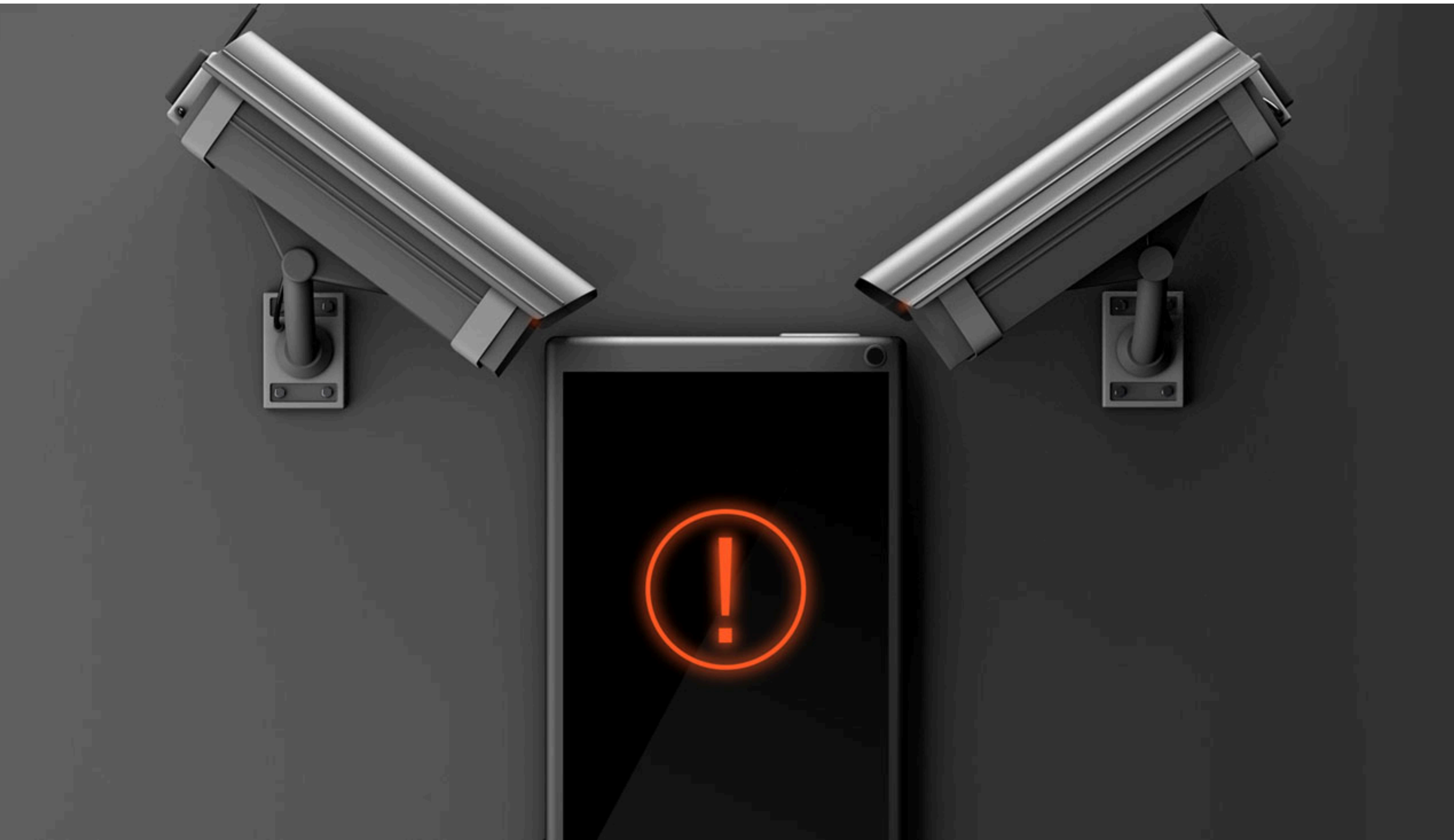
Spyware can come in many forms and have various labels. A web search on terms like “stalkerware,” “family tracking,” and “employee tracking” will all yield plenty of results and provide links to software that is undoubtedly designed for spying. And these are just the commercially available solutions.

Hacking software, toolkits, spyware kits, spyware services, and spyware source code are commonly traded and shared on the dark web, which is a hidden part of the internet that is not accessible through traditional search engines. The dark web is often used by cybercriminals to buy and sell illegal goods and services, including malware and hacking tools.

Moreover, the same kits and tools are sometimes made available via online repositories like GitHub or online communities like Reddit. While these platforms have policies against the distribution of malicious software, some users still find ways to share such content. You can learn more here: https://github.com/topics/spyware.

The spread of spyware tools on these platforms is a significant concern, as it lowers the barrier to entry for would-be cybercriminals. With access to these tools and services, even individuals with limited technical knowledge can launch sophisticated cyberattacks, leading to a rise in cybercrime.

Additionally, cybercriminals often develop and sell their own spyware source code, allowing other criminals to customize the spyware to their specific needs. This has led to a proliferation of spyware variants that can evade detection by traditional antivirus software, making it more challenging for organizations and individuals to protect themselves against these types of attacks.



Key Characteristics

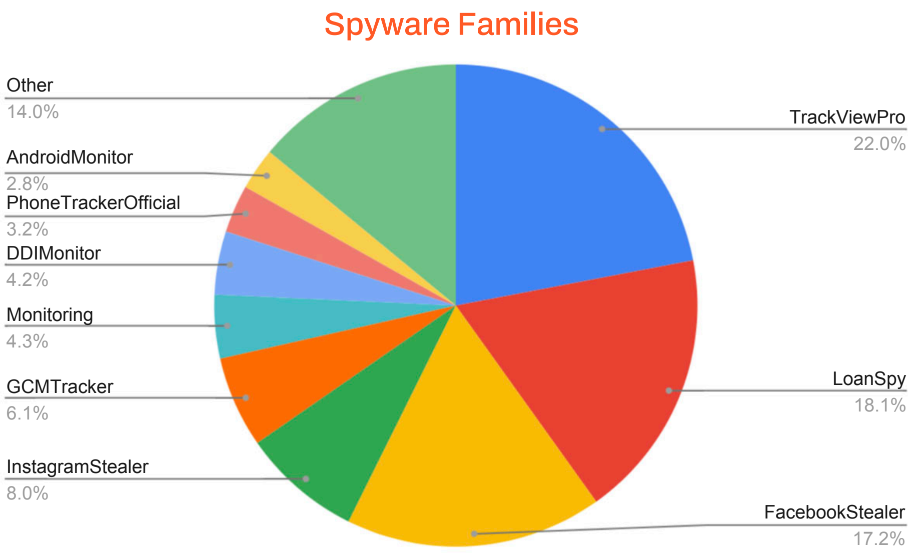
Here are a few of the key characteristics of spyware:

- **Hidden or disguised.** In order to work and remain installed, spyware needs to be undetected by the victim. Generally, the more hidden the spyware is, the longer it stays on the device. Spyware gets installed through deception, and victims aren't aware of its existence—at least not until it's too late.
- **Collection.** Spyware seeks to collect and misuse or compromise personally identifiable information, photos, communications, login credentials, and more.
- **Surveillance.** Malicious actors often gain access to a mobile device's assets or functionality so they can take pictures, view messages, record conversations, access credentials, and monitor specific GPS coordinates, to name a few.
- **Transmission or control.** Sensitive assets and control of services are ultimately handed to an unauthorized individual. This can happen via communications with a remote command-and-control server or through an attacker gaining remote control of a device.

The following sections provide a look at some prevalent spyware examples, the (known) actors behind spyware, who is using the spyware, and where mobile devices are being targeted.

Spyware Families

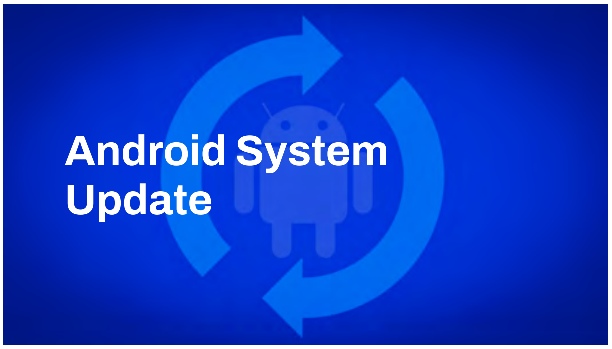
Over the course of the year, Zimperium detected 3,200 unique spyware samples. The detected samples can be categorized into a set of malware families. The graph below offers a look at the various families and their relative volume of samples.



TrackViewPro is a tracking application found on many devices. While this app may be available in third-party app stores, it nevertheless shares the capabilities of traditional spyware. Mobile device users should be very leery of installing this app unless they have a very compelling need to do so.

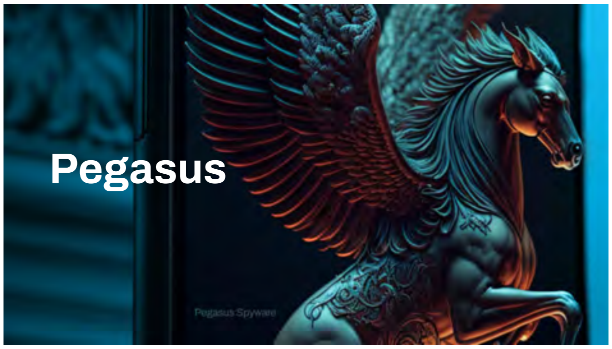
FacebookStealer is another commonly used spyware family. Discovered by Zimperium in December 2022, this stealthy spyware enables malicious actors to steal targets' Facebook credentials.[36] These malicious apps, also known as the "Schoolyard Bully Trojan," are disguised as legitimate educational apps with a wide range of books and topics for their victims to read. They are designed to trick users into believing that they are trustworthy. However, the apps contain hidden malicious code that can steal Facebook credentials, which are then uploaded to the threat actors' Firebase Command and Control server. In other words, the apps are camouflaged as legitimate but are really capable of stealing sensitive information and login credentials.

Spyware Examples



Android System Update is a sophisticated spyware campaign with a range of complex capabilities.[37] The mobile application functions as a remote access trojan. Through this spyware, malicious actors can record phone calls, take photos, access messages, and more.

The Zimperium zLabs team issued a warning about RatMilad in the fall of 2022.[40] This Android spyware campaign targeted individuals in the Middle East. The spyware was hidden within a phone number spoofing app. Once users loaded the app, malicious actors could gain control over their mobile devices, including the ability to view contacts, phone call logs, media, and files. Further, they could also send SMS messages and make phone calls from the device.



Pegasus is one of the most notorious examples of spyware. First detected in 2016, this malware remains very much a threat. Pegasus made major headlines in 2021, when more than 50,000 individuals were victimized.[38] That same year, a previously unknown security flaw in iOS was found to be exploited by Pegasus.[39] This version was distributed via iMessage and was a so-called zero-click exploit, which meant a user didn't even need to click a malicious link to be infected. In 2022, the spyware continued to make headlines. During the year, prominent leaders in Israel and the EU were victimized.

Predator is a type of spyware that is known for its advanced and sophisticated features. Like any spyware, Predator is able to capture and exfiltrate a broad range of data, including passwords, screenshots, and keystrokes.

Predator has many of the same capabilities as Pegasus spyware. At this time, however, there is no evidence that Predator spyware is capable of zero-click attacks. According to research conducted by Google's Threat Analysis Group and the University of Toronto's Citizen Lab, state-sponsored actors in a significant number of countries bought Predator. Customers were located in Armenia, Côte d'Ivoire, Egypt, Greece, Indonesia, Madagascar, Serbia, Spain, and more. The most recently reported version of the spyware exploited five previously unknown Android vulnerabilities. It also exploited known vulnerabilities, for which fixes were available but that users had yet to patch.[41]

Spyware Developers

Several companies are in the business of selling spyware. Here are some of the more prominent organizations:

- **DSIRF**. In July 2022, Microsoft's Threat Intelligence Center issued a report on an Austria-based spyware and hack-for-hire firm called DSIRF.[42] This organization's spyware had targeted individuals in banks, law firms, and consultancies in several countries. The firm advertises "due diligence" services to businesses implying that these hacking operations were undertaken on behalf of private clients.
- **NSO Group**. NSO Group gained widespread notoriety in 2021 when it was discovered that the organization's spyware, Pegasus, had been used by authoritative governments to target over 50,0000 journalists, activists, and legal professionals from over 50 countries. NSO Group continues to evolve and sell its spyware.
- **QuaDream**. QuaDream was founded in 2016 by a former Israeli military official and two former NSO employees. Over the last six years, the firm has delivered powerful spyware that provides its users with access to their targets' email, photos, texts, and contacts. In addition, QuaDream spyware provides access to instant messages from WhatsApp, Telegram, and Signal—in spite of the end-to-end encryption touted by these messaging providers.

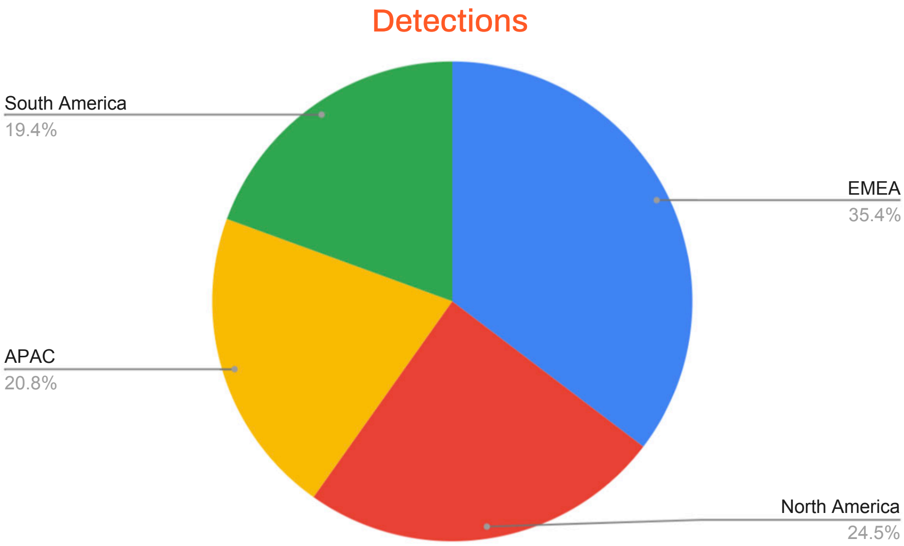
Spyware Users

Today, the use of spyware is increasingly widespread, not only through criminal organizations but also various other entities:

- **Government agencies and contractors**. Government-affiliated agencies and contractors are common users of spyware. These organizations use spyware to pursue surveillance of citizens, gather intelligence on adversaries, etc.
- **Corporations**. There has been an increase in the visibility of corporate espionage activity over the past few years, with a recent public award to Appian in the amount of $2+ billion in damages.[43] While there is no explicit data at this time, it seems highly likely that the use of spyware and malware tools will accompany and support the increased activity in corporate espionage.[44]
- **Individuals**. Today, an individual can go onto the dark web, visit code repositories and forums, and even do a simple web search and locate a range of spyware alternatives. With publicly available spyware, these individuals can pursue a number of activities, such as stalking, fraud and identity theft, ransomware attacks, and more.

Spyware by Region

The chart below offers a view of the regional distribution of spyware threats Zimperium has detected.



The numbers illustrate the global nature of the spyware problem. While EMEA has the highest percentage of spyware detections per capita, the numbers across the board show mobile device users in any region are susceptible to attack. It should be noted that the data was normalized for the number of devices Zimperium is protecting in each region. If the data was not normalized, North America is unquestionably the region with the most spyware attacks detected.

Mobile Ransomware Is Now a Legitimate Threat

Key Takeaways

Here are the key takeaways associated with mobile ransomware in the last year:

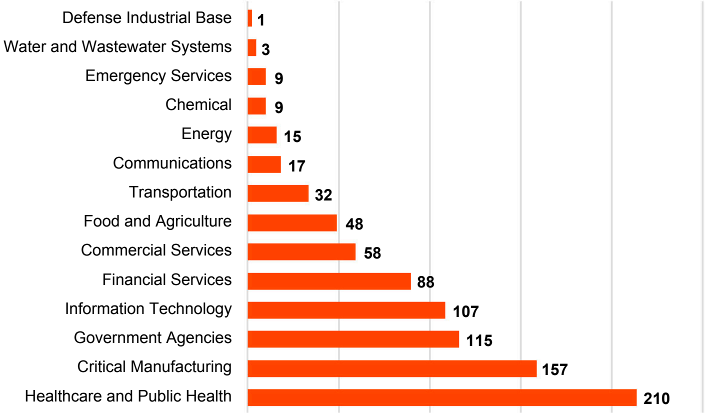
- Ransomware profits decreased by 40% in 2022, but that did not slow down overall activity.
- In 2022, mobile ransomware moved from an experiment to a legitimate threat, from simple overlays that could be dismissed with a reboot to ones that encrypted files and locked down the device.
- During 2022, Zimperium detected 17,000 unique ransomware samples and protected organizations from more than 90,000 ransomware attacks, with the main ransomware families being lockers, crypto, and leaker ransomware.

In the following sections, we examine these and other key findings in more detail.

Ransomware Business Goes Mobile

Ransomware profits dropped to $457 million throughout 2022, a drop of roughly 40% from the record-breaking $765 million recorded in the previous two years.[45] In 2022, 59% of victims refused to pay a ransom to get their data back, but this did not slow down the number of attacks, as 2022 proved to be one of the most active years in ransomware activity.[46] The FBI reported that 14 critical infrastructure sectors had at least one member fall victim to ransomware.[47]

Infrastructure Sectors Victimized by Ransomware



Source - Federal Bureau of Investigation Internet Crime Report 2022

In a typical scenario, desktop ransomware would encrypt the files on a host machine prompting the victim to submit a payment (often using cryptocurrency) in order to get the decryption key. At the same time, desktop ransomware uses OS vulnerabilities to infect the host and propagate to other devices (for example, WannaCry used a vulnerability called EternalBlue, released by The Shadow Brokers, which was later granted the following common vulnerabilities and exposures (CVEs): CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, and CVE-2017-0148).

Based on the Windows permission model, desktop ransomware can encrypt the whole file system without any limitation (it does leave the OS files untouched so that the machine can still run).

Ransomware functions differently on mobile devices. This is because Android and Apple iOS devices employ sandboxing and permission models, which is a way to improve security by isolating and shielding apps from outside intruders or malware and to limit the harm a rogue application or user can do to a device. Each mobile app runs in its own sandboxed environment, which limits its access to data and system resources. When attacks do occur, sandboxing is a way to limit the damage.

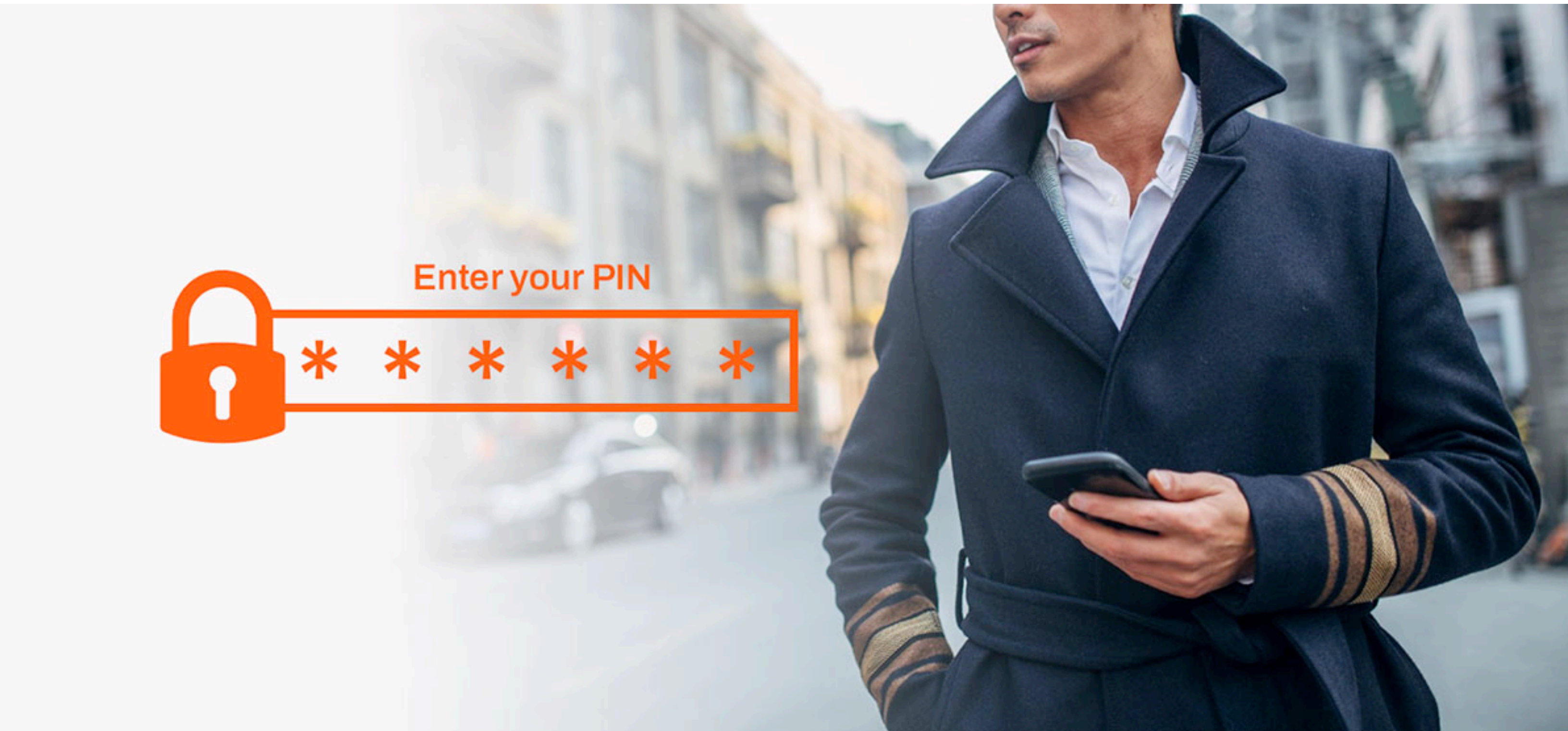
For these reasons, malicious developers employ a range of techniques and methods to craft mobile ransomware that can effectively take control of a device or lock out a user from their data. These approaches are observed in the following:

- Locker ransomware: blocks the victim from interacting with the device by creating a lock screen. This can be achieved either by changing the system PIN number or by overlaying a screen that overrides methods that block normal device interactions. You can see the locker ransomware technique in action in this sample.
- Crypto ransomware: compromises a device by encrypting files, usually pictures and document files. Most crypto ransomware contacts a Command and Control (C&C) server to get a dynamically generated key, preventing the victim from decrypting their files without paying the ransom. You can see an example of this type of ransomware here.
- Leaker locker: an unusual type of ransomware that employs a variation of social engineering to compromise mobile devices. After infecting a device, it gets access to personal information, including contacts. Victims are extorted for payment, and if payment is not made, those behind the ransomware will distribute all personal information that was accessed to the victim's contacts. An example of this type of ransomware can be viewed in this sample.

During 2022, Zimperium detected 17,000 unique ransomware samples and protected organizations from more than

90,000

ransomware attacks



Exploited Mobile Vulnerabilities in 2022

iOS Had the Majority of Zero-Day Mobile Vulnerabilities Actively Being Exploited

It seems that the world is inundated by security vulnerabilities. From the venerable Microsoft patch Tuesday to the latest flashy exploit sweeping the headlines to your quarterly mandatory security awareness training, the message is clear: we have a long way to go until we can deliver complex, functional code that is completely free of security issues. That said, some vulnerabilities pack more of a punch than others. Vulnerabilities that are actively being exploited in the wild, some of which even have proof of concept exploit code publicly available, can provide great danger to the security of devices in the enterprise--including mobile ones.

Apple's WebKit has been long beleaguered with vulnerabilities. This is not necessarily from any deficiency on the part of its development, but rather from the many eyes on it as an ideal place to gain a foothold into iOS with the browser's unique capability to run unsigned code combined with the relative difficulty of rendering the Internet safely. WebKit was formerly used in Android's Chrome Browser as well, adding double the fun to a successful exploit, but Google has since forked WebKit into its own Blink project. In February 2022, CVE-2022-22620, a use-after-free vulnerability in WebKit affecting both iOS and macOS, was patched after being found to be actively exploited in the wild. Project Zero's Maddie Stone released a root cause analysis on this vulnerability and dubbed it a "zombie" vulnerability. In this case, the original bug was reported and patched in 2013, but it was later reintroduced into the codebase during refactoring in 2016. Zombie vulnerabilities like this sometimes give attackers a leg-up in exploitation if proof of concept exploit code is publicly released after the issue is patched. This code can often be refactored to work for the modern reintroduced bug.

Speaking of cross-platform vulnerabilities, in January 2022, Apple released iOS/iPadOS 15.3 and macOS 12.2. Among feature enhancements and bug fixes, these releases patched a critical memory corruption vulnerability in IOMobileFrameBuffer, which could allow a local application to run arbitrary code with kernel privileges. IOMobileFrameBuffer is a kernel extension that manages the screen buffer and has been subject to security problems in the past, including multiple issues in 2021.

Key Takeaways

Here are the key takeaways associated with vulnerabilities and exploits in the last year:

- The iOS operating system accounted for 80% of the mobile zero-day exploits in 2022. (source: Mandiant)
- Pegasus spyware and other mobile zero-click attacks--those that do not require any user input and automatically proceed as soon as the malicious code is installed on the device--continued to make news in 2022.
- Fragmentation in the availability of patches in the Android ecosystem, as well as delays in users applying the latest security patches, continues to plague mobile security.

The following sections examine these and other key findings in more detail.

Due to the fragmentation of the Android ecosystem, it is common for exploits to target particular platforms due to vulnerabilities in hardware or code implementations. In January 2022, along with 18 additional security vulnerabilities, Samsung released a patch for CVE-2022-22265, a double free vulnerability in the neural processing unit (NPU) driver for select versions of the long-suffering Exynos chipset. Google Project Zero marked this vulnerability as actively being exploited in the wild. Likewise, in March 2022, Google provided a patch for Pixel devices fixing CVE-2022-22706, a memory write issue in the Mali GPU driver. This vulnerability was found to be actively exploited in a multi-part exploit chain, discussed later in this section.

In 2022, Mandiant tracked 55 zero-day vulnerabilities that were actively being exploited in the wild. On these six affected mobile operating systems, iOS was targeted by five of the six mobile zero-days, with one targeting Android. Though Android accounts for roughly two-thirds of mobile devices worldwide, the fragmentation of the Android ecosystem makes developing an exploit that works for all Android devices daunting. On the other hand, a vulnerability in the latest version of iOS should work on all iOS devices.

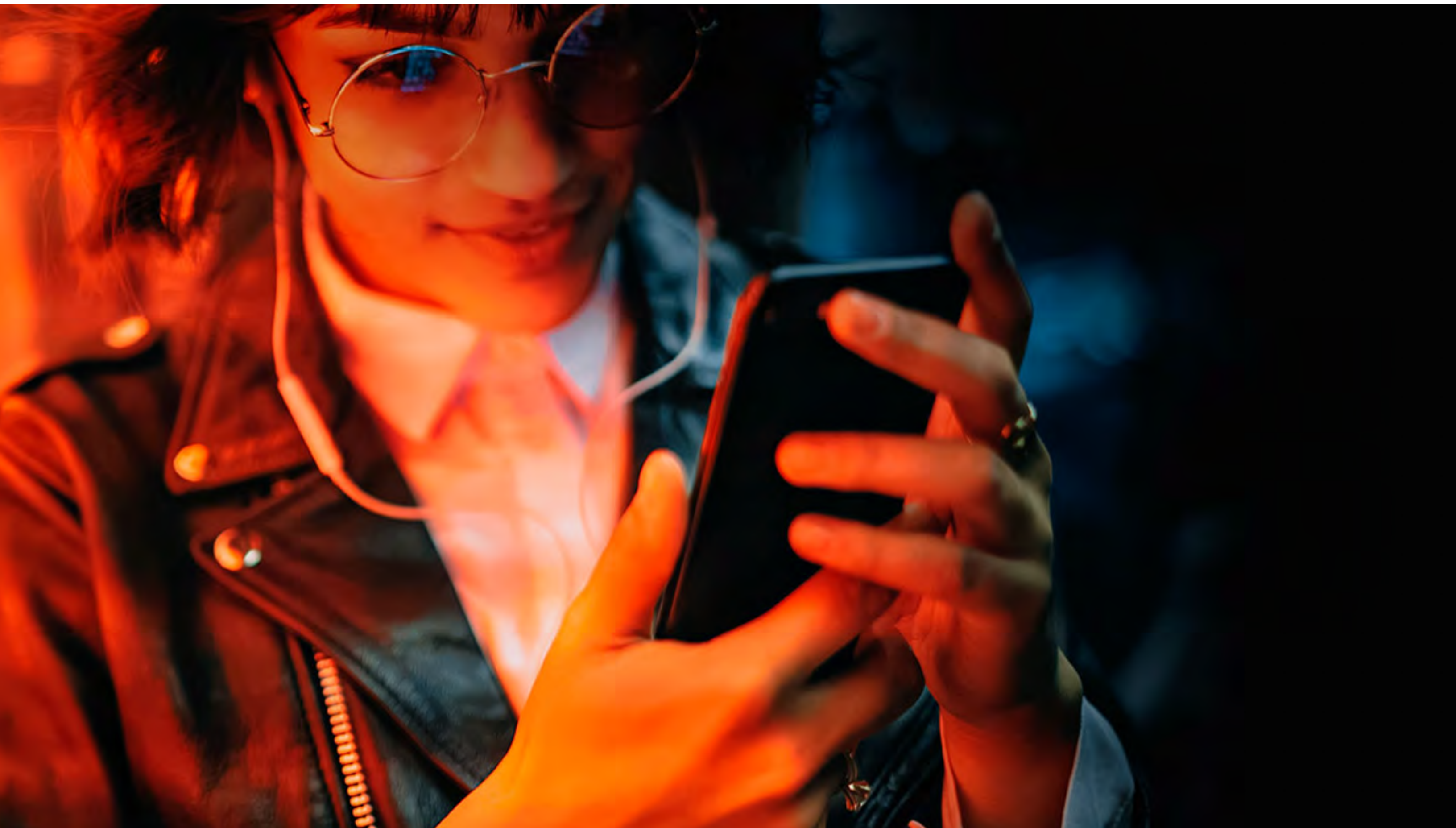
Dangerous Zero-Click Attacks Continue to Emerge

Zero-click attacks are a type of cyberattack that do not require any user input and automatically proceed as soon as the malicious code is installed on the device. With zero-click attacks, threat actors can penetrate the device without relying on social engineering or user participation, making it easier for them to gain unauthorized access. For these reasons and more, this places zero-click attacks among the most dangerous attack techniques.

Zero-click attacks on mobile devices have often targeted vulnerabilities in messaging or mail applications. Attackers can leverage this by sending a carefully crafted message to the targeted device. Once the attack is underway, threat actors can then deploy spyware, trojans, ransomware, or other types of malware to compromise the device's security.

NSO Group's Pegasus Spyware continued to make news in 2022. Citizen Lab reported that in 2022, three particularly dangerous "zero-click" exploit chains (exploit chains where no user interaction at all is required) had been used to deploy the Pegasus spyware on iPhones of human rights defenders in Mexico. The three discovered exploit chains included:

- LATENTIMAGE – Zero-click exploit chain targeting iOS 15. May involve the "Find My" function.
- FINDMYPWN – Zero-click exploit chain targeting iOS 15. Attacks vulnerabilities in the "Find My" function. It is believed to be a two-part attack targeting the MessagesBlastDoorService after exploiting the "Find My" feature.
- PWNYOURHOME – Zero-click exploit chain targeting iOS 15 and 16. Attacks vulnerabilities in the Apple HomeKit Daemon followed by MessagesBlastDoorService in iMessage.



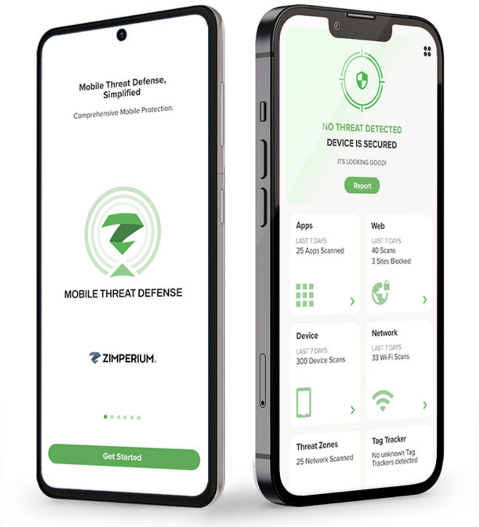
Even N-Day and Some-Click Exploits are Dangerous

In addition to zero-day exploits, fragmentation in the availability of patches in the Android ecosystem, as well as delays in users applying the latest security patches, continues to plague the security of mobility. Google's Threat Analysis Group (TAG) discovered targeted campaigns against mobile devices in 2022 involving exploit chains made up of zero-day and n-day exploits, which were known to the vendor and have a patch available. The first campaign, which was discovered in November 2022 targeting users in Kazakhstan, Italy, and Malaysia, began with an SMS phishing attack including a link leading to a website hosting exploits for both Android and iOS. The browser was then redirected to legitimate shipment tracking sites based on the victim's country. On iOS, the exploit chain targeted iOS prior to 15.1 and included one zero-day CVE-2022-42856, a type confusion remote code execution (RCE) vulnerability in WebKit giving browser-level access to the device. The next exploit in the chain was a Pointer Authentication Code (PAC) bypass in WebKit, for which Apple had released a patch in March 2022. A sandbox escape and privilege escalation vulnerability in AGXAccelerator CVE-2021-30900 was used next. A proof-of-concept exploit for this issue was made available on GitHub in 2020.

Users who clicked the phishing link from an Android device encountered an exploit chain targeting ARM (Advanced RISC [reduced instruction set computer] Machine) devices with missing patches running an outdated version of Google Chrome below version 106. First, they received an exploit for CVE-2022-3723, a type confusion vulnerability first discovered in the wild and patched in October 2022. A Chrome graphics processing unit (GPU) sandbox escape which was zero-day at the time of the campaign before being fixed in November. 2022 CVE-2022-4135 came next. Finally, an ARM privilege escalation bug CVE-2022-38181 resulted in the complete compromise of vulnerable devices. Once again, the exploit chain included zero-day exploits but also relied on missing patches to be successful.

TAG discovered a second campaign in December 2022 targeting Android devices running Samsung Internet Browser in the United Arab Emirates. Once again, the attack began with an SMS phishing link. At the time, Samsung Internet Browser ran on Chromium 102, which did not include the latest security patches for known issues. The exploit chain began with a zero-day at the time of the attack, CVE-2022-4262, a type confusion in Chrome that was patched in December 2022. The attack then escaped the sandbox with CVE-2022-3038. This issue was fixed in August 2022 in version 105. This time the issue was not users failing to apply the latest security patches; the current version of Samsung Internet Browser at the time of the attack ran on version 102, which was vulnerable to this attack. Next, CVE-2022-22706, the Mali GPU issue discussed previously, was exploited. Though it had been patched by ARM and on Google Pixel devices, the latest Samsung firmware at the time had not patched this issue. Finally, another zero-day CVE-2023-0266 gave the exploit chain read/write access to the kernel. Though this exploit chain used multiple zero and n-day vulnerabilities, even users who were completely patched could still be vulnerable due to the fragmentation of the Android ecosystem around patching.

These exploit chains demonstrate the ongoing critical importance of both patches being made available and users updating their devices in a timely fashion. Though these exploit chains were both targeted and sophisticated, they would not have been successful had the targets fully updated their devices and vendors provided patches for all known vulnerabilities in third-party components.



How Can One Combat These Threats?

Mobile security products such as Zimperium MTD can protect users from both known vulnerabilities and zero-days alike. For example, Zimperium MTD identifies out-of-date and vulnerable OSs. Though unknown zero-day vulnerabilities will not have a known exploit signature in a database, they will, in the process of performing their work, likely trigger indicators of compromise, and Zimperium MTD will alert the security team that something is amiss. While known and unknown mobile vulnerabilities are and will continue to be exploited in the wild, a strong mobile security program can significantly limit your organization's risk.

Vulnerability Spotlight: Vulnerabilities Affecting Apple Devices

Douglas McKee, Principal Engineer & Director of Vulnerability Research at Trellix

Early in 2023, the Trellix Advanced Research Center vulnerability team announced the discovery of a significant class of vulnerabilities that affect Apple iPhones, iPads, and Macs. The risks posed by these vulnerabilities can be significant. By exploiting these bugs, malicious actors could gain access to a range of sensitive services and information on user devices, including messages, location data, photos, and call history.

Apple iOS Security: The Protections of Code Signing

Over the years, Apple has received a lot of recognition for its approach to security, and for good reason. Since it first unveiled the iPhone and iOS, Apple has enforced careful restrictions on the software that can run on its mobile devices. In iOS devices and increasingly in macOS devices, the company has employed code signing. This means apps can only run if they've been cryptographically signed by a trusted developer. In addition, Apple didn't allow scripting languages like AppleScript to run on iOS.

Through this code-signing approach, Apple nearly completely eliminated the ability of unauthorized apps to dynamically execute code. This presented a fundamental safeguard for users and businesses, and an inherent obstacle for malicious actors.

Proactive Research Yields Discovery of Entire Class of Vulnerabilities

Through proactive analysis, Trellix discovered a large new class of bugs that allow malicious actors to bypass code-signing safeguards. By executing malicious code in several platform apps, attackers can perform privilege escalation and sandbox escape.

By uncovering this class of vulnerabilities, we've been able to alert Apple, security vendors, security teams, and the general public to the risks so mitigation measures can be pursued.

How it Works

The vulnerabilities stem from NSPredicate, which is a class (or capability for creating objects) available to developers. This class is intended to let developers filter lists of objects in apps. While the nature of this capability sounds innocuous, the reality is that it's a complete scripting language—and one that can be exploited to gain unfettered access and control.

As Seen in... The Press Coverage of the Trellix Vulnerability Discovery

More than 150 publications ran articles on the Apple vulnerabilities Trellix discovered. Here are a few of the top articles:

WIRED

"A New Kind of Bug Spells Trouble for iOS and macOS Security"

TechCrunch

"Security researchers warn of a new class of Apple bugs"

digitaltrends

"This major Apple bug could let hackers steal your photos and wipe your device"

Macworld

"Large new class of bugs' leaves Messages and Photos vulnerable in iOS and macOS"

tom's guide

"Huge Apple bug could let hackers access your photos, messages and location"

Here are specific examples of the vulnerabilities in this class:

- The first vulnerability we found is in coreduet, a process that collects data about user behavior on the device. An attacker can send a malicious NSPredicate and execute code in a process with entitlements, such as Messages or Safari, and inherit the privileges of this process. These processes run as root on macOS and give the attacker access to the user's calendar, address book, and photos.
- A very similar issue with the same impact also affects contextstored, a process related to CoreDuet. In this case, an attacker can use vulnerable XPC services, which are effectively helper tools for apps. Through these services, attackers can execute code from a process that has greater access to the device.
- The appstored daemons also possess vulnerable XPC services. Once attackers have control over a process that can communicate with these daemons, they can exploit these vulnerabilities. This gives them the ability to install unsigned apps, potentially even system apps.

This class of vulnerabilities also affects services that could be accessed by any app with no entitlements necessary. The first of this type was found in OSLogService, an XPC service that can be used to read potentially sensitive information from the syslog. More significantly, an attacker can exploit an NSPredicate vulnerability in UIKitCore on the iPad. By setting malicious scene activation rules, an app can achieve code execution inside of SpringBoard. SpringBoard is a highly privileged app that can access location data, the camera and microphone, call history, photos, and other sensitive data. This app can even wipe a device completely.

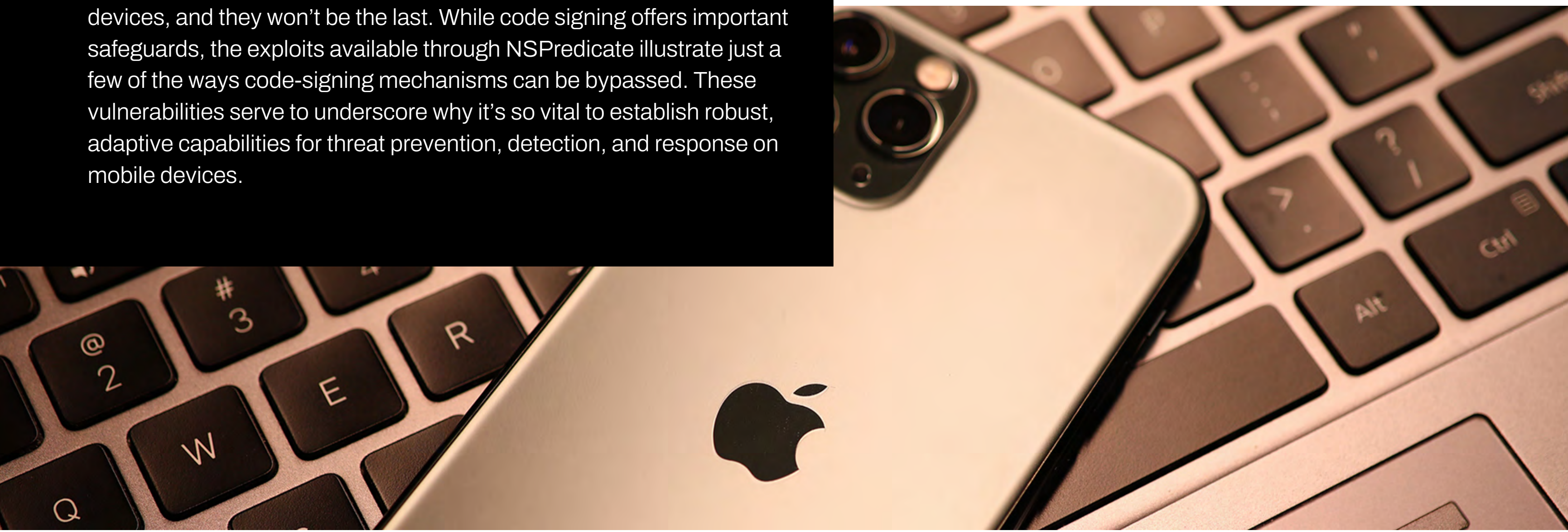
These Vulnerabilities Aren’t the First, Just the Latest

The class of vulnerabilities above are just the latest in a series of discoveries surrounding Apple devices. In fact, these revelations weren’t even the first time NSPredicate was in the news. It was back in September 2021 that Citizen Lab announced an exploit known as FORCEDENTRY. This was a zero-click exploit, meaning a device could be infected without the user even clicking a link. FORCEDENTRY was allegedly used by the NSO Group, purveyors of Pegasus spyware. Researchers discovered that a Saudi activist had their iPhone infected by Pegasus through this exploit.

This exploit employed two key techniques, one of which was leveraging NSPredicate to bypass code signing. Since then, Apple has made a number of changes to address the risks posed by NSPredicate. For example, the vendor employed mitigations that prevented the use of certain classes that could jeopardize security. However, our recent research illustrates the wide range of potential vulnerabilities that remain.

Conclusion

Security teams within today’s organizations should be very clear: the class of vulnerabilities discovered were not the first affecting Apple iOS devices, and they won’t be the last. While code signing offers important safeguards, the exploits available through NSPredicate illustrate just a few of the ways code-signing mechanisms can be bypassed. These vulnerabilities serve to underscore why it’s so vital to establish robust, adaptive capabilities for threat prevention, detection, and response on mobile devices.

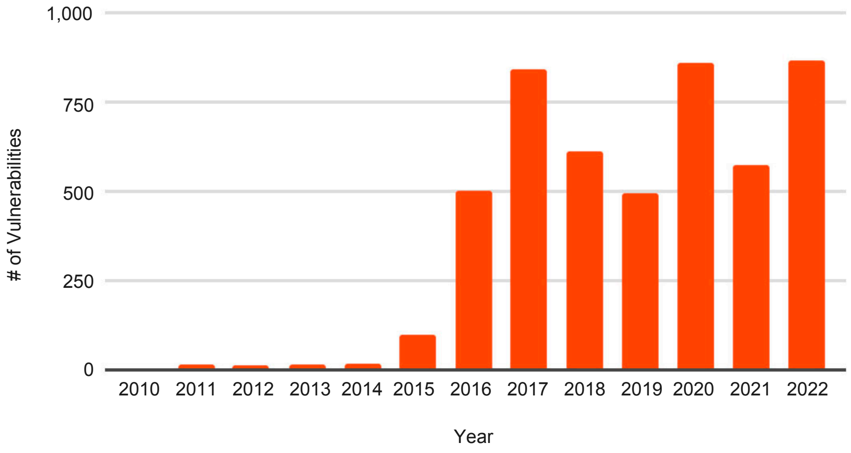


Mobile Platform and Ecosystem Risk in 2022

Android Vulnerabilities Increased, Overall & in the Number of Severe Vulnerabilities

According to vulnerability tracking,[48] the Android operating system saw an increase in the number of vulnerabilities discovered in 2022, to a record high of 897 CVEs tracked. In 2021, 571 were discovered. The most common vulnerabilities were code execution, system bypassing, and overflow of code or memory.

Android CVEs by Year



Of the reported and tracked Android vulnerabilities in 2022:

69%

are categorized with a low attack complexity.

16%

are categorized with a medium attack complexity.

15%

(138) of the tracked CVEs rated a Common Vulnerability Scoring System (CVSS) score of 7.2 or higher, with 43 falling into the critical category. This is a significant increase (139%) from the previous year, with 18 critical vulnerabilities discovered and reported in 2021.

Key Takeaways

Here are key takeaways associated with mobile vulnerabilities and ecosystem risk in 2022:

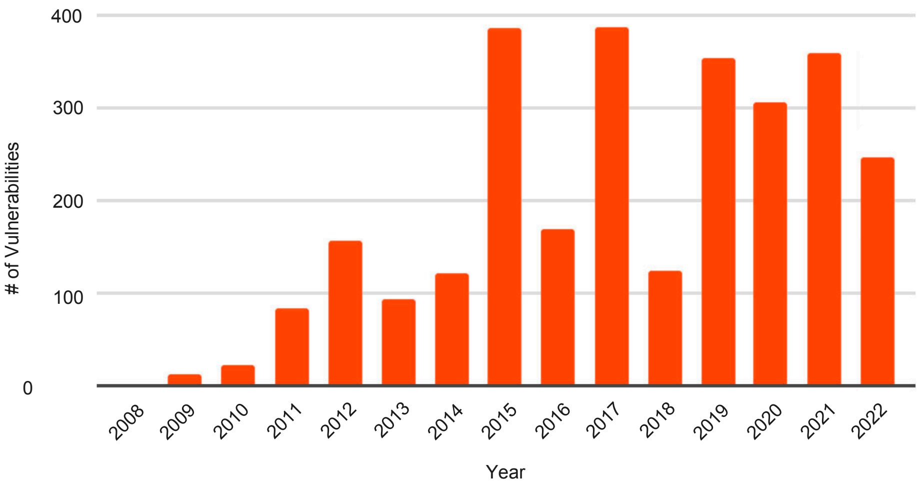
- The Android operating system saw an increase in the total number of vulnerabilities discovered, from 571 in 2021 to a record high of 897 in 2022.
  - 43 of the Android vulnerabilities were in the critical category, which was a 138% increase from 2021.
- The iOS operating system saw a decrease in the total number of vulnerabilities discovered, from 380 in 2021 to 242 in 2022.
  - 27 of the iOS vulnerabilities were in the critical category, which was a 40% decrease from 2021.
- During 2022, 53% of the Android devices detected as compromised were in the hands of attackers and not just rooted by users. Of the iOS devices that were compromised, 18% were exploited by threat actors. Overall, 23% of all compromised devices were exploited and not just jailbroken/rooted.
  - At report publication, 43% of all devices detected as compromised were not jailbroken or rooted. This is a 187% increase over the 2022 numbers. While Android remained constant, the iOS percentage jumped 127% to 41% of all compromised iOS devices being controlled by attackers.
- Vulnerabilities and attacks in the mobile supporting ecosystem, such as carriers and MDMs, continued to be seen in 2022.

The following sections examine these and other key findings in more detail.

iOS Vulnerabilities Decreased, Overall & in the Number of Severe Vulnerabilities

According to vulnerability tracking,[49] Apple iOS had 242 CVEs assigned throughout 2022. This is a decrease from the 380 discovered and reported in 2021. The most common vulnerabilities were code execution, followed by memory corruption and overflow of memory or code.

iOS CVEs by Year



Of the reported and tracked iOS vulnerabilities in 2022:

74%

are categorized with low attack complexity.

12%

are categorized as medium attack complexity.

14%

(34) of the CVEs rated a CVSS score of 7.2 or higher, with 27 falling into the critical category. With 45 critical vulnerabilities identified and reported in 2021, this was a 40% reduction year over year.

Jailbreaking/Rooting

Since the advent of iOS with its restrictions such as App Store-only applications and mandatory code signing, there has been a market for jailbreaking—privilege escalation exploitation run by the user to bypass App Store restrictions. Users typically do this to install third-party apps and user interface tweaks. Apple does not approve of jailbreaking and, in addition to patching vulnerabilities that have been used for jailbreaking in new releases, they have released a series of anti-jailbreaking patches. The latest of these was the introduction of Cryptex1 with the release of iOS 16 in September 2022. Cryptex1 is designed to allow Apple to push Rapid Security Responses outside of the normal patch cycle but has the consequence of making downgrading nearly impossible. As jailbreaking typically relies on running older, out-of-date versions of iOS, adding blocks to downgrading a device to an older iOS version creates additional complications for jailbreaking.

2022 saw the release of five new iOS jailbreaking tools:

p0laris
Released April 20, 2022. Targets all versions of iOS 9. As iOS 9 was released in June 2015, iOS 9 was out of date in 2022. Open-sourced, semi-tethered.

openpwnage
Released May 19, 2022. Targets iOS versions 8.4b4 through 9.3.6. Open-sourced, semi-tethered.

palera1n
Released September 17, 2022. Targets iOS versions 15.0 through 16.3.1. As iOS 15 and 16 were released in September 2021 and 2022, respectively, these are current operating systems. palera1n uses the older checkm8 (CVE-2019-8900) vulnerability which is considered unpatchable as it is in the boot ROM of A5 through A11 chips. palera1n only works on devices with A8 through A11 chips that are capable of running iOS 15/16. These include iPhone X and iPad Pro 2nd Generation, among others. Open-sourced, semi-tethered/tethered.

Fugu15
Released October 31, 2022. Targets iOS versions 15.0 through 15.4.1. Fugu15 can be installed via Safari and has been tested on iPhones X through 13. Open-sourced, semi-tethered.

XinaA15
Released December 7, 2022. Targets iOS versions 15.0 through 15.1.1. XinaA15 works on devices with chips A11 through A15, which includes iPhones 12 and 13, among others. Open-sourced, semi-tethered.

With many Android platforms supporting unlocking the bootloader, allowing users to flash their Android device with custom firmware that includes root access, there is less emphasis in the root/jailbreak community on finding working exploits for Android. That said, Android platform vulnerabilities are still of interest to the security research and bug bounty community, with Google offering rewards up to $1,000,000 for the kinds of exploit chains observed in the wild from spyware companies like NSO Group and QuaDream.

Since jailbroken and rooted devices are typically running out-of-date versions of the operating system and have key platform security features turned off, it is an enterprise best practice to not allow jailbroken devices on the corporate network, thus blocking them from using corporate apps and accessing corporate data. Additionally, it is a best practice for apps with high security requirements, such as mobile banking, to detect whether the device is jailbroken/rooted and refuse to run high-risk functionality, such as transferring money if the device is detected to be jailbroken/rooted. Some apps will refuse to run at all if jailbreaking/rooting is detected.

Of course, with each detection, anti-detection mechanisms are created to trick apps, devices, and supporting infrastructure into believing that a device is not rooted/jailbroken when it really is. For example, the most primitive of jailbreaking/rooting detection (and sadly, the only one still in use by many platforms) involves searching installed apps for the Cydia third-party app store on iOS devices or the SU (SuperUser) app on Android devices. There is no requirement that these apps must still be installed after jailbreaking or rooting a device, or they could just be renamed something else if the user does want these apps, or an alternative could be installed. Unfortunately, simply changing the name of the "SU" app to "SU1" is enough to stump primitive jailbreaking/rooting detection. Advanced indicators of compromise detection will be discussed in the next section.

Device Tampering

Android and iOS platform vulnerabilities can also be used by attackers to gain persistence on the device for nefarious purposes. There is a key distinction between device users rooting and jailbreaking their own devices and malicious attackers using the same exploit chains to compromise mobile devices. While both are of interest to the enterprise, the latter is decidedly more sinister and traditionally has gone undetected.

Zimperium keeps track of all devices that have been compromised by attackers and by users rooting/jailbreaking them. When rooting/jailbreaking or during a persistence attack by a malicious entity on the device, key indicators of compromise are created on the device. Some examples of indicators of compromise Zimperium detects include turning off code execution protections and OS security features. A user rooting/jailbreaking their device will trigger indicators of compromise, but a persistence attack by a malicious entity will not typically include common jailbreaking/rooting tools and frameworks. When these apps and libraries are detected on the device, the device is also flagged as rooted or jailbroken.

During 2022, 53% of the Android devices detected as compromised were in the hands of attackers and not just rooted by users. Of the iOS devices that were compromised, 18% were exploited by threat actors. This can partially be attributed to the relative popularity of jailbreaking vs. rooting. On Android, it is trivial for a user to, for example, sideload apps without rooting their device, whereas, on iOS, jailbreaking is the most popular way to allow sideloading of applications on a device. Overall, 23% of all compromised devices were exploited and not just jailbroken/rooted.

2022

OS type	% tampered but not rooted/jailbroken
🤖	53%
	18%
Total	23%

› › ›

At Report Publishing

OS type	% tampered but not rooted/jailbroken
🤖	51%
	41%
Total	43%

At report publication, 43% of all devices detected as compromised were not jailbroken or rooted. This is a 187% increase over the 2022 numbers. While Android remained constant, the iOS percentage jumped 127% to 41% of all compromised iOS devices being controlled by attackers.

Mobile Ecosystem Risk

When considering the risk of mobility to the enterprise, it is worth noting that for every mobile device present, there is a supporting infrastructure from the mobile carrier, the device manufacturer, the operating system vendor, etc. This mobile infrastructure is often in the form of cloud systems subject to the same security issues as any other cloud vendor, with the potential for missing patches, poor password hygiene, administrators falling victim to phishing attacks, software security mistakes, and more. Gaining information from or access to mobile supporting infrastructure can be seen as an alternative route to exploiting mobile devices.

Krebs on Security reported that three separate cybercriminal groups laid claim to gaining internal access to telecom provider T-Mobile's internal network in excess of 100 times. This attack involved phishing T-Mobile employees to gain access to internal resources that were then used to provide SIM-Swapping services for hire, whereby a customer can temporarily reroute mobile traffic from a target phone number to a device in their control. This is commonly used to capture SMS messages used in two-factor authentication as part of a larger attack. The cybercriminal groups advertise their wares on Telegram, and as of 2023, all three groups are still active.

When one thinks of Mobile Device Management (MDM), security risk is probably not the first thing that comes to mind. But like any other software, MDM is subject to security bugs and must be deployed with a strong authentication policy, access management, and other consistent security practices.

In July 2022, researchers from Claroty disclosed **two critical vulnerabilities in the FileWave MDM**. CVE-2022-34907 was an authentication bypass that allowed a remote attacker to gain superuser access, and CVE-2022-34906 was a hardcoded cryptographic key. The vulnerabilities were responsibly disclosed and patched by the vendor, but if they had been exploited in the wild, attackers could have stolen information about enrolled devices and could have even managed and installed malware on affected devices.

Likewise, researchers at Immersive Labs began disclosing vulnerabilities in 42Gear's SureMDM products in 2021 and into early 2022. The vulnerabilities included issues with the SureMDM web console that could allow attackers to disable security tools and install malware on enrolled devices and issues with the SureMDM agent that could allow local attackers to perform command injection for local privilege escalation.

Though there is no evidence that either the FileWave or SureMDM vulnerabilities from 2022 were exploited in the wild before being discovered and disclosed by researchers, there have been instances in the past where MDM compromises have been used to breach an enterprise. For example, in 2020, news broke that a variant of the Cerberus banking trojan was deployed to 75% of enrolled Android devices of an unnamed multi-national corporation via a compromised MDM. Additionally, in December 2022, posts were made on a hacking forum by a threat actor called UberLeaks, claiming to have breached the MDMs for Uber and Uber Eats, as well as third-party MDMs from Teqtivity and TripActions. Archives claiming to be source code from the breached MDMs were among the dumped data.

It is important for enterprises to consider that for each mobile device in the organization, there is additional technology from the vendor, the carrier, and, within the enterprise, supporting technology, such as cloud services and MDMs, that are all part of the mobile risk profile.

Mobile Threat Chains: The Anatomy of Multi-Phase Attacks

Mobile Threat Chains

Over the years, there have been plenty of examples of successful attacks against mobile devices and users. In the vast majority of cases, multiple steps needed to be executed before attackers achieved their end goal.

Threat chain terminology is used in cybersecurity to describe multiple consecutive threats that attackers utilize to compromise a specific network or system. When multiple related events are tagged to the same entity, then the significance of each event in the threat chain can increase. Each of these steps is required in order for the full attack to be successful.

For example, in the case of a phishing attack that seeks to steal data from the keychain, multiple steps need to be completed. In the event of an SMS-based phishing text, also known as smishing,

- The phishing link is delivered via SMS.
- The victim clicks on the smishing link.
- The victim is tricked into installing a malicious app.
- The app exploits known vulnerabilities to compromise the device.

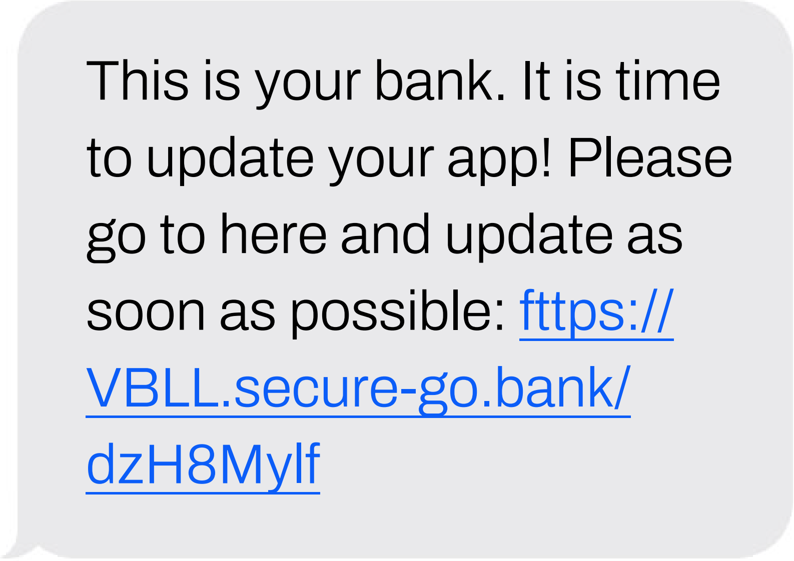
It is only after these steps have been completed that the attacker will have achieved their goal of stealing the keychain data (and likely other data that is on the device as well).

Key Takeaways

Here are the key takeaways associated with mobile threat chains in the last year:

- In order to establish effective, holistic mobile device security, it is vital to gain an understanding of threat chains that are occurring.
- With robust MTD defenses, teams can establish the safeguards that thwart these attacks.
- Over the past year, Zimperium MTD solutions have been able to identify and prevent many of these multi-phase attacks, as demonstrated in a few examples.

The following sections examine these and other key findings in more detail.



This is your bank. It is time to update your app! Please go to here and update as soon as possible: fttps://VBLL.secure-go.bank/dzH8Mylf

Often, some phases in the threat chain succeed due to a lack of, or failure of, technological safeguards. In other cases, user behavior will be to blame. The reality is that many existing defenses, such as carrier protections, are prone to failure. The fact that individuals receive phishing texts on an almost daily basis is proof of this reality.

In order to establish effective, holistic mobile device security, it is vital to gain an understanding of threat chains that are occurring. With the right visibility and capabilities, each step in the threat chain represents a potential opportunity to identify and stop an attack—before any damage is done.

Network Attacks

Malicious actors can use a variety of network-based attacks to achieve their objectives. For instance, they may set up a Wi-Fi network in a public location and wait for victims to connect to it. Additionally, they may conduct reconnaissance activities to gather information about their target.

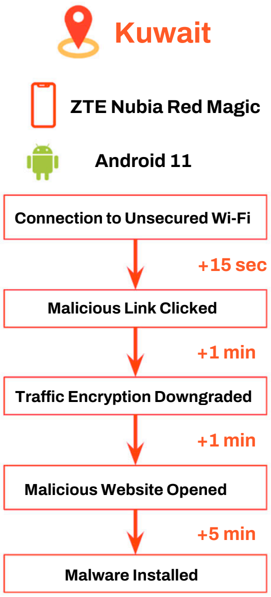
In the context of network security, reconnaissance refers to the initial phase of an attack where the attacker gathers information about the target network or system. This information can include IP addresses, network topology, operating systems, and services running on the network.

Reconnaissance is a critical step for an attacker as it helps them identify vulnerabilities and weaknesses that can be exploited in later stages of the attack. In one example, the attacker may use packet sniffing or port scanning techniques to collect unencrypted transmissions, which can reveal valuable information about the target network's configuration and potential vulnerabilities.

Once reconnaissance is done (and a target is chosen), the next part of the threat chain, such as a man-in-the-middle (MitM) attack, can unfold. MitM attacks are cybersecurity threats that occur when an attacker intercepts communication between two parties who believe they are communicating directly with each other. During an MitM attack, the attacker can eavesdrop on the communication, manipulate the message, or impersonate one of the parties involved.

MitM attacks can manifest in several forms, including the use of a rogue access point or Domain Name System (DNS) spoofing, where the attacker manipulates the DNS system to redirect users to a fake website. Other forms of MitM attacks include redirection of traffic to a phishing website, injection of malicious elements such as cryptominers, Transport Layer Security (TLS) downgrade where the attacker disables the use of encryption, session hijacking where the attacker takes control of a session between two parties or clones the session on a different browser, and Secure Sockets Layer (SSL) stripping, which downgrades secure HTTPS connections to unencrypted HTTP connections.

In 2022, Zimperium detected a range of network-based attacks. Here are a few examples.



Kuwait

ZTE Nubia Red Magic

Android 11

Connection to Unsecured Wi-Fi

+15 sec

Malicious Link Clicked

+1 min

Traffic Encryption Downgraded

+1 min

Malicious Website Opened

+5 min

Malware Installed

Malware Installed on Android Device in Kuwait

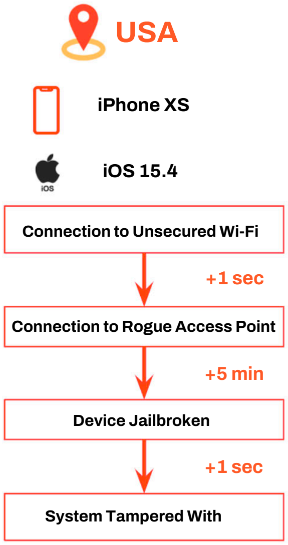
A mobile phone user in Kuwait was victimized in this case. They had a Nubia RedMagic device from the carrier ZTE and were running Android 11.

This threat chain resulted in an attacker installing malware on the device. The threat chain consisted of these steps:

- To start, the user connected to an unsecured Wi-Fi network.
- The user clicked on a malicious link.
- The threat actor employed a TLS downgrade to ensure the connection wasn't encrypted.
- Clicking the link brought the user to a malicious website.
- Upon loading the site, malware was installed on the device. Most likely, the user was prompted to install the code.

It is important to underscore that at some of these phases, teams could potentially employ manual, error-prone interventions to mitigate the threat. However, with an advanced MTD solution like Zimperium MTD, teams can establish automated actions that could have stopped the attack at each phase of this threat chain. Zimperium MTD could:

- Have automatically turned off the user's Wi-Fi as soon as they started to connect to the insecure network.
- Identify that the site was malicious and prevent the user from accessing the link.
- Detect that the malware was installed, and prompt the user, so they could delete it.



USA

iPhone XS

iOS 15.4

Connection to Unsecured Wi-Fi

+1 sec

Connection to Rogue Access Point

+5 min

Device Jailbroken

+1 sec

System Tampered With

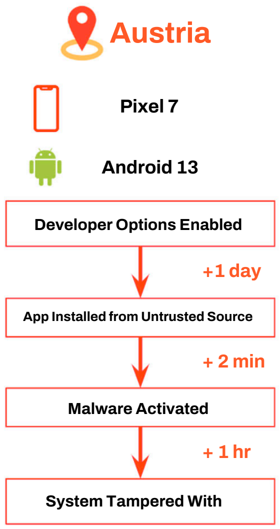
Attackers Jailbreak iPhone in US

In the US, an iPhone XS user running iOS 15.4 was targeted. The user connected to a rogue access point via an insecure Wi-Fi network.

Through a series of steps, the attacker was able to gain direct control over the device and jailbreak it. The attacker was then able to tamper with the system.

Here again, an advanced MTD solution like Zimperium MTD could have stopped this attack at several points. Zimperium MTD could:

- Have automatically turned off the user's Wi-Fi as soon as they started to connect to the insecure network or rogue access point.
- Identify attempts at jailbreaking.
- Detect system tampering.



Austria

Pixel 7

Android 13

Developer Options Enabled

+1 day

App Installed from Untrusted Source

+ 2 min

Malware Activated

+ 1 hr

System Tampered With

Device Compromise: Malware Infects Pixel 7 Device in Austria

In this example, a Pixel 7 user in Austria was targeted. The user's device had the Android 13 OS installed.

One day, the user enabled developer options on the device. The following day, the user sideloaded three different apps.

One of these apps turned out to be malicious.

An hour later, a system tampering event was identified, most likely when the victim opened the malicious application.

Within seconds, the application disabled SELinux, a Linux-based security module that can support access control policies. This demonstrates that the malware enabled the attacker to gain full control of the device.

Here again, an advanced MTD solution like Zimperium MTD could have stopped this attack at several points. Zimperium MTD could:

- Notify the security team that developer options were enabled.
- Issue a notification to the device user about the risks of enabling developer options.
- Detect sideloaded apps.
- Identify the presence of the malicious app on the device, and issue a warning.
- Detect system tampering.

How Fast Mobile Device Exploits Lead to Fast Corporate Breaches

The examples above show how quickly threat chains can lead to a successful action. In many cases, these multi-step threat chains can be executed in a few minutes and lead to a complete compromise of the device.

When it comes to attacks against employees' mobile devices, however, the problems don't stop there. Once initial compromises occur, it doesn't take long for attackers to gain access to corporate networks and begin to make lateral moves to locate and ultimately exfiltrate corporate assets.

The time between initial device exploit and time to corporate asset breach is defined as a mean time to mobile exploit (MTME). Based on Zimperium research, the MTME has been established to be two hours and 29 minutes. This is very consistent with the statistics seen in the context of traditional endpoint compromise. In other words, whether a traditional or mobile endpoint is compromised, the damage to corporate assets can happen rapidly—and be just as devastating.

How Malicious Actors Are Attempting to Bypass Apple Safeguards

The Pros and Cons of Apple's "Walled Garden"

For the vast majority of people, the Apple App Store is the only place to download mobile apps for their iOS devices. This is very much by design. Developed and maintained by Apple, the App Store is intended to be the only source for vetted mobile apps. It is a critical part of the Apple ecosystem, which is commonly referred to as Apple's "walled garden." In the walled garden, Apple hardware, software, and services all exist in a closed environment with controlled access to third parties (e.g., app developers).

In order to ensure the security of the apps it makes available to users, Apple has established a number of mechanisms around the process of submitting apps to the App Store. For example, Apple validates the developer certificate used to sign the app. The company has established capabilities for automated analysis of code being submitted, and occasionally conducts manual analysis as well. It is only after they have successfully passed these assessments that apps can be made available on the App Store.

Apple's walled garden strategy, including its fortified App Store, has its pros and cons. On the positive side, the App Store's stringent security measures work effectively to maintain a relatively malware-free environment for iOS devices. The App Store is widely regarded as a trusted source for apps due to Apple's strong track record of preventing malicious apps from getting into the stores, and removing any that have somehow bypassed initial detection. According to Apple, nearly 1.7 million app submissions were rejected from the App Store in 2022. Some of those were apps using malicious code with the potential to steal users' credentials from third-party services. In other instances, the App Review team identified several apps that disguised themselves as innocuous financial management platforms but had the capability to morph into another app.[50]

Key Takeaways

Here are the key takeaways associated with attackers' attempts to bypass Apple security in the last year:

- Historically, iOS devices have faced lower rates of malware than those encountered by Android devices.
- Malicious actors employ a number of tactics to lure people onto unsanctioned, third-party sites—and trick users into downloading malware.
- Attackers are also leveraging existing OS features to attempt to get malware installed on user devices (such as Profiles/ Shortcuts).

The following sections examine these and other key findings in more detail.

Circumvention Approaches

For malicious actors, the over 1.5 billion Apple users around the world represent a highly prized target. Zimperium researchers have observed several ways that malicious actors try to circumvent the App Store restrictions. Here are a few tactics that have been employed:

- **Third-party app stores & malicious profiles.** Rather than combat the impressive vetting of the official Apple App Store, malicious actors employ a number of tactics to lure people onto unsanctioned, third-party sites—and trick users into downloading malware.
- **TestFlight.** Designed for distributing code for testing, malicious actors are using this capability to distribute malware.
- **Malicious apps in disguise.** Malicious actors publish apps that appear safe upon initial inspection. It is only after users start to engage with the apps that the malicious or unsanctioned functionality is exhibited.
- **Abuse of automation and shortcuts.** iOS shortcuts were introduced in iOS/iPadOS 12 (although iOS/iPadOS 13 and above is recommended for full functionality). Shortcuts enable automation of various actions on the device and can allow a malicious actor to carry out different actions that are detrimental to users, including delivering malware.

The sections below offer more details about the security mechanisms in place in the App Store and the different approaches for circumventing these protections.

Third-Party App Stores & Malicious Profiles

As a general rule, malicious actors would opt to pursue their objectives by having their malicious apps installed by a victim. While mechanisms may be created that can directly exploit a mobile device, these approaches tend to be much more difficult and far less reliable.

To achieve their objectives, malicious actors try to get victims to download malware from unsanctioned third-party sites. To do so, they develop apps that violate Apple's terms of service but are sought-after by many people, such as apps for gambling, pornography, and crypto-currencies. In addition, they create apps that are purported to enhance the capabilities of widely-used apps. For example, Zimperium researchers have seen a "WhatsApp+" offering being promoted. The threat actors then attempt to lure victims into downloading those apps via third-party app stores.

In some cases, visitors are fully aware they are going to a third-party app store. In other cases, the user may not even realize that they're doing so. Often, users lack an understanding of the potential danger they're subjected to. To download an app from a third-party app store, a user must agree to the installation of a configuration profile. This is what enables the user to download an app outside of the standard App Store channels. Depending on the app promised, some users willingly grant this installation. In other cases, malicious actors may try a variety of different ways to dupe a user into granting the permissions necessary. For example,Zimperium has observed cases in which a user is promised that they are about to download the desired app, but in fact, they are installing the configuration profile, which in turn installs the malicious app.

It should be noted that these iOS third-party app stores are often accessed via a browser rather than directly, which does limit the success of attackers because only a portion of the overall iOS users will ever take the time and effort to access the stores.

TestFlight

Another way malicious actors circumvent the App Store's restrictions is by leveraging TestFlight. TestFlight is a service provided by Apple that enables developers to distribute early versions of their code for testing. By the very nature of TestFlight, these are typically apps that have yet to be published on the Apple App Store. Through TestFlight, malicious actors can send various links through social media that trick the user into installing the app. Once installed, the app can then execute the attacker's desired functionality.

In 2022, researchers discovered that an organized crime campaign known as "CryptoRom" was distributing fake cryptocurrency apps to iOS and Android users using TestFlight.[51]

In another example of this abuse, Meta identified a cybersecurity operation where threat actors had convinced victims to download an iOS chat application via Apple's legitimate TestFlight service.[52] The threat actors, which appear to be part of the Bitter APT Group, operate out of South Asia. The Bitter APT Group has been active since 2013 and has targeted victims in New Zealand, Pakistan, India, and the UK. The app appeared to support social engineering on a chat medium controlled by Bitter APT. The use of legitimate Apple services to distribute the app gave it the appearance of being more trustworthy.[53]

Malicious Apps in Disguise

Malicious actors have also bypassed Apple's security policies by publishing apps that appear benign upon initial inspection. To start using the app, users are required to enter a code. It is only after that code has been entered that the app begins to exhibit malicious behavior or enable activities that violate the App Store's terms of service. While these apps may bypass initial detection, they typically don't stay on the App Store long before they're detected and removed. However, the apps will still remain on end-user devices until manually deleted.

Risks of iOS Shortcuts

According to Apple's website, iOS shortcuts provide "a quick way to get things done with your apps, with just a tap or by asking Siri." While they are convenient for users, Zimperium has seen them used in malicious ways too.

There are multiple reasons why threat actors are having success leveraging shortcuts:

1. Even though iOS shortcuts are hosted on Apple's iCloud servers, they are unmanaged and do not undergo any sort of approval process (unlike apps being vetted before being allowed in the App Store).
2. Shortcuts are tied to an Apple ID, so they are not entirely anonymous; however, the author of a shortcut is not currently reflected in the Shortcuts UI. Moreover, it is up to the user to inspect the shortcuts' permissions and actions prior to installation. However, with enough complexity, most users will not spot any malicious behavior on a first glance. There is a reporting feature in the installation sheet, but the user needs to be able to differentiate between useful and harmful behavior.
3. If a user shares a shortcut, it will generate a new iCloud link, so the same potentially harmful shortcut will still be available through the new link even if the original one was already reported.
4. Shortcuts can be installed either from the "Shortcut Gallery" or from third-party locations. These third-party locations are essentially the same as "third-party app stores," but are solely used for shortcuts—and therefore exhibit the same risks to the user.

By leveraging these dangerous and nefarious shortcuts, threat actors can take several actions that are harmful to the user, like extraction of personal information, sending messages to a user's contacts, or opening websites with malware that, in turn, could compromise the device.

Below are shown examples of abuses and vulnerabilities associated with shortcuts:

- A vulnerability in the shortcut framework[54] allowed an attacker to add additional actions to applications. This was abused to exfiltrate files from outside the application sandbox.
- Shortcuts were used to perform path traversal[55] and copy any directory owned by mobile with all its data.
- Shortcuts were used to write files in system folders,[56] bypassing iOS permissions.
- The state-sponsored spyware Predator[57] used iOS shortcuts to achieve persistence in the filesystem and keep the surveillance tool enabled even after a reboot.

Network Threats: Millions of Attacks, and Counting

Here are a few of the key takeaways associated with network attacks in 2022. During the year, Zimperium detected:

Over
2.4M
man-in-the-middle (MitM) attacks

3.3M
unsecured networks

450K
devices connected to unsecure networks

1 MILLION
reconnaissance scans, which are often used by attackers to discover exploitable vulnerabilities on mobile devices

13,500
rogue access points

Trojans Jeopardize Mobile Banking, And More

Key Takeaways

Here are the key takeaways associated with banking trojans in the last year:

- Three out of four Americans (193 million) are using banking apps to perform daily banking activities like depositing checks, viewing account balances, or transferring financial assets.
- The financial services sector continues to experience increasingly sophisticated attacks by trojans designed to steal credentials and funds.
- The most prolific banking trojans include Teabot (targeting 410 or 64% of the 639 apps analyzed), and ExobotCompact.D/Octo (targeting 324 or 51% of the apps analyzed). Exobot/Compact.D/Octo also targets popular, non-financial apps for credential theft.
- The most targeted mobile banking application is BBVA Spain | Online Banking, with over 10 million downloads. This one application is the target of six of the ten reported banking trojans.

In the following sections, we examine these and other key findings in more detail.

Mobile Banking Heists Revisited

The Zimperium zLabs research team analyzes several hundred thousand apps each day with state-of-the-art machine learning models and other proprietary techniques. In this section, the research team provides an excerpt from a report that was published in 2022, where the team examined ten prolific banking trojans targeting Android mobile apps of users worldwide. The financial application targets covered in this report are available through the Google Play Store. A complete list of all 639 financial apps covering banking, investment, payment, and cryptocurrency services and the different banking trojan families targeting each is provided in the full Mobile Banking Heists report located here.

Today, financial customers have more access to their money and financial assets than ever before. Globally, bank branches have moved from the corner of Main Street to the palm of the customer's hand, where they can instantly access finances and move assets with the swipe of a finger. Attackers have evolved their approaches accordingly, and with increasing sophistication.

The number of potential attack vectors posed to mobile financial apps is endless and continues to increase yearly. Malicious actors no longer don masks—instead, turning to their computers and malicious code to plan the next digital heist. **Gone are the holdups, now replaced by benign-looking apps packed with malicious payload:** the banking trojan. These digital bank robbers are easy to distribute to the masses, hiding in plain sight and waiting for users to fall victim. With every financial services company providing convenient, mobile access, every customer is at risk of the ultimate digital bank robbery.

As the story goes, the Trojan Horse, a large wooden structure, was presented as a gift to the city of Troy—yet inside, enemies hid. Once the horse was brought into the city gates, the soldiers let more of their fighters in and waged an attack within the city gates. This is an appropriate analogy for the modern cyber threat that bears the trojan name. Trojans are malicious apps that are in some way disguised to trick a potential victim into believing they are legitimate. They can be hidden in apps such as productivity tools or games, waiting for the right time to deploy. Once inside a targeted device, this software can pursue several tactics, including gaining control of a system, disseminating malware to other systems, corrupting device data, or collecting sensitive information, credentials, or other assets.

There is a wide range of trojans, including Remote Access Trojans (RAT), backdoor trojans, Short Message Service (SMS) trojans, and many more. The use of trojans goes back to the 1970s with the creation of ANIMAL, and since then, the variants and uses have continued to increase. The first mobile-specific trojan made an appearance in 2004, infecting Symbian devices and spreading through Bluetooth.

The banking and financial services sector continues to experience increasingly sophisticated attacks by trojans, wreaking financial havoc across their customer base. Banking trojans are specially crafted to target mobile financial apps (though many are also versatile enough to target non-financial apps too). Banks, investment firms, cryptocurrency wallets, and more are subject to attacks by banking trojans in an attempt to steal money directly from victims.

Three out of four Americans (193 million) are using banking apps to perform daily banking activities like depositing checks, viewing account balances, or transferring financial assets, making them an active target for banking trojans. And nearly half of teens (48%) use mobile devices or websites to manage their money, putting their Personally Identifiable Information (PII) at risk without them or their guardians ever knowing.

The malicious actors behind banking trojans are counting on mobile apps and endpoints lacking comprehensive security solutions to detect and prevent their actions. With the growing number of mobile financial apps available to users, new targets are being added every day.

3 out of 4

Americans (193M) are using banking apps to perform daily banking activities like depositing checks, viewing account balances, or transferring financial assets, making them an active target for banking trojans.

Report Findings

Here are a few of the interesting findings from the Banking Heist report:

- **1 billion exposure points:** The targeted mobile banking, investment, payment, and cryptocurrency apps in this report have been downloaded over one billion times from the Google Play Store, globally.
- **Noteworthy trojans:**
  - Teabot is targeting 410 of the 639 apps tracked.
  - ExobotCompact.D/Octo targets 324 of the 639 apps tracked and is the only one targeting popular, non-financial apps for credential theft.
  - Sharkbot is only targeting four financial apps (with over 70,500,000 downloads, collectively), but they include two of the largest cryptocurrency trading services in the world.
- **Noteworthy targets:**
  - The most targeted mobile banking application is BBVA Spain | Online Banking, with over 10 million downloads. This one application is the target of six of the ten reported banking trojans. (Medusa, Xenomorph, Coper, Flubot, ExobotCompact.D/Octo, and Sharkbot).
  - Of the 639 apps covered in this report, 50 are related to investing in stocks, cryptocurrency, or portfolio management. Those 50 apps account for over 285,000,000 downloads from the Google Play Store, with Teabot targeting most of them, followed by ExobotCompact.D/Octo.
  - India's PhonePe mobile application has the largest attack surface for banking trojans to target, with over 100,000,000 downloads from the Google Play Store.

Most Targeted Countries

United States	121 apps targeted
United Kingdom	55 apps targeted
Italy	43 apps targeted
Turkey	34 apps targeted
Australia	33 apps targeted
France	31 apps targeted
Spain	29 apps targeted
Portugal	27 apps targeted
Switzerland	19 apps targeted

Top Targeted Financial Apps

PhonePe
India
100,000,000 downloads

Binance
Malta
50,000,000 downloads

Cash App
United States
50,000,000 downloads

La Banque Postale
France
10,000,000 downloads

Ma Banque
France
10,000,000 downloads

Caf - Mon Compte
France
10,000,000 downloads

Garanti BBVA Mobile
Argentina
10,000,000 downloads

Postepay
Italy
10,000,000 downloads

BBVA México
Mexico
10,000,000 downloads

Mobile Banking Trojan Capabilities

When it comes to the banking trojans disseminated today, there is a mix of both old and new techniques. Malicious actors deliver a core set of capabilities that are common across most trojans. However, they'll also add a mix of unique capabilities to more effectively pursue their objectives, whether that's to better evade detection, fool more victims, or better tailor their focus to a specific bank, geography, or target.

Many banking trojans share the following common characteristics and capabilities:

- **Dissemination.** Many trojans are spread through app stores, especially third-party app stores. Others are spread through SMS messages purporting to be from a recognized entity.
- **Deception**. To deceive potential victims, cyber attackers exploit consumers' familiarity and trust in name brands. They often try to make their messages and web pages appear as if they're coming from banks, as well as shippers, communication app vendors, and entertainment sites. They use this approach to lure unsuspecting targets to click on malicious links and download malware.
- **Exploitation.** Upon installation, many trojans target accessibility services, which can be used to steal login credentials through keylogging or to grant permission to malicious apps automatically. They can employ overlay attacks, pointing a victim to a fake banking login page that can be used to steal the credentials entered.
- **Communication and control.** Trojans often interact with command-and-control servers to share stolen data and establish remote control over devices. Trojans can also do real-time screen sharing with servers. They can generate and receive SMS messages, locate and spam contacts, and more.
- **Evasion.** In order to evade detection, trojans often hide the app icon from the operating system's launcher so users are less likely to discover the trojan's existence. They may also disable or take steps to avoid detection by anti-malware apps. A small number of trojans also take steps to avoid being uninstalled if detected by the victim.

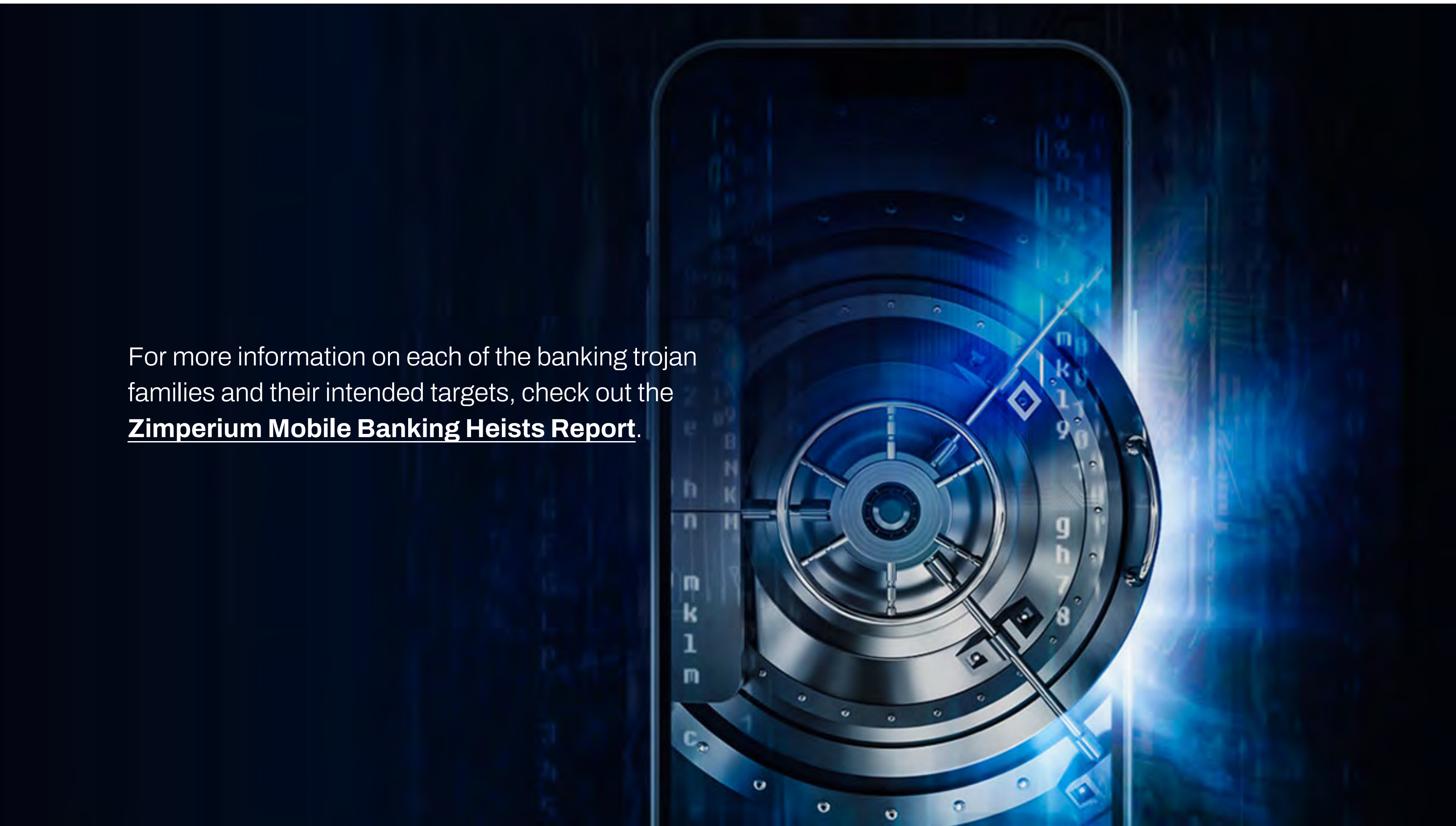
There are two styles of banking trojans targeting global mobile banking users. The first is part of a larger attack chain with features designed to exfiltrate banking credentials and data, as well as impact security controls like multi-factor authentication connected with the account holder's account. The second style adds features like screen scrapers and keyloggers, along with data input capabilities designed to steal money directly through the app when a user logs in.

Like other malware on Android, many banking trojans rely on social engineering and a victim's trust to enable access and permission for the app, allowing it to act as the device's admin. These steps allow the banking trojans to impact security controls, monitor the screen and text inputs, and ultimately enact the factory reset after the money is stolen from the victim. With this control and capability, advanced banking trojans can also capture any multi-factor authentication messages and inputs, bypassing security controls and user input.

The Risks of Inadequate Mobile Financial Application Security

The risks to the providers of financial apps are manifold and continue to negatively impact a business long after the initial attack. Here are some of the most damaging outcomes of a successful fintech security breach.

- **Data Theft:** Sensitive personal identifiable information (PII) and other valuable data, including names, passwords, and payment card details, can be easily accessed through compromised financial apps. Mobile banking trojans, such as Sharkbot and Medusa, and other mobile malware, use various techniques to exfiltrate data, including keyloggers, overlay screens, and exploiting accessibility services.
- **Regulatory Fines and Damage Payments:** A wealth of global legislation on data security outlines the penalties for breaches of financial app security. For instance, under the E.U.'s General Data Protection Regulation (GDPR), a firm may be fined up to 4% of its global revenue if they suffer a breach. In addition to fines, breached companies may be required to pay significant compensation to affected users. A notable example is the $300 million (potentially rising to $425 million) compensation fund that Equifax was ordered to set up after they were found negligent in securing their customer data.
- **Loss in Customer Confidence:** Customers lose trust in companies that suffer cybersecurity breaches. Research shows that 83% of U.S. consumers would stop doing business with an affected firm for at least a few months, while over 40% of U.K. customers said they would never do business with them again. Moreover, it costs more to gain new customers. These costs arise from the extra marketing spend needed to repair brand reputation and business model changes, such as increased product discounts or charging lower service rates.
- **Stolen Assets Used in Fraud:** Banking apps contain various items of direct monetary value, including the ability to transfer money, the ability to buy and sell stocks and cryptocurrencies, and payment tokens used for mobile transactions. Theft of these assets will directly lead to fraud and damage for the consumers and banks. According to a recent report by the Federal Trade Commission,[58] consumers reported a 70% increase in fraud from 2020 to 2021, equating to more than $5.8 billion.[59]



For more information on each of the banking trojan families and their intended targets, check out the **Zimperium Mobile Banking Heists Report**.

Securing Mobile Payments in 2023 and Beyond

Innovation is happening rapidly in the financial and mobile payment industry. With the introduction of new standards and innovations, the software-based point-of-sale (SoftPOS) segment is poised for exponential growth; but only if critical security challenges are addressed. There is much more to come now that the Payment Card Industry (PCI) has delivered an appropriate industry-wide standard for SoftPOS on commercial, off-the-shelf (COTS) devices. To read the latest content from Zimperium on this topic, visit zimperium.com/mobile-payments/

An Introduction to SoftPOS and Why It's Poised for Extreme Growth

In the POS market, SoftPOS is gaining significant traction. SoftPOS is the practice of using a smartphone to accept contactless card and mobile payments via a mobile application instead of a hardware payment terminal. In addition, these SoftPOS solutions enable merchants to receive payments on Near Field Communication (NFC) enabled mobile devices, such as Android or iOS smartphones and tablets.

SoftPOS isn't new. Small merchants and payment brands have been piloting mobile apps to accept contactless payments for a few years now, and solution providers like MyPinPad, Rubean, Amadis, VivaWallet, Synthesis, and PayFelix have emerged to serve this burgeoning market. To date, SoftPOS solutions have predominantly been available for Android devices. In 2020, Apple acquired Mobeewave, one of the first SoftPOS solution providers, and unveiled its own SoftPOS solution, Tap to Pay on iPhone, in 2022. However, SoftPOS has not yet been widely adopted by merchants. One key reason for this is the fact that the Payment Card Industry (PCI) has only just now delivered an appropriate industry-wide security standard for SoftPOS on commercial, off-the-shelf (COTS) devices. This new standard is the Mobile Payments on COTS (MPoC) standard that was released at the end of 2022.

Key Takeaways

Here are the key takeaways associated with mobile paymentsin the last year:

- The Payment Card Industry (PCI) released the new Mobile Payments on COTS (MPoC) standard at the end of 2022. MPoC supports the secure delivery of software-based point-of-sale (SoftPOS) on commercial, off-the-shelf (COTS) devices.
- The new MPoC standard introduces a fundamental change from highly prescriptive to objective-based security requirements, changing the approach from simplistic compliance to actual security assurance.

The following sections examine these and other key findings in more detail.

The Emergence of MPoC and the Implications

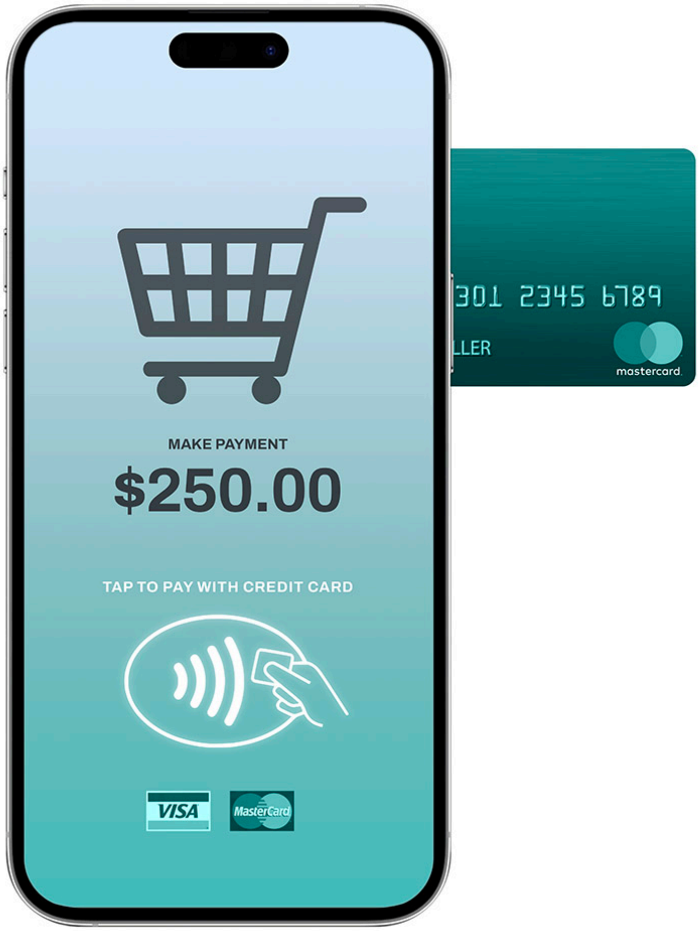
MPoC aims to provide an industry-wide standard for SoftPOS solutions. By complying with the standard, SoftPOS solutions will enable merchants to receive payments securely on NFC-enabled devices, including smartphones and tablets running on Android and iOS. PCI MPoC will accelerate merchants' transition to digital transactions and the global adoption of SoftPOS solutions by small and micro merchants, but also larger retailers and adjacent markets where SoftPOS technology can be beneficial (e.g., transportation and authentication).

Why MPoC Is Different

Until the end of 2022, PCI had two standards in the mobile payments arena: the Software-based PIN Entry on COTS (SPoC) standard and the Contactless Payments on COTS (CPoC) standard. These existing standards imposed restrictions for solution developers and end-users as they either had to use an external physical device (the secure card reader in the case of SPoC) or could not accept payment above the cardholder verification method (CVM) limit, as PIN was not supported in the case of CPoC. In contrast to these existing standards, the new MPoC standard introduces modularity, new certification options, and new use cases, including support for offline transactions, component certification, and software-based PIN without the need to use a secure card reader.

Next to the functional expansion and advancements in the certification options, the MPoC standard introduces a fundamental change for PCI in the security requirements themselves, which are moving from highly prescriptive to objective-based security requirements.

The objective-based security requirements bring an important shift from prescribing what a developer must do (for example, obfuscate code) to what the solution needs to achieve (in the same example, that is, be highly resistant to reverse engineering). This critical change in the nature of the security requirements not only brings more design and implementation freedom to developers but also changes the approach to security from simplistic compliance to actual security assurance. This shift is like comparing the "letter of the law" to the "spirit of the law." By enabling any merchant to accept electronic (card or mobile-based) payments instead of cash, SoftPOS offers enormous potential. However, moving from traditional hardware-based POS technology to SoftPOS solutions comes with a challenge.



Why Security is Key to Realizing the Potential of MPoC

The PCI MPoC standard is expected to accelerate merchants' global adoption of SoftPOS solutions. To participate in the growth that will be fueled by the MPoC standard, developers will need to have their solutions PCI MPoC certified. This certification requires solutions to be evaluated by PCI-accredited security labs to ensure that the solutions effectively comply with the security requirements of the standard, which includes measurable security robustness requirements. In contrast to PCI SPoC and CPoC, solution developers aiming to gain MPoC certification must ensure that their SoftPOS solutions meet the attacker resistance thresholds as specified in the MPoC's security requirements. This includes the protection of cryptographic keys and resistance to advanced reverse engineering and tampering of the SoftPOS mobile apps. In addition, solutions must offer visibility into threats and compromise of the COTS platform as part of the attestation and monitoring system. These requirements are defined to prevent the disclosure or manipulation of assets such as the cardholder's primary account number (PAN) and PIN data.

The High Stakes of Addressing Security Imperatives

To guard against attacks and subsequent fraud, SoftPOS solutions must resist all relevant attacks and threat actors, including malware, criminal organizations, remote attackers, and malicious actors with physical access to the device running the SoftPOS app. The stakes are high. If the SoftPOS app isn't adequately protected, the solutions can be abused in several ways, including consumers or attackers faking or refunding payments, merchants performing unauthorized transactions, and criminal organizations collecting card data for card-not-present fraud (CNPF). Further, as the scale of SoftPOS adoption grows, the scale of this exposure will expand as well, exposing merchants, payment processors and issuers, and ultimately consumers.

To learn more about the most critical requirements for securing SoftPOS solutions, including the specific threats that need to be addressed, why other approaches are falling short, and how Zimperium solutions uniquely address the demands, read the full paper here.

4.3

Mobile Apps and Insecure Cloud Storage: A Dangerous Mix

Key Takeaways

Here are the key takeaways associated with unsecured cloud storage:

- 2% of all iOS and 10% of all Android mobile apps accessed insecure cloud instances.
- 30% of the inspected unsecured cloud storage instances expose potentially sensitive information, such as passwords, encryption keys, and personally identifiable information.

The following sections examine these and other key findings in more detail.

We use mobile apps. A lot of mobile apps. During 2022, mobile device users downloaded 255 billion apps.[60] In addition, the digital transformation driving enterprise cloud usage continues to create explosive growth. Between 2015 and 2022, the percentage of corporate data stored in the cloud doubled, moving from 30% to 60%.[61]

There are three primary types of cloud storage in use. These include object storage, file storage, and block storage. File storage is the best choice for organizing data in a hierarchical folder and file format. Object storage is designed to handle unstructured data, while block storage stores data in the form of blocks, making it an efficient choice for enterprise applications that utilize databases.

As an example, Google Cloud is a general-purpose cloud storage service that can be used to store any type of data. On the other hand, Google Firebase is a cloud storage service that is specifically designed for mobile and web applications, providing features such as real-time data synchronization, offline access, and user authentication.

All of this cloud infrastructure is highly attractive for mobile app developers. As organizations increasingly rely on cloud environments, mobile app developers are following suit by leveraging cloud infrastructure to the greatest extent practical. One way developers accomplish this is by utilizing cloud-based storage. This approach offers several advantages, but also exposes potential security risks.

The team at Zimperium does extensive research into the apps that are being downloaded from the major app stores. In fact, the team has analyzed thousands of mobile apps over the course of 2022. As part of the extensive investigation and monitoring of these apps, Zimperium analyzes the cloud storage instances that these apps access. The team then specifically looks at which instances have read permissions without requiring any authentication. Across the entire database of inventoried mobile apps, 2% of all iOS and 10% of all Android mobile apps accessed insecure cloud instances.

Here's a breakdown of the type of cloud storage instances being accessed that don't require authentication to access:

- **40%** are Google Firebase instances
- **25%** are Google Cloud Platform instances
- **23%** are Amazon S3 instances
- **11%** are Microsoft Azure Cloud Storage instances

It is important to note that this problem is not the fault of the cloud providers. Google, Microsoft, and AWS all offer options for employing authentication on their storage instances. In fact, AWS has even made authentication part of the default configuration for S3 instances. The problem is that development teams aren't configuring their cloud instances properly to leverage these protections.

A Small Number of Insecure Instances Present a Big Threat

Out of all the apps accessing unprotected cloud storage instances, 60% are accessing a very small percentage of instances, roughly 1%. The research team suspects that this small percentage of unprotected instances is offered by service providers or featured within specific software development kits (SDKs). This underscores how even a small number of unprotected instances or improperly configured apps can introduce a lot of exposure.

The Threat: Approximately 30% of Insecure Instances Expose Sensitive Data

For legal reasons, Zimperium doesn't inspect the contents of exposed Google Firebase instances, so the research team has no way of knowing how many of those instances may expose sensitive data. Of the remaining insecure cloud storage instances inspected, the team found roughly 30% expose potentially sensitive information, such as passwords, encryption keys, and personally identifiable information.

Too often, developers are unaware of the risk posed by these unprotected storage instances.

Consequently, any time these exposed cloud instances are deployed, there's always the risk of developers unwittingly starting to use them to store sensitive assets. Put another way, just because 70% of instances don't hold sensitive data today, doesn't mean they won't tomorrow.

Cybersecurity in software development is not always about a lack of awareness. Developers often give priority to releasing their products, placing security as a secondary concern, or not considering it at all. As a result, if the development team fails to evaluate and address the risk of overlooking security, both the organization and the application's users may be exposed to vulnerabilities, potentially leading to a breach that could go undetected until the damage is already done.

OWASP Mobile Top 10 and MASVS Standards: What They Say, How they Can Help Developers Create Secure Apps

Key Takeaways

Here are the key takeaways from Zimperium's analysis of the OWASP and MASVS standards within health, financial, and retail apps as reviewed in the last year:

- The OWASP Mobile Top 10 and Mobile Application Security Verification Standard (MASVS) help mobile application developers build secure mobile apps.
- There are more standards violations on Android than there are on iOS.
- While violations are heavily skewed toward security risks on both platforms, it is even more pronounced on iOS.
- There are more high-severity OWASP violations on iOS than on Android.

The following sections examine these and other key findings in more detail.

OWASP Helps Mobile App Developers

Overall, industry standards provide a valuable set of best practices and guidelines that help mobile app developers create high-quality, reliable, and secure software products that meet the needs of their target audience. Mobile app developers rely on industry standards for several reasons:

- Adhering to industry standards ensures interoperability, compatibility, and quality of software products across different platforms and devices.
- Industry standards provide a common framework that reduces the need for developers to create custom solutions, saving them time and effort.
- Following industry standards helps developers stay competitive by keeping up with the latest trends, technologies, and customer expectations.
- Industry standards also help ensure the security and privacy of mobile apps and their users by providing best practices for data protection, encryption, and authentication.
- Some industry standards are also required for specific market verticals.

Specifically, the OWASP Mobile Top 10 and MASVS help mobile application developers build secure mobile apps.

After explaining the intent and importance of each standard, the following section will show how a set of financial services, medical, and retail mobile apps fared in testing against both of them.

How Does OWASP Mobile Top 10 Help?

OWASP Mobile Top 10 is a list of the top 10 security risks associated with mobile apps. The purpose of this list is to provide guidance to mobile application developers, security professionals, and end-users on the most common vulnerabilities and threats that exist in mobile apps.

By following the recommendations outlined in the OWASP Mobile Top 10, developers can create more secure mobile apps that protect sensitive user information and prevent malicious attacks. Similarly, organizations can use the list to evaluate the security of mobile apps they use or plan to deploy, and end-users can use the list to make informed decisions about the mobile apps they download and use on their devices.

How Does MASVS Help?

The OWASP MASVS is the industry standard for mobile application security. It provides a comprehensive set of security controls that can be used to assess the security of mobile apps across various platforms (e.g., Android, iOS) and deployment scenarios (e.g., consumer, enterprise). The standard covers the key components of the mobile app attack surface, including storage, cryptography, authentication and authorization, network communication, interaction with the mobile platform, code quality, and resilience against reverse engineering and tampering.

But Are Apps Really Compliant with OWASP?

To demonstrate the value of the OWASP standards, the Zimperium zLabs team analyzed the iOS and Android versions of the top 100 apps across three critical verticals. For brevity and clarity, the OWASP Top 10 is being used to demonstrate how the apps fared against the standard. The MSVS findings were in sync with this data. Only the "average number of OWASP & MSVS risks identified per app ("violations") includes the MASVS findings. Findings are as follows:

Financial Services

	iOS	Android
Average OWASP Privacy related findings %	9	10
Average OWASP Security related findings %	91	86
Average OWASP % of findings with high severity	32	8

	iOS	Android
Top OWASP & MSVS Risk Areas	Cryptography Binary Protections Network KeyChain	Cryptography Binary Protections Network Vulnerability File System Database

Medical Industry

	iOS	Android
Average OWASP Privacy related findings %	7	10
Average OWASP Security related findings %	93	85
Average OWASP % of findings with high severity	20	4

	iOS	Android
Top OWASP & MSVS Risk Areas	Cryptography Binary Protections Network KeyChain Telephony	Cryptography Binary Protections Network Vulnerability File System Database

Retail Industry

	iOS	Android
Average OWASP Privacy related findings %	15	9
Average OWASP Security related findings %	85	85
Average OWASP % of findings with high severity	13	5

	iOS	Android
Top OWASP & MSVS Risk Areas	Cryptography Binary Protections Network KeyChain Telephony	Cryptography Binary Protections Network Vulnerability File System Database

In summary, the data shows:

- There are more standards violations on Android than there are on iOS.
- While violations are heavily skewed toward security risks on both platforms, it is even more pronounced on iOS.
- Perhaps not surprisingly, retail apps had a higher percentage of privacy-related violations than the other industries.
- There are consistently more high-severity violations on iOS than on Android.
- Medical apps have noticeably more high severity findings on iOS than the other industries. The financial services industry has the same distinction on Android.
- The top risks identified include insufficient or insecure practices around cryptography, binary protection, network communications, and data storage.

This analysis clearly demonstrates the importance of evaluating mobile apps against standards like OWASP and MASVS. Zimperium highly recommends developers build this into their development process.

Top OWASP Risk Areas

1 Cryptography Requirements

These findings indicate the mobile app's cryptographic mechanisms were not **designed or implemented securely**. As a result, sensitive data and communications may not be well protected from unauthorized access or modification.

2 Resilience Requirements

The findings indicate a lack of binary protections that may expose the application and its owner to various technical and business risks if the underlying application is insecure or exposes sensitive intellectual property. Without binary protection, an adversary can quickly analyze, reverse-engineer, and modify a mobile app.

3 Network Communication & Requirements

These findings indicate that mobile app developers **have not built secure network communication** into their apps. Therefore, sensitive user data may not be adequately protected from network-based attacks.

4 Data Storage & Privacy Requirements

Data storage and privacy requirements in mobile apps are important for protecting user data from unauthorized access or misuse. These findings indicate violations that can result in serious implications, such as data breaches, compliance violations, loss of user trust, and negative media attention. Therefore, it's important for app developers to follow these requirements to protect user data and avoid legal and reputational damages.

4.5

Mobile Application Security: Mobile Security Lab Perspective

Anis Hamdi, Senior Security Analyst, Riscure

Mobile apps have become an essential part of our daily lives. From communication and banking to entertainment and healthcare, mobile apps play a vital role in our daily activities. This trend will continue with the popularization of use cases that will test our ability to properly secure mobile apps, e.g., Identity services. With the increasing use of mobile devices for handling more sensitive information and services comes the growing risk of attacks on vulnerable software. What matters to an attacker is the cost/benefit. Therefore, as the stakes get higher, the cost of performing an attack must also increase accordingly.

The major takeaway from mobile application evaluations conducted by Riscure is that **practical security should be prioritized over blind compliance**. A lack of knowledge regarding attacker capabilities and possible countermeasures to protect apps also leads to a false sense of security among mobile developers.

Our evaluations often prove that for strong attacker models, the implemented security is lacking. This can be attributed to various factors, including inadequate security design during the development phase and a lack of awareness of potential security risks.

To mitigate these risks, it is important to prioritize security during the entire development and production cycle. Consider what information is sensitive and what tools are needed to protect the solution, and perform regular security testing and comprehensive security assessments to identify vulnerabilities and weaknesses that should be addressed. Essential security practices include implementing robust security measures, embracing the best secure coding practices, regular security testing, and security awareness training.

In order to further reduce security risks, incident response must consider each component of the product's chain, all the way from the device to the backend database.

In conclusion, mobile security is a critical aspect of our connected world, and it is essential to have a comprehensive view of the solution from design to decommission. As the trend to move more sensitive information to our mobile devices continues, the security need for those solutions will only increase.

About Riscure

Riscure is a leading vendor of security testing tools and training for edge devices. Our tooling helps global technology leaders to build robust hardware and software solutions. Riscure security analysts bring top-notch security expertise to development teams and aim to run no-pain certification projects. Built on a wealth of security research and extensive practical experience, Riscure is well recognized for its technical leadership. Riscure serves Semiconductor, Mobile Security and Mobile Payment, Automotive, and Premium Content industries as well as the Government sector.

riscure

4.6

Cryptographic Key Security: A Must for Mobile App Security

Key Takeaways

Here are the key takeaways associated with cryptographic key protection for mobile in the last year:

- In the realm of mobile apps, software-based encryption approaches pose a significant risk. In many cases, attackers can access key material by doing static analysis of the application.
- White-box cryptography, developed to address the risks of software-based encryption, is critical to securing mobile apps.

The following sections examine these and other key findings in more detail.

Cryptography refers to the process of encrypting and decrypting data. When data is encrypted, sophisticated mathematical algorithms are used to convert the data into an undecipherable ciphertext. To decrypt data or convert it from ciphertext back into its original form, a cryptographic key is needed. It is only when the key is provided to the decryption service or platform that the data can be accessed.

There are many different types of cryptographic algorithms, offering a wide range of security levels and performance characteristics. Some algorithms employ symmetric cryptography. This means the same key is used for both encryption and decryption. Asymmetric cryptography, also known as public key cryptography, involves a pair of keys: a public and a private key. Data that is encrypted with the public key can only be decrypted with the corresponding private key.

Transport Layer Security (TLS) is a commonly used protocol that is used to secure communications over a computer network. TLS is a building block for the Hypertext Transfer Protocol Secure (HTTPS) standard, which is employed by the vast majority of websites. (Diffie-Hellman Key Exchange is another important encryption approach. Through this method, two parties can securely exchange cryptographic keys over insecure and public channels.)

Generally, a given application will use multiple cryptographic schemes and protocols, depending on the nature of the operations performed and the relevant security requirements. In most cases, it is sound security practice to use a given key for a single purpose, such as encrypting a credit card number. Consequently, most apps will have several, potentially even dozens, of keys.

Keys: Encryption’s Achilles Heel

Most encryption approaches are based on a fundamental assumption: An attacker will not be able to gain access to the cryptographic key. These approaches effectively guard against a “black box” attack, one in which a threat actor somehow bypasses encryption without having access to the key.

In many implementations, cryptographic operations run in software. As a result, key values end up being stored within the application or passed as a parameter to the underlying cryptographic process. This represents a critical vulnerability. In many cases, attackers can access key material by doing static analysis of the application. In addition, they can employ debuggers and other dynamic tools to run apps and intercept communications. This form of attack is known as a “white-box” attack because the attacker can see inside the software-based encryption “box.”

Mobile Devices Further Expose Vulnerabilities of Software-Based Encryption

In the realm of mobile apps, software-based encryption approaches pose even more risk. Applications and cryptographic processes run within the mobile device, which is susceptible not only to remote attacks but also to physical theft. When the devices holding the keys and sensitive assets are stored on the device, and the device gets into the hands of a malicious actor, they're highly vulnerable to exposure and theft. Consequently, cryptographic processes—and the assets they were employed to secure—are highly vulnerable.

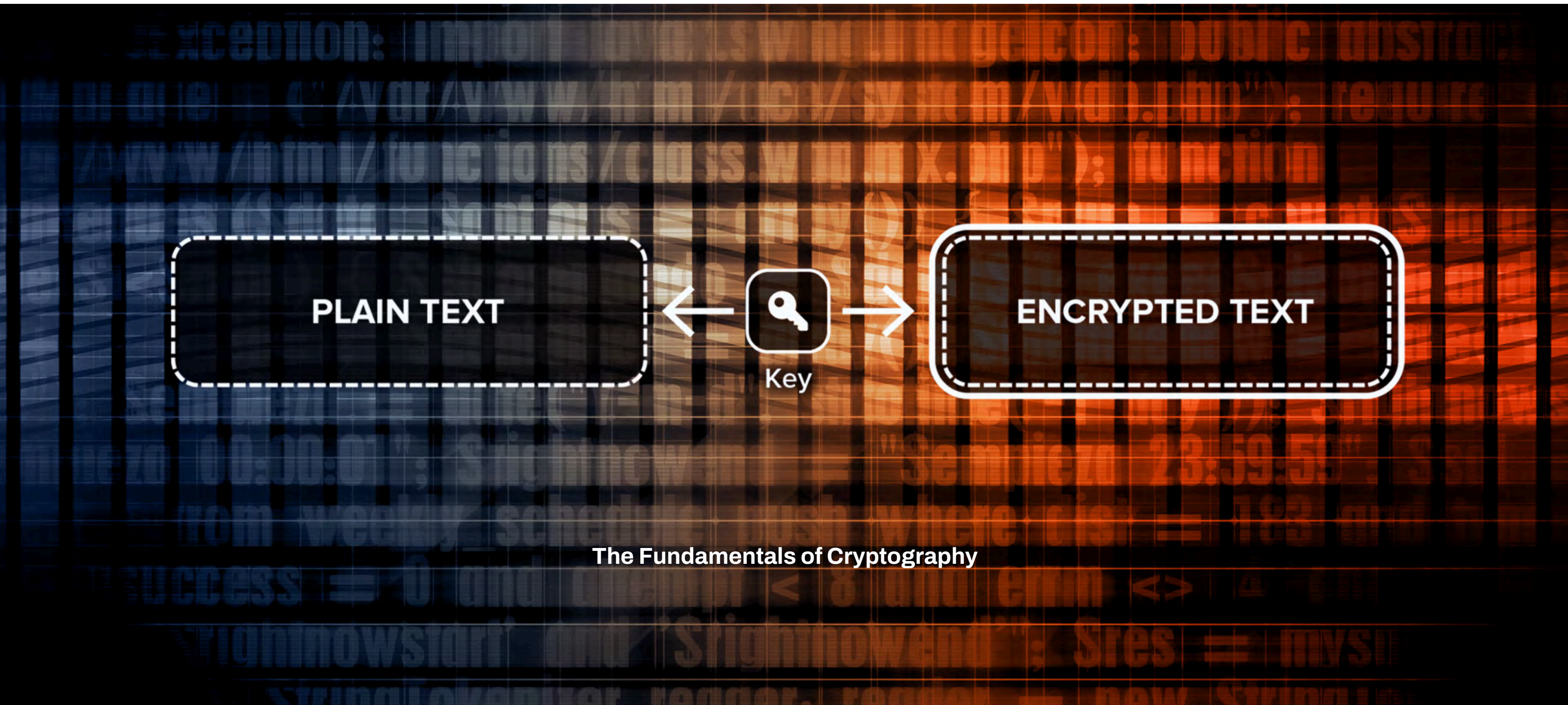
White-Box Cryptography

White-box cryptography was developed to address the risks of software-based encryption. Introduced in the early 2000s, white-box cryptography employs mechanisms to safeguard cryptographic key material. The goal is to ensure that keys are never exposed in any form, whether statically in the code or dynamically in memory. This ensures that attackers can't find and exfiltrate cryptographic keys using reverse engineering or dynamic inspection techniques. Through white-box cryptography, cryptographic keys and encrypted data will remain safe, even if a mobile device is stolen or compromised.

Common Uses for White-Box Cryptography

White-box cryptography is used in a wide range of apps, particularly those that store keys in memory and require strong protection against attacks. Here are a few of the most common apps:

- **Digital rights management (DRM).** Around the world, teams use white-box cryptography to protect copyrighted content, such as music, movies, and software. White-box cryptography can be used to protect the encryption keys used in DRM systems, making it difficult for attackers to extract the keys and bypass DRM protections.
- **Mobile payment systems.** White-box cryptography is being used in many mobile payment scenarios, helping protect sensitive financial data, such as credit card information. Through this cryptographic approach, teams can secure the keys used to encrypt these assets, ensuring threat actors can't decrypt data.
- **Communications.** White-box cryptography is also being used to secure communication apps such as instant messaging and email. By safeguarding the keys used in the encryption of these communications, teams can guard against malicious actors accessing keys and encrypted messages.



The Fundamentals of Cryptography

Why Advanced, Robust White-Box Cryptography is Essential

Black-box attacks against properly implemented cryptography remain very difficult; in most cases, they are only possible through the employment of quantum computing systems, which at this point, are a largely theoretical threat. For this reason, attackers continue to employ white-box attacks, seeking to gain access to cryptographic keys.

These threats are being fueled by the continued technical advances of attackers. For example, white-box encryption has been exposed by so-called "differential" attacks. These attacks can take various forms, such as differential fault analysis. This tactic is employed by trying to induce faults in a cryptographic system in order to reveal its internal states, including cryptographic materials such as keys.

These differential attacks are highly automatable and are available even to unsophisticated attackers, which underscores the ongoing, cat-and-mouse nature of cryptography and security. It is for these reasons that advanced, adaptable white-box cryptography mechanisms must be employed.

Conclusion

Ultimately, the security afforded by cryptography is only as strong as the security that surrounds encryption keys. Any time encryption keys are vulnerable, so too is the encrypted data. As mobile devices continue to be used for an increasingly important set of tasks, such as banking, shopping, multi-factor authentication, and more, the need for state-of-the-art white-box cryptography continues to grow more critical and widespread.

Conclusion

In this year's report, Zimperium has sought to distill some of the most important changes and developments that shaped the mobile security landscape and that are most critical to respond to in 2023.

This report draws on the research of internal experts, and the insights of Zimperium partners and leading industry observers. Thanks very much to all those contributors who have made this report possible.

In conclusion, here are the top three takeaways from this year's report.

Mobile-Powered Business Initiatives Are Here for Good

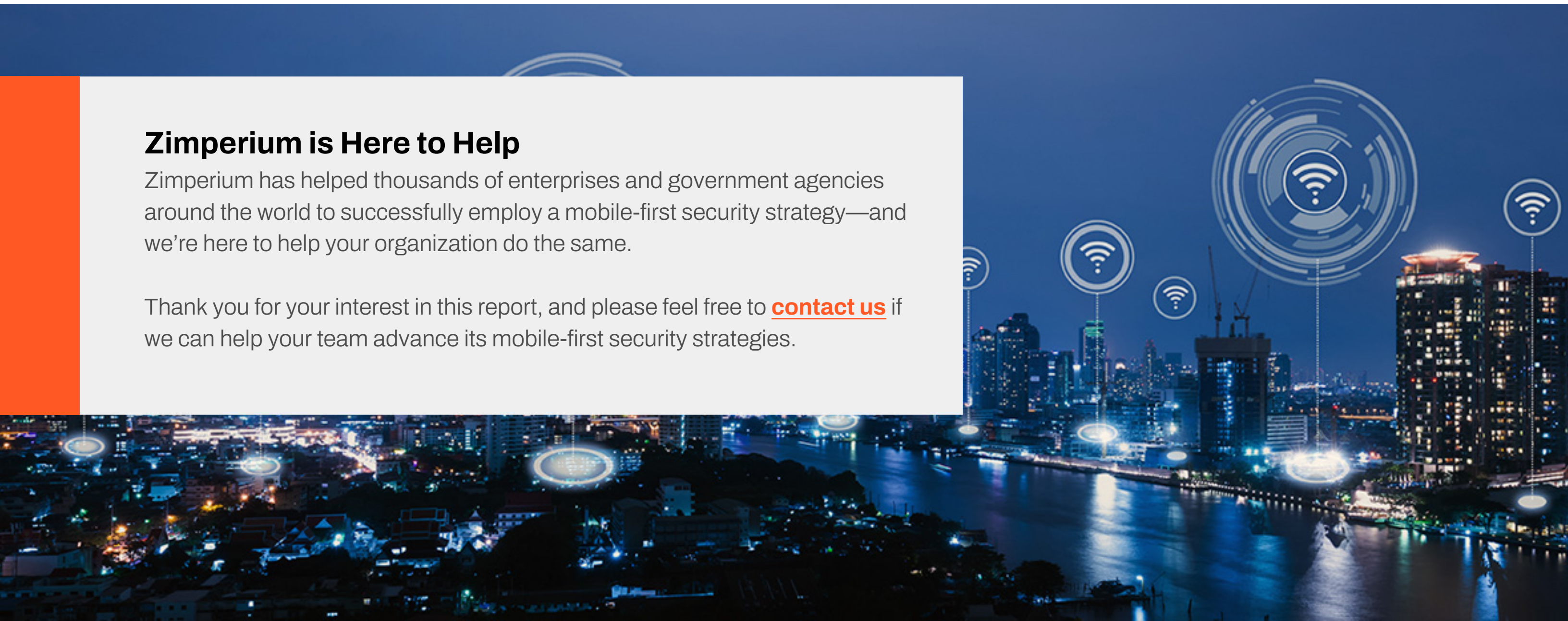
Mobile devices continue to get more integral to the daily lives of billions of users around the world. These are now the go-to devices for shopping, banking, entertainment, healthcare, and so much more. For employees, the mobile device is now an integral tool for getting work done. Given these realities, mobile-powered business initiatives only continue to grow to be more strategic. Delivering more, and more advanced, mobile-powered services represents a key requirement for an organization's success today, and will remain a key imperative moving forward.

Mobile-Powered Businesses Are Under Attack

The mobile-powered initiatives of today's enterprises and government agencies are under attack. Sophisticated cyber criminals and nation states continue to expand and refine their capabilities, which means the volume and sophistication of their attacks continue to grow. Leveraging tactics like spyware, phishing, and ransomware, attackers continue to succeed in exploiting vulnerabilities and duping users. In the process, it isn't just individual mobile device users, but entire enterprises that are being exposed.

Mobile-First Security Strategy is a Must

Fundamentally, this is the key issue: How do organizations capitalize on the opportunities of being mobile-powered—without being exposed to existential risk? To survive, let alone thrive, teams must employ a mobile-first security strategy. As outlined in the introductory section, a mobile-first security strategy is composed of five key principles. By applying these principles, teams can establish advanced, adaptive protections that safeguard against device, network, phishing, and app attacks.



Zimperium is Here to Help

Zimperium has helped thousands of enterprises and government agencies around the world to successfully employ a mobile-first security strategy—and we're here to help your organization do the same.

Thank you for your interest in this report, and please feel free to **contact us** if we can help your team advance its mobile-first security strategies.

5.2

Sources

1 Statista, “Forecast number of mobile users worldwide from 2020 to 2025,” URL: https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/#:~:text=In%202021%2C%20the%20number%20of,to%207.26%20billion%20by%202022.

2 Statista, “Mobile app usage – Statistics & Facts,” November 2022

3 Statista, “eCommerce – Worldwide,” 2022, URL: https://www.statista.com/topics/1002/mobile-app-usage/

4 Insider Intelligence, “State of mobile banking in 2022: top apps, features, statistics and market trends,“ April 15, 2022,URL: https://www.insiderintelligence.com/insights/mobile-banking-market-trends/

5 Statista, “Value of e-commerce losses to online payment fraud worldwide from 2020 to 2023,” October 2022, URL: https://www.statista.com/statistics/1273177/ecommerce-payment-fraud-losses-globally/

6 RSA, “RSA Quarterly Fraud Report,” 2022

7 Verizon, “2022 Mobile Security Index,” URL: https://www.verizon.com/business/resources/reports/mobile-security-index/

8 Verizon, “2022 Mobile Security Index,” URL: https://www.verizon.com/business/resources/reports/mobile-security-index/

9 Verizon, “2022 Mobile Security Index,” URL: https://www.verizon.com/business/resources/reports/mobile-security-index/

10 The Radicati Group, Inc., “Mobile Statistics Report, 2021-2025,” URL: https://www.radicati.com/wp/wp-content/uploads/2021/Mobile_Statistics_Report,_2021-2025_Executive_Summary.pdf

11 Statista, “Mobile internet usage worldwide - Statistics & Facts,” Ceci, L., January 2023, URL: https://www.statista.com/topics/779/mobile-internet/#topicOverview

12 Statista, “Mobile internet usage worldwide - Statistics & Facts,” Ceci, L., January 2023, URL: https://www.statista.com/topics/779/mobile-internet/#topicOverview

13 Zippia, “40 Fascinating Mobile App Industry Statistics [2023]: The Success of Mobile Apps in the U.S.,” Jack Flynn, March 20, 2023, URL: https://www.zippia.com/advice/mobile-app-industry-statistics/

14 Statista, “Leading smartphone users activities worldwide from July 2021 to June 2022,” September 2022, URL: https://www.statista.com/statistics/1337895/top-smartphone-activities/

15 Zippia, “25+ Incredible US Smartphone Industry Statistics [2023]: How Many Americans Have Smartphones,” Chris Kolmar, March 2, 2023, URL: https://www.zippia.com/advice/us-smartphone-industry-statistics/

16 Zippia, “40 Fascinating Mobile App Industry Statistics [2023]: The Success of Mobile Apps in the U.S.,” Jack Flynn, March 20, 2023, URL: https://www.zippia.com/advice/mobile-app-industry-statistics/

17 https://www.mordorintelligence.com/industry-reports/byod-market

18 https://www.protocol.com/bulletins/uber-breach-hacker-twilio-mfa

19 Bleeping Computer, “Ransomware profits drop 40% in 2022 as victims refuse to pay,” Toulas, B., January 2023, URL: https://www.bleepingcomputer.com/news/security/ransomware-profits-drop-40-percent-in-2022-as-victims-refuse-to-pay/

20 Bleeping Computer, “Ransomware profits drop 40% in 2022 as victims refuse to pay,” Toulas, B., January 2023, URL: https://www.bleepingcomputer.com/news/security/ransomware-profits-drop-40-percent-in-2022-as-victims-refuse-to-pay/

21 Federal Bureau of Investigation, “Internet Crime Report 2022,” URL: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

22 Federal Bureau of Investigation, “Internet Crime Report 2022,” URL: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

23 Statista, “Most commonly reported cyber crime categories worldwide in 2022, by number of individuals affected,” March 2023, URL: https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime-global/

24 Federal Bureau of Investigation, “Internet Crime Report 2022,” URL: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

25 Anti-Phishing Working Group, “Phishing Activity Trends Report: 3rd Quarter 2022,” December 12, 2022, URL: https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf

26 Tessian, “Must-Know Phishing Statistics: Updated 2022,” Maddie Rosenthal, January 12th, 2022, URL: https://www.tessian.com/blog/phishing-statistics-2020/

27 Verizon, “2022 Data Breach Investigations Report,” URL: https://www.verizon.com/business/en-gb/resources/reports/dbir/

28 Federal Bureau of Investigation, “Internet Crime Report 2022,” URL: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

29 https://knowledgebase.constantcontact.com/articles/KnowledgeBase/5409-average-industry-rates?lang=en_US

30 https://help.klaviyo.com/hc/en-us/articles/360051110111-Campaign-SMS-and-MMS-Benchmarks-

31 Anti-Phishing Working Group, “Phishing Activity Trends Report: 3rd Quarter 2022,” December 12, 2022, URL: https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf

32 Zimperium, “Financially Motivated Mobile Scamware Exceeds 100M Installations,” Aazim Yaswant, January 26, 2022, URL: https://www.zimperium.com/blog/dark-herring-android-scamware-exceeds-100m-installations/

33 Cleafy, “TeaBot is now spreading across the globe,” January 3, 2022, URL: https://www.cleafy.com/cleafy-labs/teabot-is-now-spreading-across-the-globe

34 Zimperium, “We Smell A RatMilad Android Spyware,” Nipun Gupta, October 5, 2022, URL: https://www.zimperium.com/blog/we-smell-a-ratmilad-mobile-spyware/

35 Zimperium, “MoneyMonger: Predatory Loan Scam Campaigns Move to Flutter,” Fernando Ortega, December 15, 2022, URL: https://www.zimperium.com/blog/moneymonger-predatory-loan-scam-campaigns-move-to-flutter/

36 Zimperium, “Schoolyard Bully Trojan Facebook Credential Stealer,” Nipun Gupta, December 1, 2022, URL: https://www.zimperium.com/blog/schoolyard-bully-trojan-facebook-credential-stealer/

37 Zimperium, “New Advanced Android Malware Posing as ‘System Update,’” March 26, 2021, URL: https://www.zimperium.com/blog/new-advanced-android-malware-posing-as-system-update/

38 https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/ https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

39 Zimperium, “Pegasus Spyware Resurfaces with Newly Revealed Zero-Click Vulnerability,” September 14, 2021, URL: https://www.zimperium.com/blog/pegasus-spyware-resurfaces-with-newly-discovered-zero-click-vulnerability/

40 Zimperium, “We Smell A RatMilad Android Spyware,” October 5, 2022, URL: https://www.zimperium.com/blog/we-smell-a-ratmilad-mobile-spyware/

41 https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

42 Microsoft, “Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits,” July 27, 2022, URL: https://www.microsoft.com/en-us/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/

43 https://www.economist.com/business/2022/05/30/corporate-espionage-is-entering-a-new-era

44 https://www.bloomberg.com/news/photo-essays/2011-09-20/famous-cases-of-corporate-espionage

45 https://www.bleepingcomputer.com/news/security/ransomware-profits-drop-40-percent-in-2022-as-victims-refuse-to-pay/

46 https://www.bleepingcomputer.com/news/security/ransomware-profits-drop-40-percent-in-2022-as-victims-refuse-to-pay/

47 https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

48 https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224

49 https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49

50 https://www.apple.com/newsroom/2023/05/app-store-stopped-more-than-2-billion-in-fraudulent-transactions-in-2022/

51 https://9to5mac.com/2022/03/16/scammers-have-been-using-apples-testflight-to-distribute-malicious-ios-apps/

52 https://about.fb.com/wp-content/uploads/2022/08/Quarterly-Adversarial-Threat-Report-Q2-2022.pdf

53 https://about.fb.com/wp-content/uploads/2022/08/Quarterly-Adversarial-Threat-Report-Q2-2022.pdf

54 https://bou.ke/blog/cve-2021-1831/

55 https://github.com/userlandkernel/plataoplomo/blob/master/writeups/shortcuts-traversal.md

56 https://zachary7829.github.io/blog/shortcuts/ExtractArchiveArbitraryWrite

57 https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware

58 Federal Trade Commission, “Consumer Sentinel Network Data Book 2021,” URL: https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2021

59 Lexis Nexis Risk Solutions, “The True Cost of Fraud™ Study,” URL: https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study

60 Statista, “Mobile app usage - Statistics & Facts,” L. Ceci, Nov 17, 2022, URL: https://www.statista.com/topics/1002/mobile-app-usage/#topicOverview

61 Statista, “Cloud storage of corporate data in organizations worldwide 2015-2022,” Lionel Sujay Vailshery, Mar 28, 2022, URL: https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/

Glossary of Terms

Cryptography
Cryptography refers to the process of encrypting and decrypting data to protect the communication in the presence of an adversarial actor. When data is encrypted, sophisticated mathematical algorithms are used to convert the data into undecipherable ciphertext. To decrypt data, or convert it from ciphertext back into its original form, a cryptographic key is needed.

Device Compromise
This term refers to a cybersecurity incident in which unauthorized access to a device undermines the endpoint's confidentiality, integrity, or availability. Once devices are compromised, malicious actors may be able to manipulate device controls or steal sensitive information.

Juice Jacking
This is a form of cyberattack in which malicious actors gain access to devices through public USB-based charging stations. Once devices are connected to compromised stations, they may be susceptible to malware attacks, spyware, and device compromise.

Known Malicious Network
These are networks that have been proven to be risky or the location of prior attacks. This can include an open Wi-Fi network that presents persistent security risks to devices.

Malicious Website
Malicious websites can be used to steal sensitive information, execute an exploit, or sideload malicious apps.

Malware
This term refers to a general category of malicious software. Through the installation of malware on a victim's device, attackers can weaken or disable device security mechanisms, gain access to device functionality, steal sensitive data, and more. Common examples of malware include trojans, spyware, and adware.

Man in the Middle Attack
This refers to an attack in which a malicious actor intercepts the communication between the device and a remote location in order to exfiltrate data (such as credentials), modify or redirect the traffic.

Obfuscation
Obfuscation is a technique used to make code more difficult to reverse engineer and analyze. This can be done with legitimate purposes (such as protecting IP) or to hide malicious behavior.

Phishing
Phishing is a commonly used social engineering attack. Threat actors use authentic-looking assets, such as e-mail, webpages, and text messages, to attempt to trick users into revealing sensitive data or clicking malicious links.

Smishing
A phishing attempt delivered through SMS. This type of attack is very popular to target mobile devices.

Ransomware

Ransomware is a type of malware that is designed to lock sensitive data or system access and then extort the victim to provide a ransom payment.

Rogue Access Point

This is a wireless access point that has been installed on a network's wired infrastructure without the consent of the network's owner. Once a device is connected to a rogue access point, it may be susceptible to a range of attacks, including man in the middle attacks.

Scan

Malicious actors employ scanning across a network in order to do reconnaissance. Through scans, attackers can find hosts, identify connected devices, and collect data. This information is then used in subsequent attack stages.

Spyware

Once installed on a victim's mobile device, spyware can be used to monitor a victim's keystrokes, messages, or conversations. Spyware is also used to steal credentials and other sensitive information. Spyware is typically installed on mobile devices without the user's knowledge.

Supply Chain Attacks

These forms of attack appear in various areas within the mobile app ecosystem. Attackers wage these attacks through compromised third-party libraries and software development kits (SDKs), apps posted in app stores, ad networks, over-the-air (OTA) updates, and development tools.

Threat Chains

Threat chains represent the sequence of steps that need to be taken in order for an attack to be successfully executed. For example, in the case of a phishing attack, a threat chain could include a user receiving an SMS-based phishing link, clicking on the link, being directed to a malicious website, and submitting their login credentials.

Traffic Manipulation

This is a general category of network-based attack. One example of this is a TLS downgrade attack in which malicious actors force a website to disable encryption, so they can access data transmissions of site visitors.

Trojan

Trojans represent one of the most common forms of malware. Through some form of disguise or deception, malicious actors fool potential victims into downloading what they think are legitimate apps. Attackers have used banking trojans to steal banking credentials, monitor keystrokes and other activities, steal money, and more.

Zero-Day

Zero-day is used to refer to vulnerabilities that have yet to be addressed by software developers and vendors. A zero-day attack refers to cases in which threat actors successfully exploit these vulnerabilities to pursue nefarious ends.

Credits

Contributing Zimperium Writers
Adam Wosotowsky
Asaf Peleg
Aazim Bill SE Yaswant
Chilik Tamir
Elad Golan
Georgia Weidman
Gianluca Braga
Grant Goodes
Jon Paterson
JT Keating
Krishna Vishnubholta
Monique Becenti
Nico Chiaraviglio
Nikias Bassen
Santiago Rodriguez
Sebastian Lopez
Shridhar Mittal
Vishnu Madhav

Contributing Partner Writers
Anis Hamdi, Senior Security Analyst, Riscure
Douglas McKee, Principal Engineer & Director of Vulnerability Research, Trellix
Jim Taylor, Chief Product Officer, RSA

Editors / Contributors
Christy Matthews
Jennifer VanAntwerp
John Pinson
Kasey Hewitt
Lisa Bergamo
Michael Zuckerman
Randy Budde
Sammie Walker
Tim Hartog
Lumina Communications

Layout and Design
Tom Green

About Zimperium

Zimperium provides the only mobile-first security platform purpose-built for enterprise environments. With machine learning-based protection and a single platform that secures everything from endpoints to apps, Zimperium provides on-device mobile threat defense and in-app protection to address today's growing and evolving mobile security threats. Zimperium is headquartered in Dallas, Texas and backed by Liberty Strategic Capital and SoftBank. For more information, follow Zimperium on Twitter (@Zimperium) and LinkedIn (https://www.linkedin.com/company/zimperium), or visit **www.zimperium.com**.

ZIMPERIUM®

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/.