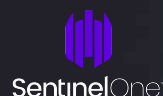




2022 Global Mobile Threat Report

With contributions by:

intertrust



Index

Executive Perspectives

1.1: Mobile Security At This Moment In Time	2
1.2: Mobile Security and the Broader Enterprise Security Strategy	4
1.3: The Continued Role for AI and Machine Learning in Mobile Security	6
1.4: Managing Mobile Risk in 2022	8

The Mobile Attack Surface

2.1: 2021 Mobile Threats in Review	10
2.2: State of Mobile Endpoint Security in 2022	15
2.3: State of Mobile Application Security 2022	20

Mobile Threat Trends

3.1: Global Threat Breakdown by Region	23
3.2: Breakdown of Exploited Vulnerabilities of 2021	29
3.3: The Rise of Mobile-Specific Phishing	33
3.4: Risks and Attacks: Mobile Malware, Bugs, and Profiles	41
3.5: More Apps Signify More Than Data Is at Risk	47

Insight from the Broader Security Ecosystem

4.1: Why MTD Matters for XDR	51
4.2: Establishing Mobile Device Trust in Zero Trust Security Architectures	53
4.3: The Large and Growing Smartphone Attack Surface	55
4.4: The Increased Risks of Mobile Productivity Tools to Enterprises	60

Summary

5.1: Conclusion	62
6.1: Sources	63
6.2: Glossary of Terms	64
6.3: Credits	66
6.4: About Zimperium / Legal	67

Mobile Security At This Moment in Time

Shridhar Mittal, CEO, Zimperium

I don't have to tell you that the last few years have changed the modern workforce in ways we could have only imagined a decade ago. Distributed and hybrid forces, ever-connected devices, high speed 5G connectivity, and increased critical data access from remote locations have spread enterprises worldwide. I also don't need to tell you that 2022 will look very different from 2021 and 2020. As we all know, in the current moment, we are light years beyond what work, collaboration, and productivity looked like before and leading up to the end of 2019.

For decades, IT and security teams built on-premise infrastructure to support the on-site employees, with a fringe few moving beyond the office walls. Security and services were implemented to build a digital fortress of layers to keep employees, endpoints, and data secure. But legacy off-site services like VPNs were not designed to handle this influx of external connections back to corporate. Once most employees moved beyond the physical and digital protections, and once locally-installed productivity tools moved to software as a service (SaaS) models, security organizations began investing in advanced security controls for the endpoints and infrastructure they supported.

Thankfully, the motivation and mindset to enable secure, remote collaboration had been set in motion for many enterprises even before COVID-19 came along, as global businesses pursued mobility, remote access, zero trust, and productivity initiatives. Enterprises began investing in cloud-based services and applications, moving data from on-site storage servers to scalable solutions around the globe. Because some foundation was then set, the global pandemic acted more as validation and as a catalyst than as a disruptor to their businesses. In that context, flexibility, scalability, and accessibility were primary and crucial requirements for these new investments. But what about security?

Despite their best efforts, the reality is that the workplace evolved much faster than many of these teams and strategies had planned for. **During the last two years specifically, many organizations sacrificed security controls in order to support productivity and ensure business continuity.**

It must also be said that IT and security organizations have always invested heavily in endpoint security but have historically underestimated the potential impacts of the blurred line between mobile and traditional endpoints.

66% of organizations surveyed recently have active BYOD programs in place, with 11% looking to implement the policy over the next year.¹

Now more than ever, both managed and unmanaged devices connect to corporate data through unknown and unmanaged networks. Necessarily, security teams need to approach every endpoint with a brand new mindset. It all begins with visibility into all devices connected to corporate systems, whether managed or unmanaged. Otherwise, security teams are left blind to the threats and risks introduced every day without data attribution and device attestation. Organizations need to move beyond mobile device and application management toolsets and address the more significant security challenges that mobile devices introduce.

10% of the applications installed on the average BYO mobile endpoint are enterprise-focused, from multi-factor authentication (MFA), data access tools, and communications.¹

As enterprises evolve, they also introduce more applications connected to critical data systems to better support their now-global workforce, which means these new risks move beyond the mobile device itself. **The enterprise attack surface grows with each new application adopted and deployed in the spirit of productivity.** After all, each of these applications introduces unique sets of risks to an environment, from misconfigured code and exposed APIs to leaky cloud connections uncovering customer data.

The world during the global pandemic was sustained significantly by mobile connectivity, enabling a huge swath of businesses to remain afloat. From global enterprises powered by knowledge workers accessing corporate data from their personal devices, to small restaurants relying upon menu QR codes, online orders, and contactless payments, mobile connectivity enabled the world to remain connected in a time of necessary isolation. And there is no “putting this rabbit back” into the proverbial hat. This level of mobile connectivity will remain the expectation for workers, customers, constituents, users, and enterprises for decades to come. It is now time to come to terms with how we must effectively secure those connections in order to continue to enable them.

How We Hope You'll Use This Year's Report

For all of these reasons, and specifically at this moment in time and history, we wanted to provide greater insight into the role that mobile threats to devices and applications are playing in the overall cybersecurity threat landscape.

Our 2022 Global Mobile Threat Report aims to collect, organize, arrange and provide insight that empowers global enterprises and organizations to take well-informed and decisive action to secure their data. We have mined our data to derive meaning from a variety of perspectives, including soliciting those outside of our organization, to enable you to see the mobile threat landscape from a multitude of angles.

- **First, we take a look at the mobile attack surface, examining a year's worth of mobile threat data in review, including deeper concentration on mobile device threat and mobile application threat trends, specifically.**
- **Next, we explore how mobile threats and a modern mobile security strategy drive impact throughout the entire security ecosystem, with contributions from our ecosystem of partners including SentinelOne, Ping Identity, and Intertrust.**
- **We then provide a roundup and topical analysis of mobile threat data from the field, including prominent mobile attack vectors, regional analyses, exploited mobile vulnerabilities, mobile phishing trends, and mobile malware trends.**

It is our most sincere hope that this information and these perspectives will directly inform your organization's strategy and investments in the coming year as we all do our part to support a more secure and increasingly connected world.



Mobile Security and the Broader Enterprise Security Strategy

Jon Paterson, CTO, Zimperium

Over the last few years, security toolsets surrounding XDR and SOAR have risen to drive the traditional security evolution against the advancing threats. Identity and access management tools have expanded to support remote access at scale, and **36% of enterprises we surveyed are prioritizing the investment of zero trust architectures over the next year.**³ These advanced layers of security enable enterprises to scale beyond the corporate walls effectively, integrate into effect identity management workflows, and establish a perimeter of one around the devices and applications connected through the myriad of networks.

But all of this security investment crumbles without mobile inclusion. From modern and mobile endpoint defense and device attestation, to securing enterprise applications through the complete development lifecycle, enterprises need their security to scale with their data, access, employees, and customers.

The inclusion of modern and mobile endpoint and application security into enterprise mindsets is not the final frontier but the beginning of what is to come.

The integration of devices into our every day is paving the way for the convergence of the modern endpoint. Apple has already started to integrate OSX and iOS services across their platforms, and Windows 11 is soon introducing the ability to run Android applications on the desktop natively. Google's ChromeOS project further blurs the line between desktop and mobile endpoints with shared applications, extensions, and services.

When we consider developing applications for the modern endpoint, building secure and compliant applications begins with choosing the right architecture and framework for devices and platforms that support your business needs. Security by design allows for good foundational decisions around code, data, and cryptographic key protection. Security measures will need to account for hardware and software fragmentation. **As data stewards, enterprises must assume that applications will, and do, operate in hostile environments, making run-time visibility and protection of data at rest, use and transit a priority.**



Enterprises that get ahead of establishing zero trust architectures and applying security mindsets to application development will be ready for this coming evolution of the modern endpoint. Threats and risks will be capable of jumping across devices just like legitimate data and services, and vulnerabilities to critical systems will be shared. As recently as September 2021, the first inclination of a multi-device, single vulnerability (CVE-2021-30860) was revealed as part of the Pegasus spyware attack, impacting iMessage on iOS and OSX devices.

And this is just the beginning. The line between the mobile and traditional endpoint will continue to blur, and with it, the security mindsets will need to be in place and ready to provide visibility, attest and secure access to enterprises from our modern endpoint devices.

Multi-experience platforms will continue to transform how applications are designed and built but will exponentially increase the need for comprehensive and integrated security platforms.

The enterprise attack surface will also continue to change and evolve, driven by the challenge and opportunity that the growing attack surfaces present. From state-sponsored techniques, application exploits, and commercially available threats, the business of cybercrime is growing year over year and shows no signs of slowing down. The impact on the business is not small either, with **the cost of a data breach in 2021 increasing from \$3.86 million to \$4.24 million.**⁴

For over a decade, we have been pushing the boundaries of mobile endpoint and application security, working with forward-thinking partners to stay ahead of the risks and threats to the modern workforce. None of us could have predicted the impact the last three years had on global business, but Zimperium was prepared to scale with the mobile needs of enterprises globally.

Whether you are looking to understand the risks mobile endpoints introduce to your corporate environment, or you are exploring threats to your internally developed mobile apps, I hope the 2022 Global Mobile Threat Report provides you with data and research to direct you towards mobile security confidence.



1.3

The Continued Role for AI and Machine Learning in Mobile Security

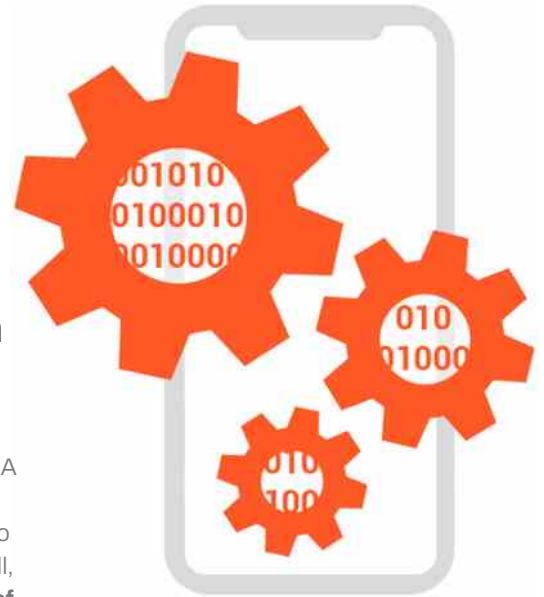
Esteban Pellegrino, Chief Scientist, Zimperium

Late in 2019, an incredible story began to circulate on various scientific-focused news sites talking about the power of the iPhone compared to the computers that took NASA to the moon. It was an exciting exploration into the history of the computing power of one of humankind's most incredible achievements 50 years prior and how it lined up to the little device we slide into our pocket every day. Without getting into the math of it all, **it's safe to say the 2019 Apple iPhone 11 would have been more than capable of processing the data and powering all six moon landings combined. And with processing power to spare.**

The capabilities of these mobile devices are often taken for granted by users, looking at the tiny screen that is always connected to a network, browsing, exploring, navigating, and computing. Sometimes they are even used to make a call. But the iPhone and Android devices that dominate the mobile market today are more computer than phone, connected into critical data systems, packed full of private information, and relied upon for daily work and personal life.

15 years ago, the first iPhone launched, and we saw the smartphone begin to make its way into enterprises through managed and rudimentary unmanaged programs. These handheld computers evolved from consumer accessories to business tools, keeping employees connected with work as they roamed. Access was basic at first, but as the years have gone by, the mobile device has grown from accessory to critical access device for services, data, and identity, with equal importance of access to the supplied laptop. But unlike the laptop, mobile endpoints and the apps they were running traditionally lacked the advanced security to keep up with the context of the current threat landscape.

10 years ago, the team that founded Zimperium recognized this lack of advanced mobile security tools to keep data and access safe. **We knew we needed to understand the threats beyond human capabilities, to detect patterns impossible to see even for experts, and most importantly, to continuously learn from the evolving mobile experience.**



In 2012, we invented and patented[®] Zimperium z9, the dynamically updatable machine learning framework that transformed Zimperium into the first mobile threat defense (MTD) vendor fully powered by on-device artificial intelligence.

For the past ten years, we've been delivering the most advanced security to endpoints and applications globally, keeping ahead of the growing threats to the mobile market. **Our mission is now to unify the security of applications and endpoints through one single technology, minimizing the attack surface of mobile devices and the applications installed within.** We aim to provide the most advanced, enterprise-ready, on-device zero-day protection to mobile endpoints and applications during development and run-time.



Today, our advanced AI provides on-device protection from malware, network reconnaissance and interception attacks, phishing, hooking, tampering, debugging, and exploiting mobile devices and applications. Endpoints and apps alike are leveraging our AI technology to be ready when novel threats emerge in the wild, and our experience will continue to provide the security needed to stay ahead of the threat.

Mobile and traditional devices are converging, and the mobile versions are increasingly replacing their traditional counterparts, capable of accessing and processing high amounts of data far from the confines of an office. With each new application's advancement in technology, there are unknown risks and threats to overcome. It is time to address them head-on, increase mobile security confidence, and be ready for whatever comes next.

One day, our mobile devices will go to the moon and far beyond, communication devices untethered from the walls but connecting future explorers more than ever. Just as the Apollo scientists could not have predicted the computer power of today's devices, we don't know what the next evolution in technology will be, but we can be confident that mobile is here to stay.



Managing Mobile Risk in 2022

Malcolm Harkins, Chief Security & Trust Officer, Epiphany Systems

“Risk surrounds and envelops us. Without understanding it, we risk everything, and without capitalizing on it, we gain nothing”

This quote from Glynn Breakwell in her book *The Psychology of Risk* says it all. I have seen, experienced, and helped promote mobile computing for decades, dating well back into my days at Intel where I was Chief Security & Privacy Officer.

When the first truly mobile laptop with ubiquitous wireless connectivity (Centrino platform) was launched in March 2003, my team and I enabled it. When the iPhone launched in 2007, we enabled it – instantly creating 50,000 BYOD devices overnight. When various enterprise apps became mobile, we enabled them. In the years since those early days of mobility, there has continued to be an explosion of devices and apps, creating new opportunities for economic growth as well as social benefits that have positively impacted businesses as well as consumers.



But have we truly understood the risks we have taken and the potential impact? In some organizations, the answer is clearly yes, but unfortunately, in far too many organizations, the answer is no.

For example, one trend mentioned in the report identifies that many have allowed iPhones and mobile devices in their ecosystem. Was that a calculated risk worth taking when security wasn't established for those channels of data access? Or, did the pursuit of the potential benefits cause a bias that not only suppressed the real risk to the organization but also created a substantial risk to individuals whose personal and financial data is now at risk?

Zimperium has created the most comprehensive mobile threat report published to date. It contains a broad view of the threat and vulnerability trends as well as the implications they could have on the security of our organizations. The World Economic Forum's global risk report for 2022 states, "growing cyber threats are outpacing society's ability to effectively prevent and manage them." The attack surface will always grow and change as computing evolves but understanding the attack depth within the context of your enterprise infrastructure is the key to understanding how mobile apps and devices could generate a material exposure that could impact your business.

In this report, in-depth details are shared from the Zimperium zLabs advanced threat research team that provide the comprehensive insight security teams need to understand the mobile risk landscape. One such trend that will reshape the risk landscape detailed in the report is the convergence of systems, blurring of mobile apps/desktop apps into the modern OS. This trend in particular will "surround and envelop us," and without proper mitigations implemented, we will "risk everything."

Here's another of my favorite quotes, this time from Art Turock:

“There's a difference between interest and commitment. When you're interested in doing something, you do it when circumstances permit. When you're committed to something, you accept no excuses, only results.”

It's clear, given the trends, that we have collectively underestimated the mobile risks we have and the exposure that has been created. I learned many years ago that there are two types of mistakes. Ones you have to live with and ones you can fix. When I have been in the latter position, I have considered myself lucky and fixed it. All our security investments crumble without the inclusion of mobile endpoints and apps. We can fix the mobility security mistakes of the past and better position ourselves to avoid risk mistakes in the future.

The choice is yours, and the time is now. If you don't make a choice to commit to addressing these risks head-on, it should be clear from this report that, inevitably, the choice will be made for you.



2.1

2021 Mobile Threats in Review

42%

Reported mobile devices & web applications led to security incident

Mobile devices aren't just a personal communication accessory—today, they're an integral part of how we get work done in an enterprise. With increased capabilities and connectivity, smartphones and tablets can now access the same data and services as traditional devices and a wealth of new cloud-based business services. In order to support both the productivity of remote workers and the security of corporate assets, mobile endpoints must be proactively and intelligently protected.

42%

Reported unauthorized apps & resources accessing enterprise data

While traditional endpoints continue to be leveraged, security teams are challenged to gain the visibility they need into mobile device usage and activity. This lack of visibility makes it difficult and time-consuming for teams to detect threats and prioritize remediation efforts. Further, with each new endpoint that starts accessing enterprise systems, the organization's attack surface expands, thus increasing the risk of nefarious activity.

10%

Reported unsecured applications due to lack of authentication or encryption

In a recent survey, technology leaders were asked to highlight the five threats that had the most significant impact on their systems in the previous twelve months. **42% of respondents reported that mobile devices and web applications have led to a security incident.** It is not just mobile endpoints introducing risk into corporate systems: another 42% of respondents reported unauthorized apps and resources accessing enterprise data, and 10% reported unsecured applications due to the lack of authentication or encryption.⁷

56%

Rely on at least four to eight enterprise applications on their mobile device

It is now more critical (and more challenging than ever) to strike a balance between enabling mobile access and minimizing the enterprise's exposure to attack. Whether a business relies on managed, corporate-owned endpoints or has an active bring-your-own-device (BYOD) program, mobile endpoints and applications introduce increased risks. 56% of technology leaders surveyed rely on at least four to eight enterprise applications for productivity. **17% of the surveyed technology leaders depend on more than eight work-specific apps on their mobile device.**⁸ Although these applications vary between vendor-provided services and internally developed toolsets, both categories rely on access to corporate data systems for effectiveness.

17%

Depend on more than eight work-specific apps on their mobile device

Attacks on mobile devices and applications had a negative impact on systems, privacy, customer data, and more. With these devices processing and accessing critical information like passwords, multi-factor authentication apps, and corporate files and communications, it's no surprise that the threats have increased over the last few years—and that malicious actors continue to invest more in targeting these devices and applications with increasing levels of sophistication.

Before the COVID-19 pandemic arose, 60% of organizations had no BYOD policies in place. Over the last two years, many teams have responded heroically and rapidly to support remote workers. But the resulting increase in the introduction of BYOD policies continues to blur the lines between devices and data, and between consumer threats and enterprise threats. In addition, it's important to recognize that just like consumers, employees are concerned about their privacy. In fact, trust and privacy concerns among employees continue to slow the adoption of device management policies in enterprises.

As we analyzed the mobile threat landscape, 2021 was the year of big revelations and reboots of previously discovered malware. Pegasus, the spyware program sold to governments around the world, reappeared in the news after revelations of a campaign targeting 50,000 journalists, human rights activists, political leaders, and more. Initially unveiled by Amnesty International, the spyware campaign featured zero-day exploits targeting iOS devices. Shockwaves of this discovery have continued for months as additional information about the attacks and victims is revealed.

Initially discovered in 2017, the Joker Trojan reappeared in 2021, targeting Android devices with updated capabilities. These trojans are malicious Android applications that have been notorious for performing bill fraud and subscribing users to premium services. As with previous forms of these attacks, the newly discovered trojans had the same objective: financial gain. Successful infections of mobile devices often slide under a victim's radar until long after the money is gone, leaving them with little to no recourse for recovery.



Over 1,000 samples of the Joker malware were discovered in mid-2021, and these more recent variants had new security-bypassing techniques built into their code.

From device exploits to application misconfigurations, malware, and leaky databases, the mobile device has become a ripe target for malicious actors globally. Zimperium's 2021 data proves there was no shortage of threats targeting mobile ecosystems. However, with the lessons learned from last year, 2022 should be the year people start approaching mobile devices and apps with the same advanced security mindset as traditional endpoints.

2022 Zimperium zLabs Research Highlights



The Zimperium zLabs Advanced Research Group continuously investigates mobile device and application threats targeting users worldwide. Compared to prior years, data and news coverage of mobile threats increased in 2021, and there was a greater focus on iOS and Android attack vectors. **In 2021, the Zimperium zLabs team discovered numerous threats impacting over 10 million devices in at least 214 countries.**

Here is a summary of the most notable discoveries from the Zimperium zLabs Advanced Threat Research team:



Forensic evidence of this active Android Trojan attack, which we named [GriftHorse](#), suggests the threat group has been running this campaign since November 2020. These malicious applications were initially distributed through both Google Play and third-party application stores. The campaign targeted mobile users from more than 70 countries. GriftHorse is exceptionally versatile. The campaign could change the language and content displayed based on the user's IP address. Between November 2020 and September 2021 (when it was publicly disclosed), GriftHorse infected over 10 million devices. Google removed the malicious applications upon reporting by the Zimperium zLabs team.



The Zimperium zLabs team identified 23 applications targeting South Korean citizens to date. This spyware campaign infected thousands of victims' devices. These malicious Android apps are designed to spy on their victims constantly. They run silently in the background without raising any suspicion. We believe the malicious actors responsible for [PhoneSpy](#) have gathered significant amounts of personal and corporate information on their victims, including private communications and photos. After public disclosure, the specific campaign was deactivated, and the command-and-control server was taken down. Infected devices are no longer under the control of the attackers.



Forensic evidence of this active Android Trojan attack, which we dubbed [FlyTrap](#), points to malicious parties operating in Vietnam. This hijacking campaign has been running since March 2021. These malicious applications were initially distributed through both Google Play and third-party application stores. The threat actors take advantage of the fact that users commonly have the misconception that logging into the right domain is always secure, irrespective of the application used. The targeted domains are popular social media platforms, and this campaign has been exceptionally effective in harvesting social media session data of users from 144 countries. These compromised accounts can be used as a botnet for different purposes. For example, actors can boost the popularity of specific pages, sites, and products. In addition, these accounts can be utilized to spread misinformation or political propaganda. Once reported by the Zimperium zLabs team, Google removed the malicious applications.



The “System Update” app was identified by the Zimperium zLabs team using the z9 malware engine, which powers zIPS on-device detection. After an investigation, researchers determined it to be a sophisticated spyware campaign with complex capabilities. The mobile application poses a threat to Android devices by functioning as a remote access trojan (RAT). The application receives and executes commands to collect and exfiltrate a wide range of data and perform a diverse set of malicious actions. Once in control, hackers can record audio and phone calls, take photos, review browser history, access WhatsApp messages, and more.



Through the Zimperium zLabs team’s analysis, researchers found that 14% of iOS and Android apps distributed globally revealed several significant configuration issues. These apps used cloud storage with unsecured configurations. These misconfiguration issues exposed personally identifiable information (PII), enabled fraud, and exposed IP addresses or internal systems and configurations. Misconfigured applications were found in almost every category.

The image below shows the distribution of apps with unsecured storage issues across various categories.

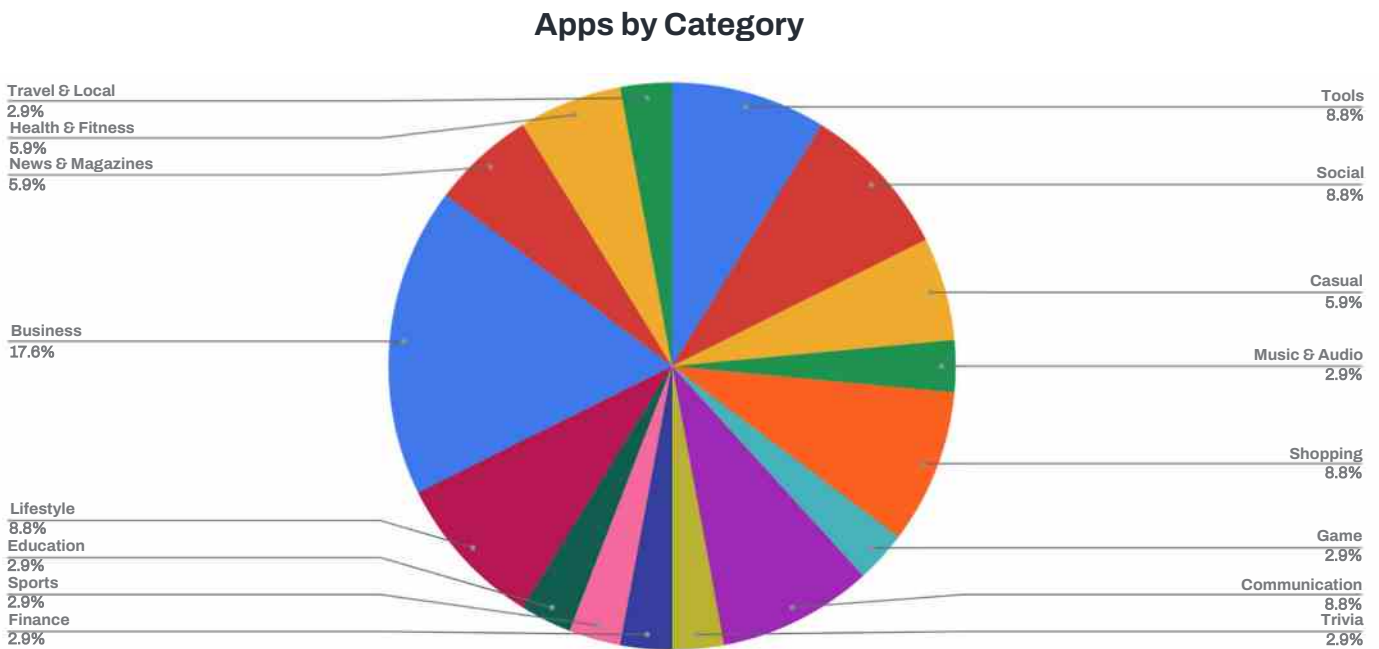


Figure 1: Apps with unsecured cloud storage, by category.

The 10 Attacks that Made Mobile Threats Into Headlines in 2021

With the rise in sophisticated attacks, zero-day vulnerabilities, and notable exploits, it is no surprise that the media coverage on these topics has been substantial. According to the Cision media monitoring platform, iOS and Android security news was widely covered across global media organizations.

Here are the top 10 most frequently covered threats and links to sample articles.



1 Apple iOS: iOS 14.4.2 - Vulnerability in Apple's WebKit Browser Engine

Coverage: Forbes, CNET, 9to5Mac, MacObserver, MacWorld, MacRumors, Appleosophy, TechGig, Laptop Mag



2 Android: GriftHorse (Zimperium Disclosed)

Coverage: WIRED, PC Magazine, Forbes, ZDNet, CPO Magazine, Security Week, Threatpost, Security Affairs, The Record, SensorsTechForum, HackRead, Android Headlines, Android Authority, TechTimes, ITechPost



3 Apple iOS: iOS 14.8 - Spyware Flaw (Pegasus)

Coverage: Forbes, CNET, The Verge, ComputerWorld, TechRepublic, TechRadar, TechNadu, Macworld, Uberglzmo, Apple Insider, TechStory, MacRumors, PhoneScoop



4 Android: FlyTrap (Zimperium Disclosed)

Coverage: Business Insider India, InfoSecurity Magazine, TechRepublic, PC Magazine, ZDNet, Threatpost, Bleeping Computer, Security Affairs, TechRadar, TechNadu, TechTimes, ITechPost



5 Android: Qualcomm + Mail GPU Vulnerabilities

May 2021 - CVE-2021-1905 (NIST-CVSS score: 7.8)
May 2021 - CVE-2021-1908 (NIST-CVSS score: 5.6)
May 2021 - CVE-2021-28883 (NIST-CVSS score: 8.8)
May 2021 - CVE-2021-28884 (NIST-CVSS score: 8.8)

Coverage: ArsTechnica, Security Week, Threatpost, Security Affairs, Bleeping Computer, The Record, IT Pro UK, TechNadu, Tom's Guide



6 Android: PhoneSpy (Zimperium Disclosed)

Coverage: TechCrunch, ZDNet, The Hacker News, Security Week, Threatpost, Bleeping Computer, Security Affairs, TechRadar, HackRead, Android Community, Android Headlines



7 Android: SharkBot

Coverage: SC Magazine, ZDNet, BankInfoSecurity, The Hacker News, Security Week, Security Affairs, The Record, TechTimes, The Digital Hacker



8 Apple iOS: 14.7 - WifiDemon Flaw

Coverage: The Hacker News, BleepingComputer, Threatpost, Security Week, The Record, Help Net Security, We Live Security, Security Affairs, HackRead, Tom's Guide, iPhone Hacks



9 Android: Qualcomm Vulnerability

CVE-2020-11261 (NIST-CVSS score: 7.8)

Coverage: Security Week, The Hacker News, Threatpost, Security Affairs, The Record, IT Pro UK, SensorsTechForum

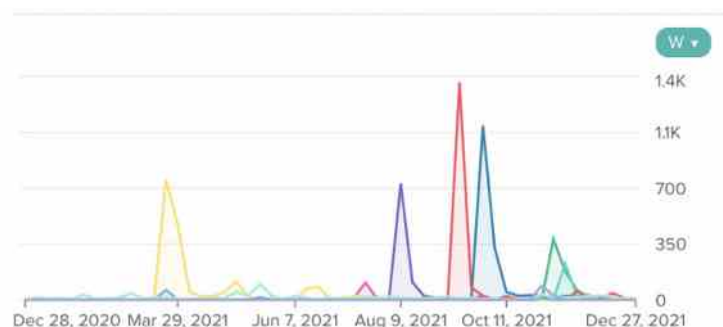


10 Android: Kernel Vulnerability

November 2021: CVE-2021-1048 (NIST-CVSS score: 7.8)

Coverage: Security Week, Threatpost, Security Affairs, Bleeping Computer, We Live Security, 9to5 Google, SensorsTechForum

Total Mentions Over Time



SEARCH NAME / MENTIONS	SEARCH NAME / MENTIONS	SEARCH NAME / MENTIONS
IOS 14.4.2	1.8K	PhoneSpy
GriftHorse	1.7K	SharkBot
IOS 14.8	1.7K	WifiDemon
FlyTrap	999	CVE-2021-1048
CVEs May 2021	902	CVE-2020-11261
		688
		299
		131
		126
		119

Credit: Cision

State of Mobile Endpoint Security in 2022

Mobile Device Market

Our smartphones continue to enable us to innovate, be entertained, and enjoy an improved quality of life. Consequently, mobile device purchases continue to grow. In 2020, nearly 1.38 billion smartphones were sold worldwide.¹⁰ In the United States, there are more than 290 million smartphone users. The penetration rate has risen consistently year over year, reaching 85% in 2021.¹¹



NUMBER OF SMARTPHONE USERS IN THE UNITED STATES IN 2021

294.15M

U.S. SMARTPHONE SHIPMENTS IN 2021

147.48M

U.S. SMARTPHONE SALES VALUE IN 2021

\$73B USD

The US smartphone market is projected to reach \$73 billion, which is a significant increase from 2010 when revenues were \$18 billion.¹² In the US market, Apple and Samsung are the leading smartphone manufacturers. Together, they account for 82% of sales.¹³ As the mobile device market continues to grow, so will mobile threats.

For security teams, the harsh reality is that it only takes one—one shared password, one deceived employee, one compromised device—to expose the business to a devastating breach. Amid the pandemic and the corresponding explosive growth in remote and hybrid work, the threats associated with mobile devices have expanded rapidly. While battling consistent, constantly evolving attacks, security teams need to safeguard more endpoints and ever-expanding attack vectors.

BYOD Stats

Despite the escalating threats, enterprises continue to enable BYOD policies. Too often in the rush to support remote work requirements teams fail to implement the robust security mechanisms needed to protect such devices.

In one survey we found that 74% of respondents indicated they have a BYOD policy in place. Yet in another survey, 30% of the respondents considered BYOD a top endpoint security worry within their organization.¹⁴



Endpoint Security Worries

35%

REMOTE OFFICE /
USERS

30%

BYOD

11%

MOBILE PHONES /
DEVICES

Time to Patch

In a distributed workforce, employees use their own network and, in some cases, their personal devices to conduct business. These practices introduce significant risk into an enterprise, broadening the attack surface and limiting the security team's ability to detect or remediate malicious activity. As teams seek to mitigate risk and prevent unauthorized access to sensitive corporate data, enforcing BYOD and guest access policies represent top challenges, as cited by 42% of respondents.¹⁵

After the release of an emergency or high-priority patch, it takes teams this long to implement a hotfix:¹⁶



42% say less than two days

28% say three to seven days

20% say one to two weeks

In 2021, nearly **50%** of respondents said their work-from-home strategy was a significant factor in cybersecurity incidents.

Mobile Endpoints: A Critical Part of The Cybersecurity Landscape

If organizations are not securing mobile endpoints, their security operations center (SOC) won't be able to establish "single-pane-of-glass" visibility into their cybersecurity posture. When employees use a personal mobile device to send an email, respond to text messages, or access secure company applications, the SOC can't monitor that activity or detect potential risks. In the wake of the growth in BYOD and work-from-home scenarios, leaders must start changing how they look at mobile device security.

Nearly half of survey respondents (44%) have added security policies or requirements due to cyber security incidents occurring within the distributed workforce. Of that population, 40% have changed authentication procedures for employees, while 34% have switched security vendors or service providers.¹⁷

Microsoft Office is a prime target among bad actors. According to one report, **Microsoft Office accounted for more than 72% of exploits, with browsers representing 13%.¹⁸**

These numbers may seem troubling, but nearly half of technology leaders think the current procedures are sufficient for reacting to zero-day incidents.¹⁹ However, the truth is, without comprehensive mobile threat defense in place, mobile endpoints will continue to be a black hole when it comes to incident response. 39% of these leaders understand that reaction time is too slow using their current procedures.²⁰

48%

of organizations review their cybersecurity strategy regularly and adjust as needed

26%

of organizations develop their cybersecurity strategy in real-time or as needed

23%

of organizations have a formal cybersecurity policy but barely review it, or no strategy at all

Figure 2: The breakdown enterprise cybersecurity strategy ²¹



Mobile Devices within the Corporate Ecosystem

IT and security teams will continue to be under increasing pressure as the threat of cyber attacks grows, as CISOs implement more stringent cybersecurity policies, and as employees express rising concerns about privacy. **Over half (61%) agree that trying to set and enforce corporate policies around cybersecurity is nearly impossible as lines blur between personal and professional lives.**²² While 46% say mobile devices in the corporate ecosystem are acceptable, 34% are concerned about privacy.²³



Figure 3: The breakdown of mobile devices in enterprises

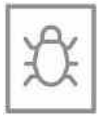
Mobile Threat Landscape in Enterprises

In 2021, Zimperium analyzed a range of mobile threats, including malware, unauthorized access, and vulnerabilities by device. Successful mobile attacks affect the bottom line, costing enterprise organizations millions of dollars. Penalties include loss of consumer trust, legal fees, fines, reputational damage, theft of sensitive data, and more.

Insider threats can cost the most to detect and remediate. While, corporate-owned and BYO devices are used to access corporate data, without tools such as mobile threat defense, mobile devices have limited visibility to IT departments and can take longer to detect malicious activity, if at all. According to survey data, the finance department is the group that poses the biggest internal threat to enterprises due to the sensitive financial and corporate data these teams process daily.²⁴ These statistics underscore why CEOs and CISOs must focus on this issue and increase investment in endpoint security.

In 2021, VC funding of cybersecurity surged to a record \$11.5 billion. Survey respondents estimate that 43% of their funding will be spent on securing the cloud, 14% on security consulting, and 14% on risk and compliance. During the COVID-19 pandemic, organizations realized the greatest return on their investment from endpoint security spending, with investments in business continuity and disaster recovery planning following right behind.²⁷ Meanwhile, 45% of technology leaders are reporting that mobile devices represent the weakest security.²⁸

Threats Affecting the Enterprise in the Past 12 Months²⁹



54%

Malware (Virus, Phishing, Ransomware)



46%

Identity or Account Theft



42%

Mobile or Web Application Security Exposure



42%

Unauthorized App or Resources Access

Mobile Security Market

Investments in endpoint detection and response are proliferating due to increased cyber threats affecting mobile devices. A large part of this growth is driven by mobile payments and the increasing need to secure BYOD programs in the enterprise.

Relative to major global security market regions, North America holds the highest share of investment at 41.1%.³⁰ However, this could quickly change as several Asian countries, including China, Singapore, and Japan, have invested heavily in developing national cybersecurity defenses, especially in mobile security.

Mobile threat defense (MTD) is a distinct category of mobile security technology that is rapidly growing its market share as it elevates detection and response on mobile devices. Security experts have argued that MTD, at a minimum, is required to be effective against modern-day mobile threats, as the solution can protect against attacks at the device, network, and application level.

Additionally, MTD protects end users against phishing attacks that target such vectors as SMS text messages, messaging apps, personal email, and corporate email, whereas MDM lacks these capabilities.

MTD goes far beyond managing settings and passcode capabilities and protecting the network through a built-in virtual private network (VPN). Detection capabilities alert administrators of rogue Wi-Fi access points, analyze the mobile ecosystem's risk, and track out-of-date operating systems (OSs), enabling teams to mitigate malicious activity. The threat intelligence from devices enables MTD to offer the visibility needed to improve detection and identify the lateral movement of attackers. In this way, MTD can be part of a more extensive, unified endpoint security (UES) infrastructure. MTD will continue to take the lead in mobile security and be a critical part of a UES or extended detection and response (XDR) system, improving an organization's overall security posture.



2.3 State of Mobile Application Security 2022

Over a relatively short period of time, our usage of mobile devices and apps has changed and grown dramatically. Enabled by evolving mobile and cloud technologies, innovative mobile apps continue to fuel digital transformation for businesses and remove friction from our everyday lives.

Today, the scope of the mobile app market is massive. **There were over 218 billion app downloads in 2020 alone.**³¹ By 2023, annual revenue from mobile apps is predicted to reach \$935 billion, with categories such as video streaming, gaming, and online fitness all generating billions of dollars in revenues.³² The payments segment alone accounted for \$1.3 trillion globally in 2020.³³

Application Development Trends

Driven by the profitability of apps, innovation in mobile app development has also accelerated. Here are some of the key application development trends changing the mobile app landscape:

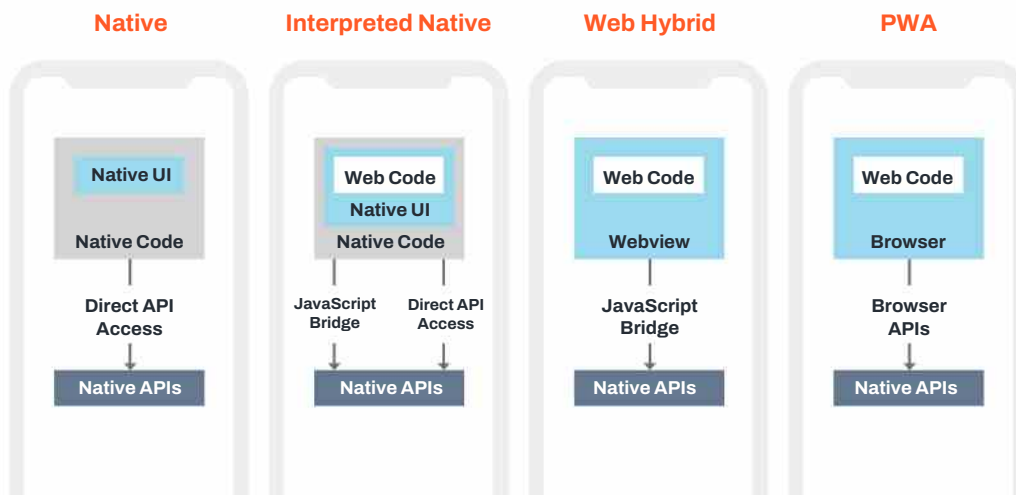
Cross-platform App Development

Through hybrid app approaches, developers can work with a single code base that can run on both Android and iOS platforms, which offers a number of appealing benefits. Developers can choose from several modern mobile application architectures. These alternatives support all types of devices (including phones and tablets) and all platforms (including Android and iOS). These hybrid approaches provide significant benefits when it comes to portability, maintenance, and distribution. Not surprisingly, the popularity of hybrid frameworks, such as React, Flutter, Uno, Kotlin, and Xamarin, has grown significantly.

Native Hybrid and Web Hybrid Apps both contain a combination of native and web code but in varying degrees. Web Hybrid applications are mostly stand-alone web applications that you can run in a standard web browser. In both these cases, the web code is more challenging to secure due to the lack of security features in the web control and the lower availability of SDKs and tools for web code.

Progressive Web Applications are an evolution of traditional web applications but have the look and feel of native mobile applications. A single code base supports multiple platforms for portability but makes it exceptionally challenging to secure data and code.

Mobile App Architecture Profiles



Low-Code and No-Code Platforms

While the move to no-code and low-code development platforms has been underway for some time, the significant talent shortage that hit organizations in recent years has served to dramatically accelerate this transition. Given this staffing shortage, development will increasingly morph from writing code into an effort of assembling and integrating open-source and third-party components.

Frictionless, Immersive Mobile User Experience

Increasingly, advancements in password-less authentication and voice integration will continue to make our mobile app interactions more seamless and immersive. The biometric authentication market is expected to exceed \$8.79 billion by 2026.³³ Facial recognition and other biometrics have become increasingly common in consumer apps, and the constant evolution of Fast ID Online (FIDO) protocols will continue to fuel growth in enterprise mobile application markets. Increased integration of voice recognition in mobile apps is inevitable, as there are few things simpler for the consumer than asking for something. This will eventually remove the need for users to unlock their phones hundreds of times a day.

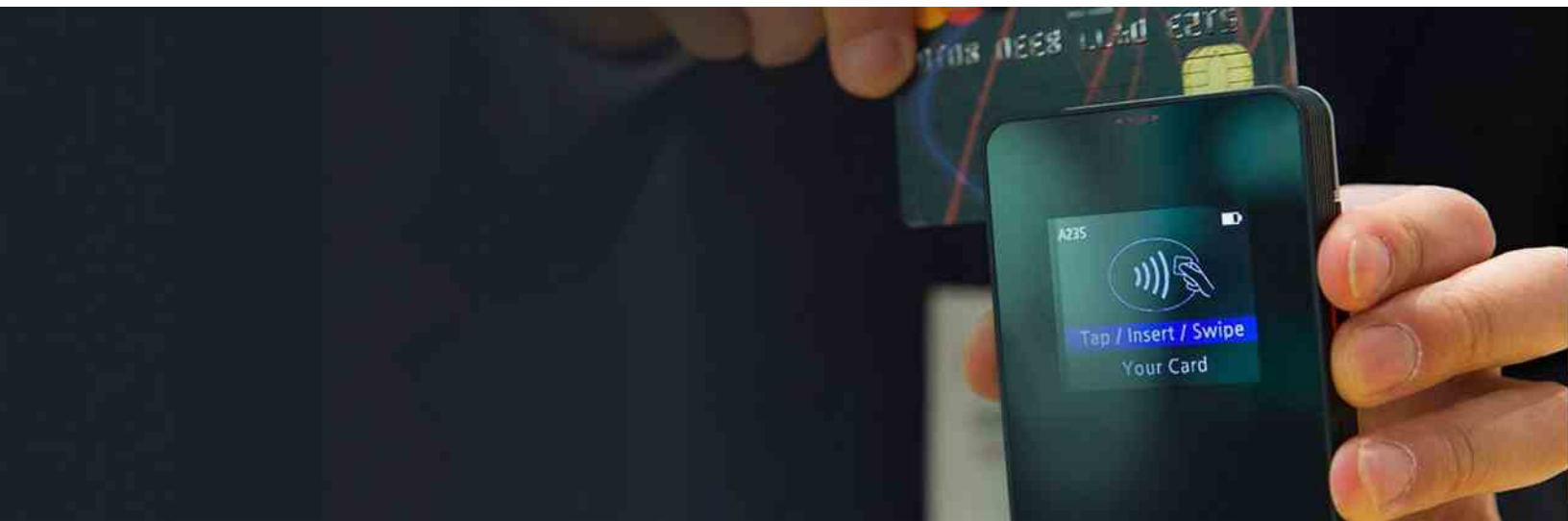
Voice technology is becoming increasingly accessible to developers, and security will need to be front and center as advances continue in AI, natural language processing (NLP), and machine learning. But mobile applications with Voice User Interfaces raise several concerns around privacy (is the app always listening?) and security (how are you securely storing what I said?). GDPR and other privacy laws globally will need to evolve with this trend to protect speech data just like other PII.



Key Technology Trends With Mobile App Security Implications

5G: With mobile device usage and cloud adoption proliferating, the volume of sensitive data being shared continues to see explosive growth. Now, 5G communications networks are able to deliver higher data transfer speeds with lower latency. **By the end of 2024, it is predicted that there will be 1.5 billion 5G mobile subscriptions, and 5G will handle 25% of all mobile data traffic.**³⁵ This of course means there will be even more sensitive data being shared, transmitted, and accessed—which, in turn, translates into even more data for cybercriminals to target.

Mobile Payments: Over the past several years, Android and iOS phones have begun to be used as point-of-sale (PoS) terminals, which has helped usher in a boom in contactless payment adoption and usage. Mobile payments revenue reached \$1.3 trillion in 2020 and was expected to hit \$1.7 trillion in 2021.³⁶ Technologies like NFC, Bluetooth, and QR codes, will increasingly enable smartphones to displace payment terminals and physical wallets.





QR Codes: The resurgence of QR codes during the pandemic has lulled us into believing that their use is not only convenient, but through their pervasiveness, that they are also benign. More than ever, QR codes are transforming products and packaging into smart products. According to a survey by Statista, **in the US alone, an estimated 11 Million households were forecast to have scanned a QR Code in 2020.** In addition, there is significantly more adoption in Asia, especially in China and India.

But various threat actors are using QR codes as an attack vector against enterprises and individuals. In the USA, the Federal Bureau of Investigations (FBI) released a Public Service Announcement warning mobile phone users against the rising scam and attack vector taking advantage of the increase in QR code adoption.³⁷ Threat actors are tampering with or deploying their own QR codes in an attempt to steal a victim's financial information or critical data, as well compromise the device through malicious applications.

Mobile Cloud Computing: The mobile cloud refers to cloud-based data, applications, and services designed specifically to be used on mobile and other portable devices. In 2020, the mobile cloud market reached a value of \$30.71 billion, and it is expected to reach \$118.70 billion by the end of 2026.³⁸ Communication between mobile devices and cloud services is maintained via a wireless network in these applications. Since we cannot trust the security posture of the mobile device at any moment, securing data, keys, and cloud connections within the application is critical.

A few patterns stand out when we look at the causes of critical breaches related to mobile applications:



App vulnerabilities. Repeatedly, the code of mobile app developers exposes employee and customer data, putting privacy and security at risk. Recent examples of compromised apps include the mobile app used by Ring doorbell customers,³⁹ the Android version of the business communication app Slack,⁴⁰ and the Klarna payment app.⁴¹



Third-party components and developers. Mobile app developers continue to grow increasingly reliant on third-party components and service providers—and this has ushered in a significant level of risk. **In 2021, the private data of 21 million customers of ParkMobile, a mobile parking app, was exposed by third-party software the company used.** Third-party libraries will continue to dominate mobile apps as they represent ease of development, speed to market, and potential cost savings. But they are a double-edged sword. They expand the attack surface and create over-privileged applications, both characteristics that cybercriminals look for in exploitable applications.



Misconfigured cloud services. One investigation into 23 mobile apps found that data of more than 100 million users was exposed.⁴² The culprit? Developers failed to properly configure their third-party cloud services. **Based on our analysis of more than 1.3 million Android and iOS apps, we found that 131,000 used public cloud services in their backend, and 14% of those apps had misconfigurations exposing users' personal information.**⁴³

“Cyberspace is not a specific environment. In 2022, cyberspace has become a free fire zone with a multiplicity of actors. As the physical world and cyberspace have converged via smart phones; mobile malware, proximity attacks and application attacks are allowing for cybercriminals and spies to manifest in both your digital and physical life. From stealing your money; to turning on the microphone and camera specific to your location, to using your device to compromise your work network, cybercrime cartels have gone wireless. Security and safety are dependent on mobile security.”

Tom Kellermann

Head of Cybersecurity Strategy for VMware and Global Fellow for Cyber Policy at the Wilson Center

Global Threat Breakdown by Region



From a global perspective, there is no denying that mobile endpoints are exposed to increased threats, putting enterprise data and services at risk. Several observations emerge from the enterprise clients and the risk data reported back from the Android and iOS devices secured by Zimperium globally. To note, the data provided in these charts is inclusive of all threats and risks detected and prevented on Zimperium secured enterprise clients. This anonymized enterprise data also includes detected threats reported on installation as part of the visibility stage of deployment.

Unless stated otherwise, the following data and analysis is derived from the anonymized and aggregated data provided with permission to Zimperium from its enterprise clients.

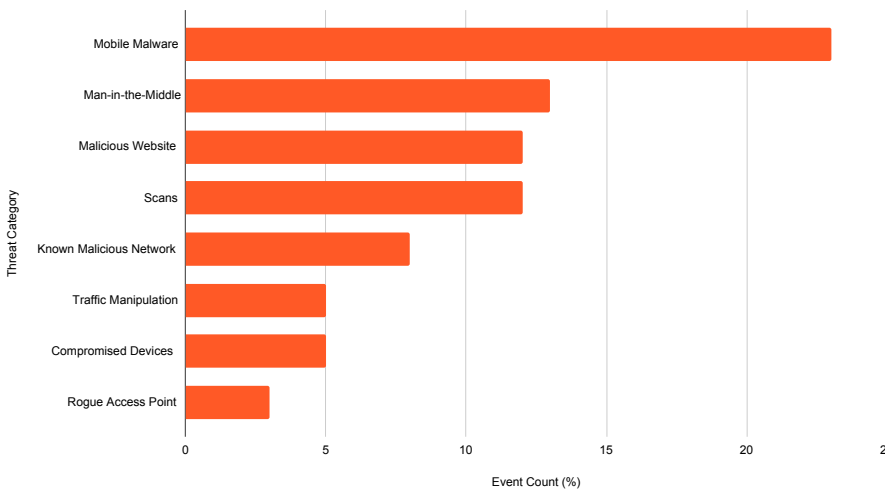
Mobile malware is more prolific than many believe to be the case, with a global average of 23% of endpoints encountering one form or another of these malicious applications in 2021.

Whether sideloaded from a third-party source or direct from an OEM store, malware presents the greatest statistical risk to mobile devices, users, and cloud-connected data.

Man-in-the-middle attacks and scans also presented significant risks to endpoints as part of larger attack chains against corporate systems and highly valued data access, acting as critical steps in attack chains for intelligence gathering and reconnaissance. An average of 12% of mobile endpoints, or 1 in 10, encountered phishing and the malicious websites, risking user credentials, device integrity, and enterprise security.

Expected Events per Year per Device | Global Average

Global Mobile Threat Events

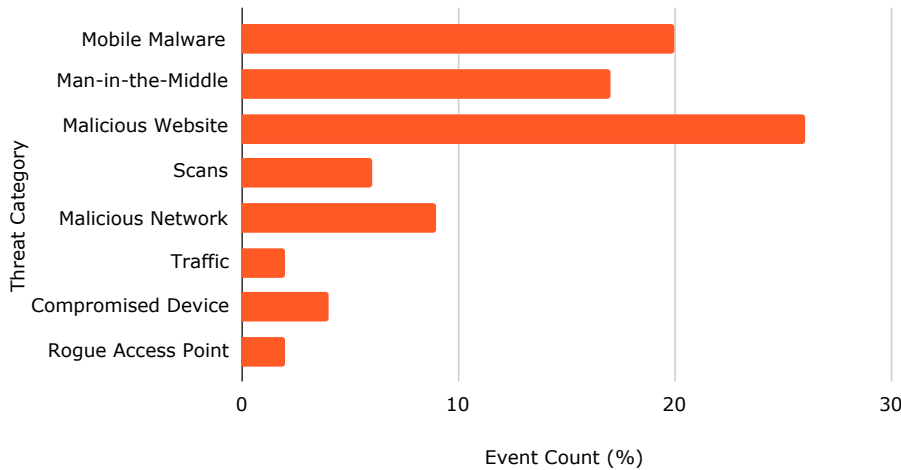


- 23%** encountered malware
- 13%** encountered man in the middle
- 12%** encountered a malicious website
- 12%** encountered scans
- 8%** encountered a known malicious network
- 5%** encountered traffic manipulation
- 5%** compromised devices
- 3%** encountered a rogue access point

Threats to Mobile Endpoints by Region

Expected Events per Year, per Device | APAC

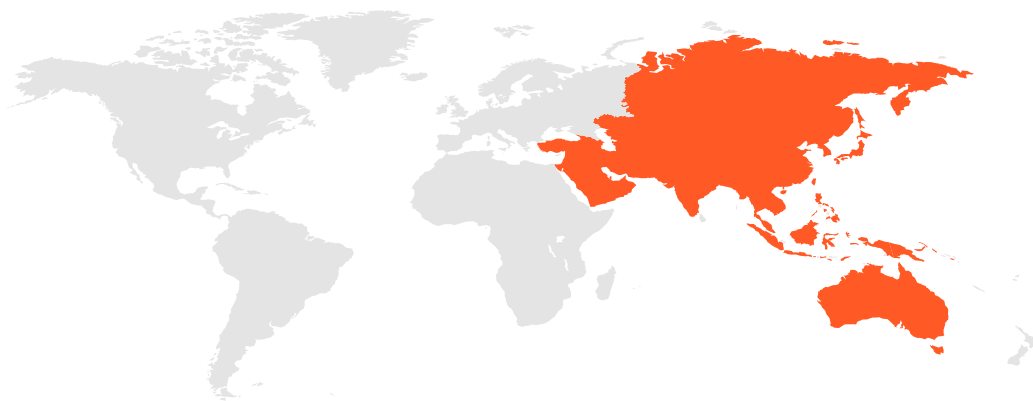
Asia/Pacific, Mobile Threat Events (2021)



- 26%** encountered a malicious website
- 20%** encountered malware
- 17%** encountered man in the middle
- 9%** encountered a known malicious network
- 6%** encountered scans
- 4%** compromised devices
- 2%** encountered traffic manipulation
- 2%** encountered a rogue access point

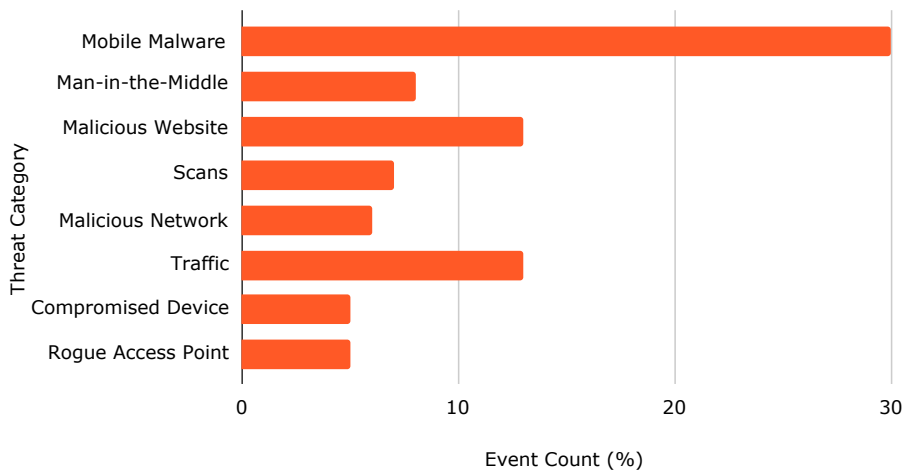
APAC | Mobile users in Asia/Pacific Region are twice as likely to encounter malicious websites compared to the worldwide average.

1 in 4 - or 25% - of mobile enterprise devices encountered phishing at least once in 2021. Phishing dominated the Asia/Pacific region, targeting mobile devices through common communications tools like SMS, social media, and other chat programs. In-app messages also bypassed many external security controls, delivering phishing websites directly to the mobile device. 1 in 5 mobile devices encountered malware, with evidence indicating the top culprits were third-party app stores and sideloading through phishing. 17% of enterprise secured mobile devices encountered man-in-the-middle attacks, with just under 10% having their devices scanned from critical data and information by a network.



Expected Events per Year, per Device | Africa

Africa, Mobile Threat Events (2021)



30% encountered malware

13% encountered a malicious website

13% encountered traffic manipulation

8% encountered man in the middle

7% encountered scans

6% encountered a known malicious network

5% encountered a rogue access point

5% compromised devices

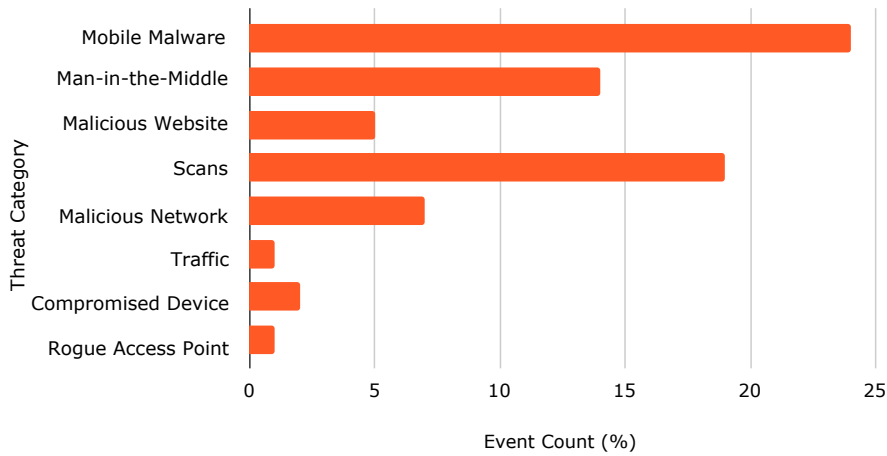
Africa | In 2021, a staggering 30%, or 1 in 3, mobile endpoints in Africa encountered malware, accounting for the biggest risk to enterprises and users in the region.

Phishing and spear-phishing attacks using SMS or communication tools were detected on 13%, or just over 1 in 10, mobile devices. Another 13% of endpoints encountered traffic manipulation, impacting the actual security of the connection the mobile device had with its network. Around 8% of devices are connected to risky networks, and these connections put the communication and data at risk through man-in-the-middle attacks.



Expected Events per Year, per Device | Europe

Europe, Mobile Threat Events (2021)



24% encountered malware

19% encountered scans

14% encountered man in the middle

7% encountered a known malicious network

5% encountered a malicious website

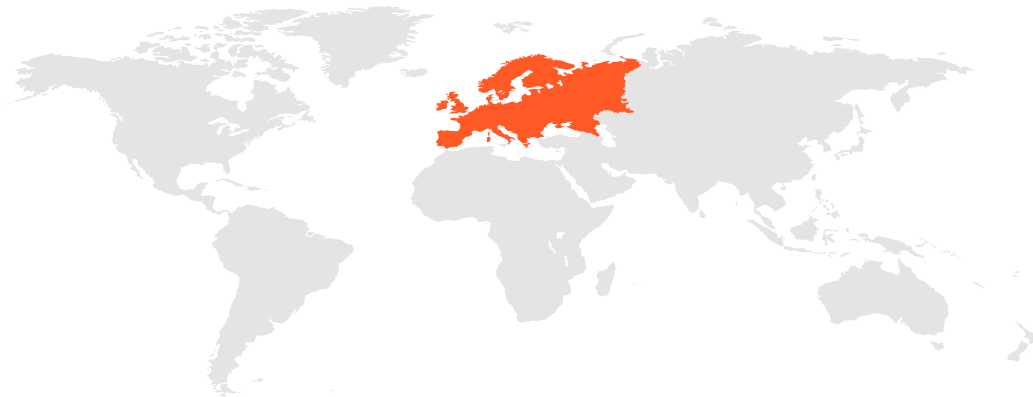
2% compromised devices

1% encountered traffic manipulation

1% encountered a rogue access point

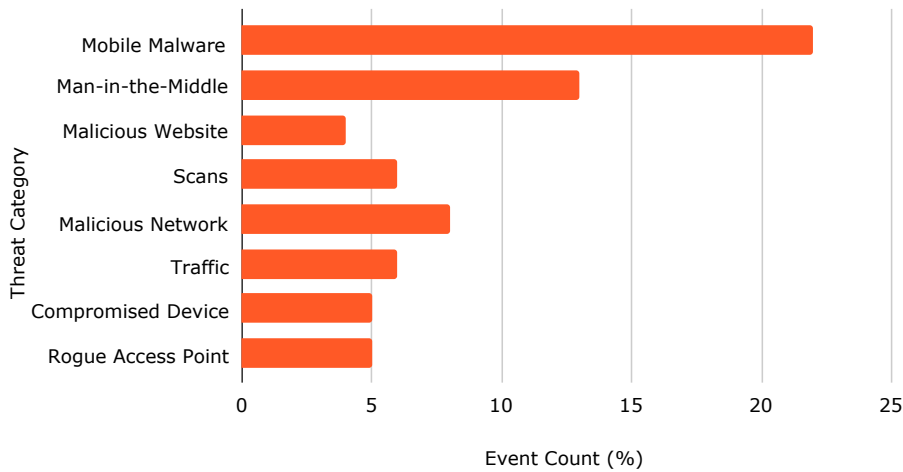
Europe | 1 in 4, or 24%, European mobile users encountered malware on their devices, putting personal and enterprise data at risk.

All combined, compromised and malicious networks and data handling accounted for the biggest risk to mobile users in European nations. 1 in 5, or 19%, mobile users encountered network reconnaissance through scans, potentially revealing critical data about the device. 14% of devices experienced man-in-the-middle attacks, with 7% connecting into networks with high risks and security concerns.



Expected Events per Year Per Device | North America

North American Mobile Threat Breakdown



22% encountered malware

13% encountered man in the middle

8% encountered a known malicious network

6% encountered traffic manipulation

6% encountered scans

5% encountered a rogue access point

5% compromised devices

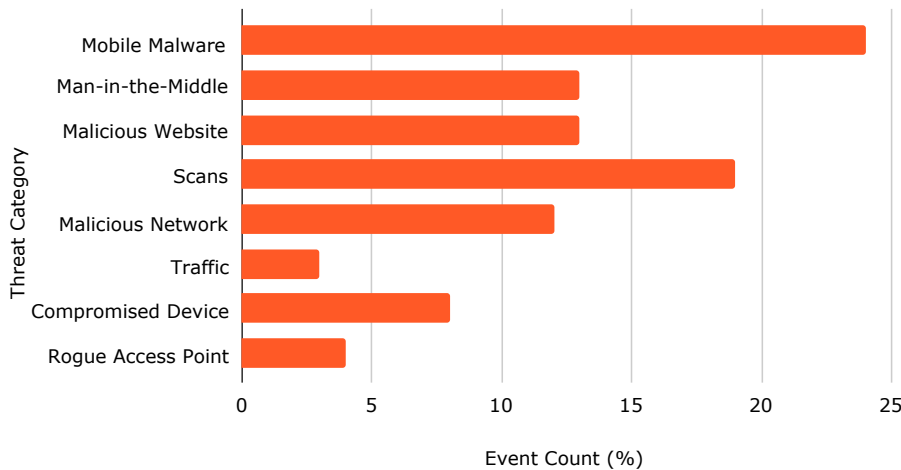
4% encountered a malicious website

North America | 1 in 4 enterprise mobile devices encountered malware in North America, putting devices and data at risk for both the end user and organization. Man-in-the-middle attacks were also prominent against phones and tablets, accounting for 13% of the attempts to intercept communications. While not as pronounced as the other two threats, known malicious network and traffic manipulation risks highlight data tampering as an enterprise risk arising from poorly secured networks.



Expected Events per Year Per Device | South America

South America Mobile Threat Breakdown



24% encountered malware

19% encountered scans

13% encountered a malicious website

13% encountered man in the middle

12% encountered a known malicious network

8% compromised devices

4% encountered a rogue access point

3% encountered traffic manipulation

South America | 1 in 4 mobile endpoints, or 24% of those in South America, encountered mobile malware in 2021. It was usually delivered through either direct downloads from app stores or sideloaded to bypass regional restrictions. 1 in 5 mobile devices

encountered network scans, putting critical device information at risk from attackers. 13% of devices, or a little over 1 in 10, in South America also encountered phishing and man-in-the-middle attacks, putting critical data at risk through communication monitoring or credential theft.



The data shows the diversity in risks, threats, and attacks targeting mobile endpoints on a global scale. Mobile malware continues to dominate the threat landscape, acting as the most efficient and effective methods to attack, compromise, and steal from mobile endpoints. Network-based attacks are also incredibly effective and prominent, taking advantage of the mobile phone's significant differentiator - the ability to always seek connectivity. With the rise in remote and distributed workers and customers, enterprises need to prepare and secure against an ever-changing landscape of threats based on where their employees, apps, and data are in the world. The modern attack surface has grown, and the threats against enterprises continue to be prevalent and effective against unsecured devices.

Breakdown of Exploited Vulnerabilities of 2021

2021 was the “Year of the Exploit.” Security teams fought against an increase in zero-day, or never-before-seen, exploited vulnerabilities across endpoint systems, including mobile Android and iOS systems. **The increased reliance on and growth of the mobile market has presented viable opportunities for malicious actors to exploit typically unsecured systems, with over 30% of known, zero-day vulnerabilities discovered in 2021 targeting mobile devices⁴⁴. This trend represents the most significant increase in zero-day exploits in the history of smartphones and tablets.** Even Google’s Project Zero addressed this in a recent disclosure of multiple zero-day vulnerabilities.

Whether known or unknown, each exploit presents a potential gap in managing a mobile device’s attack surface. In the world of BYOD, the mobile device attack surface is no longer a consumer-only threat. Each one represents a risk to enterprise security. In the hands of the right attackers, any exploit could be an effective tool in an attack on a managed or unmanaged mobile endpoint, helping them gain a foothold in enterprise systems and networks.

Unpatched and unaddressed, these known CVEs put enterprises at risk by leaving gaps in systems. To complicate matters and environments further, manufacturers manage their security release cycles differently. Meanwhile, many older phones do not receive the newest updates, leaving them at risk to older, known vulnerabilities and easier targets by malicious actors.

Over the last few years, researching mobile device zero-day vulnerabilities has become increasingly lucrative. With that in mind, more researchers are actively looking for exploits. In response, enterprises need to mitigate these new threats to their systems and networks.

“The growth of mobile platforms has resulted in an increase in the number of products that actors want capabilities for.”

—Maddie Stone & Clement Lecigne,
Google Threat Analysis Group, 2021 ⁴⁵

As discoveries of mobile exploits become increasingly profitable for many security researchers, more zero-day exploits have been discovered and reported. Official and unofficial bug bounties abound with big payouts for advanced discoveries, at least compared to exploits for traditional endpoints. For previously unreported mobile exploits, Zerodium, an exploit acquisition platform for premium zero-days and advanced cybersecurity research, currently has bounties up to \$2,500,000.⁴⁶ Since mobile device bounties can yield researchers more than double the payout, they are high-value research.

Here is a summary of the Android and iOS vulnerabilities in 2021, highlighting the complex attack surfaces of these two mobile ecosystems. Included is a history of the zero-day vulnerabilities, used in real-life attacks against mobile devices, throughout the mobile endpoint history.

Android CVE Tracker ⁴⁷

According to vulnerability tracking, the Android operating system saw a dip in the number of vulnerabilities discovered in 2021, with 574 CVEs tracked. In 2020, 859 were discovered. The most common vulnerabilities were code execution, system bypassing, and overflow of code or memory.



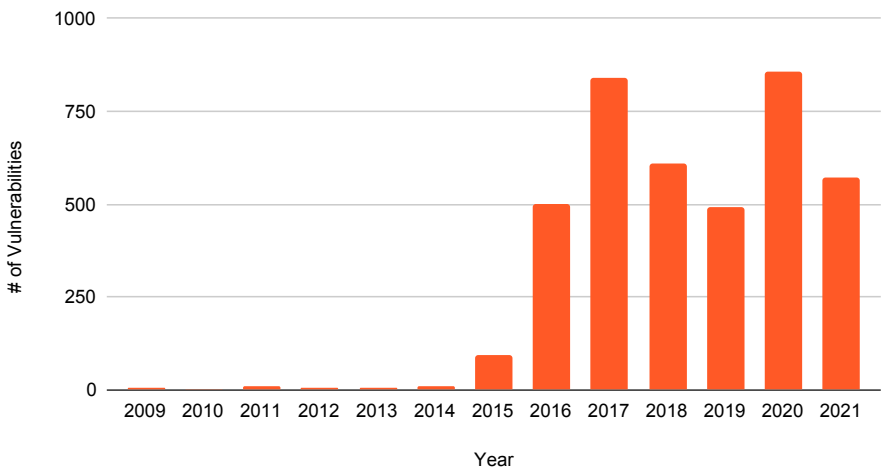
Of the reported and tracked vulnerabilities:

21% are categorized with a medium attack complexity.

79% are categorized with a low attack complexity.

135 (**23%**) of the tracked CVEs rated a CVSS score of **7.2** or higher, with **18** falling into the critical category. This is a decrease from the previous year, with **62** critical vulnerabilities discovered and reported in **2020**.

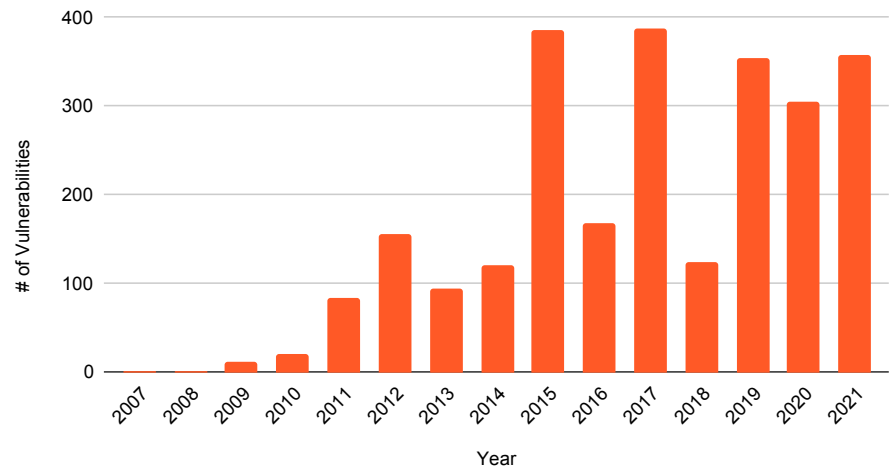
Android CVEs by Year



iOS CVE Tracker ⁴⁸

According to vulnerability tracking, Apple iOS had 357 CVEs assigned throughout 2021. This is an increase from the 305 discovered and reported in 2020. 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 vulnerabilities:

24% are categorized with low attack complexity

2% are categorized with high attack complexity.

74% are categorized as medium attack complexity.

63 (**17%**) of the CVEs rated a CVSS score of **7.2** or higher, with **45** falling into the critical category. In **2020**, **67** critical vulnerabilities were identified and reported.

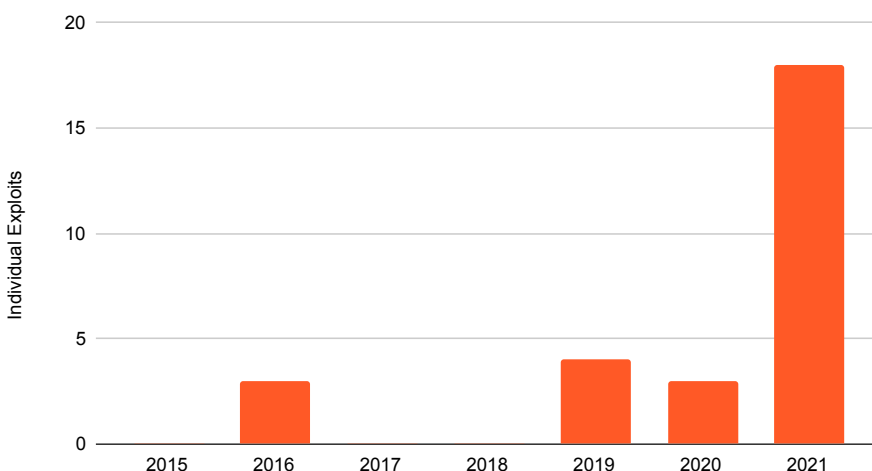
2021 was the year of mobile-specific zero-day exploits, as is evident by the markedly sharp increase from previous years.

The zLabs research team attributes this rise to the increase in personal, private, and critical data systems connected to mobile endpoints. When malicious threat hunters seek out new, exploitable opportunities, they look for devices with data access and low security coverage. Mobile endpoints present viable targets that, when exploited, become the keys to the data kingdom.

Zero-Day Exploits Discovered in the Wild in 2021 ⁴⁹

Zero-day, in the wild, exploits are vulnerabilities detected in actual attacks against users where neither the public nor the vendor knew of the vulnerability. This means that no patch was available when the attack took place.

Exploited In-The-Wild Mobile Zero Days



A look at the trends gives insight into the changing mobile device zero-day vulnerability landscape:

In 2021, there was a 466% increase in exploited, zero-day vulnerabilities used in active attacks against mobile endpoints.

- **2021:** 58 total zero-day exploits, with 31% (17) mobile-specific
- **2020:** 26 total zero-day exploits, with 11% (3) mobile-specific
- **2019:** 21 total zero-day exploits, with 19% (4) mobile-specific

Despite the massive popularity of mobile devices over the previous decade, the last three years saw zero-day vulnerabilities that target mobile endpoints - like phones and tablets - becoming a more significant challenge than ever before.

In 2021, iOS vulnerabilities accounted for 64% of mobile-specific exploited zero-days attacks.

The Rise of Mobile-Specific Phishing

References to phishing go back as far as 1995, but unfortunately, rather than receding into history, it has remained a significant part of the cyber attacker's arsenal. At a high level, here's how phishing works:

- Criminals create websites that mimic well-established organizations and then attempt to lure users to visit those sites.
- When a user submits their credentials or confidential information to the site, the attacker can use those credentials to take control of accounts and pursue other tactics.
- Because many users have the same password across sites, one successful attack can often expose multiple services and accounts.
- It uses social engineering to exploit the end-user's trust and curiosity in official looking communications.

Attackers typically target victims through electronic channels, such as email, website hijacking, and SMS messaging. However, attackers can also use phone interactions to dupe a target. Over the years, some different subcategories have emerged:

- **Spear phishing.** An attacker targeting a specific organization or person.
- **Whaling.** Attacks targeting senior high-level executives and other high-profile targets.



Phishing continues to be employed because, quite simply, **it works.**

Phishing Prevalence

One report found that phishing was present in 36% of breaches, and that the practice grew 10% between 2020 and 2021.⁶⁰ Additional research found phishing emails were the leading point of entry for ransomware, constituting around 54% of these attacks.⁶¹

In our research, when asked about risks that most concerned them, “exploitation via phishing” was the top-rated response (55%). In addition, 61% of respondents said they’d seen a spike in phishing attacks during the COVID-19 pandemic. Further, crafting phishing attacks continues to get easier: tools and phishing kits now enable even novice users to deploy deceptive sites with just a few clicks.

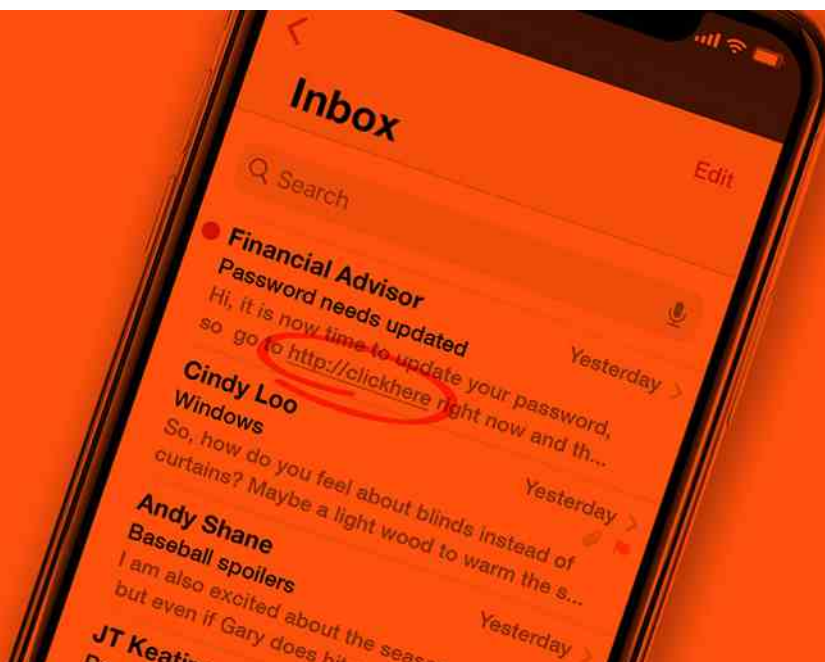
Over the years, we’ve continued to grow increasingly reliant upon our mobile phones, both in our personal and professional lives. While that was the trend for some time, the COVID-19 pandemic served to turbo-charge the transition. This increased reliance on smartphones for work means users are routinely accessing corporate assets and apps. This, combined with the fact that these devices don’t have the same level of security typically found on traditional laptops and desktops, is encouraging would-be attackers to focus on mobile devices.

Typically, mobile endpoints don’t have any security or, if they do, those security mechanisms are not up to the same level as on a traditional endpoint. When teams attempt to apply legacy security tools to mobile devices, they often encounter several limitations. For example, processing constraints may limit potential analysis capabilities. On mobile devices, sandboxing tools don’t deliver all the information needed for advanced threat detection.

Further, mobile devices inherently present additional challenges. The smaller screens of mobile endpoints may hide clues that could tip off a user about a malicious site, as the screen size may hide a red flag from view. Mobile devices are used for many communication vectors, including email, chat, in-app messaging, instant messaging, and more. These various channels offer an expanding number of attack surfaces for criminals to exploit.

61%

of respondents said they’d seen a spike in phishing attacks during the COVID-19 pandemic



When you couple the insecurity of mobile devices with the fact that those devices are now gateways to sensitive corporate and personal assets, it is no surprise that these devices are increasingly the focus of attackers.

While phishing used to be predominantly device-agnostic in nature, Zimperium has detected a rise in mobile-specific phishing websites. We conducted an analysis of our data and public data over a period of two and a half years. For the analysis, we analyzed more than 500,000 sites. **Over that period, the number of mobile-specific phishing websites grew by 50%. Further, over the course of 2021, 75% of the phishing sites analyzed specifically targeted mobile devices and deliver content appropriate for the mobile format.**

Phishing Sites Exploiting Mobile, 2019-2021

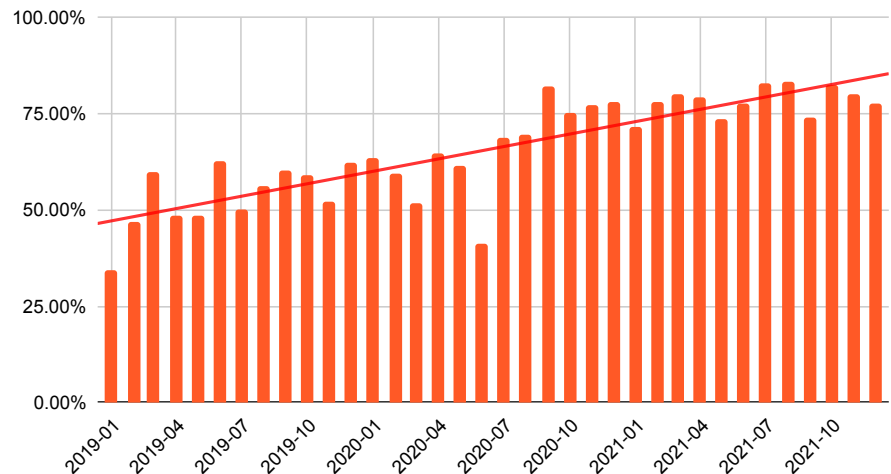


Figure 4: The number of phishing sites that specifically target mobile devices has seen rapid growth, and now these mobile-targeted sites make up more than three-quarters of all sites analyzed.

In addition, there has been an increasing sophistication in the attacks being tracked. **Between 2019 and 2021, for example, the percentage of phishing sites using secure communication (commonly known as HTTPS) has grown steadily, making it increasingly difficult for users to distinguish these sites from those that are legitimate.**

Phishing Sites Using https, 2019-2021

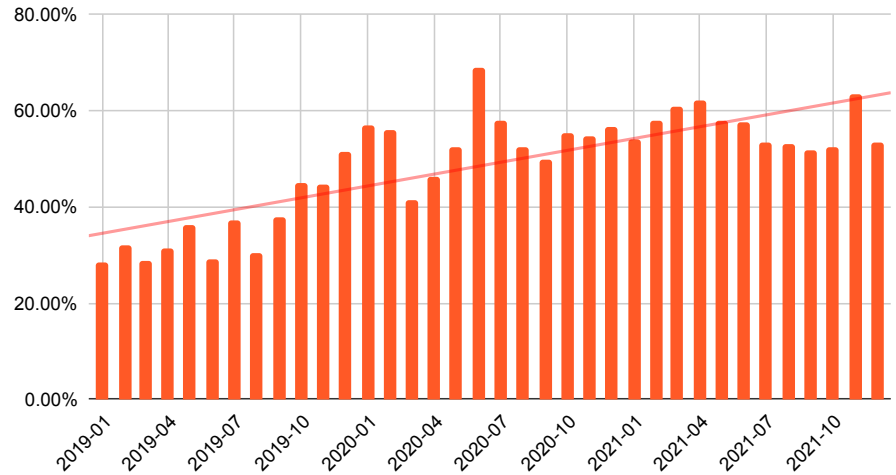


Figure 5: The percentage of phishing sites that use the HTTPS protocol has seen consistent growth.

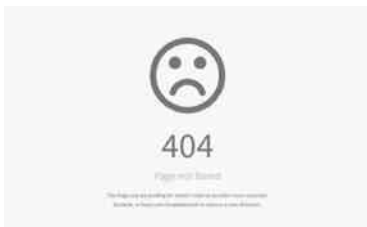


Figure 6: While a user browsing this malware site with a laptop will receive a 404 error message, a mobile device user will see a phishing site that mimics a PayPal login screen.

How Attackers Target Mobile Devices

To target mobile devices, attackers use either adaptive or responsive techniques. Here is a summary of some of these approaches.

Adaptive Websites

Adaptive websites can load completely different content and redirect to alternate sites, depending on the device being used. Attackers adapt content based on the user agent of the mobile endpoint. Through this approach, an attacker can exclusively target mobile devices. For example, if a desktop is detected, they can keep the page from loading at all. In this way, attackers can avoid detection by desktops with threat detection tools.

Responsive Websites

Responsive websites adapt the placement and size of objects according to the screen size of the endpoint in use, and show OS appropriate dialog interfaces. While this responsiveness enables legitimate app developers to provide a better user experience, these same capabilities can give attackers an edge in phishing.

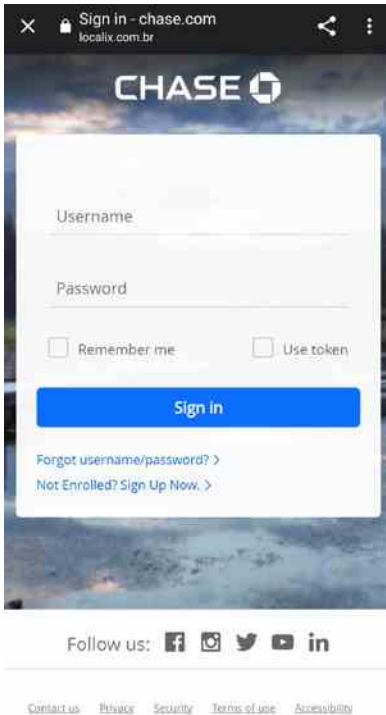


Figure 8: An example of a mobile user's view of the same phishing site.

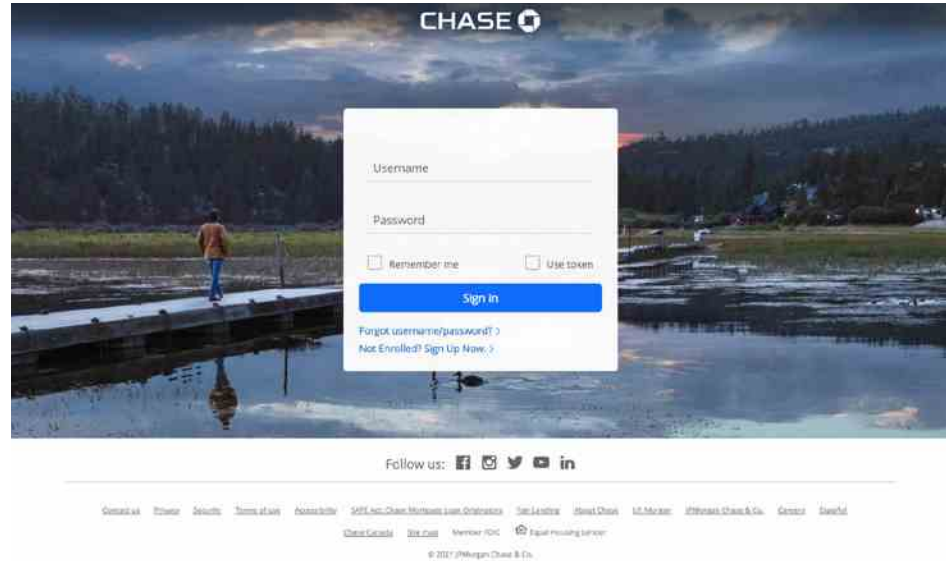


Figure 7: An example of a responsive phishing site targeting Chase customers. This is the view a desktop user would see.

The Most Phished Brands, Globally

When waging phishing attacks, criminals aim to fool their victims into thinking they're hearing from an organization they routinely conduct business with. Given that, it's no surprise that there is a clear correlation between a brand's popularity and its propensity to be targeted. **The most recognizable, consumer-facing retail, social media, technology, and financial services institutions dominate the phishing category. Phishers hope that a consumer's trust or reliance on a specific brand will get that individual to submit their credentials.** Following are region-specific results in terms of brands most used by phishers.

North America

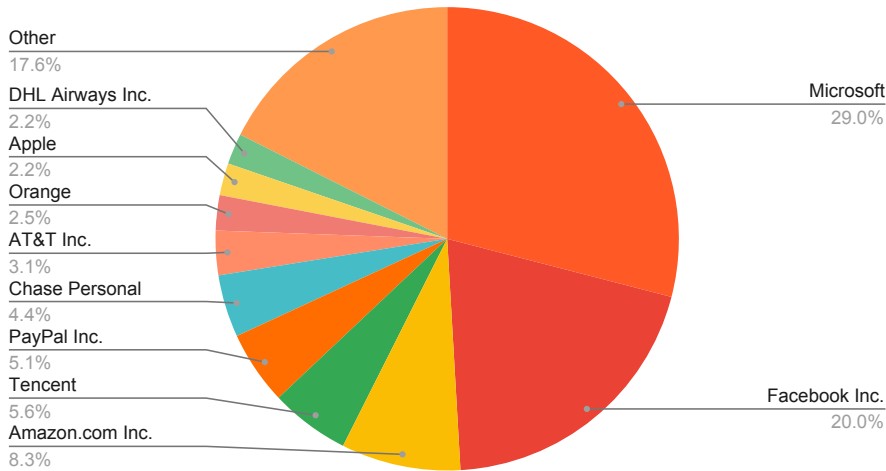


Figure 9: The percentage of businesses mimicked by phishing sites targeting users in North America.

In North America, almost one-third (29%) of enterprise phishing attacks purported to be from Microsoft. Phishing sites emulating Facebook and Microsoft (20%) accounted for nearly half of all attacks waged. Amazon was a distant third, with slightly over 8.3%. The remaining sites also included financial services institutions (with PayPal and Chase combined accounting for 9.5%), telecommunications companies (with AT&T accounting for 3.1% and Orange 2.5%), and a shipping business (DHL Airways had 2.2%).

Central / South America

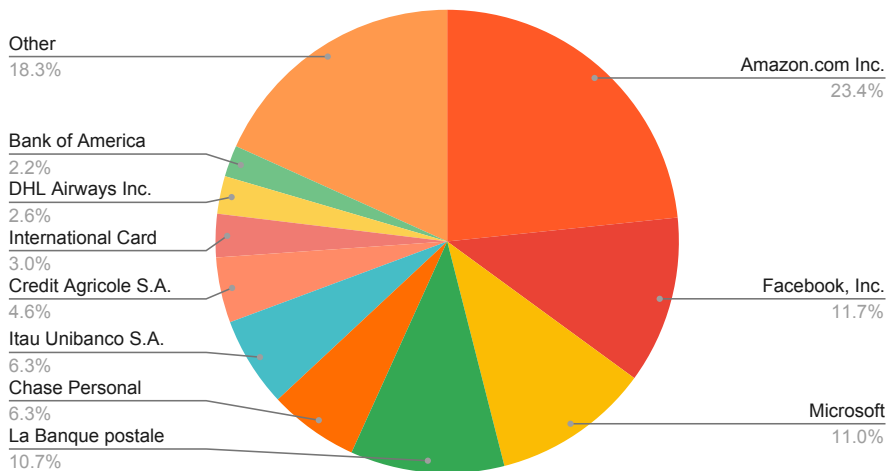
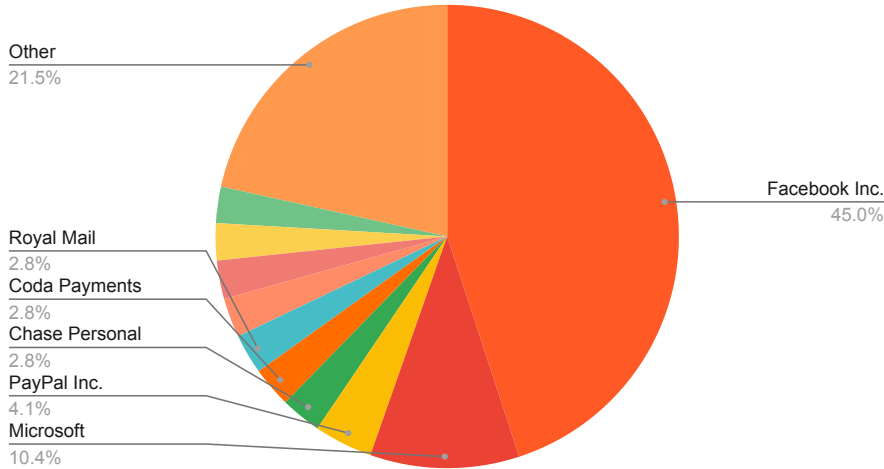


Figure 10: The percentage of businesses mimicked by phishing sites targeting users in Central and South America.

Within Central and South America, Microsoft and Facebook, number one and two in North America, were supplanted by Amazon, which appeared in almost one-quarter (23.4%) of all phishing sites. Facebook and Microsoft were number two and three, respectively. With the exception of DHL Airways (2.6%), the remaining top phished brands were all financial services firms, with La Banque postale featured in 10.7% of attacks.

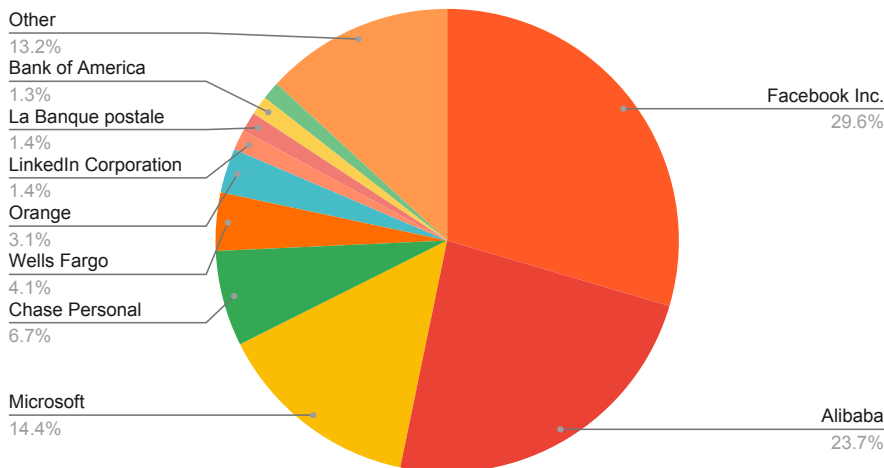
Europe / Middle East



In Europe and the Middle East, Facebook is by far the favored brand for phishing attacks. The social media firm accounted for 45% of targeted brands. Microsoft was a distant second at 10.4%. Financial services firms were targeted in six of the remaining nine most targeted brands.

Figure 11: The percentage of businesses mimicked by phishing sites targeting users in Europe and the Middle East.

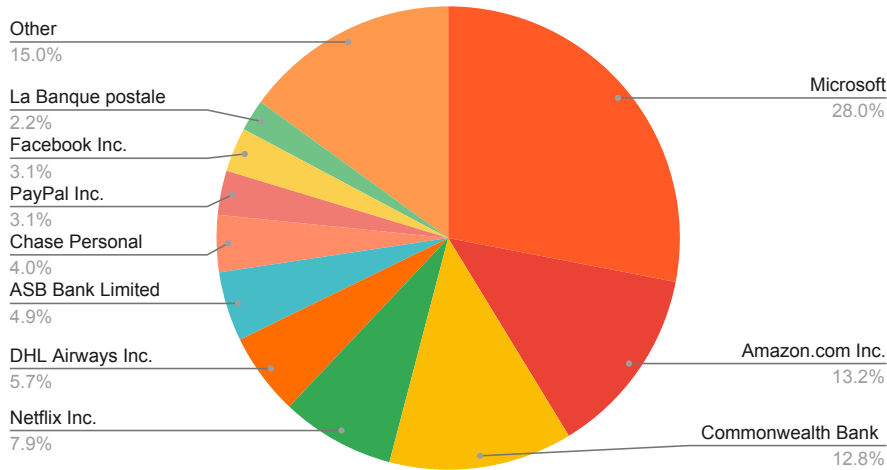
Africa



In Africa, as in Europe and the Middle East, Facebook was the number one choice of attackers, featured in 29.6% of phishing sites. The large market share of Alibaba in Africa was reflected in the result, comprising 23.7% of attacks. Microsoft (14.4%) was number three, followed by Chase (6.7%) and Wells Fargo (4.1%).

Figure 12: The percentage of businesses mimicked by phishing sites targeting users in Africa.

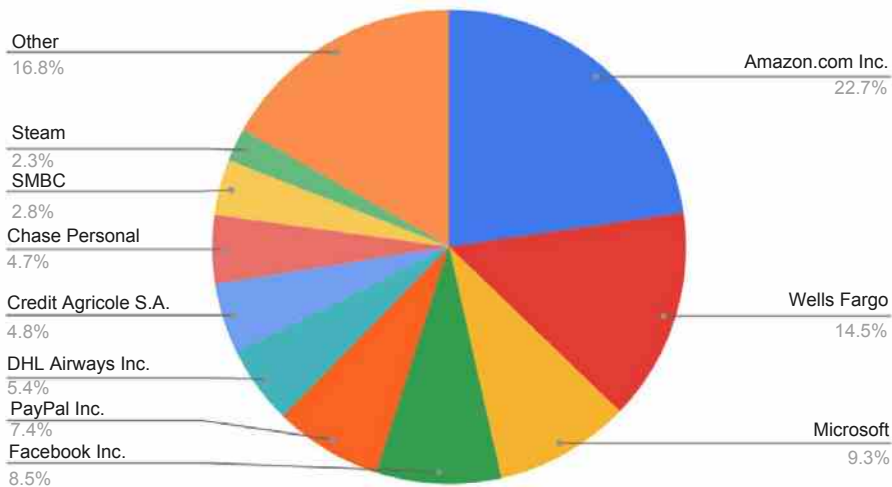
Australia



In Australia, as in North America, Microsoft is the most targeted brand, appearing in 28% of phishing sites. Amazon (13.2%) and Commonwealth Bank (12.8%) were followed by Netflix (7.9%), which didn't feature nearly so prominently in other regions. In addition to Commonwealth, several financial services firms were in the top 10, including ASB Bank (4.9%), Chase (4.0%), PayPal (3.1%), and La Banque postale (2.2%).

Figure 13: The percentage of businesses mimicked by phishing sites targeting users in Australia.

Asia/Pacific



In the Asia Pacific Region, Amazon (22.7%) was the brand most used by phishers. Wells Fargo, while present in several regions, shows up higher here than anywhere else, with 14.5%. Despite having a dominant market position in the area, Steam only showed up in 2.3% of attacks.

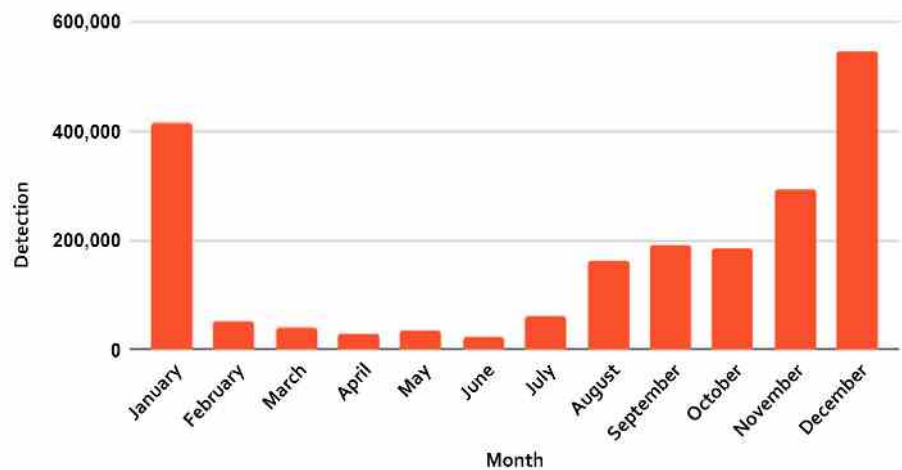
Figure 14: The percentage of businesses mimicked by phishing sites targeting users in the Asia-Pacific region.

Risks and Attacks: Mobile Malware, Bugs, and Profiles

Malware is in every bad actor's arsenal because it is easy to access and deploy while wreaking havoc on a massive scale. There are millions of unique malware variants, with thousands of new apps created and released daily. Malware has become the single biggest source of profit for attackers, and for this reason, it is a moving target.

In 2021, Zimperium's mobile security analysis uncovered 2,034,217 new malware samples detected in the wild. On average, that is nearly 36,000 new variants of malware a week - over 5,000 a day.

New Android Malware, 2021



Although the number of new, unique malware is down 50 percent from the prior year, our findings indicate that contributions to this change included recycled families of malware. 2020 was the year of big changes, from an increase in mobile workers to workflows with new apps and services, along with health apps related to the COVID-19 pandemic, giving malicious actors unique opportunities to deliver malware. 2021 experienced far less change and disruption to everyday life, and the novel impact of the previous year's news wore off, forcing malicious actors to focus on more effective exploits and attacks. Researchers also noted that threat actors have invested heavily in sophisticated frameworks in 2021, like Flutter, Cordova, and Unity, over traditional code from years past.

In 2020, attackers took advantage of the pandemic lockdowns that forced companies worldwide to adopt a distributed workforce.

In 2020, attackers took advantage of the pandemic lockdowns that forced companies worldwide to adopt a distributed workforce. These novel situations accounted for a significantly larger attack surface as workforce members often use both company-supplied and personal devices, like mobile devices, to maintain productivity. Ultimately, this situation contributed to increased malware, ransomware, and exploitation across enterprise organizations.

In 2021, our data showed that new mobile malware variants increased from October and reached a peak in December. The increase was no surprise. Bad actors leverage online and retail discounts promoted through links in emails and text messages during shopping holidays, hoping users will download malware through their mobile phones.

Mobile malware is unique because the mobile attack surface is different. Some mobile malware variants act like traditional endpoint attacks, like spyware and trojans. Others malware can impact users in a way traditional malware cannot, including:

- Stealing 2FA credentials through SMS or app notifications
- Performing overlay attacks where a user enters credentials into a secondary app, believing it to be the legitimate app
- Monitoring other installed apps through Accessibility Service permissions
- User location tracking through GPS services
- Activate the cameras and microphone, recording audio and video
- Access sensitive content like photos, contacts, and personal data
- Capture and track sensor data such as gyroscope and location / nearby devices

Evasion and exploitation techniques evolve to circumvent detection mechanisms and avoid killing the golden goose, evidenced by the number of new mobile malware samples we see every single day. Not only is detecting mobile malware increasingly sophisticated, but mobile devices collect high-value data. This creates a perfect storm for bad actors who want to carry out a quick, high-payout attack.

Advanced Novel Malware Techniques Targeting Mobile

Mobile malware is following the path of traditional, advanced attacks in what can almost be described as a renaissance period. New and advanced capabilities are making their way into the mobile attack chain, taking advantage of the new capabilities, constant data access, and lack of security across the ecosystems. Past samples of mobile malware were often viewed as simple and granular, but recently discovered samples of mobile malware and attacks show complicated techniques used in targeting traditional endpoints and services are starting to make their way into mobile attacks.



2FA Interception

Sample: 4a7d9ee4d3a7132d2838a78a8744522b5324c7267fa2675ab70e36b73ceecf

Disguised as an adult version of TikTok. After installation, it asks for the user's phone number and immediately sends it to the C&C. The backend starts generating login attempts for a series of services, like Telegram, Google, AliPay, Amazon, MPL, Ludo, Viber, and as well as various Russian services. The app is then responsible for intercepting the 2FA codes. The codes are then sent back to the C&C, completing the account takeover.

Persistent Attacks

Sample: ed4a7d9ee4d3a7132d2838a78a8744522b5324c7267fa2675ab70e36b73ceecf



A new variation of a classic banker trojan, this app mimics a flash player but doesn't have any function. This advanced mobile malware heavily relies on the TOR network to anonymously deliver a malicious payload and communicate with the C&C. The flow of the attack starts with the extraction and execution of the payload in memory (no traces on disk). Afterward, the app downloads the TOR binaries for the specific architecture, requesting the C&C address via the TOR network, and downloads the overlay payload from the C&C. From there, additional APK payloads are downloaded, leading to an overlay attack on 238 target applications with the capability to dynamically add support for additional targets. It aggressively asks for accessibility services and cannot be uninstalled or opened again. There is no way to remove the malware after installation and requires a factory reset of the device.

Credential Theft

Sample: 1f403159ec3c5e1f1ef739ca01f5eff76d3fdfe1d8b7dd40d75de9cf30506958

This credential stealing app disguises itself as an Instagram follower tool. In actuality, it is a Facebook credential stealer, getting the cookies after a legit login attempt.

Sample: 5d065ed8c31e32041120722db9f3b7c24225e07935c720efe345ffd1e86b-d8ce targets



Facebook credentials, injecting malicious JavaScript in the displayed WebView to intercepts a victim's credentials. Credential theft mobile malware is on the rise due to the common practice of reusing passwords across multiple services, giving attackers access to various tools and logins.

Apple iOS's Increased Attack Surface

It is not just malware that can directly impact the security of an iOS-powered device. iOS configuration profiles give businesses the capability to install and run applications signed by the provider without the scrutiny of Apple's App Store submission and were initially designed for configuration management, for example, use by MDMs. Once approved, Apple provides the developer a signed certificate for the business to apply to the device, enabling them to install any app they have produced in-house onto the device. However, this feature also allowed end-users to sideload unapproved and often unsecured apps without established OEM protections from third-party stores, increasing the risk of data theft and exploitation on the device as there are limited or no vetting of submitted apps in these third-party stores.

iOS configuration profiles serve a wide range of legitimate scenarios for enterprises that have adopted mobile-managed and unmanaged mobile devices into their ecosystem. For example, MDMs use profiles to enforce configurations in the devices, and 30% of the profiles Zimperium evaluates are from management tools. But the remaining 70% are installed by users, outside the control and visibility of the enterprise.

Most common end-user installed iOS configuration profiles



Figure 15: Zimperium researched data highlighting the most common end-user installed iOS configuration profiles.

Each iOS configuration profile type exposes the user to a different potential risk. While a profile used to set up a font on the device or to install a printer through Airplay could be considered as a low-risk profile to a user, the installation of a new certificate authority could allow a potential attacker to decrypt all the secured traffic from a specific device while a malicious VPN profile or proxy configuration can redirect all the network traffic on the device to a server controlled by a malicious actor.

A malicious profile would enable system-wide settings and allow untrusted certificates to be installed on the device. From free VPNs to proxy configurations, third-party app stores to root certificates, data can be re-routed and shared in its unencrypted state, or data such as contacts and email credentials shared to malicious parties. There is no way to know where any data from compromised devices is sent or decrypted after a malicious profile is loaded.

Risk distribution of unmanaged iOS configuration profiles

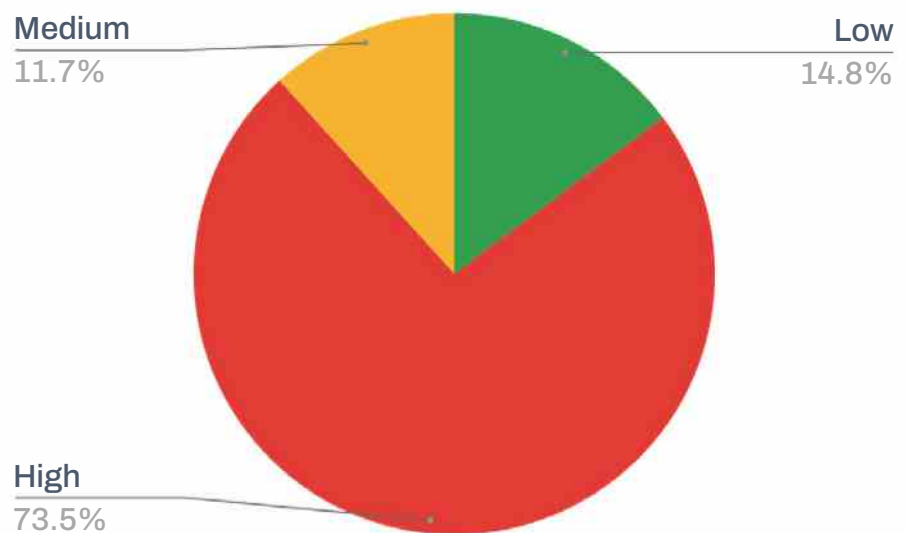


Figure 16: Zimperium researched data highlighting the risk distribution of unmanaged iOS configuration profiles

However, in a report released in October 2021 aiming to defend its locked ecosystem, Apple revealed that this program had inadvertently increased the attack surface of iOS devices with little way to stop the exploitation. A rise in third-party services, like external stores and app signing services, has taken advantage of the feature since its launch to bypass Apple's AppStore security controls, allowing signed applications on non-jailbroken devices.

“Despite the program’s tight controls and limited scale, bad actors have found unauthorized ways of accessing it, for instance by purchasing enterprise certificates on the black market... Apple has increased efforts to tighten controls on the program and add user protections, but abuse has persisted.”⁵²

“Despite the program’s tight controls and limited scale, bad actors have found unauthorized ways of accessing it, for instance by purchasing enterprise certificates on the black market... Apple has increased efforts to tighten controls on the program and add user protections, but abuse has persisted.”⁵²

A compromised certificate enables malicious actors to develop applications that Apple ecosystem will consider legitimate and exempt from any review process. Unfortunately, the organizations only detect the abuse when the certificate is revoked. This user-activated option poses a considerable risk to enterprises.

In 2021, 11 separate zero-day exploited in-the-wild vulnerabilities were revealed targeting Apple iOS and Apple WebKit, accounting for 19% of all zero-day exploits for the year.⁵³ While malware used against iOS devices is not as common in the news, the bugs and vulnerabilities receive significant attention due to their impact and customer base.

Security vendor ZecOps also revealed research behind WiFiDemon, a zero-click Wi-Fi proximity vulnerability on iOS 14 through iOS 14.4 without any assigned CVE. The research team at ZecOps reported that the network crash issue was actually an unpatched zero-day vulnerability. The vulnerability enabled attackers to remotely execute code on the victim’s phone or tablet without any interaction by or notification to the end-user. While the zero-click component of the vulnerability was patched with iOS 14.4, newer versions of the mobile OS did not receive the patch until iOS 14.7 was released.

Mobile App Threats: More Than Data Is at Risk

For mobile app developers, having an incredible, one-of-a-kind mobile app idea is one thing. But what about security? The security of a mobile app is critical, especially as attacks on mobile devices continue to evolve and expand. Mobile phones and apps are a soft target, and attackers are keenly aware of this.

As of the first quarter of 2021, close to 3.5 million apps were available on the Google Play Store and 2.2 million apps on the Apple App Store.⁵⁴

In the 2nd half of 2021, Zimperium researched and analyzed the risk posture of over 160 global financial mobile applications. Our research found that **approximately 81% of those financial applications potentially leaked sensitive information**, either directly from the application or indirectly through integrated libraries and SDKs.

Adopting encryption is insufficient as poor implementations and key management practices can expose confidential and cryptographic data to bad actors. Expanding the breadth of applications beyond financial applications to include healthcare, retail, and lifestyle apps, **we found that 77% of Android and 46% of iOS apps use, or potentially use, at least one vulnerable encryption algorithm.** This can jeopardize data at rest, in transit, or on access in any of these highly critical categories.

Securing, and protecting an app does not stop once the application is published. Through reverse-engineering tactics, malicious actors can find weak entry points within the application's code. Therefore, it's critical to do penetration testing of applications on an ongoing basis. However, 24% of respondents state they perform these tests on their mobile applications once a year.⁵⁵

Privacy and security are top priorities for consumers and enterprises, so it is vital that developers harden their mobile apps. Why is this critical for enterprises? Consider 51% of our respondents say they have installed four to eight work-specific apps on their mobile devices, while 31% have at least one.⁵⁶

The mobile threat landscape constantly evolves as new vulnerabilities and techniques are discovered. This requires security solutions to be comprehensive and fast and easy to update. When left unchecked, vulnerabilities in mobile apps can have a devastating impact on revenue, brand reputation, and operations.

However, in a recent survey, 49% of respondents say that when a new risk is discovered, they only update their apps at the time of the next planned release.⁵⁷ Further, even after a new release is issued, customers may not actually deploy those updates immediately. Particularly for enterprises with large application footprints, this could mean apps and data remain exposed for 12 to 18 months while the entire install base chooses to upgrade the app.

Mobile Application Risks by Industry

As bad actors continue to exploit mobile apps, compliance and regulatory factors are at play in several industries:

- **Healthcare.** If health data gets into the wrong hands, healthcare organizations are subject to Health Insurance Portability and Accountability Act (HIPAA) fines and penalties.
- **Financial services.** Financial organizations are subject to fines for data breaches and compliance failures. Further, breaches have skyrocketed since the COVID-19 pandemic.⁵⁸
- **Retail.** Poor security practices can leave retailers vulnerable to fines for breaches of the Payment Card Industry Data Security Standard (PCI DSS). These businesses could also face legal fees and penalties if consumers are affected by a cyberattack.



Businesses across industries must comply with relevant regional privacy regulations, including the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These laws give consumers specific rights regarding how their data is managed and used. In addition, they apply to any organization that manages personally identifiable information (PII) of people in regions governed by these laws. Therefore, these rules apply to financial, retail, and healthcare apps, as well as lifestyle apps. Failure to comply can leave a business subject to fines and class action lawsuits. This includes cases where customer data is part of a data breach or cyberattack due to a lack of adequate security measures.



Android

iOS

Financial Apps

Data Protection Lacking	49.9%	41.2%
Use Vulnerable Encryption Algorithms	79.8%	42.3%
Code Protection Lacking	64.4%	71.9%

Healthcare Apps

Data Protection Lacking	45.4%	36.6%
Use Vulnerable Encryption Algorithms	72.4%	41.4%
Code Protection Lacking	82.4%	72.2%

Retail Apps

Data Protection Lacking	61.1%	48.0%
Use Vulnerable Encryption Algorithms	80.4%	54.0%
Code Protection Lacking	69.7%	82.34%

Lifestyle Apps



Data Protection Lacking	54.6%	44.5%
Use Vulnerable Encryption Algorithms	77.4%	49.0%
Code Protection Lacking	74.8%	74.0%

App Cloud Storage and databases - the developer shadow IT service

Many apps rely on cloud storage or databases to perform their functions and provide centralized support. Developers can use the cloud to store configuration files, media files, and other resources. Setting up cloud storage or remote datastores for an app is extremely easy. However, setting up the needed security configurations is often either not prioritized or completely overlooked. This poses a significant risk: By analyzing apps, attackers can determine if an app is using cloud storage, and more importantly, whether any security measures protect that cloud storage.

It should be noted that in some cases, developers may be working with sample code or libraries that access cloud storage and not even be aware of these interdependencies. As a result, they may not know about, let alone address, the potential risks.

By accessing cloud storage, an attacker can extract sensitive information, such as health information, configuration files, personally identifiable information (PII), and much more.

	 Android	 iOS
Total number of apps with leaky cloud configuration	18.85%	8.19%

4.1

Why MTD Matters for XDR

Rick Bosworth, Director of Product Marketing, SentinelOne

7 of 10

organizations say mobile devices are critical to their business

1 of 3

zero-day attacks targeted iOS and Android devices

Mobile devices have become a must-protect asset class. Work-from-anywhere and BYOD policies are now the rule, not the exception, with **7 of 10 organizations stating that mobile devices are critical to their business.**⁶⁹ That same proportion of employees are using their personally-owned mobile devices to access corporate resources - customer lists, account strategies, financial models, the list goes on. Ironically, mobile devices are the primary means (i.e., via a 2FA app) of verifying identity and trust when accessing those resources. And that makes them a prime target in your enterprise attack surface, highlighting why **mobile threat defense is a critical component of an XDR security stack.**

There is a common misconception that mobile operating systems are secure by design. While security practitioners know this to be false, they still must convince a skeptical management upline - you know, the ones holding the purse strings - of the need. Zero-day exploits, malicious apps, risky user behavior, and phishing attacks are very real threats to the mobile enterprise. Google Project Zero reports that in 2021, **1 of every 3 zero-day attacks targeted iOS and Android devices**; it was 1 in 10 the year prior. App stores have malicious apps uploaded that sneak past the security gatekeepers; a malicious 2FA app was removed from the Google Play Store in Feb 2022, after having been downloaded 10,000 times.⁶⁹ Users jailbreak their devices and sideload apps. Rogue access points positioned in high-traffic areas such as coffee shops intercept traffic. And then, of course, there is the omnipresent specter of phishing (email) and smishing (SMS) attacks.

Mobile threat defense (MTD) is specifically dedicated to threat prevention, detection, and response for mobile devices running on iOS, Android, and even Chrome OS. Most organizations already have a mobile device management (MDM) system in place, but MDM is not security. It is management: administration and basic enforcement. Calling an MDM a security solution is like calling a handyman a plumber: sure, there's a little overlap, but you know who to call when a freeze causes your pipes to burst. An MDM is great for management: track a mobile, lock it, wipe it. In contrast, MTD shields an organization from phishing attacks, malware, and network exploits like man-in-the-middle (MitM) attacks. An MTD and an MDM are complementary solutions, not mutually exclusive.

Securing mobile devices is a vital aspect of any XDR strategy.

Mobile devices are just one of many attack surfaces - user endpoints, cloud workloads, IoT, email, identity, and so on. The nature of XDR is a 3-step, machine-speed process: (1) ingest data from these multiple attack surfaces, (2) automate its analysis and correlation, mining for insights, and (3) prescribe and potentially automate some response action on the insights gathered. There are some powerful reasons to weave an MTD solution into your security stack. **The mere detection alone of an attack on a mobile user, even when successfully blocked by an MTD solution, can prove to be powerful, actionable information to a SOC.**

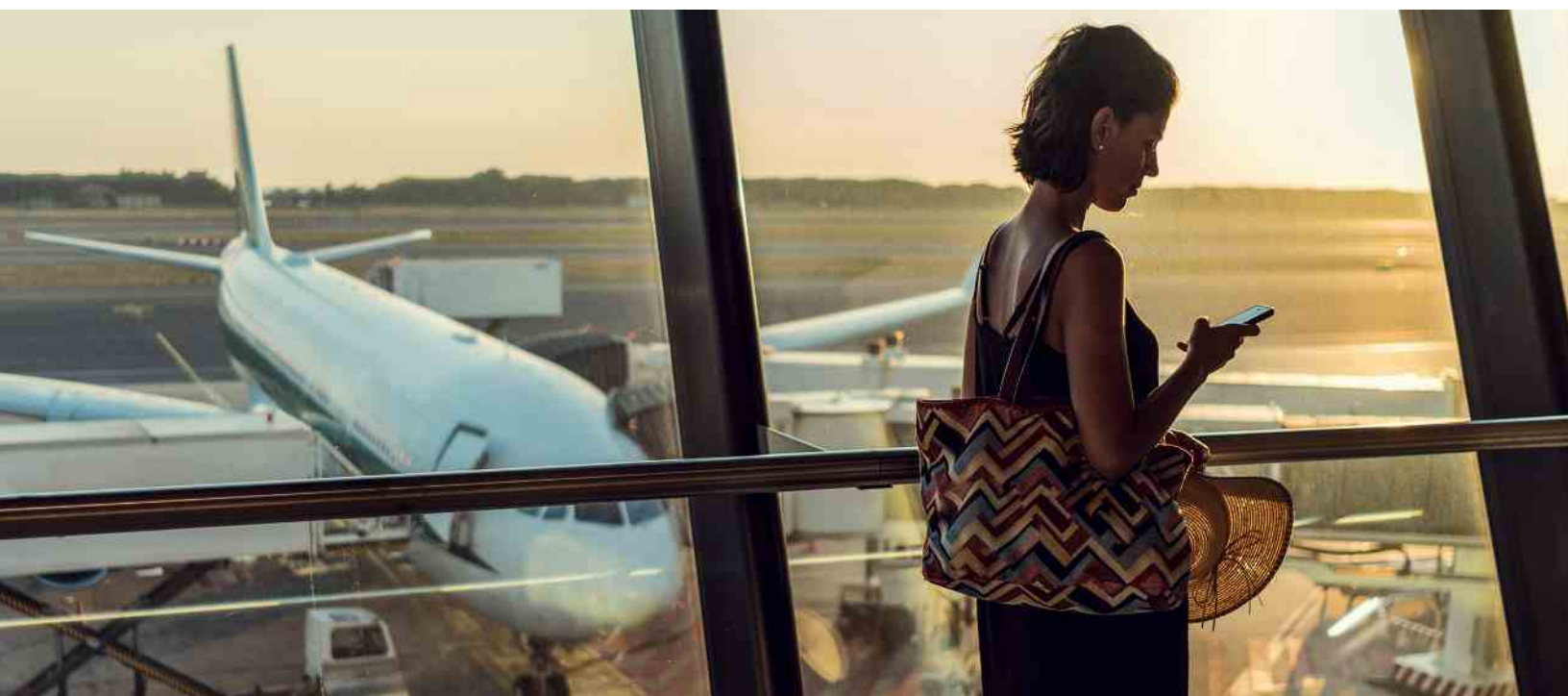
Consider the example of a high-value target, perhaps a CEO, being driven to the airport. She is taking calls and reading emails, one of which comes from a division GM with a link to information requiring her disposition. Of course, it is a carefully engineered spear-phishing attack. With an MTD solution, the attack on her mobile is immediately detected via behavioral AI, stopped, and the SOC alerted. With cross-stack visibility, the attack is immediately traced to a successful phish of the division GM's email. In an XDR world, this confirmation automatically triggers a reset of their email credentials. The SOC then calls the CEO to assure her that not only is she secure, but also they have identified the cause and are on top of the situation, all within the span of 2 minutes... or less. Bigger picture, the SOC is alerted to an active campaign targeting highly positioned executives.



Knowing that a mobile device has malware on it allows us to cut off access, and can also tell the SOC something about user security competency.

A proper XDR model will automatically assign a riskier profile to that user, and might even use a linked entitlements tool to restrict access as much as possible, thereby limiting the risk to the organization. Or it might force more frequent 2FAs on the user until such time as the risk abates, such as by removing the malicious app.

The way an enterprise functions has fundamentally changed, accelerated by the events of the last two years. **With so many employees thriving beyond the corporate perimeter, our security strategies are evolving to meet the challenge of keeping our assets both available and confidential. Mobile threat defense is vital to the success of our cohesive, cross-platform XDR security.**



Establishing Mobile Device Trust in Zero Trust Security Architectures

Loren Russon, Vice President of Product Management, Ping Identity

The pandemic-driven shift of employees to more virtual, mobile work environments has inspired large enterprises to move away from conventional, static, perimeter-based security approaches. This shift has made it more urgent for enterprises to invest in identity-based security capabilities as part of a strategy to implement zero trust security models for their dispersed workforce.

The zero trust security model – based on the principle of *Never Trust; Always Verify* – treats everyone as a potential threat and prevents access to data and resources until verified. The zero trust transformation promises to address new challenges in keeping employees, customers, and operations safe from ever-evolving cyber threats, while also improving compliance and employee productivity. The goal is to deliver a superior online experience for employees and customers, regardless of where work gets done.

But with the rapid proliferation of mobile devices accessing enterprise assets, security teams need better ways to establish more trusted relationships with devices on the network. To ensure employees have secure access to the data they need on the devices they use the most, zero trust must be enabled with advanced mobile threat defense.

That's where the partnership between Ping Identity and Zimperium excels. Our two companies work closely together to enhance zero trust security models by delivering comprehensive mobile risk posture data. The Ping Identity/Zimperium security solution enables large enterprises to establish more trusted relationships with all elements in the network: users, devices, applications, transactions, APIs, etc.



Building Trusted Relationships

Identity is the crucial first step towards building a zero trust architecture, since you can't trust what you can't identify. Identity security is structured around the idea that all users and devices must first be authenticated before they can gain access to sensitive resources or data. This may seem obvious in the current era, but it is a departure in thinking from the security approaches of the past, where users were trusted once they were on the corporate network.

Ping Identity provides the identity-based platform and underlying suite of services that help security teams implement more robust security controls and policies on virtually any user, device, or other element in the network, whether the elements work in any cloud, hybrid, or on-premise environment.

Users, for example, must be intelligently authenticated. They must prove their identities with multiple pieces of evidence, also known as multi-factor authentication (MFA). The combination of factors often breaks down into a piece of evidence that the user knows, such as a password, a device they own, like a smartphone, and perhaps a biometric factor such as facial recognition or fingerprint. Different levels of activities and security risk may require employing different levels of multi-factor authentication.

Solely relying on authenticating users is not sufficient for achieving zero trust. Even properly authenticated users can fall prey to using compromised mobile devices. Authenticating these endpoints is just as critical to establishing effective mobile threat defenses since compromised devices can be exploited by threats like ransomware, spyware, and trojans.

But security for mobile devices is often sacrificed for convenience. Consequently, these mobile endpoints are exposed to increased attack vectors that enterprises have no visibility into, much less the ability to prevent, leaving gaps in their zero trust architecture. And even if a mobile device has been proven not to be tampered with, it could be missing a security patch that could compromise an enterprise's security posture.



Zimperium and Ping Identity work together to enhance mobile device identity management and access controls, bringing all mobile endpoints into a security perimeter. Zimperium provides real-time, on-device, AI-based protection against Android, iOS, and Chromebooks threats. This real-time intelligence, in turn, enhances Ping Identity's platform with greater security visibility, access control, and device security needed to secure both enterprise-owned and mobile endpoints. Security teams can better understand their whole risk posture and strengthen their mobile security protection against device, network, phishing, and malicious app attacks.

The technology continuously monitors devices and delivers clear, actionable alerts that direct security teams on how to resolve security or compliance issues. With the real-time mobile threat detection, notification, and response from Zimperium, security teams using the Ping Identity platform can ensure mobile endpoint coverage is an integral part of their zero trust security posture.

Identity is the new perimeter that enterprises need to secure, and the best way to effectively do that is to leverage a zero trust approach that unifies mobile threat defense with strong authentication.

The integration of Ping Identity's IAM platform with Zimperium will make zero trust implementation easy for security teams to deliver a more seamless and secure user experience.

4.3

The Large and Growing Smartphone Attack Surface

Julian Durand, VP Product Management, Intertrust

The number of internet-connected mobile smartphones has grown rapidly. As they become more essential to our personal and work lives, their technology and applications have become more complex and more connected and, accordingly, more of a target for bad actors. But to best prepare for the threats of today and tomorrow, we must understand smartphone mobile attack surface and explore three key maturity levels of detect, protect, and defend to mitigate attack surface risks.

Worldwide yearly smartphone shipments have grown from 173.5m in 2009 to 1.43 billion forecasted for 2022 with an over 10% compound annual growth rate of 23 years.⁶¹ It would have been even higher had semiconductor supply chains not been adversely affected by the pandemic.

Today the number of internet-connected mobile phones slightly exceeds the world's population of 7.6 billion.

While density varies from the Maldives (246 mobile connections per 100 citizens) to very low ones such as Cuba and North Korea (12 connections per 100), the reality is that mobile phones have become ubiquitous.⁶²



To better understand the cybersecurity threats to these ubiquitous devices, the U.S. National Institute of Standards and Technology (NIST) offers a mobile threat catalog.⁶³ It's a useful framework to enumerate the growth of the attack surface of these systems, especially when considered through the lens of enterprise cyber risk identification and mitigation. As we shall see, the attack surface has been growing non-linearly, perhaps even exponentially, as each element of complexity, the number of connections, and the centrality of these devices to our lives have each exhibited such dramatic growth. Taken together, these represent compound growth as each element exacerbates the next threat level and further expands the overall attack surface associated with enterprise mobility.

The technology stack of a smartphone today starts with the chips providing application and communication performance. For example, Qualcomm's flagship Snapdragon 8 Gen1 gives an idea of what 2022 smartphones will feature. These include a 3 GHz multi-core CPU; a high performance AI engine; a 5G modem clocked at 10 Gbps; a console-class gaming engine; an advanced location module supporting 6 separate multi-constellation Global Navigation Satellite System (GNSS) satellite systems; advanced camera, video, and sensor processing modules and the latest Wi-Fi, Bluetooth, NFC modems all packed into an 4 nm process node.⁶⁴

All this hardware requires firmware to access the power on self-test, initial boot loader, and drivers for each of these technology cores.

A mobile operating system like iOS or Android further builds on the firmware. Android, the world's most popular mobile phone OS by volume, recently released its 11th version. Updating a smartphone requires a download of approximately 2 GB.³⁶ That is a lot of software with any number of new features, each representing a significant complication and potential opportunities for multiple new threats. The size of the OS alone is a significant contributor to the rapidly growing attack surface associated with mobile devices.


And what would a smartphone today be without app downloads?

Apps offer an even wider and much more heterogeneous source of threats since they can be loaded with malware, vulnerabilities to malware, or often both.

A modern smartphone today offers a wide range of connectivity modalities, each of which can offer a bad actor a direct avenue of attack. These include:

- A cellular modem that will connect automatically to a cell tower with the best signal. Rogue stations can be tuned and focused on a victim device to provide the impression that it is the station the phone should connect to.
- Bluetooth has been widely criticized for its security limitations. Bluetooth related attacks include:
 - Bluejacking – sending arbitrary malicious messages to a person's phone
 - Bluesnarfing – theft of information
 - Bluebugging – remote code execution and device take over
- Wi-Fi has several security protocols; most are ineffective and broken. Even when the network layer is secured, a smartphone will often connect to hotspots of dubious trustworthiness in public places such as cafes, hotels, and airports. Even if the link is protected, it is trivial for a hotspot controlled by a bad actor to spy on, intercept and modify communications.





Zero Trust Network Architecture (ZTNA) is one approach, independent of the state of network security, to assure the integrity and privacy of communications. Intertrust offers a ZTNA based solution that brings an end-to-end, mobile device to cloud architecture that enterprises can use to further protect sensitive data.

Smartphones are mobile general purpose computers that are customized with apps. These apps are downloaded from app stores, so if you trust the app store, you generally trust the apps it distributes.

This can be taken to an extreme. The current dispute between the largest game maker in the world versus one of the largest technology companies in the world is an example. Epic Games filed suit against Apple for its control of the Apple smartphone ecosystem, making it impossible for Apple users to use a competing app store. Epic filed suit because they feel Apple's 30% revenue share requirement for apps makes freemium games like Fortnite too expensive. Apple claims the issue is all about cybersecurity, when the truth is far more complicated. But it does point to the essential need for apps to be reviewed and cryptographically signed for integrity and authenticity.

- Enterprises increasingly develop their own apps that they verify themselves and sign cryptographically to ensure the app's integrity and authenticity. Done well, this is a secure way of adding functionality to a company's workforce. Done badly, it represents another vector for attacks.
- In all cases, enterprise-developed apps add yet another fast growing element of the mobile attack surface in the enterprise.



Smartphone as IoT hub

Because smartphones are ubiquitous and have significant hardware cybersecurity features, they are often used to manage IoT devices and networks. Even cars may be turned on and off by your phone.

This convenience is popular with both consumers and enterprises. But, it significantly grows the available attack surface because many IoT devices and networks, especially those used by consumers, do not have the same sophisticated cybersecurity features used in modern smartphones. As such, attackers can take over devices, hubs, and gateways and lay in wait for a vulnerable device to connect. This is how malware that propagated the Mozi botnet spread so rapidly around the world.⁶⁰

Malware like Mozi can lay in wait. When a smartphone with a vulnerability connects to a compromised IoT hub, it will attack. If the smartphone hasn't been updated or employed other defenses, it may well become infected.

Mitigating threats – three phases of security maturity

1. Detecting Threats

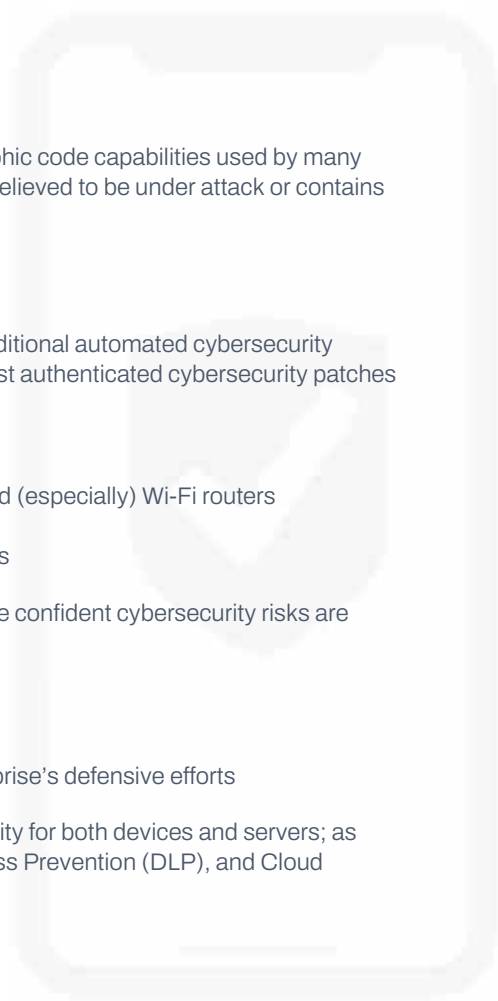
- Monitor a smartphone
- Machine learning detection algorithms are needed because the polymorphic code capabilities used by many malware developers elude signature checkers. Send alerts if a device is believed to be under attack or contains known vulnerabilities

2. Protecting Smartphones

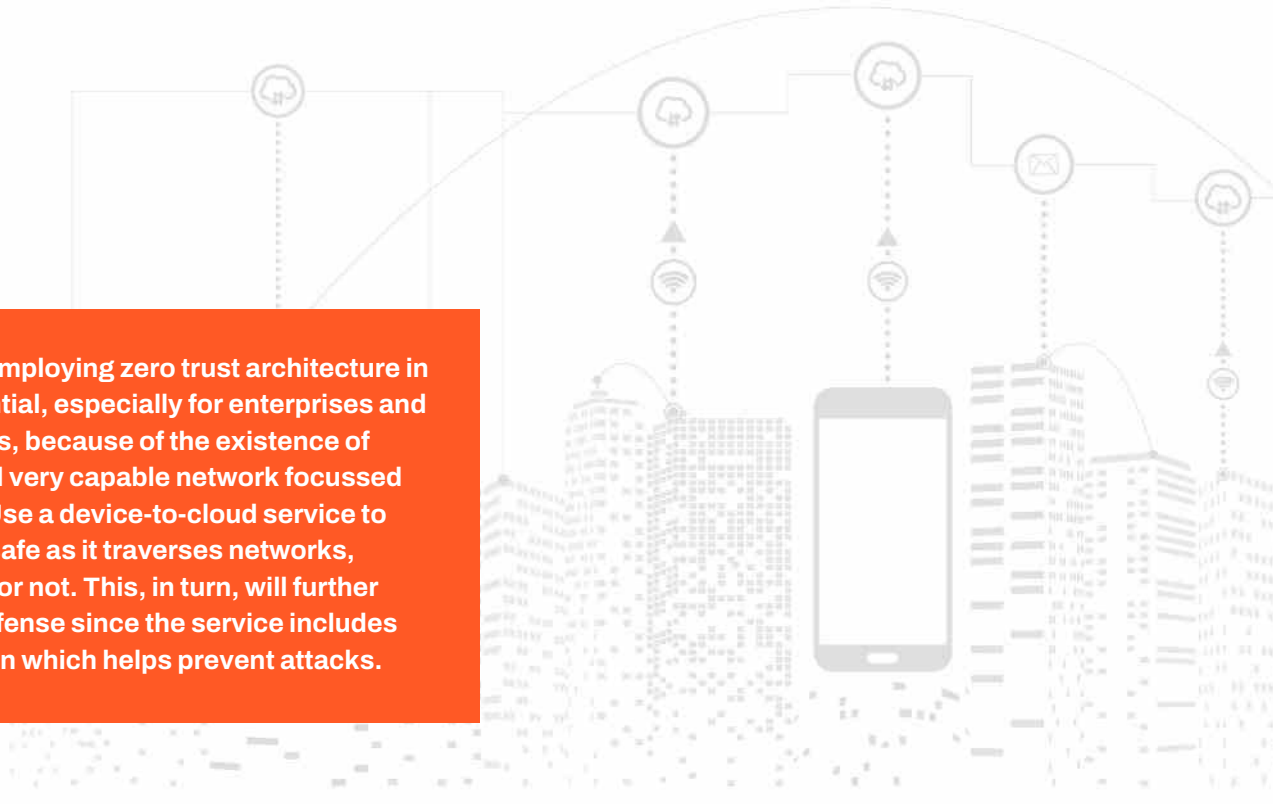
- In addition to capabilities for detecting threats, the device should have additional automated cybersecurity features, for example, automated downloading and application of the latest authenticated cybersecurity patches
- Protections from phishing messages using sand boxing techniques
- On-demand VPN capabilities to protect data from untrusted gateways and (especially) Wi-Fi routers
- Access controls to compartmentalize sensitive information and processes
- For enterprises, it is especially important to scale policy enforcement to be confident cybersecurity risks are properly addressed

3. Defense

- In addition to detection and protection, defense is about scaling an enterprise's defensive efforts
- It includes device-agnostic cybersecurity systems, centralized web security for both devices and servers; as well as tools for unified Identity and Access Management (IAM), Data Loss Prevention (DLP), and Cloud Access Security Broker (CASB)



End-to-End Data Cybersecurity



On top of all these, employing zero trust architecture in the network is essential, especially for enterprises and IoT related use cases, because of the existence of many significant and very capable network focused attack techniques. Use a device-to-cloud service to ensure data is kept safe as it traverses networks, whether it is trusted or not. This, in turn, will further provide a layer of defense since the service includes device authentication which helps prevent attacks.

The growth of mobile hyper-connected computing has brought unprecedented access to inexpensive communications, access to knowledge, and sophisticated computing to most of the world's population. The wide reach and sophistication of these mobile computing platforms has also put us at risk, particularly in enterprises that manage sensitive data. Acknowledging this threat landscape is the first step, and maturing processes to detect, protect and defend ourselves is more important than ever. Fortunately, we have the tools and expertise to both reduce attack surfaces and minimize exposure to risks. But it takes commitment, tools, and a concerted effort that needs to be driven by senior management.

The Increased Risks of Mobile Productivity Tools to Enterprises

JT Keating, SVP of Product Strategy, Zimperium

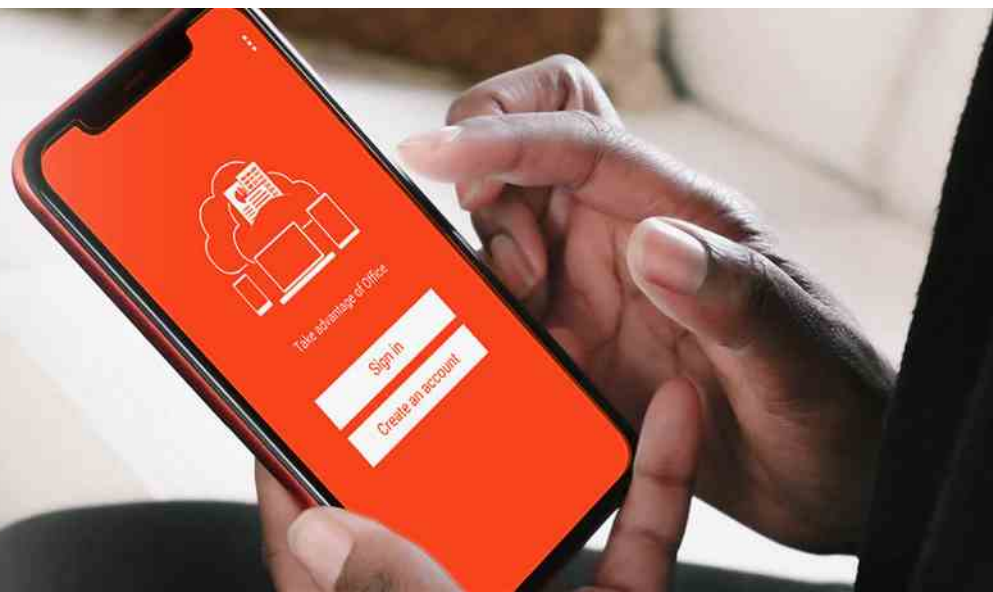
The COVID-19 pandemic sparked a wave of employees working from home, significantly changing the way organizations do business in what is now referred to as “today’s workplace.” At the beginning of the shut down, employees were quickly packing up laptops, monitors, and other devices to begin their new work from home journey. While working from home was seen as added perk prior to 2020, it is now a way of life for most. At the same time, BYOD significantly increased, along with employers enabling the use of productivity tools on personal mobile devices to ensure their distributed workforce had the tools and connectivity they needed to be just as much, or more productive, in their new environment.

Since then, mobile devices have become indispensable productivity tools in today’s modern workplace, providing its users with the same level of access to applications and data that traditional endpoints have had for years. In fact, 84% of the security professionals responding to a recent Zimperium poll said they had enabled Microsoft Office 365 on mobile devices.⁶⁷

84% of security professionals have enabled Microsoft Office 365 on mobile devices.

Enabling the use of productivity tools like Office 365, authorize devices that are approved by an organization to access Office 365 content, such as emails, messages from teams, documents, and more, improving communications and team collaboration. These cloud-based productivity apps allow the remote workforce to finally break away from the desk and be productive on the go. While IT admins use mobile device management (MDM) to have a higher level of control over devices that access apps like Word, Excel, PowerPoint, Outlook, and OneDrive content, the level of access does not come without risk.

If 2020 proved anything, it’s that attackers are taking advantage of the COVID-19 pandemic, and the expansion of a remote workforce. It is no surprise that mobile vulnerabilities have grown 50% since the pandemic. A common vulnerability that various security researchers can agree on is, since the height of the pandemic, BYOD has broadened the attack surface for organizations of all sizes. As teams rushed to set up a remote workforce, some had to prioritize implementing a distributed workforce over securing all BYOD devices, including their own endpoints.



36% of Zimperium’s survey respondents said they had finished implementing security solutions to protect Office 365 on mobile devices, while 38% are still in the process.⁶⁸ Commenting on the disconnect, Eric Green, former global head of mobile security for HSBC, said, **“Since O365 on mobile gives the same depth of access that was once only provided to users on fully secured desktops or laptops, it would be irresponsible not to secure the data on mobile devices too.”**

In today’s threat environment, mobile devices must be equipped to protect against the full spectrum of device, network, phishing, and malicious app risks and attacks.

Protecting the enterprise against mobile attacks involves much more than MDM compliance checks or having to over restrict the device, preventing employees from downloading certain apps. As a result, over restricting the device with additional management policies can be contradictory to improving productivity.

Securing mobile access to Office 365 along with a better end-user experience involves organizations lowering security restrictions with a Mobile Threat Defense solution. MTDs can detect threats, prevent incursions, and provide the essential device risk attestation and scoring features required for Zero Trust and conditional access models.

Despite having to choose between an MDM and MTD, organizations can leverage both to supplement the gaps in coverage, data coverage, and security. Privacy is a major component of securing BYOD that contributes to lower than expected adoption of mobile security, but leveraging both an MDM and MTD allows the enterprise to loosen restrictions. The workforce community is reluctant to give full access to BYOD devices because of trust and the thought of corporate IT teams having access to personal information like photos, phone numbers, and messages.

It would seem prudent to ensure these mobile devices cannot easily be compromised. If a breach occurs, the resulting incident response and recovery efforts can be costly and include significant regulatory penalties if personally identifiable information is exposed.

Few would disagree. Today there is broad industry consensus that mobile devices must be secured. However, the efficacy of these mobile defenses remains to be seen. They will be probed and tested by cybercriminals who correctly perceive mobile devices as the weakest link in the security chain.



5.1

Conclusion

In 2021, the mobile attack surface experienced complex attacks and exploitations, fueled by threat actors exploring the increased attack surface and opportunities the mobile endpoint provides. We witnessed privacy and critical information breaches targeting mobile devices used by everyone from world leaders to journalists, business leaders to private citizens, and more. Globally popular applications were exploited by threat actors, revealing customer data, critical investor information, and more. Spyware, scamware, misconfigurations, and poor security filled the news headlines. In 2022, these mobile exploitations and attacks will continue and increase in number and severity as the reliance upon our mobile devices steadily grows.

The past novelty of mobile data access often overshadowed the need for advanced security measures, but 2021 proved that the mobile security risks to enterprises, governments, and people are higher than ever. The techniques and capabilities behind the threat actors are continuously refined, pulling back the curtain of confidence in the mobile device. Their goals range from but are not limited to financial crimes to data exfiltration, capitalizing on the “lesser” security posture that often exists on mobile systems. With each new vulnerability discovery, threat actors will target more enterprises and critical systems through the exploits. And if the past year’s data points to any definitive takeaway, it is maybe this: no one mobile ecosystem is more secure than the other.

The mobile world grows in complexity, with new apps, features, and capabilities introduced yearly. Still, it is essential to realize that security, like these devices, is a constantly moving target. It is about understanding the risks involved and their potential impact and making a calculated decision with the right tools and resources in place.

With each new technological innovation comes the adoption of new practices, technologies, and workflows into the enterprise. IT and security teams must continuously monitor their growing attack surface, balancing the user experience with a security mindset. Developers need to adopt new security perspectives to protect IP, data, consumers, and employees from increasingly capable threat actors. As devices, data, and employees have gone mobile, so must the advanced security solutions.

As mobile threats continue to evolve and expand, Zimperium remains dedicated to providing the advanced mobile threat defense and mobile application security tools necessary for organizations to stay ahead of the threats. We hope this report and the data herein serves as to inform how your organization tackles the current challenges, as well as the evolving challenges that will undoubtedly arise as we all explore the infinite new use cases for these complex computing devices we refer to as our “phones.”



It is essential for enterprises not to lose sight of the strategic importance of comprehensive mobile security surrounding the devices and applications connected to their critical systems.

Sources

1. Zimperium. (2021). When did your organization actively enable BYOD?. Pulse QA
2. Zimperium. (2021). How many work-specific apps are installed on your mobile device?. Pulse QA
3. Zimperium. (2021). Which technology will be your top priority to invest in next year?. Pulse QA
4. IBM. (2021) Cost of a Data Breach Report 2021. <https://www.ibm.com/security/data-breach>
5. Karta, Y. (2013, January 14). Classifier-based security for computing devices. Google Patents. <https://patents.google.com/patent/US9208323B1/en>
6. Margaritelli, S. (2018, September 7). Detecting malware in mobile applications via static analysis. Google Patents. <https://patents.google.com/patent/US10929532B1/en>
- 7, 15, 20, 29. Zimperium. (2021). Secure Access Practices In North America. Pulse QA
8. Zimperium. (2021). How many work-specific apps are installed on your mobile device?. Pulse QA
9. Zimperium. (2021). When did your organization actively enable BYOD?. Pulse QA
10. Statista. (2021). Number of smartphones sold to end users worldwide from 2007 to 2021. <https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/>
- 11, 12, 13. O'Dea, S. (2021, August 4). Smartphones in the U.S. - Statistics & Facts. Statista. <https://www.statista.com/topics/2711/us-smartphone-market/#dossierKeyfigures>
14. Zimperium. (2021). What's your top endpoint security worry?. Pulse QA
16. Zimperium. (2021). How long does it take your organization to patch impacted endpoints in your enterprise after an emergency or high-priority patch or hotfix that would affect security becomes available?. Pulse QA
17. Zimperium. (2021). How have you shifted your remote work strategy as an organization as a result of cybersecurity incidents in the past year?. Pulse QA
18. Chebyshev, V. (2021, April 28). IT threat evolution Q3 2019. Statistics. Securelist. <https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/>
19. Zimperium. (2021). AI In Cybersecurity. Pulse QA
21. Zimperium. (2021). How would you currently describe your company's cybersecurity strategy?. Pulse QA
22. Zimperium. (2021). Do you agree with this statement? IT teams agree trying to set and enforce corporate policies around cybersecurity is impossible now that the lines between personal and professional lives are so blurred. Pulse QA
23. Zimperium. (2021). Is it right for a company to expect you to use your personal phone number when you work from home? Pulse QA
24. Zimperium. (2021). The majority of smartphone devices in my organization are:. Pulse QA
25. Zimperium. (2021). The majority of tablets in my organization are:. Pulse QA
26. Zimperium. (2021). Which departments/groups within your organization present the biggest risk for insider threats?. Pulse QA
27. Zimperium. (2021). Which of the following areas will receive the greatest investment by the end of the year? Pulse QA
28. Zimperium. (2021). Which of the following category of endpoints represents the weakest security in your organization?. Pulse QA
30. Hunt, S. (2021, December 22). Mobile Security Market 2022. Datamation. <https://www.datamation.com/security/mobile-security-market/>
31. TechJury. (2022) 55+ Jaw Dropping App Usage Statistics in 2022. Techjury. <https://techjury.net/blog/app-usage-statistics/#gref>
32. Statista. (2021). Mobile app revenue worldwide 2017–2025, by segment. <https://www.statista.com/forecasts/1262892/mobile-app-revenue-worldwide-by-segment>
- 33, 36. Curry, D. (2022, January 11). Mobile Payments App Revenue and Usage Statistics (2022). Business of Apps. <https://www.businessofapps.com/data/mobile-payments-app-market/>
34. ReportLinker. (2021). Biometric Authentication and Identification Market - A Global and Regional Analysis: Focus on End User, Function, Product Type, Deployment Model and Country - Analysis and Forecast, 2021–2026. https://www.reportlinker.com/p06178590/Biometric-Authentication-and-Identification-Market-A-Global-and-Regional-Analysis-Focus-on-End-User-Function-Product-Type-Deployment-Model-and-Country-Analysis-and-Forecast.html?utm_source=GNW
35. Ericsson. (2018). 5G estimated to reach 1.5 billion subscriptions in 2024 – Ericsson Mobility Report. Telefonaktiebolaget LM Ericsson. <https://www.ericsson.com/en/press-releases/2018/11/5g-estimated-to-reach-1.5-billion-subscriptions-in-2024-ericsson-mobility-report>
37. FBI. (2021). Internet Crime Complaint Center (IC3) | Cybercriminals Tampering with QR Codes to Steal Victim Funds. <https://www.ic3.gov/Media/Y2022/PSA220118>
38. Mordor Intelligence. (2021). Global Mobile Cloud Market | 2022 - 27 | Industry Share, Size, Growth - Mordor Intelligence. <https://www.mordorintelligence.com/industry-reports/global-mobile-cloud-market-industry>
39. Morrison, S. (2019, December 28). His Amazon Ring doorbell got hacked. Now he's suing. Vox. <https://www.vox.com/recode/2019/12/27/21039517/amazon-ring-hacking-lawsuit>
40. Page, C. (2021, February 11). Slack Urges Users To Reset Passwords After Android Bug Potentially Exposed Credentials. Forbes. <https://www.forbes.com/sites/carlypage/2021/02/11/slack-urges-users-to-reset-passwords-after-android-bug-potentially-exposed-credentials/?sh=64d367cf683c>
41. Abrams, L. (2021, May 27). Klarna mobile app bug let users log into other customers' accounts. BleepingComputer. <https://www.bleepingcomputer.com/news/security/klarna-mobile-app-bug-let-users-log-into-other-customers-accounts/>
42. Sharma, M. (2021, May 20). Android apps put data of 100 million Google Play Store users at risk. TechRadar. <https://www.techradar.com/uk/news/android-apps-put-data-of-100-million-google-play-store-users-at-risk>
43. Newman, L. H. (2021, March 4). Thousands of Android and iOS Apps Leak Data From the Cloud. Wired. <https://www.wired.com/story/ios-android-leaky-apps-cloud/>
- 44, 49, 53. Google Project Zero. (2021). Oday "In the Wild." Google Docs. <https://docs.google.com/spreadsheets/u/1/d/1IkNj0uQwbeC1ZTRxdtuPLClI7mUreoKfSglnSyY/edit#gid=2129022708>
45. Stone, M. (2021, July 14). How we protect users from 0-day attacks. Google. <https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/>
46. Zerodium. (2021). How to Sell Your Zero-Day (0day) Exploit. <http://zerodium.com/program.html>
47. CVE Details. (2021). Google Android : CVE security vulnerabilities, versions and detailed reports. https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224
48. CVE Details. (2021). Apple iPhone OS : CVE security vulnerabilities, versions and detailed reports. https://www.cvedetails.com/product/15558/Apple-Iphone-Os.html?vendor_id=49
50. Verizon. (2021). 2021 Data Breach Investigations Report. Verizon Business. <https://www.verizon.com/business/resources/reports/dbir/>
51. Johnson, J. (2021, September 9). Phishing - statistics & facts. Statista. <https://www.statista.com/topics/8385/phishing/>
52. Apple. (2021) Building a Trusted Ecosystem for Millions of Apps: A threat analysis of sideloading October 2021. https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps_A_Threat_Analysis_of_Sideloading.pdf
54. L. Ceci. (2021). Mobile app usage - Statistics & Facts. Statista. <https://www.statista.com/topics/1002/mobile-app-usage/>
- 55, 56, 57. Zimperium. (2021) - When did your organization actively enable BYOD?. Pulse QA
58. Woolacott, E. (2021, January 4). Fines against banks for data breaches and noncompliance more than doubled in 2020. The Daily Swig | Cybersecurity News and Views. <https://portswigger.net/daily-swig/fines-against-banks-for-data-breaches-and-noncompliance-more-than-doubled-in-2020>
59. Verizon Business. (2021). 2021 Mobile Security Index. <https://www.verizon.com/business/resources/reports/mobile-security-index/>
60. Humphries, M. (2022, January 28). Did You Install This Malicious Android 2FA Authenticator App? PCMag. <https://www.pcmag.com/news/did-you-install-this-malicious-android-2fa-authenticator-app>
61. IDC. (2021). 2021 Smartphone Growth to Reach Its Highest Level Since 2015, According to IDC. https://www.idc.com/getdoc.jsp?containerId=prUS4770921&utm_medium=rss_feed&utm_source=alert&utm_campaign=rss_syndication
62. WikiWand. (2021). List of countries by number of mobile phones in use. https://www.wikiwand.com/en/List_of_countries_by_number_of_mobile_phones_in_use
63. NIST. (2021). Attack Surface - Mobile Threat Catalogue. <https://pages.nist.gov/mobile-threat-catalogue/background/mobile-attack-surface/>
64. Qualcomm. (2022). Snapdragon 8 Gen 1 Mobile Platform. <https://www.qualcomm.com/products/snapdragon-8-gen-1-mobile-platform>
65. Rutnik, M. (2022). When will your phone get the Android 11 update?. Android Authority. <https://www.androidauthority.com/android-11-update-tracker-1155652/>
66. Durand, J. (2021, October 26). The IoT is Breeding Killer Botnets. Device Authenticity and Data Integrity Can Save It | IOT. MyTechMag. <https://iot.mytechmag.com/the-iot-is-breeding-killer-botnets-device-authenticity-and-data-integrity-can-save-it-1336.html>
67. Zimperium. (2021). , Has your organization enabled employees to access Office 365 from mobile endpoints?. Pulse QA
68. Zimperium. (2021). What is your organization's current status for implementing endpoint security to protect O365 on mobile devices?. Pulse QA
69. NIST. (2021b). Glossary | CSRC. <https://csrc.nist.gov/glossary/term/compromise>
70. NIST. (2021b). Glossary | CSRC. <https://csrc.nist.gov/glossary/term/malware>
71. NIST. (2021b). Glossary | CSRC. <https://csrc.nist.gov/glossary/term/mitm>

Glossary of Terms



Known Malicious Network

Locations previously detected with risky networks and attacks. Can include an open Wi-Fi network that presents persistent security risks to devices that connect to it

Device Compromise

A cybersecurity incident where unauthorized access to a device that undermines the endpoint's confidentiality, integrity, or availability. Impacted resources can include manipulation, theft, modification, substitution, or use of sensitive information⁶⁹



Malicious Website

A compromised or malicious website that is part of a phishing or spear-phishing attack chain masquerading as a legitimate or reputable source in an attempt to steal sensitive information, execute an exploit, or sideload malicious applications

Malware

A malicious software or firmware that can be file-based or fileless malware used to perform unauthorized activities on a device to undermine an information system's confidentiality, integrity, or availability. Examples of this malicious code include a virus, worm, Trojan horse, spyware, and adware⁷⁰



MITM

Man in the Middle

An attack that uses insecure networks to intercept and modify data during its transmission between a device and application. MitM can be used to compromise personal information, like login credentials⁷¹

Phishing / Smishing

A widespread social engineering attack vector using authentic-looking assets, such as e-mail, webpages, and text messages, to trick users to reveal critical data or direct them to a fake website that requests information. Spear phishing, or smishing, is a direct-target form of phishing



Rogue Access Point

A wireless access point that has been installed on a network's wired infrastructure without the consent of the network's owner. Often used for various attacks, including denial of service, data theft, and other malware deployment

Scan

Malicious actor is scanning across a network during the reconnaissance phase of an attack to find hosts, identify devices, and collect information for use in subsequent stages of an attack



Traffic Manipulation

A tactic deployed across multiple traffic-based threats, including SSL Stripping, Traffic Tampering, and TLS Downgrade. Malicious actors can use external, forced reductions to traffic security or packet manipulation

6.3

Credits

Contributing Zimperium Writers

Adam Wosotowsky
Asaf Peleg
Esteban Pellegrino
Jon Paterson
JT Keating
Kern Smith
Krishna Vishnubholta
Monique Becenti
Nico Chiaraviglio
Richard Melick
Santiago Rodriguez
Shridhar Mittal
Jessica Vose

Contributing Partner Writers

Julian Durand, VP Product Management, Intertrust
Loren Russon, Vice President of Product Management, Ping Identity
Rick Bosworth, Director of Product Marketing, SentinelOne

A Special Thank You To

Malcolm Harkins, Chief Security & Trust Officer, Epiphany Systems
TK Kellermann, CISM. Head of Cybersecurity Strategy, Networking & Advanced Security

Editors

Eric Block
Jennifer VanAntwerp
Jessica Vose
Karen Walsh
Randy Budde
Richard Melick

Layout and Design

Tom Green
Douglas Kraus

6.4

About Zimperium

Founded upon the premise that mobile security requires an entirely novel approach, Zimperium secures both mobile devices and applications so they can safely and securely access data. A single unified platform protects the endpoint and secures the entire application development cycle with the only on-device, machine learning-based engine. Zimperium provides visibility and protection against known and zero-day threats and attacks across device, network, phishing, and application threat vectors against Android, iOS, and ChromeOS devices. Headquartered in Dallas, Texas, Zimperium is backed by Warburg Pincus, SoftBank, Samsung, Sierra Ventures, and Telstra Ventures.

Find additional information or contact us at [zimperium.com](https://www.zimperium.com).



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/>.