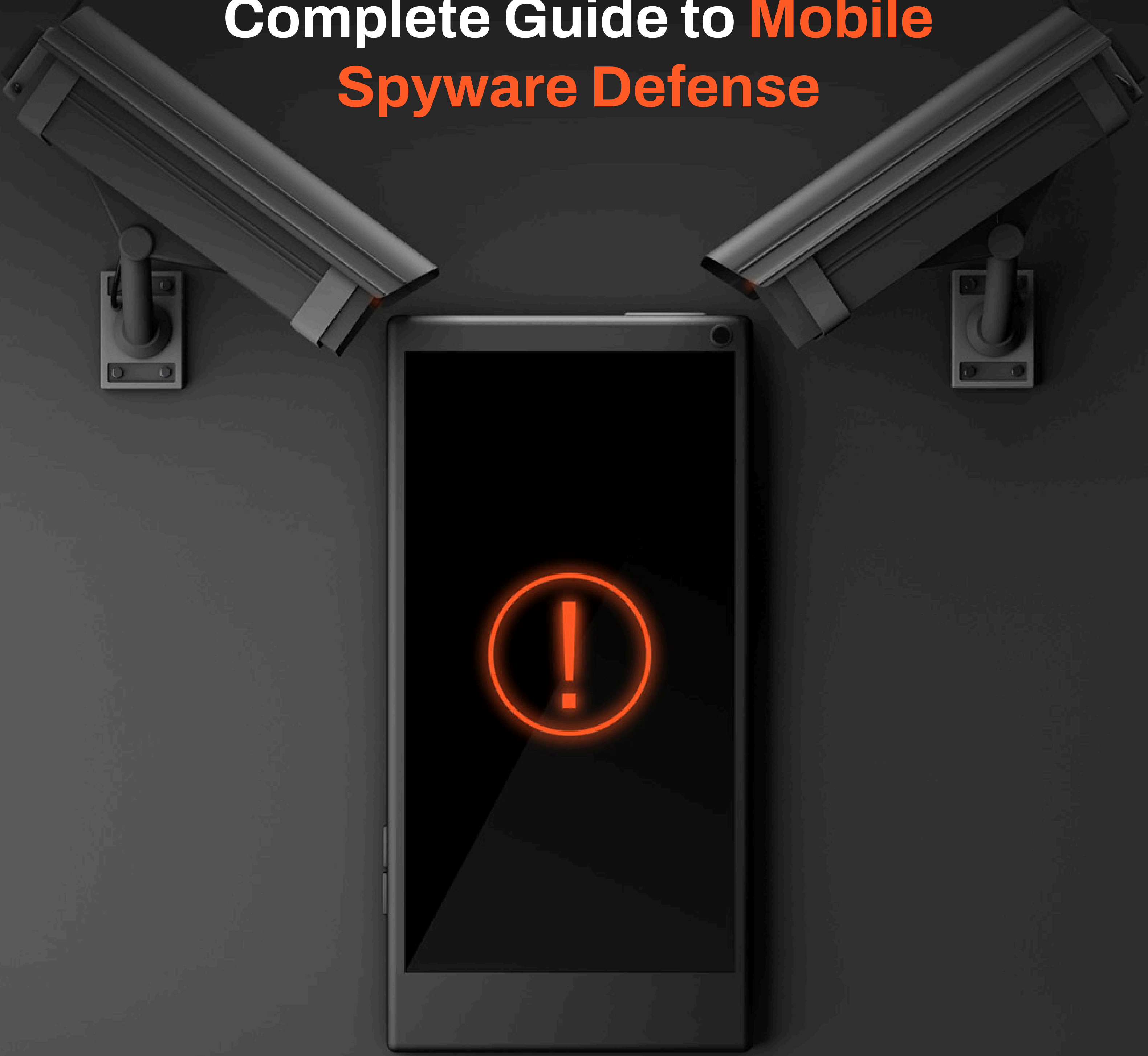
ZIMPERIUM®

Complete Guide to Mobile Spyware Defense



Executive Summary

In recent years, spyware has hit tens of thousands of mobile devices, and in the process, created significant risks to organizations and employees across industries and regions. For government agencies, guarding against these threats is a critical imperative, one that can literally have life-or-death stakes. In this paper we examine spyware and the increasing threat it poses, and explore the key requirements organizations need to meet in order to thwart these attacks.

Introduction: Spyware Definition and Evolution

Evolution

For virtually as long as computers have been able to communicate with each other, techniques have been employed to abuse these connections. Early examples of malicious software emerged back in the 1970's. While early malware was used largely in a malicious way, for example to disrupt or deface a web site, it ultimately came to be used by criminals to make a profit and for nation-states and others to perform acts of surveillance and espionage.

Today, spyware is a big business, with well-established firms selling their wares to the highest bidder. Examples have been uncovered of more than $8,000,000 being paid for a single zero-day exploit. Complete products, easy-to-use spyware kits, and even turnkey spyware services are being sold. Malicious apps and source code are available on the dark web, in source repositories like GitHub, and on online communities like Reddit.

Today, organizations are reaping hundreds of millions of dollars in profits through the sale and use of spyware. As long as the development and employment of spyware remains this lucrative, government organizations, contractors, non-governmental organizations, and enterprises will continue to be targeted.

Spyware Definition

While definitions vary, and nearly infinite permutations have sprung up, here are a few of the key characteristics of spyware:

Hidden or disguised. Fundamentally, victims aren't aware of the spyware's existence—at least not until it's too late. This can be because the spyware was installed without their knowledge or because they were deceived into thinking they were downloading and installing a legitimate, trustworthy application.

Collection. Spyware gathers assets that would otherwise remain private. This can include personally identifiable information, photos, communications, login credentials, and more.

Surveillance. Often, through a combination of malware and tricking users into granting specific permissions, malicious actors gain access to a mobile device's assets or functionality, so they can take pictures, record conversations, access corporate multi-factor authentication services, track specific GPS coordinates, and so on.

Transmission or control. Sensitive assets and control of services are ultimately handed to an unauthorized individual. This can happen via communications with a remote command-and-control server or through a remote attacker gaining direct access and control of a device.

Spyware Examples

Pegasus

Just because malware is detected doesn't mean it's no longer a threat. Pegasus, one of the most notorious examples of spyware, is a prime example of this reality. First detected in 2016, this malware remains very much in play. In 2021, more than 50,000 individuals were victimized, including journalists, activists, and officials within government organizations.[1]

Also in 2021, a previously unknown security flaw in iOS was found to be exploited by Pegasus.[2] This version was distributed via iMessage and was a so-called zero-click exploit, which meant a user didn't even need to click a malicious link to be infected.

Late in 2021, it was announced that U.S. State Department officials were hacked by Pegasus.[3] This underscores that U.S. officials and citizens continue to be targeted and vulnerable to attack.

In 2022, the spyware continued to make headlines. During the year, prominent leaders in Israel and the EU, including Spain's prime minister, were victimized.

PhoneSpy

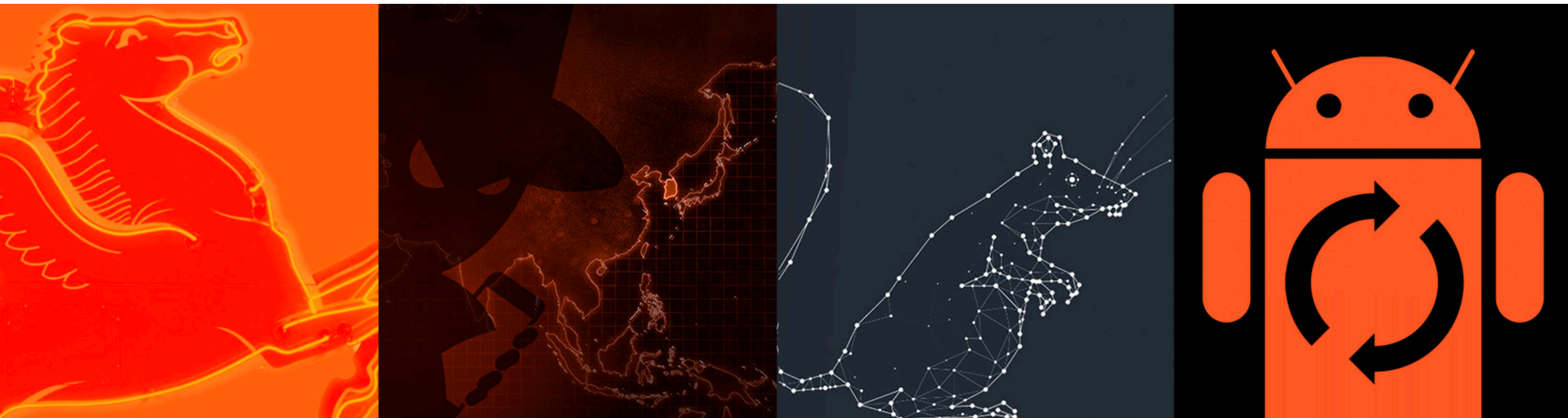
Late in 2021, Zimperium zLabs discovered PhoneSpy. This spyware campaign infected thousands of victims' devices. In all, Zimperium zLabs identified 23 applications, which targeted South Korean citizens.[4] These malicious apps run silently in the background in order to evade detection, but they're designed to spy constantly on victims.

RatMilad

In fall 2022, the Zimperium zLabs team issued a warning about RatMilad, an Android spyware campaign that targeted individuals in the Middle East.[5] The spyware was hidden within a phone number spoofing app, and was distributed under the guise of enabling users to independently verify a social media account. Once users loaded the app, malicious actors could gain control over their mobile devices, including viewing contacts, phone call logs, media, and files. Further, they could also send SMS messages and make phone calls from the device.

Android System Update

This is a sophisticated spyware campaign with complex capabilities.[6] The mobile application functions as a remote access trojan. Once in control, hackers can record audio and phone calls, take photos, access WhatsApp messages, and more.



Understanding the Risks Posed to, and by, Mobile Devices

Mobile Devices Being Targeted—and Proving Vulnerable

Increasingly, spyware is being used to attack mobile devices. Quite simply, mobile devices represent the low-hanging fruit for the threat actors employing spyware today.

While traditional endpoints like laptops and desktops tend to have well-established defenses, that's not the case with mobile devices. Across the board, mobile devices are less likely to be protected by strong security mechanisms. That's especially true for bring your-own-device (BYOD) endpoints, which are increasingly being used by employees to do their jobs. For example, one report found that more than one-third of state and local government employees were using personal devices for work.[7] Not only do these personal devices tend to lack robust defenses, they tend to access a broader range of websites and apps. Consequently, they're often more exposed to spyware than company-owned devices.

The Multi-Faceted Risks of Spyware on Mobile Devices

The problem isn't just that mobile devices are more vulnerable. Successful attacks against these devices can be even more pernicious than an attack against a desktop or laptop. For example, an attacker can employ spyware to gain access to a compromised mobile device's audio recording features. Given many people tend to keep their phones nearby virtually all the time, this means the exposure is far more extensive than a similar attack against a compromised laptop.

The Inspector General's Report: Highlighting the Risks of Mobile Devices

A recent report from the Inspect General underscores the excessive risks posed by the lack of control and visibility over mobile endpoints and apps—even for government-issued devices. The report found that Department of Defense personnel are using unauthorized applications on their government-issued mobile devices.

The report indicated that groups "allow their personnel unrestricted access to public application stores, and DISA's lack of controls over public application stores increase the risk that personnel will download compromised applications that can expose DoD information or introduce malware to DoD systems." [8]

What's worse, the report noted that, while Pentagon personnel downloaded the unauthorized apps in violation of DoD policy, the department "lacked controls over personal use of DoD mobile devices to ensure that personal use was limited, complied with DoD policies and regulations and did not pose operational and cybersecurity threats to the DoD."

Spyware Apps and Apps that Enable Spying: The Blurring Lines

A range of mobile apps can be used as spyware. While some spyware is purely malicious, in other cases, popular, widely used apps have been employed to spy on victims. Ultimately, this has led leaders at both government agencies and enterprises to ban numerous apps.

The Inspector General's report also highlighted how ostensibly benign applications can pose risks. The authors noted that even "seemingly harmless commercial applications" pose a threat to DoD data and related information systems." They detailed how, "Video games, shopping, or weather applications routinely require access to a device's contact list, messaging platforms, location data, or other personal information, and often lack sufficient security or encryption standards.

The Central Risk to Government Agencies: Spyware that Harvests Credentials

The threats posed by mobile spyware may start on the mobile device, but they don't end there. Once attackers compromise an employee's mobile device, they can steal what's on that device, and they can exploit the device to gain access to organizational networks, services, and assets.

In particular, it is the credentials that reside on mobile devices that are often the ultimate target of malicious actors. One study found that, between 2020 and 2021, credential-harvesting attacks against U.S. government employees increased 30%.[9]

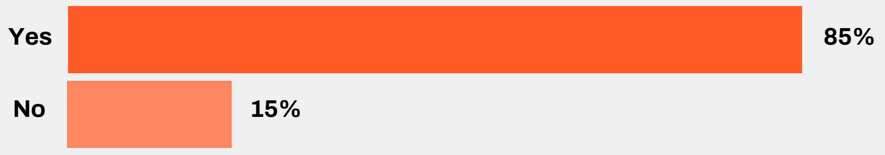
Preparing for the Unknown: Contending with the Rise of Zero-Day Attacks

In recent years, there have been ample examples of spyware being used that exploited previously unknown, or "zero-day" vulnerabilities. Without effective, real-time visibility on mobile devices themselves, too often, these zero-day attacks don't get detected—until it's too late. When you consider that more than one-third of the zero-days discovered specifically targeted mobile devices, this represents a significant exposure, not only to mobile device users, but the organizations they're employed by.[10]

Mobile Spyware Defense: Why the Time is Now

There's growing recognition of the dangers of spyware. A Zimperium survey found 85% of respondents acknowledged that spyware poses a threat to them and their organizations.

Do you think that mobile spyware poses a threat to you, or your organization's enterprise data security?



N - 112 technology leaders
Powered by www.pulse.qa

The reality is that all organizations must be able to establish strong safeguards against mobile spyware. This is particularly true for government agencies: According to Verizon's 2022 Mobile Security Index, 88% of public sector organizations said a mobile security breach could put people's lives at risk.[11]

Issued in February 2023, the Inspector General's report on the DoD's use of mobile applications underscores the severity and urgency of the problem. The report is sure to raise alarm bells, and precipitate the enactment of new policies and controls, not only within the DoD, but across government agencies and the private sector.

NIST Special Publication 800-124 Provides Blueprint for Mobile Device Protection

Government agencies are already expected to adhere to a range of security policies and best practices. For example, it is incumbent upon many security teams to demonstrate adherence to standards documented by the National Institute of Standards and Technology (NIST. For example, NIST Special Publication 800-124 offers guidelines for managing the security of mobile devices in the organization.

The standard details the technologies and strategies that teams can use to guard against evolving threats. The standard offers mobile security guidance in such areas as mobile devices, centralized device management, and endpoint protection technologies, and looks at both organization-provided and BYOD scenarios.

Guidance From the Federal Mobility Group Specifies Requirements for On-Device Security

Chartered under the Federal Chief Information Officers Council, the Federal Mobility Group (FMG works across the federal government to identify challenges and develop and share best practices. In 2022, the FMG issued guidance for employees traveling internationally.

Section 4.1.3, “Install Mobile Threat Defense Software,” specified that, “As an additional countermeasure to detect anomalous behavior in real-time, mobile threat defense (MTD) should be installed on the device.” The guide also indicated that “On-device detection should be used to support the always-on nature of mobile devices.”[12] These defenses represent vital safeguards as organizations look to defend against evolving, zero-day attacks.

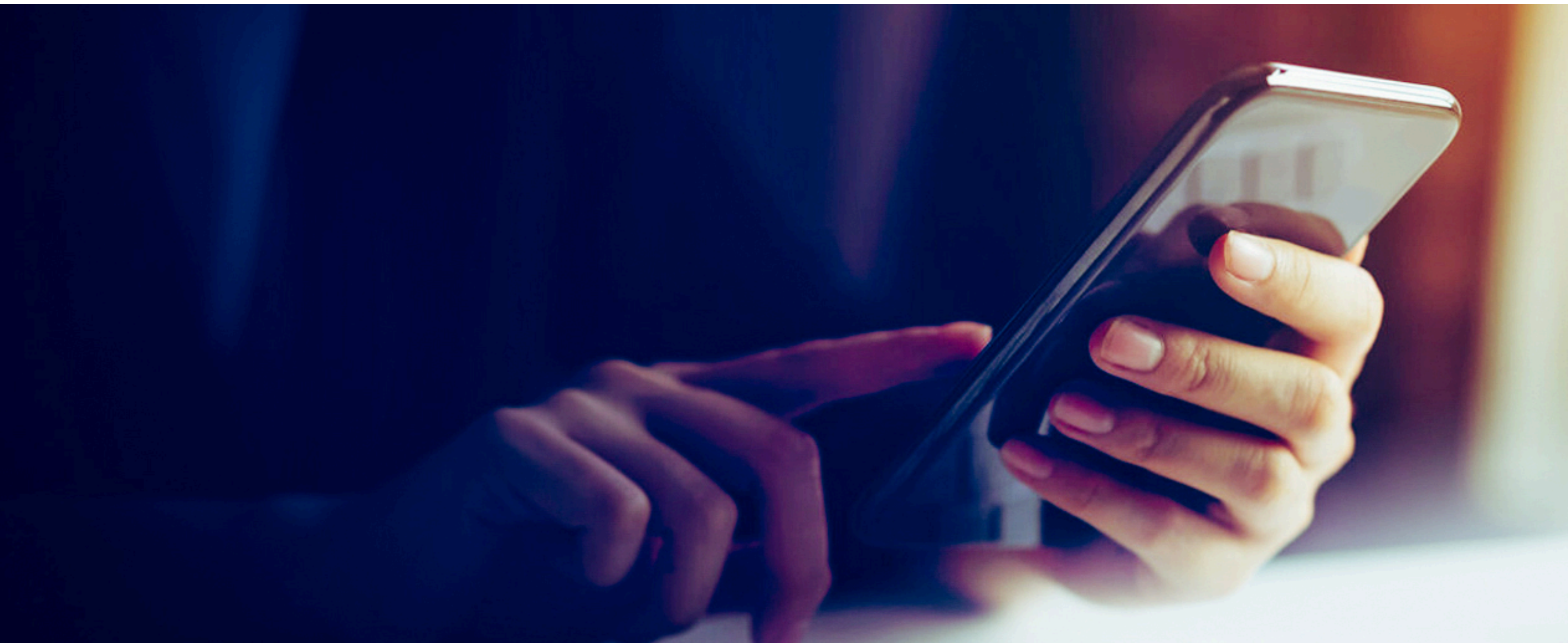
National Defense Authorization Act Intensifies Demand for Spyware Protections

The focus on combating spyware is gaining the increased attention of policy makers. For example, with the most recent National Defense Authorization Act (NDAA, which was signed into law in December 2022, the need to address spyware became an even more urgent imperative for a number of government agencies. Section 6318 of the Intelligence Authorization Act, which was included in the NDAA, specifically requires the implementation of “Measures to mitigate counterintelligence threats from proliferation and use of foreign commercial spyware.”[13]

In addition, the act:

- places guardrails on how U.S. intelligence agencies themselves use commercial spyware.
- requires the FBI, CIA, and NSA to issue a report on the threats posed by spyware.
- requires the Director of National Intelligence to issue best practices for protecting against spyware.

These requirements underscore the severity of the threats posed by spyware, and the criticality of addressing these threats effectively—and immediately. The key question then becomes, how do government organizations and enterprises address the threats posed by spyware targeting mobile devices?



The Requirements

Today, it's clear mobile devices need to be protected, at minimum to the same degree as traditional endpoints, and perhaps even more extensively. It's vital to implement safeguards that detect spyware and prevent it from operating and extracting sensitive information. Teams must also ensure a mobile device's protections stay ahead of evolving, modern-day attacks. Following are two key requirements for gaining holistic safeguards against spyware.

Employing MTD Solutions to Establish On-Device Protections

NIST SP 800-124 and NIST SP 1800-4B discuss the unique security risks that mobile devices pose to an organization's networks and systems. The NIST 800-124 standard specifically recommends the use of MTD solutions to guard against these threats. Delivering continuous, on-device threat detection, MTD can deliver the robust mobile device security that teams need to achieve compliance with regulatory mandates and organizational policies.

NIST 800-124 distinguishes MTD from mobile device management (MDM) and mobile application management (MAM) in section 4.2.3 "Mobile Threat Defense," by outlining the following MTD capabilities:[14]

- Real-time continuous monitoring
- Assessing apps after deployment and during runtime
- Detecting and protecting mobile devices, apps, and end users against attack via wireless network
- Detecting attacks against an app or OS software, such as side-loaded apps
- Detecting and alerting users to unexpected interactions among apps or the use of data on the device

With these capabilities, MTD supplements your MDM and MAM tools, enabling you to take a comprehensive approach to mobile security.

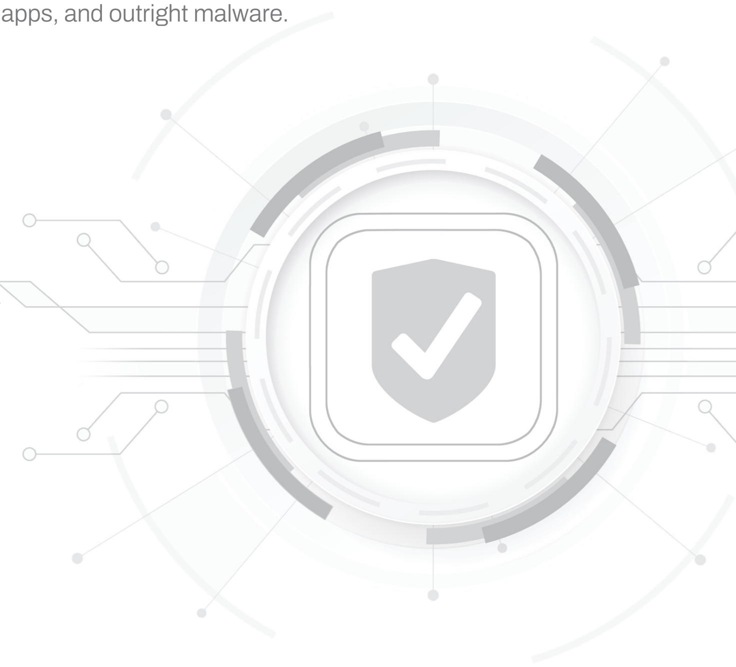
Establishing Mobile App Vetting to Prevent Use of Risky Apps

While it's one thing to ban a mobile app, it's another thing to enforce that ban, particularly in a BYOD world. Further, while bans can be applied to major apps that have been identified as a threat, what about all the other new apps that continue to spring up?

In 2022, Apple's App Store and Google Play had a combination over 4.834 million apps and games in their stores.[15] It's impossible for any security professional to keep up with the volume of new apps potentially entering their environment. That's why it's critical to employ mobile app vetting (MAV) tools that can help distinguish between legitimate and risky apps, and outright malware.

Section 4.3.8 of the NIST SP 800-124 specifically calls for MAV: "MAV tools can be employed to identify vulnerabilities and malicious code in mobile applications."

Teams need to employ MAV technologies that leverage centralized threat intelligence in terms of all the apps available, and that can continuously identify whether an app poses a risk. It is also important for teams to gain capabilities for preventing banned or malicious apps from being accessed on a device. Further, if banned or malicious apps have been installed on a device, teams need a way to spot that and prevent the device from accessing the organization's services. MAV should work together with the MTD agent to identify applications and alert users of conflicts with policy. With an integrated MAV and MTD solution, compliance policy can be implemented to generate alerts on the device when apps are installed. An integrated solution can notify administrators based on specific behavior characteristics if new apps do not conform to Agency policies rather than being dependent on a banned app list.



How Zimperium Can Help

As headlines continue to remind us, organizations of virtually every size and type are being targeted by spyware—and these attacks continue to expose sensitive assets. More than ever, it's critical to establish strong safeguards that protect mobile devices from these threats. This is especially true in the public sector, where the stakes of a device breach can be so severe.

Given this, it's clear teams need to establish robust defenses that are specifically designed for the realities of mobile devices. That's where Zimperium comes in. With Zimperium MTD and MAV solutions, teams can address the massive security gaps currently posed by mobile devices and apps.

Zimperium MTD Solution

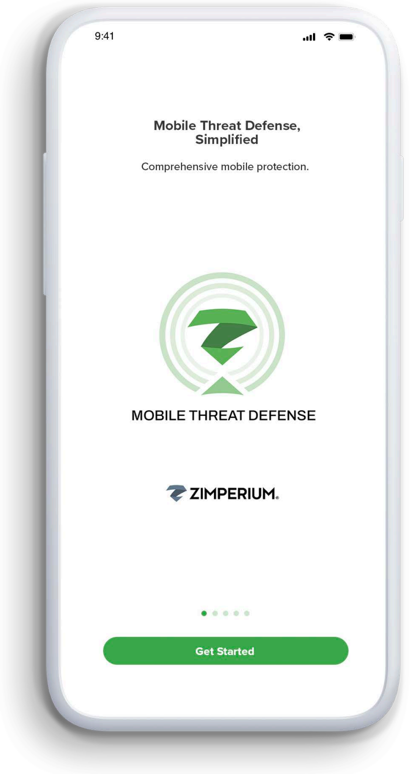
Zimperium Mobile Threat Defense (MTD) - formerly known as zIPS - is an advanced mobile threat defense solution that secures mobile devices, apps, and data—and in the process, it safeguards the resources and services that these devices can access. MTD detects mobile threats, notifies security teams of incidents, and blocks unauthorized access to resources.

MTD is the only on-device mobile threat defense solution that protects Android, iOS, and ChromeOS devices. The solution offers robust safeguards against known and zero-day, advanced persistent threats. MTD keeps mobile devices secure—without relying on cloud-based lookups, content scanning, or other privacy-invasive techniques.

MTD is powered by Zimperium's z9, a dynamically updatable engine. z9 offers behavioral and machine learning techniques that detect device, network, phishing, and mobile application attacks, without having to rely on updates or an active network connection.

Zimperium MAV Solution

Zimperium's Advanced App Analysis (z3A) enables MTD to perform in-depth mobile application scanning for privacy and security risks. z3A continuously monitors and evaluates mobile applications, and then delivers detailed privacy ratings, malware classifications, security ratings, and customizable app privacy settings.



Mobile Threat Defense, Simplified

Comprehensive mobile protection.

Zimperium solutions can help organizations prevent exposure to banned or malicious apps. These solutions support two different approaches:

- Teams can employ MTD and an MDM solution for app identification and access control. Within Zimperium's zConsole, security administrators can flag any banned mobile app as "out of compliance (OOC)" or "deny." This enables MTD to enforce compliance actions locally or through enterprise mobility management (EMM), conditional access controls with mobile access management, or single sign-on (SSO). In this way, if a user installs a banned mobile app, teams can prevent employees from accessing enterprise apps, their device, and SSO. The banned app would need to be removed before the user can regain access.
- Teams can leverage MTD app policies, z3A app analysis capabilities, and content filtering to prevent banned apps from being accessed on a mobile device. Security administrators can leverage z3a app analysis to review a technical report on the mobile app in question and identify its specific domains. Next, the administrator can flag a group of root domains that restrict devices from accessing the banned app, including through a browser or directly through the app.

Conclusion

Mobile devices represent a critical area of exposure for many organizations today. Without strong protections, these devices are susceptible to the increasingly sophisticated and ubiquitous spyware that's being employed to steal money, access, and intelligence. With Zimperium MTD and MAV solutions, your organization can establish robust defenses that effectively guard against these attacks. For more information on how Zimperium solutions can help your organization, contact us today.

Sources

1 Zimperium, "Pegasus Mobile Spyware used to target journalists, activists, and more," July 19, 2021, URL: https://www.zimperium.com/blog/pegasus-mobile-spyware-used-to-target-journalists-activists-and-more/

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

3 Washington Post, "NSO Pegasus spyware used to hack U.S. diplomats' phones," December 3, 2021, URL: https://www.washingtonpost.com/technology/2021/12/03/israel-nso-pegasus-hack-us-diplomats/

4 Zimperium, "PhoneSpy: The App-Based Cyberattack Snooping South Korean Citizens," November 10, 2021, URL: https://www.zimperium.com/blog/phonespy-the-app-based-cyberattack-snooping-south-korean-citizens/

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

6 Zimperium, "New Advanced Android Malware Posing as 'System Update,'" March 26, 2021, URL: https://www.zimperium.com/blog/new-advanced-android-malware-posing-as-system-update/

7 KnowBe4, "Phishing for Feds: Credential-Harvesting Attacks Found in New Study," URL: https://blog.knowbe4.com/phishing-for-feds-credential-harvesting-attacks-found-in-new-study

8 Inspector General, U.S. Department of Defense, "Management Advisory: The DoD's Use of Mobile Applications," February 9, 2023, https://media.defense.gov/2023/Feb/09/2003159201/-1/-1/1/DODIG-2023-041.PDF

9 KnowBe4, "Phishing for Feds: Credential-Harvesting Attacks Found in New Study," URL: https://blog.knowbe4.com/phishing-for-feds-credential-harvesting-attacks-found-in-new-study

10 Zimperium, "2022 Global Mobile Threat Report: Key Insights on the State of Mobile Security," Richard Melick, March 14, 2022, URL: https://www.zimperium.com/blog/global-mobile-threat-report-key-insights/

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

12 Federal Mobility Group, "International Travel Guidance for Government Mobile Devices," January 2022, URL: https://www.cio.gov/assets/files/FMG%20International%20Travel%20Guidance%20-Final.pdf

13 US Congress, "H.R.7776 - James M. Inhofe National Defense Authorization Act for Fiscal Year 2023," December 12, 2022, URL: https://www.congress.gov/bill/117th-congress/house-bill/7776/text

14 NIST, SP 800-124, Rev 2, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," March 2020, URL: https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/draft

15 Business of Apps, https://www.businessofapps.com/data/app-stores/

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244