# The Growing Risks of Spyware and Unvetted Applications

Highlights from a Government Webinar, hosted by ATARC, in partnership with Zimperium, June 2023

As technology continues to accelerate, securing government-issued mobile devices against malicious apps, spyware, and the latest zero-days is critical to national security. When organizations lean on the security of others, sensitive information can quickly be compromised and undermine national security, as evidenced in a recent cyberattack that exploited a vulnerability in the widely used government app, MOVEit.

While agencies are working diligently to understand the impacts of this recent attack, they are continuing to take proactive measures to mitigate risk within a growing attack surface. In a recent webinar discussion hosted by the Advanced Technology Research Center (ATARC) in partnership with Zimperium, cybersecurity experts discussed the evolution and advancement of spyware technology, the challenges agencies face when safeguarding devices, and strategies to address unvetted, unwanted or compromised mobile apps.

## Spyware & Mobile Devices

**"The single biggest risk in an organization is, and always has been, carbon-based life form – human beings make really stupid decisions."**
**- JT Keating, Zimperium**

"The new currency of today is data," said Tim Goodwin, the CIO of the U.S. Patent and Trademark Office. Because mobile devices are constantly with us and access personal and professional data, they're perfectly tailored for spyware and collecting that valuable data. Not only are exploit opportunities growing, but spyware is also becoming more sophisticated and more difficult to detect.

When functioning, spyware is capable of capturing virtually all information contained within a mobile device, including photos, contacts, password keychains, email attachments, and more. Some spyware is also able to take pictures and turn on microphones. While the spyware itself is generally sophisticated, the delivery method isn't always as sophisticated. In the past, we usually saw spyware installed via complex methods from highly organized groups. Now, we're frequently seeing spyware delivered by simply tricking users into installing applications through various social engineering schemes.

## Evolution of Cybersecurity and Spyware

Today it's easier than ever to communicate with one another, but it's also easier for people to initiate scams or impersonate individuals, such as senior executives. Spoofing numbers and phishing emails are becoming more sophisticated with the rise of open-source generative AI, such as Chat GPT. Attackers are quickly becoming more convincing and harder to identify as new technology aids in their ability to change URLs to seem more trusting and to write polished-sounding messages.

**"Emerging research conducted at zlabs, Zimperium's research arm, indicates the average user is six to ten times more likely to click on a phishing link in a SMS text than they are in an email."**

The Solar Winds event shone a spotlight on the role procurement and supply chain management have on cybersecurity in government. Because agencies put so much trust in vendors, sub-vendors, and partners, agencies quickly started reviewing procurement laws and including cybersecurity provisions into contracts to mitigate risks throughout the supply chain.

Compared to ten years ago, agencies are much more cyber-aware today. But as Goodwin notes, agencies must be more proactive at increasing cyber literacy among employees in order to fortify the entire government against threat actors. This involves a significant cultural change to prioritize cybersecurity across all Federal agencies.

# BYOD (Bring Your Own Device)

Organizations, both in the public and private sectors, are challenged by the risks associated with employees using their own devices at work. While BYOD has always been a common workplace occurrence, securing personal devices effectively to reduce risks can be complicated. Agencies are particularly challenged by ensuring the protection of information on personal devices without compromising privacy.

Organizations are working around these challenges by shifting from mobile device management (MDM) to mobile application management (MAM). Instead of managing the personal device, organizations are able to manage access to specific applications. However, device and application management without mobile threat defense (MTD) still falls short to defend against spyware, phishing attempts, device compromises, network attacks, and application risks.

Zimperium Mobile Threat Defense (MTD) is a privacy-first application that provides comprehensive mobile security for organizations. It is designed to protect corporate-owned and/or BYOD from advanced persistent threats, such as spyware, and can be used with an MDM or MAM.

There are benefits to the end user when organizations implement mobile device defense protocols, such as zero-trust conditional access. If spyware were to infiltrate a personal device, it's not just the organizations' information that is at risk.

The BYOD trend will continue, as will the reliance on zero trust to manage device identity and access, but it does not have to stop there. Before providing access to workplace systems, ensuring the device is free of threats, such as spyware and banned applications, is critical to prevent important information from falling into the wrong hands.

# Unintended Consequences of Unvetted Apps

The unintended consequences of downloading an innocuous application, like a simple game, can be significant. Many third-party apps, like social media apps, request unnecessary and excessive privileges to access cameras, photos, emails, and more. Some applications are establishing VPNs outside of the organization, while others are sending traffic to foreign countries. Further, apps can be intentionally malicious and deliver malware, or they can have unintentional security vulnerabilities as a result of third-party SDKs, open-source code or just simple mistakes. Whether intentional or unintentional, organizations get exposed to risks from mobile apps.

Minimizing the risk of unvetted applications is of paramount importance. Controlling which apps are allowed to be installed is one approach agencies can take to minimize risk, but banning just one app may not be effective, as there are multiple versions of that application in existence or copycats on third-party stores. Further, how can organizations ban apps and restrict use at scale?

**"If you have to put your trust in your security into an end user, the game's over. It's too late."**
**- Tim Goodwin, CIO of the US Patent and Trademark Office**

With so many applications constantly being developed, agencies must create policies and enforcement mechanisms to scale compliance. Investing in mobile security that scans applications for vulnerabilities and threats, while providing security teams with a comprehensive report of where data is sent, which countries the app is sharing data with, and known vulnerabilities found in the app, can help reduce the amount of resources required.

When implemented with Mobile Threat Defense, MDM or BYOD programs can provide confidence in the security capabilities of mobile devices. Zimperium MTD can automatically enforce conditional access controls as part of a zero-trust strategy, which prevents the use of enterprise apps and access to sensitive corporate data while these banned apps are installed. App analysis solutions, like Zimperium's z3A technology, can extract data from applications, run the data against security databases and create reports for security teams to analyze and manage mobile app security at scale.

## Best Practices to Minimize Risk

**"If you're not talking about this with your peers, with your leadership, you're way behind the eight ball."**
**- Tim Goodwin, CIO of the US Patent and Trademark Office**

The majority of malware, including spyware, comes from third-party app stores for Android. It is advisable that users only download apps from legitimate sources and avoid third-party app stores. Doing so will significantly lower a user's risk posture. In following Europe's antitrust legislation, if Apple were to allow third-party app stores on iOS in the future, the risk of malware on that platform will likely increase.

Keeping devices up-to-date with the latest OS is especially important to defend against vulnerabilities. While it takes time to develop and deploy patches, Apple recently introduced the Rapid Security Patch, which can help mitigate specific targeted attacks. However, it is not bulletproof. On-device mobile security is critical to ensure targeted attacks and zero-day attacks can be remediated before they become a full-blown outbreak.

Ultimately, agencies should have conversations about mobile security with everyone in their organization. Doing so increases awareness and enables agencies to take more informed, proactive steps to address risks when they arise.

**LEARN MORE ABOUT ZIMPERIUM'S MARKET LEADING SOLUTIONS AT**

**HTTPS://WWW.ZIMPERIUM.COM/**