CHECK POINT™

COMPLETE MOBILE SPYWARE PROTECTION

Scan every app and file type, block phishing, and prevent zero-click attacks, all without disrupting device use

YOU DESERVE THE BEST SECURITY

Contents

Executive summary 3

Introduction 4

Why the Mobile Platform Is a Dangerous Entry Point to Your Organization........ 4

The Attack Modus Operandi 4

The Impact 5

Types of Mobile Spyware 6

Common Types 6

New Forms 6

Nation-Level Spyware 6

Modified Applications........ 7

A Local Police Force Gets Hit 7

Best Practices for Preparedness........ 8

Key Steps 8

Protecting Against Zero-Click Attacks 8

Complete Spyware Protection with Check Point Harmony Mobile 9

Complete Protection 9

Broad Functionality........ 10

Simple Management........ 10

Conclusion........11

Executive summary

Mobile devices are central to how we all work today. But they're also a major source of vulnerability.

Although these devices don't have the requisite cyber protection, employees still use them for business ends, such as sending, receiving, and storing corporate data.

Moreover, users are not as cyber-aware when using mobile devices. And because their screens are small, it's difficult to detect phishing pages and whether certain apps are safe or not, with both of these often serving as the launching pad for spyware.

Threat actors have taken notice, and they're taking advantage of these multiple vulnerabilities. One strategy they use is launching spyware, which is a major threat to the organization, as it is very difficult to prevent, detect, and uproot, without the appropriate preventive measures and tools.

Every single day spyware attacks result in data theft, the spread of malware, blackmail and extortion, banking and financial fraud, and other forms of harm— both to the user and the organization.

No matter what industry you're in, whether enterprise, government, or other, you have digital assets that need to be protected. Failing to protect the mobile endpoint against spyware will leave the door open to threat actors.

In this paper, we'll discuss what spyware does, how it does it, and the damage it causes to organizations. We'll also introduce a recent example of an attack, best practices for preparedness, and how Mobile Harmony from Check Point Software offers complete spyware protection.

Introduction

Why the Mobile Platform Is a Dangerous Entry Point to Your Organization

Employees are increasingly accessing corporate data from their mobile devices. And threat actors know that these devices are the weakest link in the organization's security chain:

- They are **less protected** than other entry points
- Users are **less cyber-aware** when using them.
- Their **small screens** make it difficult to detect malicious links which may lead to a spyware installation.

This means that every single one of these devices is a potential entry point into your organization, making you more vulnerable than ever to malware.

And one type of malware that is particularly damaging is mobile spyware.

The Attack Modus Operandi

What makes spyware so dangerous is that it can collect personal information from a device without the user's knowledge or explicit consent.

Spyware can invade a user's mobile device in one of several ways.

User downloads a malicious app

Malicious apps can be disguised as legitimate apps, making this one of the most common ways that spyware attacks mobile devices. Sometimes the application may appear to be or may actually be legitimate at first. But, with future updates it may contain malicious services.

User clicks a malicious link

This could be a link in an email, text message, or social media post that ultimately causes spyware to be installed on the device without the user's knowledge.

User does nothing

Even if the user does absolutely nothing to download or activate the malware on their device, today's newest "zero-click malware" can infect the device without the user needing to do a thing, just by taking advantage of existing vulnerabilities.

User opens a malicious attachment

Malicious attachments to email or text messages are one of the most common ways spyware is installed on mobile devices. These are usually disguised as legitimate files, such as PDF, Word, or image files. Opening the attachment installs the spyware.

Once threat actors gain access to a user's device with spyware, they can **infiltrate** other personal and corporate devices, and **gain access and control** over components such as microphones and cameras, as well as sensitive information such as user credentials, which may be used to access organizational assets.

Next, they may **exfiltrate** a wide range of potentially sensitive corporate data from your network, such as payment card data, protected health information (PHI), PII, trade secrets, and more.

And they may also **propagate the chain attack** by using the contact information that they harvested, spreading the malware even further.

The Impact

When spyware makes it into a mobile device, it can wreak havoc, for example:

Financial loss due to blackmail on data or credentials that have been stolen

Intellectual property theft as well as that of other sensitive corporate or financial data

Reputation damage, with users, vendors, and employees losing faith and sometimes even filing lawsuits

A launching pad for other attacks through identity and credential theft

Non-compliance fines due to privacy breaches resulting from data leaks

Types of Mobile Spyware

Regardless of how spyware gets into your mobile fleet, the damage will be great. So, it's very important for your security team to be aware of the different ways that threat actors launch these attacks.

Common Types

The most common types of spyware include:

⊗ **Trojans**
malware that masquerades as a legitimate program while concealing malicious functionality

⊗ **Adware**
designed to collect information for marketing purposes or to serve unwanted, deceptive, or malicious advertisements

⊗ **Tracking cookies**
which is accessed by sites to track a user across the Internet

⊗ **System monitors**
for monitoring a user's activities on a computer and sending them to the attacker

New Forms

There are two new types of spyware that have come to the fore – nation-level spyware and modified applications.

Nation-Level Spyware

Nation-level spyware is developed for high-level government users, as well as for other organizations within the government and civil sectors.

There are currently more than 1,000 stalkerware apps[1] that are being used to access users' device cameras, microphones, location, and more, without consent. This provides rival governments and corporations with the ideal platform for conducting espionage[2].

Among the biggest name in spyware are NSO Group's Pegasus, Cytrox's Predator[3], and other open-source spyware[4] that is being used by a growing number of advanced persistent threat (APT) groups.

[1] https://www.theregister.com/2023/02/07/stalkerware_developer_fined/

[2] https://www.cnbc.com/2023/06/21/inside-chinas-spy-war-on-american-corporations.html

[3] https://thehackernews.com/2023/05/predator-android-spyware-researchers.html

[4] https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229

Modified Applications

Another growing spyware threat comes from modified applications. These apps are often disguised as legitimate apps and are downloaded by users without being aware of the imminent risk.

Once installed, modified apps, just like other types of spyware, can steal data, user account details, and credentials, as well as track location, access onboard cameras and microphones, collect contacts, and spread malware. This is a variation of the classic Trojan Horse type of malware, but with a spyware twist.

A Local Police Force Gets Hit

In a recent case, a local police force had received an alert on their Harmony Mobile dashboard that the device of one of their senior officers had been infected with spyware.

After receiving guidance on how to remove it, our investigation was launched. The Check Point team found a previously known spyware named Exaspy on the device. This is a malware-as-a-service, which was developed by cybercriminals for selling on the spyware darknet.

Once installed, the bad actors could have gained access to the officer’s mobile device and manually set extensive permissions and admin rights. And since Expaspy runs independently, disguised as a Google services app, it would have been very hard to detect.

The attacker could have opened the camera and microphone on the officer’s infected device to record calls and capture activity and data from the device screen.

In fact, this spyware gives attackers practically unlimited access to a device and user data. And if users try to uninstall it, they receive a notification that this is an admin app, which often successfully discourages them from removing the malware.

The damage can be severe. Sensitive personal information can be extracted and used to extort the device owner. Attackers can listen in on confidential meetings and use the information to compromise an organization’s initiatives and goals.

But in the case of this local police force, thanks to the anti-spyware protection of Harmony Mobile, the spyware was detected and immediately removed. No damage done.

Best Practices for Preparedness

Spyware can be very difficult to detect without the right measures and tools. This is why the right strategy is very important for mitigating the risk.

Key Steps

Among the key steps to take to help you make sure you ready, are:

✓ **1. Update**

make sure devices have the latest security patches

✓ **2. Authenticate**

by using strong passwords, biometric security, and two-factor authentication

✓ **3. Educate**

employees that they should never install apps from unknown sources, rather only from official stores, such as Google Play or Apple's Apple Store.

✓ **4. Verify**

whether an email or text message is from a known sender before opening

✓ **5. Centralize**

security policies, device usage tracking, and remote device wiping when needed, with a mobile device management (MDM) platform

But the defense initiative can't stop there.

Protecting Against Zero-Click Attacks

There is one more formidable challenge to mobile spyware protection – zero-click spyware.

A zero-click attack takes advantage of vulnerabilities in software to carry out an attack without the user needing to click on a link, open a malicious file, or take any action at all.

This makes zero-click exploits a significant threat. Mitigating the threat requires proactive, preventative actions, such as keeping devices and apps up to date and avoiding unsafe applications, as noted above. But it also requires installing anti-spyware and anti-malware solutions.

That's why the most important step you can take to keep your assets safe is to implement a mobile security solution that, in addition to scanning apps and files for malicious content and blocking phishing attacks, will also defend against zero-click spyware.

Complete Spyware Protection with Check Point Harmony Mobile

Harmony Mobile is the market leading mobile threat defense solution.

It protects corporate data with 360-degree visibility – securing employee mobile devices against all threats and across every attack vector, including applications, files, the network, and operating systems.

It delivers multi-layered protection – before the user is exposed, before the threat reaches the device, and before damage can be done to the organization, even if the spyware has already made it to the device.

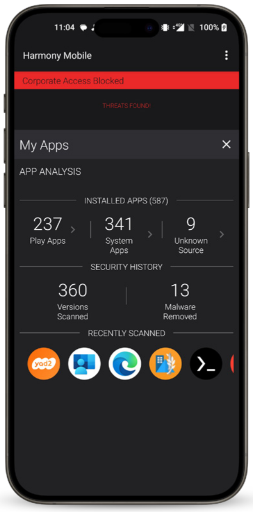
Moreover, Harmony Mobile blocks phishing attacks and zero-click exploits. And it protects the organization by preventing compromised devices from accessing sensitive corporate assets.

Harmony Mobile provides complete protection with broad functionality and simple management.

Complete Protection

Harmony Mobile secures mobile devices across all attack vectors:

- **Apps:** blocking malware by detecting and preventing malicious app downloads in real time.
- **Network**: extending Check Point's industry-leading network security technology to the mobile endpoint.
- **OS and device:** with real-time risk assessments, detecting attacks, vulnerabilities, configuration changes, and advanced rooting and jailbreaking.
- **Files:** detecting and blocking the download of malicious files, regardless of the file type.



Corporate Access Blocked

THREATS FOUND!

My Apps

APP ANALYSIS

INSTALLED APPS (587)

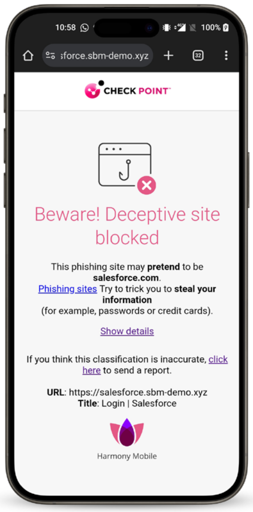
237 Play Apps	341 System Apps	9 Unknown Source

SECURITY HISTORY

360 Versions Scanned	13 Malware Removed

RECENTLY SCANNED

App protection



Beware! Deceptive site blocked

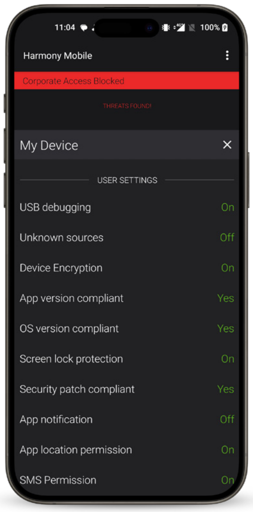
This phishing site may **pretend** to be **salesforce.com**.
Phishing sites Try to trick you to **steal your information**
(for example, passwords or credit cards).

Show details

If you think this classification is inaccurate, click here to send a report.

URL: https://salesforce.sbm-demo.xyz
Title: Login | Salesforce

Network protection



Corporate Access Blocked

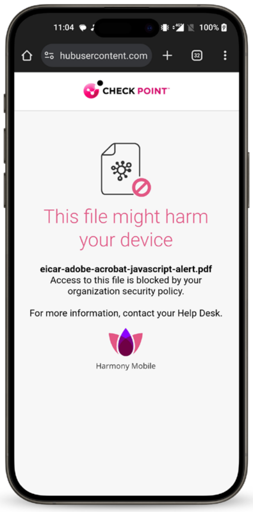
THREATS FOUND!

My Device

USER SETTINGS

USB debugging	On
Unknown sources	Off
Device Encryption	On
App version compliant	Yes
OS version compliant	Yes
Screen lock protection	On
Security patch compliant	Yes
App notification	Off
App location permission	On
SMS Permission	On

OS & device protection



This file might harm your device

eicar-adobe-acrobat-javascript-alert.pdf
Access to this file is blocked by your organization security policy.

For more information, contact your Help Desk.

File protection

Broad Functionality

The extensive mobile threat defense functionality of Harmony Mobile includes:

Command and control (C&C) detection with access to the ThreatCloud AI database of C&C signatures, any communication to or from known bad domains are blocked.

Vulnerability risk management, enabling an administrator to define risk levels based on a device's current OS patch level and whether the OS has known vulnerabilities.

Malicious content blocking by using ThreatCloud AI and Check Point Threat Extraction and Threat Emulation engines to identify and block malicious downloads and to detect malicious content on Android storage.

Rooting/jailbreak detection, enabling administrators to manage the risk of attackers gaining privileged access to protected functionality and control over the applications installed on the phone.

Sideloaded app detection with alerts to unofficial and malicious apps for blocking spyware from infecting a device.

Simple Management

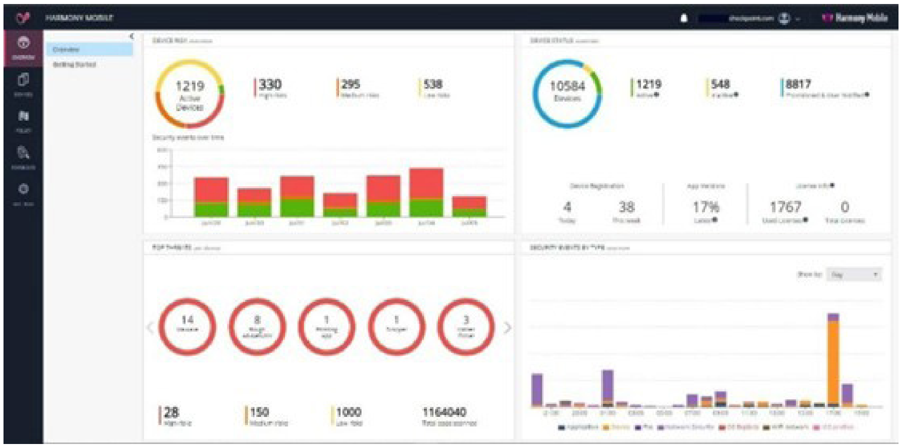
Harmony Mobile integrates with any mobile management solution (MDM/UEM), supports any device-ownership program (BYOD, COPE) and device work settings.

This makes the solution highly scalable, delivering operational and deployment efficiencies for managing mobile security within a broader security infrastructure.

The on-device app installs on the employee's device with a single click and without any interaction, leveraging existing MDM/UEM for zero touch deployment.

And its cloud-based and intuitive management console provides the ability to oversee mobile risk posture and set granular policies.

Harmony Mobile Management Console



Conclusion

Employees today are constantly checking work emails, accessing corporate records, submitting expense reports, sharing documents, and making work-related audio or video calls—all from their mobile devices.

That's why a mobile security solution that lets users get their work done while keeping all your assets safe is critical for robust security.

Check Point Harmony Mobile keeps your organization safe against evolving and ever more sophisticated spyware threats without slowing users down.

It protects corporate data with 360-degree visibility, delivers multi-layered protection, blocks phishing attacks and zero-click exploits, and prevents access to corporate assets even when a mobile device has been compromised. This is what complete anti-spyware protection is all about.

Harmony
Mobile

unique capabilities

Blocks
phishing, spear phishing, whaling, zero-phishing, smishing (SMS/text phishing)

Prevents
zero-click attacks

Provides
any file protection, including PDFs, Microsoft Office files, executables

Integrates
with leading UEMs, SIEMs, logging and reporting tools, and more

Simplifies
with zero touch deployment

Streamlines
with one-click integration

To learn more about how Check Point can help you ensure complete anti-spyware mobile protection, we invite you to start a free trial of Harmony Mobile today.

You can also request our experts to run a spyware check on your device with a full report free of charge.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com