network solutions®

Your Guide to Mobile Device Security

WWW.NETWORKSOLUTIONS.COM

Introduction

Keeping your mobile phone safe from hackers can be challenging. Bad actors have countless opportunities to take control of your phone without your knowledge and invade your business networks. Mobile-based malware is a particularly tempting option for hackers because it broadens the attack surface area and can exploit the many vulnerabilities inherent in smartphones. As corporate users become more comfortable using their phones, they can unwittingly bring these vulnerabilities inside a corporate network. Not helping matters is the fact that users often aren't paying attention when reading emails on mobile devices, which makes clicking on a phishing lure more likely. Plus, many mobile apps have limited or no inherent security, and the apps are constantly updated, making it hard for users to keep current.

This means that mobile app consumers are caught between two difficult positions. On the one hand, they want more usable mobile apps. But they also want to keep themselves secure. This leaves the app creators to choose between adding features or adding security. And these choices place a bigger burden on users — especially those from smaller organizations with less sophisticated IT departments — to vet their apps and maintain a more secure mobile device on their own.

Let's explore some of the cyber threats that can turn your phone into a recording or hacking device along with ways to protect yourself and your business.

Contents

Chapter 1

Malware Targets You and Your Device

Mobile malware efforts aren't new. Sophos has been tracking them for more than a decade.[1] Let's review a few key attack methods and some of the more memorable circumstances.

Mobile malware falls under four different types of attacks:

- **Fake applications**, where malware tricks users into installing an app that does something malicious while looking benign.
- **Phone-based attacks**, where attackers leverage some aspects of a cellular phone network to take control of a user's phone and account.
- **Man-in-the-middle**, where the malware inserts a malicious piece of code between the mobile user's intended application and assumed destination.
- **Spyware or monitoring applications**, where malware inserts a hidden piece of code that records keystrokes and other user movements and then transmits them to a central place, where this data is then sold on the black market.

All of these techniques rely on several factors. First, since many people own smartphones, malware creators can target users who own their own phones and don't have them managed by an IT department. Second, users often respond quickly to suggestive emails or texts, and these can contain phishing lures or other malware-laced URLs that can end up infecting the phone. Finally, there are many phones that aren't patched or running the latest operating system update, and the attackers can quickly find these outdated models and exploit them.

Let's start off with fake apps. These can take several forms:

- **The apps themselves are fake** and contain malware, which could be anything from

ransomware to spyware. One class of malware is called "**fake anti-virus**." These are apps that look like they are protecting you against infections but are actually malware themselves. The creators of these malicious apps count on the fact that many users will just click on a tempting offer and download the app without ever giving it a second thought. Few users do any vetting or research to find out if these apps[2] are legitimate. The Google Play and Apple iTunes stores are full of these apps, despite attempts by both companies to continually clear them from their online listings.

- Another type of fake app contains malware **hidden within legitimate-looking products**, such as games for kids and back-up products. How about a flashlight app that requires access to your photos?[3] The world of mobile malware is sketchy, to say the least.
- The apps **disguise some other malicious activity**, such as banking trojans designed to steal money from your bank or Bitcoin accounts. Or they contain code that causes ad click fraud, by activating a series of automated clicks to increase a criminal's ad commissions.

Why is this important? There are two main reasons. First, **some adware (as these apps are usually called) can steal sensitive information**, such as passwords and account data. An example of this is the adware app CopyCat,[4] which operated during 2016-2017 and eventually found its way onto more than 14 million Android devices, stealing $1.5 million in ad revenue over a period of two months. This is a good example of malware that packs a punch: in addition to the click fraud, it also can take complete control over a device so it can

Malware Targets You and Your Device

launch any app without the user's knowledge or permission.

Second, they can damage devices further and allow additional attacks without the user's knowledge, even causing a device to **become part of a botnet**. This collection of devices is then used to attack other devices on your internal business network or coordinated across the world for some major global attack. For example, the DressCode malware was popular back in 2016, but resurfaced at various times since then[5] with new infrastructure and updated code. These fresh instances would be posted on the Google Play store and disguised as new apps. The malware creators used this method to evade detection with more sophisticated methods that hid the command and control servers used to generate the click fraud commands. One method was to hide the code inside images. These newer DressCode versions were found on Android phones in 70 different countries and on thousands of devices.

Another botnet-type attack was the WireX attacks during 2017, which used 300 different disguised apps downloaded by tens of thousands of users located in more than 100 countries. These apps — which included fake media players, ringtone generators and storage managers — created a gigantic botnet that was used to perform denial-of-service attacks.

So far, we have discussed mainly Android malware. **Apple's devices aren't immune to these types of attacks**, although the company does a better job of policing potential problems. One issue with fake apps happened in 2015 when Chinese app developers introduced an infected version of Apple's app development environment called XcodeGhost. It injected malware code into thousands of different apps that were quickly discovered by researchers[6] and then removed from the iTunes App Store. Another series of iOS-related attacks involved to do with sending malicious texts that can crash devices: this has happened several times.[7]

The second broad type of attack uses various weaknesses in the cellular phone system and the people that operate their customer support lines. These include a variety of techniques and are very hard to prevent, mainly because they don't really rely on malware *per se*. Some of these techniques include:

- **Smishing**, whereby an attacker sends an SMS text to a cellular phone user and tricks them into downloading a piece of malware code. (The name comes from using SMS to send the phishing lure.)

- **Signaling System 7-based attacks**.[8] These are based on the underlying network protocols used to run the phone system. All that is needed is the target user's phone number, and the attacker can listen to their phone calls, read their texts and track their location.

- A different kind of attack exploits what is called **WAP billing**.[9] This is a form of mobile payment where a user's mobile phone bill is charged directly by an app so there is no need to use a credit card or bank account. A user is sent a phishing lure that directs them to an innocent-looking web page, where they enter their phone number.

- Another kind of attack involves using social engineering to manipulate the customer service representatives of the cellular providers. The attacker gets the phone company to reassign a target user's phone number to their own phone, and then they take control over the user's accounts. There have been numerous accounts of these attacks and how users have had their phones compromised when the cellular provider is tricked. This has occurred particularly with users who own a lot of virtual currencies[10] and manage these accounts from mobile apps on their phones. More recently, Brian Krebs has documented an interesting scam[11] whereby two hackers coordinate calls: one calls the intended victim pretending to be their bank while the other calls the bank pretending to be their customer. They both use caller ID spoofing technologies to hide their true identities.

Malware Targets You and Your Device

Next are **MITM attacks**. These are harder to track because the changes to any app on your phone are very subtle. Instead of connecting to your bank's website, for example, you might end up going to a phishing or copycat site that appears to be your bank. A popular MITM method is to take advantage of cross-site scripting, where an attacker injects malicious code into a web page, thanks to credential theft allowing access to its code. While this isn't strictly a mobile-only attack, mobile browser users can easily be affected by it because of their smaller screens and tendencies while mobile browsing. These attacks usually result in stolen user credentials with more dire consequences. Back in 2017, security researchers identified more than 70 apps[12] in the iTunes Store that were vulnerable to MITM attacks, with many of them leaving sensitive data exposed to be harvested by hackers.

Another MITM example was the BlueBorne[13] attack. It used a series of vulnerabilities to connect to another device running Bluetooth protocols. This isn't strictly a mobile malware example; in fact, this attack could infect anything running Bluetooth, including home control devices such as Google Home and Amazon Echo as well as ordinary PCs and laptops. What made this attack particularly dangerous was the fact that it didn't require any user interaction or device configuration. An attacker could gain remote control over user devices as a result, and numerous vendors had to patch their operating systems accordingly.

The final category of attacks is spyware, where an app is used to record all sorts of private information and then send it back to a central repository. That data is then sold on the black market to criminals who use it for credit card and other financial fraud. One of the worst examples of this kind of attack happened in 2016, with the Android BLU (the acronym stands for Bold Like Us) phones sold by Amazon and Walmart. The phones inadvertently contained malware that recorded user data and sent it to Chinese hackers.

After a series of technical missteps and legal challenges, the company finally settled with the U.S. Federal Trade Commission.[14] A more current piece of Android-based malware is called Eventbot,[15] which was discovered in March 2020. It is a combination of banking Trojan, fake app and spyware, which can be very potent. It leverages the accessibility services to bypass SMS-based authentications to steal your login credentials. It has targeted over 200 different banking and cryptocurrency apps.

> "...much of the de facto security of a company comes from having people who are making good decisions when they're using computers."
>
> — Dan Woods, Early Adopter Research

Chapter 2

Using Personal Phones Doesn't Safeguard Your Network

Faced with all of these mobile threats, enterprise IT managers have not been standing still. Several years ago, one IT initiative was created to stem the mobile malware tide: the bring your own device (BYOD) movement.

While it has since fallen out of favor, BYOD was all the rage in 2013-2015,[16] when corporations thought they could control how users purchased and used their smartphones. It didn't work for any number of reasons: first, users would buy whatever personal phones they wanted, whether an IT department supported them or not. Second, the corporate-owned phones were often so locked down that users couldn't get their work done, or had to carry around two phones, a major inconvenience. Understanding BYOD's implications was often difficult for businesses because it meant they had to define what was and what wasn't an acceptable use of their phones,[17] along with what corporate servers and services could be securely accessed from each device.

There were a variety of efforts created to help manage the mobile device portfolios that resulted from the BYOD effort to try to make mobile users more secure. Let's review them, based on three different metrics: their inherent security, their ability to display typical Microsoft Office files across mobile and desktops with a degree of fidelity and what types of software are run on the mobile clients. We categorize these technologies into two broad groups: those that forced poor results because of particular compromises, and those that are better solutions.

There were a variety of efforts created to help manage the mobile device portfolios that resulted from the BYOD effort to try to make mobile users more secure. Let's review them, based on three different metrics: their inherent security, their ability to display typical Microsoft Office files across mobile and desktops with a degree of fidelity and what types of software are run on the mobile clients. We categorize these technologies into two broad groups: those that force poor results because of particular compromises and those that are better solutions.

Examples of ways around BYOD include:

- Emailing yourself a document to your mobile device as an attachment
- Using a cloud-based storage option such as Dropbox or One Drive and a mobile client
- Uploading the documents to cloud-based office services such as Google Docs or Office 365
- Using a virtual private network secure file transfer app or remote desktop or virtual desktop app on your smartphone
- Using a mobile device manager or a pupose-built mobile security app
- Using a secure file transfer application

> ...it's impossible to hide the fact that you are under Distribution Denial of Serivce (DDoS) attack.
>
> — Jamie Cochran, Cloudflare

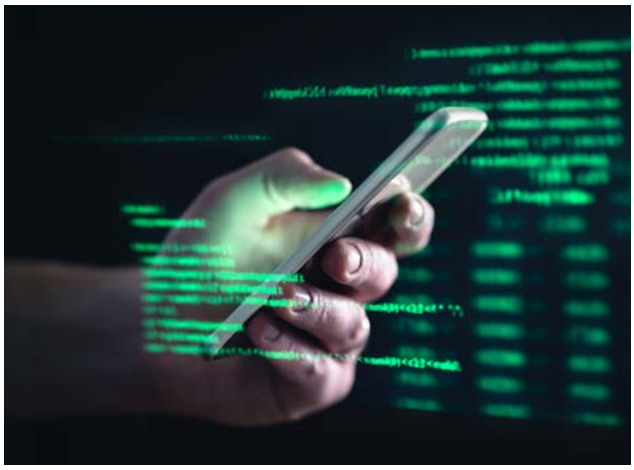
Using Personal Phones Doesn't Safeguard Your Network

COMPARISON OF SOLUTIONS:

Solution	Security	File Fidelity	Client Versions
Group 1—Poor Compromises			
Send an Email Attachment to Your Mobile Device	Poor	Fair	N/A
Cloud-Based Storage	Poor	Fair	iOS and Android
Cloud-Based Office Apps	Poor	Good	Browser-based
Run a Native Mobile Office App	Poor	Fair	iOS and Android
VPN	Varies	Uncertain	Varies
Group 2 – Better Solutions			
Secure File Transfer	Excellent	Excellent	iOS and Android
Remote or Virtual Desktop	Excellent	Excellent	iOS and Android
Complete MDM solution	Excellent	Excellent	Varies
Mobile-based security app	Excellent	Excellent	iOS and Android

Malware-Infected Apps Could Access Your Network

To try to get around some of these issues with BYOD policies, many corporations began using virtual private networks (VPNs). These tools have been in place for decades and mostly for laptop users, but the growth in smartphones — and smartphone attacks — have made VPNs the first



piece of protective gear for many businesses, even smaller ones that don't have large IT departments.

The concept of a VPN is that you avoid exposing your network traffic to and from your phone across the Internet by using encryption. That is essential when users are on a public WiFi hotspot, such as at a local library or coffee shop, where someone on that network might be listening in to your digital conversations. There are a number of VPN providers that offer iOS/Android and Windows/macOS software to make it easier for users to protect all of their mobile devices.

But VPNs can provide a false sense of security, particularly for mobile users. They often expose too much of the network to too many applications on the mobile device and require excessive bandwidth to work across poor mobile connections. The typical VPN also assumes that all apps on your mobile device are well behaved. Once you open a VPN connection, every app can have full access to your corporate network, including rogue applications that may have been deposited on your device by a malware attack. The role a VPN plays is somewhat different on a mobile device than on a desktop because so many different communications technologies are packed into the typical mobile device: voice and video calls, instant messaging, text messages and email. These communications tools make it difficult for any solution to offer universal protection.

Another early problem for VPNs was that many of the VPN vendors didn't support both iOS and Android devices, and only designed them for desktop operating systems like Windows and macOS. That changed as more users flocked to their mobile devices and requested better protection.

> "Everybody I know in the cryptocurrency space has gotten their phone number stolen."
>
> — Joby Weeks, a Bitcoin Entrepreneur

Enterprise Solutions Often Don't Fit Small Businesses

The original idea behind MDM was based on the idea that managing and administering an organization's mobile devices could make them more secure. That meant that IT departments had to decide on a series of policies that would actually improve security. Unfortunately, that didn't happen, and MDM often made user's phones more difficult without any security benefits to the business.

Many MDM products were created in its early years, including Airwatch (which was purchased by VMware and incorporated into its Workspace One product), MobileIron (which has a number of mobile threat protection products now besides its MDM) and Blackberry (which went from an early mobile smartphone vendor to a security software company). These are still large-scale and expensive enterprise IT solutions.

MDM was a good idea in theory; it tried to use a software layer to handle mobile exploits. However, several challenges eventually torpedoed the effort:

- **What controls need to be in place for MDM to be successful?** IT managers had to walk a narrow line when managing apps, devices, users and files. The problem is that no matter how good the MDM product is, nothing will stop a user from using an insecure app to send personal data to their phone's storage.

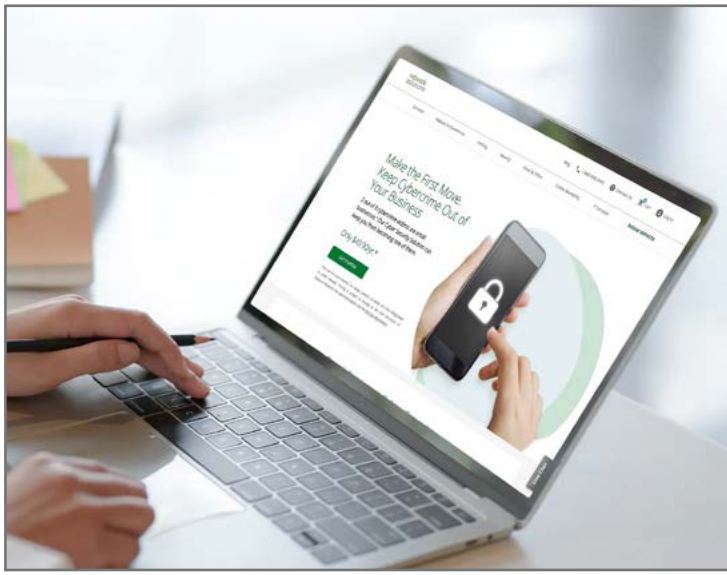
- **How is personal data managed on mobile devices?** Many MDM tools made it difficult to manage data, and these controls made users stop using their corporate-owned devices as a result.

- **What workflows did MDMs require?** The workflows to map and manage mobile devices were complex and required a lot of IT handholding to make it all work. This put MDMs out of the reach of small businesses. The management overhead of tracking device and app-specific policies was also immense.

- **What apps can the MDM manage?** One big failure of MDMs was that they needed to be carefully configured for each specific mobile app. That left a usability gap between the apps that users wanted to use and those that were protected by the MDM.

- **Finally, what killed off MDMs were the newer iOS and Android versions themselves.** Apple started adding MDM features to iOS v.7, such as per-app usage of virtual private net works, single sign-on support and selective message blocking. Android devices have had them included for several years as well.

> "BYOD means my phone, my tablet, my pictures, my music. It's all about the user."
>
> — Eric Maiwald, Gartner analyst



Chapter 5

New Technology Detects and Blocks Malware

These limitations of both VPNs and MDMs don't mean that they aren't useful protective technologies: on the contrary, they still form the backbone of protection used by many business networks to secure remote and mobile devices. But in the past several years, the focus has shifted to a series of new tools. The first is a new class of products specifically designed to reside on the device itself.

Cyber Security Solution from Network Solutions is one such product.

These solutions take the form of iOS or Android apps that fit in between an MDM and a security event analyzer that is used on the network level. They typically use a web interface to manage your entire mobile collection. You will still need an actual MDM if you want to whitelist your custom applications, provide segregated work and personal environments, remediate any malware on your device and control network access. Many of the above apps integrate with MDMs for this purpose.

These apps have other features that are looking at the behavior of potential malware:

- Running your device's apps through a "sandbox" or a protected environment to analyze whether it exhibits any suspicious behaviors.
- Advanced code flow analysis to look for evasive maneuvers or specific malware clues such as MITM attacks.
- Reputation management and the ability to gather threat intelligence about what is running on your device.

A Better DNS

In addition to using one of the above tools, another defensive technology is to substitute a different domain name server (DNS) entry. This is one of the easiest and simplest ways to protect your mobile device. The DNS is the Internet's phone book; it allows you to look up a URL and other resources by using names rather than the Internet Protocol numbers. In the overall Internet infrastructure, there are a variety of public, semi-public and private providers who maintain the "master" series of phone books, known as DNS root servers.

Normally, when you set up your mobile device, you don't give your DNS settings a second thought. Usually, these settings are filled in for you by your device's operating system. But there are a number of alternate DNS entries that offer certain benefits, such as the ability to block spam, filter content (such as adult sites) and malware and allow for speedier performance with those lookups. There are numerous companies that now offer these DNS alternatives, many of which are freely available:

- Cloudflare's 1.1.1.1 and Warp VPN
- Level 3 4.2.2.1
- Google's 8.8.8.8
- Quad9 9.9.9.9
- Cisco's OpenDNS 208.67.222.222
- Norton DNS 199.85.126.20
- Yandex DNS 77.88.8.7
- Comodo DNS 8.26.56.26

> "These (new) technologies can sense malware and block it from operating, or quarantine an app that has too many permissions or that connects to known bad command and control websites."

Summary

Understanding the scope and effect of mobile malware attacks can be daunting. This is because there are so many places where malware can find its way into your phone or tablet and wreak havoc on your business network. Studying past patterns of attacks and understanding the various defensive measures at your disposal can help make your organization more secure. To improve your mobile security, get started with Cyber Security Solution from Network Solutions today.

About Us

Network Solutions is the expert in domains. In 1993, Network Solutions was the sole company registering the .com, .net, .org and .edu extensions. Since then, we've been an active part of the evolution of the Internet and our Customer Service team is here to help you succeed online. Whether you're looking for assistance, insight, resources or answers, we'll be glad to provide the solutions you need.

End Notes

A HISTORY OF MOBILE MALWARE

1 https://www.sophos.com/en-us/medialibrary/PDFs/marketing%20material/sophos-threat-infographic-ten-years-malware-mobile-devices.pdf?la=en

2 https://corrata.com/why-google-and-apples-malware-protection-might-not-be-good-enough-part-1/

3 https://blog.avast.com/flashlight-apps-on-google-play-request-up-to-77-permissions-avast-finds

4 https://blog.checkpoint.com/2017/07/06/how-the-copycat-malware-infected-android-devices-around-the-world/

5 https://blog.lookout.com/dresscode

6 https://unit42.paloaltonetworks.com/more-details-on-the-xcodeghost-malware-and-affected-ios-apps/

7 https://hotforsecurity.bitdefender.com/blog/text-bomb-crashes-iphones-ipads-macs-and-apple-watches-what-you-need-to-know-23067.html

8 https://www.theguardian.com/technology/2016/apr/18/phone-number-hacker-read-texts-listen-calls-track-you

9 https://securelist.com/wap-billing-trojan-clickers-on-rise/81576/

10 https://www.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html

11 https://krebsonsecurity.com/2020/04/would-you-have-fallen-for-this-phone-scam/

12 https://arstechnica.com/information-technology/2017/02/dozens-of-popular-ios-apps-vulnerable-to-intercept-of-tls-protected-data/

13 https://www.armis.com/blueborne/

14 https://www.ftc.gov/news-events/blogs/business-blog/2018/04/lesson-blu-make-right-privacy-security-calls-when-working

THE RISE OF BYOD

15 https://www.cybereason.com/blog/eventbot-a-new-mobile-banking-trojan-is-born

16 https://www.networkworld.com/article/2172364/review--best-tools-for-mobile-device-management.html?nsdr=true

17 https://www.csoonline.com/article/2133789/five-things-to-consider-for-a-mobile-security-policy.html