intetics
Where software concepts come alive

MOBILE HACKING EXPOSED:

Security Secrets & Solutions

www.intetics.com

There is a lot of uncertainty with regards to viruses on mobile phones and tablets. Malicious software for mobile devices expands in different forms from stealing your credit card details to extorting money for not publishing your photos or location history to public sources. In line with that, numerous famous antivirus companies release multiple products for mobile security. Let's try to get at the heart of the matter and see the real state of things.

What do the mobile OS manufacturers say?

According to the Sydney Morning Herald post from November 2011, "The open source programs manager at Google, Chris DiBona, said anti-virus companies were playing on consumers' fears "to try to sell you protection software" and claimed that the supposed mobile phone malware problem was a bogus scare campaign created by the security software companies."

In 2014, Adrian Ludwig, the lead engineer for Android security at Google repeated the same idea. "I don't think 99 per cent plus users even get a benefit from [anti-virus]. There's certainly no reason that they need to install something in addition to [the security we provide]. If I were to be in a line of work where I need that type of protection it would make sense for me to do that. [But] do I think the average user on Android needs to install [anti-virus]? Absolutely not."

We didn't find similar claims from Apple which could be considered as their official position, but in March 2015 they simply expelled antivirus software from the iOS AppStore (see the reports from 9to5Mac and The Register) which proves their confidence in the strength of iOS and the uselessness of mobile antivirus software.

How viruses can penetrate my phone?

It's logical that every manufacturer praises the products they sell but we can't always take their word for it. Let's try to understand how viruses can trick mobile OS's numerous security barriers and get inside.

The first thing that we need to clarify is what viruses are. It is "A computer virus is a type of malicious software program ("malware") that, when executed, replicates itself by modifying other computer programs and inserting its own code." From this definition we can learn two things:

1. Usually we call all of them "viruses" but viruses are just a kind of malware;
2. Viruses can replicate themselves while other malware cannot.

It means that if a mobile phone was infected by a virus, then it can infect another phone all by itself, while any other kinds of malware need the user's interaction to get inside the device. Let's think about the ways which malicious code can spread.

Vulnerabilities in mobile operating systems. All programs are written by humans, and humans tend to make mistakes. Steve McConnell, the author of the book "Code Complete," says that the industry average is about 10-20 defects per 1000 lines of code. Keeping in mind

that Android 4.0 had over 1,000,000 lines of code you can imagine how many defects are still uncovered.

Some of the defects can be exploited by hackers to take control of the system. Manufacturers constantly issue patches to fix the holes (that's why it's so important to always install the latest updates), but when someone discovers a new bug they're always ahead of those who then fix them.

The usual way to exploit vulnerabilities is to direct the victim to an infected website or send them a file which is disguised as a picture or document. For example, Komando.com reported in August 2016 about an extremely dangerous exploit. "According to the security researchers, once an iPhone is infected, attackers could turn the device into a "digital spy." The attackers could then use the iPhone's camera and microphone to "snoop on activity in the vicinity of the device," record calls, log messages and texts, and track movement. This exploit chain was uncovered by Lookout and Citizen Lab when UAE human rights defender Ahmed Mansoor's iPhone was targeted with texts containing malicious links. Thankfully, instead of clicking the links, Mansoor forwarded the messages to Citizen Lab researchers." Apple urgently issued a security update to cover the holes which had been used by the exploit.

Malicious applications from trusted sources. What if someone decides to make an application which looks like legitimate software, however has some hidden features like stealing your passwords or bank card numbers?

Both Android and iOS devices have Google Play Store and Apple App Store accordingly as download sources. All applications in the stores are automatically reviewed for the presence of malicious code. You can think that if you don't use 3rd party software repositories you'll be safe. Sounds reasonable but there are still some hidden backdoors that remain:

- A very sophisticated code can trick built-in store malware checkers;
- An application from the store could be free of malicious code at the time when you installed it, but it can download the malicious part later; and
- In a corporate environment you can get an application directly from your company. These applications are never submitted to the stores, thus bypassing their checks.

In order not to be unfounded let's look for some examples.

In September 2015, a new malware for iOS and OS X was found. What was unusual is that the malware didn't target mobile phones directly; instead of this, it infected development tools which were used to create applications for iOS. This means that developers who used the infected environment produced malicious applications unintentionally. These applications were successfully uploaded to the App Store, and Apple's security checkers failed to detect malicious code which had been attached.

A very recent example was revealed in the end of May 2017 by a famous security solutions provider Check Point. 41 applications on Google Play were found to be infected by a malware which generated false clicks on advertisement thus earning money for the intruders.

Malicious applications from untrusted sources. As it follows from the previous section, even official stores aren't fully protected from malware. But using 3rd party repositories is much more dangerous. Let's figure out where these repositories can come from.

iOS doesn't let you install apps from any source except their official App Store. The only way to remove this limitation is called jailbreaking, which is "the process of removing software restrictions imposed by Apple on iOS and tvOS. It does this by using a series of software exploits. Jailbreaking permits root access to iOS, allowing the downloading and installation of additional applications, extensions, and themes that are unavailable through the official Apple App Store."The irony is that jailbreaking uses the same technologies as malware does, so you can only believe that it does only jailbreaking. As for jailbreaking itself, while some people claim that they just want to unlock the full capabilities of their phones, others do it to install cracked applications from 3rd party repositories. Needless to say, you never know what comes with the crack. But the most important thing is that jailbreak allows applications to bypass built-in iOS security barriers thus making cracked applications incomparably more dangerous than relatively harmless malware which works under a common iOS security model.

Android is less strict with their proprietary Google Play Store. If you enable "Unknown sources" in your phone you can download and install any software package with no hassle including the cracked ones. Some applications still require more permissions than Android allows, that's why you may wish to root your device – similar to jailbreaking on iOS with the same security outcome.

Untrusted networks. Have you ever thought why sometimes you get warned before connecting to open Wi-Fi networks? As it follows from the word "open", traffic between you and Wi-Fi hotspots in such networks is not encrypted. Having a laptop and a basic skillset, anyone sitting at the next table can read everything which goes in and out of your phone. It doesn't make the phone vulnerable directly but could potentially reveal your passwords thus making it easier to inject malware into your personal accounts on the web, especially if you use the same password everywhere.

In order not to exaggerate the danger, we don't think it's a big threat nowadays as all popular mail, social and banking websites tend to already be switched to HTTPS – encrypted protocol which eliminates the need of additional security layer between you and a hotspot. But God saves man who saves himself, so using VPN over public networks still could be a wise idea. Another kind of attack which can be done from public networks (no matter open or encrypted) is a direct injection of malware via vulnerabilities in mobile OSs. While it was a headache for the desktop Windows family (remember notorious Blaster/Lovesan and their successors), we haven't found any trustworthy evidence that the threat can be related to mobile devices. Nevertheless, it's better to be aware than not, so we'll leave the choice of using public networks to you.

Malicious hardware. At a Black Hat conference in July 2013, three hackers presented a device which they called "Mactans" - a small computer that looked like a common charger. As soon as you plug your iPhone into it to refill the battery, it starts to crack it. Mactans needs only about a minute to replace the FaceBook application with the crafted one which can take screenshots and simulate screen touch events as well as hardware button presses. As they said, "Although we deliberately chose to implement weaker payloads as in our proof-of-concept, it is ot inconceivable that adversaries could easily engineer a payload with a substantially higherpact."

This vulnerability was quickly patched by Apple but Mactans clearly proved the idea that your phone can be hijacked if you use chargers in public places or simply leave it unattended.

Antiviruses for mobile operation systems

By this moment you're probably already quite scared and thinking about antivirus? Let's look at what famous security providers can offer for your peace of mind.

Apple iOS. As it was told at the beginning, two years ago Apple removed antivirus solutions from the App Store; however, a Google search on "iOS antivirus" returns lots of results with links to some major players.

Avast offers password manager, Call Blocker, Wi-Fi Finder and VPN. You can hardly consider it all an antivirus solution.

Avira protects your photos and videos by password, locates missing or stolen devices, checks contact identities and encrypts connection via VPN. Not a real antivirus.

TrendMicro guards against phishing, backs up contacts, provides a secure browser, blocks advertising trackers from collecting your data, etc. Still not an antivirus.

Sophos sheds more light on it. As they say, "Apple's iOS development model doesn't allow the sort of interaction with the operating system that we'd need to build an effective anti-virus program. In particular, to qualify for the App Store, an app is limited to its own sandbox, where it isn't supposed to be able to read or interfere with other apps, or to sidestep Apple's commercial controls. That makes it impossible for an anti-virus to analyze other apps, or to hook into the operating system itself to scan files after they are downloaded but before they are used." This makes further investigations here a bit senseless, so let's move on to Android.

Google Android. Quick search returns a number of antivirus applications: AVG, Avast, Bitdefender, McAfee, Kaspersky, Sophos, Norton, Trend Micro, Avira and some other from less famous software manufactures. According to what their producers say, they offer real-time protection and offline scanning which makes them true antiviruses. You can even compare them and choose the best one based on AV-TEST Institute reports where they check the capabilities of antivirus software on real malware samples.

Here you can see top Mobile Antiviruses according to latest research by Independent IT-Security Institute (Magdeburg):

AhnLab V3 Mobile Security	100%	100%
Antiy AVL	100%	100%
Avast Mobile Security	99.5%	99.9%
Bitdefender Mobile Security	100%	100%
Cheetah Mobile CM Security	100%	100%
G Data Internet Security	100%	100%
Kaspersky Lab Internet Security	99.8%	99.9%
McAfee Mobile Security	99.9%	100%
Norton Mobile Security	100%	100%
Sophos Mobile Security	100%	100%
Tencent WeSecure	100%	100%
Trend Micro Mobile Security	99.9%	100%

Conclusions and recommendations

Despite boastful and self-confident declarations of mobile OS manufacturers, it's clear that the threat of malware should not be underestimated. No one knows how many vulnerabilities in the mobile OSs remain undisclosed and are exploited by intruders and governments. Here we compiled a list of simple recommendations which everyone can follow for their safety:

- Never install applications from untrusted sources;
- Don't click on suspicious links even if they've come from your friends. Remember that their accounts could've been hijacked to distribute malware;
- Avoid applications from unknown publishers with low counts of downloads;
- Carefully read which permissions an application is asking for. If a calculator wants to have access to your contacts, camera and microphone, you should probably avoid it;
- Don't root or jailbreak your phone;
- Protect it with a PIN, a password or a fingerprint;
- Don't leave it unattended;
- Avoid usage of untrusted networks; and
- If you own an Android phone, install an antivirus.

About Intetics

Intetics is a leading global technology company focused on creation and operation of distributed professional teams for custom software development, software testing, systems integration, and data processing. Intetics is the pioneer of Offshore Dedicated Teams and the inventor of Remote In-Sourcing, which allows clients to create their ideal IT teams most efficiently. Intetics has broad industry experience, deep software engineering expertise, an outstanding quality management platform and an unparalleled methodology for talent recruitment, team building and talent retention that guarantee that clients receive exceptional results for their software applications and data processing projects. At Intetics, our outcomes do not just meet clients' expectations, they have been exceeding them for our two decades in business.

Intetics is ISO 9001 (quality) and ISO 27001 (security) certified and Microsoft and Oracle Gold Partner. The company's innovation and growth achievements are reflected in winning prestigious Inc 5000, Software 500, Chicago Innovation, CRN 100, Deloitte Technology Fast 50, European IT Excellence and Best European BPO awards, and inclusion into Top 100 Global Service Providers and Top 100 Outsourcing Companies lists.