BLUE COAT SYSTEMS
2015 MOBILE MALWARE REPORT
Executive Summary

The broad acceptance of BYOD in the workplace has long produced anxiety that the mobile platform is the next great exploit opportunity for hackers. In addition, organizations are rapidly adopting cloud-based, mobile versions of enterprise applications such as Salesforce.com, potentially opening up another avenue for attackers. The recent actions by Apple to pull several products from its App Store over concerns they could comprise users’ personal and sensitive information highlights yet another potential risk.

A look back at the majority of the year 2015 shows those worries are not unfounded, although not necessarily in the way initially predicted. While 2015 did not show a sharp rise in the volume of malware, what is alarming is the increasingly insidious and malicious nature of the types of malware and attacks. From the increasing instances of ransomware – essentially cyber blackmail – to the stealthy insertion of spyware on devices that allow cyber criminals to profile behavior and manipulate sales, these are just some of the examples that seem to be the favored exploits of today’s mobile platform.

This report describes the latest trends and vulnerabilities in mobile malware, provides advice for strengthening corporate defenses and educating mobile device users, and offers predictions about the future of mobile threats.
Introduction – The Sky Is Not Falling – But Putting on a Helmet isn’t a Bad Idea

Mobile malware has worried people for years. As mobile devices, whether smartphones, smart watches or tablets, steadily infiltrate more facets of our daily lives, we must assume the bad guys will figure out how to write sophisticated malware for these devices and wreak havoc with our digital world. And we can’t forget about the multitude of devices still to come as the Internet of Things (IoT) trend continues to grow.

While there is a lot more mobile malware these days, strictly by count of unique malware samples, the average mobile user is still rarely affected by malware.

In Blue Coat’s first Mobile Malware Report (2013), we listed several key takeaways that are still true today:

1. A high percentage of mobile threats are still mischiefware – attacks have not yet broken the device’s security model.
2. The most successful mobile malware tactics – including scams, spam, and phishing – are classics, typically device-agnostic, easy-to-deploy attacks.
3. Pornography continues to be the great weakness for mobile users.
4. The mobile threat landscape is becoming more active.

Many of these points are driven home in the 2015 Verizon Data Breach Investigation Report (DBIR) in its section on mobile malware, titled: “I Got 99 Problems and Mobile Malware Isn’t Even 1% of Them”.

The Plague of “Potentially Unwanted Software”

What Verizon terms “adnoyance-ware” – and what others in the security industry call “Potentially Unwanted Applications” or “Unwanted Programs” – we call “Potentially Unwanted Software” or PUS. Generally, this class of program exhibits behavior typical of “adware” or “spyware” — spying on your on-line activity and your personal data – or serving you extra ads (Hey, who doesn’t want to see more ads?).

“Adware is malware with a legal team” – Twitter meme

We’ve seen a major shift in the volume of such software in the traditional malware space – and this is also true of the mobile space – as the number of junk mobile apps hosted on sites we classify in this category has been rising steadily. This type of mobile app, notable for its dubious utility, frequently finds its way onto a mobile device through the use of deceptive advertising, or other social engineering attacks designed to deceive the victim into installing the unwanted program.

Increasingly, we’re seeing the companies behind these apps employ a number of methods cribbed from truly malicious mobile malware, such as the “scareware” attack examples shown in this section. Here, the PUS applications pose as useful or valuable tools, such as fake antivirus software as illustrated by the following examples:

The page at http://com-20.mobi says:

Generic Android Tablet Security Alert!

The last website you visited might have infected your device with a virus.

Press OK to begin the repair process.

OK
Another technique used both by malware criminals and PUS-hustlers is the use of randomization technology to generate unique PUS programs. Each time a victim requests a copy of the application from the page where it is hosted, the server triggers a “generator” to build a file that shares 99% of the same code as its siblings, but has tiny variations in the form of garbage data placed in innocuous locations within the file itself. Using a technique borrowed from the PC virus world, bad actors generate unique “polymorphic” binary files designed specifically to bypass signature-based detection mechanisms and thwart research attempts. Automated app-packaging frameworks are becoming available, leading to an increase in this technique.

As a result, many antivirus scanners have a difficult time identifying these apps right away, as the app’s true nature does not reveal itself unless someone runs each variant in a sandbox separately and observes its actual behavior.

So, while there are relatively few unique PUS applications, there are potentially millions of variants of each. That makes it hard to get a handle on the overall count of PUS applications and how their number compares to the total volume of mobile malware apps in the wild at any given point in time.
One way to count the number of PUS-infected mobile devices is to look at web traffic in which the communicating device identifies itself as “Android” in its User-Agent and “reached out” to a site or domain known to be used for hosting PUS content.

Depending on the access permissions you grant, PUS might use your SMS messaging mechanism against you – signing your phone up for a plethora of junk that costs you real money each month – or it might siphon off the data in your contact list and send it out to unknown parties.

The silver lining to these gray clouds is that PUS does not steal your credit card numbers, your email, or your banking credentials, and it won’t encrypt files on your phone or tablet and hold them for ransom.

That said, PUS does need a “payday” – that’s its primary purpose in life – and that payday usually comes in the form of the “license” you grant it, to use whatever features it claims to be able to perform.

Ransomware: Truly Evil Malware

The world of mobile ransomware has grown dramatically over the past year. While some varieties that run on Android devices cause little damage beyond convincing victims to pay the cyber hostage-taker, many have adopted more sophisticated approaches common to ransomware in the Windows environment.

With the increased performance capabilities of modern smartphones, it was only a matter of time before more advanced cryptographic ransomware, such as SimpleLocker, started showing up on mobile devices. These insidious threats render music files, photographs, videos, and other document types unreadable – while typically demanding an untraceable form of payment such as Bitcoin – and employing a strict time limit for payment before the files become permanently inaccessible to the owner. As shown in the screenshot of Android’s activity logs below, SimpleLocker runs continuously until it has encrypted all the user’s documents, then it issues the demand for payment.

The techniques employed by some forms of mobile ransomware seem to have paralleled the behaviors exhibited by the explosion of ransomware on traditional desktop and laptop PCs. More advanced cryptographic ransomware has abandoned the use of a static encryption key embedded within the malware sample itself, and instead uses a more sophisticated method whereby the malware generates a key that’s unique to an individual victim’s infected device, making it far more difficult – if not impossible – to recover hijacked files. Some even use “real” (AES) encryption that is nearly unbreakable – even for experts – in the small window of time permitted by the attacker before the data is effectively destroyed.
Creators of mobile ransomware are also taking advantage of the Tor anonymity network to obscure the real destination of the ransom payment. It’s not uncommon to see “.onion” addresses used in ransom demands. Victims have very little time to get up to speed on the intricacies of Tor before the deadline to pay clicks away and their precious files are lost forever.

Like other mobile malware, ransomware doesn’t just jump onto your phone by itself. Much of the damage is often self-inflicted. Users seek out and install pirated, or otherwise shady, mobile apps, which are generally only available from unsavory websites or unsanctioned app stores. By the time they realize they’ve been hit with ransomware, the damage is already done.
Browsing for naughty stuff plays perfectly into the ransomware pitch, feeding on the victim’s fear of getting caught by law enforcement, IT, or their spouse/significant other. It is likely that victims of ransomware obtained through porn apps would be far less likely to take their mobile device to IT – or to any other knowledgeable expert source – for help in removing the embarrassing malware. Instead, these victims are more likely to simply pay the ransom and hope that the problem goes away. Unfortunately, many victims have learned the hard way that simply paying a nameless and faceless cyber-criminal does not always ensure that the other end of the bargain will actually be upheld.

Information Leakage

While some people regard their mobile phone as a status symbol – How do you know when somebody gets a new iPhone? They tell you! – there’s plenty more that a mobile device can say about them and their habits, often unknown to the device’s owner. Most people are unaware that apps on their mobile device may be watching them – and reporting out – on a 24x7x365 basis, almost as intently as they might be concentrating on whatever addictive game or hilarious cat video they’re engaged in at the time.

This information leakage is usually a minor drip, showing the version of their phone’s operating system, the manufacturer, the specific app or browser being used, and similar information. Ideally this data would all be encrypted, but many app designers either do it wrong or don’t bother with encryption at all. Making matters worse, there are no included system tools available for casual users to see or know what data is going out of their devices.

Leaky data is often openly revealed in the “User Agent” string, whether on Android...

```
Mozia8.0.0.0; mac. U; Android 4.0.1; en-us; T900 Build/MM760; AppleWebkit/534.30
Mozia8.0.0.0; mac. U; Android 4.0.1; zh-cn; E966 Build/GRK05F; AppleWebKit/533.1
Mozia8.0.0.0; mac. U; Android 4.0.4; en-us; VR999 USA Cricket Build/MM760; AppleWebKit
Mozia8.0.0.0; mac. U; Android 4.1.2; de-de; HTC One Build/U3545K; AppleWebKit/534
Mozia8.0.0.0; mac. U; Android 4.1.2; en-us; GT-N7000 Build/MM760; AppleWebkit/534
Mozia8.0.0.0; mac. U; Android 4.1.2; en-us; HTC Sensation XE with Beats Audio/7715a
Mozia8.0.0.0; mac. U; Android 4.2.2; pt-br; GT-R8655 Build/U3929f; AppleWebkit/534
Mozia8.0.0.0; mac. U; Android 4.4.2; en-us; SAMSUNG-SM-G900A Build/KOT49H; AppleWebkit
Mozia8.0.0.0; mac. U; Android 4.4.2; SAMSUNG-I9505 Build/U3545K; AppleWebKit/534
Mozia8.0.0.0; mac. U; Android 4.4.2; en-us; M966 Build/MM760; AppleWebKit/534
Mozia8.0.0.0; mac. U; Android 4.4.2; en-us; SAMSUNG-I9505 Build/U3545K; AppleWebkit
Mozia8.0.0.0; mac. U; Android 4.5.3; en-us; IdeaTab A1070A H Build/M74A; AppleWebkit
Mozia8.0.0.0; mac. U; Android 4.5.3; en-us; GoogleAnalytics/1.2; Linux; U; Android 2.3.7; en-us; HTC Vision Build/G9440
Mozia8.0.0.0; mac. U; Android 4.0.4; en-us; A13-MD Build/MM760; AppleWebKit/534
Mozia8.0.0.0; mac. U; Android 4.2.2; en-us; GT-R9650 Build/U3929f; AppleWebkit/534
Mozia8.0.0.0; mac. U; Android 4.2.2; en-us; SGN-MM19 Build/KOT49H; AppleWebkit/534
Mozia8.0.0.0; mac. U; Android 4.0.4; en-us; M966 Build/MM760; AppleWebKit/534
Mozia8.0.0.0; mac. U; Android 4.0.4; zh-tw; TXY90 Build/9.7.54; AppleWebKit/534
Mozia8.0.0.0; mac. U; Android 4.0.3; en-us; TM-7538H Build/M74K; AppleWebKit/534
Mozia8.0.0.0; mac. U; Android 4.2.2; en-us; GT-R9650 Build/KOT49H; AppleWebkit/534
Mozia8.0.0.0; mac. U; Android 4.3; en-us; Nexus 4 Build/KXR61Y; AppleWebkit/534
Mozia8.0.0.0; mac. U; Android 4.1.2; en-us; HTCONE Build/U3545K; AppleWebkit/534
```
...or on an iPhone:

Internet-connected apps typically transmit this information with every web request – and it is considered to be normal traffic – but at the same time, it is visible to anyone who is monitoring the network, including Wi-Fi environments. Such queries may also dribble out as a result of advertising code, serving up ads that are appropriate to the mobile environment being used.

Sometimes, instead of “dripping,” information may be gushing out. Data from smartphone apps may be deliberately transmitted back to the app-creator – or leaked to advertisers, web statistics firms, or other unknown third parties – to be used for measuring performance or tracking down bugs in games. Analytics tools built into apps can provide click-by-click or touch-by-touch tracking of how users interact with the app, but they can also reveal information about a user’s app habits to third parties, all to a detailed degree that many would consider overly intrusive.

On both Android and iOS platforms, there’s another sensitive piece of data that’s being revealed all the time, sometimes as a matter of course. On phones, the International Mobile Equipment Identity (or IMEI) is an identifier that’s even more unique than your phone number. You can always move your SIM card from phone to phone – thereby migrating your phone number from one device to another, unless you get a new SIM that has new phone number associated with it – but the IMEI stays with your phone forever. While precisely identifying the phone itself, the IMEI is no garden-variety serial number. This code uniquely identifies your phone to the mobile network, also revealing it to bad guys. So-called “cloned” phones are simply everyday phones programmed to utilize the same IMEI as another phone currently on the network. Routine leaking of the IMEIs makes it far easier for bad actors to hijack an innocent victim’s phone service – perhaps even a celebrity or a politician – and to intercept calls meant for someone else.
Information leakage can impact privacy. For example, as fitness apps have steadily become more popular – witness the success of Fitbit and Apple Watch as prominent examples – they may also pose an ever-increasing risk to personal privacy. Many of these applications use the GPS or Glonass satellite navigation systems to create digital “breadcrumb trails” detailing the precise path of a bike ride, fun run, or power walk.

In addition, many of these immensely popular apps encourage social networking and friendly online competition, including the detailed sharing of fitness data, trails taken, gyms frequented, and other individual particulars. In doing so, they also readily reveal where we live, work, socialize, and play – showcasing our daily routines. Information leakage is fundamentally different from data theft – in this case a user willingly gives it out – however most of us have no idea of the full extent of this potentially dangerous over-sharing. Take it as serious food for thought the next time a casual online acquaintance invites you into a “weekday warriors” competition using that free fitness app you just downloaded.

**Top Infection Vectors**

On mobile devices, most infections happen by means of social engineering of the end user, where the attacker uses misinformation to convince a victim to install a malicious mobile Trojan horse. That isn’t likely to remain the case. A number of vulnerabilities in Android and iOS were revealed in the past year which may give hostile third parties the ability to force our devices to infect themselves without our willing assistance.

While the two largest mobile operating system makers – Apple and Google – have been working to update their OSes, getting your hands on such an update is not trivial. Mobile phone providers have other considerations they must make before they approve and push down “over-the-air” (OTA) updates, and as a result, many phones older than a year will, probably, never receive another OTA update, rendering them potentially vulnerable to these novel attacks.

One of the most prominent examples is the “Stagefright” vulnerability in Android devices. Named after the operating system’s multimedia rendering component, a vulnerable phone can become compromised with self-installing malware if the victim’s phone simply receives a specially-crafted multimedia (MMS) message. Android users can mitigate the problem by turning off automatic downloads of MMS messages, but the vulnerable OS components continue to reside on millions of handsets that may never get updates.

To study the problem, we looked at anonymized Blue Coat WebPulse data. We identified Android devices by the User-Agent string a device passes during web communication, and found that as the volume of network traffic originating with Android-based mobile devices rises steadily, there has been a larger-than-expected jump in the number Android visitors to websites known to host malware.
Distressingly, it has become obvious that vast numbers of potentially vulnerable mobile devices are still widely used. Versions of Android prior to 4.4 lack some of the mitigation technologies introduced to thwart attacks in later models. There are still significant enough numbers of people running four-year-old Android “Gingerbread” versions 2.3.4 and 2.3.6 that those extremely vulnerable OSes still show up on our list of the top 20 Android versions that visited a site known to host malware. Your phone doesn’t have to be this old for these kinds of sites to be dangerous, but it sure helps the criminals.

It has also become apparent that the only reason the mobile platforms of the world have not been targeted more thoroughly or more aggressively is probably due to numbers: While there are more unpatched, vulnerable mobile devices in existence than ever before, there are still larger quantities of more readily-infectable PC laptops and desktops out there.

Among the more traditional vectors for mobile threats, the more things change the more they stay the same.

The big news, compared to the top categories of the “infection vectors” in our 2014 report, is that sites hosting pornography are back as the #1 vector, reclaiming the top spot from WebAds, which fell all the way back to #3 (dropping from almost 20% last year to less than 5% this year). These include both malvertising attacks and sites which host Trojan horse apps designed to appeal to porn site visitors.

Porn isn’t just back on top – it’s bigger than ever – jumping from 16.55% (2014) to over 36% this year. That is, when we see a mobile user’s traffic heading to a malicious site, 36% of the time that user is following a link from a porn site. To put this into perspective: when porn led the pack in the 2013 report, it was with a market share of just 22.16%.

Note, however, that the “Suspicious” category also includes WebAd networks that are known to be heavily involved in malware, scams, PUS, and other shady activities – so collectively, WebAds may not have fallen quite as far as it appears.
11

The Suspicious category also includes some of the large networks we track that are set up solely to take users to shady places – namely malnets – where the activity is more at the spam/scam/PUS end of the scale than on the true “malware” side.

With the increased volume of vulnerabilities in the Android platform, it’s also important to keep the phone’s firmware up to date, as well as web browser and messaging apps. For most users, the version of Android installed on the phone when it becomes yours never changes. Such change will depend on the mobile carriers actively releasing updates for both current and older-generation phones.

Tips for Staying Safe

One of our researchers succinctly summed up our thoughts, noting “There is a huge difference between data breach-class mobile malware (which is very rare), and PUS-class malware (which there’s a ton of).” With BYOD becoming the norm in the workplace – and more users carrying a single device for everything – casual personal usage carries with it the growing potential to negatively impact business networks with mobile malware and PUS.

Keeping in mind this important difference, what does it imply about corporate defenses against mobile threats, especially on mixed-use devices that are only on secured networks for a portion of their total usage time?

1. Invest in visibility solutions from trusted security vendors that extend to mobile devices.

2. Enable Guest Wi-Fi with intelligent policies around data access – not including the corporate crown jewels – so that employees and business guests will be encouraged to utilize the protected network most of the time. Overly restrictive policies will motivate users to utilize their own cellular data plans, thus bypassing corporate visibility.

3. Train (or at least warn) your users about the common infection vectors for the threats they’re most likely to encounter:
   - Don’t download apps from unofficial sources
   - Resist the temptation to search for free/cracked versions of popular apps
   - Don’t surf for porn
   - Don’t jailbreak (override the inherent security of) your phone
   - Be wary of connecting to free or unsecured Wi-Fi networks, and pay attention to any warnings you receive if you do.

When a third-party SSL certificate is installed on an Android device (such as in an environment where SSL interception takes place by policy), the OS will periodically warn the end user that the presence of the installed certificate makes such interception possible.

- Use the “press and hold” technique on your phone to reveal the true destination of on-screen links, like shortened URLs or phishing URLs

The Future of Mobile Threats

With no sign of slowing down, the market for mobile devices is booming. Anticipating that millions more of these devices will hit the street in the coming years, we make the following observations and predictions about the future of this trend.

- Mobile payment systems are set to grow, and services including contactless payment methods will incorporate additional security features, such as biometrics or two-factor authentication.

- There are already too many mobile devices vulnerable to a host of threats in use. These devices will almost certainly not receive needed OS updates, and that will drive a market in security solutions that can support both traditional PC and mobile platforms, such as Blue Coat’s K9 tool.

- Mobile carriers and handset makers are already working on plans to fast-track critical OTA updates to vulnerable devices, but the work is slow and it may be some time before this segment of the mobile market matures.

- While mobile malware rarely shows up in a breach investigation, the potential for data breach-class mobile malware can be expected to grow as bandwidth gets faster and accessing larger quantities of data becomes easier. As usage of cloud apps such as Salesforce.com, Box.com and others grow, so too will the motivations of the bad guys. We should look at this “advanced malware” used in Advanced Persistent Threat (APT) attacks or similar data breach situations, and also advanced ransomware, or advanced (rootkit type) spyware – anything that can’t simply recover by rebooting the phone, or even doing a factory reset.