BLUE COAT®

Security Empowers Business

# BLUE COAT SYSTEMS 2014 MOBILE MALWARE REPORT

## A New Look at Old Threats




## Mobile Malware: A New Look at Old Threats

It's ironic that mobile devices have fundamentally changed how we work, live and play, yet the tricks used by cybercriminals to install malware or applications with shady behavior are the same ones that have been used for years. It's true that if it isn't broken, don't fix it.

Despite a significant increase in the number of mobile devices in use, mobile threats are still defined by the types of socially engineered attacks that simply trick the consumer into accepting what the cybercriminal is selling. The Blue Coat Security Lab has yet to see the types of malware that fundamentally break the security model of the phone.

The most prolific mobile threats are spam, poisoned links on social networking sites and rogue apps. The social engineering nature of these threats means that user behavior is key in both identifying where attacks might occur (social networking sites, for example) and understanding how attacks may evolve.

Likewise, the various mobile malware Trojans which are capable of data theft are able to operate over either the mobile phone network or any connected Wi-Fi network. When these applications transmit their information over mobile phone networks, they present a large information gap that is difficult to overcome in a corporate environment.

## Lack of Underground Economy Impacts Mobile Malware

It's hard to argue that the market for mobile computing is overtaking the traditional PC market, which includes both desktops and laptops. According to the research service BI Intelligence, at the end of 2013, six percent of the global population owned a tablet and 22 percent owned smartphones. That compares to 20 percent who own PCs.

Given the proliferation of the devices and the roughly 1.5 billion new ways to steal data, passwords or money, it is, perhaps, surprising that the mobile malware problem isn't more widespread. In part, this relative safety from the mass market malware maelstrom that PC users face results from the lack of a cohesive underground economy.

Over the last several years, mass market malware has developed into a robust, highly functioning, if highly illegal economy. Cybercriminals can purchase exploit kits and even new vulnerabilities on the open (black) market. They can rent botnets, sell the data they steal and are even protected by service-level agreements. Like other market-based economies, the mass market malware economy is subject to the laws of supply and demand. For example, when the Blackhole exploit kit was taken down last year, the price for the Magnitude exploit kit skyrocketed.

In the mobile world, there is nothing resembling the same type of well-developed exploit kit economy. That means there are no readily available exploit kits where the vulnerabilities have been commoditized and made easier to use as there is in the Windows world. As a result, mobile devices still remain largely free of the drive-by downloads that surreptitiously install malware without the consumer ever knowing.

## Stages of a Mobile Attack

The types of mobile attacks that are common are ones that require users to take action – to change their security settings, download an app or otherwise give control of their device to a third-party. This type of social engineering remains the primary way cybercriminals shape user behavior to make unsafe decisions that compromise their device.

Blue Coat does not see a widespread use of exploit kits or methods which do not require user interaction to infect Android devices with malicious APKs. Users are typically prompted heavily, using social engineering techniques, to disable the "trusted market sources" restriction setting within Android that limits the platform's ability to install arbitrary applications from sources other than Google's own market.

We do see a number of malicious apps originating with porn websites that have a mobile component. Many of these sites have a link that allows users to download the app, which in some cases contain malicious SMSbot components buried among the code running the declared APK functions.

We've also seen growth in the number of rogue Android antivirus "products" touted through advertising networks or the use of scripting on mobile websites to promote them via popup windows in the mobile browser. The threat relies on the user's own gullibility to follow fairly complex instructions and make changes to the security profile of their mobile devices that are detrimental to their device.

A tried and true method that has been the bread and butter of mass market malware attacks for years, such as fake anti-virus scams, these types of scams are now being successfully adapted to mobile devices. In a recent attack tracked by the Blue Coat Security Lab, a mobile advertisement was the first step in a four-stage (Figure 1) socially-engineered attack:

- **Stage 1**: Mobile advertisement from legitimate-sounding security.alert.us tells consumer they have a virus and directs them to click the "OK" button to remove
- **Stage 2**: An Android warning then pops up and prompts the user to remove the virus
- **Stage 3**: This is the classic social engineered fake anti-virus scan used to target desktop and laptop users for years, in which a "scan" is performed and returns information about the purported virus, including details about its malicious behavior – in this case stealing passwords and credit card information. It prompts the user to Install App Now.
- **Stage 4**: Once the file is downloaded, the window prompts the user to change the 3rd party app installations in Setting – the feature that prevents app downloads from sites other than the Google Play market that may host shady or malicious apps that haven't been vetted.

ONE IN EVERY FIVE TIMES A USER IS DIRECTED TO MOBILE MALWARE, IT IS THROUGH WEB ADS

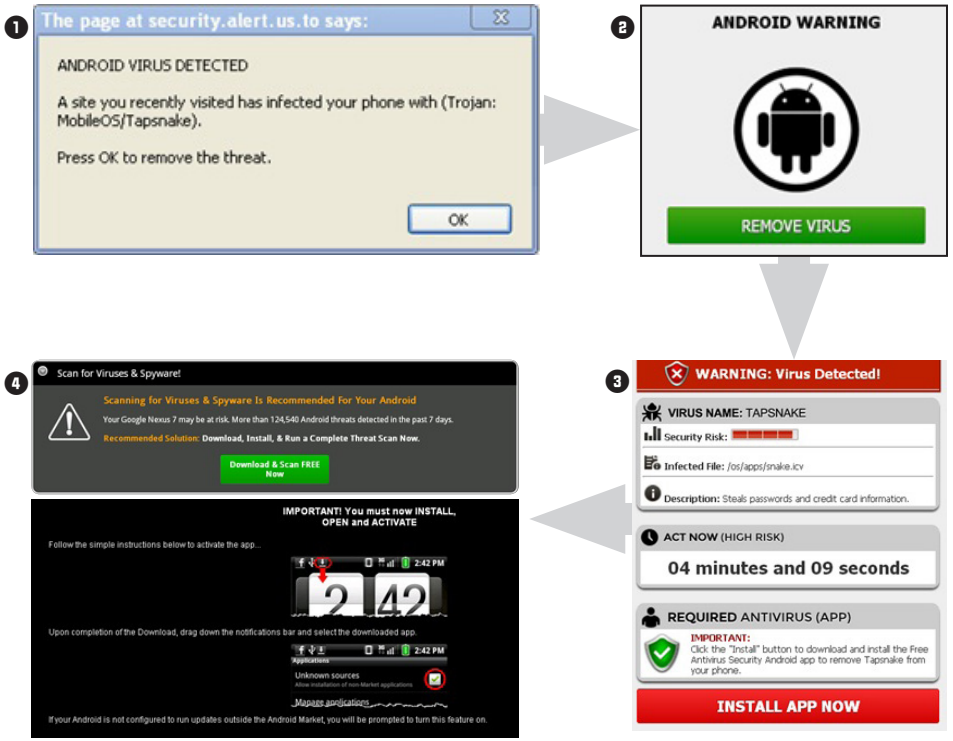



*Figure 1: Mobile advertisement warns about the virus*

## User Behavior Drives Mobile Threats

Understanding how users behave on their mobile devices, then, becomes critical for understanding where they might be at risk.

When we look at consumer behavior on PCs versus behavior on mobile devices, a few key distinctions are stark. First and foremost, social networking continues to decrease as an activity that consumer's engage in on their desktop or laptop computers. Instead, that activity has shifted to mobile devices.

This is representative of the mobile device as part of a consumer's lifestyle. Within the top 15 categories of most requested content, recreation categories (shopping, entertainment, sports/recreation) account for 11.74 percent of all content requested by mobile users. For desktop users, recreational content (shopping, entertainment, games) is just 6.69 percent (Figure 2).

Retailers should pay close attention to this shift in recreational behavior, especially when it comes to shopping. Shopping on mobile devices is the fifth most popular activity, representing more than seven percent of the all mobile activity. As retailers look at next-generation customer experiences – experiences that are more social, local and mobile, this activity will only increase.

Mobile devices open the door for many new opportunities as well, such as targeted coupons while consumers are in the store and click and mortar experiences that unify online and in-store presence. All of these will continue to drive shopping as a category and potentially make it a target for cybercriminals that are looking for popular watering holes to target unsuspecting consumers.

Increasingly, mobile users are being subjected to more ads – even more so than PC users – as sites everywhere continue to refine their mobile advertisement strategies.

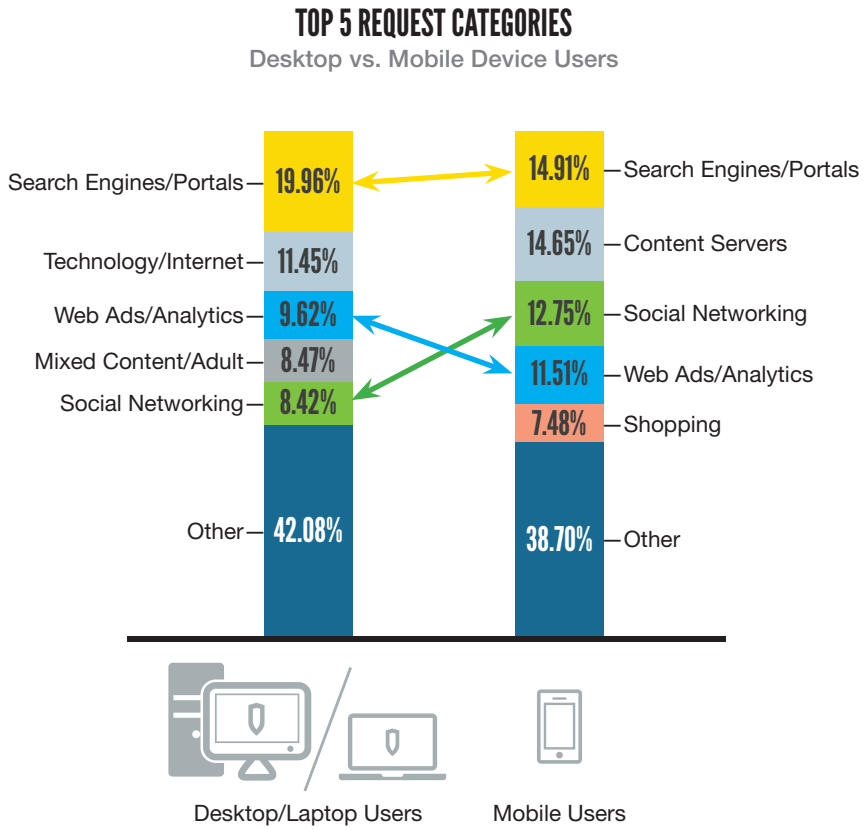



*Figure 2: Comparing requests between computer and mobile device users*

This is a particularly worrying trend as it coincides with a significant increase in malvertising.

While mobile users are not yet subject to the same drive-by downloads that PC users face, mobile ads are increasingly being used as part of many socially engineering attacks (as seen in our example above). The increased frequency of mobile ads conditions users to see them as normal, which makes users more vulnerable to the attacks that are launched through ads.

One of the clearest differences the behaviors of PC and mobile users also shows why this matters: For PC users, viewing audio/video clips represents more than 7 percent of all Internet activity. For mobile users, that number is just over one percent. It's not that mobile users aren't watching video clips, it's that they are doing it through branded video apps like YouTube and Hulu.

As a result of this preference for video viewing the fake video codec attacks that were very common on PCs five years ago are not something the Blue Coat Security Lab sees transferring to mobile devices.

## Best Practice

Avoid clicking on ads on your mobile device

# THE LACK OF TRANSPARENCY INTO AN APP'S BEHAVIOR SETS USERS UP TO FAIL BY PUTTING THEM AT GREATER RISK FOR PRIVACY VIOLATIONS

## Malvertising Overtakes Porn as Leading Threat Vector

Often times the Internet is a much different place on the mobile device. Smaller screens and more difficult text entry methods have changed how we access and view online content. So it's not surprising that it also changes how we are exposed to malicious content.

For desktop users, search engine poisoning and email links are by far the most prevalent vectors that drive users to threats or malicious content. When we look at mobile users, however, we see a much different picture. Search engines barely crack the top 10 – sending unsuspecting users to malware only 3.13 percent of the time.

Web ads, on the other hand, have outperformed even pornography. In February 2014, web ads represented the single biggest threat vector for mobile users – one in every five times a user is directed to mobile malware, it is through web ads. That is almost triple the rate in November 2012.

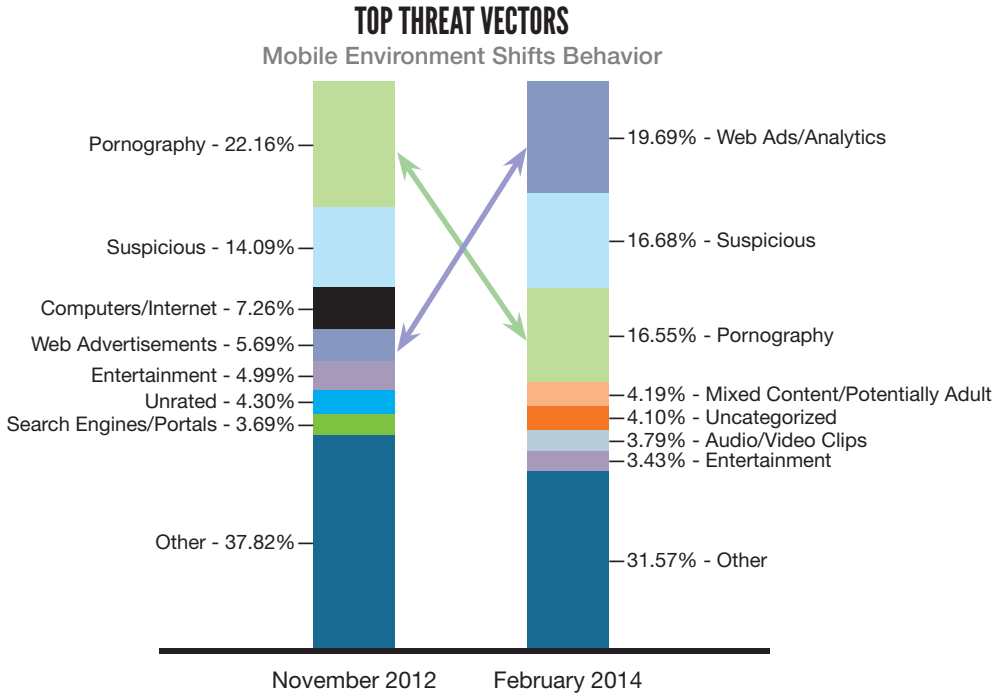



*Figure 3: Shift in behavior for mobile users*

The rise of malvertising – web ads delivered through legitimate ad networks that direct users to malicious sites or contain malicious code – as a leading attack vector mimics the rise of web ad traffic on mobile devices. This is a largely unregulated network of ad servers that can easily be tricked into serving malicious ads unknowingly.

What a difference a year makes. Last year, when Blue Coat Security Labs looked at the mobile malware landscape, pornography was the leading threat vector for mobile users. This year, it has dropped nearly six points and is the third leading threat vector, responsible to driving users to malware 16 percent of the time (Figure 3).

However, pornography remains the most dangerous category of content for mobile users. With web ads, the rise as a threat vector correlated with a rise in web ad requests. The story is different for pornography. Requests for pornography on mobile devices don't even reach one percent of all requested content, yet it accounts for more than 16 percent of all attacks. While users don't access pornography that frequently, when they do, they are very vulnerable to malware.

### Best Practices

- Avoid pornography on your mobile devices
- Consider blocking web ads as a category of content

## Mobile Malnets: Trial and Error

The Blue Coat Security Lab has yet to see any real commitment to mobile malware among the top malnets it is tracking. Shnakule, which consistently ranks as the world's largest malnet, dabbles in mobile malware, with a preference for premium SMS texting scams. Much smaller malnets (too small to even be named) pop up from time to time. It could be that the behavior we are seeing among malnets is an attempt to find vulnerabilities and adapt the infrastructures to these mobile environments.

Malnets are the infrastructures used to drive users to malware through a series of relay and exploit servers. The components are reused in multiple attacks, allowing cybercriminals to quickly launch new attacks.

## Application Overshare: Potentially Unwanted Applications and the Threat to Privacy

The malware threats targeting mobile devices are still pretty basic – largely confined to potentially unwanted applications and premium SMS scams.

Potentially unwanted applications, or PUAs, are simply apps, usually disguised as something interesting like the hottest mobile game, that engage in tracking user behavior or otherwise sharing personal information.

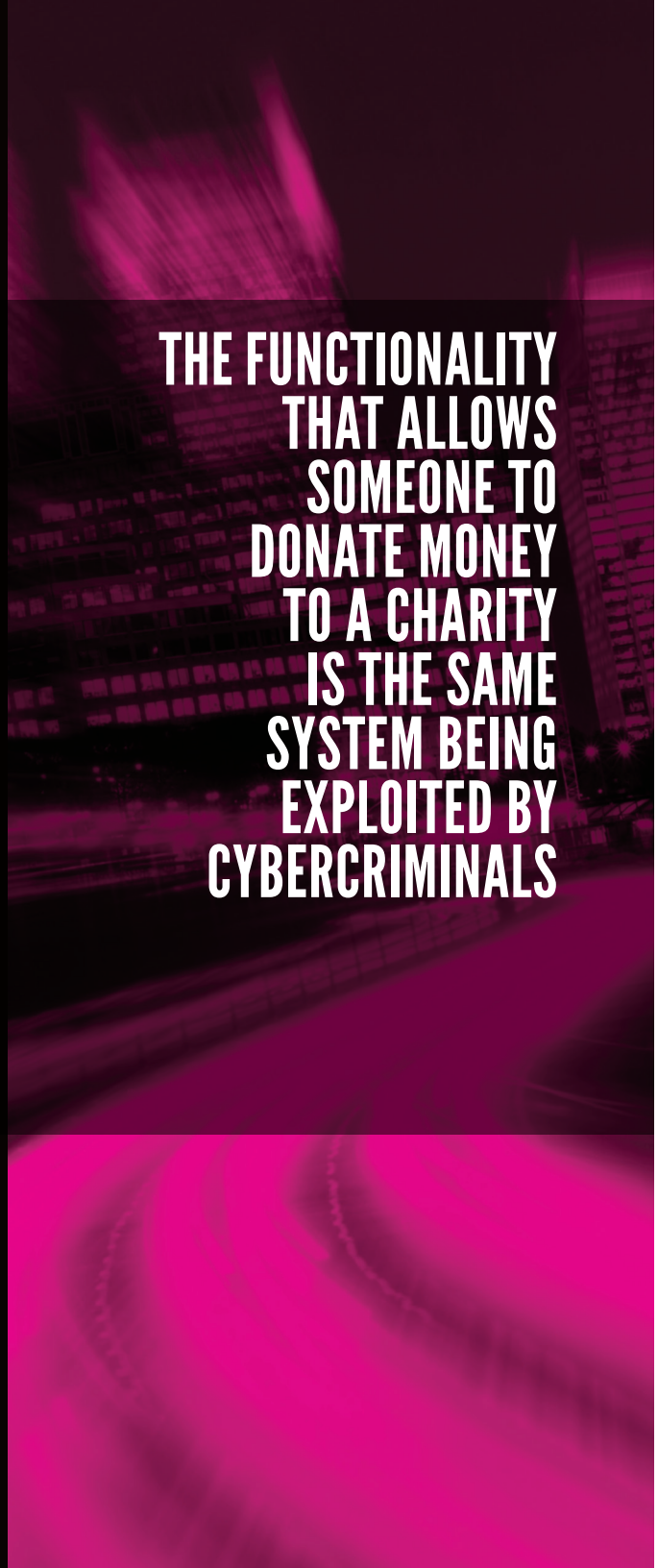
Among the type of data that is tracked are User-Agent strings, which identify the mobile operating system, its version, the type of installed browser and version, and (depending on the app) additional information about the mobile app the user is running. In addition, HTTP traffic generated by the mobile device's browser or by mobile advertising services may reveal the mobile device user's habits, interests, or searches.

Many apps also include embedded analytics tools used to identify bugs or simply report on app usage. These tools can disclose the mobile device's telephone number, the SIM card's unique IMEI code, and may reveal the relationships between the device's owner and frequent contacts in the address book.

Analytics tools embedded in apps are also capable, depending on how the developer has configured them, of revealing virtually all aspects of the user's behavior within the app, from key stroke, to "shared" high scores with friends over social media or on online leaderboards.

The majority of this activity is not transparent to the user and potentially exposes their data to interception. The lack of clear requirements for developers to explicit identify what data their apps access, log, store and share, which makes it difficult for users to make risk-based decisions about how they use.

The lack of transparency into an app's behavior sets users up to fail by putting them at greater risk for privacy violations. It also makes it impossible for users to make risk-based decisions about the apps they want to use and the information they want to share.




While many potentially unwanted apps appear in legitimate markets, they are typically quick to respond to customer complaints and will remove a known-malicious app from the market. In some cases, the market will also remotely uninstall known-bad apps from the phones of users who downloaded and installed them.

Unfortunately, malicious mobile apps tend to have longer lives in collections of allegedly-pirated mobile software and in foreign app markets or stores where the operators of the market less thoroughly (or don't at all) scrutinize mobile apps before allowing people to post them for others to download.

### Best Practices

- Never download or purchase an app outside of legitimate markets such as the App Store or Google Play.
- Enterprises that have bring your own device or corporate mobility initiatives should look at pre-approving mobile apps that present a lower risk of data leakage or privacy violations. Third-party services are in the early stages of offering risk profiles on applications to help enterprises assess their exposure and balance the risks of using a particular app against the benefits.

## Premium SMS Apps: The New 900 Number Scam

A significant number of Android apps, in particular, engage in premium SMS scams. These apps surreptitiously sign up users for messaging services that charge the victim's mobile phone account a per-use or per-month fee, similar to the old 900 number scams that racked up hundreds and thousands of dollars in bills for unsuspecting callers.

Premium SMS apps have quickly become the most popular piece of Android malware due to the fact that mobile devices have a banking system built into it. The functionality that allows someone to donate money to a charity during a natural disaster is the same system being exploited by cybercriminals. Each SMS text message of $5 or more to a number owned by the cybercriminal is added to your mobile bill.

The SMS text messages are often sent without mobile phone users being able to detect it and could run up hundreds of dollars in charges before the users receives their mobile phone bill.

Most of these malicious apps have some connection with mobile porn sites. Either the sites have links to download a mobile porn app that is really a malicious SMSbot APK or social engineering techniques on a mobile porn site are used to convince a user to download the malicious app.

As a result of the volume of consumer complaints about premium SMS scam applications, some mobile phone service providers are actively working to thwart these scams by giving phone users the ability to block this type of service entirely.

## Summary

Blue Coat predicts that mobile malware will continue to present a threat to users both in the corporate and home environment. The makers of mobile phone operating systems would do well to help users better manage how, when, and with whom mobile applications can communicate with the outside world.

v.BC-2014-MOBILE-MALWARE-REPORT-EN-v1e-0214

BLUE COAT®

Security Empowers Business

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000